

SmartTAP 360° Live

SmartTAP 360° Live Enterprise Recording Solution

Version 5.4

Smart**TAP** 360° Live



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: June-16-2021

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

Related Documentation

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

Document Revision Record

LTRT	Description
27173	<p>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 Announcement; Announcement Server Configuration Parameters; Managing Security Profiles; Announcement 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</p> <p>Added Sections: Saving Search Queries; Deleting Calls and Instant Messages</p> <p>Removed Section: Recording Beep Tones (merged to Section "Editing Media Proxy Server" in the SmartTAP 360° Live Installation Guide)</p>
27174	<p>Updated Sections: Features Overview; About this Guide; Inter-Components Communication; Skype for Business and Teams Video and Screen Sharing; Configuring an LDAP User</p> <p>Added Sections: Adding a Microsoft Teams User Attribute; Microsoft Azure Active Directory; Microsoft Blob Storage</p>
27175	<p>Updated Sections: Step 5 Add Azure Active Directory Mapping in SmartTAP 360° Live; Determining Storage Statistics; Configuring Media</p>
27176	<p>Updated Sections: About SmartTAP; SmartTAP Benefits; Features Overview; Architecture; About this Guide; Logging In; Determining User Device Status; Viewing and Searching an Audit Trail; Targeted User Licenses (Skype for Business); Concurrent Recording Licenses (Skype for Business); Viewing Managed Devices; Monitoring Storage Statistics; Configure Live Monitoring Location; Single Sign-On Client Browser Settings; Troubleshooting Single Sign-on; Managing Recording Profile; Playing Back Recorded Media; Searching for</p>

LTRT	Description
	<p>calls; Recording Health Monitor; General Configuration (Health Monitor); Adding a Microsoft Teams IM Recording Attribute; Skype for Business and Teams Video and Screen Sharing; Announcement Server (Skype for Business); PSTN and Federated Calls; All Inbound Calls; Azure Active Directory User Authentication</p> <p>Added Sections: Microsoft Teams Client Licenses; Managing Microsoft Teams Instant Messages; Managing Microsoft Teams Video Calls; Enabling Microsoft Edge browser with IWA.</p>
27177	Updated Section: Step 2 Configure API Permissions for User Mapping
27179	<p>Updated Sections: About SmartTAP Live; Competitive Advantages; Determining User/Device Status; SmartTAP Architecture; Logging in; Managing Licenses; Alarm Notifications; Alarm History; Windows Event Log; Configuring System Settings; Adding a Recording Location; Configure Live Monitoring Location; Adding a Recording Profile; Managing Instant Messages; AAD User and Group Mapping; AAD Security Profile Mapping; AAD Recording Profile Mapping; AAD Retention Policy Mapping; Viewing and Modifying Users; Step 2 Configure API Permissions; Step 3 Configure Certificates & Secrets for Azure AD Mapping; Step 3 Configure Certificates & Secrets; Configuring OVOC Connection; Configuring an LDAP User; Configuring Group Mappings; View and Modify Groups; Adding a Security Profile; Viewing/Modifying a Security Profile; Recording Profile-Call Type Configuration Examples; Adding a Microsoft Teams AAD User Attribute; Troubleshooting Single Sign-On; REST-API Configuration; Step 5 Assign Security Profile to Azure Active Directory user in SmartTAP 360° Live; Prerequisite - Join Calls in Teams Tenant; Create Application Instance; Create New Compliance Recording Policy; Set Compliance Recording Policy; Grant the Policy to a Recorded User</p> <p>Added Sections: White-listing certificate files; SmartTAP Alarms</p>

Table of Contents

1	About SmartTAP 360° Live	1
	SmartTAP 360° Live Benefits	2
	Competitive Advantages	2
	Features Overview	3
	Architecture	12
	About this Guide	13
2	Logging In	16
	Logging in with Microsoft Office 365 Credentials	16
3	Getting Acquainted with the GUI	19
	Determining User/Device Status	21
4	Performing Initial Configuration	26
5	Testing the Initial Configuration	28
	Making Sure a Recording is in Progress	28
	Listening to a Recording and Viewing a Video	28
6	Configuring Advanced Features	30
	Viewing/Searching an Audit Trail	30
	Exporting an Audit Trail	32
	Managing Licenses	33
	Licenses for Other Integrations	33
	Microsoft Teams Licenses	35
	License Configuration Parameters	38
	Viewing Managed Devices	39
	Inter-Components Communication	42
	Adding a Device Manually to the Application Server	42
	Alarms	43
	Alarm History	43
	Alarm Notifications	44
	Monitoring System Health	46
	Windows Event Log	47
	SCOM Integration	48
	Monitoring Storage Statistics	49
	Using Call Tagging	50
	Adding a Call Tag	51
	Viewing / Deleting a Call Tag	53
	Assigning Values to a Call Tag and Applying to Call	53
	Generating and Loading HTTPS Certificates	54
	Browser Connection Certificate Requirements	54
	Step 1: Generate Certificate Signing Request (CSR)	55
	Viewing/Modifying the Certificate List	57
	Step 2: Load Certificates	59

Loading Web Browser Certificate	59
Loading Digital Files Certificate	60
Configuring Call Retention	64
Save on Demand Call Retention	66
Configuring System Settings	67
Configuring a Digital Signature	67
Configuring Email Server Settings	68
Configuring Media	69
Configuring User Credentials	70
Extracting User Credentials from Microsoft Azure Fileshare Account	73
Setting up Microsoft Azure Blob Storage Account	75
Adding a Recording Location	77
Viewing and Modifying a Recording Location	81
Defining a Recording Format	82
Configure Live Monitoring Location	83
Configuring Single Sign-on	85
Validating SSO	86
Configuring Web Session Timeout	87
Configuring an LDAP Connection	87
Configuring SSL	89
Configuring an LDAP User	91
Configuring User Mappings	91
Configuring Group Mappings	96
Configuring Security Group Mappings	99
Configuring OVOC Connection	101
White Listing Certificate Files	104
Managing Users	106
Sending Email	109
Managing Groups	110
Adding a Group	110
View and Modify Groups	112
Managing Security Profiles	113
Adding a Security Profile	114
Viewing or Modifying a Security Profile	116
Managing Recording Profiles	118
Adding a Recording Profile	119
Viewing or Modifying Recording Profiles	125
Assigning Recording Profile to User or Device	127
Managing Recordable Devices	129
Recording Profile-Call Type Configuration Examples	131
Adding a Device Attribute	133
Adding a General Device Attribute	134
Adding a Device Attribute for Recording	135
Adding a Microsoft Teams AAD User Attribute	136
Adding a User	138

View and Modify Users	140
Update an Admin User	144
Reset User Password	145
Modify a User Password	145
Uploading an Image	146
Managing Calls	147
Searching for Calls	149
Saving Search Queries	159
Deleting Calls and Instant Messages	160
Playing Back Recorded Media	162
Listening to Call and Viewing Call Video	164
Managing Microsoft Teams Video Calls	166
Skype for Business and Teams Video and Screen Sharing	167
Time Line View	169
Downloading Call Recordings	174
Downloading an Audio Call	174
Downloading a Video Call	176
Downloading a Video and Screen Sharing Call	178
Emailing Call Recordings	181
Using the Evaluation Feature	183
Adding a New Evaluation Form	184
Viewing and Copying an Evaluation Form	186
Adding a New Section [Evaluation Forms]	187
Adding Questions and Answers to an Evaluation Form	188
Finalizing Forms	191
Performing an Evaluation	192
Managing Instant Messages	200
Searching for Messages	203
Specific Considerations for Microsoft Teams Instant Messages	210
7 Single Sign-On for SmartTAP 360° Live	212
Single Sign-On Variables	213
Configuring Active Directory for Single Sign-On	216
Single Sign-On Client Browser Settings	218
Enabling Microsoft Edge Browser with IWA	219
Enabling Firefox Browser with IWA	222
Enabling Chrome Browser with IWA	223
Testing Single Sign-On	224
Troubleshooting Single Sign-On	225
8 SmartTAP 360° Live Skype for Business Toolbar	231
Toolbar Features	231
9 Media Exporter	234
10 API Integration	240

11	Recording Health Monitor	242
	General Configuration	242
	REST API Configuration	244
	Report Formats	245
12	Announcement Server (Skype for Business)	247
	Simple Announcement	247
	IVR	248
	Configuring IVR Script Files	248
	Enabling Text-to-Speech Platform	249
	Consent to Record Calls	250
	Example Announcement Server Scenarios	252
	PSTN and Federated Calls	252
	All Inbound Calls	253
	Announcement Server Configuration Parameters	254
	Announcement Server Advanced Call Scenarios	258
13	Microsoft Azure Active Directory	262
	Azure Active Directory User Mapping	262
	Step 1 Application Registration in Microsoft Azure	262
	Step 2 Configure API Permissions	265
	Step 3 Configure Certificates & Secrets for Azure AD Mapping	268
	Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live	270
	Step 5 Add Azure Active Directory Mapping in SmartTAP 360° Live	271
	AAD User and Group Mapping	271
	AAD Security Profile Mapping	277
	AAD Recording Profile Mapping	284
	AAD Retention Policy Mapping	293
	Azure Active Directory User Authentication	300
	Step 1 Register App in Azure Active Directory	300
	Step 2 Check API Permissions	303
	Step 3 Configure Certificates & Secrets	308
	Step 4 Configure OpenID Connect OIDC Client	309
	Step 5 Assign Security Profile to Azure Active Directory user in SmartTAP 360° Live	311
14	Integrate SmartTAP Personal App in Teams	317
	Create and Register the SmartTAP Personal App	317
	Set Microsoft API Permissions for Personal App	320
	Configure Connection with SmartTAP Server	325
	Configure and Upload Manifest	325
15	Enable Users with Compliance Recordings	329
	Prerequisite - Join Calls in Teams Tenant	329
	Create Compliance Recording Policy	330
	Create Application Instance	330
	Create New Compliance Recording Policy	332

Set Compliance Recording Policy	333
Grant the Policy to a Recorded User	335
16 SmartTAP Alarms	337
Alarm – Component Unreachable	337
SmartTAP Event – Component Restart	337
Event – Component Resource Failed	338
Alarm - Component Resource Threshold Exceeded	339
Alarm – Connection Failure	340
Call Recording Error Event	341
Alarm – Certificate Expired	342
Alarm – Component Event Viewer Dropped	342
Alarm – Component Performance Counter General	342
Alarm – Component Service Status	343
Alarm – Disk Space	344
Event – Configuration Error	345
Recording Resource Failure	345

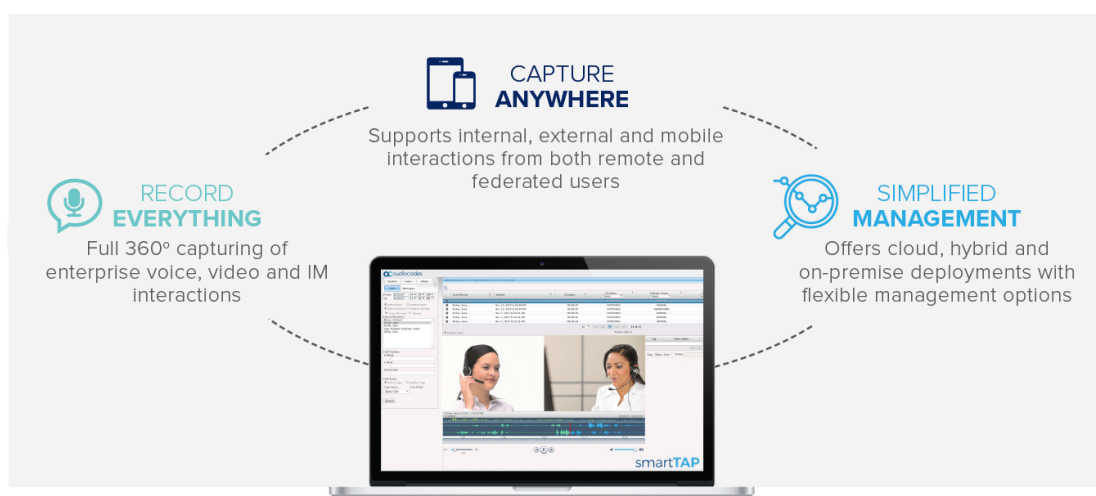
1 About SmartTAP 360° Live

AudioCodes SmartTAP 360° Live is an intelligent, fully-secured enterprise compliance-recording solution, allowing companies to capture and index any customer or organizational interactions across both external and internal communication channels.

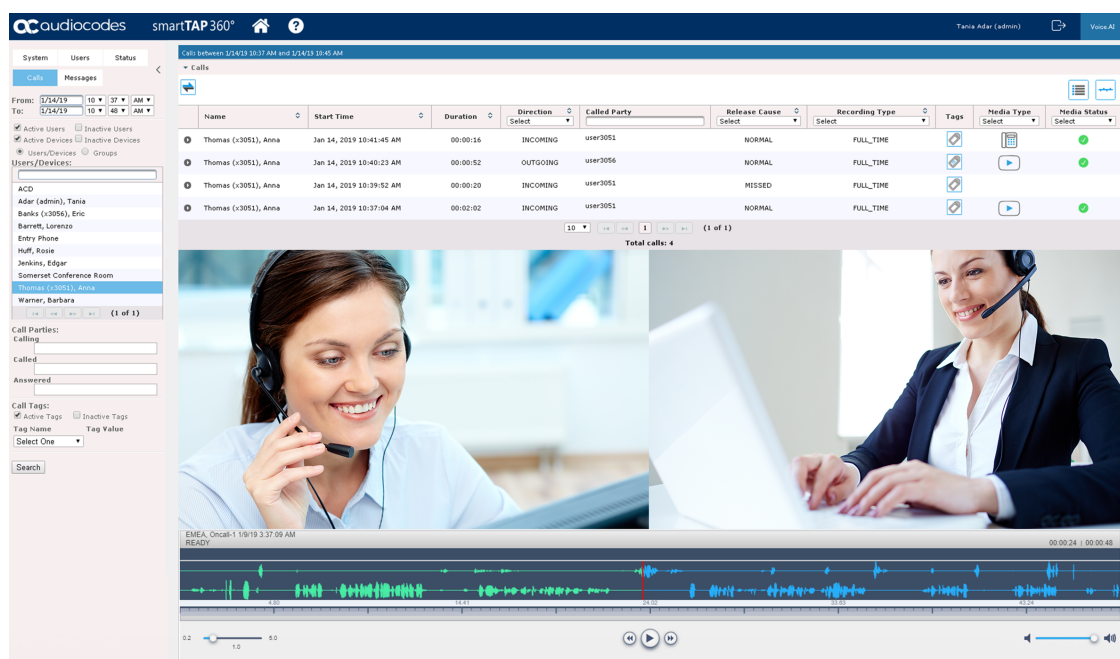
Companies using Microsoft Teams can seamlessly apply SmartTAP 360° Live to record all voice, video and IMs interactions for later-stage AI analysis and for meeting regulatory compliance demands.

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

Figure 1-1: SmartTAP 360° Live Solution



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



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
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° Live Benefits

SmartTAP 360° Live benefits organizations and enterprises as follows:

- Captures corporate interactions including voice, video and instant messages
- 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
- Supports internal, external and mobile interactions from both remote and federated users
- Certified by Microsoft Teams as an On-premises call recording solution for Microsoft Teams customers. The solution has been tested and verified to provide the quality, compatibility, and reliability that organizations and customers expect from Microsoft solutions, backed by best-in-class product maintenance, service operations, and support.
- Compliance-grade recording and regulation-specialized features

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° Live 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 a low number of recordings and scale upwards.
- 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° Live recording features.

Table 1-1: SmartTAP 360° Live Features

Feature	Details
Status Page	<ul style="list-style-type: none"> ■ Displays the current user call status ■ Live Call Monitoring ■ Notes can be added to an active call ■ Allows switching between Grid and List View ■ Pause / Resume Recording ■ Record or Save on Demand
Record or Save on Demand	<ul style="list-style-type: none"> ■ Record on Demand (ROD): Recording contains audio from the point network administrator decides to record the call. ■ Save on Demand (SOD): Recording contains audio from the beginning of the call. ■ Recording using ROD or SOD is manually selected from the GUI or Skype for Business CWE or Microsoft Teams 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.

Feature	Details
PCI Compliance	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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 BusinessConversation 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	<ul style="list-style-type: none"> ■ Can be created and assigned to multiple parties to define security access in SmartTAP 360° Live.
LDAP Integration	<ul style="list-style-type: none"> ■ Allows SmartTAP 360° Live to use Active Directory users, groups, and security groups ■ LDAP Filtering by user, group or security group.
Microsoft Teams Integration	<ul style="list-style-type: none"> ■ Record calls of Targeted Users on different devices, including Teams desktop, web, mobile applications and phones. ■ Record the calls audio, video, instant messaging and screen sharing. ■ Microsoft Azure Active Directory users mapping into SmartTAP 360°Live.
Legal Hold	<ul style="list-style-type: none"> ■ The user's retention process does not purge their recordings when placed on legal hold.

Feature	Details
Audit Trail	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ Fast-forward / Rewind or select playback position controls. ■ Volume control.
Call and Instant Message Retention	<ul style="list-style-type: none"> ■ Number of retention periods can be added and applied to specific user(s). ■ Recordings are automatically deleted based on retention period. ■ Option to retain recordings based on evaluation status.
Automatic Email Notifications	<ul style="list-style-type: none"> ■ Automatic email notifications when Alarms are triggered or thresholds are exceeded (Recording licenses or

Feature	Details
	Storage capacity).
Encryption of Stored Recordings	<ul style="list-style-type: none"> ■ Option to encrypt stored audio recordings.
Recordings Storage in Local Drive, NAS or SAN	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Audio recordings stored as G.711 (normal compression) or G.729a (high compression).
Agent Evaluation	<ul style="list-style-type: none"> ■ Evaluation forms can be created: agents evaluations, review evaluations, and reports can be generated.
Distributed Architecture	<ul style="list-style-type: none"> ■ One SmartTAP 360° Live 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	<ul style="list-style-type: none"> ■ One SmartTAP 360° Live server is capable of recording diverse call signaling and voice protocols. ■ SmartTAP 360° Live records PSTN, Lync, Analog, and VoIP simultaneously and transparently to end users.
Skype for Business Client Toolbar	<ul style="list-style-type: none"> ■ Auto extended Skype for Business CWE for convenient access to features like ROD / SOD, PCI and Call Tagging
Call Tagging	<ul style="list-style-type: none"> ■ 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.
Single Sign-On	<ul style="list-style-type: none"> ■ A user gains access into the SmartTAP 360° Live GUI or Skype for Business client toolbar after validation of their SmartTAP 360° Live security profile and authentication of their credentials with LDAP Active Directory. ■ For Microsoft Team clients: Single Sign-on is supported

Feature	Details
	for logging onto the SmartTAP 360° Live Personal App. Refer to Step 8 Setup SmartTAP Personal App in the <i>SmartTAP 360° Live Deployment Guide</i>
SIPRec	<ul style="list-style-type: none"> ■ Session Initiation Protocol (SIP) establishes an active recording session and reporting of metadata to the SRS (SmartTAP 360° Live) of the active communication session traversing the SRC (AudioCodes SBC or Gateway). ■ https://datatracker.ietf.org/doc/draft-ietf-siprec-protocol/
REST API	<ul style="list-style-type: none"> ■ Allows third-party applications integrated with SmartTAP 360° Live 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	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ✓ Plays announcement to inbound PSTN call participants ✓ Deploys on Physical or Virtual Servers ✓ Supports N+1 Resiliency
SmartTAP 360° Live Media Proxy (Skype for Business)	<ul style="list-style-type: none"> ■ 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° Live to capture a copy of the SRTP conversation.

Feature	Details
	<ul style="list-style-type: none"> ■ Advantages: <ul style="list-style-type: none"> ✓ 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	<p>A SmartTAP 360° Live user or device attribute has three purposes:</p> <ul style="list-style-type: none"> ■ Additional information can be added to the user account within SmartTAP 360° Live, i.e., Ext, Tel URI, Address, etc., for informational purposes only. ■ Designates to SmartTAP 360° Live 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° Live triggers a recording based on the SIP_URI. ■ Mapping Active Directory attributes to user / device information on SmartTAP 360° Live. ■ Mapping Microsoft Azure Active Directory Teams users object ID to user properties on SmartTAP 360° Live.
Automatic Instant Message Recording	<ul style="list-style-type: none"> ■ Recording of instant messages for person-to-person chat between two users or group chat between two or more users.
Video Recording	<ul style="list-style-type: none"> ■ 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	<p>Skype for Business and Microsoft Teams Video and Screen Sharing over VBSS (Video Based Screen Sharing) recording is supported.</p>
Timeline View	<p>View call results data for a specific user/device over a time line. Each call type is represented on the timeline by a</p>

Feature	Details
	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.
New User Interface Design	The SmartTAP 360° Live 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° Live 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° Live Media Proxy.
Test calls in Skype for Business Deployment	Enhanced System Health Monitoring with an option to activate periodic test calls and with alarms.
Communication status icons	SmartTAP 360° Live 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° Live 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° Live Announcement and Application server- 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° Live SIPRec solution scalability enhancement

Feature	Details
	with an option to reroute a call to another recording server when the server is at the maximum capacity.
SmartTAP 360° Live low-end Profile	SmartTAP 360° Live low-end profile system can be deployed on the GX-1KB OSN4B 256 GB SSD alongside the SBA with up to 250 users and 8 trunks.
Multilingual support	<p>The SmartTAP 360° Live interface supports the following languages:</p> <ul style="list-style-type: none"> ■ English ■ German ■ Spanish ■ French
Personal App in Microsoft Teams	SmartTAP 360° Live can be added to Microsoft Teams as a Teams App that includes On-demand recording buttons full application access tab. Once setup can be uploaded to the customer organization's App Store and run on Teams desktop or Teams mobile clients.

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

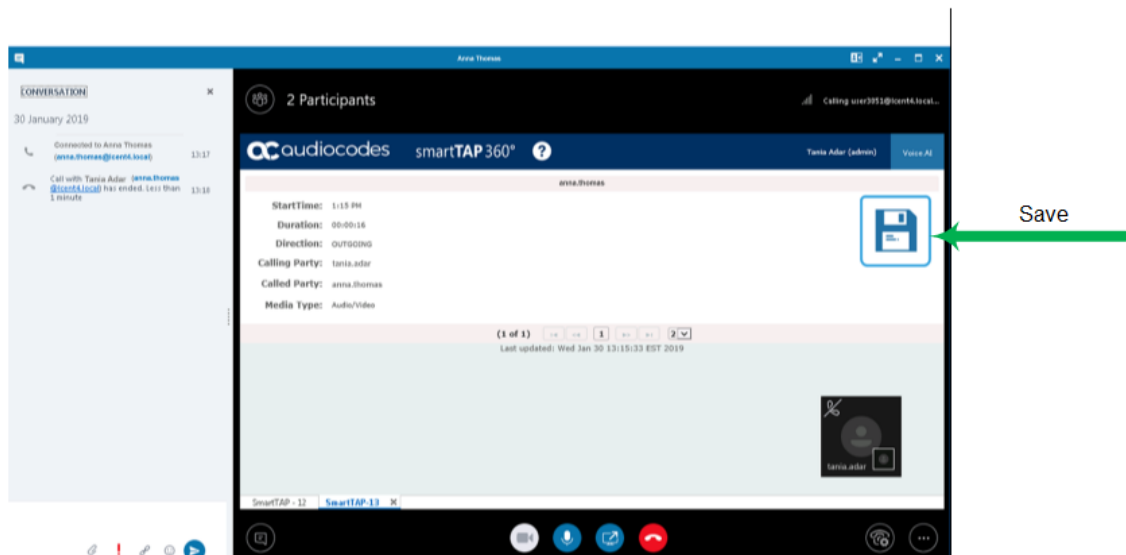


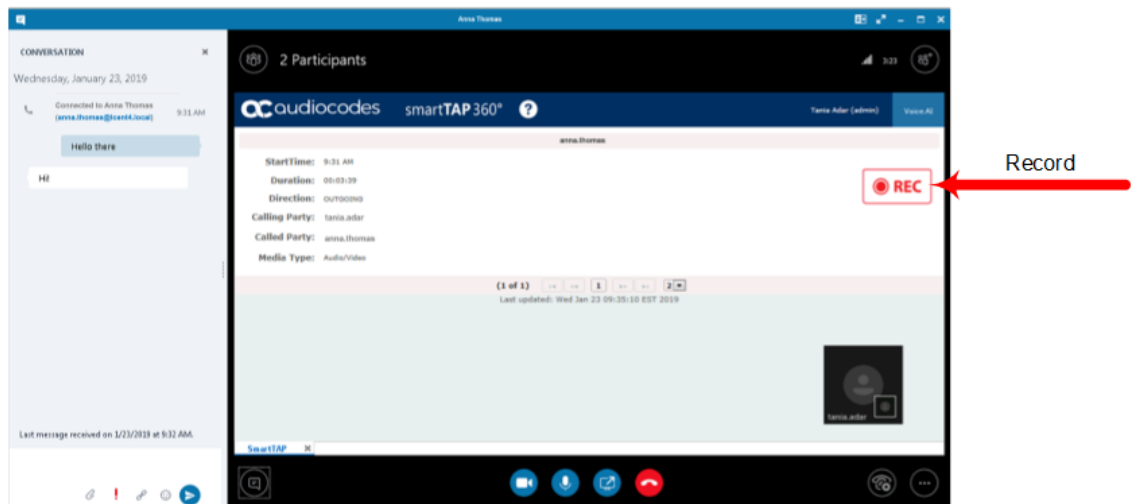
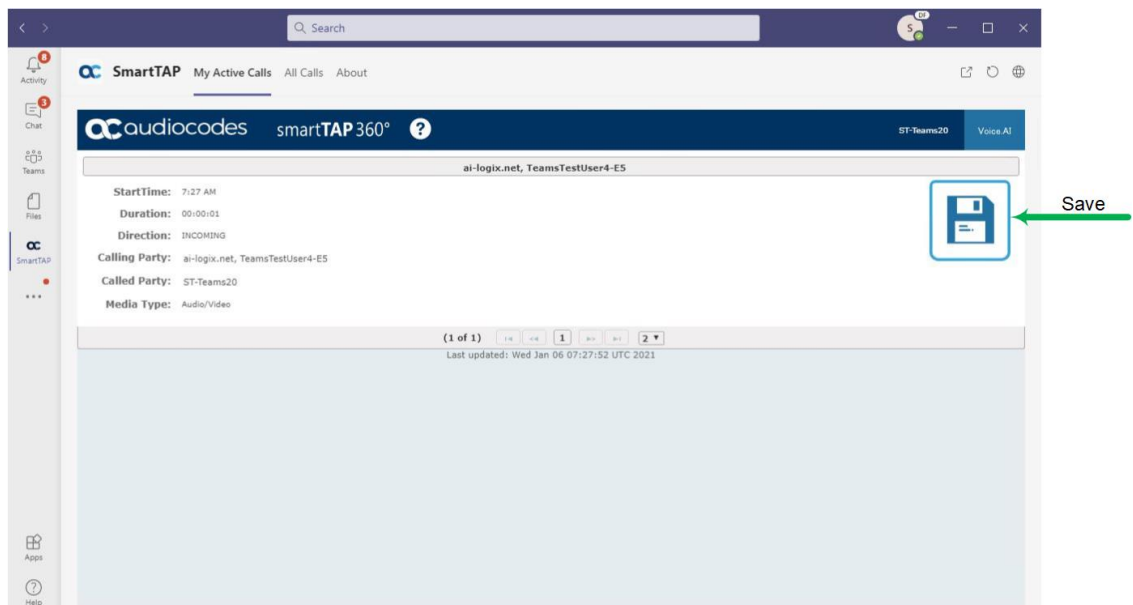
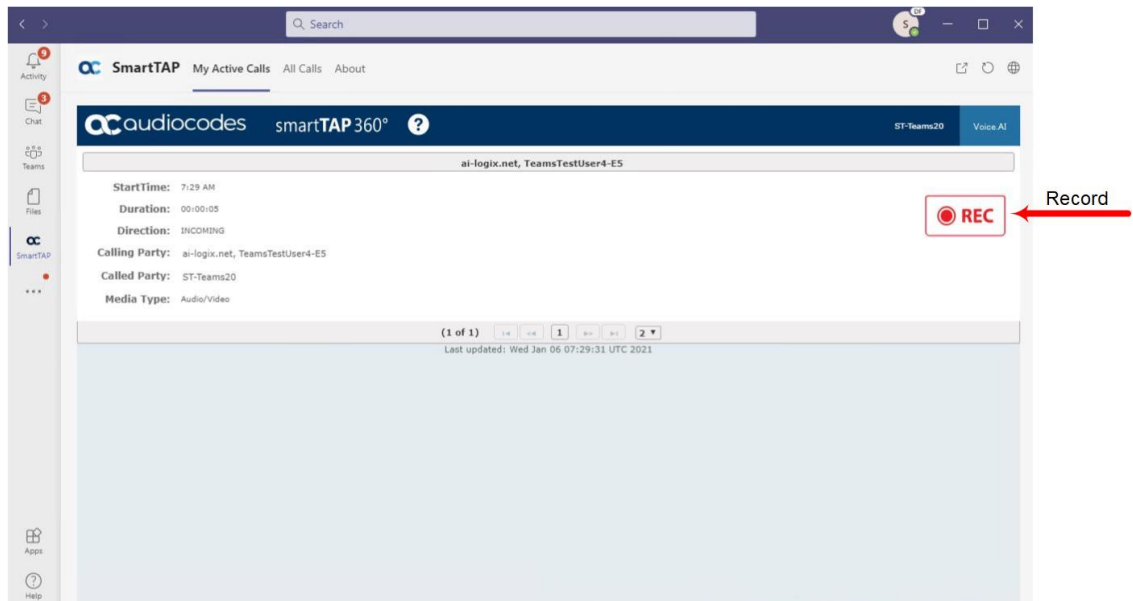
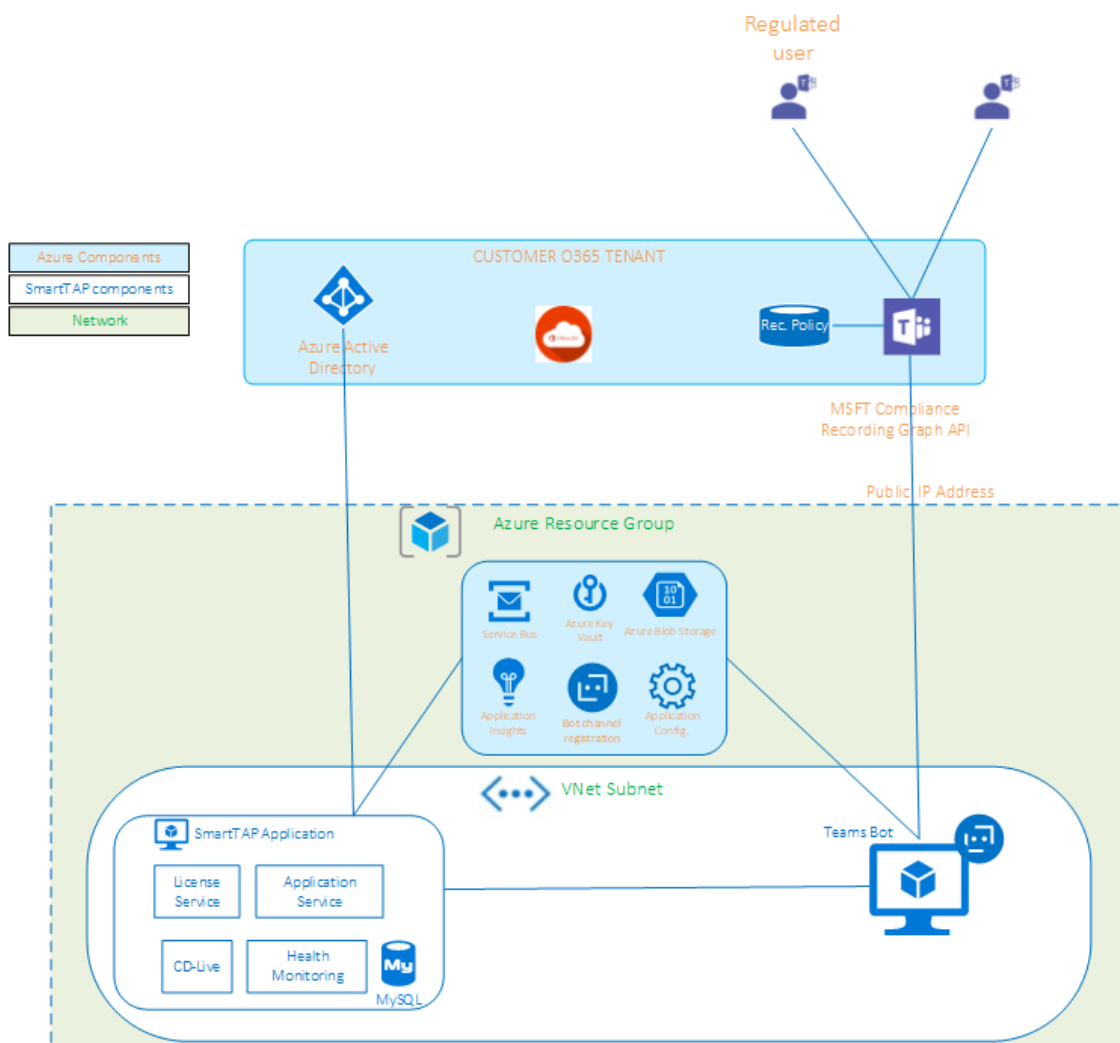
Figure 1-3: Record on Demand (ROD) in SmartTAP 360° Live Live Skype for Business Client**Figure 1-4: Save on Demand (ROD) in SmartTAP 360° Live Microsoft Teams Client**

Figure 1-5: Record on Demand (ROD) in SmartTAP 360° Live Live Microsoft Teams Client

Architecture

The figure below illustrates SmartTAP 360° Live architecture.

Figure 1-6: SmartTAP 360° Live Architecture

About this Guide

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

Table 1-2: About this Document

Section	Description
Logging In on page 16	Shows how to log in to the SmartTAP 360° Live Web Interface.
Getting Acquainted with the GUI on page 19	Gets the network administrator acquainted with the SmartTAP 360° Live management GUI.
Performing Initial Configuration on	Describes the steps to take to perform initial SmartTAP 360° Live configuration in order to record a call.

Section	Description
page 26	
Searching for Messages on page 203	Searching for Messages
Searching for Calls on page 149	Searching for Calls
Testing the Initial Configuration on page 28	Shows how to record a call to test the initial configuration.
Configuring Advanced Features on page 30	Details the user interface, features and procedures.
Single Sign-On for SmartTAP 360° Live on page 212	Shows how to simplify the login process for domain users with Single Sign-On (SSO).
SmartTAP 360° Live Skype for Business Toolbar on page 231	Shows how to use the SmartTAP 360° Live Skype for Business toolbar.
Media Exporter on page 234	Describes the Bulk Media Exporter tool to download Meta Data and Call Records.
API Integration on page 240	Describes the API Reference.
Recording Health Monitor on page 242	Describes the Recording Health Monitor utility
Announcement Server (Skype for Business) on page 247	Describes the setup and use of the Announcement Server (Skype for Business)
Microsoft Azure Active Directory on page 262	Describes the setup for Microsoft Azure Active Directory Teams user mapping and authentication.
Integrate SmartTAP	Describes how to integrate SmartTAP Personal App in Microsoft

Section	Description
Personal App in Teams on page 317	Teams.
Enable Users with Compliance Recordings on page 329	Describes how to enable users with Compliance Recordings using PowerShell scripts on the local machine that need to run with permissions on the required Teams environment.
SmartTAP Alarms on page 337	Describes the SmartTAP SNMP alarms that are raised on the One Voice Operations Center (OVOC).

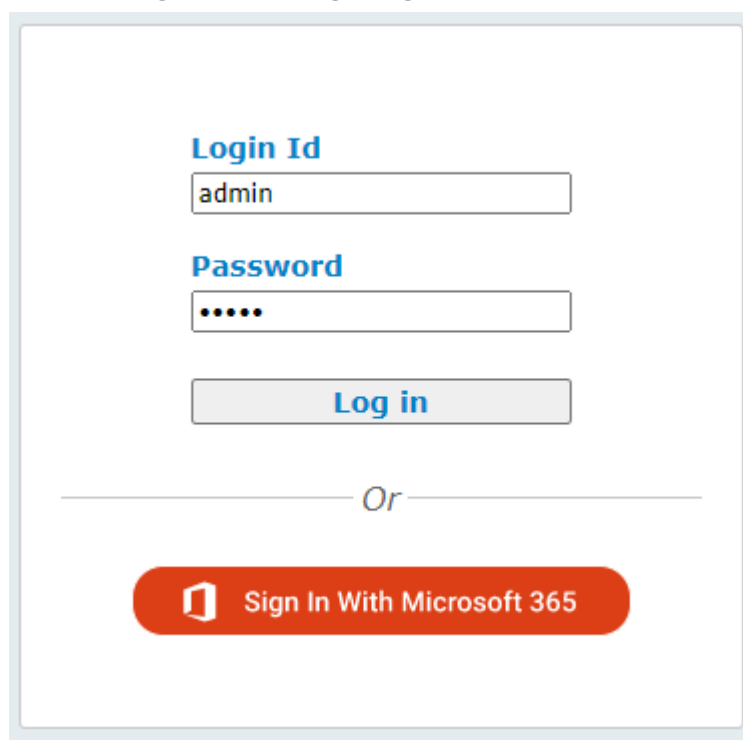
2 Logging In

After the SmartTAP 360° Live software is installed, an Admin user account is created by default. This user account allows the administrator to access the SmartTAP 360° Live's Web-based management tool for the first time and start initial configuration and administration (see Chapter [Performing Initial Configuration](#) on page 26). Alternatively, you can log in using the credentials of the Office 365 user.

➤ **To log in:**

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

Figure 2-1: Login Page



3. Log in using one of the following options:
 - **Log in:** Enter default Login ID 'admin' and default password 'admin'
 - **Sign In With Microsoft 365:** Enter the credentials of the Microsoft 365 Office user (see [Logging in with Microsoft Office 365 Credentials](#) below)

Logging in with Microsoft Office 365 Credentials

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



This option is disabled until the OIDC Client is configured (see [Step 4 Configure OpenID Connect OIDC Client](#) on page 309).

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

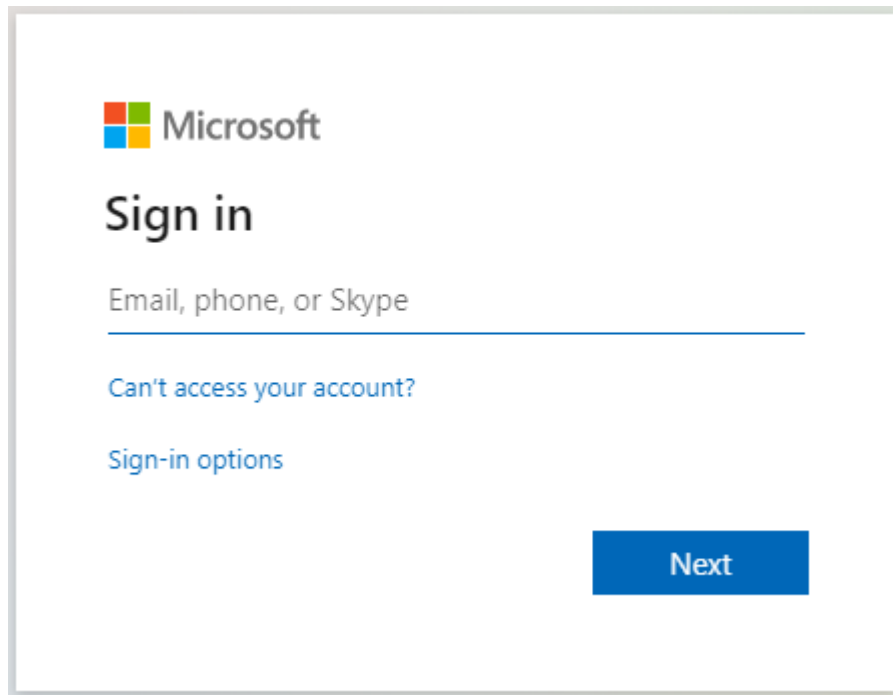
1. Click **Sign-in with Microsoft 365** button.

Figure 2-2: Microsoft Sign In

The screenshot shows a login interface. At the top, there is a label 'Login Id' in blue, followed by a text input field containing the text 'admin'. Below this is a label 'Password' in blue, followed by a password input field with five black dots. Underneath the password field is a grey button with the text 'Log in' in blue. A horizontal line with the word 'Or' in the center separates this from the bottom section. The bottom section features a red button with the Microsoft logo on the left and the text 'Sign In With Microsoft 365' in white.

The user is redirected to Microsoft MFC Login page:

Figure 2-3: Microsoft MFC Login Page

The image shows the Microsoft MFC Login Page. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed in a large, bold font. Underneath "Sign in" is a text input field with the placeholder text "Email, phone, or Skype". Below the input field are two links: "Can't access your account?" and "Sign-in options". At the bottom right of the page is a blue button with the text "Next".

Microsoft

Sign in

Email, phone, or Skype

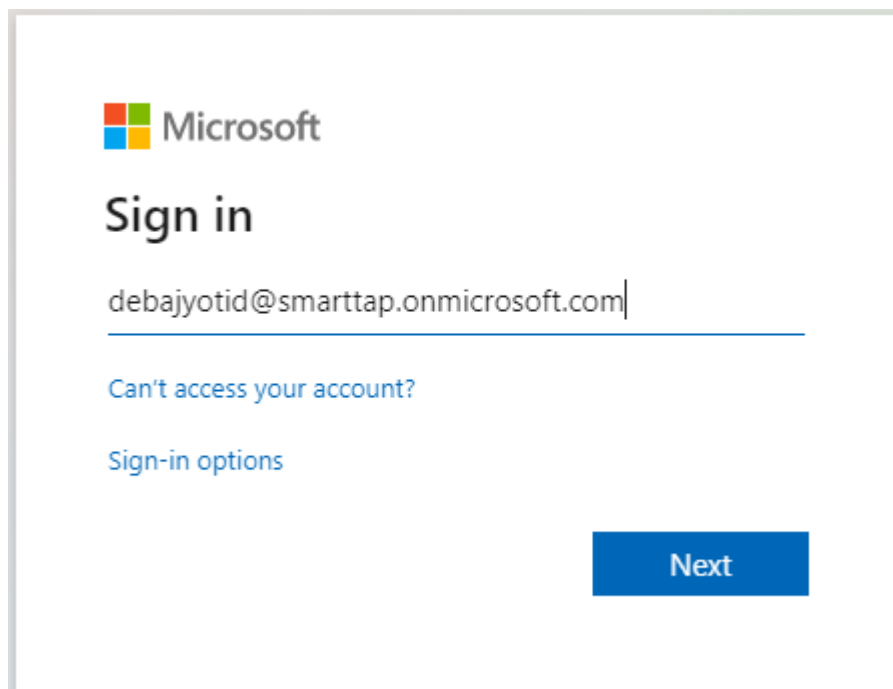
[Can't access your account?](#)

[Sign-in options](#)

Next

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

Figure 2-4: Sign in MFC

The image shows the Sign in MFC page. It has the same layout as Figure 2-3, but the text input field now contains the email address "debajyotid@smarttap.onmicrosoft.com". The other elements, including the Microsoft logo, "Sign in" heading, links, and "Next" button, are identical to Figure 2-3.

Microsoft

Sign in

debajyotid@smarttap.onmicrosoft.com

[Can't access your account?](#)

[Sign-in options](#)

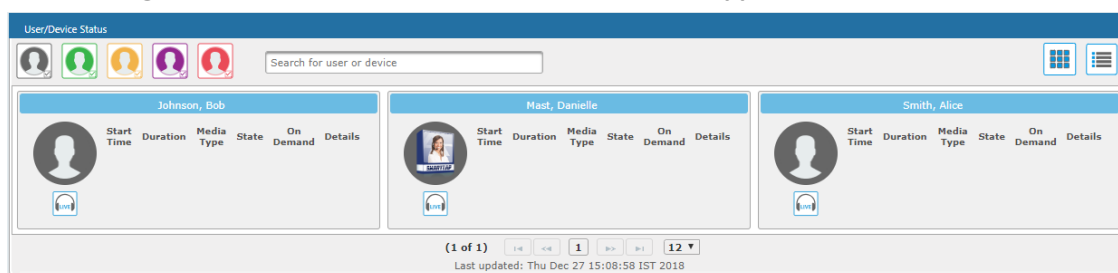
Next

3 Getting Acquainted with the GUI

This section introduces the SmartTAP 360° Live 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° Live Main Screen – Upper Banner

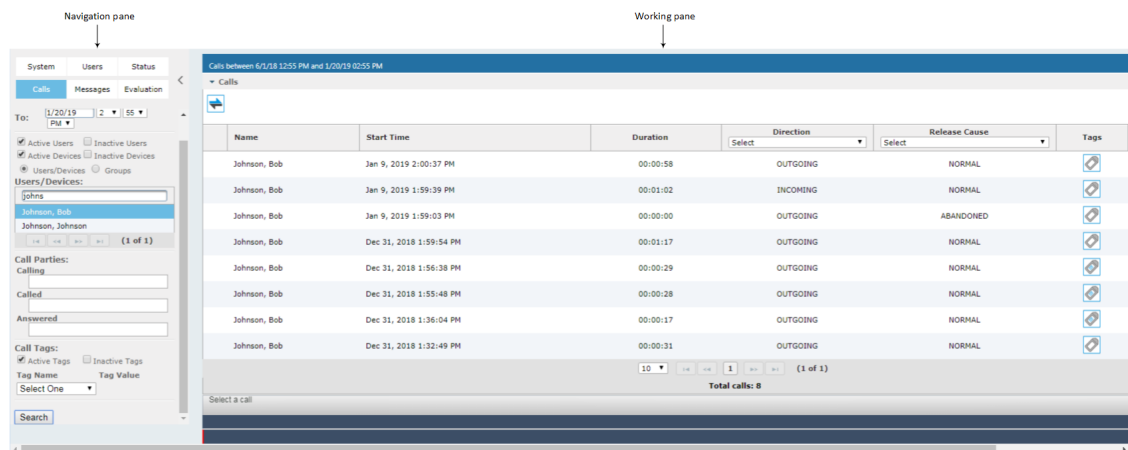


The table below describes the active buttons on the toolbar.



Table 3-1: SmartTAP 360° Live 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		Toggles between the following interface languages: <ul style="list-style-type: none"> ■ English ■ German ■ Spanish ■ French
Log off		Log off user (identified to the left of this button)

Figure 3-2: SmartTAP 360° Live Main Screen

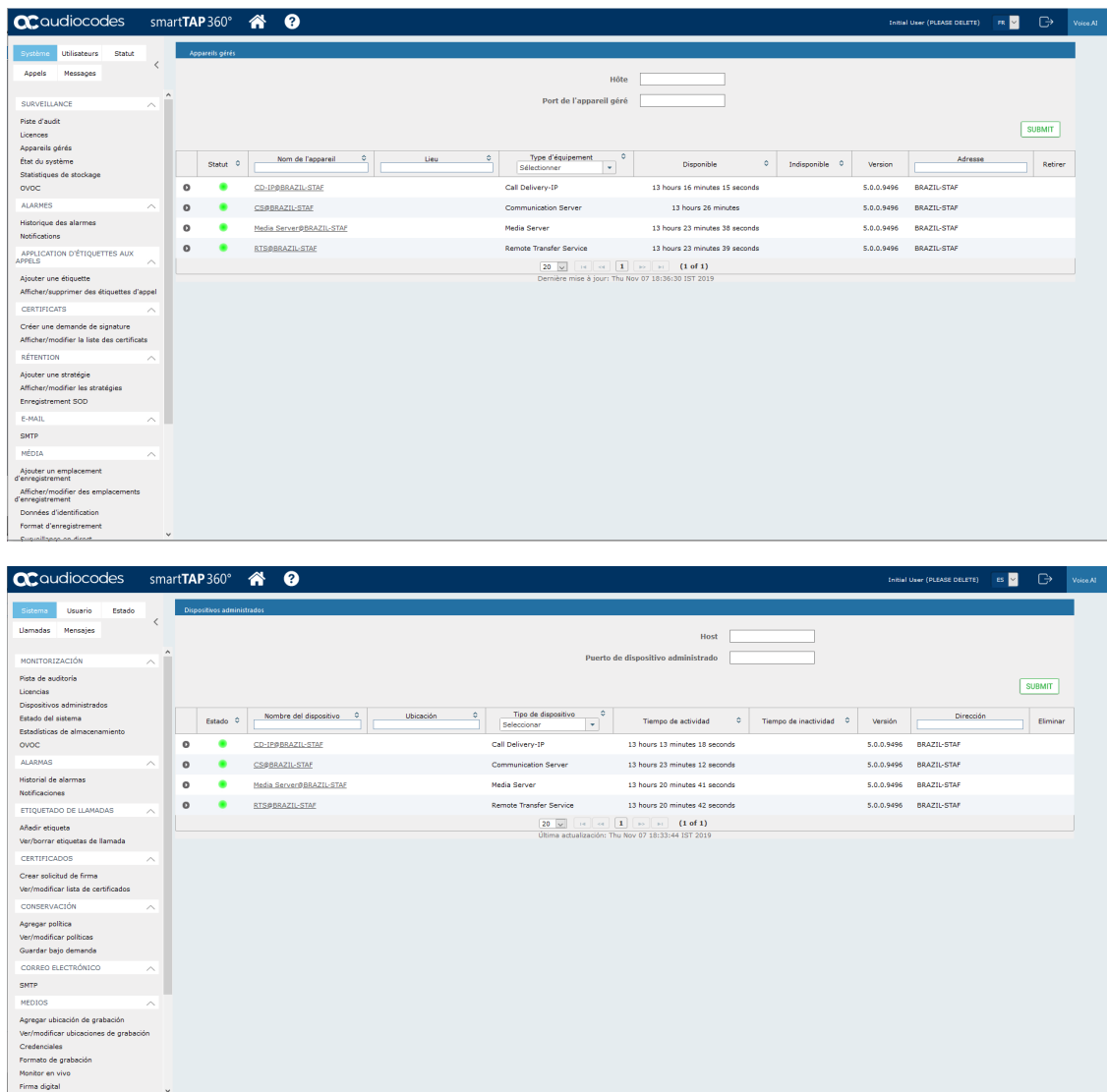
The figure above shows the following three areas below the upper banner:

- Navigation area, allowing users to perform queries, configuration, and all the other features available on the platform.
- Results display and data entry area, showing displays associated with the items selected in the Navigation area.
- Command execution results and data entry display area, displayed when an executed command results in 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



Determining User/Device Status

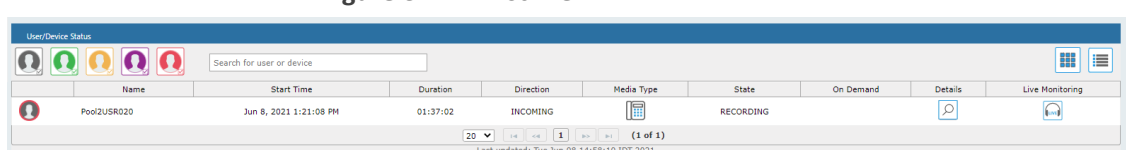
The User/Device Status screen is accessible by clicking the Home button on the upper banner, or by selecting **Status** tab > **User Call Status**. The screen features two views:

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

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

The figure below shows the List View

Figure 3-4: List View




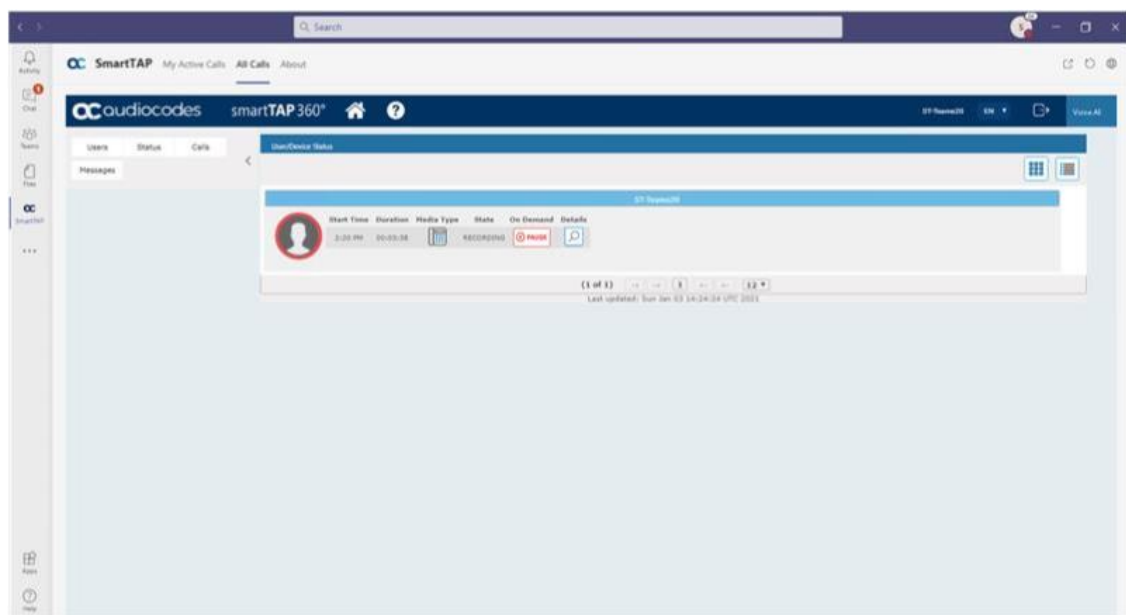
The figure below shows the Grid View 

Figure 3-5: Grid View






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












Figure 3-6: User/Device Status with an Active Call Microsoft Teams Client

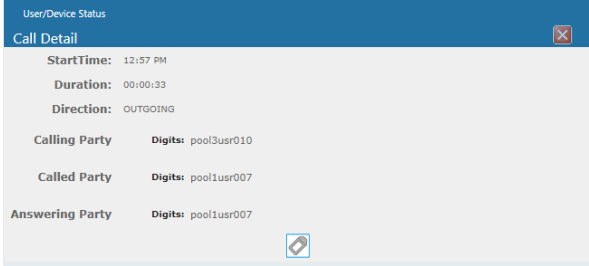










The screen provides near real-time information on the targeted users and their recording status. The table below describes the Status screen features.

Table 3-2: Status Features

Field	Description
Name	Sorted ascending/descending by clicking header up/down arrows. Name field entry displays only entries with matching pattern.
Call Started	The time the call started. Sortable by clicking the up/down arrows.
Call Duration	The duration of the call. Sortable by clicking the up/down arrows.
Call Direction	One of the following values: <ul style="list-style-type: none">  Incoming  Outgoing  Conference

Field	Description		
	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		
			
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		Select to pause the recording (for PCI compliance).	
		Select to Resume the recording (for PCI compliance).	
ROD / SOD		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		<p>Users with 'Live Monitoring' privileges can listen to active calls by clicking the Live Monitor microphone button. The following popup player launches:</p> 	

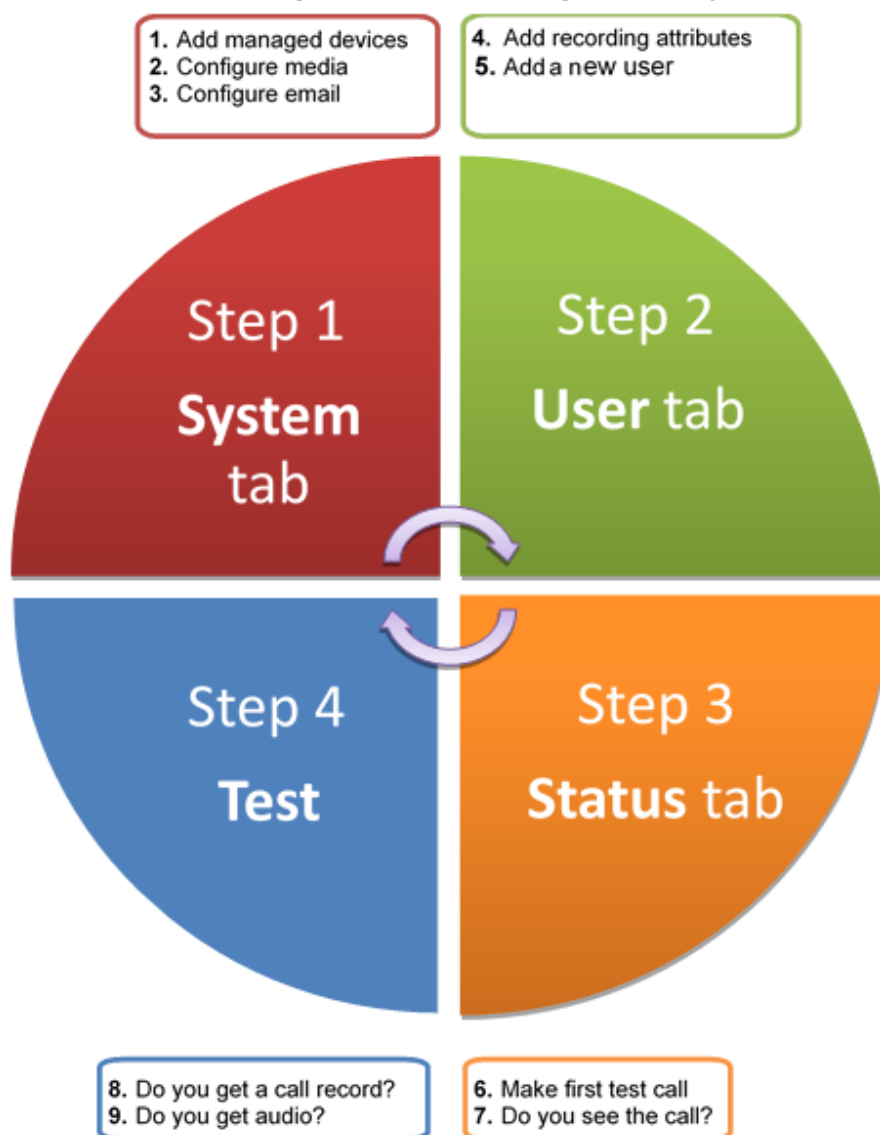
Field	Description	
		 When a user has permissions to listen to active calls for a targeted user who is licensed for both Teams and other integrations, support is only provided for listening to the active Teams calls.
Page Navigation buttons	These are shortcuts to the beginning/end, previous page/next 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° Live configuration (Step 1-Step 2) in order to record a call. Detailed instructions follow below it.

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

Figure 4-1: Performing Initial Setup



➤ **To perform initial setup:**

1. Log in for the first time (see [Logging In](#) on page 16 for more information)
2. Configure media (see [Configuring Media](#) on page 69 for more information).
3. Configure email (see [Configuring Email Server Settings](#) on page 68 for more information).

4. Add a user attribute for recording purposes (see [Adding a Device Attribute](#) on page 133 for details).
5. Add a user (see under Managing Users for more information).
6. Make sure the new user is assigned a recording profile (see under [Managing Recording Profiles](#) on page 118 for more information).
7. Make sure the user's recording attribute field is populated (for more information, see [Managing Recording Profiles](#) on page 118).

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 26). 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 30 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, configure the advanced SmartTAP 360° Live 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° Live. The Audit Trail is searchable but cannot be edited or deleted. You can view / search the user changes made to the SmartTAP 360° Live 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

The screenshot shows the 'Audit trail' interface. On the left, under 'Selection criteria', there is a list of users: 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; Ilyae, 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. On the right, there are input fields for 'From: 12/31/18' and 'To: 12/31/18', and a 'Search' button.

2. Select the desired users and date range (Use the table below as reference).

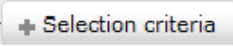

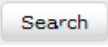


Figure 6-2: Audit Trail Query Result

The screenshot shows the 'Audit trail' interface with a query result table. The table has columns: Name, Action, Timestamp, and Description. The data rows show various login and playback events for users like ST-Teams100, ST-Teams100, ST-Teams31, ST-Teams2, TeamsTestUser2, TeamsTestUser5-ES, and User (PLEASE DELETE). The table is paginated, showing 1 of 2 pages.

Name	Action	Timestamp	Description
ST-Teams100	LOGIN	01/14/2021 11:05:58 AM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/14/2021 11:17:23 AM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:11:53 PM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:18:58 PM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:21:46 PM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.
ST-Teams100	PLAY_CALL_MEDIA	01/17/2021 02:22:02 PM	ST-Teams100 requested playback of media for call id 43. Elav
ST-Teams100	PLAY_CALL_MEDIA	01/17/2021 02:23:06 PM	ST-Teams100 requested playback of media for call id 43. Elav
ST-Teams100	PLAY_CALL_MEDIA	01/17/2021 02:23:46 PM	ST-Teams100 requested playback of media for call id 43. Elav
ST-Teams100	LOGIN	01/17/2021 02:28:11 PM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:29:44 PM	User ST-Teams100@smartap.onmicrosoft.com successfully logged in.

Table 6-1: Audit Trail

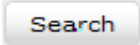
Field	Description
Selection criteria	Click to hide the Search area


Field	Description
	Click to show the  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.
	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.
<p>Navigation buttons under the search display:</p>  <p>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.</p>	

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  to see the results.

4. Click the Excel  icon.



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

Managing Licenses

This section describes how to manage the SmartTAP 360° Live licenses. Licenses are generated and loaded to SmartTAP as described in the SmartTAP 360° Live Installation Guide. This interface displays data on the purchased and loaded license items for all integrations types:

- **Targeted user licenses:** Enables SmartTAP 360° Live users to be assigned recording profiles for different types of communication recordings in an enterprise. The total amount of purchased Target User licenses pre-configured in the License file are the same for all integration types.
- **Concurrent recording licenses:** Determines 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 total amount of purchased Concurrent recording licenses pre-configured in the License file can be different for each integration type.

This section includes the following:

- [Licenses for Other Integrations](#) below
- [Microsoft Teams Licenses](#) on page 35
- [License Configuration Parameters](#) on page 38



For Microsoft Teams integrations, its possible to allocate user licenses using this interface, however for other integrations user licenses are allocated on-the-fly.

Licenses for Other Integrations

This section describes the management of licenses for other integrations. The following licenses are available:

- **Targeted User Licenses:**
 - **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.

■ **Concurrent Recording Licenses:**

- **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 determines the maximum number of concurrent Video and Audio recordings of the users that are assigned to Audio and Video enabled recording profile.
- **Screen Sharing Concurrent Recordings:** This license determines the maximum number of concurrent Screen Sharing recordings of users that are assigned to an audio or video recording profile.
















Only the concurrent recording licenses can be enabled for users with Audio& IM targets or Video & Audio & IM targets (Screen Sharing concurrent recordings does not require a dedicated target user license as its a component of the Video & Audio target license).

➤ **To view Managed Licenses:**

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

Figure 6-3: Licenses for Other Integrations

Licenses							
<div>  CD-IP@qalab-ST-Pool2 </div> <div> Sales Order Number 2714587 Product Key AVD100Lic Date Issued 02/26/2019 Customer Name AudioCodes-QA </div>							
License Usage							
Last Updated Sunday, December 8, 2019 11:00:43 AM							
License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value	
Audio & IM Targets	300	97	203	97		<input type="text" value="0"/>	
Audio Concurrent Recordings	100	0	100	1		<input type="text" value="0"/>	
IM Targets	10	0	10	0		<input type="text" value="0"/>	
Video & Audio Concurrent Recordings	10	0	10	2		<input type="text" value="0"/>	
Video & Audio & IM Targets	100	2	98	2		<input type="text" value="0"/>	
Desktop Sharing Concurrent Recordings	10	0	10	1		<input type="text" value="0"/>	
							<input type="button" value="Refresh"/>

The figure above shows an example of different Target and Concurrent recording licenses.

Microsoft Teams Licenses

This section describes the management of user licenses in a mixed environment with Microsoft Teams .



Compliance Call Recording can be enabled on Microsoft 365 A3/A5/E3/E5/Business Premium and Office 365 A3/A5/E3/E5 users.

Targeted User Licenses:

- **Audio Targets:** This license sets the number of users that can be assigned to a Recording Profile for recording Audio. "Audio Concurrent" licenses (described below) are required to record these users calls.
- **All Included Targets:** This license sets the number of users that can be assigned to a Recording Profile for recording Audio and Video, Video and Screen Sharing and Instant Messages. "Audio & Video Concurrent Recordings" licenses (described below) are required to record these users calls

Concurrent Recording Licenses:

- **Audio Concurrent Recordings:** This license determines the maximum number of total concurrent Audio recordings of users that are assigned to an Audio enabled recording profile (Video and Screen Sharing disabled).

- **Audio & Video Concurrent Recordings:** This license determines the maximum number of concurrent Video and Video and Screen Sharing recordings of the users that are assigned to Video or Video and Screen Sharing enabled recording profile.

Figure 6-4: Microsoft Teams Licenses

Total License Targets Usage
Last Updated Sunday, May 30, 2021 6:21:02 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value	Assign License
Audio Targets	100	1	99	17	98		
All Included Targets	100	17	83	17	0		

Teams Concurrent Calls Recordings License Usage
Last Updated Sunday, May 30, 2021 6:21:02 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	100	0	100	6	0	
Audio & Video Concurrent Recordings	100	0	100	6	0	

CD-IP@il-sharonbi-lp Concurrent Calls Recordings License Usage
Last Updated Sunday, May 30, 2021 6:21:02 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	100	0	100	0	2	
IM Targets	100	0	100	0	0	
Video & Audio Concurrent Recordings	100	0	100	0	0	

This screen is divided into three sections:

- The top section "Total License Target Usage" displays the total number of licenses (configured in License file) and currently consumed licenses accumulated for all integration types.
- The middle section "Teams Concurrent Calls License Usage" displays the total number of concurrent recording licenses and the number of these licenses currently consumed for Microsoft Teams users.
- The lower section shows that total number and currently consumed concurrent recording licenses for other integrations (if exists).



The preconfigured license totals in the license file for Targeted Licenses is **identical** for all integrations. The preconfigured concurrent recordings **may differ** between integrations.

➤ **To assign licenses to a target:**


1. Click  adjacent to the license type for which you wish to assign users.

Figure 6-5: Licensed Targets

Licensed Targets

Used Licenses/Available Licenses: 9 / 500

Select all UnSelect all

First Name Recording Profile Recording license

TeamsTestUser5-E5	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams17	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams14	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams13	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams12	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams11	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams102	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams101	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams100	yehuditTest	<input checked="" type="checkbox"/>

20 1 (1 of 1)

- From the Recording Profile drop-down list, select the Recording profile for the users that you wish to assign licenses. The users list is updated to reflect the selection.
- Select the check boxes adjacent to the users for whom you wish to assign licenses. Select **Select all** to select the entire list or **UnSelect all** to not select any users in the list.

The license allocation are automatically updated as shown in the figure below.

Figure 6-6: License Successfully Modified

• License successfully modified

Licensed Targets

Used Licenses/Available Licenses: 6 / 500

Select all UnSelect all


First Name Recording Profile Recording license

ST-Teams100	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams101	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams102	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams11	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams12	yehuditTest	<input checked="" type="checkbox"/>
ST-Teams13	yehuditTest	<input type="checkbox"/>
ST-Teams14	yehuditTest	<input type="checkbox"/>
ST-Teams17	yehuditTest	<input checked="" type="checkbox"/>
TeamsTestUser5-E5	yehuditTest	<input type="checkbox"/>

20 1 (1 of 1)

You can view the updated totals in the figure below. Note that 6 licenses (matching the 6 selected check boxes shown in the figure above) have been allocated out of a total of 500.




Figure 6-7: Updated License Allocations




LICENSE_SERVER@SmartTAP54

Sales Order Number 1214578
Product Key Yeh500
Date Issued 06/02/2021
Customer Name AudioCodes-QA

Total Targets License Usage
Last Updated Sunday, June 6, 2021 7:25:30 PM



License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value	Assign License
Audio Targets	500	6	494	12 	<input type="text" value="0"/>		



LICENSE_SERVER@SmartTAP54


Sales Order Number 1214578
Product Key Yeh500
Date Issued 06/02/2021
Customer Name AudioCodes-QA



Teams Concurrent Calls Recordings License Usage
Last Updated Sunday, June 6, 2021 7:25:30 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	500	0	500	140 	<input type="text" value="0"/>	

Refresh

License Configuration Parameters

Parameter	Description
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.
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 43.
Set/Modify Threshold Value	Set or modify the Threshold value adjacent to each license item.

Parameter	Description
	
 Allocation Licenses	Enables the allocation of licenses for targeted users for Microsoft Teams users only.



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

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° Live 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° Live 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 42 [Adding a Device Manually to the Application Server](#) on page 42 for the procedure to add Host devices.

➤ To view managed devices:

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

Figure 6-8: Managed Devices

Managed Devices

Host

Managed Device Port

	Status	Device Name	Location	Device Type	Up Time	Down Time	Version	Address	Remove
1		127.0.0.1:161		Host	14 days 20 hours 8 minutes 32 seconds			127.0.0.1	
2		AC-MediaProxy@ST-CLUSTER-N1		Integration Specific	5 days 21 hours 24 minutes 8 seconds		4.3.0.9238	ST-CLUSTER-N1	
3		AC-Plugin@QALAB-POOL4-FE1		Integration Specific	33 days 14 hours 47 minutes 39 seconds		4.2.0.9161	QALAB-POOL4-FE1	
4		AC-Plugin@SFB19-POOL1-FE1		Integration Specific	18 days 20 hours 17 minutes 23 seconds		4.3.0.9238	SFB19-POOL1-FE1	
5		AC_HealthMonitor@ST-CLUSTER-N1		Health Monitor	14 days 20 hours 7 minutes 40 seconds		4.3.0.9238	ST-CLUSTER-N1	
6		CD-IP@st-cluster-n1		Call Delivery-IP	4 days 22 hours 7 minutes 55 seconds		4.3.0.9220	st-cluster-n1	
7		CS@st-cluster-n1		Communication Server	5 days 23 hours 49 minutes 34 seconds		4.3.0.9240	st-cluster-n1	
8		Media_Server@st-cluster-n1		Media Server	5 days 21 hours 26 minutes 22 seconds		4.3.0.9220	st-cluster-n1	
9		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 sent 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 or more of the deviceconnections are DOWN.
	 Device status is DOWN: the device stops sending heartbeat messages.
Device Name	<p>Display Name of the Device. Sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.</p> <p>Note: Clicking the Device Name link opens the control panel page for this device.</p>
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	<p>Type of the device provided during registration. A manually added device has type 'Host'. In SmartTAP 360° Live, 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, Teams Bot and Media Delivery</p> <p>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.</p>
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 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° Live inter-components communication status helps to quickly detect connection issues and to take the appropriate actions. Each managed device reports the status of its connections with other components in the system.














Figure 6-9: Inter-Component Communications

Managed Devices

Host

Managed Device Port

SUBMIT

	Status	Device Name	Location	Device Type	Up Time	Down Time	Version	Address	Remove
1		AC_HealthMonitor@STTeamsQ453		Health Monitor	2 hours 53 minutes 4 seconds		5.3.0.9829	STTeamsQ453	
2		CALL_DELIVERY_LIVE@STTeamsQ453		Call Delivery-Live	2 hours 53 minutes		5.3.0.9829	STTeamsQ453	
3		CS@STTeamsQ453		Communication Server	2 hours 52 minutes 53 seconds		5.3.0.9829	STTeamsQ453	
4		REMOTE_TRANSFER_SERVICE@ntivm000000		Remote Transfer Service	6 hours 56 minutes 7 seconds		5.3.0.9828	ntivm000000	
5		REMOTE_TRANSFER_SERVICE@ntivm000001		Remote Transfer Service	6 hours 55 minutes 39 seconds		5.3.0.9828	ntivm000001	
6		REMOTE_TRANSFER_SERVICE@ntivm000002		Remote Transfer Service	6 hours 54 minutes 39 seconds		5.3.0.9828	ntivm000002	
7		REMOTE_TRANSFER_SERVICE@ntivm000003		Remote Transfer Service	6 hours 54 minutes 9 seconds		5.3.0.9828	ntivm000003	
8		REMOTE_TRANSFER_SERVICE@ntivm000004		Remote Transfer Service	6 hours 53 minutes 39 seconds		5.3.0.9828	ntivm000004	
9		TEAMS_BOT@ntivm000000		Teams Bot	5 hours 20 minutes		5.3.0.9764	ntivm000000	
10		TEAMS_BOT@ntivm000001		Teams Bot	6 hours 55 minutes 1 second		5.3.0.9764	ntivm000001	
11		TEAMS_BOT@ntivm000002		Teams Bot	6 hours 55 minutes 1 second		5.3.0.9764	ntivm000002	
12		TEAMS_BOT@ntivm000003		Teams Bot	6 hours 55 minutes 1 second		5.3.0.9764	ntivm000003	
13		TEAMS_BOT@ntivm000004		Teams Bot	6 hours 55 minutes 1 second		5.3.0.9764	ntivm000004	

20

1

<=<

>=>

1

(1 of 1)

Last updated: Wed Jan 13 16:54:47 UTC 2021

Adding a Device Manually to the Application Server

The Application Server's Web service manages all devices (software elements).

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 39, 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 .

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 6-10: Alarm History

Alarm History: Alarms between 1/21/19 and 1/21/19						
From: 1/10/19		To: 1/10/19		Search		
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.	
(1 of 1) < > 10						

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° Live 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 6-11: 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.	
Call Recording Error	Call not recorded or recorded with errors	
Configuration Error	Failed to execute configuration.	



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 .

Figure 6-12: Link Up Alarm Notification

Communication Down Alarm Notification

Name Communication Down

Alarm Description Communication between processes has been lost.

Non Recipients

- pool1usr010
- pool1usr011
- User (PLEASE DELETE), Initial


Recipients

>> > < <<

SUBMIT CANCEL

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.

For a list of alarms and possible causes with recommended remedial actions, see [SmartTAP Alarms](#) on page 337

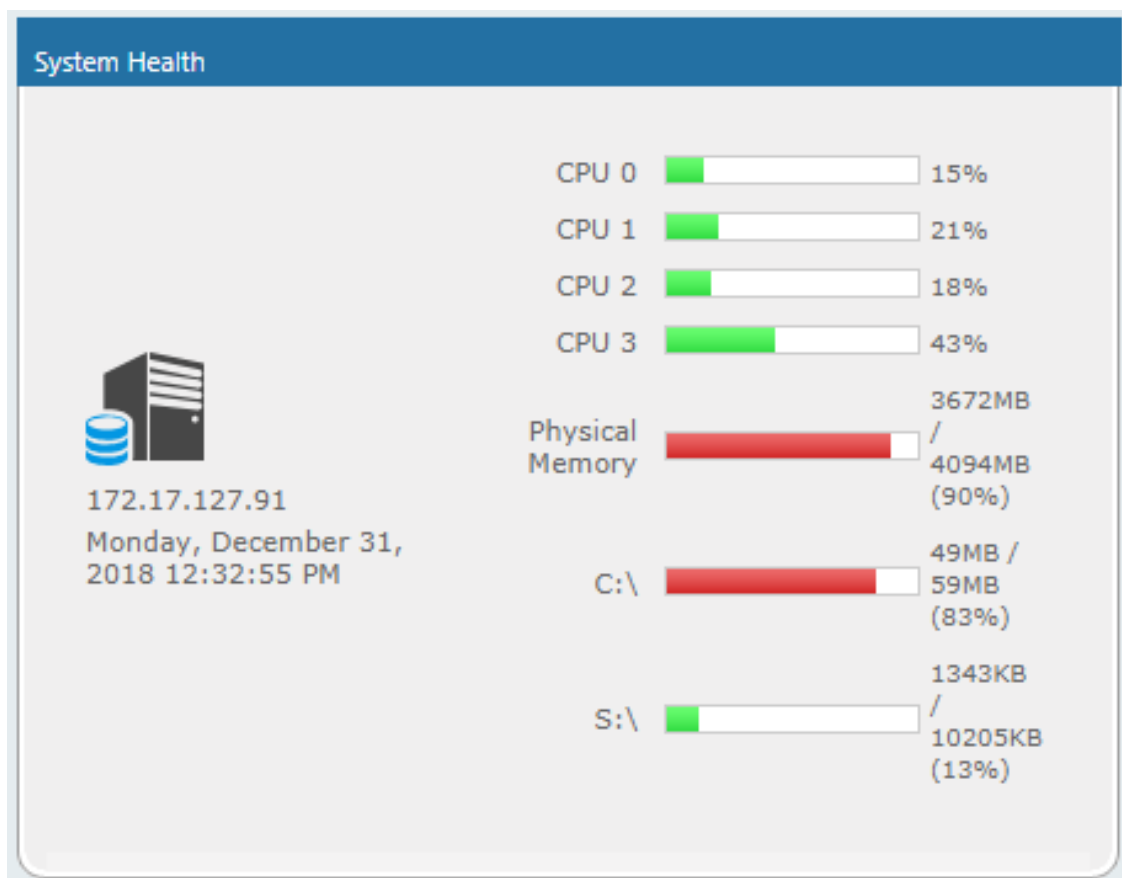
The figure below shows alarm notifications for the 'Resource Threshold Exceeded' notification; sent when the system utilization has exceeded the maximum number of available licenses. The 'Resource Threshold Cleared' notification is sent when the system license utilization falls back within the threshold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

Figure 6-13: 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.	
Call Recording Error	Call not recorded or recorded with errors	
Configuration Error	Failed to execute configuration.	

Monitoring System Health

The health of the SmartTAP 360° Live 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 6-14: System Health

Windows Event Log

By default alarms and events raised on SmartTAP 360° Live are sent to the OVOC server as SNMP traps (see [Configuring OVOC Connection](#) on page 101) and are not sent by default to the Windows Event Log.

➤ **To enable sending SmartTAP 360° Live 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 6-15: useEventViewer

```

101 Description: The interval (in milliseconds) between ems keep alive traps
102 DefaultValue=30000
103
104 adminRefreshInterval="3600000"
105 Description: The interval (in milliseconds) between admin info requests
106 DefaultValue=3600000
107
108 localSnmpPort="161"
109 Description: Local SNMP port to recieve requests from EMS
110 DefaultValue=161
111
112 alarmHistorySize="10000"
113 Description: Maximum size of history alarms
114 DefaultValue=10000
115
116 activeAlarmSize="1000"
117 Description: Maximum size of active alarms
118 DefaultValue=1000
119
120 sbcInternalIP="169.254.100.1"
121 Description: IP address of the associate SBC over internal VLAN/PrivateNetwork
122 DefaultValue=169.254.100.1
123
124 httpLicenseMode="https"
125 Description: HTTP mode for licence requests. Can be 'http' or 'https'
126 DefaultValue=https
127
128 useEventViewer="false"
129 Description: Use Event Viewer as Alarms/Events destination
130 DefaultValue=false
131
132 publicOvocInternalIp="169.254.0.1"
133 Description: The internal ip of the public OVOC, incase connecting via PublicOvocConnector
134 DefaultValue=169.254.0.1
135
136 ovocConnectorAccessUrl="http://localhost:8867/"
137 Description: The url for sending requests to Public Ovoc connector
138 DefaultValue = "http://localhost:8867/"
139
140 ovocGroup="Generic App"
141 Description: The name that used in sysDescription and select mib file
142 DefaultValue = "Generic App"
143 -->
144 <System httpClientMode="http" adminAccessUrl="http://localhost:80/rs/audiocodes/recorder/api/" ovocGroup="SmartTap" useEventViewer="true"/>
145

```

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 “SmartTAPCalls” and Event ID=<EventID> <Task Category> where 1-Alarm and 2-Event.
- **SmartTGeneral:** this log includes all other alarm 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 6-16: Event Viewer SmartTCalls

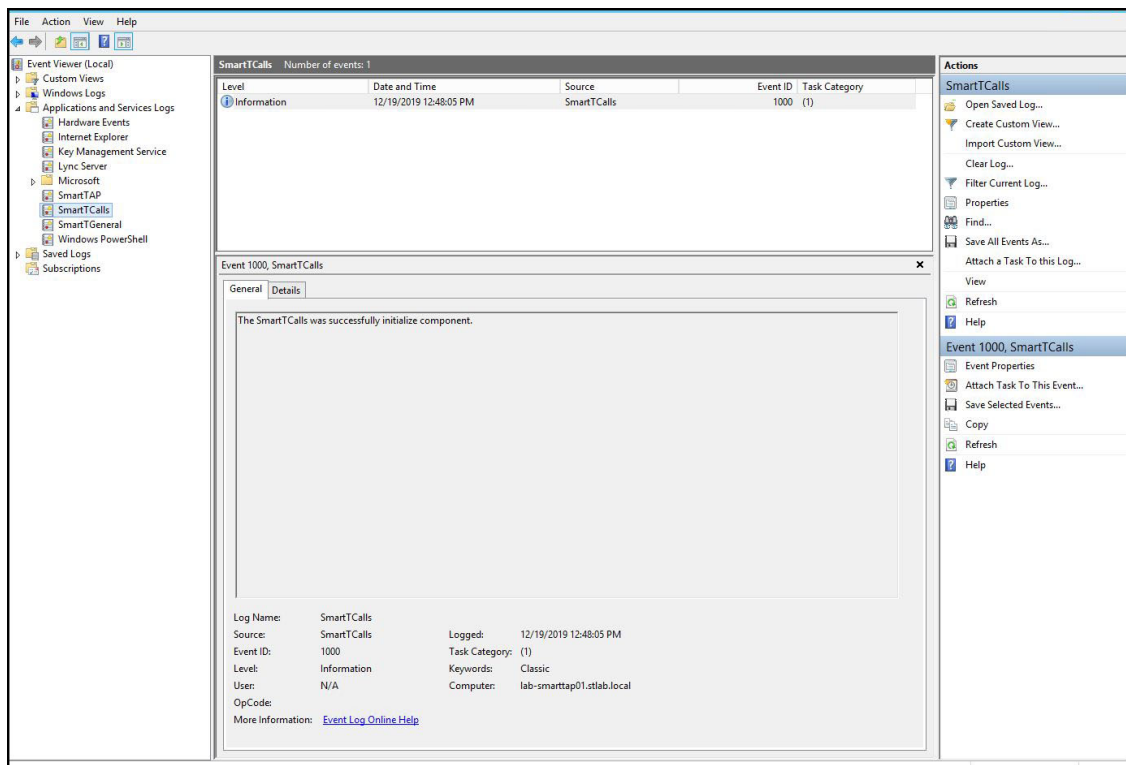
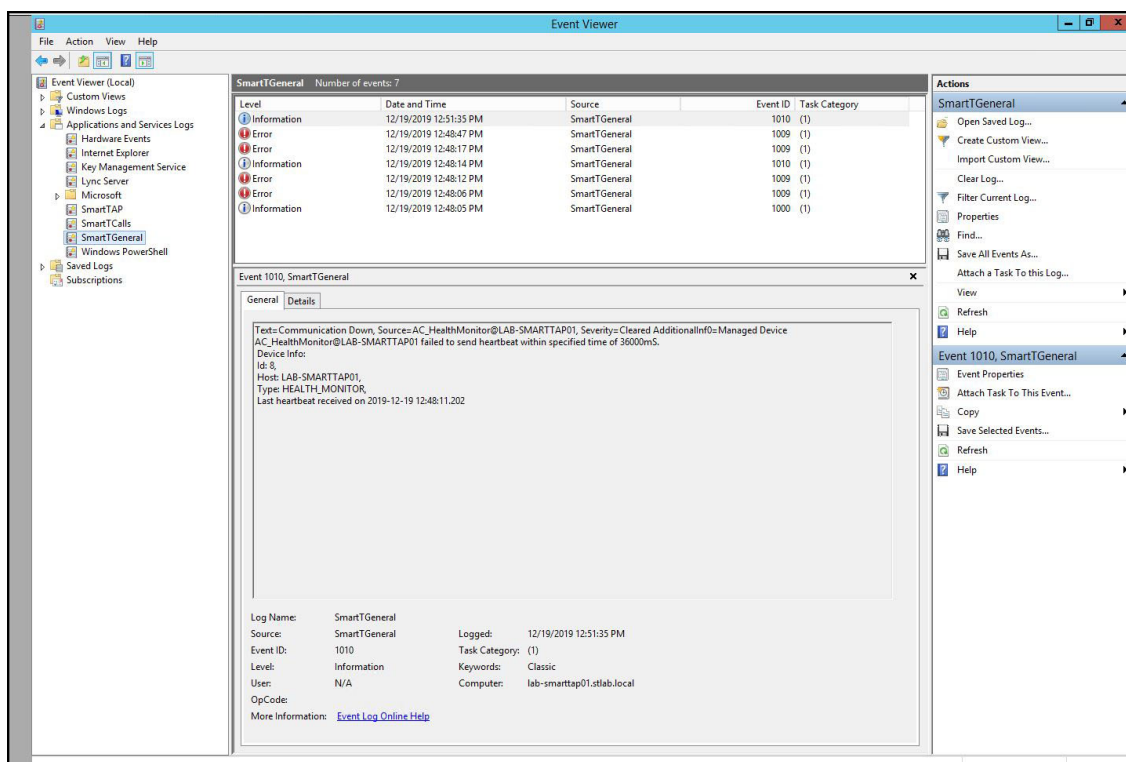


Figure 6-17: Event Viewer SmartTGeneral



SCOM Integration

The SmartTAP 360° Live 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°

Live, the monitored events source should be configured to “SmartTAP 360° Live” with Event ID 4096. For more information, see the following link: [Monitor Event Log](#)

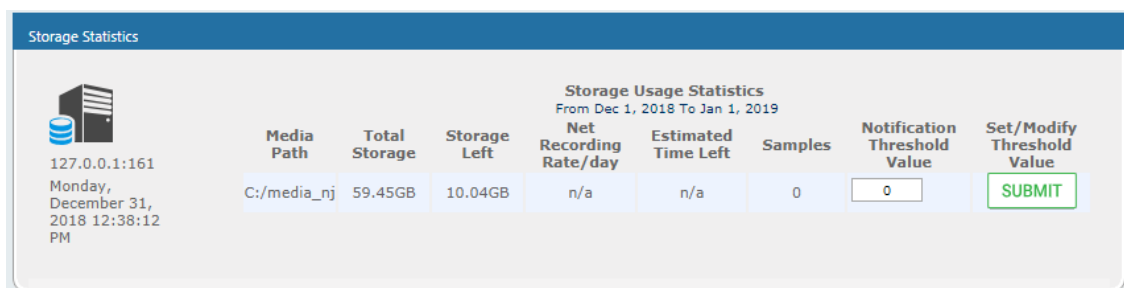
Monitoring Storage Statistics

The SmartTAP 360° Live 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.
- For Microsoft Teams deployments, only Audio Licenses and total Audio Concurrent recording licenses are supported.


Figure 6-18: Storage Statistics Screen






Use the table below as reference.

Table 6-5: 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).
	Apply changes

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



- 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  to submit changes.
- 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  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 6-6: 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: <ul style="list-style-type: none"> ■ None (Tag requires no administrator input) ■ Text (the 'Notes' field supports a maximum of 256 characters) ■ Boolean (Select/clear the checkbox: Yes / No or True / False) ■ Select_One (Define a list of options for the administrator to choose from, i.e., Excellent, Very Good, Good, Poor)
Allow Private	Allows an administrator to add the tag as private. Once tagged as private, only the specific administrator account will be able to view the tag.
	Applies changes.
	Cancels changes.

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 6-19: Add Call Tag Screen

Table 6-7: 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	<p>Tag Type:</p> <ul style="list-style-type: none"> ■ 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) <p>Mask (Use with Text Tag Types):</p> <p>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:</p> <p>*(Any printable character)</p> <p> #(Must be a digit: 0-9)</p> <p>A(Must be a letter: A-Z, a-z)</p> <p>\$(Must be alpha or numeric: A-Z, a-z, 0-9)</p> <p>\(Following character is a fixed literal character)</p> <p>' ' (All characters within single quotes are a fixed literal string)</p> <p>For example, the mask for a tag with the format 'Sales-#####A\$ will</p>

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 6-20: 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			
Title	Notes about the call.	TEXT			
Participants	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 149)


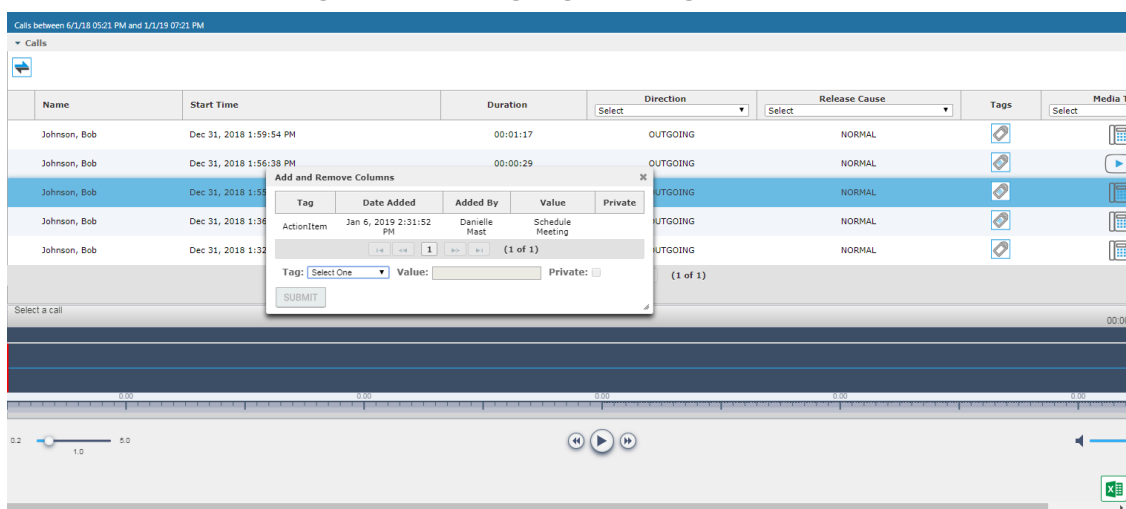
2. Select the call record to tag and ensure that the Tags column is displayed.
3. Double-click the Tags icon in the call record.
4. In the Tag field, select the type of tag that you wish to add and enter the desired value in the Value field.
5. Select the Private check box to list a personal reminder (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 .

Figure 6-21: Assigning a Call Tag



Generating and Loading HTTPS Certificates

SmartTAP 360° Live 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° Live server
- Digitally signing audio files



SmartTAP 360° Live 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° Live components or used to manage SmartTAP 360° Live 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° Live components reside, and all computers used to manage SmartTAP 360° Live 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° Live 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° Live will automatically use Key type = RSA, Key size = 2048 and Cryptographic Hash = SHA-256.

➤ To generate a CSR:

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

Figure 6-22: Certificate Signing Request Screen

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

Table 6-8: 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)	<ul style="list-style-type: none"> ■ 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/enterprise.
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° Live.



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.

- Click **SUBMIT**; the CSR is automatically available for download from the browser.
- 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 6-23: 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 6-9: 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:**


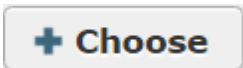

1. Open the View/Modify Certificate List page (**System** tab > **Certificates** folder > **View/Modify Certificate List**).
2. Click the  **Import** icon and then the Browse button  to navigate to the location of the appropriate certificate file: 'filename.cer'

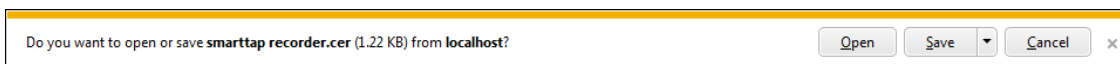
Figure 6-24: Import Certificate

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.



➤ **To view a certificate:**


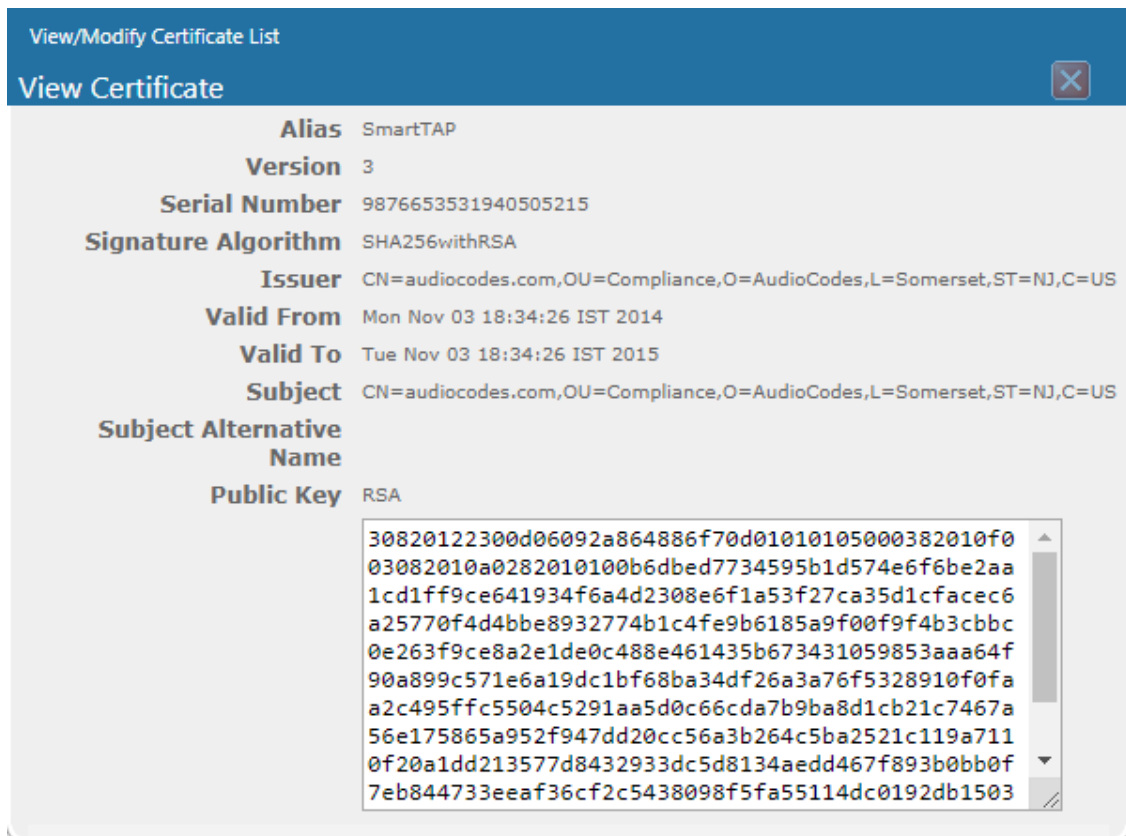
1. Open the View/Modify Certificate List page (**System** tab > **Certificates** folder > **View/Modify Certificate List**), click the  **View** icon.

Figure 6-25: View Certificate



Step 2: Load Certificates

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

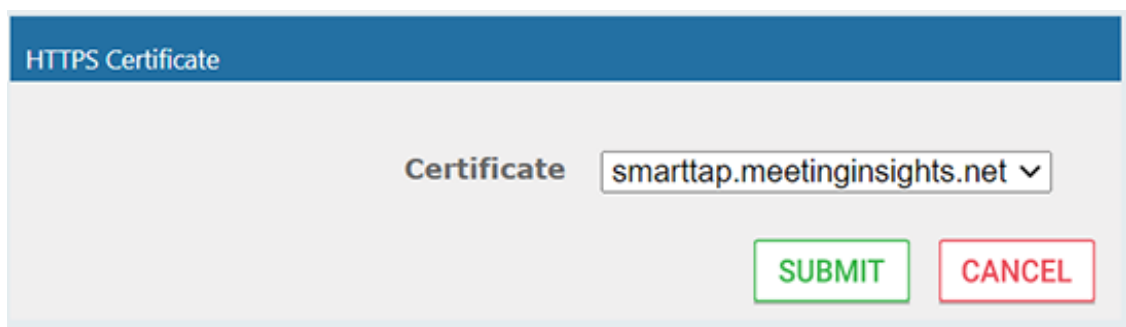
Loading Web Browser Certificate

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

➤ To load the Web browser certificate:

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

Figure 6-26: HTTPS Certificate



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

SUBMIT

- Restart the SmartTAP 360° Live server.

Loading Digital Files Certificate









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

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

- Open the Digital Signature page (**System** tab > **Media** folder > **Digital Signature**).
- Select the appropriate certificate from the Certificate list box.

- Click **SUBMIT**.

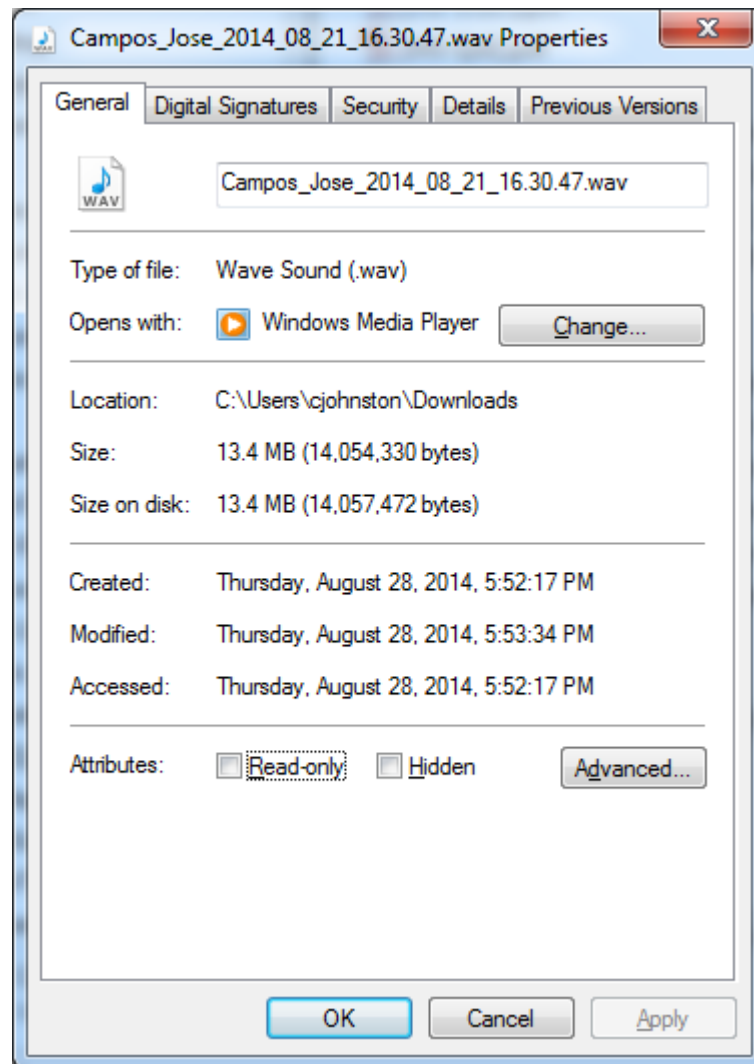
Figure 6-27: Digital Signature

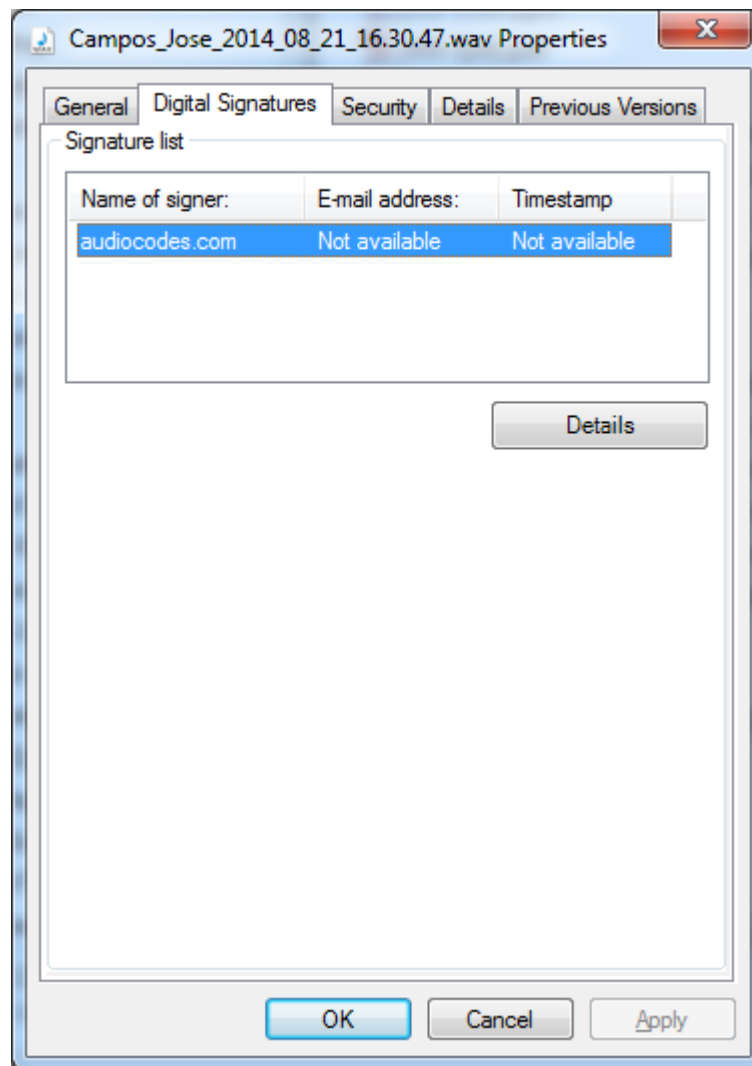
View/Modify Retention Policies				
Name	Description	Evaluation Retention Rule	Days	Modify
Default	Default Retention Group	DELETE_CALLS_KEEP_EVALS	365	
British Columbia	90 Days	DELETE_CALLS_AND_EVALS	90	
Energy calls	365	KEEP_CALLS_AND_EVALS	365	
One Year	Hold Call for One Year	DELETE_CALLS_AND_EVALS	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	
<div> 20 ▼ << 1 >> (1 of 1) </div>				

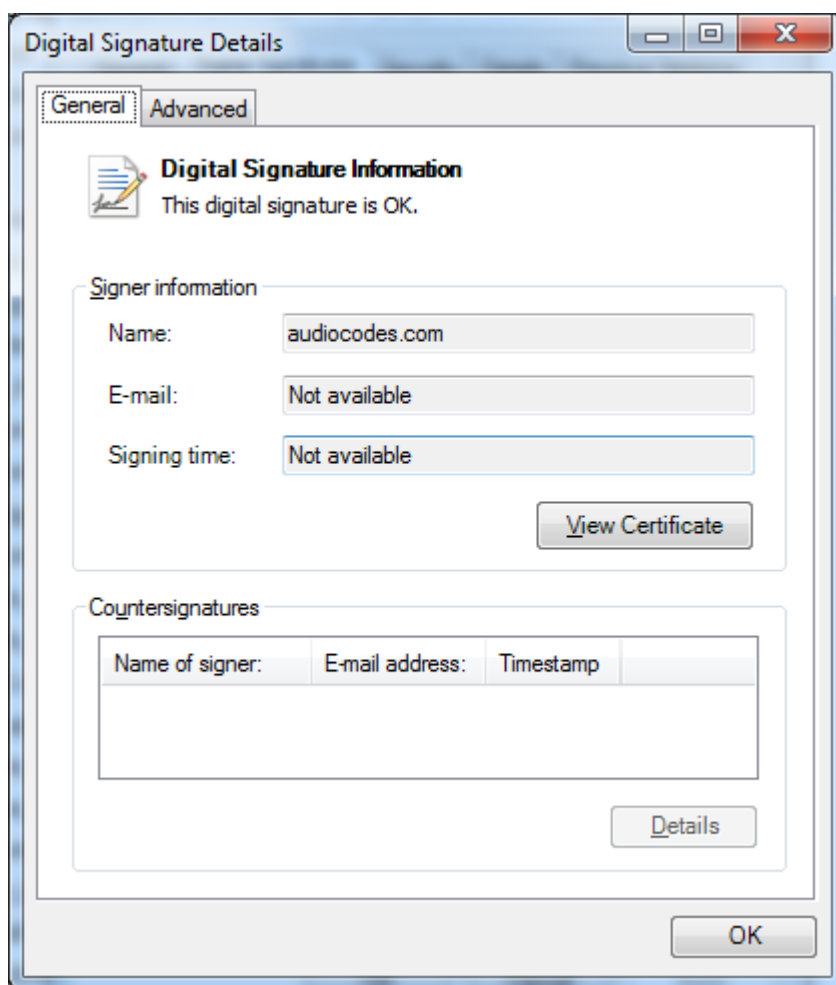
If a user 'optionally' chooses to add a Digital Signature during the download process, the configured certificate is used to digitally sign the audio file. The SmartTAP 360° Live Digital Signature file properties add-on must be installed on the local user PC to properly view the digital signature in the downloaded audio file.

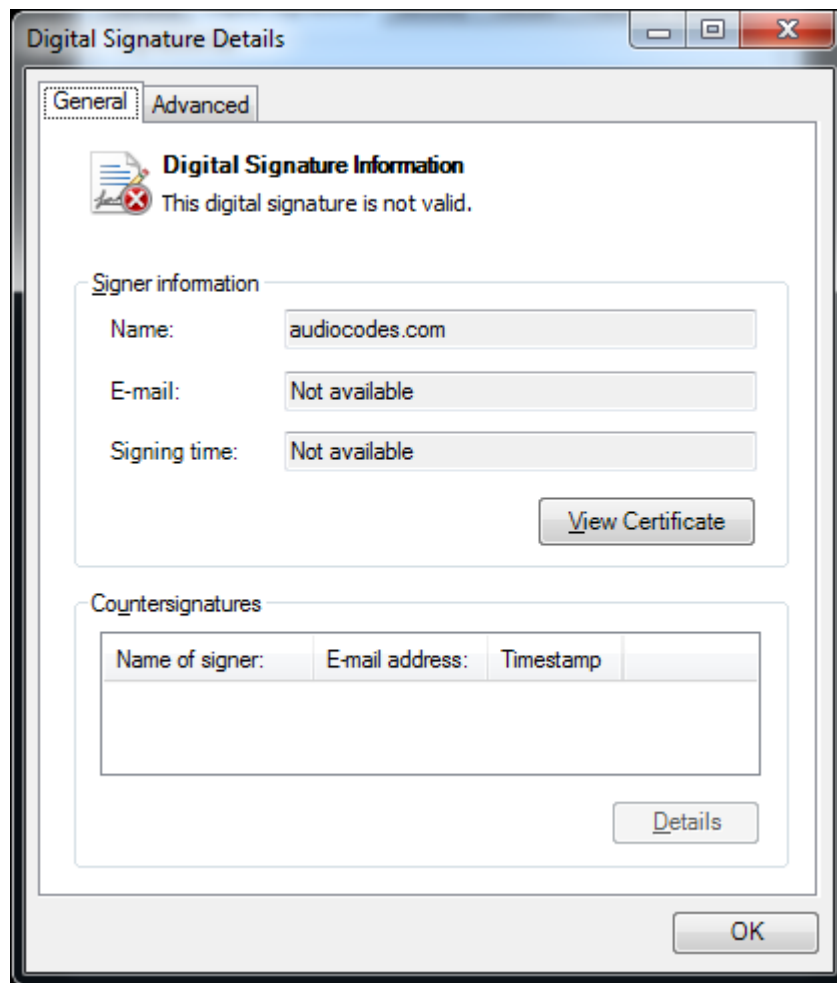
Once installed, the Digital Signatures tab appears in the file properties of the downloaded audio recording. Click it to view the certificate and make sure it's from a trusted source. The certificate must be installed on the local PC in the Trusted Root authority.

Figure 6-28: Digital Signature Details









For instructions on how to install the add-on, refer to the *SmartTAP 360° Live 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° Live 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 6-29: Call Retention Screen – Add Retention Policy
Table 6-10: 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 6-11: 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 describing the policy and to whom it applies.
4. Enter the value for the Call Retention Period.
5. Select the appropriate 'Evaluation Retention Rule' assuming Evaluation is enabled.
6. Click  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  to apply changes.

Figure 6-30: 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	

20 ▼ |<< << 1 >> >>| (1 of 1)

Save on Demand Call Retention

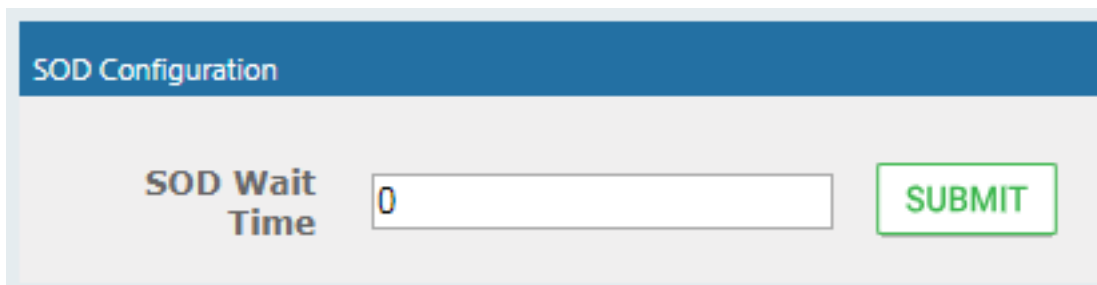
This feature enables the recording of a Save on Demand call after the call is no longer active. Such a call can be recorded after an elapsed time period of up to 10 minutes. By default, this parameter is set to 0 (a Save on Demand call cannot be recorded after it is no longer active).

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 6-31: SOD Configuration



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:

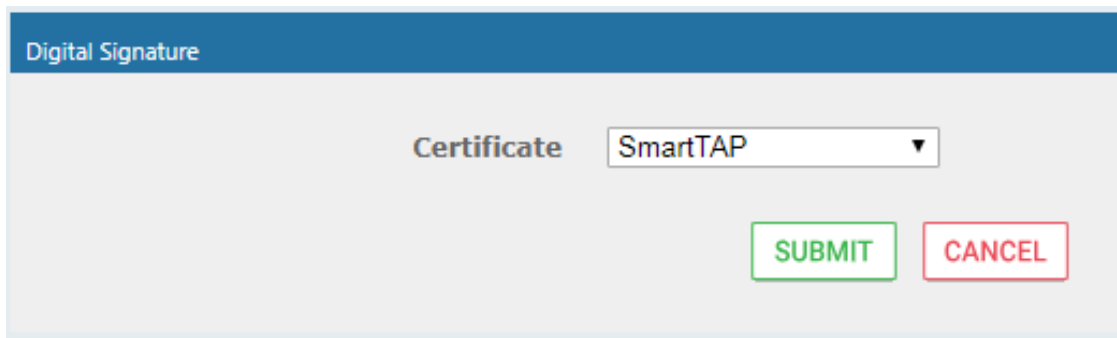
- Digital Signature to ensure that a recording is authentic.
- SMTP interface to allow the SmartTAP 360° Live server to send outbound emails
- LDAP interface to allow SmartTAP 360° Live to use Active Directory users, groups, and security profiles
- Media storage location which may be stored on a network 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 54.

Figure 6-32: Digital Signature



The screenshot shows a 'Digital Signature' configuration window. It has a blue header bar with the title 'Digital Signature'. Below the header, the word 'Certificate' is displayed next to a dropdown menu currently set to 'SmartTAP'. At the bottom right of the window, there are two buttons: a green 'SUBMIT' button and a red 'CANCEL' button.

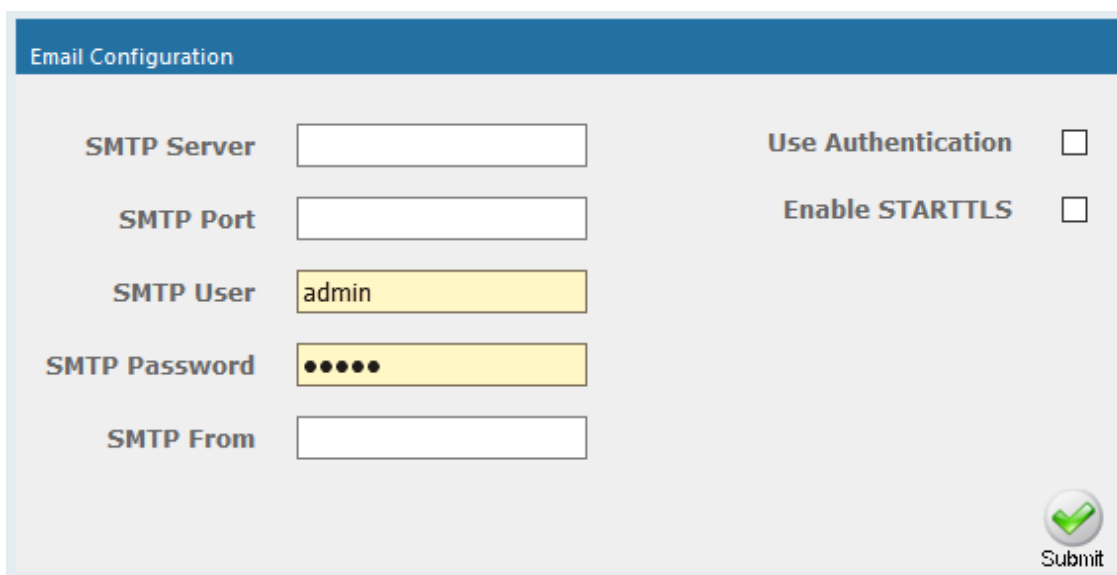
Configuring Email Server Settings

SmartTAP 360° Live 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 6-33: Email Configuration





The screenshot shows the 'Email Configuration' screen. It has a blue header bar with the title 'Email Configuration'. Below the header, there are several input fields and checkboxes. On the left, there are labels for 'SMTP Server', 'SMTP Port', 'SMTP User', 'SMTP Password', and 'SMTP From', each followed by an input field. On the right, there are two checkboxes: 'Use Authentication' and 'Enable STARTTLS'. The 'SMTP User' field contains the text 'admin', and the 'SMTP Password' field contains six dots. At the bottom right, there is a green circular icon with a checkmark and the word 'Submit' below it.

2. Enter the SMTP server information (provided by the SMTP administrator).
3. Use the table below as reference.

Table 6-12: Email Screen

Field	Description
SMTP Server	Hostname or IP address of the email server.
SMTP Port	TCP port of the email server.

Field	Description
SMTP User	Email user for authentication. By default, SmartTAP 360° Live will send emails from <a href="mailto:CallRecording@<SNMPServerDomain>.com">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 STARTTLS	Select the option when the SMTP server requires TLS.
	Applies the changes.

4. Apply changes (SmartTAP 360° Live tests the Email interface when the user clicks the  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° Live 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 6-13: Media Folder

Item	Description
Credentials	Sets the credentials to access the media recording locations. The

Item	Description
	credentials should be valid for all defined locations. See Configuring User Credentials below. See also Configuring User Credentials for Microsoft Teams Deployments on the next page.
Add Recording Location	Defines and adds a new media storage location. See Adding a Recording Location on page 77. See also Adding a Recording Location for Microsoft Teams Deployments on page 78
View/Modify Rec. Locations	Allows viewing and modifying an existing media location. SmartTAP 360° Live 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 81
Recording Format	Defines a recording format, e.g., encryption and compression. See Defining a Recording Format on page 82
Live Monitoring Location	The Live monitoring feature allows users to listen to calls in real time. See Configure Live Monitoring Location on page 83

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° Live 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 77) 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 configure user credentials:

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

Figure 6-34: Credentials

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

Table 6-14: 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 .

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° Live 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 78), otherwise, the attempt to add the location will fail.

➤ To configure credentials for Microsoft Teams deployments:

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

Figure 6-35: Credentials

The image shows a web form titled "Credentials". It has three input fields: "Username" with the value "NULL", "Password", and "Domain". A green "SUBMIT" button is located at the bottom right of the form.

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

Table 6-15: 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. Leave this value blank if the domain is the default value "core.windows.net". This value is shown as the "EndpointSuffix" in the Azure Portal.

For extracting these credentials, see [Extracting User Credentials from Microsoft Azure Fileshare Account](#) on the next page

Table 6-16: Credentials for Accessing a Microsoft Blob Account

Parameter	Description
Username	Specify the storage account name where the Blob container was created.
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 75

Figure 6-36: Microsoft Azure Storage Credentials

3. Click

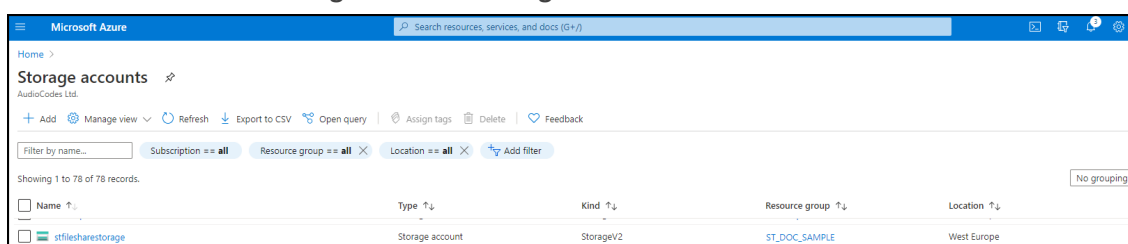
Extracting User Credentials from Microsoft Azure Fileshare Account

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

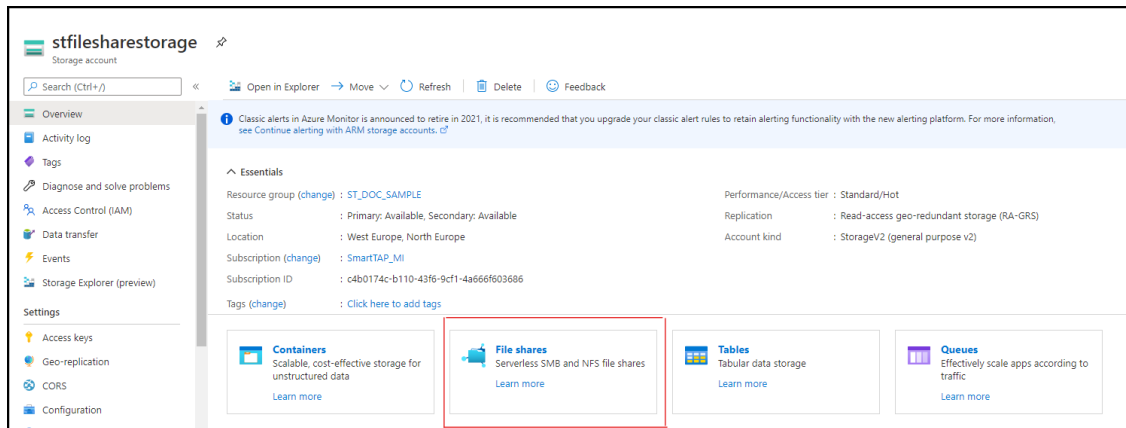
- Azure Storage Address
- Storage Domain\Username
- Storage password
- Fileshare name

➤ To extract these credentials from Microsoft Azure:

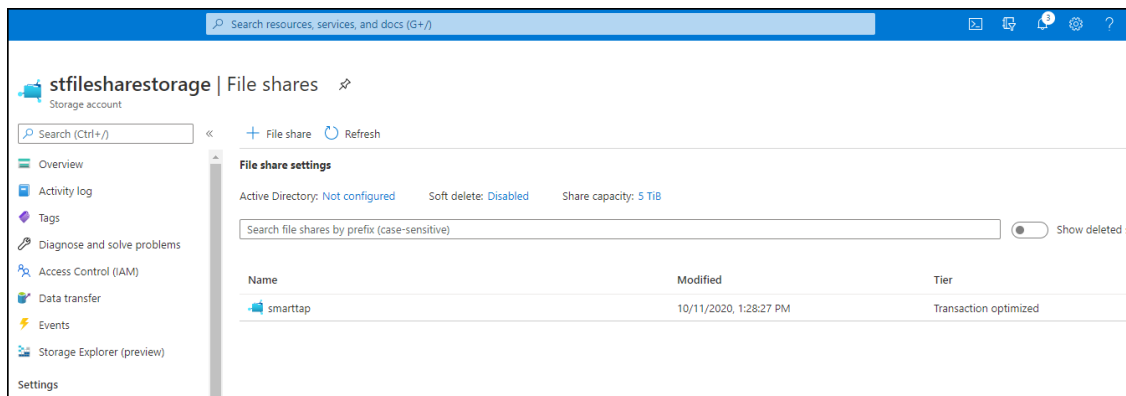
1. Go to **Azure Portal > Storage Accounts**.

Figure 6-37: Storage Accounts

2. Double-click the relevant storage account.

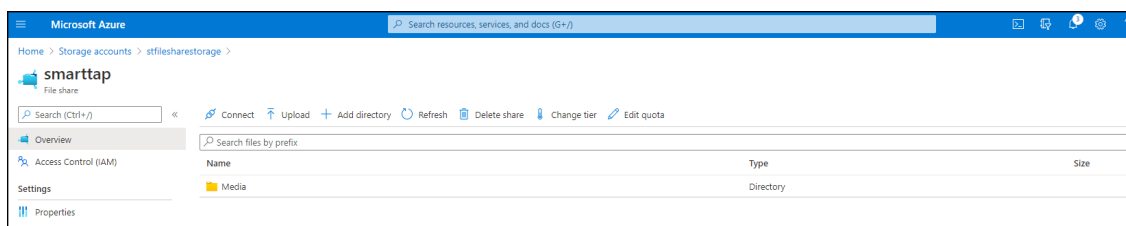
Figure 6-38: File Shares

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

Figure 6-39: File Share Settings

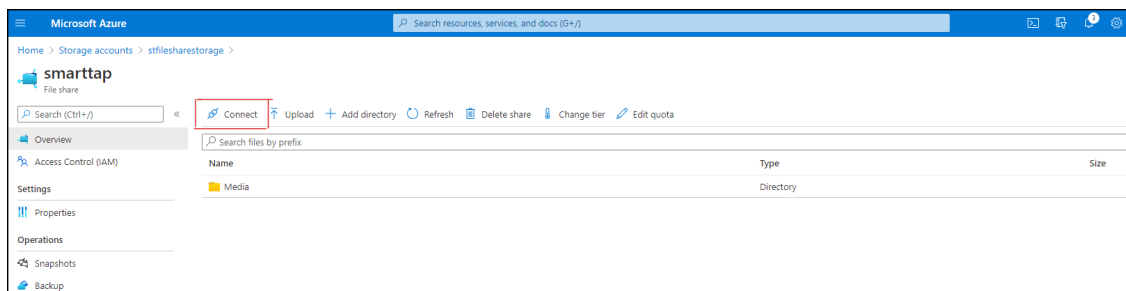
4. Copy the relevant File share name and click on it.

Example: Fileshare name="smarttap"

Figure 6-40: Media Directory Name

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/fbeB7tR3CFBCX71JWCQgj9xdJmBmX38fcAsn0EioGTaEw==`" "
```

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/fbeB7tR3CFBCX71JWCQgj9xdJmBmX38fc
Asn0EioGTaEw==

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° Live BOT in the Microsoft Teams deployment.

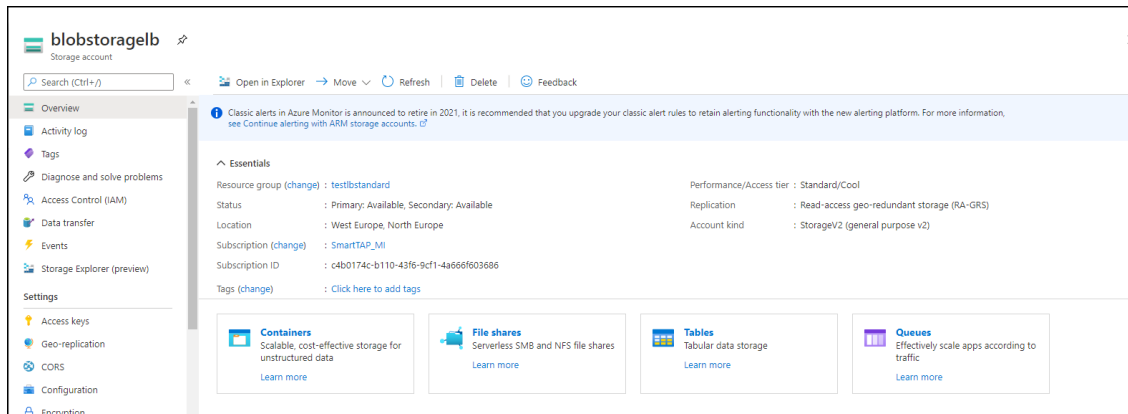


When the Microsoft Teams deployment is hosted in the customer's Azure subscription, the SmartTAP Server can be deployed On-premises, utilizing the On-premises Server Message Block (SMB) storage for media storage (described in [Viewing and Modifying a Recording Location](#) on page 81). You cannot configure both On-Premises and Blob Storage.

➤ **To configure Microsoft Blob:**

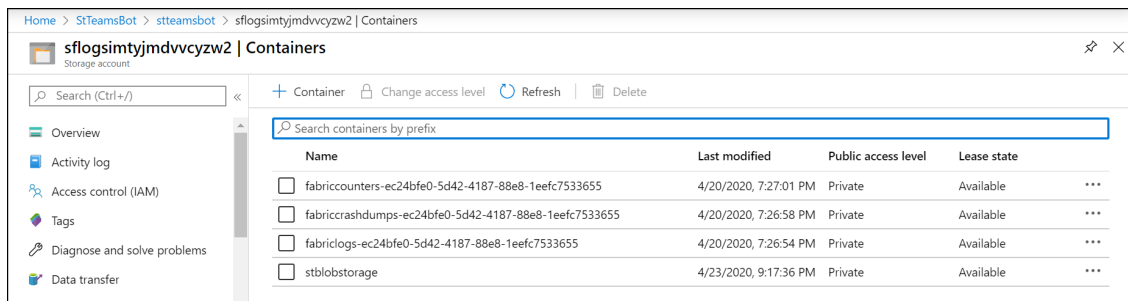
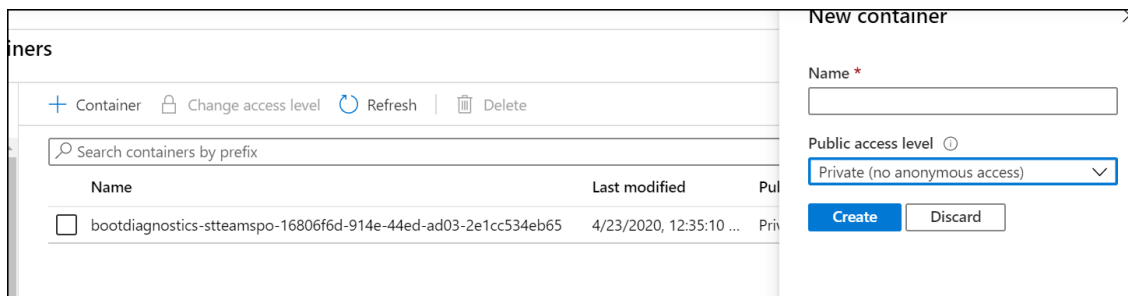
1. Login to the Microsoft Azure portal (<https://portal.azure.com/>).
2. Open the Storage account settings page.
3. Create or use existing storage account.

Figure 6-41: Microsoft Blob Storage Account



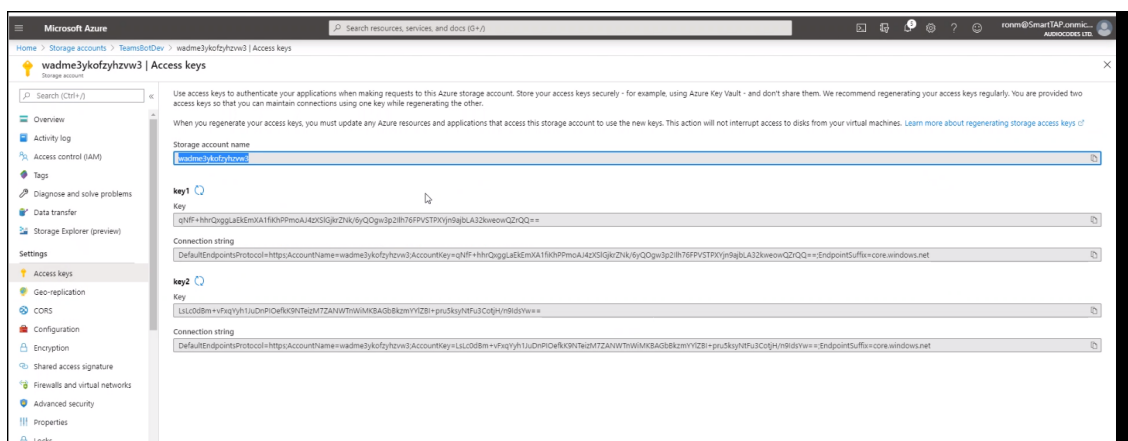
4. Save the storage name for SmartTAP 360° Live settings.
5. Create a new container for BLOB media storage and save the name.

Figure 6-42: Create New Blob Container



6. Save the storage name and credentials.

Figure 6-43: Storage Name and Credentials



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° Live 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 70) 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 the next page

Figure 6-44: Add Recording Location

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

Table 6-17: 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: <ul style="list-style-type: none"> ■ Server Message Block (SMB) Shared File

Parameter	Description
	<div> <div></div> File (local) </div>
Host	The IP address or FQDN of the SMB Scheme host machine.
Path	Defines the media path pattern.

Figure 6-45: Add Recording Location

3. Click



- 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° Live 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° Live 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 71)

Figure 6-46: Add Recording Location

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

Table 6-18: 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

Parameter	Description
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 73

Figure 6-47: Microsoft Azure Fileshare Recording Location

The screenshot shows a web form titled "Add Recording Location". It contains the following fields and values:

- Location Name:** SmartTAP Azure
- Description:** SmartTAP Azure Storage Account
- Scheme:** smb (selected from a dropdown menu)
- Host:** stfilesharestorage.file.core.windows.net
- Path:** '/smarttap/Media/'yyyy'/MM'/dd'/HHmmss

At the bottom right, there are two buttons: a green "SUBMIT" button and a red "CANCEL" button.

Table 6-19: 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 75

Figure 6-48: Microsoft Blob Recording Location

The screenshot shows a web form titled "Add Recording Location". It contains the following fields:

- Location Name:** Text input field containing "Azure Blob".
- Description:** Text input field containing "Azure Blob Storage".
- Scheme:** Dropdown menu with "https" selected.
- Host:** Empty text input field.
- Container:** Text input field containing "SmartTAPBlobStore".

At the bottom right of the form are two buttons: a green "SUBMIT" button and a red "CANCEL" button.

3. Click .



- If you define the media location in a different domain to the SmartTAP 360° Live 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 6-49: View/Modify Recording Locations - with Default Location Only

The screenshot shows a table titled "View/Modify Recording Locations". The table has columns for "Location Name", "Path", "Description", "Modify", and "Remove".





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

Figure 6-50: 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		

- Click  to open the Modify Recording Location screen.

Add Recording Location

Location Name

Description

Scheme

Host

Path

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

Table 6-20: 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). For Microsoft Blob storage: Scheme=https. "Container" field replaces "Path".
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 6-51: Recording Format

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

Table 6-21: Recording Format

Parameter	Description
Audio Encoding	<p>From the drop-down list, choose one of the following:</p> <ul style="list-style-type: none"> ■ g711Ulaw (uncompressed storage) ■ g711Alaw (uncompressed storage) ■ g729 (compressed storage) <p>'Encryption' check box: Select this option to encrypt media files as they are recorded. Files are encrypted using AES 128 bit key encryption.</p>
Video Encoding	Video recordings are by default saved in MP4/H.264 format (not configurable).

3. Click  to submit changes.

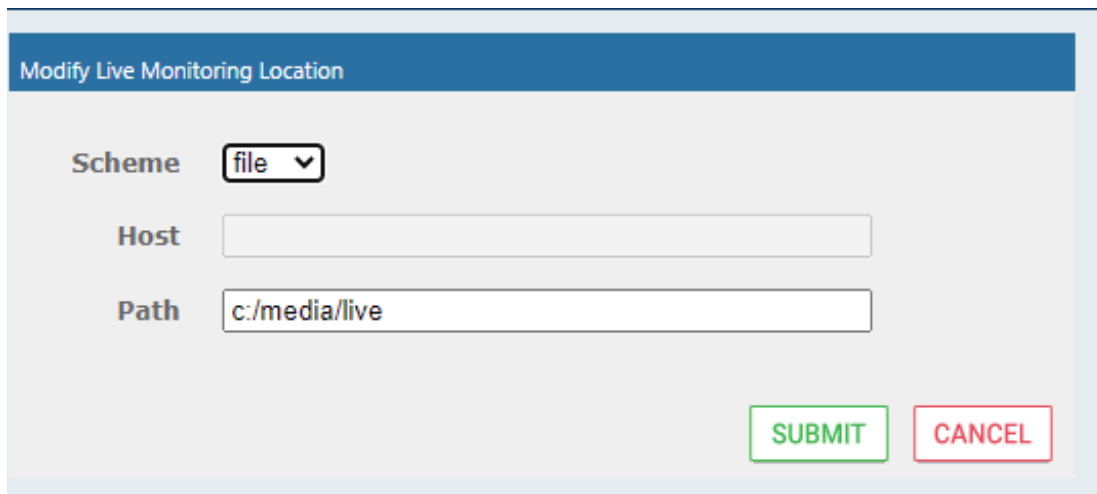
Configure Live Monitoring Location

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° Live client and can be played back by the user by clicking the Live Monitor microphone button (see [Determining User/Device Status](#) on page 21).

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

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

Figure 6-52: Modify Live Monitoring Location



In this page, the following can be configured:

- **Scheme:** A protocol for storing and retrieving live monitoring files. The following optionSchemes are available:
 - **File:** Used when recordings are stored on the same server as the Application Server.
- **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 70).
- The HTML5 Live Monitoring player is not supported for the SMB scheme (only Flash player is supported).

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

Figure 6-53: Modify Live Monitoring Location-Successfully Update

• *Live Monitoring location successfully updated.*

Modify Live Monitoring Location

Scheme

file ▼

Host

Path

/media/live

SUBMIT

CANCEL

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

Figure 6-54: Modify Live Monitoring Location-Update Error

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

Modify Live Monitoring Location

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 (Microsoft Edge, 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° Live 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° Live.



The SmartTAP 360° Live 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 6-55: Single Sign-On

The screenshot shows the 'SSO Configuration' page. At the top, there's a blue header with 'SSO Configuration'. Below it, a section titled 'Single Sign-On (Kerberos)' contains four fields: 'Enable SSO' with a checked checkbox, 'KDC' with the value 'aiads01.corp.audiocodes.com', 'Principal' with the value 'HTTP/smarttap.corp.audiocodes.com@CORP.AUD', and 'Password' which is empty. A green 'SUBMIT' button is located at the bottom right of the configuration area.

2. Configure the parameters described in the table below.

Table 6-22: 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° Live.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 .
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 203 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 6-56: Session Timeout

Session Timeout Configuration

Session Timeout (in min.)

2. Specify the appropriate Session Timeout.
3. Click 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° Live 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 6-57: LDAP Connection Configuration

Add LDAP Configuration

Host Principal Use SSL ☐

Port Password

User Mappings

Base Context

Mapping Filter

First Name

Last Name

Login

Email

Alias

OID

☒ One Level ☐ Subtree

Base DN	Filter	Search Scope	Modify Mapping	Delete
No records found.				

[Group Mappings](#)

[Security Group Mappings](#)

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

Table 6-23: 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 on the next page.

➤ **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° Live:**

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  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° Live and AD for all LDAP transactions.

➤ **To enable encryption between SmartTAP 360° Live 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° Live server, copy from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----.

Figure 6-58: Copy Client Certificate From Active Directory

```

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
MRUwEwYKCZImiZPyLGBGRYFbG9jYVWwxFzAUBgoJkiaJk/IsZAEZFgdXVWxhYkU
MRgwFgYDUQDEw9xYVWxhYkUFLUFEREMtQ0EwHhcNMTUwOTMwMTM1MTMwHhcNMzEx
MDAxMDAwMTI5UjBKMURwEwYKCZImiZPyLGBGRYFbG9jYVWwxFzAUBgoJkiaJk/Is
ZAEZFgdXVWxhYkUFLUFEREMtQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggE
KAoIABAQC2dHX0Cdu4kGZX/drEv9fU+YHUtqidi9A9lxeRlG8pMCnOUBUPq/+rg77z
I9rMMYzvoGAw5uLImx+2oikrcY+zFpZd+gGJw2r46YwpUwAP5jd3hgg4kbwDpxv
XmSiXfw4CDYTD0oN4Gute+38miejzWd25vPY5qski/ihUKQteAlip1FFFLY+zLm
KR71yvLt5vXveZijp8Q8DnZWw7ARQ1TtsJulQ+d3UbfN7/clc8a4hsUxFTp4bTSq
8Uf6cv9HSoj9QD8GtTLqc5+We6So/JS6HtK5Fr2TKkoIYGD1ejiXZBj0cd0Bx
Ffha8jyCSWCYA405S6bJQMUUC/AtAgMBAAGJUTBPMA5GA1UdDwQEAwIBhJA PBg
NUHRMBAF8EBTADAQH/MB0GA1UdDgQWBRRh4ofriwZMGK6kLidd8PRjoc2nDAQBgk
rBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAAOCAQEASusySykyIvZoi+9N1M
OfR+QFt0RWbjaw2goWCMUxT/Xl1Slsx2bPHIUYujDlM4t9b/FJWu16FU+wpWz
yjk40Lp8uIPmyoBhtw6vTXnJ3wnC9fb6eDSjL1jx6dOLrQh7XShPhNI0+zDJZ0
B2ggLHUPE1T3jK3zFFi02Sjlg5wqlbA8mDdcw0pkbGqGIBncSZtUDhNFug500s
G1QksmDUiRoXlkZ9bWau+f2zS8ESGelfCEXX1BdfxGBFIbECzwUkz9MJ0/mcXcX
J0dGZ45MdLedt0maDgZhEXytpFNeDWN0YpQJWhrdExsxYSftsZkBB6trtS7vptX
72kk+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>

```

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

```

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

```

Figure 6-59: Copy Client Certificate to SmartTAP 360° Live 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 location for the client.crt file .
- When prompted Trust this certificate? [no]: enter yes to confirm the key import.


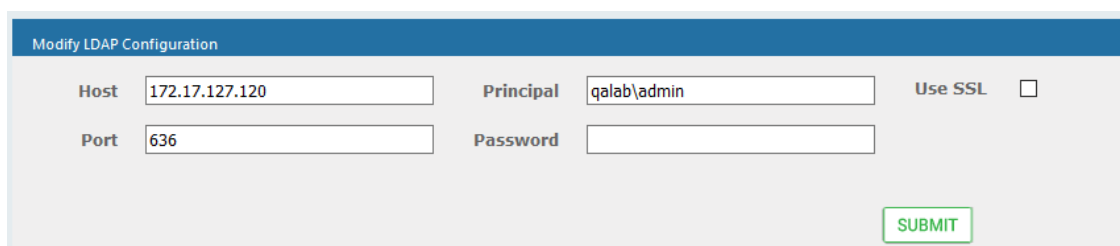

- Restart the SmartTAP 360° Live Application server for the new certificate to be loaded.
- The default port for LDAPS (LDAP with SSL support) is 636 (see the figure below).
- Check the 'Use SSL' checkbox (see the figure below).
- Click  to continue (see the figure below).

Figure 6-60: LDAP SSL Configuration



Modify LDAP Configuration			
Host	<input type="text" value="172.17.127.120"/>	Principal	<input type="text" value="qalab\admin"/>
Port	<input type="text" value="636"/>	Password	<input type="text"/>
			Use SSL <input type="checkbox"/>
			

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](#) below)
- Group Mappings ([Configuring Group Mappings](#) on page 96)
- Security Group Mappings ([Configuring Security Group Mappings](#) on page 99)



The retrieved LDAP Active Directory data i.e. member, name and description cannot be modified in SmartTAP, only directly from Active Directory.

Configuring User Mappings

The procedure below describes how to configure User Mappings.



➤ To configure User Mappings:

- Open the User Mappings screen shown below.

Figure 6-61: User Mappings

2. Use the table below as reference.

Table 6-24: User Mappings – Field Descriptions

Field	Description
User Mappings	<ul style="list-style-type: none"> ■ User Base Context (LDAP path for users). ■ User Filter (Create / Manage User filter). ■ First Name (LDAP Attribute that maps to the user first name). ■ Last Name (LDAP Attribute that maps to the user last name). ■ Login (LDAP Attribute that maps to the user login. The login should map to an attribute that contains a unique value across all LDAP providers, else users with the same login value will be considered the same user). ■ Alias (LDAP Attribute that maps to the user alias, nickname, or employee ID). ■ One Level – Retrieves LDAP attributes for the selected node. ■ Subtree – Retrieves LDAP attributes for the selected node and all its child nodes in the LDAP directory tree. ■  = expand screen ■  = shrink screen


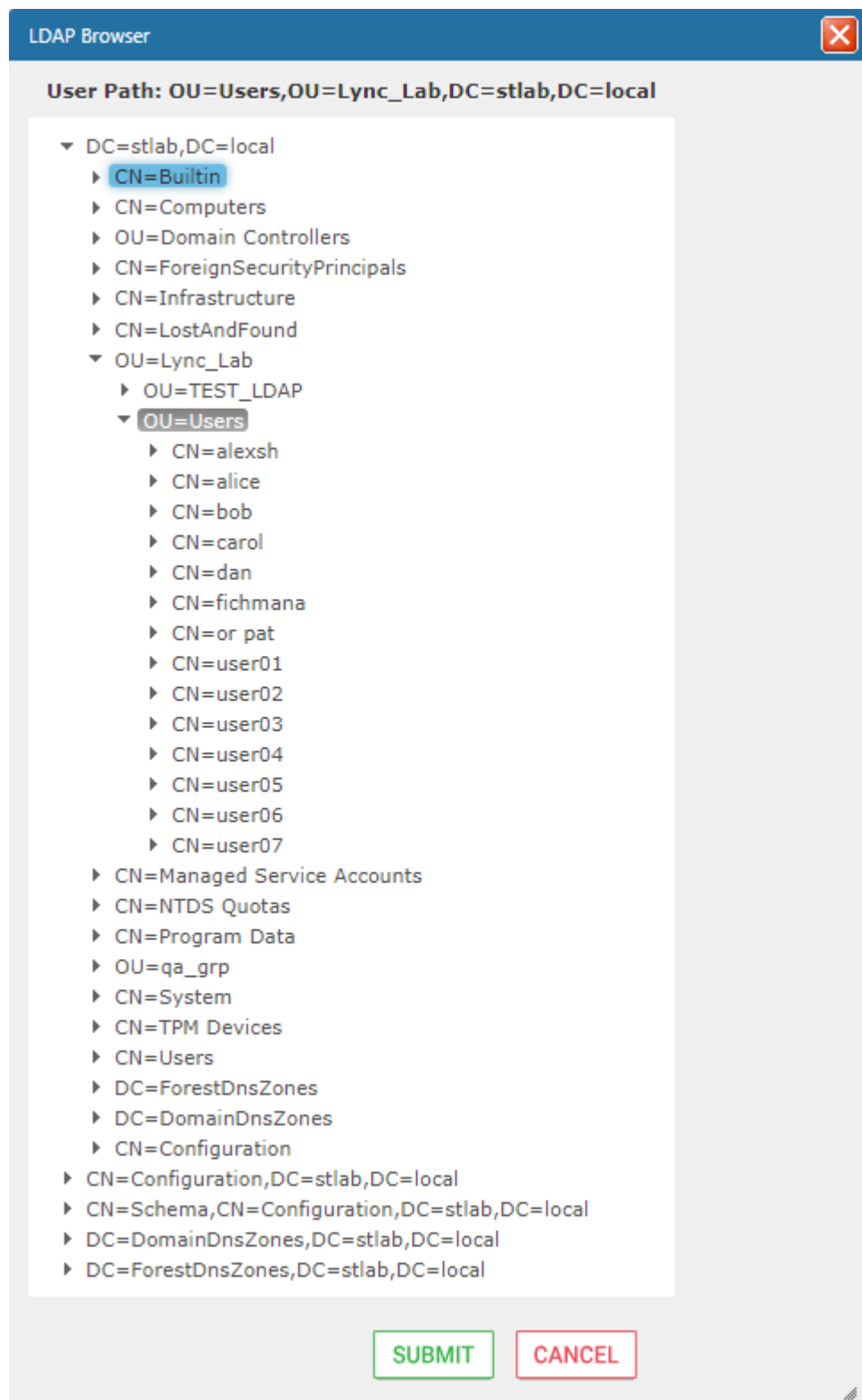
3. Enter the User Mappings Information in the 'User Mappings' screen (click  if necessary to expand the screen).
4. The default user location in Windows is displayed as follows:
OU=Ai-Logix,OU=USA,OU=AudioCodes,DC=corp,DC=AudioCodes,DC=com
5. Click **Browse** and navigate to the appropriate OU.

Figure 6-62: LDAP Browser



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:**




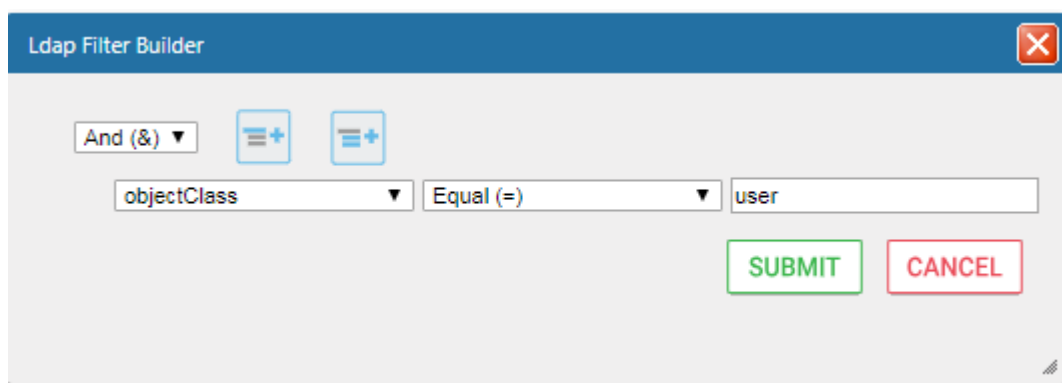
1. Select the **Create Filter** button.
2. Select the appropriate Conditional Operator (And, Or, Not)
3. Select the appropriate Attribute
4. Select the appropriate Equality Operator (>=, =, ~=, <=)
5. Specify value = (objectClass = user) recommended
6. Click  to apply changes.
7. Click the  icon to add 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 6-63: LDAP Filter Builder Example



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

Figure 6-64: User Filtering Screen

User Mappings

Base Context:

Mapping Filter:

First Name:

Last Name:

Login:

Email:

Alias:

Username:

☒ One Level ☐ Subtree

Base DN	Filter	Search Scope	Modify	Delete
No records found.				

Group Mappings

Security Group Mappings

11. Click  to apply changes.

Figure 6-65: User Mapping Configured

User Mappings

Base Context:

Mapping Filter:

First Name:

Last Name:

Login:

Email:

Alias:

Username:

☒ 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	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>


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

Figure 6-66: 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	erich			
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			
<div> 20 1 2 3 4 (1 of 4) </div>						

Configuring Group Mappings

The procedure below describes how to configure Group Mappings.



LDAP Active Directory Groups cannot be edited or removed in SmartTAP, only directly from LDAP Active Directory.

➤ To configure Group Mappings:

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


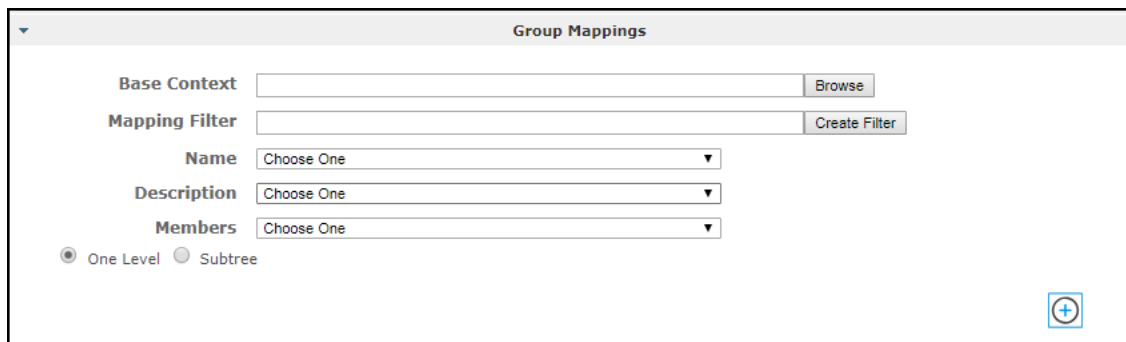


2. Open the Group Mappings screen (click  if necessary to expand screen).


Figure 6-67: Group Mappings



3. Use the table below as reference.

Table 6-25: Group Mappings - Field Descriptions

Field	Description
Group Mappings	<ul style="list-style-type: none"> ■ 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 .
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 6-68: Group Filter



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 6-69: Group Filtering Screen




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

Figure 6-70: Group Mapping Configured

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 6-71: 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° Live Security Profiles.



By default, new security profiles are granted no SmartTAP 360° Live 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 6-72: 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 6-26: 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.)

Field	Description
	<p>The members attribute should contain a collection of distinguished names of users that belong to the group.)</p> <ul style="list-style-type: none"> ■ 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:**


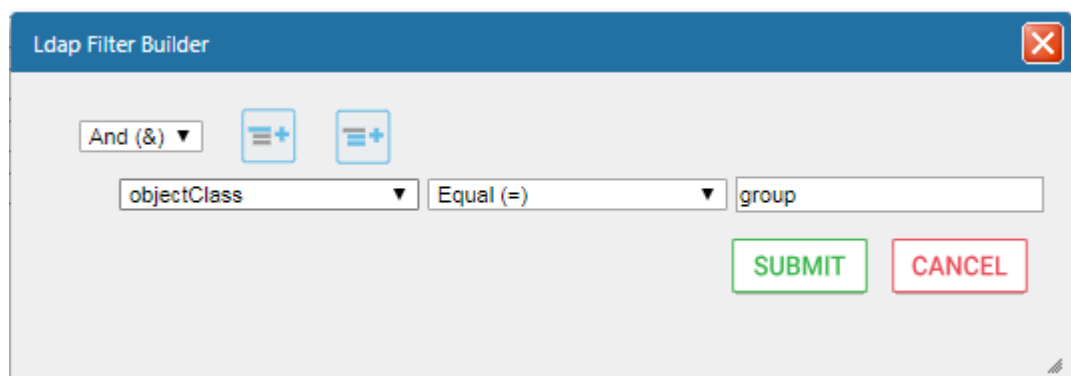
1. Select the appropriate Conditional Operator (And, Or, Not).
2. Select the appropriate Attribute.
3. Select the appropriate Equality Operator (>=, =, ~=, <=).
4. Specify a value.
5. Click  to apply changes.

Figure 6-73: Security Group Filter






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  to apply changes.

Figure 6-74: Security Group Filtering Screen

Security Group Mappings

Base Context:

Mapping Filter:

Name:

Description:

Members:

☒ One Level ☐ Subtree

Base DN	Filter	Search Scope	Modify	Delete
No records found.				

9. Click  to apply changes.

Figure 6-75: Security Group Configured

Security Group Mappings

Base Context:



Mapping Filter:


Name:

Description:

Members:

☒ 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° Live is managed under 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° Live components and forwarded to OVOC from the SmartTAP 360° Live Application server. OVOC Agents are installed on the SmartTAP 360° Live Application server for this purpose. For more information, refer to the *SmartTAP 360° Live Installation Guide*).

➤ To configure the connection with the OVOC server:

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

Figure 6-76: OVOC Settings

View/Modify OVOC settings

OVOC Connection

IP Address : 10.3.180.45

Trap Port : 162

Keep Alive Port : 1161

SNMP

☒ SNMP v2 ☐ SNMP v3

Community Read : public

Community Write : private

System Info

Name : SmartTAP

Location : 133

Access Settings

Login URL : http://172.17.127.133/

SUBMIT **CANCEL**

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° Live and the OVOC server.

Figure 6-77: SNMPv3 Settings

View/Modify OVOC settings

OVOC Connection

IP Address : 0.0.0.0

Trap Port : 162

Keep Alive Port : 1161

SNMP

☐ SNMP v2 ☒ SNMP v3

Security Name : v3

Authentication Protocol : MD5

Authentication Key :

Private Protocol : DES

Private Key :

System Info

Name : SmartTAP

Location : 133

Access Settings

Login URL : http://172.17.127.133/

SUBMIT CANCEL

5. Configure System Information:

- Name

- Location
- Login URL- this login is used for logging into the SmartTAP 360° Live Web interface from OVOC (Device Information Page). Enter the SmartTAP Server **Public** IP address.

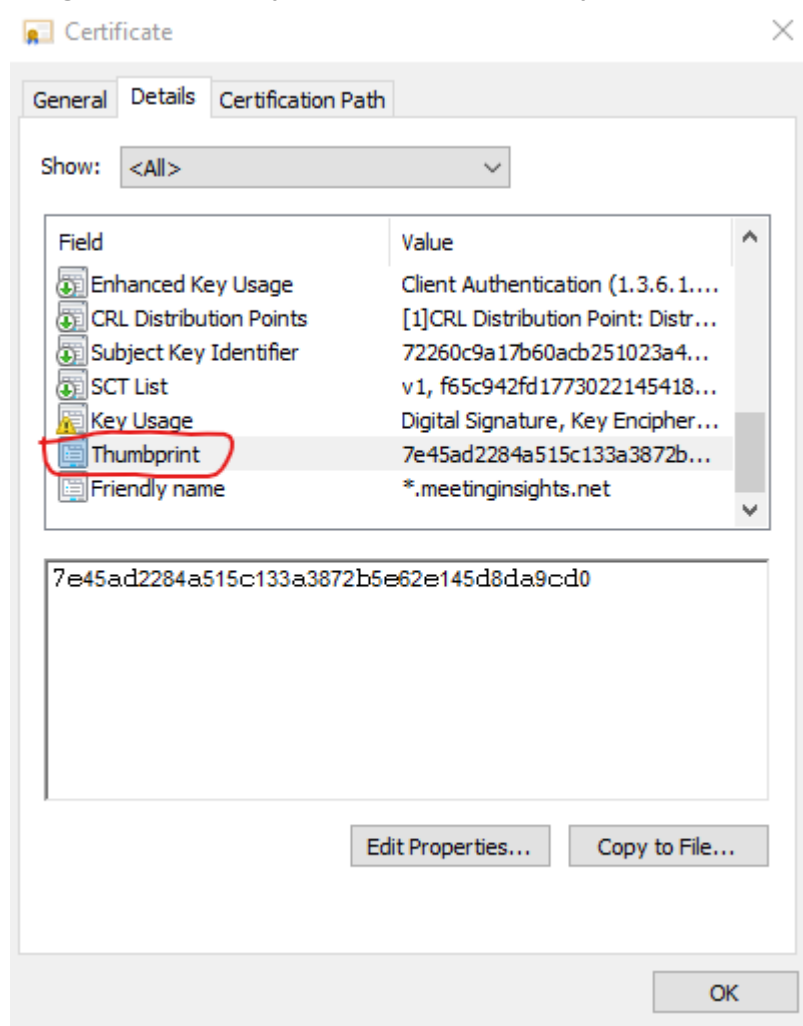
White Listing Certificate Files

This option lets you specify for which SmartTAP Microsoft Windows Server certificates, expiration notification alarms (acVaCompCertificateExpiredAlarm) are sent to OVOC. This prevents excessive notifications for redundant certificates from flooding OVOC. When “Whitelist” is configured—in the SmartTapAS_Monitor.json file, alarm expiration notifications are only sent to OVOC for those certificates listed under Whitelist . All other Microsoft certificates in the system are ignored and alarm notifications are not sent.

➤ To white list certificate files:

1. Retrieve the thumbprints of the certificates that you wish to configure. The thumbprint can be retrieved from the Certificate Details (see example figure below).

Figure 6-78: Example Certificate File Thumbprint



2. Open "C:\Program Files\Audiocodes\AlarmsAgent\Config\SmartTapAS_Monitor.json".

3. Add the thumbprint of the certificates you wish to monitor under "WhiteList".

Example

```
"CertificateExpired": {
  "IsOn": true,
  "MibName": "acGaCompCertificateExpiredAlarm",
  "ThresholdAndSeverityList": [
    {
      "Threshold": "30",
      "Severity": 4
    },
    {
      "Threshold": "2",
      "Severity": 5
    }
  ],
  "IgnoreList": [
    "245c97df7514e7cf2df8be72ae957b9e04741e85",
    "7f88cd7223f3c813818c994614a89c99fa3b5247",
    "18f7c1fcc3090203fd5baa2f861a754976c8dd25",
    "02faf3e291435468607857694df5e45b68851868",
    "a43489159a520f0d93d032ccaf37e7fe20a8b419",
    "cdd4eeae6000ac7f40c3802c171e30148030c072",
    "75e0abb6138512271c04f85fddde38e4b7242efe",
    "be36a4562fb2ee05dbb3d32323adf445084ed656",
    "dac9024f54d8f6df94935fb1732638ca6ad77c13",
    "75e0abb6138512271c04f85fddde38e4b7242efe",
    ""
  ],
  "WhiteList": [
    "1234-5678-90abc-def1",
    "abcd-5678-90abc-1234"
  ],
  "AlertWhen": 1,
  "Text": "Certificate '{1}' will expire in {0} days",
  "Source": null,
  "DefaultSeverity": null
}
```

```
},
```

4. Save the file.
5. Restart “OVOC Alarms Agent” service.

**** Not working with alias or subject ****

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 140
- [Update an Admin User](#) on page 144
- [Reset User Password](#) on page 145
- [Modify a User Password](#) on page 145
- [Uploading an Image](#) on page 146

➤ To add a user:

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

Figure 6-79: Adding a User

Add User

First Name Last Name

Email Login Id

Id / Alias SIP URI

TEL URI Retention Policy

Recording Profile Legal Hold

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






11. Click  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° Live 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 6-27: 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 Profiles	Lists the Security Profiles that can be assigned to the user. Highlighted items indicate the Security Profiles that have been assigned to the user. To assign/or remove Security Profiles from the user, hold down the <ctrl> 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 <ctrl> 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.

Field	Description
	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.
	Apply the changes.
	Cancel the changes.

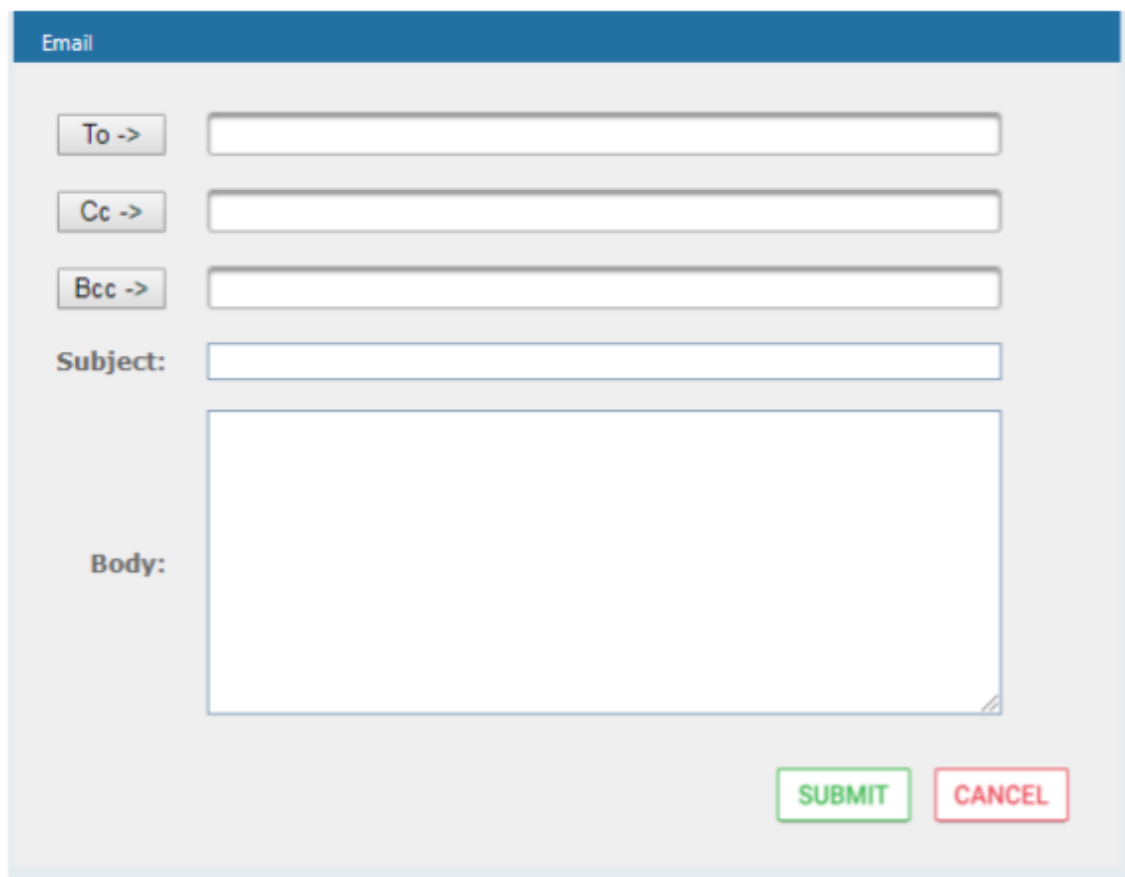
Sending Email

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

➤ To send an Email:



1. Open the New Email screen (**Users** tab > **Email** folder > **New Email**).

Figure 6-80: New Email



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

Table 6-28: 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 as 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.
	Sends the email.
	Cancels the email.

Managing Groups

This section describes how to manage groups:

- [Adding a Group](#) below
- [View and Modify Groups](#) on page 112

Adding a Group

This section describes how to add a new group of users/devices.

➤ To add a Group and associated sub groups:

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

Figure 6-81: Add Group

Add Group

Group Name

Group Description

☐ Show Inactive Users/Devices

NonMembers

- Adar, Tania
- agenttest1
- aitest, aitest
- Alyil veedu dhruva, Fnu
- Analytics User, Analytics User
- AutoAttendant
- Bauer, Eric

Members

Available Groups

- Agents-Test
- Analytics
- Company XYZ
- COO
- Default
- Demo
- Engineering




Sub Groups


SUBMIT **CANCEL**

2. Use the table below as reference.

Table 6-29: Group Screen Settings

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

Field	Description
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>
	Apply the changes.
	Cancel changes
	Delete Group – displayed only when you modify an existing group.

3. Enter the Group Name.
4. Enter the Group Description.
5. 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.
6. (Optionally, Sub Groups for the Group just being added can be entered from the Add Group screen).
7. Click .








View and Modify Groups

This section describes how to view and modify groups.

➤ To view/modify a Group:

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

Figure 6-82: View/Modify Group**Figure 6-83:**



View/Modify Groups			
Name	Description	Modify	Delete
Default	Default group		
rachels			
rachels test video			
rachelsTest	testingAAD		
racheltest3			
test4			





AudioCodes Azure Active Directory groups and LDAP Active Directory groups cannot be edited or removed in SmartTAP.

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

Figure 6-84: 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  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° Live resources.

- [Adding a Security Profile](#) on the next page

- [Viewing or Modifying a Security Profile](#) on page 116

Adding a Security Profile

This section describes how to add a Security Profile.

➤ To add a Security Profile:

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




Figure 6-85: Add Security Profile


2. Use the table below as reference.

Table 6-30: Security Profile Settings

Field	Description
Security Profile Name	The name of the new security profile.
Security Profile Description	Description of the new security profile.
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	Select this option to allow users with this security profile to access calls

Field	Description
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.
ROD/SOD	Select this option to record on demand and save on demand for 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 and IMs	Select this option to delete calls and instant message conversations according to the different user privileges described above. For more information, see Deleting Calls and Instant Messages on page 160.
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.

Field	Description
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° Live Web interface.
	Apply changes.
	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 .

Viewing or Modifying a Security Profile

This section describes how to modify a Security Profile.

➤ To view/modify Security Profiles:

1. Open the View/Modify Security Profiles screen.

Figure 6-86: View/Modify Security Profiles

View/Modify Security Profiles				
Name	Description	Permissions	Modify	Delete
STQATeam	SmartTAP QA Team			
ST-load-test-dynamic-rename	ST-load-test-dynamic			
supervisor	Supervisor	Tag calls Download Media Related to a call Live Monitor Email Media Related to a call Access calls within user's groups Play Media Related to a call		
agent_ROD_SOD	Agent	Tag calls ROD/SOD other users Download Media Related to a call Live Monitor Email Media Related to a call Access calls within user's groups Play Media Related to a call		
ST-Teams-Users				
administrator	Administrator	Create and modify users and groups Tag calls Download Media Related to a call Access all calls Email Media Related to a call Configure system Play Media Related to a call		



AudioCodes Azure Active Directory and LDAP Active Directory Security Profiles cannot be edited or removed in SmartTAP.

2. Click adjacent to the Security Profile that you wish to modify.

Figure 6-87: Modify Security Profile

Modify 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
 ☒ ROD/SOD other users



☒ Configure system
 ☒ Create and modify users and groups

SUBMIT

CANCEL

3. Use the table below as reference.

Table 6-31: 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
- Video and Screen Sharing – enable if Video and Screen Sharing recording are desired
- Pause or Resume – enable if the assigned 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

■ **Announcements:** Enables Announcements for one or more of the above call types.

■ **Recording Beep tone:** Plays a beep tone in the background during the recording.

■ **Instant Messages:** Enables Instant Messaging recording

This section includes the following:

- [Adding a Recording Profile](#) on the next page
- [Viewing or Modifying Recording Profiles](#) on page 125
- [Assigning Recording Profile to User or Device](#) on page 127
- [Managing Recordable Devices](#) on page 129
- [Recording Profile-Call Type Configuration Examples](#) on page 131

Adding a Recording Profile

This section describes how to add a recording profile.

➤ To add a Recording Profile:

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

Figure 6-88: Add Recording Profile

Recording Profile Name

Recording Profile Description

Call

Recording Type None

☐ Video
 ☐ Desktop Sharing
 ☐ Pause or Resume

Call type

Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☒ All

Internal ☒ Incoming ☒ Outgoing

PSTN ☒ Inbound ☒ Outbound

Federated ☒ Inbound ☒ Outbound

☒ Calls with Internal Conferences
 ☒ Teams Queue Calls (conference mode) *

* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☒ Referred by Response Group

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

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

Announcements

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

Call type

Internal	<input type="checkbox"/> Incoming ANN	<input type="checkbox"/> Play to calling party <input type="text"/>	<input type="checkbox"/> Play to answering party <input type="text"/>
	<input type="checkbox"/> Outgoing ANN	<input type="checkbox"/> Play to calling party <input type="text"/>	<input type="checkbox"/> Play to answering party <input type="text"/>
PSTN	<input type="checkbox"/> Inbound ANN	<input type="checkbox"/> Play to calling party <input type="text"/>	<input type="checkbox"/> Play to answering party <input type="text"/>
	<input type="checkbox"/> Outbound ANN	<input type="checkbox"/> Play to calling party <input type="text"/>	<input type="checkbox"/> Play to answering party <input type="text"/>
Federated	<input type="checkbox"/> Inbound ANN	<input type="checkbox"/> Play to calling party <input type="text"/>	<input type="checkbox"/> Play to answering party <input type="text"/>
	<input type="checkbox"/> Outbound ANN	<input type="checkbox"/> Play to calling party <input type="text"/>	<input type="checkbox"/> Play to answering party <input type="text"/>

☐ Record Announcement

Don't Play Announcement Destination Numbers :

☐ Block Calls on Announcements Unavailability

Applicable for MSFT Teams only

Recording Notification Enable on all recorded calls (default)

Recording Beep Tone

Applicable for Skype for Business and Lync A/V Recording. Beep can be played on the calls which media traverses Media Proxy Server

☐ Play Beep Tone

Instant Messaging

Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ Record Instant Messages

- 119 -

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 Announcements pane. For more information, use table below as a reference.
4. In the Announcements pane, assign audio files to playto the Calling party, the Answering party orboth 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 playto 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 247


- See example configurations in [Example Announcement Server Scenarios](#) on page 252

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

7. Click SUBMIT.

Table 6-32: 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	<p>Select one of the following:</p> <ul style="list-style-type: none"> ■ None (default): User is not recorded. Do not assign a recording profile to a user or device if you do not want to record them. ■ Full Time: (supported for Audio, Video, Instant messages and Video and Screen 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 decides to record. ■ Save on Demand: (supported for Audio, Video, and Video and Screen Sharing) recording will contain audio and/or video from the beginning

Field	Description
	<p>of the 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° Live Skype for Business Toolbar on page 231</p> <p>Audio/Video recording can be triggered from the GUI Status page or from the Skype for Business CWE toolbar.</p> <div>  <p>For Microsoft Teams, SmartTAP can be integrated into the Microsoft Teams client as a Personal App (Refer to Step 8 Setup SmartTAP Personal App in the <i>SmartTAP 360° Live Deployment Guide</i>).</p> </div>
Video	Record a video call (Full Time or Save on Demand).
Pause / Resume	<p>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.</p> <p>Pause/Resume of a recording can be triggered from the SmartTAP 360° Live Web interface status page or from the Skype for Business CWE toolbar.</p>
Instant Message	Automatic Instant Message recording for both Skype for Business recordings and Microsoft Teams recordings.
Video and Screen Sharing Recording	Recording of Video and Screen 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° Live users and devices regardless of the users or devices location (intranet, internet, mobile device).



The call types described in the table below are relevant for Microsoft Teams, Skype For Business; Audio; Video and and Screen Sharing recording.

Table 6-33: 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 Skype for Business calls with an Internal conference bridge in the Enterprise domain.
Teams Queue Calls (conference mode)	Record Microsoft Teams calls that have been retrieved from a queue by a call agent. The recording is triggered as soon as the call is connected to an agent.
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

Field	Description
	<p>user or device with the network mapping attributes that are associated with the response group (the Response Group URI).</p> <p>This configuration is applicable to Skype for Business integrations.</p>
Filter Calls User Receives Filter Calls User Makes	<p>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. 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: <code>^(1{1} \+1{1})?(732 609)\d*\$</code>. 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.</p> <p>This configuration is applicable to Skype for Business integrations.</p>

■ Announcements

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

Table 6-34: Announcements

Field	Description
Internal (incoming, outgoing)	<p>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”</p>

Field	Description
PSTN (inbound, out-bound)	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, out-bound)	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 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).
Recording Notification	<p>This option is applicable for Microsoft Teams recording notifications only and requires the customer to sign a waiver to allow AudioCodes to disable Microsoft notifications using this parameter. Alternatively audio notifications can be disabled through Microsoft Teams recording policy. By default, Microsoft notifications are enabled.</p> <p>The configuration options below are relevant for all call participants:</p> <ul style="list-style-type: none"> ■ Enable All: Recording notification are enabled for all calls (Default) ■ Disable All: Recording notifications are disabled on all calls (visual and audio notifications) ■ Disable PSTN: Recording notifications are disabled on PSTN calls (visual and audio notifications) <p>Note: This parameter is applicable for Teams Native Integration only.</p>
Configure Media Files to Play on Announcements	<ul style="list-style-type: none"> ● 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

Field	Description
	<p>example, PSTN_Inbound.wma</p> <ul style="list-style-type: none"> ANN and IVR files must be pre-saved to the StateMachineConfig folder on the ANN server: see 'Step 3-Configuring Announcement Server (Skype for Business)' in the <i>SmartTAP 360° Live Installation Guide</i>.

- **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 whose media traverses 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° Live Installation Guide*.

Field	Description
Play Beep Tone	The beep tone is played in the background during the call recording (disabled by default). The Beep tone can be played on the calls whose 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 6-89: 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	
<div> 20 ▼ << 1 >> (1 of 1) </div>						

2. Use the table below as reference.

Table 6-35: View/Modify Recording Profiles – Field Descriptions

Field	Description
Name	Recording Profile name, sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Description	Recording Profile description sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Audio Recording Type	Full Time, Record on Demand or Save on Demand.
Video Recording Type	Full Time or Save on Demand.



Field	Description
IM Recording Type	Full Time or None
Video and Screen 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° Live. 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  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° Live 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 6-90: 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
- Ilyae, 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

>> > < <<

SUBMIT CANCEL

2. Use the table below as reference.

Table 6-36: Add Users to Recording Profiles Screen

Field	Description
No Recording Profile	List of available Users / Devices in SmartTAP 360° Live unassigned to a specific recording profile.
Recording Profiles	Choose from one of the available recording profiles that were defined above to assign a User / Device (Full Time is the default profile)
>>	Add all available users / devices to a specific recording profile.
>	Add a user / device to a specific recording profile.
<	Remove a selected user / device from a specific recording profile.

Field	Description
<<	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° Live 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 6-91: Add Recordable Device

2. [Use the table below as reference] Enter a Name for the device.
3. Enter a Description for the device.
4. Select the Type from the dropdown menu.

5. From the list of Available Groups, select the groups and move them to the Assigned Groups by clicking the > / >> buttons.
6. Click Submit to apply changes.

Table 6-37: Recordable Device – Settings Descriptions


Field	Description
Name	Name of the new recordable device.
Description	Description of the new recordable device.
Type	Type of recordable device. Dropdown menu shows valid entries.
Retention Policy	Select an appropriate retention policy for the device.
Recording Profile	Select an appropriate recording profile for the device.
Available Groups	User groups available to assign to this device. Select groups by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>.
Assigned Groups	User groups assigned to this device. Select group by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>.
>>	Add all Available Groups to the Assigned groups.
>	Add selected Available Groups to the Assigned groups.
<	Remove selected Groups from the Assigned group.
<<	Remove all Groups from the Assigned group.
	Apply the changes.
	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 6-92: View/Modify Recordable Devices

View/Modify Recordable Devices





Name	Description	Type	Modify	Delete
<input type="text"/>	<input type="text"/>	Select		
Lobby Phone	Ext 5001	PHONE		
NCR	NCR Support	OTHER		
DCI	DCI Support	PHONE		
AutoAttendant	Corp AutoAttendant	ACD		
Menachem Honig-USA		PHONE		

20   1   (1 of 1)

2. Use the table below as reference.

Figure 6-93: 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 MSFT Teams, Skype for Business and Lync A/V Recording

☐ All

Internal ☐ Incoming ☐ Outgoing

PSTN ☒ Inbound ☐ Outbound

Federated ☐ Inbound ☐ Outbound

☐ Calls with Internal Conferences

☐ Teams Queue Calls (conference mode) *

* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☐ Referred by Response Group

Filter Calls User Receives : List Type: **Block** Numbers: Regular Expression:

Filter Calls User Makes : List Type: **Block** Numbers: Regular Expression:

■ Record all PSTN Calls:

Call type
Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ All

Internal ☐ Incoming ☐ Outgoing

PSTN ☒ Inbound ☒ Outbound

Federated ☐ Inbound ☐ Outbound

☐ Calls with Internal Conferences

☐ Teams Queue Calls (conference mode) *

* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☐ Referred by Response Group

Filter Calls User Receives : List Type: **Block** Numbers: Regular Expression:

Filter Calls User Makes : List Type: **Block** Numbers: Regular Expression:

■ Record External calls (PSTN and Federation):

Call type
Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ All

Internal ☐ Incoming ☐ Outgoing

PSTN ☒ Inbound ☒ Outbound

Federated ☒ Inbound ☒ Outbound

☐ Calls with Internal Conferences

☐ Teams Queue Calls (conference mode) *

* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☐ Referred by Response Group

Filter Calls User Receives : List Type: **Block** Numbers: Regular Expression:

Filter Calls User Makes : List Type: **Block** Numbers: Regular Expression:

■ Record PSTN Inbound calls and calls from Response Group:

Call type

Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ All

☐ Internal
 ☐ Incoming
 ☐ Outgoing

☐ PSTN
 ☒ Inbound
 ☐ Outbound

☐ Federated
 ☐ Inbound
 ☐ Outbound

☐ Calls with Internal Conferences

☐ Teams Queue Calls (conference mode) *

* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☒ Referred by Response Group

Filter Calls User Receives :

List Type :

Numbers :

Regular Expression:

Filter Calls User Makes :

List Type :

Numbers :

Regular Expression:

Adding a Device Attribute

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

Table 6-38: SmartTAP 360° Live Device Attributes

Attribute Purpose	Priority	Description
Trigger Recording	Critical	To designate to SmartTAP 360° Live 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° Live 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° Live, 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° Live attributes to Active Directory attributes to auto populate device information within SmartTAP 360° Live. To map a device attribute to an Active Directory device attribute, see [Configuring an LDAP Connection](#) on page 87

Table 6-39: User Attributes

User Attribute	Description
Name	Unique easily identifiable name to the attribute.
Description	Brief Description of the attribute.
Network	Indicates whether attribute mapping is required. When selected, the

User Attribute	Description
Mapping	'Network Mapping Type' drop-down list is available.
Network Mapping Type	<p>Indicates the type of network mapping that is required for the user. Choose from one of the following values:</p> <ul style="list-style-type: none"> ■ TEL_URI ■ SIP_URI ■ IP_ADDRESS ■ TERMINAL_ADDRESS ■ USERNAME ■ EXTENSION ■ TRUNK_ID ■ 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 AAD User Attribute](#) on page 136

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 6-94: 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.

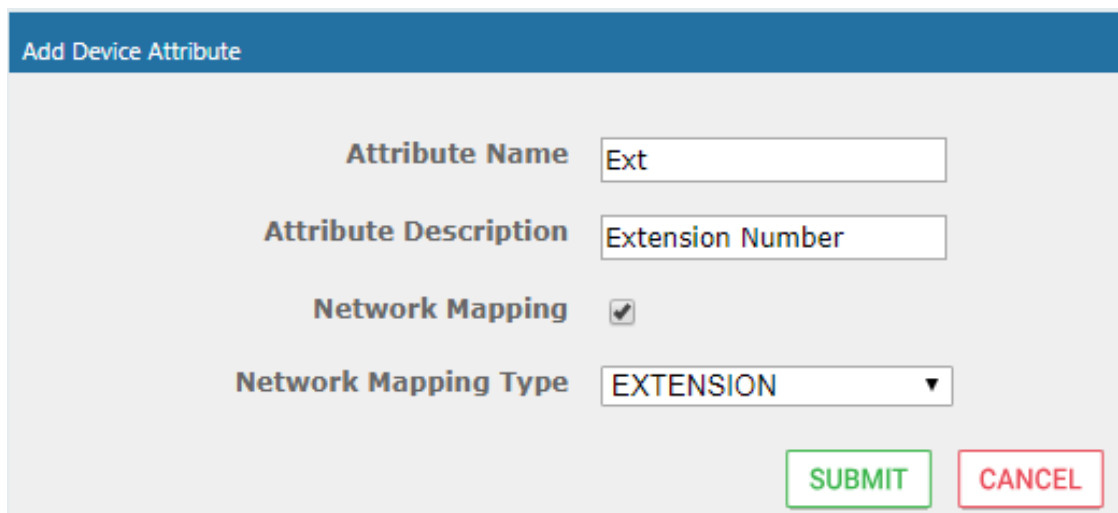
Following are examples of device attributes created for recording purposes:

Figure 6-95: Add Device Attribute - Example 1

The screenshot shows a web form titled "Add Device Attribute". It contains the following fields and controls:

- Attribute Name:** A text input field containing "SIP URI".
- Attribute Description:** A text input field containing "SIP URI".
- Network Mapping:** A checkbox that is checked.
- Network Mapping Type:** A dropdown menu with "SIP_URI" selected.
- Buttons:** Two buttons at the bottom right, "SUBMIT" (green border) and "CANCEL" (red border).

Figure 6-96: Add Device Attribute - Example 2



Add Device Attribute

Attribute Name

Attribute Description

Network Mapping ☒

Network Mapping Type

SUBMIT **CANCEL**

Adding a Microsoft Teams AAD 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° Live](#) on page 271).

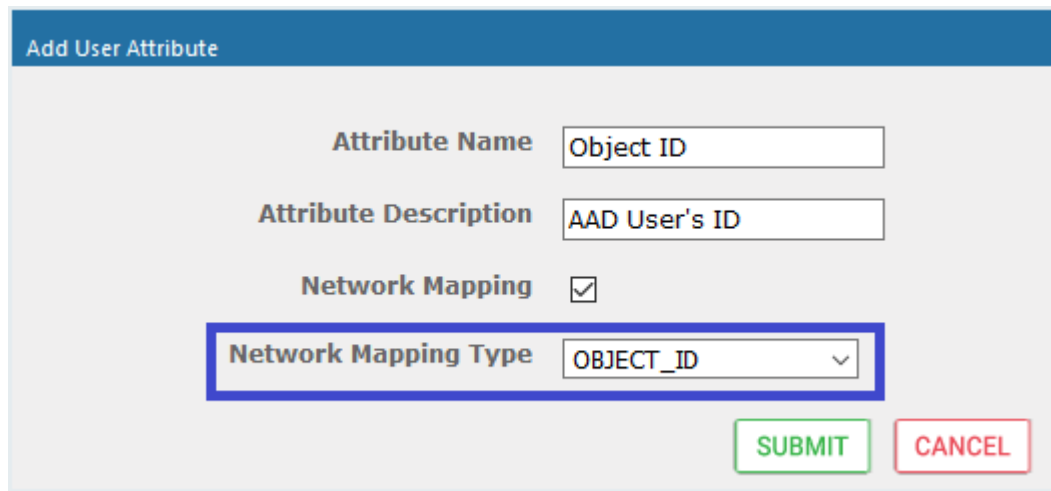


The SmartTAP users must have an AudioCodes Active Directory OBJECT_ID attribute mapping type set with the matching Teams User ID.

➤ To map SmartTAP 360° Live 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 6-97: Add User Attribute



Add User Attribute



Attribute Name

Attribute Description

Network Mapping ☒

Network Mapping Type

SUBMIT **CANCEL**

6. Click  to apply the new device attribute.
7. Associate the Object ID attribute to the relevant Microsoft Azure id attribute (see [AAD User and Group Mapping](#) on page 271).
8. Open the View/Modify Users screen (**Users** tab > **User Management** folder> **View/Modify User**).
9. Click  adjacent to the relevant Teams user.

The Active Directory idattribute for the user is retrieved in SmartTAP synchronization with theAAD and displayed in the Modify User screen.

Figure 6-98: Configure Teams User ID Attribute

Modify User

First Name: ST-Teams10 Last Name:

Email: ST-Teams10@smarttap.onm Login ID: ST-Teams10@smarttap.onm

Alias: <script>:

OID: 4c0cdfc2-0e7e-4ddc-8b3c-8l Object ID: e-4ddc-8f4c-800adb71926dt

TeamsUserId: Retention Policy: Default

Recording Profile: SOD Legal Hold: OFF

Security Profiles

- administrator
- agent
- Custom
- supervisor

Groups

- Default
- Sales
- Support

SUBMIT CANCEL [Lock Icon] [Edit Icon]

Adding a User

This section describes how to add a SmartTAP user.

➤ To add a SmartTAP user:

1. Open the Add User screen (**Users** tab > **User Management** folder > **Add User**).
2. Fill in the appropriate fields using the table below as a reference.

Figure 6-99: Add User

Add User

First Name Last Name

Email Login ID

Alias OID_XX

Retention Policy Recording Profile

Legal Hold OFF Recording license ☐

Security Profiles



- administrator
- agent
- supervisor

Groups

- Default

Table 6-40: Add User

Field	Description
First Name	User first name sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Last Name	User last name sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Email	User email address sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Login Id	User login ID sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Id / Alias	User ID / Alias sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.

Field	Description
	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 to apply changes.

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**).

Figure 6-100: View Modify Users List

View/Modify Users						
First Name	Last Name	Email	Login ID	Alias	Modify	Delete
			NOT_compliance-user1@smarttap.onmicrosoft.com			
Daniel	Kochav		danielk@smarttap.onmicrosoft.com	Kochav		
Deb	Dutta		debajyotid@smarttap.onmicrosoft.com	Dutta		
Initial	User (PLEASE DELETE)	notauser@nodomain.com	admin			
NOT_compliance-user2		NOT_compliance-user2@smarttap.onmicrosoft.com	NOT_compliance-user2@smarttap.onmicrosoft.com			
Sharon	Biner		sharonbi@smarttap.onmicrosoft.com	Biner		
ST-Teams06	ST-Teams06	ST-Teams06@smarttap.onmicrosoft.com	ST-Teams06@smarttap.onmicrosoft.com	ST-Teams06		
ST-Teams10	ST-Teams10	ST-Teams10@smarttap.onmicrosoft.com	ST-Teams10@smarttap.onmicrosoft.com	ST-Teams10		
ST-Teams100	ST-Teams100	ST-Teams100@smarttap.onmicrosoft.com	ST-Teams100@smarttap.onmicrosoft.com	ST-Teams100		
ST-Teams11	ST-Teams11	ST-Teams11@smarttap.onmicrosoft.com	ST-Teams11@smarttap.onmicrosoft.com	ST-Teams11		
ST-Teams12	ST-Teams12	ST-Teams12@smarttap.onmicrosoft.com	ST-Teams12@smarttap.onmicrosoft.com	ST-Teams12		
ST-Teams13	ST-Teams13	ST-Teams13@smarttap.onmicrosoft.com	ST-Teams13@smarttap.onmicrosoft.com	ST-Teams13		
ST-Teams14	ST-Teams14	ST-Teams14@smarttap.onmicrosoft.com	ST-Teams14@smarttap.onmicrosoft.com	ST-Teams14		
ST-Teams17		ST-Teams17@smarttap.onmicrosoft.com	ST-Teams17@smarttap.onmicrosoft.com			
ST-Teams18		ST-Teams18@smarttap.onmicrosoft.com	ST-Teams18@smarttap.onmicrosoft.com			
ST-Teams19		ST-Teams19@SmartTAP.onmicrosoft.com	ST-Teams19@SmartTAP.onmicrosoft.com			
ST-Teams20		ST-Teams20@SmartTAP.onmicrosoft.com	ST-Teams20@SmartTAP.onmicrosoft.com			
ST-Teams21		ST-Teams21@SmartTAP.onmicrosoft.com	ST-Teams21@SmartTAP.onmicrosoft.com			
ST-Teams22		ST-Teams22@smarttap.onmicrosoft.com	ST-Teams22@smarttap.onmicrosoft.com			
ST-Teams23		ST-Teams23@smarttap.onmicrosoft.com	ST-Teams23@smarttap.onmicrosoft.com			
<div> 20 1 2 3 4 5 (1 of 5) </div>						

Figure 6-101: Users List Displaying Licensed Users

View/Modify Users							
First Name	Last Name	Email	Login ID	Alias	Recording license	Modify	Delete
Initial	User (PLEASE DELETE)	notausers@nodomain.com	admin				
Shirel			Shirelchen.Megidish_audiocodes.com#EXT#@SmartTAP.onmicrosoft.com				
ST-Teams10			ST-Teams10@smarttap.onmicrosoft.com				
ST-Teams100			ST-Teams100@smarttap.onmicrosoft.com		✓		
ST-Teams101			ST-Teams101@smarttap.onmicrosoft.com		✓		
ST-Teams102			ST-Teams102@smarttap.onmicrosoft.com		✓		
ST-Teams11			ST-Teams11@smarttap.onmicrosoft.com		✓		
ST-Teams12			ST-Teams12@smarttap.onmicrosoft.com		✓		
ST-Teams13			ST-Teams13@smarttap.onmicrosoft.com		✓		
ST-Teams14			ST-Teams14@smarttap.onmicrosoft.com		✓		
ST-Teams17			ST-Teams17@smarttap.onmicrosoft.com		✓		
ST-Teams18			ST-Teams18@smarttap.onmicrosoft.com		✓		
ST-Teams19			ST-Teams19@SmartTAP.onmicrosoft.com				
ST-Teams20			ST-Teams20@SmartTAP.onmicrosoft.com				
ST-Teams21			ST-Teams21@SmartTAP.onmicrosoft.com				
ST-Teams22			ST-Teams22@smarttap.onmicrosoft.com				
TeamsTestUser2			TeamsTestUser2@ai-logix.net				

2. Use the table below as reference to search for a specific user to modify.

Figure 6-102: View/Modify Users

Modify User

First Name: user100 Last Name: SIPREC Teams

Email: user100@fanta.local Login ID: user100

Alias: OID: 3b47f7f8-bd88-4cd7-a9

userName: user100 Retention Policy: Default

Recording Profile: Audio Legal Hold: OFF

Recording license: ☒

Security Profiles

- administrator
- agent
- supervisor



Groups



- Default

SUBMIT CANCEL

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 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.

Field	Description
Id / Alias	User ID / Alias sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries.
Retention Policy	Indicates the retention policy that is assigned to the user.
Legal Hold	Indicates whether the Legal Hold is enabled for the user
Recording Profile	Indicates the recording profile that is assigned to the user
Recording License	Indicates whether a recording license is assigned to the user.
	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  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 68).

➤ 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 6-103: 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		ejenkins				
Barbara	Warner		bwarner				

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 6-104: 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  to change the password; the system automatically logs off and the user is required to log in with the new password.

Figure 6-105: Change Password

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



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

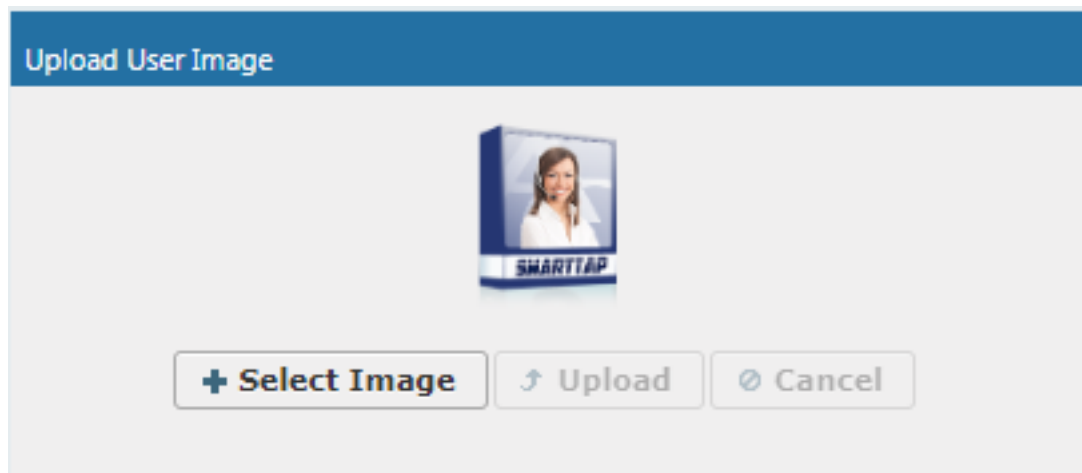
Uploading an Image

This section describes how to upload an image.

➤ **To upload an image:**

Select this option to upload your own image.

Figure 6-106: 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. The figure below shows retrieved Microsoft Teams calls, all successfully recorded.

Calls between 5/16/21 11:02 AM and 5/20/21 11:02 AM

Calls

Name	Start Time	Duration	Direction	Calling Party	Called Party	Release Cause	Media Type	Media Status
ST-Teams11	May 29, 2021 3:23:00 PM	00:02:29	INCOMING	CONFERENCE...	ST-Teams11	NORMAL	📄	✓
ST-Teams11	May 29, 2021 3:23:00 PM	00:02:29	INCOMING	CONFERENCE...	ST-Teams11	NORMAL	📄	✓
ST-Teams11	May 29, 2021 3:23:00 PM	00:02:29	INCOMING	CONFERENCE...	ST-Teams11	NORMAL	📄	✓
ST-Teams11	May 29, 2021 3:23:00 PM	00:02:29	INCOMING	CONFERENCE...	ST-Teams11	NORMAL	📄	✓
ST-Teams14	May 27, 2021 4:13:12 PM	00:02:58	INCOMING	CONFERENCE-ST-Teams13@smarttap.onmicrosoft.com...	ST-Teams14	NORMAL	▶	✓
ST-Teams13	May 27, 2021 4:13:10 PM	00:03:01	INCOMING	CONFERENCE-ST-Teams14@smarttap.onmicrosoft.com...	ST-Teams13	NORMAL	▶	✓
ST-Teams12	May 27, 2021 4:13:07 PM	00:03:04	INCOMING	CONFERENCE-ST-Teams14@smarttap.onmicrosoft.com...	ST-Teams12	NORMAL	▶	✓
ST-Teams11	May 27, 2021 4:12:58 PM	00:03:13	INCOMING	CONFERENCE-ST-Teams14@smarttap.onmicrosoft.com...	ST-Teams11	NORMAL	▶	✓
ST-Teams14	May 27, 2021 4:12:48 PM	00:02:56	INCOMING	CONFERENCE-ST-Teams13@smarttap.onmicrosoft.com...	ST-Teams14	NORMAL	▶	✓
ST-Teams13	May 27, 2021 4:12:42 PM		INCOMING	CONFERENCE...	ST-Teams13			✓

10 (1 of 579)

Total calls: 5786

Select a call

00:00:00 | 00:00:00

0.2 1.0 5.0

⏮ ⏪ ⏩ ⏭ 🔊

Figure 6-107: Call Search

System Users Status

Calls Messages

▼ Search Criteria

Custom Dates 1

From: 12/31/20 8 57 PM

To: 1/20/21 9 57 PM

☒ Active Users ☐ Inactive Users

☒ Active Devices ☐ Inactive Devices

☒ Users/Devices ☐ Groups

Users/Devices:

☒ Select All

ST-Teams100

TeamsTestUser5-E5

(1 of 1)

Call Parties:

Calling

Called

Answered

Call Tags:

☒ Active Tags ☐ Inactive Tags

Tag Name Tag Value

Select One

Search

▼ Saved Searches

No records found.

(1 of 1)

Figure 6-108: Search Calls Navigation Screen - Calls Tab

Field	Description
From:	Earliest date and time to search from. Click the date field for a calendar to pop up showing one month at a time. From the dropdown, change the time of day. Note: When searching for calls within a time range, only calls that start within the range are returned in the search results.
To:	Latest date and time upon which to search. Click the date field for a calendar to pop up showing one month at a time. From the dropdown, change the time of day.
Active Users	Users whose accounts are enabled in the SmartTAP 360° Live system.
Inactive Users	Users whose accounts have been deleted from the SmartTAP 360° Live system.
Active Devices	Devices that are not associated with users enabled in the SmartTAP 360° Live system and can be targeted for recording.
Inactive Devices	Devices that have been deleted from the SmartTAP 360° Live 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 Criteria 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 6-109: 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 6-110: 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)

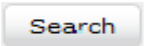
4. Select the type of Users and Devices.
5. Select either the Users/Devices or Groups Radio button.
6. Selecting the User/Devices option changes the display below to show a list of Users/Devices.
7. Selecting the Groups option changes the display below to show a list of Groups and Sub Groups (if the 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  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 6-111: Retrieved Calls List for Specific User

The screenshot shows the SmartTAP 360° interface. On the left, there's a sidebar with 'System', 'Users', and 'Status' tabs. Under 'Calls', there's a 'Search Criteria' section with filters for 'Last Days' (set to 2), 'From' (11/24/19), and 'To' (11/26/19). There are also checkboxes for 'Active Users', 'Inactive Users', 'Active Devices', and 'Inactive Devices'. The main area displays a table of calls between 11/24/19 06:41 PM and 11/26/19 06:41 PM. The table has columns for Name, Start Time, Answered, Released, Duration, Direction, Calling Party, Called Party, Answering Party, Recording Type, Tags, Media Type, Media Status, and Media Status Reason. Below the table, there's a 'Call Particles' section with 'Calling' and 'Called' filters, and a 'Call Tags' section with 'Active Tags' and 'Inactive Tags' checkboxes. A 'Search' button is at the bottom left.

Name	Start Time	Answered	Released	Duration	Direction	Calling Party	Called Party	Answering Party	Recording Type	Tags	Media Type	Media Status	Media Status Reason
John Smith	Nov 26, 2019 12:00:38 PM	Nov 26, 2019 12:08:40 PM	Nov 26, 2019 12:08:40 PM	00:00:28	OUTGOING	pooluser010	shreftest3	shreftest3	FULLTIME			None	
John Smith	Nov 26, 2019 11:56:08 AM	Nov 26, 2019 11:56:12 AM	Nov 26, 2019 11:56:12 AM	00:00:13	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:37:01 AM	Nov 26, 2019 11:37:02 AM	Nov 26, 2019 11:37:02 AM	00:00:37	OUTGOING	pooluser010	shreftest3	shreftest3	FULLTIME			None	
John Smith	Nov 26, 2019 11:36:52 AM	Nov 26, 2019 11:36:59 AM	Nov 26, 2019 11:37:02 AM	00:00:10	OUTGOING	pooluser010	shreftest3	shreftest3	FULLTIME			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	pooluser010	shreftest3	shreftest3	FULLTIME			None	
John Smith	Nov 26, 2019 11:36:47 AM	Nov 26, 2019 11:36:59 AM	Nov 26, 2019 11:36:59 AM	00:00:16	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:35:47 AM	Nov 26, 2019 11:36:29 AM	Nov 26, 2019 11:36:29 AM	00:01:09	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:31:22 AM	Nov 26, 2019 11:31:46 AM	Nov 26, 2019 11:31:46 AM	00:00:24	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:22:39 AM	Nov 26, 2019 11:22:45 AM	Nov 26, 2019 11:22:45 AM	00:00:25	OUTGOING	pooluser010	shreftest3	shreftest3	FULLTIME			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	pooluser010	shreftest3	AnnouncementsApp-s4b-2015-sile1	FULLTIME			None	

- Optionally, specify a Call Tag & Value.

Figure 6-112: Call Tags

The 'Call Tags' configuration window has a title bar 'Call Tags:'. Below it are two checkboxes: 'Active Tags' (checked) and 'Inactive Tags' (unchecked). There are two input fields: 'Tag Name' with the value 'ActionItem' and a dropdown arrow, and 'Tag Value' with the value 'Schedule Meeting'. At the bottom is a 'Search' button.

- 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 6-113: Call Tags

The 'Call Tags' configuration window is shown with a right-click context menu open over the 'Tag Name' field. The menu has two options: 'Insert Row' and 'Delete Row'. The 'Tag Name' field contains 'ActionItem' and the 'Tag Value' field contains 'Schedule Meeting'. A 'Search' button is at the bottom.

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  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 6-114: Search Calls Results



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 160.

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: <ul style="list-style-type: none"> ■ 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 or Microsoft Teams Desktop Application (Video and Screen Sharing): The Video and Screen 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 Video and Screen Sharing has been successfully recorded.
Expires	<p>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.</p> <p>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).</p>
Notes	<p>There are no notes associated with this call. There are notes associated with this call.</p> <p>Notes are displayed adjacent to the Player screen as highlighted in the figure above with the note example “Executive Call”.</p>
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	Corresponding Media Reason

Field	Description
Reason	
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.
	<ul style="list-style-type: none"> 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.
	Deletion
	Pending Deletion

➤ **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 6-115: Add/Remove Columns from the Search Call Results Screen

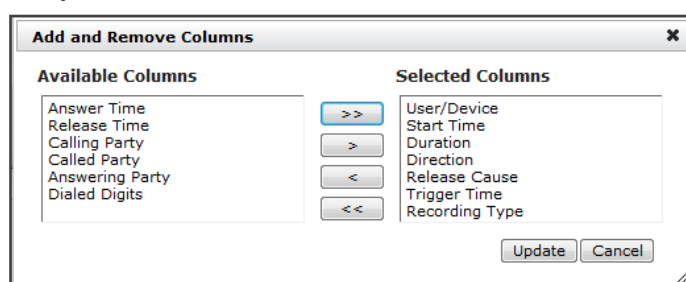
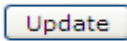
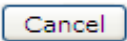


Table 6-43: Add and Remove Columns – Field Descriptions

Field	Description
Available Columns	List of columns that can be added to the search results table.
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.
	Applies changes and closes the screen.
	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.

Field	Description	
Duration	Total duration of the call, from the Start Time to the Release Time.	
Calling Party	The call initiator.	
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	<div> <input checked="" type="checkbox"/> Full Time </div> <div> <input checked="" type="checkbox"/> Record on Demand </div> <div> <input checked="" type="checkbox"/> Save on Demand </div>	
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.	

Field	Description
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.
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


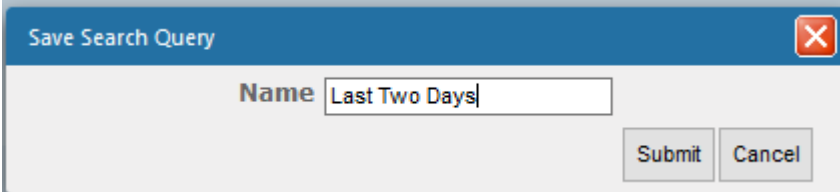
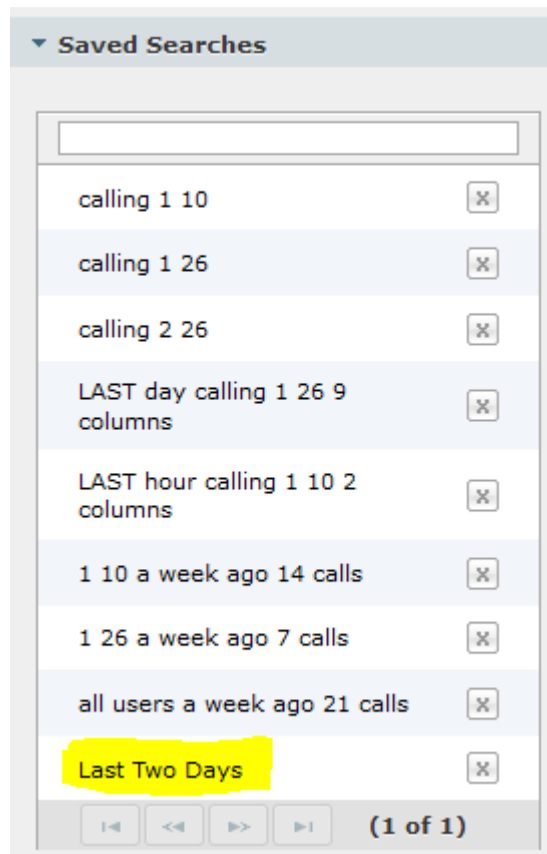
selecting the  in the bottom right-hand corner of the screen. The saved query is added to the Saved Searches pane in the bottom left-hand corner of the screen. In the figure below "Last Two Days" is added as the saved query.

Figure 6-116: Save Search Query



The image shows a dialog box titled "Save Search Query" with a close button (X) in the top right corner. Inside the dialog, there is a label "Name" followed by a text input field containing the text "Last Two Days". At the bottom right of the dialog, there are two buttons: "Submit" and "Cancel".



Deleting Calls and Instant Messages



SmartTAP 360° Live 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 113).



- This feature is enabled through the SmartTAP 360° Live Call Deletion license (SW/SMTP/CALLDEL)
- If a user is on Legal Hold, their Calls and Instant Messaging cannot be deleted (see [Managing Users](#) on page 106)
- 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 149).

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 6-117: Delete Calls

Calls Between 9/1/19 11:28 AM and 12/31/19 12:28 PM							
Calls							
	Name	Start Time	Duration	Direction	Release Cause	Media Type	
				Select	Select	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		
10 1 2 3 4 5 (1 of 5)				Total calls: 43			


3. Click , a confirmation dialog is displayed:

Figure 6-118: Delete Calls Confirmation

Delete Calls

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

Submit

Cancel

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 6-119: 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 6-120: 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
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° Live HTML5 player is listed below:

- **Audio:**

- ✓ Audio Playback: Microsoft Edge Version: 88.0.705.56, Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 85.0 and later
- ✓ Wave form rendering: Microsoft Edge Version 88.0.705.56, Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 85.0 and later
- ✓ Stereo wave form rendering (for recordings **other than Microsoft Teams**): Microsoft Edge Version 88.0.705.56, Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 85.0 and later
- ✓ Wave form rendering: Microsoft Edge Version 88.0.705.56, Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 85.0 and later
- ✓ For **Microsoft Teams Native recording**, audio mixed – on waveform is recorded.
- ✓ Playing while loading: Microsoft Edge Version 88.0.705.56, Google Chrome Ver. 58 and later

- **Video:**

- ✓ Video: Microsoft Edge Version 88.0.705.56, Google Chrome Ver. 58 and later, Mozilla Firefox Ver. 85.0 and later
- ✓ Playback with 'Display Video' selected is limited to five concurrent sessions.
- Skype for Business and Microsoft Teams Desktop Application Recording (Video and Screen Sharing): Skype for Business Video and Screen 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:
 - ✓ [Skype for Business VBSS](#)

Figure 6-121: Audio Player Screen

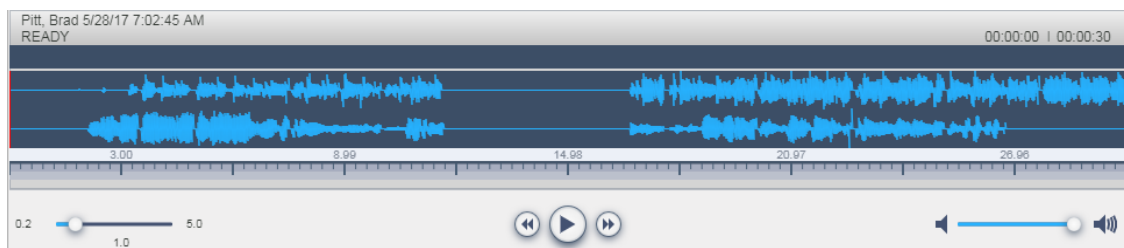

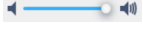








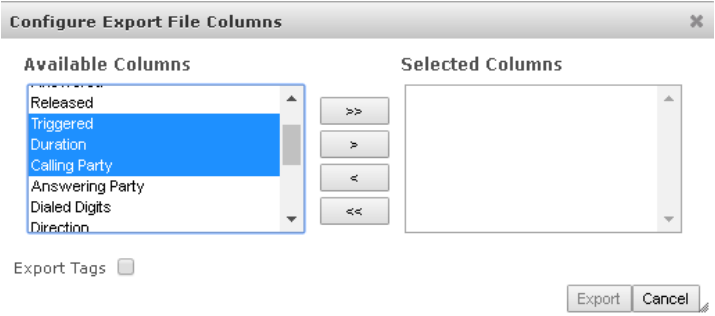





Table 6-45: Player Screen Overview

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 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 to replay the segment.
	Playback speed in milliseconds.
	Send call information to an excel worksheet. When this option is selected, you can use the arrow keys to select those columns to include in your report. 
	Email audio call information. When this option is selected, the Email Audio dialog opens. See Sending Email on page 109
	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 149
	Download call information to your PC. When this option is selected, the Download Media dialog opens. See Downloading Call Recordings on page 174

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

The call recorder is displayed with the frequency spectrum of the call.



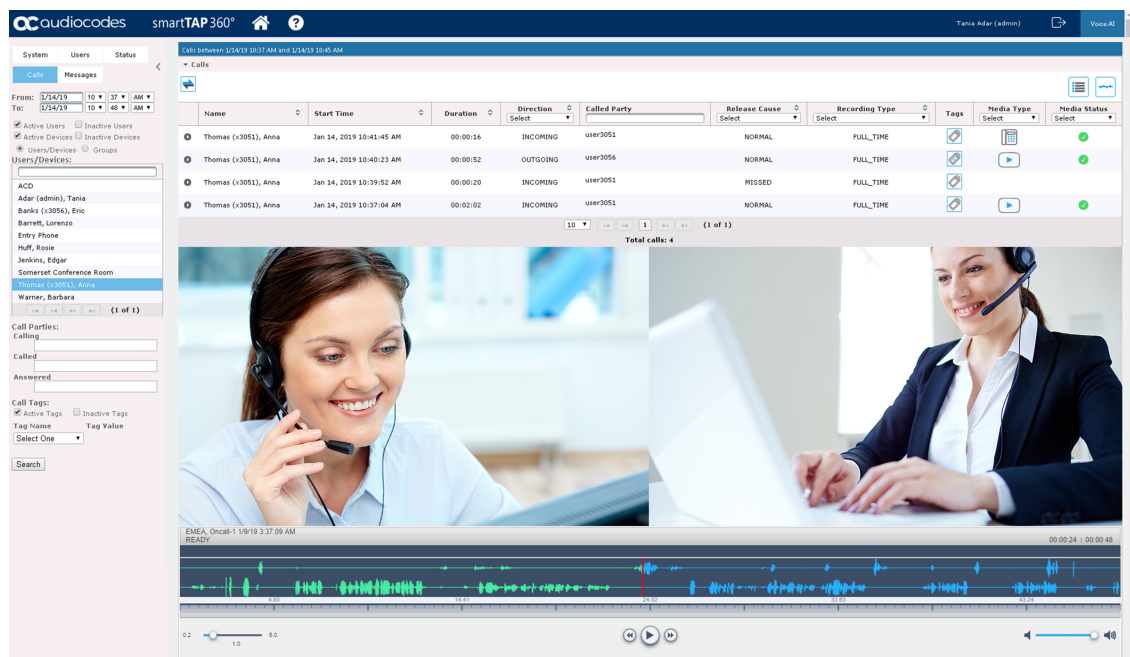
4. Click the  button to start listening to the call and/or view the video (if you selected “Display Video” check box); the button changes to  while the call is playing, to allow the administrator to pause the player while playing the audio or video.

Figure 6-122: Viewing Video



The screenshot displays the SmartTAP 360° interface. On the left, there's a sidebar with navigation options like System, Users, Status, Calls, and Messages. The main area shows a call log with columns for Name, Start Time, Duration, Direction, Called Party, Release Cause, Recording Type, Tags, Media Type, and Media Status. Below the log, there's a video player showing two participants in a conference call. The video player has a play button and a frequency spectrum at the bottom.

Name	Start Time	Duration	Direction	Called Party	Release Cause	Recording Type	Tags	Media Type	Media Status
Thomas (+3051), Anna	Jan 14, 2019 10:41:45 AM	00:00:16	INCOMING	user3051	NORMAL	FULL_TIME			
Thomas (+3051), Anna	Jan 14, 2019 10:40:23 AM	00:00:52	OUTGOING	user3056	NORMAL	FULL_TIME			
Thomas (+3051), Anna	Jan 14, 2019 10:39:52 AM	00:00:20	INCOMING	user3051	MISSED	FULL_TIME			
Thomas (+3051), Anna	Jan 14, 2019 10:37:04 AM	00:02:02	INCOMING	user3051	NORMAL	FULL_TIME			

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 6-123: Multiple Conference Participants

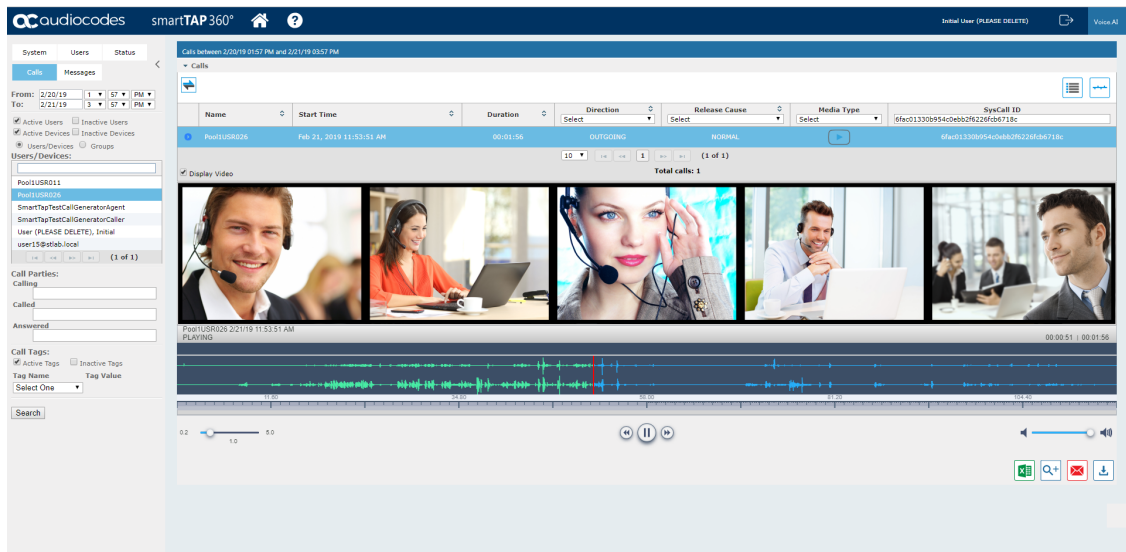
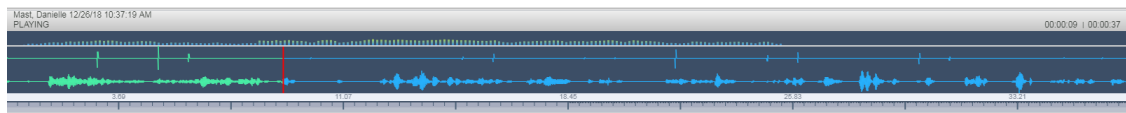


Figure 6-124: Playback Audio Signaling Data



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

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

5. Manipulate the call recording in the following ways:


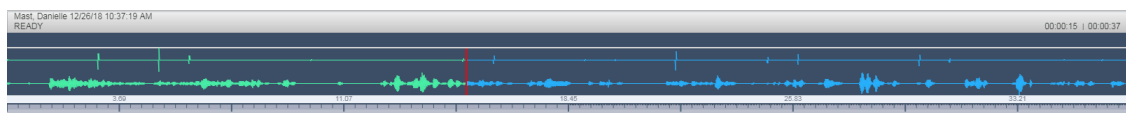
- Move the cursor to any random point in the recording and left-click and release;
- The selected segment is colored green. Click the  button; the call recording is played from the left-click selection point forward (shown by the red line in the figure below).

Figure 6-125: Random Selection Point in Call Recording




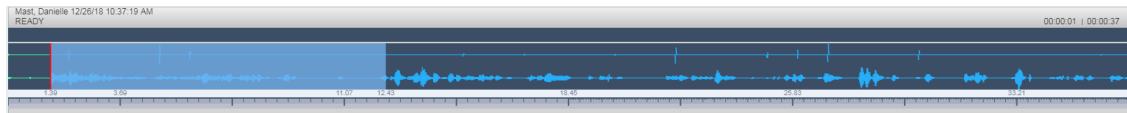



- Left-click and drag the mouse over the desired segment in the call recording and release; the selected segment is shaded blue. Click the  button; the shaded segment of the call recording is played back.

Figure 6-126: Highlighted Segment in Call Recording

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

Managing Microsoft Teams Video Calls

The following describes the recording and playback/download factors for managing Microsoft Teams video calls.

■ Video Recording

- SmartTAP supports the recording of up to 4 video streams provided by the Microsoft Recording API.
- If the number of video-enabled call participants exceeds the number of configured streams and/or exceeds the maximum available streams (4) then existing streams are replaced accordingly. The replacement logic is managed by the Bot and is mainly based on dominant speakers prioritization where targeted users have priority i.e. if they start video they are recorded in any case.
- Each stream is recorded in a separate media file.
- Peer-to-Peer calls are stored with a resolution of 720p per stream, Conference calls are stored with a resolution of 360p per stream

■ Playback\download:

- During playback, a composite screen is displayed consisting of up to four video tiles and Video and Screen Sharing (if available)
- Video Tiles represent one tile per recorded stream
- Video Tiles may be set as a grid, or in line in case Video and Screen Sharing is active
- The Target compliance user's tile has highlighted borders.
- Each tile is labeled with Participant identifier (Name- if available)
- Media files of a single call are processed (rescaled, mixed, composed, etc) prior to playback\download
- In case, media is stored in Azure Blob, media files are downloaded to server and then processed

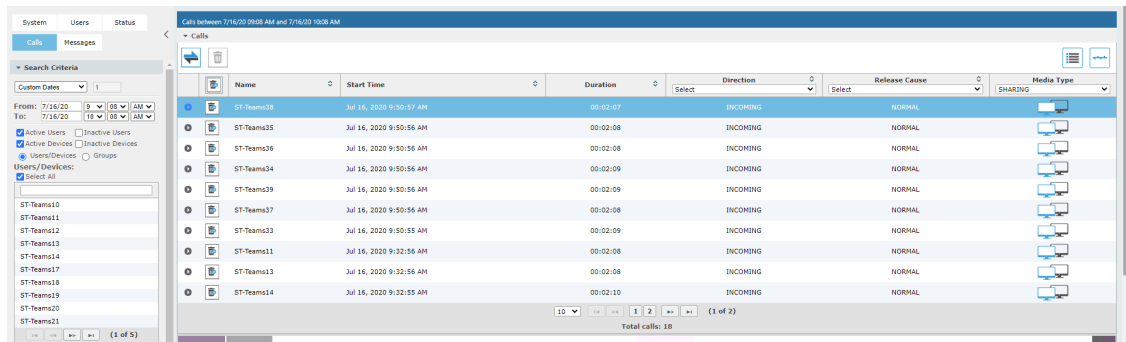
Skype for Business and Teams Video and Screen Sharing

This section describes how to playback a Video and Screen Sharing recording.

➤ To playback Video and Screen Sharing recording :

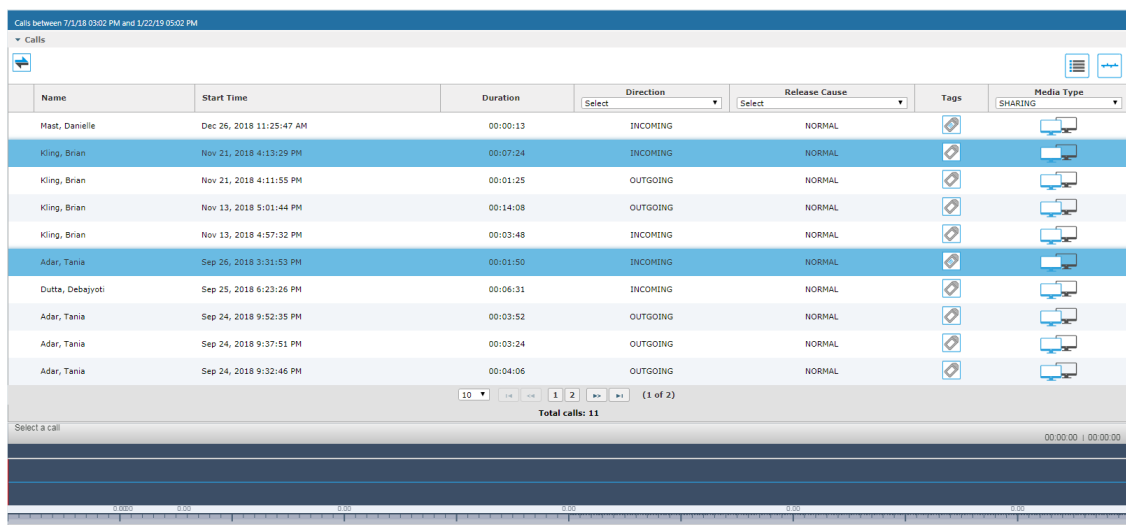
1. Follow the instructions described in [Searching for Calls](#) on page 149 to search for calls.
2. From the Media Type drop-down list, select Sharing to filter the search results for the Video and Screen Sharing recordings.

Figure 6-127: Media Type-Video and Screen Sharing with Teams



Name	Start Time	Duration	Direction	Release Cause	Media Type
ST-Teams18	Jul 16, 2020 9:50:57 AM	00:02:07	INCOMING	NORMAL	Video
ST-Teams35	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	Video
ST-Teams36	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	Video
ST-Teams34	Jul 16, 2020 9:50:56 AM	00:02:09	INCOMING	NORMAL	Video
ST-Teams39	Jul 16, 2020 9:50:56 AM	00:02:09	INCOMING	NORMAL	Video
ST-Teams37	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	Video
ST-Teams33	Jul 16, 2020 9:50:55 AM	00:02:09	INCOMING	NORMAL	Video
ST-Teams11	Jul 16, 2020 9:32:56 AM	00:02:08	INCOMING	NORMAL	Video
ST-Teams13	Jul 16, 2020 9:32:56 AM	00:02:08	INCOMING	NORMAL	Video
ST-Teams14	Jul 16, 2020 9:32:59 AM	00:02:10	INCOMING	NORMAL	Video

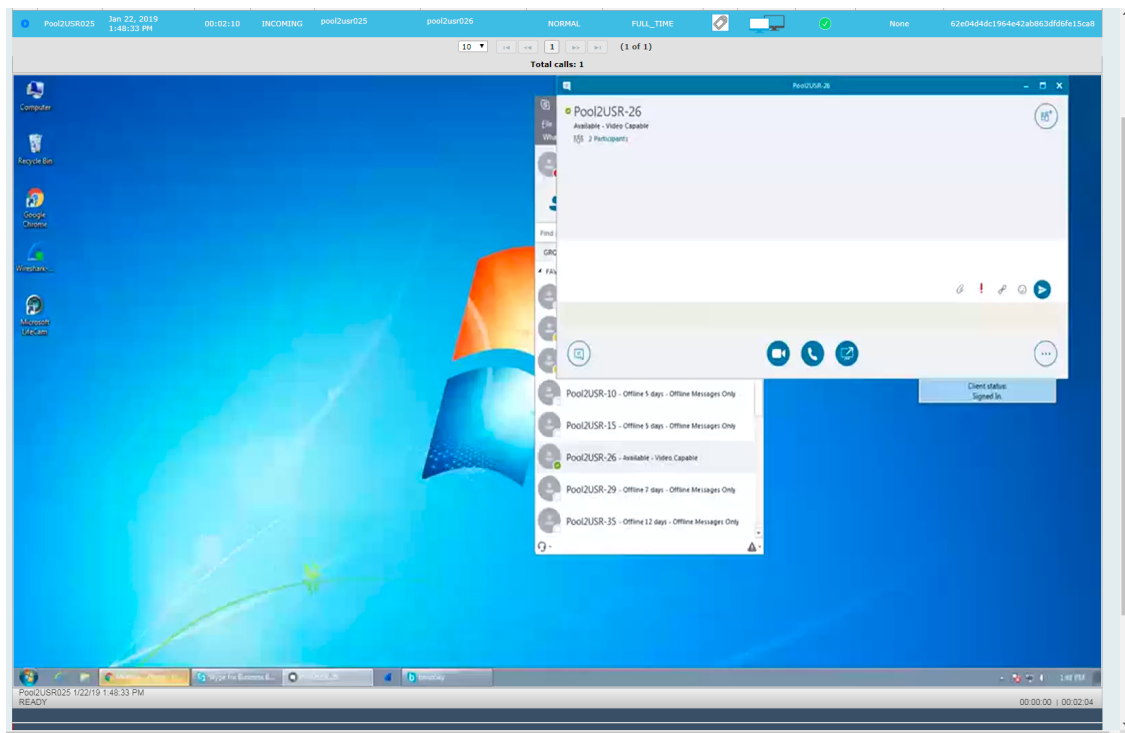
Figure 6-128: Media Type-Video and Screen Sharing with Skype for Business




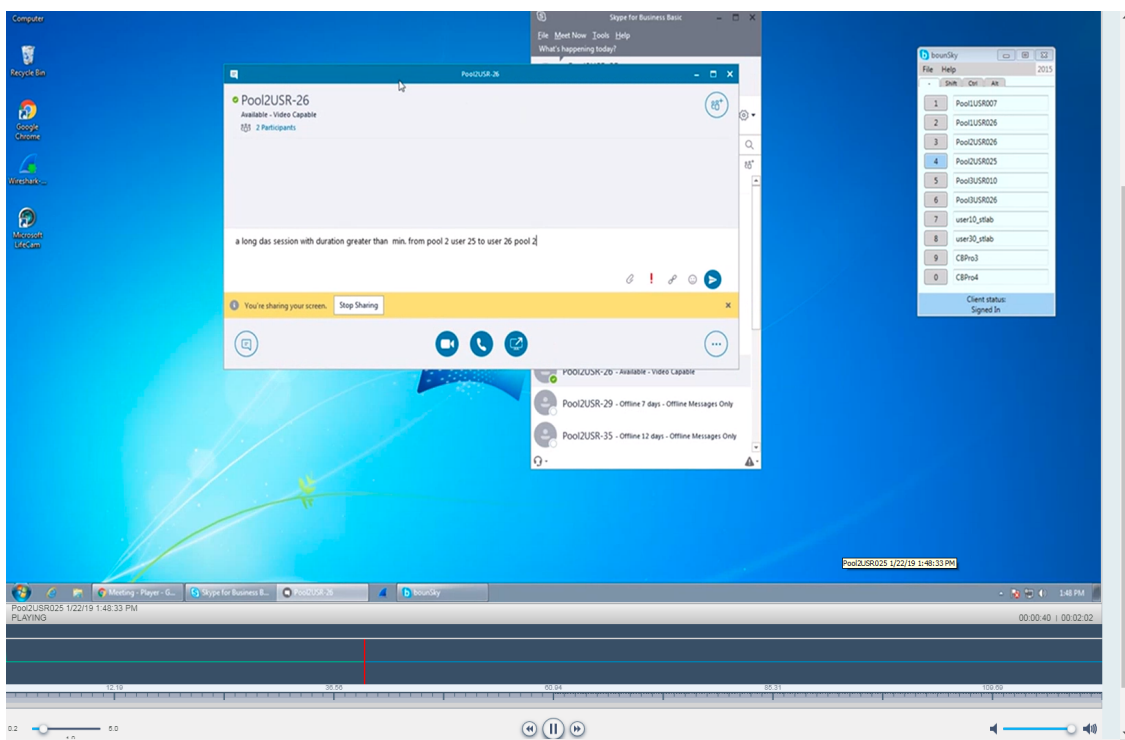
Name	Start Time	Duration	Direction	Release Cause	Tags	Media Type
Mast, Danielle	Dec 26, 2018 11:25:47 AM	00:00:13	INCOMING	NORMAL		Video
Kling, Brian	Nov 21, 2018 4:13:29 PM	00:07:24	INCOMING	NORMAL		Video
Kling, Brian	Nov 21, 2018 4:11:55 PM	00:01:25	OUTGOING	NORMAL		Video
Kling, Brian	Nov 13, 2018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


3. Double-click a row to display the Video and Screen Sharing recording.



Figure 6-129: Video and Screen Sharing Recording



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



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.

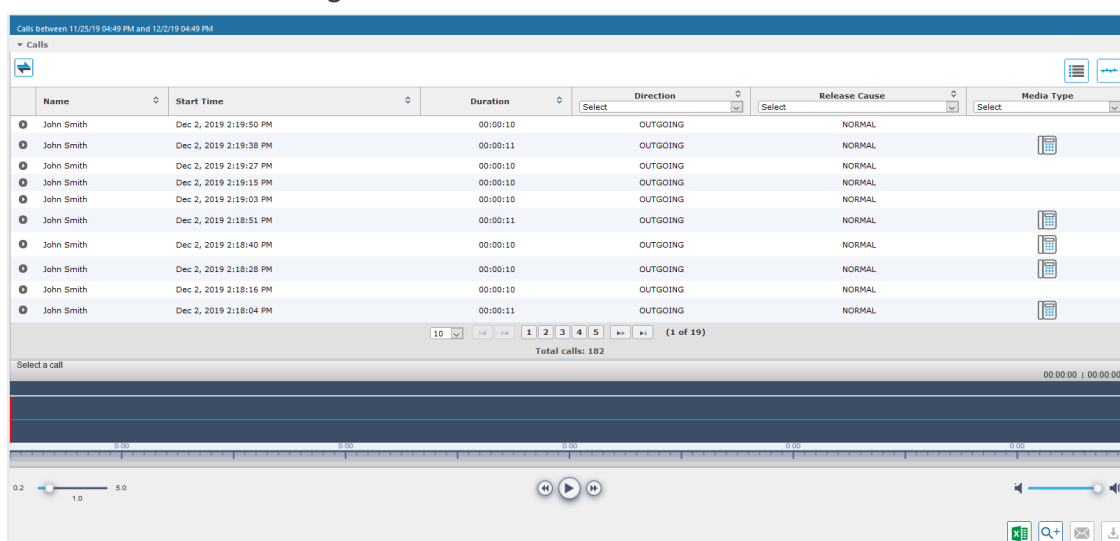
Time Line View

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:

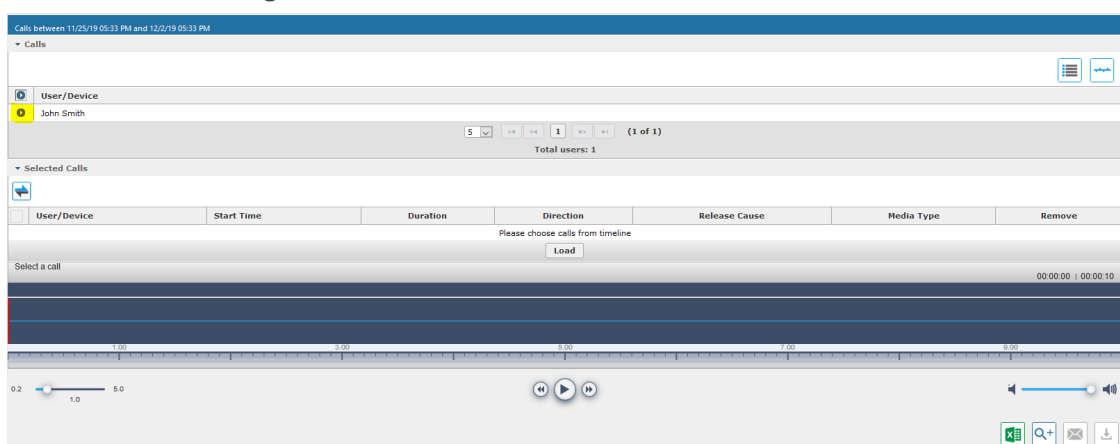
1. Follow the instructions described in [Searching for Calls](#) on page 149 [Searching for Calls](#) on page 149 to search for calls.

Figure 6-130: Calls List



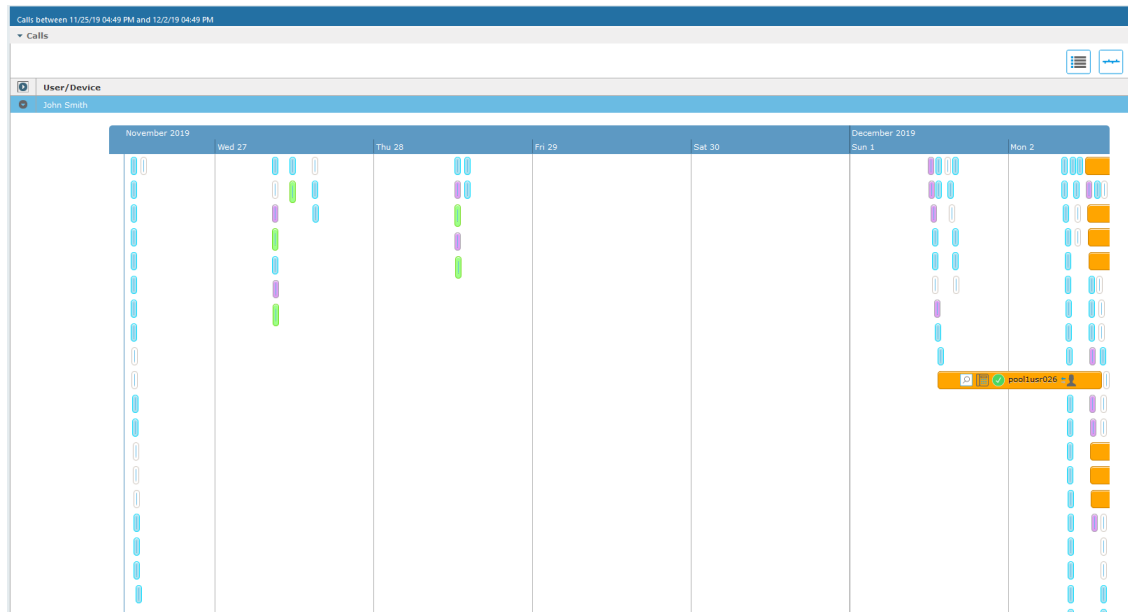
2. Select the Timeline view icon . A screen similar to the following is displayed:

Figure 6-131: Select User in Timeline View



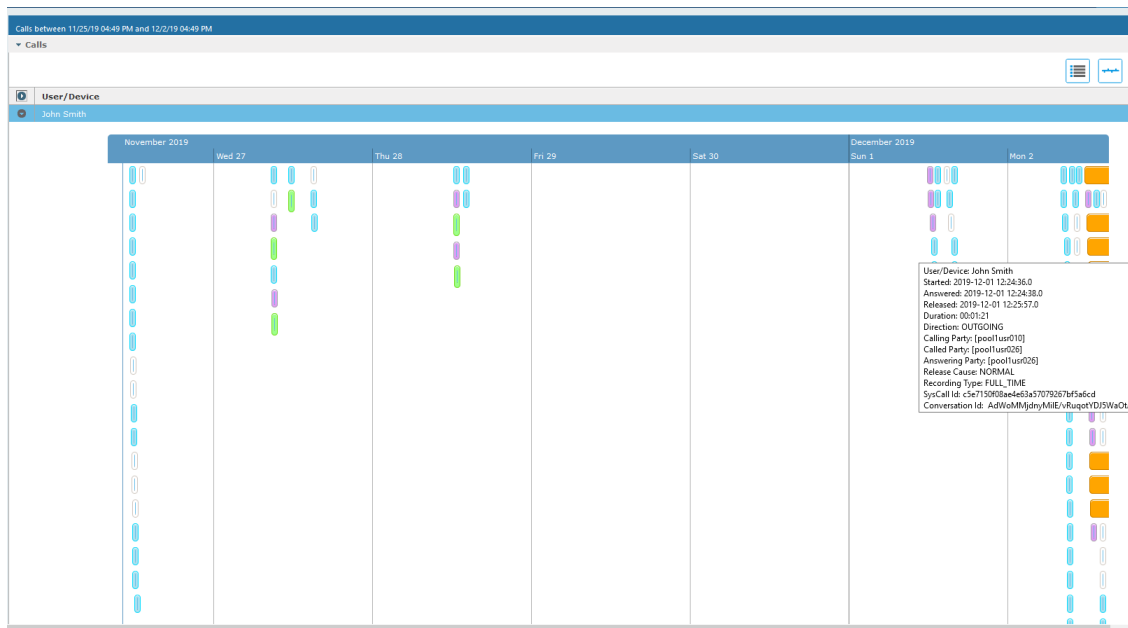
3. Select the arrow adjacent to the User/Device whose timeline you wish to view. The Calls List is displayed:

Figure 6-132: User Timeline



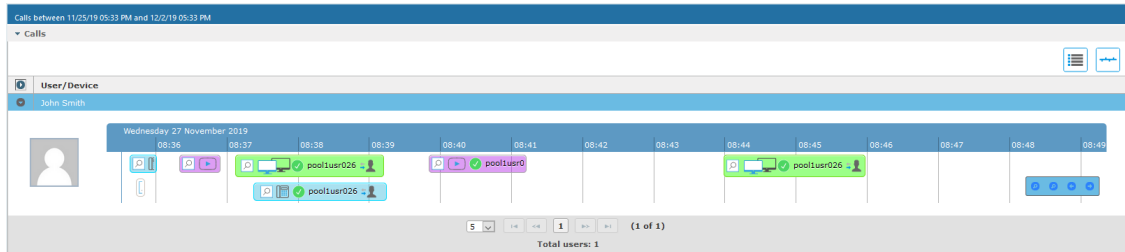
4. Hover over a call event to view details of the call.

Figure 6-133: Call Event Details



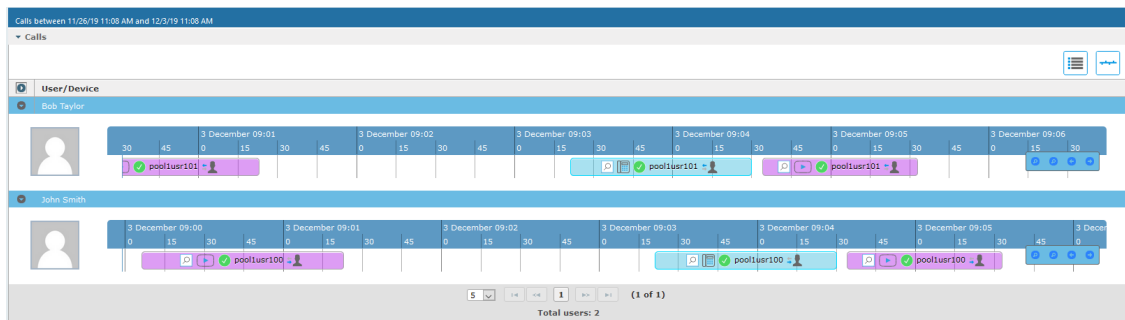
5. Zoom in on a specific day to view the details using either the mouse roller or the navigation buttons that are highlighted below.

Figure 6-134: Zoom In



- 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 6-135: Call Events from Multiple Timelines






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 Video and Screen 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 Video and Screen Sharing call segment
 - An Audio Video call segment can overlap with a Video and Screen Sharing call segment
 - An Audio call segment can't overlap with another Audio or Audio Video call segment
 - A Video and Screen Sharing call segment can't overlap with another Video and Screen Sharing call segment










Table 6-46: Call Events Description

Media Type	Description
 pool2usr	Represents an Audio call.

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

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

Table 6-47: 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.

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

Figure 6-136: Load Media Player

The screenshot shows the 'Load Media Player' interface. At the top, there are two user timelines for 'Bob Taylor' and 'John Smith'. Below these, a table lists 'Selected Calls'.

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	[Icon]	[X]
Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	[Icon]	[X]

Below the table, there is a 'Load' button and a 'Selected a call' field. At the bottom, there is a media player interface with a timeline, volume controls, and playback buttons.

The selected files are loaded to the Media Player.

Figure 6-137: Loading Files to Media Player

This screenshot shows the 'Loading Files to Media Player' interface. It is similar to Figure 6-136, but the 'Selected Calls' table is the same, and the media player at the bottom shows a 'LOADING' status with a progress bar. The progress bar has markers at 0.00, 8.10, 16.20, 24.30, 32.40, 40.50, and 48.60. The media player also includes volume controls and playback buttons.

Figure 6-138: Files Ready to Play

The screenshot shows the SmartTAP 360° Live interface. At the top, there are two user profiles: Bob Taylor and John Smith. Below each profile is a timeline showing call activity. The 'Selected Calls' table lists the following data:

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	Audio	[Remove]
Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	Video	[Remove]

Below the table, the media player shows a timeline for the selected call, with a play button and a volume slider.

- b. Click  to play the selected call.

Figure 6-139: Play Call

The screenshot shows the SmartTAP 360° Live interface with the 'Display Video' checkbox selected. The 'Selected Calls' table is the same as in Figure 6-138. The media player at the bottom shows the call is now playing, with a play button and a volume slider.

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 149 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 6-140: 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

SUBMIT

CANCEL

Figure 6-141: 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

SUBMIT **CANCEL**

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 149 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 6-142: 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

SUBMIT **CANCEL**

Figure 6-143: 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

SUBMIT **CANCEL**

Downloading a Video and Screen Sharing Call

This section describes how to download a Video and Screen Sharing call.

➤ **To download a video and screen sharing call:**

1. Follow the instructions in [Searching for Calls](#) on page 149 to search for the call to download.
2. From the Media Type drop-down list, select Sharing.
3. Select the Video and Screen Sharing session you wish to download.
4. Select the Sharing check box.

Figure 6-144: Downloading a Video and Screen 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


SUBMIT CANCEL

5. Use the table below as a reference.

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

Field	Description	Basic/Advanced
File Format	Option to select the format of the downloaded file:	Basic
	Audio: <input type="checkbox"/> Wave <input type="checkbox"/> MP3	Basic
	Video: <input type="checkbox"/> WEBM	Basic
	Video and Screen Sharing: <input type="checkbox"/> WEBM	Basic
Digitally Sign	Add a Digital Signature to download call. See Configuring a Digital Signature on page 67 for more details. This feature is only supported for Audio downloads.	Advanced
Audio Encoding	Option to select the encoding of the downloaded file: <input type="checkbox"/> ALAW <input type="checkbox"/> MPEG1L3 <input type="checkbox"/> Opus <input type="checkbox"/> PCM_Signed <input type="checkbox"/> ULAW	Advanced
Video Encoding	<input type="checkbox"/> VP8	Advanced

Field	Description		Basic/Advanced
Mixing	Option to select the mixing of the downloaded file.		Advanced
	Mono	All audio tracks from the selected call will be mixed into a single mono track in the downloaded file.	Advanced
	Multi-Track	All tracks from the selected call will be placed on a separate track within the downloaded media file.	Advanced
	Stereo	Audio of each side of a call will be placed on a separate track within the downloaded media file.	Advanced

6. Click  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 149 to find the call to email.
2. Select the call entry to email and then click the email button ; the Email screen opens.

Figure 6-145: Email Screen

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

Email

To ->

Cc ->

Bcc ->

Subject:

Attachments: Johnson, Bob_2018_12_31_01_55_48_000.wav

Body:

SUBMIT CANCEL

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

Table 6-48: Email – Field Descriptions

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

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° Live 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 6-146: 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			

(1 of 1) **1** 10 ▾

Use the table below as reference.

Table 6-49: Evaluation Forms – New Form Subscreen

Field	Description
 New Form	Click to close the Add Form sub screen.
 New Form	Click to open the Add Form sub screen.
Name (in the New Form menu)	The name of the new form.
Description (in the New Form menu)	The description of the new form.
 (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 186
- [Adding a New Section \[Evaluation Forms\]](#) on page 187
- [Adding Questions and Answers to an Evaluation Form](#) on page 188
- [Finalizing Forms](#) on page 191

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  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  to rename the form.

Figure 6-147: Evaluation Forms

Evaluation Forms

Change Name

Name:

Description:

	Name (click to change) ↕	Status	Finalized Date ↕	Modify	View/Copy	Delete
	<u>Agent Scoring</u>	FINAL	Apr 24, 2018			
*	<u>Agent Scoring Draft</u>	DRAFT	N/A			
*	<u>Agentscoring_002</u>	DRAFT	N/A			
	<u>Customer Service</u>	FINAL	Nov 17, 2014			
*	<u>guy_vest</u>	DRAFT	N/A			
	<u>Sales</u>	DRAFT	N/A			
	<u>test</u>	FINAL	Sep 7, 2017			

(1 of 1) **1** 10 ▼

Table 6-50: Evaluation Forms – Field Descriptions

Field	Description
New Form	Click to close the Add Form subscreen.
New Form	Click to open the Add Form subscreen.
Name (click to change)	Form Name sorted ascending/descending by clicking header up/down arrows.
Status	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ (date) (Date when the form was finalized) ■ N/A(Not Applicable; the form is not finalized)
	The form is not completed and cannot be finalized.




Field	Description
	Click to modify the form.
	Click to view or copy the form.
	Click to delete the form.

Figure 6-148: View/Copy Evaluation

View Evaluation form Agentscoring 002

Section Greeting

The agent thanked the customer for calling

Q: a: Yes 1 pt. ☐

a: No 0 pt. ☐

The agent mentioned their company name

Q: a: Yes 1 pt. ☐

a: No 0 pt. ☐

The agent identified themselves to the customer

Q: a: Yes 1 pt. ☐

a: No 0 pt. ☐

The agent stated that the call is being recorded

Q: a: Yes 1 pt. ☐

a: No 0 pt. ☐

Section Account Verification

The agent verified account

Q: a: Yes 1 pt. ☐

a: No 0 pt. ☐

Section djgztd


No records found.

Back Copy As

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:**


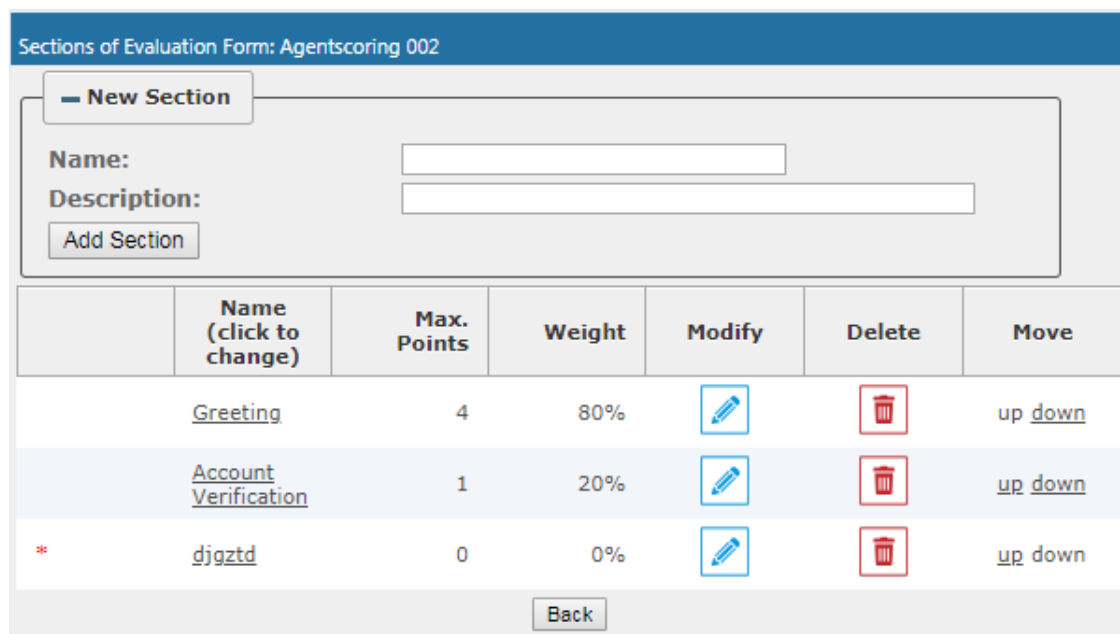
1. Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms**).
2. Click  on the row listing the form to change to open it.

Figure 6-149: Sections of Evaluation Form – New Section Sub-screen









Sections of Evaluation Form: Agentscoring 002

New Section

Name:

Description:

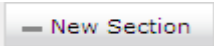
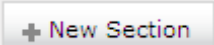
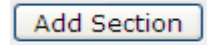
Add Section

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

Back

3. [Use the table below as reference] Enter the new section Name and Description in the New Section sub-screen.
4. Click **Add Section** to create the new section; the new Section appears in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized.

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

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

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 6-150: Sections of Evaluation Form – New Questions Sub-screen

Questions of Evaluation Form: Agentscoring 002 Section: Greeting

— New Question

Question:
Description:









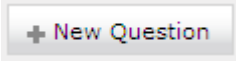
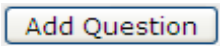


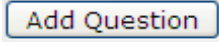
	Question (click to change)	Add Answer	Delete	Move
Q:	The agent thanked the customer for calling a: Yes a: No			up down
Q:	The agent mentioned their company name a: Yes a: No			up down
Q:	The agent identified themselves to the customer a: Yes a: No			up down
Q:	The agent stated that the call is being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

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

Field	Description
— New Question	Click to close the New Question sub-screen.


Field	Description
	Click to open the New Question sub-screen.
Question	The name of the new Question.
Description	The description of the new 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 sub-screen.
5. Click  to create the new Question; the new Question appears in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized.

➤ **To add a New Answer [Evaluation Forms]:**

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

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 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 6-151: Sections of Evaluation Form - New Answer Sub-screen



5. Enter the new Answer information.



You must provide at least two answers for each question.

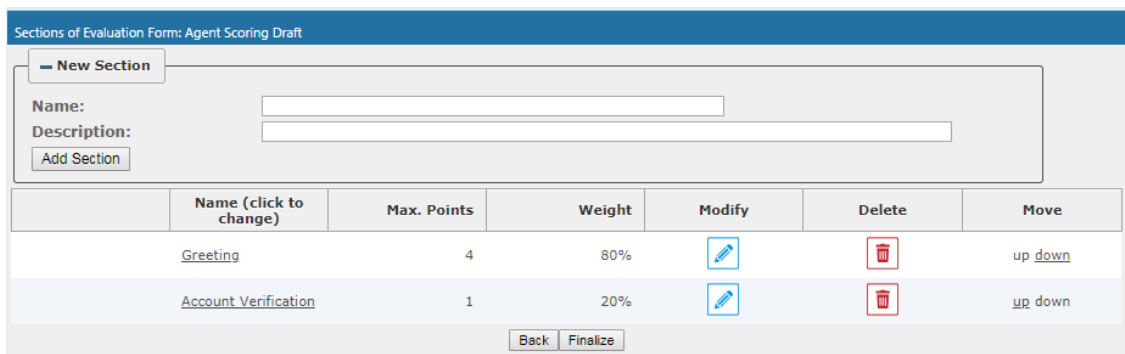
6. Click  to create the new Answer; the new Answer will appear in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized. There is a minimum of two (2) answers required before a form can be finalized.





Finalizing Forms

This section describes how to finalize forms.


➤ To finalize a Form [Evaluation Forms]:


Figure 6-152: Form Subscreen



	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  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 6-54: Select Evaluation Form Screen

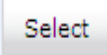
Field	Description
Name	The name of the form.
Description	Description of the form.
Select	 click to select the form.

Figure 6-153: Call Search/Selection Evaluation Form

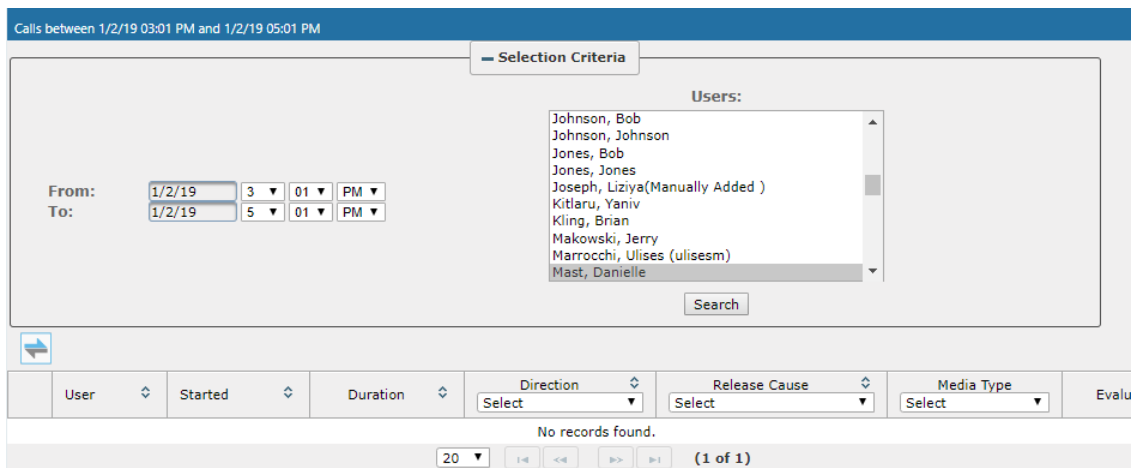
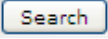



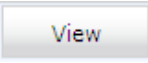

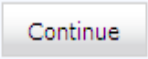


Table 6-55: Call Search/Evaluation Form – Field Descriptions

Field	Description
From:	Earliest date and time to search from. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
To:	Latest date and time to search to. Click the date field for a calendar to

Field	Description
	pop up showing one month at a time. Use the dropdown to change the time of day.
Users	Users whose account is enabled in SmartTAP 360° Live.
	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: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Video and Screen Sharing <input checked="" type="checkbox"/> 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.
	A Finalized Evaluation exists for the selected Evaluation form and call, and will be presented for viewing.
	A new Evaluation will be created for a previously selected Evaluation Form, and the call selected.

Field	Description
	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 6-154: Select Evaluation Form

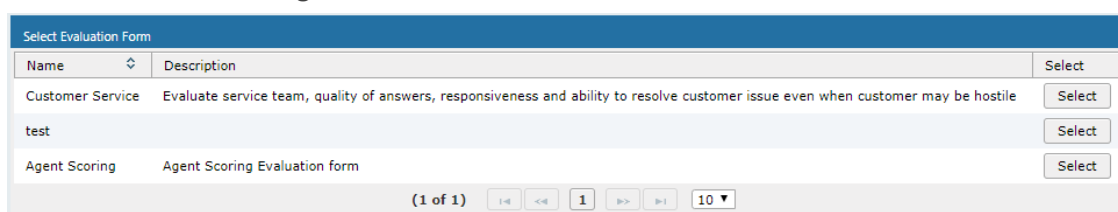
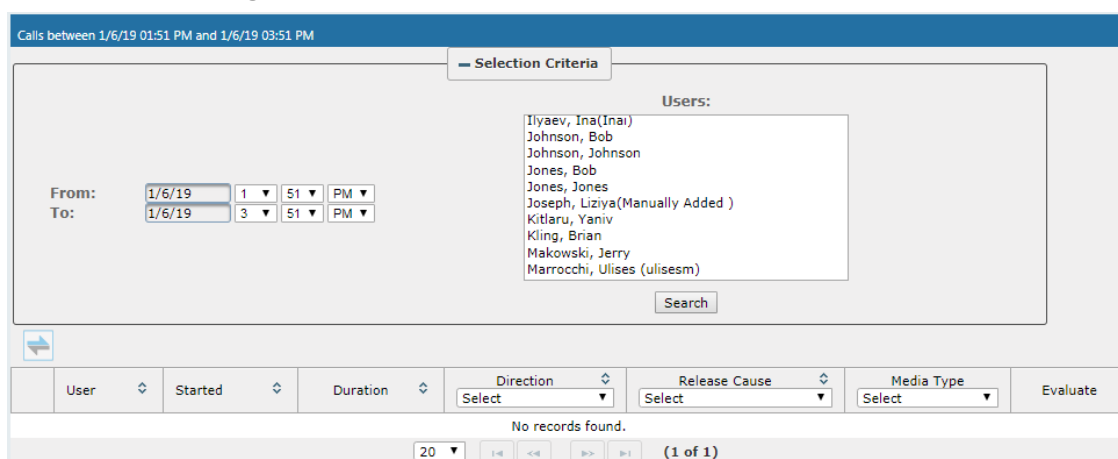


Figure 6-155: Evaluation Form User Selection



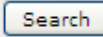
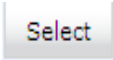
2. Select the user to evaluate, select a search date range and then click . A list of call records for the selected user is displayed.
3. Click  to select the form for this evaluation; the Call Search/Selection screen launches for the user to select the calls to evaluate.

Figure 6-156: Select Call to Evaluate

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

Selection Criteria

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
- Ilyayev, Ina(Inai)

Search

	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

20 1 (1 of 1)

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

Figure 6-157: Perform Evaluation Screen

Perform Evaluation: Customer Service

Johnson, Bob 2018-12-31 13:36:04.0 00:00:00 | 00:00:12

READY

0.2 1.0 5.0

⏮ ⏪ ⏩ ⏭ 🔊

Evaluate: 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%)



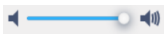
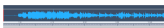





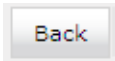
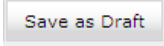
Questions	Answers	Score	Notes
How well did the agent communicate at an understandable rate and sound positive?	Choose One	0 out of 10	
How well did the agent seem to empathize with the customer?	Choose One	0 out of 10	
How well did the agent use probing questions to identify the problem?	Choose One	0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

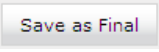
Section: Closing Section: Closing Score: 0 out of 30 (0%)

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	

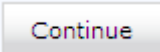
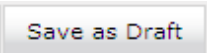
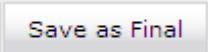
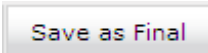
Save as Draft Save as Final

Table 6-56: 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 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.
Evaluatee:	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.
	Abort evaluation.
	Save Evaluation as a draft. Save as Draft to save evaluation before all answers scored.

Field	Description
	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  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  to save the current evaluation and resume later.
6. After all questions are answered, the  button becomes available.
7. Click  to complete the evaluation.

➤ **To review evaluations:**

Figure 6-158: Review Evaluations

Review Evaluations						
Form Name	Description	Status	Evalued	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 6-57: Review Evaluations – Field Descriptions

Field	Description
Form Name	Form Name used in the evaluation. Clicking this header sorts the search results in Ascending / Descending order alternating with each click. The dropdown entry shows only the matching results.

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.
	<div>View</div> <div>Click to view evaluation; the View Evaluation screen opens.</div>
	<div>Continue</div> <div>Click to continue evaluation; the Perform Evaluation screen opens.</div>
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**).

Average score report.

— Report Filter

Select form ▼ From: To:


Create 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.

Export Data

 ☒ Average ☐ All

2. Select the Average or All button and click **Export Data** to export the data; you're prompted to save or open the exported file.

Figure 6-159: 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

Create Report

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

Export Data


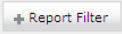
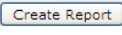
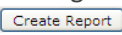
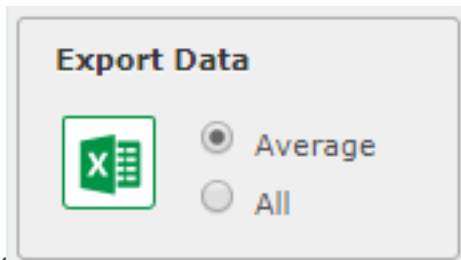
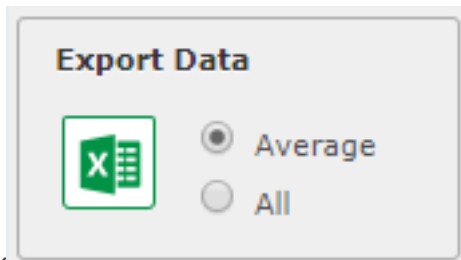
 ☒ Average ☐ All

Table 6-58: Average Score Report – Field Descriptions

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

Field	Description
	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° Live; can be changed by the user.
To:	Search before this call date(s). Automatically populated by SmartTAP 360° Live; can be changed by the user.
List of users	List of evaluatees. Automatically populated by SmartTAP 360° Live; select by clicking the required user.
	Only active when an Evaluatee is selected.
Only visible after clicking 	<ul style="list-style-type: none"> ■ Name (Name of Evaluatee) ■ 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) <div data-bbox="563 1305 1026 1563">  <p>The dialog box titled "Export Data" contains an Excel icon on the left. On the right, there are two radio buttons: "Average" (which is selected) and "All".</p> </div> <ul style="list-style-type: none"> ■ 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 6-160: Managing Instant Messages

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

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
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 6-161:
Instant Message Display-Skype for Business

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
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

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
How are you?
Dec 26, 2018 11:05:55 AM

sip:user2@sfb2019.lab
Great

Table 6-59: Search Messages

System Users Status

Calls Messages

From: 1/20/21 9 27 PM

To: 1/20/21 11 27 PM

☒ Active Users ☐ Inactive Users

☒ Users ☐ Groups

Users:

☒ Select All

ST-Teams100

ST-Teams30

ST-Teams31

ST-Teams32

TeamsTestUser2

TeamsTestUser5-E5

User (PLEASE DELETE), Initial

(1 of 1)

Text:

Search

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

Field	Description
From:	Earliest date and time to search from. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
To:	Latest date and time to search to. Click the date field for a calendar to pop up showing one month at a time. Use the dropdown to change the time of day.
Active Users	Users whose account is enabled in the SmartTAP 360° Live application.
Inactive Users	Users whose account has been deleted from the SmartTAP 360° Live 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.

Field	Description
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 6-162: Instant Message Search

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° Live'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

Operator	Description	Example
		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 negative. A message containing such a word is rated lower than others, but is not excluded altogether, as it would be with the - operator.	'+apple ~macintosh'Find messages that contain the word 'apple', but if the message also contains the word 'macintosh', rate it lower than if message does not.
*	The asterisk serves as the truncation (or wildcard) operator. Unlike the other operators, it is appended to the word to be affected. Words match if they begin with the word preceding the * operator.	'apple*'Find messages that contain words such as 'apple', 'apples', 'applesauce' etc.
"	A phrase that is enclosed within double quote (""") characters matches only rows that contain the phrase literally, as it was typed.	"some words"Find messages that contain the exact phrase "some words".



Some words (also known as stopwords) are ignored in full-text searches. In SmartTAP 360° Live, the minimum length of the word for full-text searches is 2.

- 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.
- From the Chat Type drop-down list, select either Chat or Group Chat; the results are filtered accordingly.

Figure 6-163: 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
1	Adar, Tania	Nov 21, 2018 7:59:02 PM	Nov 21, 2018 8:05:41 PM	sip:alejandro.orta@audiocodes.com; Adar, Tania	CHAT
2	Adar, Tania	Nov 21, 2018 8:28:48 PM	Nov 21, 2018 8:32:38 PM	sip:debajyoti.dutta@audiocodes.com; Adar, Tania	CHAT
3	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 1:34:40 PM	sip:user2@sfb2019.lab; Mast, Danielle	CHAT
4	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 6-164: 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
1	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 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: <ul style="list-style-type: none"> Chat: person-to-person chat Group Chat: chat for two or more persons. For Group Chat, the Conference ID is also displayed.

- 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 203).

Figure 6-165: 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
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:

PDF

Adar, Tania

Hello Alex

Nov 21, 2018 7:59:17 PM

Adar, Tania

Hello Alex

Nov 21, 2018 7:59:51 PM

Adar, Tania

Can you please approve the transaction #1234567

Nov 21, 2018 8:00:55 PM

Adar, Tania

Great! Thank you

sip:alejandro.orta@audiocodes.com

Hi Tania

Nov 21, 2018 8:00:16 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	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 6-166: 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
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: PDF
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

50 1 (1 of 1)

Figure 6-167: 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
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:

Dec 26, 2018 11:06:18 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.
	Export the conversation messages to a PDF file (including file transfer information from messages).



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

Specific Considerations for Microsoft Teams Instant Messages

SmartTAP utilizes Microsoft Graph Teams Export API for recording Microsoft Teams Chat messages. Before you can view Instant Messages, the following Microsoft Teams prerequisites and licenses must be installed:

[Prerequisites to access Teams Export APIs](#)



Microsoft Beta API, as well as the feature itself are not yet supported for production applications.

Features:

- When Editing a chat message, the new message content will be replaced with the original one, and “This message has been edited” will be displayed on top of it.
- When Deleting a chat message, the content of the message will still be displayed, and “This message has been deleted” will be displayed on top of it.
- Clicking ‘Undo’ on deleted message will be considered as Edited.
- HTML based messages, such as Formatted\Tables\Links are not supported, only the content will be displayed .
- Text formatting is not reflected in Teams Chat messages (Bold\Underline\Italic\etc.)
- Emojis, Gifs and any other special content will not be displayed in Teams chat messages.
- Channel messages are not supported
- URLs of attached or transferred files are displayed in SmartTAP when a chat is included the attachment/transfer (see below)

Figure 6-168: Channel Messages

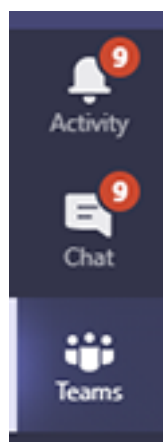


Figure 6-169: Instant Message Display Microsoft Teams


Instant Messages between 12/20/20 12:10 PM and 12/20/20 02:10 PM

User	First Message Time	Last Message Time	Messaging Parties	Chat Type
Test	Dec 20, 2020 2:08:29 PM	Dec 20, 2020 2:08:29 PM	Test; ST-Teams100	CHAT

Begin Time: 12/20/20 12 PM
End Time: 12/20/20 2 PM

Search text:

Participants:
Test ☒
ST-Teams100 ☒

Export To: 

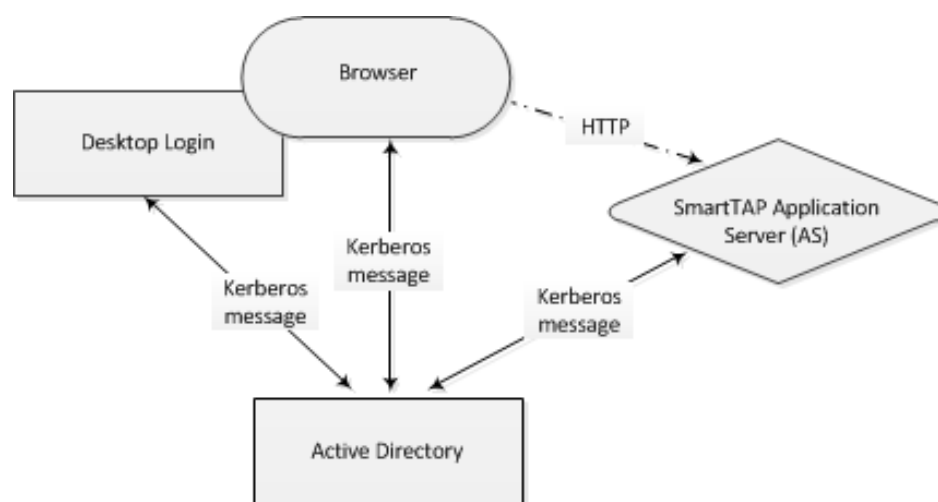
Test
Hi! I'm sending you files.

Attachments:
Name: attach1.txt
ContentUrl: [https://smarttap-my.sharepoint.com/personal/teamstestuser2_ailogix_net/Documents/Microsoft Teams Chat Files/attach1.txt](https://smarttap-my.sharepoint.com/personal/teamstestuser2_ailogix_net/Documents/Microsoft%20Teams%20Chat%20Files/attach1.txt)
Name: attach3.txt
ContentUrl: [https://smarttap-my.sharepoint.com/personal/teamstestuser2_ailogix_net/Documents/Microsoft Teams Chat Files/attach3.txt](https://smarttap-my.sharepoint.com/personal/teamstestuser2_ailogix_net/Documents/Microsoft%20Teams%20Chat%20Files/attach3.txt)
Name: attach2.txt
ContentUrl: [https://smarttap-my.sharepoint.com/personal/teamstestuser2_ailogix_net/Documents/Microsoft Teams Chat Files/attach2.txt](https://smarttap-my.sharepoint.com/personal/teamstestuser2_ailogix_net/Documents/Microsoft%20Teams%20Chat%20Files/attach2.txt)
Dec 20, 2020 2:08:29 PM

7 Single Sign-On for SmartTAP 360° Live

This chapter describes the Single Sign-On functionality for SmartTAP 360° Live. 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° Live Web server via a Web browser (Microsoft Edge, 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° Live 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° Live Web interface and for quick access to different SmartTAP 360° Live 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° Live server.
- SSO was successfully tested with both Client Users and the SmartTAP 360° Live 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° Live 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° Live database. If they were not manually added, then LDAP must be configured so that SmartTAP 360° Live can validate the user and find the user's Roles/Permissions (see [Configuring SSL](#) on page 89)

■ 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	Description
{username}	New domain user required for SmartTAP 360° Live 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° Live 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 the example in this section : 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° Live server. Must be in the form {machine name}.{domain}. Example: SmartTAP 360° Live.myDomain.local. If a CNAME alias is used to map an unfriendly machine name to a friendlier one such as SmartTAP 360° Live, 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° Live.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° Live 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° Live 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° Live 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° Live does not need this file to be exported. The Client obtains an encrypted version of the keytab and sends it to SmartTAP 360° Live 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° Live 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° Live – 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

testUser testUser Properties (General Tab)

Published Certificates | Member Of | Password Replication | Dial-in | Object

Security | Environment | Sessions

Remote control | Remote Desktop Services Profile

Personal/Virtual Desktop | COM+ | UNIX Attributes | Attribute Editor

General | Address | Account | Profile | Telephones | Organization

User login name: testUser @myDomain.local

User login 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

OK Cancel Apply Help

testUser testUser Properties (Attributes Tab)

Published Certificates | Member Of | Password Replication | Dial-in | Object

Security | Environment | Sessions

Remote control | Remote Desktop Services Profile

General | Address | Account | Profile | Telephones | Organization

Personal/Virtual Desktop | COM+ | UNIX Attributes | Attribute Editor

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_ACCOUNT1
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 1
whenCreated	10/27/2014 10:17:25 AM Eastern Daylight 1

Edit Filter

OK Cancel Apply Help

Figure 7-3: After Running the ktpass Command

The figure shows two side-by-side screenshots of the 'testUser testUser Properties' dialog box in Windows Active Directory.

Left Screenshot (General Tab):

- User logon name:** HTTP/smarttap.myDomain.local @MYDOMAIN.LOCAL
- User logon name (pre-Windows 2000):** MYDOMAIN\testUser
- Logon Hours...** and **Log On I...** buttons are present.
- Unlock account:** ☐ (unchecked)
- 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

Right Screenshot (Attributes Tab):

Attribute	Value
objectSid	S-1-5-21-2092303587-4016032574-4140064
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	10/27/2014 10:33:28 AM Eastern Daylight T
replicPropertyMetaData	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° Live Application Server to use for authenticating clients login attempts. The SSO User is only to be used within SmartTAP 360° Live and should not be used to log into any machine on the domain, including the SmartTAP 360° Live 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

■ 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° Live 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° Live.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° Live 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° Live 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° Live 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° Live, you should enable Integrated Windows Authentication (IWA) on your Web browser. This enables the silent authentication of the connection negotiation to the SmartTAP portal URL:

- [Enabling Microsoft Edge Browser with IWA](#) on the next page
- [Enabling Firefox Browser with IWA](#) on page 222

- [Enabling Chrome Browser with IWA](#) on page 223

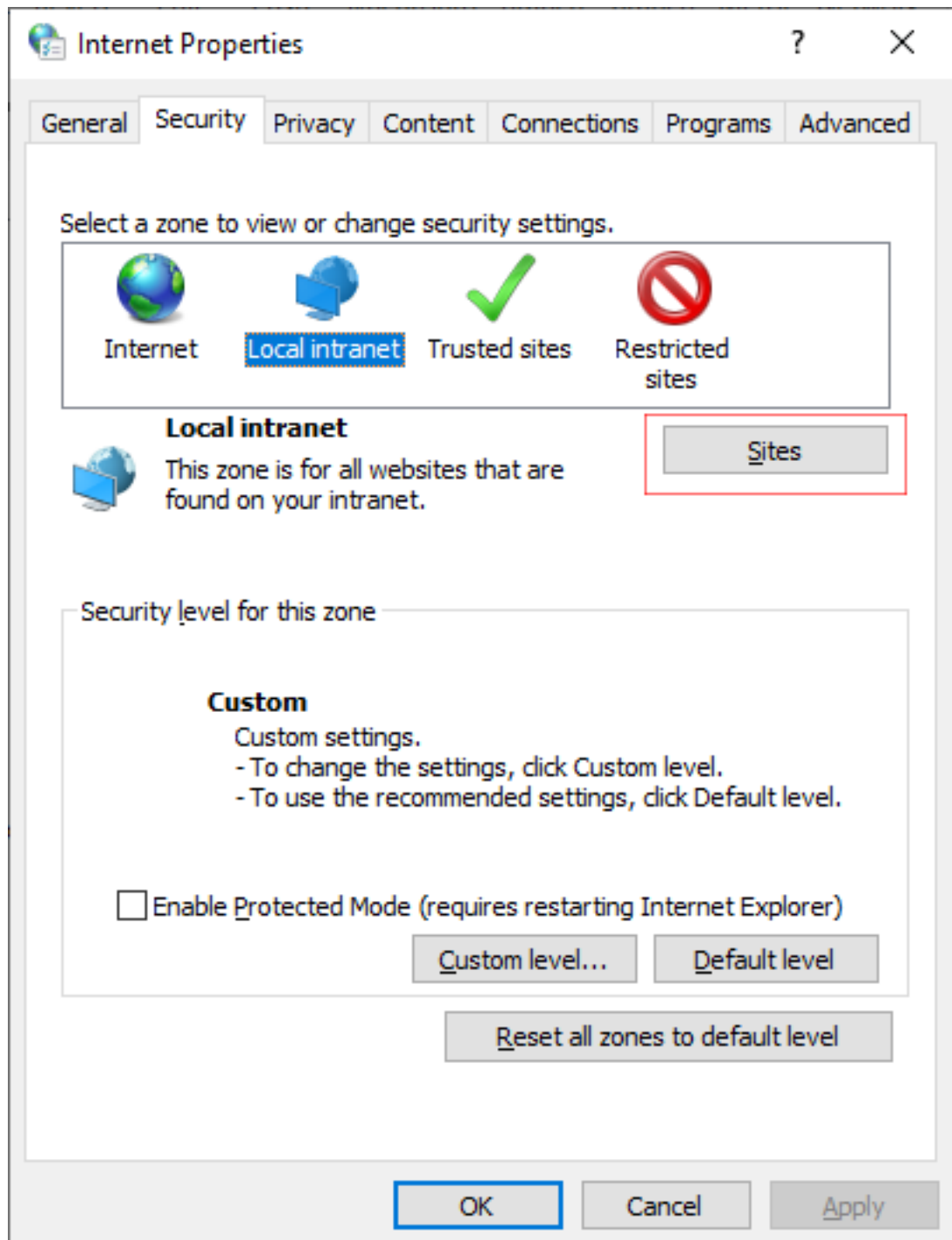
Enabling Microsoft Edge Browser with IWA

When using Microsoft Edge to open the SmartTAP Portal, users can only be authenticated silently when the browser has Integrated Windows Authentication (IWA) enabled. For Edge, Integrated Windows Authentication (IWA) only works for sites explicitly configured under the 'Local Intranet' security zone under 'Internet Options' control-panel applet. A server is recognized as part of the local Intranet Security zone when the user specifies a URL with a fully qualified name that has been explicitly configured as a local intranet site in Edge. Use the following procedure to enable silent authentication on each computer (or through policy).

➤ To enable Microsoft Edge with IWA:

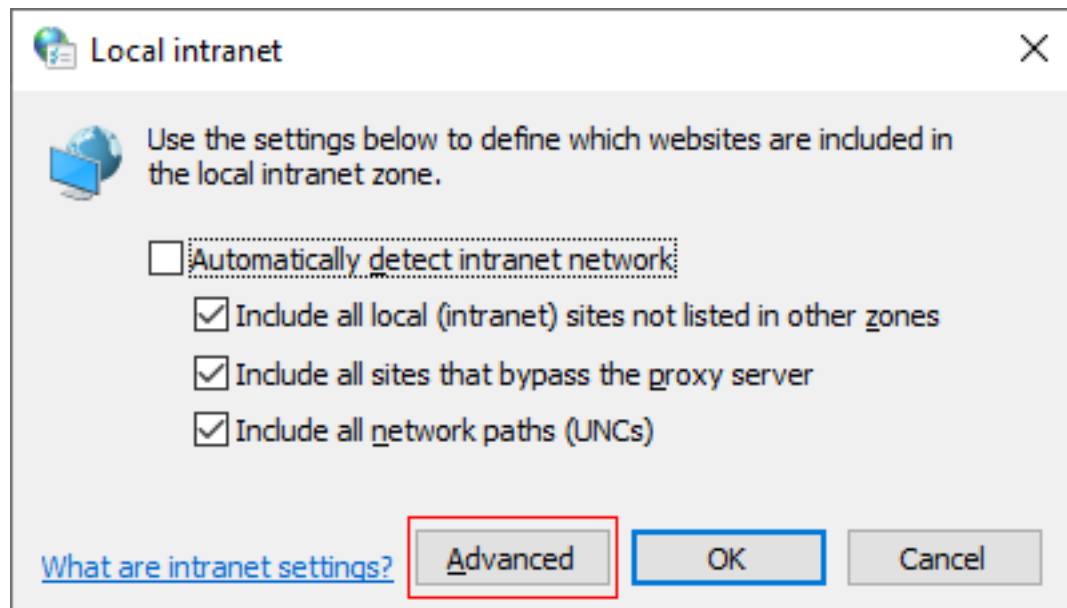
1. Open the Windows Settings and search **Internet Options**.

Figure 7-5: Internet Properties



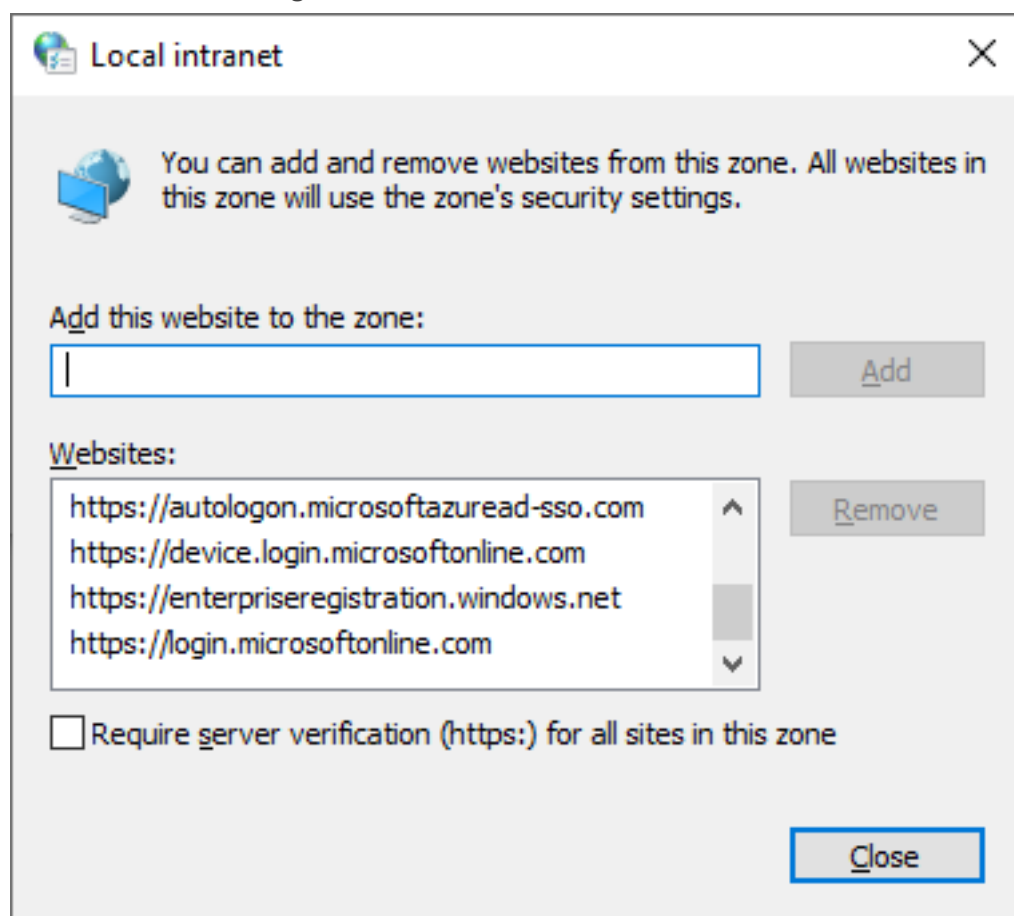
2. Click **Local intranet** > **Sites**.

Figure 7-6: Sites



3. Click **Advanced** -> Enter the tenant specific URL for the SmartTAP portal into the Websites text box.

Figure 7-7: Tenant URL



4. Click **Close**.

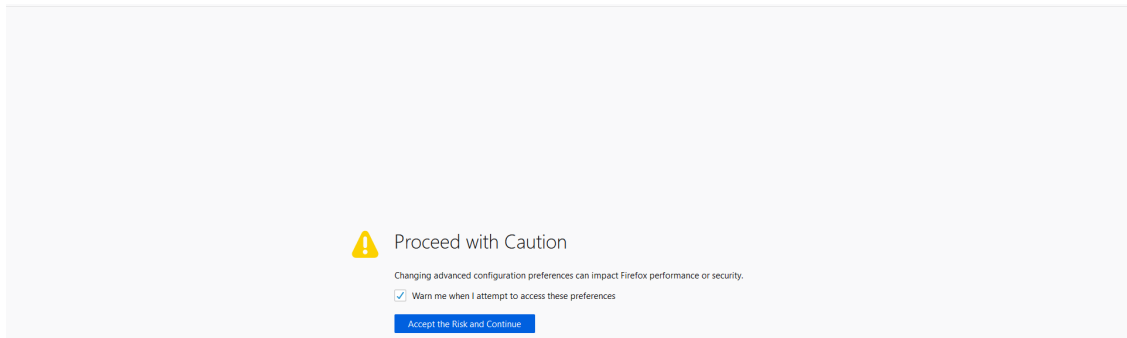
Enabling Firefox Browser with IWA

This section describes how to enable Firefox browsers with Integrated Windows Authentication (IWA) for Silent Authentication.

➤ To enable Firefox browsers with IWA:

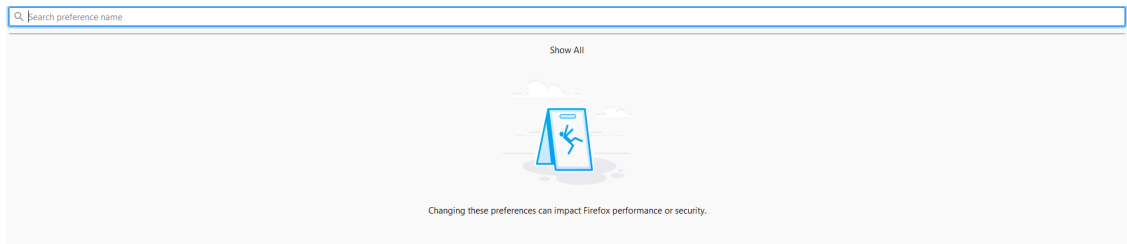
1. Open Firefox, enter the URL **about:config** and then press Enter; Firefox warns you're updating its internal settings.

Figure 7-8: Proceed with Caution



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

Figure 7-9: Firefox Negotiation Options



3. In the 'Search' field, enter **network.negotiate-auth** to show all negotiation options.

Figure 7-10: Network.Negotiate-Auth

Search: network.negotiate-auth		
network.negotiate-auth.allow-non-fqdn	false	⚙
network.negotiate-auth.allow-proxies	true	⚙
network.negotiate-auth.delegation-uris		✎
network.negotiate-auth.gsslib		✎
network.negotiate-auth.trusted-uris		✎
network.negotiate-auth.using-native-gsslib	true	⚙
network.negotiate-auth	<input checked="" type="radio"/> Boolean <input type="radio"/> Number <input type="radio"/> String	+

4. Enter the tenant specific URL for the SmartTAP portal to the list of trusted URIs by updating the option **network.negotiate-auth.trusted-uris**.

Figure 7-11: Add SmartTAP 360° Live FQDN

Field	Value	Control
network.negotiate-auth.allow-non-fqdn	false	Boolean
network.negotiate-auth.allow-proxies	true	Boolean
network.negotiate-auth.delegation-uris		String
network.negotiate-auth.gsslib		String
network.negotiate-auth.trusted-uris	Smarttap.myDomain.local	String
network.negotiate-auth.using-native-gsslib	true	Boolean

- Restart Firefox; SSO now functions on Firefox.



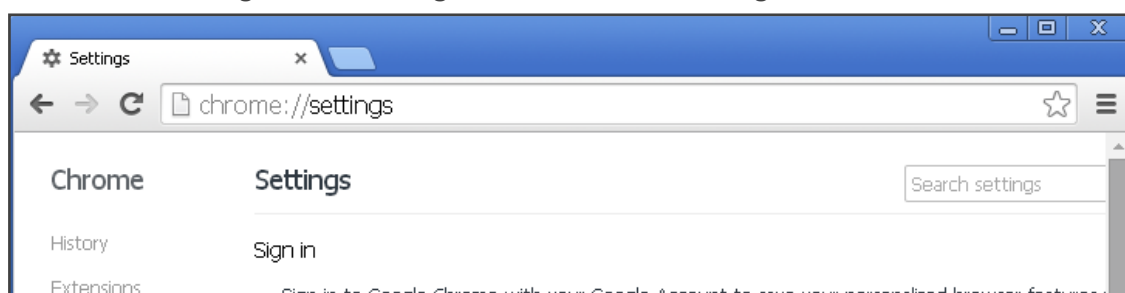
Additional changes may be required for Firefox. If SSO does not function immediately after these changes, see. [Troubleshooting Single Sign-On](#) on page 225

Enabling Chrome Browser with IWA

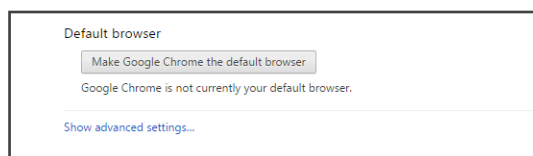
This section describes how to enable Chrome browsers with Integrated Windows Authentication (IWA) for Silent Authentication.

➤ To configure Chrome browser settings:

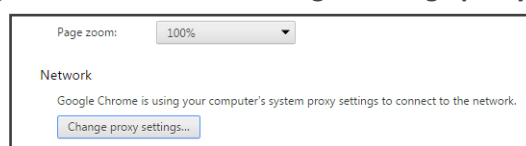
- Open the Chrome browser and click the menu icon located to the right of the address field, and then select **Settings**. Alternatively, browse to `chrome://settings`.

Figure 7-12: Google Chrome Browser Settings

- 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.

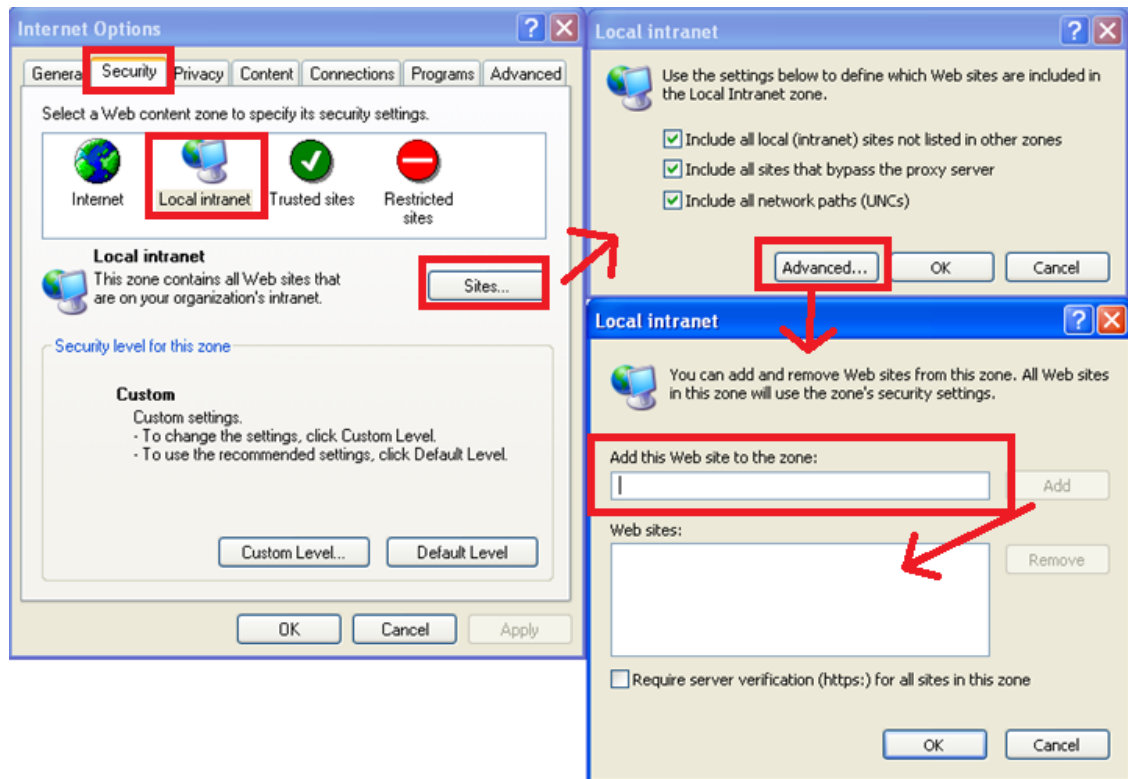
Figure 7-13: Google Chrome Browser Settings – Show advanced settings

- Locate the 'Network' setting and click the button Change proxy settings under the Connections tab

Figure 7-14: Google Chrome Browser Settings – Change proxy settings

4. (Security tab > Local Intranet zone > Sites... > Advanced... > add the SmartTAP 360° Live FQDN to the local Intranet zone.
5. Close all Google Chrome windows and restart; SSO takes place.

Figure 7-15: Google Chrome Browser Settings – Adding a Web Site to the Zone



Testing Single Sign-On

After logging into the domain computer and configuring the browser to trust the SmartTAP 360° Live server as described in previous sections, you can browse to the SmartTAP 360° Live Web server, preferably via the SmartTAP 360° Live 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 7-16: Browsing to the SmartTAP 360° Live Web Server

If an error page is displayed, or if the normal login form for SmartTAP 360° Live 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° Live 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° Live 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° Live via SSO. The form login page of SmartTAP 360° Live must be accessed in order to log in as this user.

It is recommended that a domain user be given valid SmartTAP 360° Live permissions to make system changes so that the default SmartTAP 360° Live 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° Live 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° Live 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, if the trust relationship is not present (SmartTAP 360° Live 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° Live 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 which prompts for the client's domain credentials, not the SmartTAP 360° Live login credentials.

What can I do when this login prompt pops up ?

There are a few directions this prompt can go:

- Enter a valid username and password for a domain user; SSO is attempted using those credentials. If successful, you will be logged into SmartTAP 360° Live 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 however 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° Live 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° Live 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° Live.xml file for the SmartTAP 360° Live Application Server: <code>org.apache.coyote.http11.Http11Protocol.MAX_HEADER_SIZE</code> 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° Live 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.
403 – Forbidden	The user is forbidden from viewing this page. The user was authenticated correctly (SSO is functioning) but is trying to view a restricted page. Can occur if the user manually browses to a page they're not allowed to

Error Code	Description
	access. Another cause is if SmartTAP 360° Live cannot determine the User Roles/Permissions for this user. Make sure the user performing SSO is part of the domain and that SmartTAP 360° Live 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° Live 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° Live server though instances occur in which the Firefox browser does not attempt to authenticate even when the SmartTAP 360° Live server is trusted. For 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 which was then upgraded to the latest version. 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 due to the fact that a previous configuration from the older version of Firefox conflicted with the configuration of the later version of Firefox. It has not been determined exactly which configuration caused this error.
- 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° Live.

- 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° Live 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° Live 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° Live server.
- Org.ietf.jgss.GSSEException 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° Live. 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° Live from a Firefox browser, with trusted site configured.

■ Troubleshooting with More Detailed SmartTAP 360° Live 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° Live logging.

The loggers can be configured through the SmartTAP 360° Live 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° Live.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° Live. 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° Live 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° Live 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° Live server as a trusted server.
- e. Attempt SSO again.

8 SmartTAP 360° Live Skype for Business Toolbar

The SmartTAP 360° Live 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° Live 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](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.

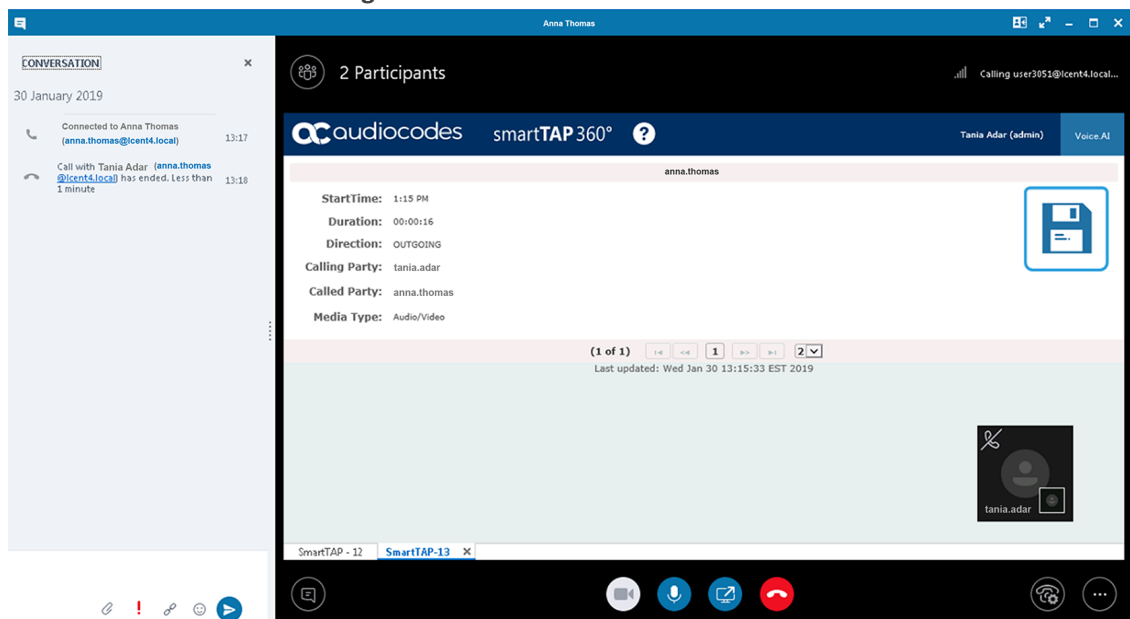
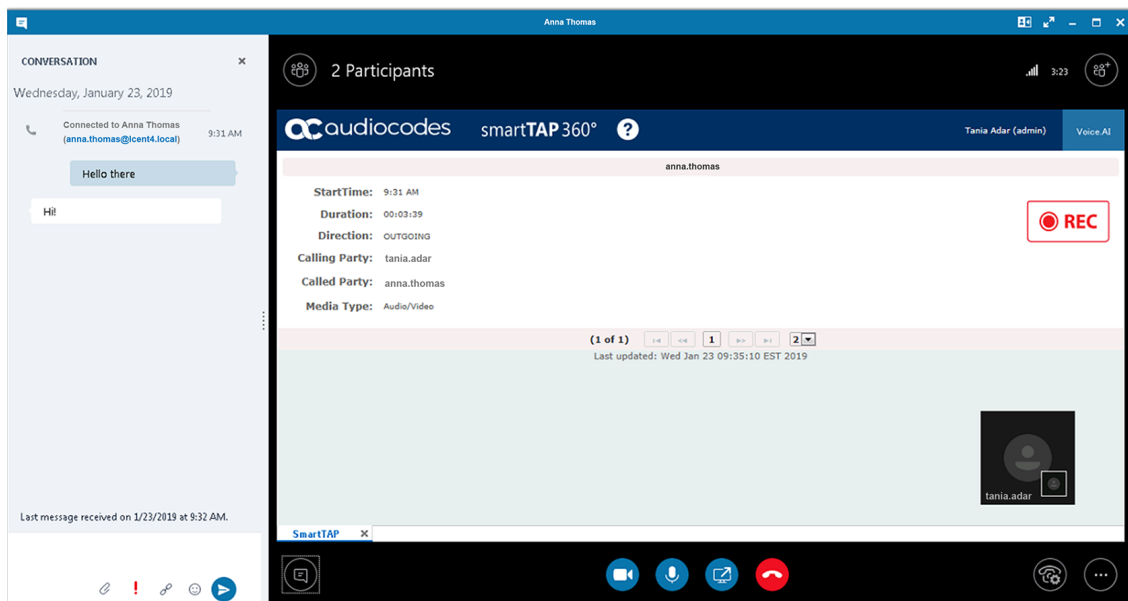
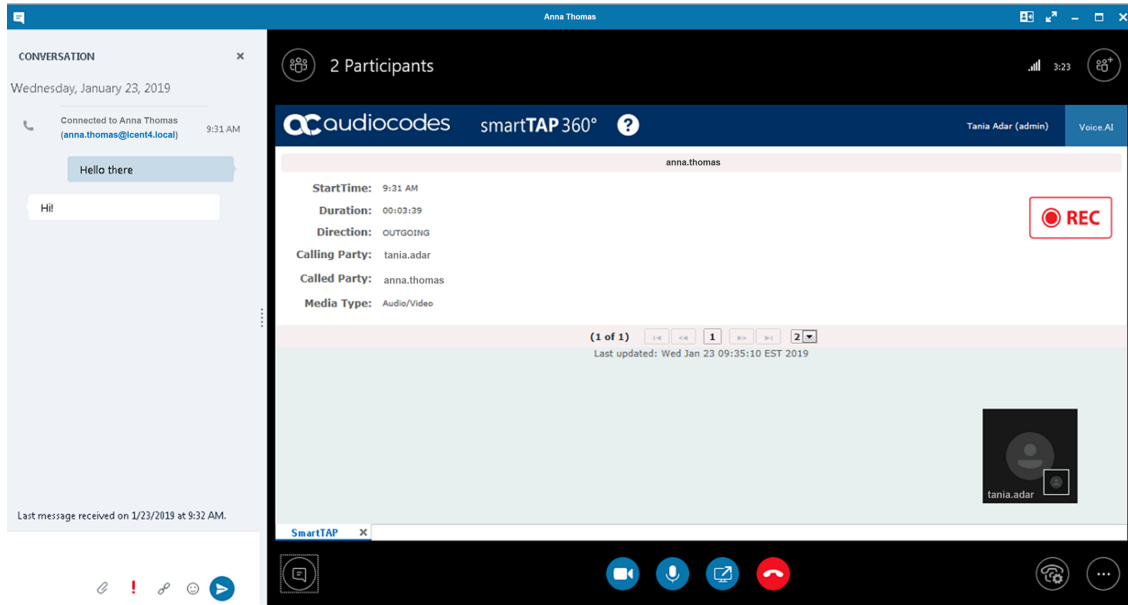
Figure 8-1: SmartTAP 360° Live: Save On Demand (SOD)**Figure 8-2:****Figure 8-3: Record on Demand (ROD)**

Figure 8-4: SmartTAP 360° Live Skype for Business CWE Toolbar (Pause / Resume)

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° Live 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° Live UI. Administrators must enter their credentials to access the application. Security credentials assigned by SmartTAP 360° Live determine which users will be visible and whose associated calls will be available for downloading.

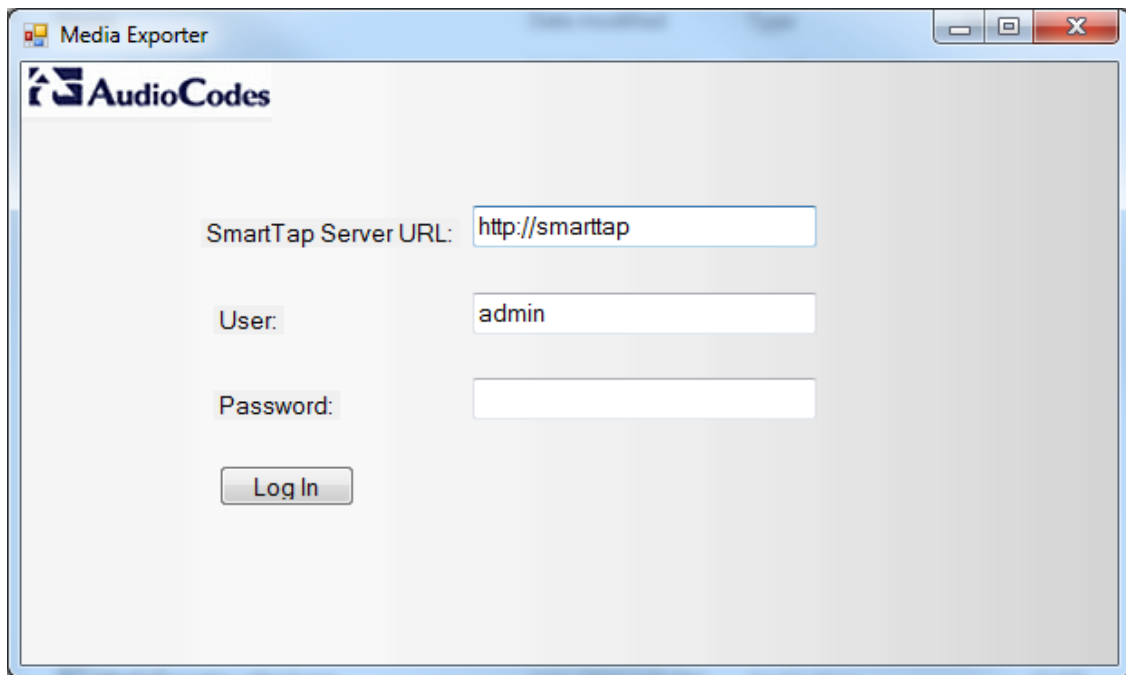


Currently both audio and video call types can be exported together. The video component of video calls is not exported in the current version. Alternatively, only the audio of video calls is exported in this version.

➤ To run the Media Exporter:

1. Run the MediaExporter.exe tool from your Windows PC.
2. Enter the access details and credentials:
 - SmartTAP 360° Live URL to be used to access the SmartTAP 360° Live UI
 - Enter the username (same as that used to access the SmartTAP 360° Live UI)
 - Enter the password

Figure 9-1: Credentials



The screenshot shows a window titled "Media Exporter" with the AudioCodes logo in the top left corner. The window contains the following fields and controls:

- SmartTap Server URL:** A text input field containing the value "http://smarttap".
- User:** A text input field containing the value "admin".
- Password:** An empty text input field.
- Log In:** A button located below the password field.

3. Enter the Search Criteria.

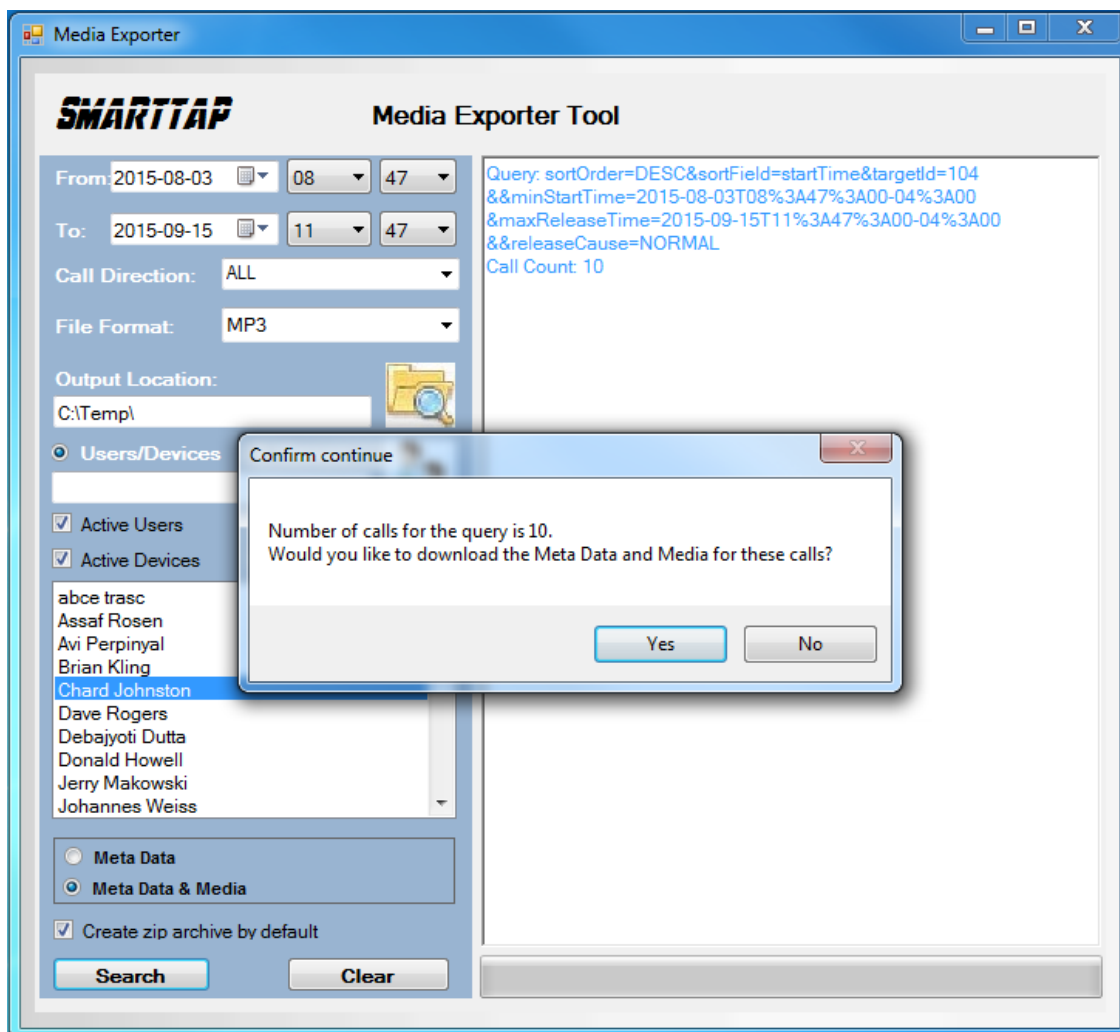
Figure 9-2: Enter the Search Criteria

The screenshot shows the 'Media Exporter Tool' window. The interface includes the following fields and options:

- From:** 2015-09-15, 08:47
- To:** 2015-09-15, 11:47
- Call Direction:** ALL
- File Format:** MP3
- Output Location:** C:\Temp\
- Search Scope:** ☒ Users/Devices, ☐ Groups
- Filters:**
 - ☒ Active Users, ☐ Inactive Users
 - ☒ Active Devices, ☐ Inactive Devices
- User List:**
 - abce trasc
 - Assaf Rosen
 - Avi Perpinyal
 - Brian Kling
 - Chard Johnston** (highlighted)
 - Dave Rogers
 - Debajyoti Dutta
 - Donald Howell
 - Jerry Makowski
 - Johannes Weiss
- Export Options:**
 - ☐ Meta Data
 - ☒ Meta Data & Media
 - ☒ Create zip archive by default
- Buttons:** Search, Clear

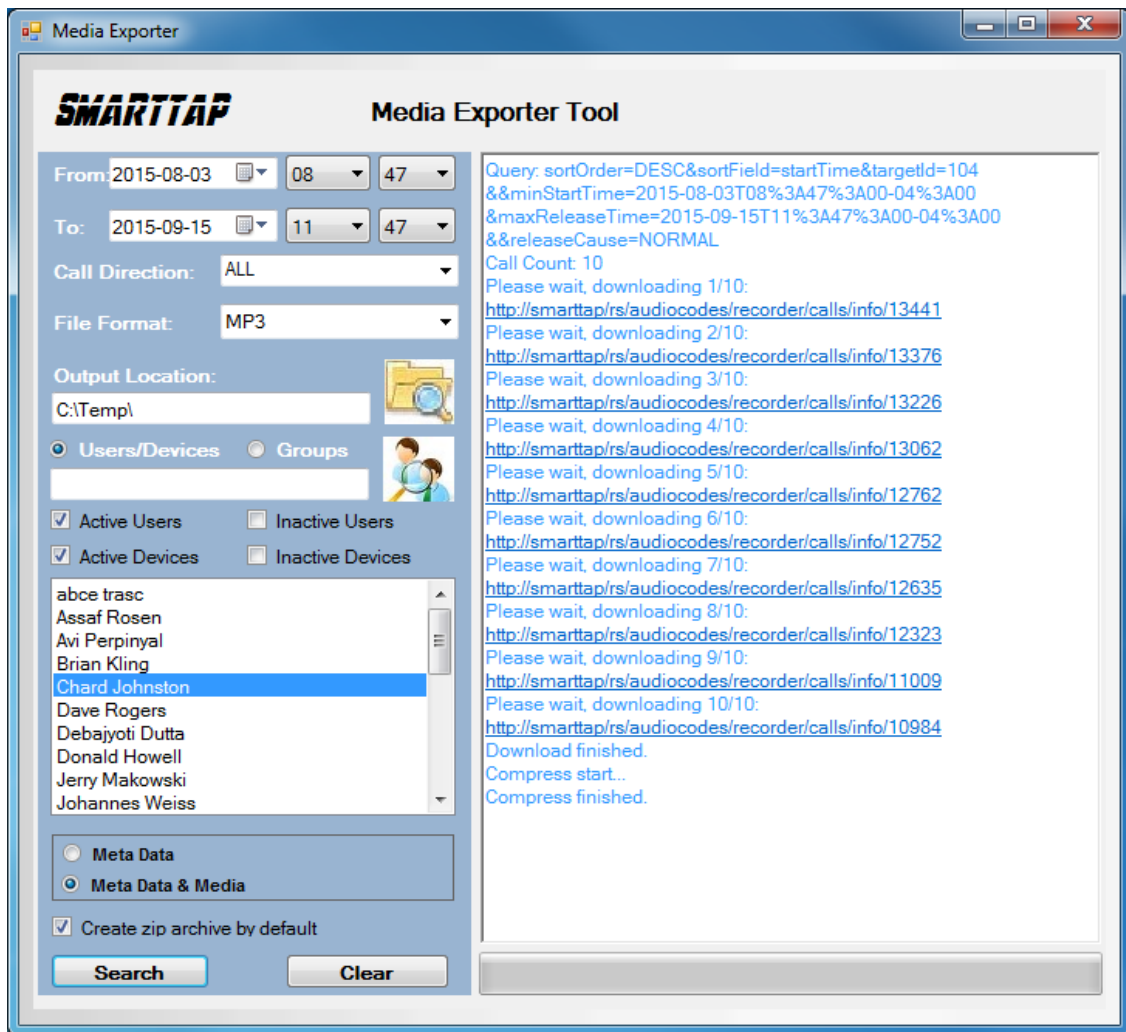
- The following search criteria definitions are identical to those of the SmartTAP 360° Live Web interface:
 - ◆ File Format (MP3, WAV) Either format can be played using standard Media Player
 - ◆ Output location: Where do you want the zip file and contents to be saved?
 - ◆ Meta Data or Meta Data & 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



4. Select Yes to start downloading the calls.

Figure 9-4: Downloading



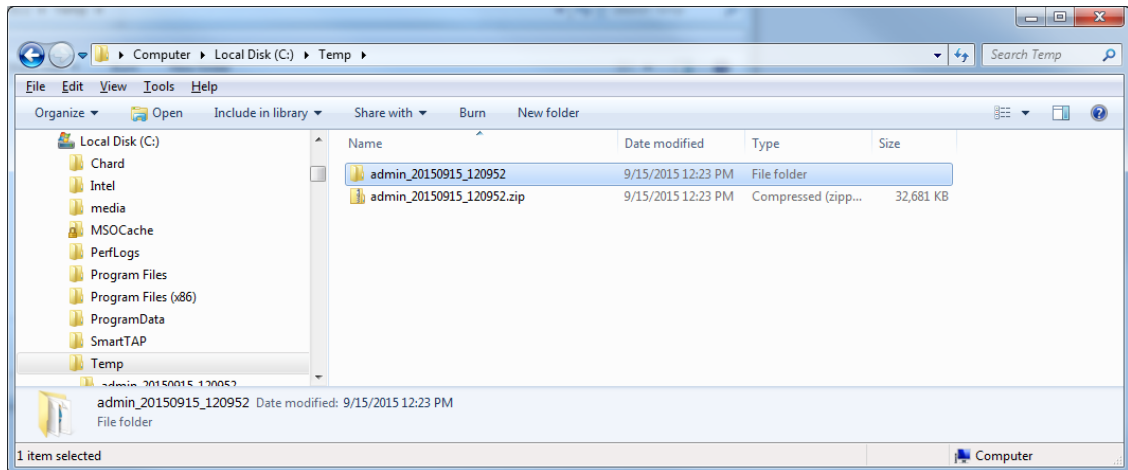
After the download completes, the default browser automatically opens presenting the Call Manifest for the calls from the search results.

Figure 9-5: Call Manifest

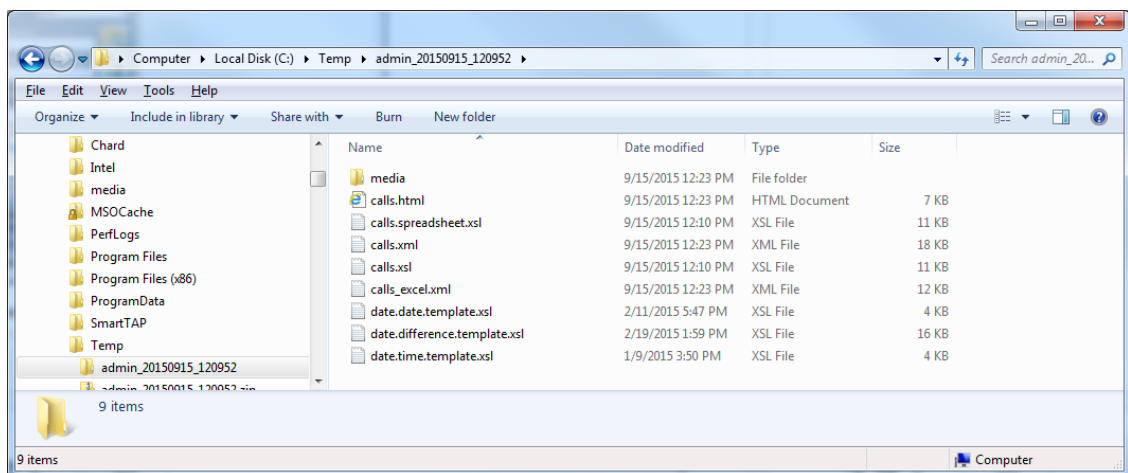
The screenshot shows a web browser window displaying the 'Call Manifest' table. The table lists call details for Chard Johnston, including dates, times, durations, directions, and parties involved. The table is filtered to show 10 results.

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	9:55:46	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	6:6:21	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	9:30:29	OUTGOING	chard.johnston	conf-Ronald Romanchuk	conf-Ronald Romanchuk		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	9:34:10	OUTGOING	chard.johnston	conf-Philippe Blancart	conf-Philippe Blancart		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	9:38:45	OUTGOING	chard.johnston	+01133390677043	+01133390677043		NORMAL	media:Johnston, Chard, 2015_09_02_09_02_38.mp3
Johnston, Chard	2015-08-27	13:00:38	2015-08-27	13:01:01	2015-08-27	13:32:46	9:31:48	OUTGOING	chard.johnston	+18775664408	+18775664408		NORMAL	media:Johnston, Chard, 2015_08_27_13_00_38.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

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

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

Figure 9-7: Contents of Folder

Calls.html: Call Manifest

Calls.xml: Call Meta Data exported from SmartTAP 360° Live 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° Live API is a RESTful Web Services API that provides complete access to and control over the SmartTAP 360° Live 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>



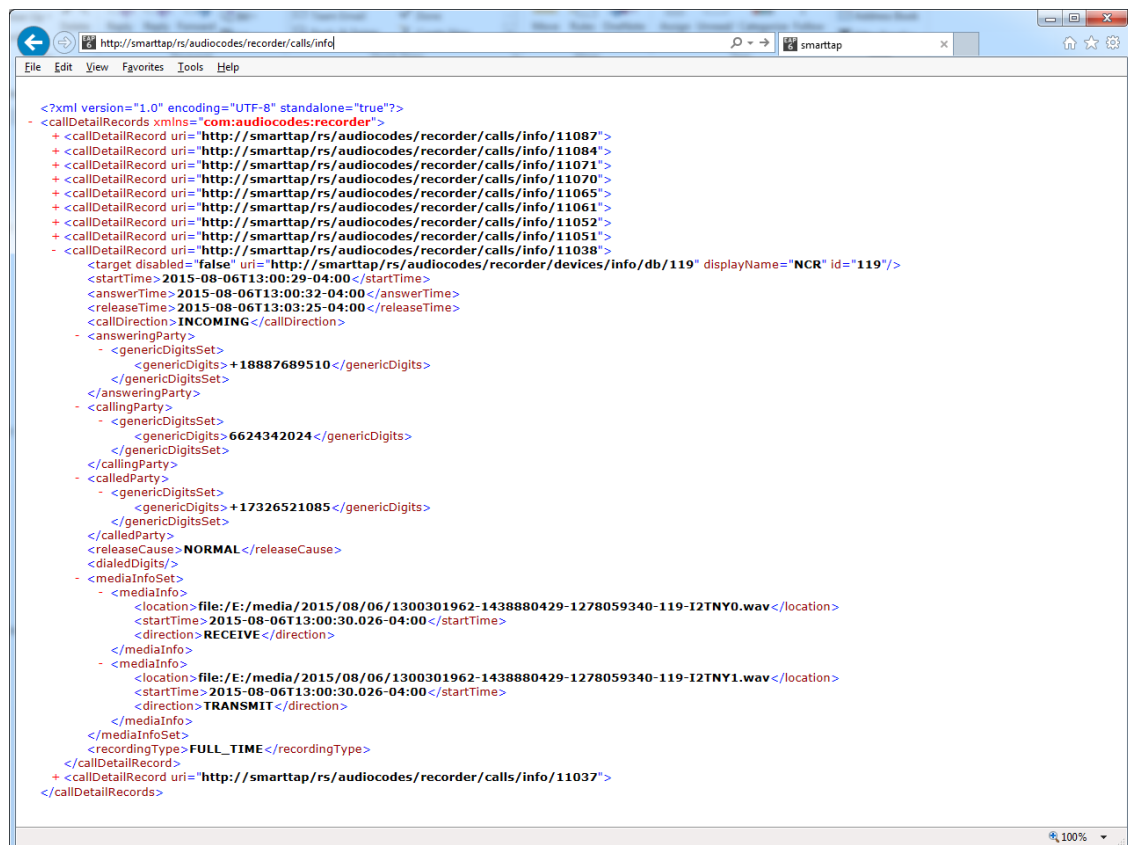
Change 'URL' to the IP address or the name of your SmartTAP 360° Live product.

<http://SmartTAP 360° Live/rs/audiocodes/recorder> - path to SmartTAP 360° Live

/calls - SmartTAP 360° Live Rest API resource

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

Figure 10-1: API Integration



To learn more about the SmartTAP 360° Live REST API, see the HTML documentation included with the SmartTAP 360° Live 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 for each user enabled for recording
- Silent or nomedia 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).

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° Live server as a part of the SmartTAP 360° Live 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 244

General Configuration

This section describes the general configuration for Recording Health Monitor utility.



The user interface should be configured once following the installation and further updates should be made directly in the AudioCodes\Tools\HealthMonitor\Config.

Figure 11-1: General Configuration

The screenshot shows the 'General Configuration' window. It features a tabbed interface with 'General' selected. Under the 'Configuration' heading, there is a list of days (Monday to Sunday) for scheduling reports. Next to it is a 'Report Time' field with a clock icon. Below that is an 'Email notification' checkbox. A large green 'SAVE' button is at the bottom.

- **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 68 Default: Disabled.
- **DelayReportInSec:** Provides delay time before starting and generating reports. Default -0 not enabled (seconds)


```
AudioCodes
\Tools\HealthMonitor\ConfigDelayReportInSec>0</DelayReportInSec>
```

- **FileAccessRetryIntervalSec:** Enables the Health Monitor to retry to access Blob\SMB location. The value reflects the time to wait between each retry. Default-1 (seconds)

```
AudioCodes
\Tools\HealthMonitor\Config<FileAccessRetryIntervalSec>1</FileAccessRetryIntervalSec>
```

- **FileAccessRetryCount:** Enables the setting of the number of retries to access Blob\SMB locations. Default-3

```
AudioCodes
\Tools\HealthMonitor\Config<FileAccessRetryCount>3</FileAccessRetryCount>
```

- **ReportLocaton:** Enables the storage of reports in a custom location. Default is [HM LOCATION]\Reports.

```
AudioCodes
\Tools\HealthMonitor\Config<ReportLocation>Reports\</ReportLocation>
```

REST API Configuration

This section describes the REST API configuration for the Recording Health Monitor.

Figure 11-2: REST API Configuration

The screenshot shows the REST API Configuration page. The top navigation bar has four tabs: 'General', 'REST Api' (which is active and highlighted in green), 'SMB', and 'SMTP'. Below the tabs, there are three input fields: 'Address (http(s):#)*', 'Username*', and 'Password*'. At the bottom of the page is a large green button labeled 'SAVE'.

The Health Monitor uses a dedicated user for REST communication with Application Server. It is not necessary to modify this configuration.



- In case the Application server is configured for HTTPS or OAuth, 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.
- For OAuth configuration, configuration changes should be performed in RecordingHealthMonitor.config file. See "Health Monitor with HTTPS" in the SmartTAP 360° Live Installation Manual.

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 11-3: 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
```

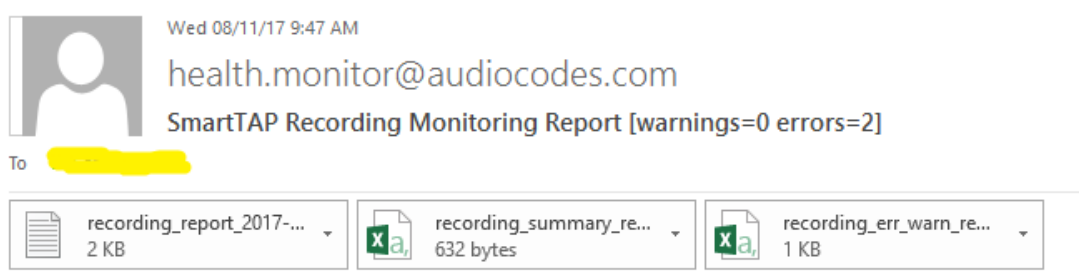
Figure 11-4: Example 2: recording_summary_report_YEAR-Month-Day.csv:

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 11-5: 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 11-6: Email Format:



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

Received from: <http://172.17.127.133>

12 Announcement Server (Skype for Business)

SmartTAP 360° Live 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° Live 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 118 and [Announcement Server - Example Configurations](#)). For installing and setting up the Announcement server,



- SmartTAP 360° Live 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.
- **For Microsoft Teams:** For Microsoft Teams recording notifications are provided by Microsoft.

This section includes the following:

- [Simple Announcement](#) below
- [IVR](#) on the next page
- [Example Announcement Server Scenarios](#) on page 252
- [Announcement Server Configuration Parameters](#) on page 254
- [Announcement Server - Example Configurations](#)

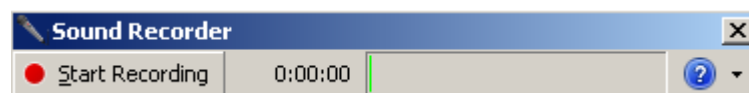
Simple Announcement

SmartTAP 360° Live 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



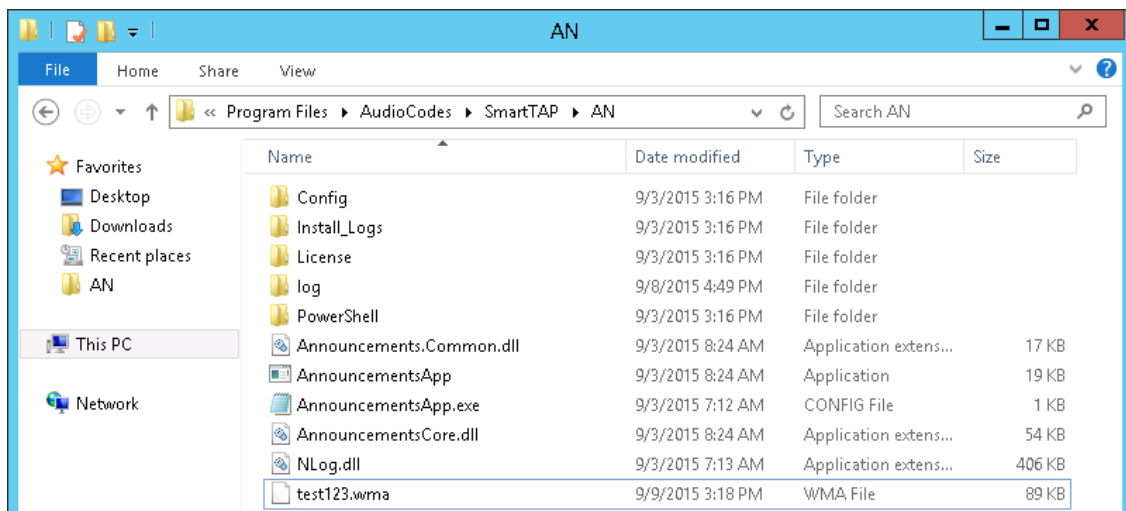
Example: "Thank you for calling Company A, your call may be recorded for quality assurance".

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° Live\AN\Config\StateMachineConfig



Ensure that you save the file in WMA format.

Figure 12-2: Announcement Server



IVR

SmartTAP 360° Live 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 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 250)

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 118).

Configuring IVR Script Files

The IVR files are located as follows:

- The prompt media files are located under ...\\Program Files\\AudioCodes\\SmartTAP 360° Live\\AN\\Languages. USA English media files are under en-us folder.
- The IVR state machines are located under Program Files\\AudioCodes\\SmartTAP 360° Live\\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 118).

- The IVR sample state machines are located under Program Files\AudioCodes\SmartTAP 360° Live\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.vma",
      "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"
        }
      ]
    },
    {
      "Type": "AnnouncementsCore.AnnTree.AnnMenuNode, AnnouncementsCore",
      "PromptName": "ivr.vma",
      "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.vma",
      "Id": "3",
      "NextId": null,
      "ErrorNextId": null,
      "IsFirst": false
    },
    {
      "Type": "AnnouncementsCore.AnnTree.AnnPlayPromptNode, AnnouncementsCore",
      "PromptName": "DeclineResultPrompt.vma",
      "Id": "4",
      "NextId": null,
      "ErrorNextId": null,
      "IsFirst": false
    },
    {
      "Type": "AnnouncementsCore.AnnTree.AnnPlayPromptNode, AnnouncementsCore",
      "PromptName": "errorPrompt.vma",
      "Id": "5",
      "NextId": null,
      "ErrorNextId": null,
      "IsFirst": false
    }
  ],
  "ToneHandlerConfig": {
    "Type": "AnnouncementsCore.AnnTreeModel.ToneHandlerConfig, AnnouncementsCore",
    "MaxAttempts": 5,
    "WaitTimeDtmfSec": 5,
    "StartRecognizeAfterPromptDtmf": false
  },
  "Id": "1",
  "NextId": "2",
  "ErrorNextId": "5",
  "IsFirst": true
},
}
```

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.

- 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, these 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.

- To enable TTS copy over and if required modify state machine(s) from the folder ending with tts in ...\\Program Files\\AudioCodes\\SmartTAP 360° Live\\AN\\Repo to the Program Files\\AudioCodes\\SmartTAP 360° Live\\AN\\StateMachineConfig folder.

Consent to Record Calls

SmartTAP 360° Live 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:

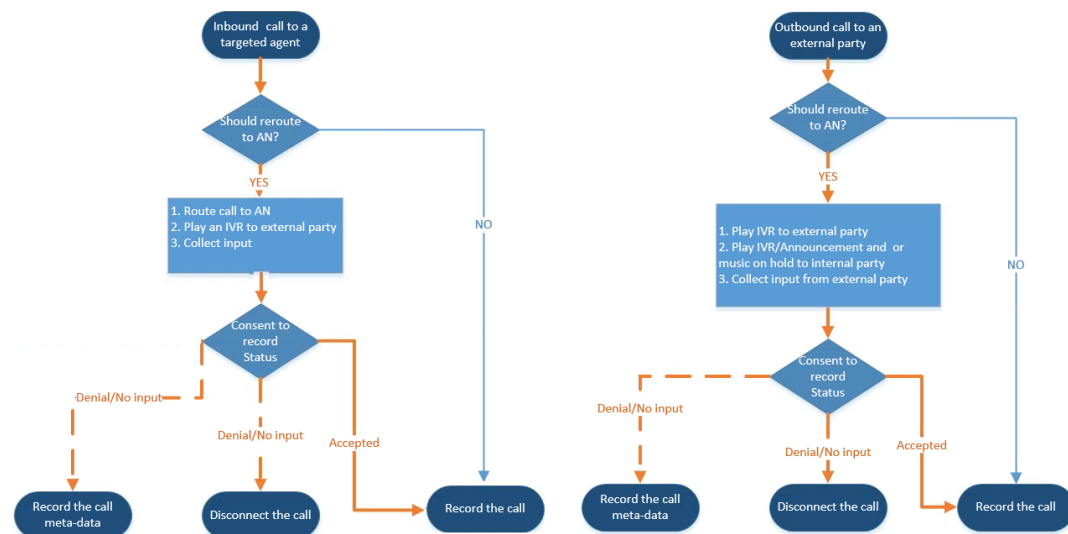
"This call may be recorded for quality assurance purposes. Press one to accept or press zero to continue without recording."



The Demo IVR files provided by SmartTAP 360° Live, 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	Release Cause
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	Release Cause
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

System Users Status

Calls Evaluation

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

Search

Example Announcement Server Scenarios

This section describes the following example scenarios for assigning Media files and IVR script files for the Announcement 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 type
Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ All
☐ Internal
☐ Incoming
☐ Outgoing
☒ PSTN
☒ Inbound
☒ Outbound
☒ Federated
☒ Inbound
☒ Outbound
☒ Calls with Internal Conferences
☐ Teams Queue Calls (conference mode) *
* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☒ Referred by Response Group

Filter Calls User Receives : List Type : **Block** Numbers: Regular Expression:

Filter Calls User Makes : List Type : **Block** Numbers: Regular Expression:

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

Call type

Internal	<input type="checkbox"/> Incoming	ANN	<input type="checkbox"/> Play to calling party	<input type="text"/> File name	<input type="checkbox"/> Play to answering party	<input type="text"/> File name
	<input type="checkbox"/> Outgoing	ANN	<input type="checkbox"/> Play to calling party	<input type="text"/> File name	<input type="checkbox"/> Play to answering party	<input type="text"/> File name
PSTN	<input checked="" type="checkbox"/> Inbound	IVR	<input checked="" type="checkbox"/> Play to calling party	PSTN_Inbound_IVR	<input type="checkbox"/> Play to answering party	<input type="text"/> File name
	<input checked="" type="checkbox"/> Outbound	ANN	<input type="checkbox"/> Play to calling party	<input type="text"/> File name	<input checked="" type="checkbox"/> Play to answering party	PSTN_Outbound.wmf
Federated	<input checked="" type="checkbox"/> Inbound	IVR	<input checked="" type="checkbox"/> Play to calling party	Fed_Inbound_IVR.json	<input type="checkbox"/> Play to answering party	<input type="text"/> File name
	<input checked="" type="checkbox"/> Outbound	ANN	<input type="checkbox"/> Play to calling party	<input type="text"/> File name	<input checked="" type="checkbox"/> Play to answering party	Federated_Outbound.w

☐ Record Announcement

Don't Play Announcement Destination Numbers : 911

☐ Block Calls on Announcements Unavailability

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 MSFT Teams, Skype for Business and Lync A/V Recording

☐ All

Internal ☒ Incoming ☐ Outgoing

PSTN ☒ Inbound ☐ Outbound

Federated ☒ Inbound ☐ Outbound

☒ Calls with Internal Conferences

☐ Teams Queue Calls (conference mode) *

* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☒ Referred by Response Group

Filter Calls User Receives : List Type: **Block** ▼ Numbers: Regular Expression:

Filter Calls User Makes : List Type: **Block** ▼ 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 **PSTN_IVR_Outbound** File name

☐ Outbound **ANN** ▼ ☐ Play to calling party File name ☒ Play to answering party File name

Federated ☒ Inbound **IVR** ▼ ☒ 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 Unavailability

Announcement 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 theApplication User agent. The default value is " AnnouncementsApp".
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 "".

Parameter	Description
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: <ul style="list-style-type: none"> ■ \${longdate} \${level} \${message} ■ \${exception:format=Message}\${newline}
referredByAddedParamName	This parameter name is added to the SIP 'Referred-By' header. The default value is " X-Announcements".

Parameter	Description
referredByAddedParamValue	This parameter value is added to the SIP 'Referred-By' header. The default value is "AnnouncementsApp".
transferType	Defines the Transfer Type. Valid Values: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ True (default) ■ False
mohFileName	Defines the Music on Hold file name. The file must be located in the project directory tree inside theMusicOnHold 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: <ul style="list-style-type: none"> ■ True ■ False (default)
uaReceiveReferRegex	If UserAgent matches the regular expression then 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.

Parameter	Description
	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
restClientTimeoutMilliseconds	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: <input type="checkbox"/> True <input checked="" type="checkbox"/> False (default)
managedDeviceHeartbeatInterval Ms	Interval in milliseconds between each heartbeat request to AS. Valid range [1000 - max int] Default Value: 30000
disableAlarms	Disables the alarms mechanism. Possible values: <input type="checkbox"/> True (disable) <input checked="" type="checkbox"/> 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"
noAttendedTransferSupportRegex	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

Parameter	Description
	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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ True ■ False (default)

For AN Server installation instructions, refer to the *SmartTAP 360° Live Installation Guide*.

Announcement 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 Announcement Server*
Supervised/blind transfer	A	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	B + C	<ol style="list-style-type: none"> 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 is played (set

Call Scenario	Targeted Users	Flow and expected results from Announcement Server*
		AllowMultipleAnnSameUser to true to play)
Supervised transfer	A + B + C	<ol style="list-style-type: none"> 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)

*The second line is not applicable for each of the above scenarios in case of Blind Transfer

■ 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° Live 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 300

Azure Active Directory User Mapping

SmartTAP 360° Live Version 5.1 and later allows mapping of an Organizations' (Tenant) users from Microsoft Azure Active Directory (AAD). SmartTAP 360° Live 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° Live (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 265)
- **Step 3:** Configure Certificates & Secrets for this app in AAD (see [Step 3 Configure Certificates & Secrets](#) on page 308)
- **Step 4:** Configure this client application in SmartTAP 360° Live (see [Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on page 270)
- **Step 5:** Add new User Mappings in SmartTAP 360° Live (see [Step 5 Add Azure Active Directory Mapping in SmartTAP 360° Live](#) on page 271)

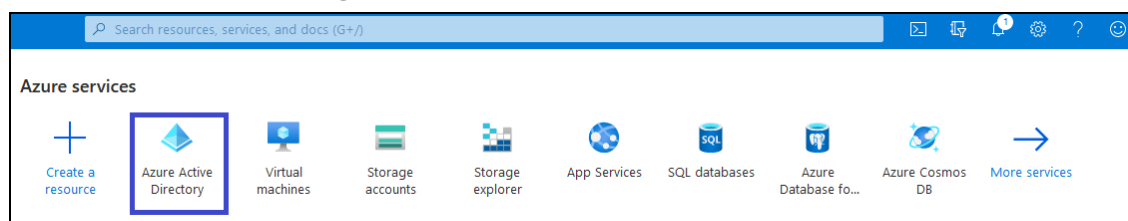
Step 1 Application Registration in Microsoft Azure

This step describes how to register an Application in Microsoft Azure.

➤ Do the following:

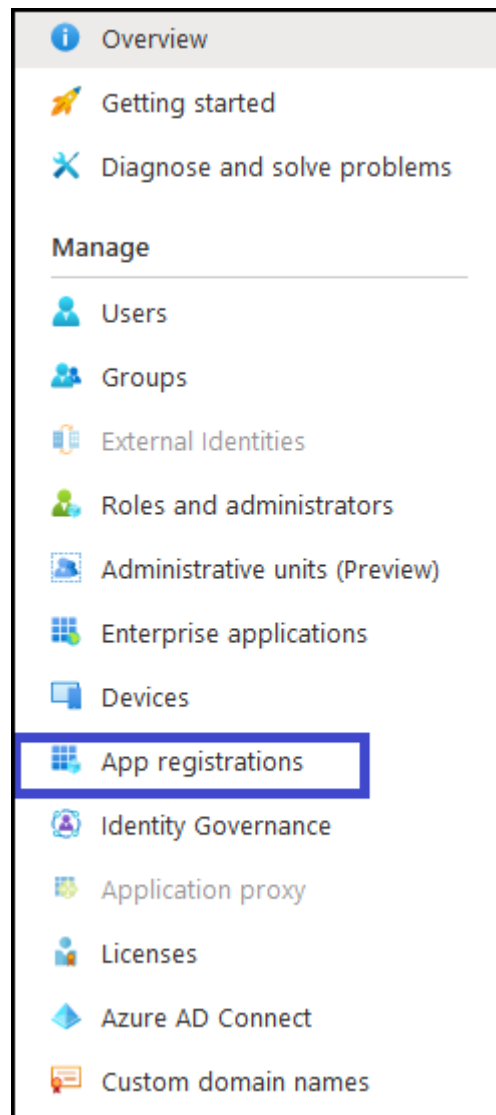
1. Login to the Microsoft Azure portal (<https://portal.azure.com/>).

Figure 13-1: Azure Services



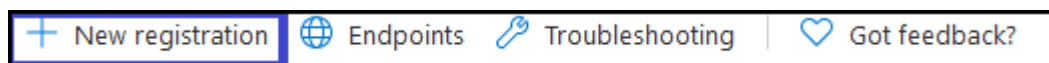
2. Click **Azure Active Directory**.

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](#)

Register

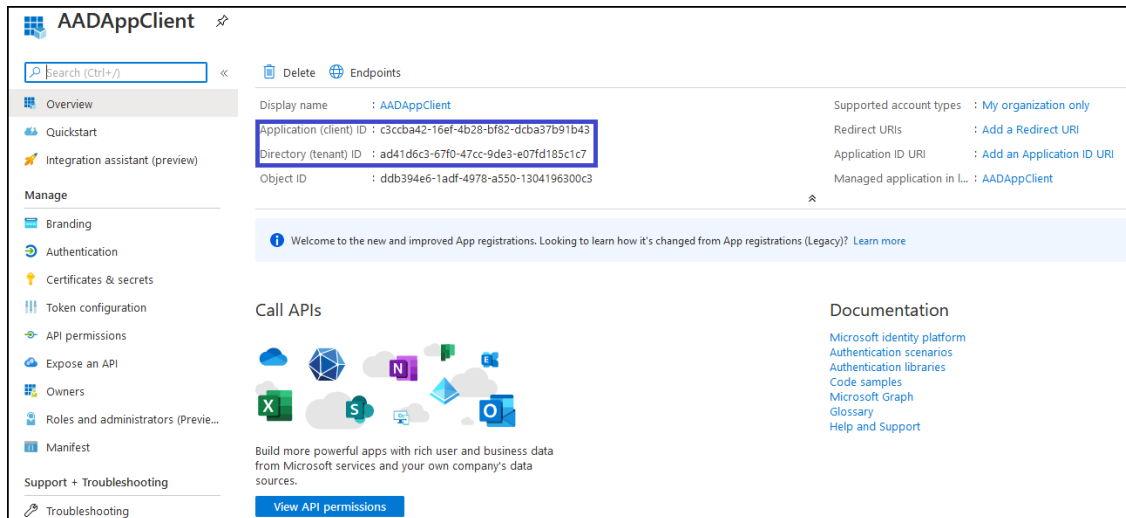
5. Enter the following details:

- 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



7. Copy the value of Application (client) ID and Directory (tenant) ID for Client Configuration in SmartTAP 360° Live ([Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on page 270).

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

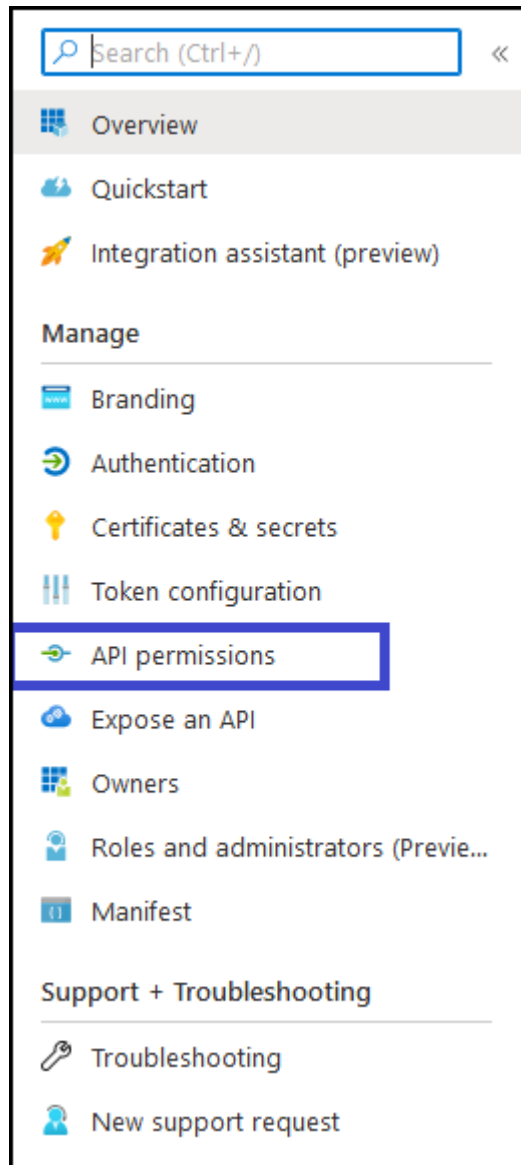
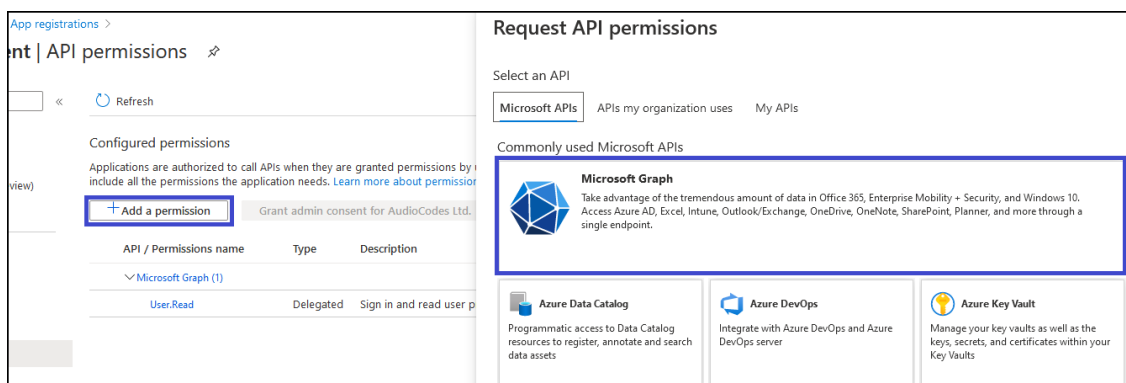
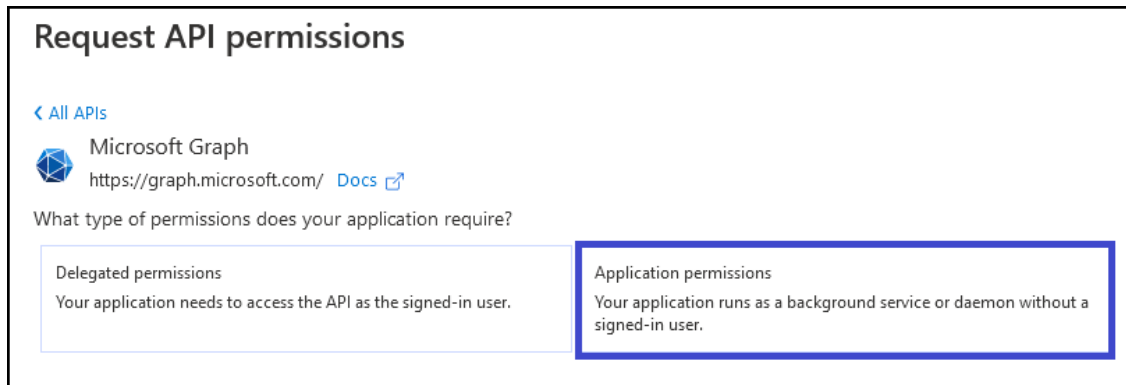


Figure 13-7: Add a Permission




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?

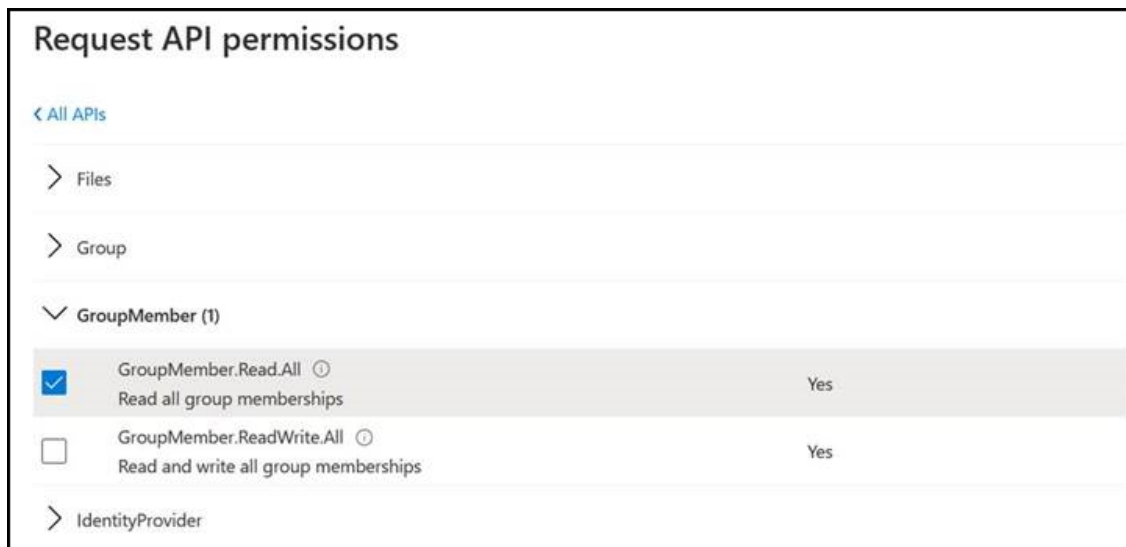
Delegated permissions

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 Permissions



Request API permissions

[← All APIs](#)

> Files

> Group

▼ GroupMember (1)

<input checked="" type="checkbox"/>	GroupMember.Read.All ⓘ Read all group memberships	Yes
<input type="checkbox"/>	GroupMember.ReadWrite.All ⓘ Read and write all group memberships	Yes

> IdentityProvider

4. Under "Select permissions" list, check the following permissions:
 - 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 13-10: Configured Permissions

Refresh | Got feedback?

Warning: 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 myorganization

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (3)				
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for myorga...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for myorga...

To view and manage permissions and user consent, try [Enterprise applications](#).

6. Once Admin Consent is granted, the permissions are displayed as follows:

Figure 13-11: Configured Permissions

Refresh | Got feedback?

Success: Successfully granted admin consent for the requested permissions.

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 myorganization

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (3)				
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for myorganiza...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for myorganiza...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for myorganiza...

To view and manage permissions and user consent, try [Enterprise applications](#).

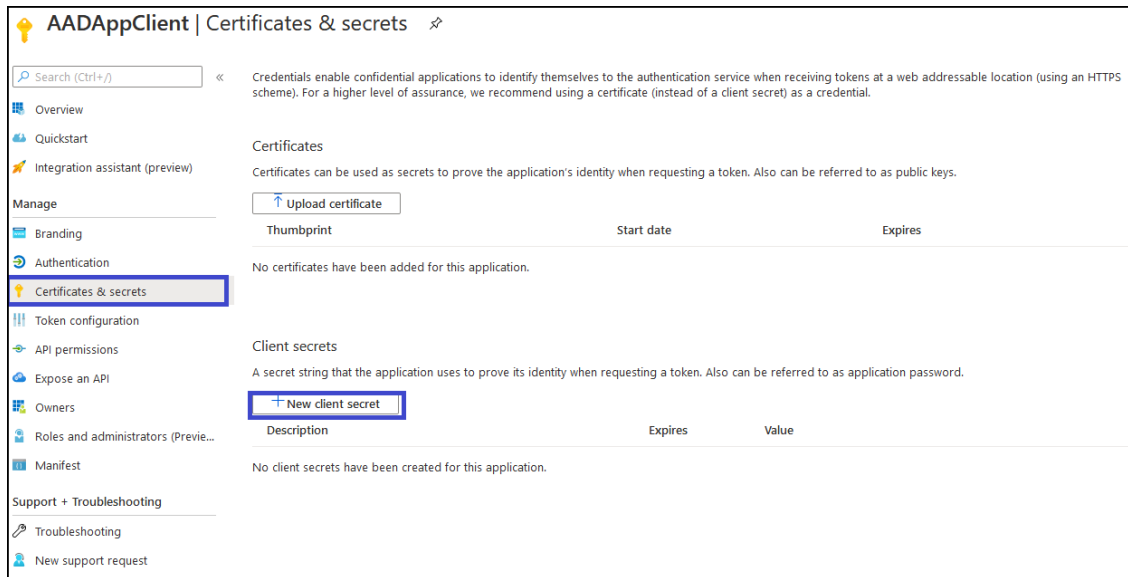
Step 3 Configure Certificates & Secrets for Azure AD Mapping

This section describes how to configure certificates and secrets for Azure AD mapping.

➤ **Do the following:**

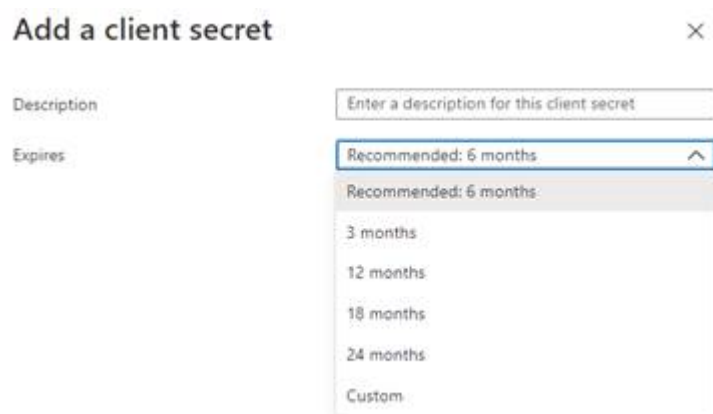
1. In the Navigation pane, select **Manage > Certificates & secrets**.

Figure 13-12: Certificates and Secrets



2. Click **+ New client secret**.

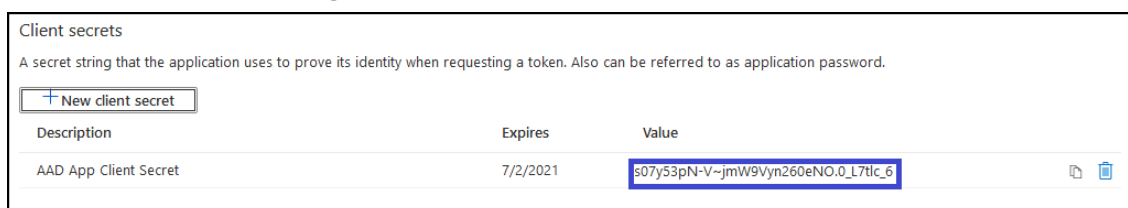
Figure 13-13: Add a Client Secret



The New Client Secret must be generated before the expiration time and set in SmartTAP to avoid possible issues that may arise with the recording service. Note the new client secret as it must be later configured.

A client secret is generated and displayed as below.

Figure 13-14: New Client Secret



3. Copy the Value of the client secret for further configuration in SmartTAP 360° Live (see [Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on the next page).

Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live

To configure the client application in SmartTAP 360° Live, 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° Live Web with Administrator role.
2. Open the Add AAD Configuration screen (**System > AAD > Add AAD Configuration**).

Figure 13-15: AAD Tab

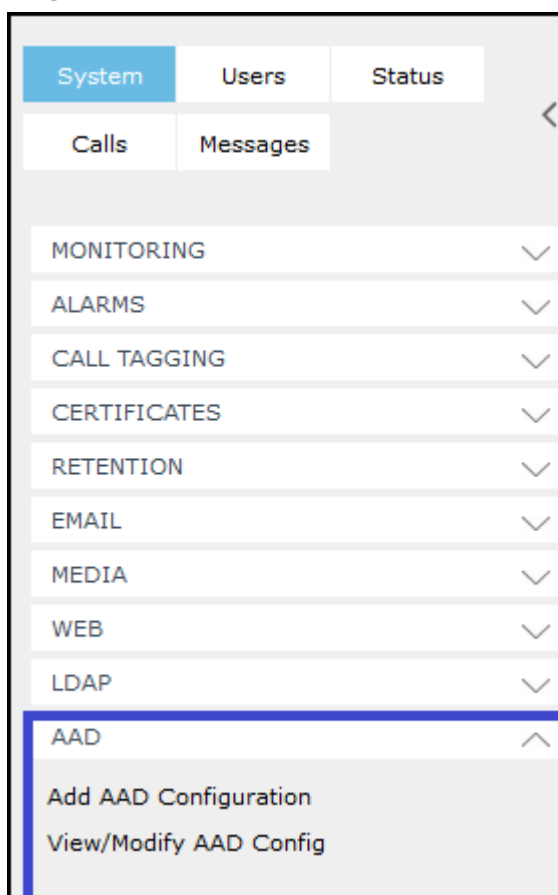



Figure 13-16: Add Active Directory Configuration

• 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-dcb37b91
Client Secret	

3. Enter the name of the Active Directory configuration.
4. Enter the Directory (Tenant) ID and the Application (Client) ID.
5. Enter the Client Secret.
6. Click . 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° Live

This section describes how to map Azure Active Directory objects to SmartTAP entities:

- Define AAD User Mapping Profile and map to one or more member groups. All users belonging to the mapped groups inherit the mapped profile (see [AAD User and Group Mapping](#) below). Once the AAD group is mapped, it is added to the SmartTAP Groups table.
- Define AAD Security Mapping Profile and map to one or more member groups. All users belonging to the mapped groups inherit the mapping profile (see [AAD Security Profile Mapping](#) on page 277). Once the AAD Security Profile is mapped, it is added to the SmartTAP Security Profiles table.
- Define AAD Recording Mapping Profile and map to one or more member groups. All users belonging to the mapped groups inherit the mapping profile (see [AAD Recording Profile Mapping](#) on page 284). Once the Recording Profile is mapped, it is added to the SmartTAP Recording Profiles table.
- Define AAD Retention Mapping Profile and map to one or more member groups. All users belonging to the mapped groups inherit the mapped profile (see [AAD Retention Profile Mapping](#)). Once the Retention Profile is mapped, it is added to the SmartTAP Retention Policies table (see [AAD Retention Policy Mapping](#) on page 293).



- The AAD data that is retrieved from Azure i.e. member, name and description cannot be modified in SmartTAP, only directly from Azure.
- If you remove a group from any mapping, then the corresponding entity is also removed from the SmartTAP database i.e. the mapping configuration is deleted.
- If you delete a group in Azure, the mapping and configuration are not removed from the SmartTAP database.

AAD User and Group Mapping

SmartTAP 360° Live allows mapping of AAD user from one or more member groups. Each group and its 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° Live custom user attributes. In this step, you must assign the custom user attribute that was defined in [Adding a Microsoft Teams AAD User Attribute](#) on page 136 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. Once the Users and Groups have been added, they can be viewed in the

View/Modify Users page (Users > User Management > View/Modify Users) and View/Modify Groups page (Users > Group Management > View/Modify Groups).



- Changing the group in Azure i.e. member, name and description will automatically be updated to SmartTAP.
- AudioCodes Azure Active Directory Groups cannot be edited or removed in SmartTAP, only directly from Azure.

➤ **Do the following:**

1. Ensure that you mapped the user attribute Object_ID for the Microsoft Teams user (see [Adding a Microsoft Teams AAD User Attribute](#) on page 136).
2. Open the Add AAD Config page (**System tab** > **AAD folder** > **Add AAD Config**).

Figure 13-17: Add Active Directory Configuration

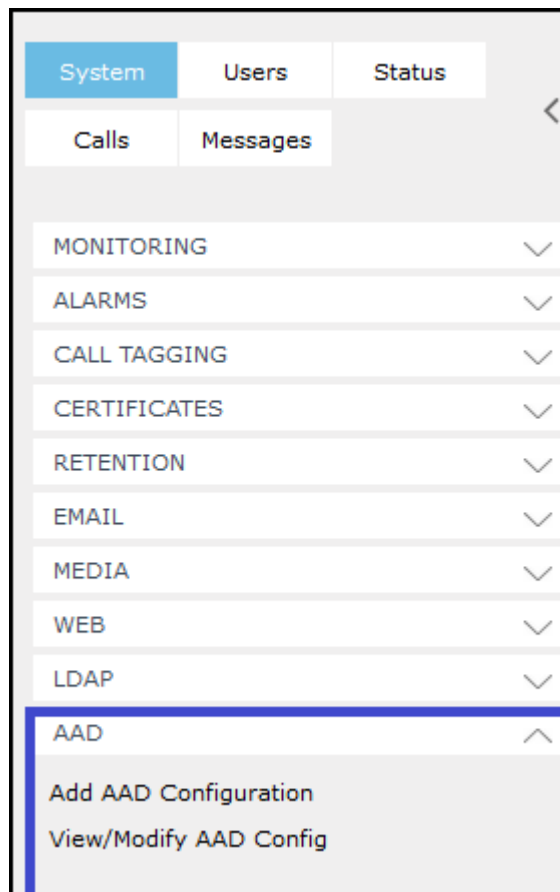


Figure 13-18: Active Directory Providers

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° Live](#) on page 270 and then click .

Figure 13-19: Modify Active Directory Configuration

Modify Active Directory Configuration

Name: OmarAAD_mapping

Directory (Tenant) ID: ad41d6c3-67f0-47cc-9de3-e07fd185c

Application (Client) ID: 00c65e7a-2064-443f-bb24-0de67025

Client Secret:

USER MAPPINGS

Mapping Name: omarAAD

Member Groups: ST_Test_Group, 2E5_users Select Groups

First Name: givenName

Last Name: surname

Login: userPrincipalName

Email: mail

Alias: surname

OID: id

☐ One Level ☒ Subtree

☒ Add Groups

CANCEL SUBMIT

	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
	omarAAD	ST_Test_Group, 2E5_users	SUB_TREE		

Security Profile Mappings

Recording Profile Mappings

Retention Mappings

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 required.
 - 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 'OID' (this may be any user-defined string).



The OID attribute is mandatory for Microsoft Teams calls, however different user mapping IDs can be used for other integrations.

5. Select one of the following:

5. Select the One Level to map the users from to the highest Active Directory object level. Select Subtree to map the users from to all of the subtree objects in the Active Directory

- **One Level:** SmartTAP maps the user to the highest Active Directory object level (root group)
 - **Subtree:** SmartTAP maps only the root group and assigns to it, the users from the root group and subgroups.
6. To map member groups to which users are mapped, select **Add Groups**. If the Subtree option is selected above, then all groups belonging to the Subtree are also mapped.
7. Click SUBMIT.

Figure 13-20: Select Member Groups

Select Member Groups

Searched Groups

Selected Groups

- ☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☐ SmartTapAgents [070ecda5-dbd2-4ef4-9c67-9b64e881422f]

CANCEL SUBMIT

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 13-21: Select Member Groups

Select Member Groups

Searched Groups

- ☐ 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".


8. Click  to add this mapping to SmartTAP 360° Live.

Figure 13-22: Member Groups

Successful user mapping is displayed under the User Mapping table.

Figure 13-23: Mapping Successfully Added








All mapped users are displayed in the **Users > View/Modify Users** page (see [View and Modify Users](#) on page 140).

Figure 13-24: 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		3b477f78-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		

When the "Add Groups" check box is selected, Mapped Groups can be viewed in the Groups page (see [View and Modify Groups](#) on page 112).

Figure 13-25: Mapped Groups

View/Modify Groups			
Name	Description	Modify	Delete
Default	Default group		
rachels			
rachels test video			
rachelsTest	testingAAD		
racheltest3			
test4			

AAD Security Profile Mapping

This section describes how to map AAD Security profiles. The profile should be mapped to one or more of the member groups that you mapped in [AAD User and Group Mapping](#) on page 271 and therefore users assigned to these groups are associated with the new Security profile.





A user can be assigned to multiple Security profiles in which case permissions from all profiles are added.

➤ To map AAD Security profiles:

1. Open the View/Modify AAD Config page (**System tab** > **AAD folder** > **Add AAD Config**).

Figure 13-26: Active Directory Providers Page

Active Directory Providers				
Name	Organization (Tenant) Id	Application (Client) Id	Modify	Delete
OmarAAD_mapping	ad41d6c3-67f0-47cc-9de3-e07fd185c1c7	00c65e7a-2064-443f-bb24-0de67025bd72		


2. Select the provider entry that you configured in [Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on page 270 and then click .

Figure 13-27: Modify Active Directory Configuration

Modify Active Directory Configuration

Name

OmarAAD_mapping

Directory (Tenant) ID

ad41d6c3-67f0-47cc-9de3-e07fd185c

Application (Client) ID

00c65e7a-2064-443f-bb24-0de67025

Client Secret

SUBMIT

User Mappings

Mapping Name

omarAAD

Member Groups

ST_Test_Group, 2E5_users

Select Groups

First Name

givenName

Last Name

surname

Login

userPrincipalName

Email

mail

Alias

surname

OID

id

☐ One Level ☒ Subtree

☒ Add Groups

CANCEL SUBMIT

	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
	omarAAD	ST_Test_Group, 2E5_users	SUB_TREE		

Security Profile Mappings

Recording Profile Mappings

Retention Mappings

3. Select the **Security Profile Mapping** tab.

Figure 13-28: Active Directory Security Profile Mapping

Add Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID

Client Secret

User Mappings

Security Profile Mappings

Mapping Name

Member Groups

☒ One Level ☐ Subtree

Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
No records found.				

Recording Profile Mappings

Retention Mappings

4. In the Mapping Name field, enter a name for the Security Profile.
5. Select one of the following:
 - **One Level:** SmartTAP maps the user to the highest Active Directory object level (root group)
 - **Subtree:** SmartTAP maps only the root group and assigns to it, the users from the root group and subgroups.
6. Click the **Select Groups** button to browse to the relevant group.

Figure 13-29: Select Group

Select Member Groups

Searched Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☒ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☒ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☒ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]

Selected Groups

Use the arrow buttons to assign the relevant groups.

Figure 13-30: Select Member Groups

Select Member Groups

Searched Groups

- ☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
- ☐ STloadUsers [380fac00-b5ed-41ae-b180-a3421fd701f9]
- ☐ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]
- ☐ st-subgroup1-test-rename [14a05d00-7b09-4121-a9f4-b4d2f26b79b3]
- ☐ st-subgroup2-test [8-042-1f-0000-474d-0000-0000-000000000000]

Selected Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☐ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☐ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☐ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]



The maximum number of search results is limited to "10".



- 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.

Figure 13-31: Remove Member Group Assignment

Select Member Groups

Searched Groups

st

☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]

☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]

☐ STloadUsers [380fac00-b5ed-41ae-b180-a3421fd701f9]

☐ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]

☐ st-subgroup1-test-group [14e05d00-7b00-4131-b6f4-54d3f0c570b3]

▼

▲

Selected Groups

☒ ST-Teams-Users [9e870e1f-0c70-48d7-98da-18688886c024e]

☐ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]

☐ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]

CANCEL

SUBMIT

7. Click **SUBMIT** to apply changes.

Figure 13-32: Assigned Member Group

Modify Active Directory Configuration

Name

OmarAAD_mapping

Directory (Tenant) ID

ad41d6c3-67f0-47cc-9de3-e07fd185c1

Application (Client) ID

00c65e7a-2064-443f-bb24-0de67025t

Client Secret

SUBMIT

User Mappings

Security Profile Mappings

Mapping Name

Member Groups

ST-Teams-Users, ST-load-test-dynamiorename, STQATeam

Select Groups


☒ One Level

☐ Subtree

	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
No records found.					

Recording Profile Mappings

Retention Mappings

8. Click  to add this mapping to SmartTAP 360° Live.

The new Security Profile is displayed:

Figure 13-33: Security Profile Successfully Added

• **Mapping successfully added.**

Modify Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID

Client Secret


User Mappings




Security Profile Mappings

Mapping Name

Member Groups

☒ One Level ☐ Subtree



	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
	SmartTAP Development Apps	ST-Teams-Users, ST-load-test-dynamic-rename, STQATeam	ONE_LEVEL		

Recording Profile Mappings

Retention Mappings



By default, the security profiles are mapped with all permissions disabled (see figure "Default Security Profile" below); to configure permissions, see [Managing Security Profiles](#) on page 113. The figure "View New Security Profile" below shows an example of a new mapping for group "ST-Teams-Users".

Figure 13-34: Default Security Profile

Modify Security Profile

Security Profile Name

Security Profile Description

Call and Instant Message Permissions

☒ No Call or Instant Message Access
 ☐ Play Media Related to a call

☐ Access all calls and instant messages
 ☐ Download Media Related to a call

☐ Access calls and instant messages within user's groups
 ☐ Email Media Related to a call

☐ Access user's own calls and instant messages
 ☐ Tag calls

☐ Live Monitor

☐ ROD/SOD other users

☐ Configure system

☐ Create and modify users and groups

Figure 13-35: View New Security Profile

View/Modify Security Profiles				
Name	Description	Permissions	Modify	Delete
supervisor	Supervisor	Tag calls Play Media Related to a call Download Media Related to a call Access calls within user's groups Live Monitor Email Media Related to a call		
ST-load-test-dynamic-rename	ST-load-test-dynamic			
administrator	Administrator	Tag calls Configure system Play Media Related to a call Create and modify users and groups Access all calls Download Media Related to a call Email Media Related to a call		
agent	Agent	Tag calls Play Media Related to a call Download Media Related to a call Access user's own calls Email Media Related to a call		
ST-Teams-Users				
STQATeam	SmartTAP QA Team			

AAD Recording Profile Mapping

This section describes how to map AAD Recording Profiles. The profile should be mapped to one or more of the member groups that you mapped in [AAD User and Group Mapping](#) on page 271 and therefore users assigned to these groups are associated with the new Recording profile.



- In the event where a user is mapped to two or more recording profiles then it will not be assigned to any profile and an alarm will be raised.
- In case the recording profile of a user is mapped to two groups (of the same kind,) then no recording profile will be mapped for the user (and an alarm will be sent). For example, user “Sharon” belongs to both group A and B on Azure, and both are mapped to the recording profile group mapping. In this case “Sharon” will not be assigned to any recording profile.
- If a user is already assigned to a local recording profile, then if an AAD profile is later assigned to the same user then this profile takes precedence.
- When an Azure Active Directory Group is mapped to a recording profile then SmartTAP attempts to automatically allocate licenses to the attached users. In the event where there are no available licenses for all of the users in the group, the additionally added users will not be allocated licenses and will not be recorded. Licenses and license allocation can be managed in the Licenses page; it's recommended to verify that licenses have been successfully allocated to the newly added users (see [Managing Licenses](#) on page 33).

➤ **To configure recording profile mapping:**

1. Open the View/Modify AAD Config page (**System tab** > **AAD folder** > **Add AAD Config**).

Figure 13-36: Active Directory Providers Page

Active Directory Providers				
Name	Organization (Tenant) Id	Application (Client) Id	Modify	Delete
OmarAAD_mapping	ad41d6c3-67f0-47cc-9de3-e07fd185c1c7	00c65e7a-2064-443f-bb24-0de67025bd72		

2. Select the provider entry that you configured in [Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on page 270 and then click .

Figure 13-37: Modify Active Directory Configuration

Modify Active Directory Configuration

Name

OmarAAD_mapping

Directory (Tenant) ID

ad41d6c3-67f0-47cc-9de3-e07fd185c

Application (Client) ID

00c65e7a-2064-443f-bb24-0de67025

Client Secret

SUBMIT

▼

User Mappings

Mapping Name

omarAAD

Member Groups

ST_Test_Group, 2E5_users

Select Groups

First Name

givenName

Last Name

surname

Login

userPrincipalName

Email

mail

Alias

surname

OID

id

☐ One Level
 ☒ Subtree

☒ Add Groups

CANCEL

SUBMIT

	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
🔍	omarAAD	ST_Test_Group, 2E5_users	SUB_TREE		

▶ Security Profile Mappings

▶ Recording Profile Mappings

▶ Retention Mappings

3. Select the **Recording Profile Mappings** tab.

Figure 13-38: Active Directory Recording Profile Mappings

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

User Mappings

Security Profile Mappings

Recording Profile Mappings

Mapping Name:

Member Groups:

☒ One Level ☐ Subtree

Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
testaudio	rachelsTest	SUB_TREE	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Retention Mappings

4. In the Mapping Name field, enter a name for the Recording Profile.
5. Select one of the following:
 - **One Level:** SmartTAP maps the user to the highest Active Directory object level (root group)
 - **Subtree:** SmartTAP maps only the root group and assigns to it, the users from the root group and subgroups.
6. Click the **Select Groups** button to browse to the relevant group.

Figure 13-39: Select Group

Select Member Groups

Searched Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☒ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☒ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☒ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]

Selected Groups

Use the arrow buttons to assign the relevant groups.

Figure 13-40: Select Member Groups

Select Member Groups

Searched Groups

- ☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
- ☐ STloadUsers [380fac00-b5ed-41ae-b180-a3421fd701f9]
- ☐ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]
- ☐ st-subgroup1-test-rename [14a05d00-7b09-4121-a9f4-b4d2f26b79b3]
- ☐ st-subgroup2-test [8-042-16-11-2-474d-0000-025-1-554875-1]

Selected Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☐ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☐ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☐ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]



The maximum number of search results is limited to "10".



- 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.

Figure 13-41: Remove Member Group Assignment

Select Member Groups

Searched Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
- ☐ STloadUsers [380fac00-b5ed-41ae-b180-a3421fd701f9]
- ☐ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]
- ☐ st-subsystem-test-group [14-05d00-7500-4131-0541-54d5f3c57053]

Selected Groups

- ☒ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☐ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☐ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]

CANCEL **SUBMIT**

7. Click **SUBMIT** to apply changes.

Figure 13-42: Assigned Member Group

Modify Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID

Client Secret

SUBMIT

▶ User Mappings

▶ Security Profile Mappings

▼ Recording Profile Mappings


Mapping Name

Member Groups **Select Groups**

☒ One Level ☐ Subtree

Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
No records found.				

▶ Retention Mappings

8. Click  to add this mapping to SmartTAP 360° Live.

The new Recording Profile is displayed:

Figure 13-43: New Recording Profile

• Mapping successfully added.

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

▶ User Mappings


▶ Security Profile Mappings













▼ Recording Profile Mappings

Mapping Name:

Member Groups:

☒ One Level ☐ Subtree



	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
1	Test Recordings	ST, ST-Teams-Users, ST-load-test-dynamic-rename	ONE_LEVEL		
1	test video	test4	SUB_TREE		
1	testaudio	rachelsTest	SUB_TREE		
1	bbb	racheltest3	ONE_LEVEL		
1	Emergency Response Center	ST-Teams-Users, ST-load-test-dynamic-rename, STQATeam	ONE_LEVEL		
1	Call Center Recordings	ST-Teams-Users, ST-load-test-dynamic-rename, STQATeam	ONE_LEVEL		



By default, the newly created recording profiles are mapped with all options disabled as shown in figure "Default Recording Profile" below; to configure the profile see [Viewing or Modifying Recording Profiles](#) on page 125. The figure "View New Recording Profile" shows an example mapping for "ST-Teams-Users" group.

Figure 13-44: Default Recording Profile

Call

Recording Type: **None**

☐ Video
☐ Desktop Sharing
☐ Pause or Resume

Call type

Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ All

Internal

☐ Incoming
☐ Outgoing

PSTN

☐ Inbound
☐ Outbound

Federated

☐ Inbound
☐ Outbound

☐ Calls with Internal Conferences
☐ Teams Queue Calls (conference mode) *
* Applicable for MSFT Teams only

Applicable for Skype for Business and Lync A/V Recording

☐ Referred by Response Group

Filter Calls User Receives : List Type: **Allow** Numbers: Regular Expression:

Filter Calls User Makes : List Type: **Allow** 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
☐ Outgoing **ANN** ☐ Play to answering party File name

PSTN

☐ Inbound **ANN** ☐ Play to calling party File name
☐ Outbound **ANN** ☐ Play to answering party File name

Federated

☐ Inbound **ANN** ☐ Play to calling party File name
☐ Outbound **ANN** ☐ Play to answering party File name

☐ Record Announcement
Don't Play Announcement Destination Numbers : **911**
☐ Block Calls on Announcements Unavailability

Recording Beep Tone

Applicable for Skype for Business and Lync A/V Recording. Beep can be played on the calls which media traverses Media Proxy Server

☐ Play Beep Tone

Instant Messaging

Applicable for MSFT Teams, Skype for Business and Lync A/V Recording

☐ Record Instant Messages

Figure 13-45: View New Recording Profile

View/Modify Recording Profiles						
Name	Description	Call Recording Type	Video Recording	IM Recording Type	Desktop Sharing Recording	Modify
ST	ST	NONE	Disabled	NONE	Disabled	
test4	test4	NONE	Disabled	NONE	Disabled	
ST-load-test-dynamic-rename	ST-load-test-dynamic-rename	NONE	Disabled	NONE	Disabled	
ST-load-test-dynamic-rename	ST-load-test-dynamic-rename	NONE	Disabled	NONE	Disabled	
Audio	Audio , save on demand , P/R	SAVE_ON_DEMAND	Disabled	NONE	Disabled	
Omar SIPREC		FULL_TIME	Disabled	NONE	Disabled	
Video+DAS+IM		FULL_TIME	Enabled	NONE	Enabled	
Omar AVD Record on demand		SAVE_ON_DEMAND	Enabled	NONE	Enabled	
rachelsTest	rachelsTest	NONE	Disabled	NONE	Disabled	
ST-Teams-Users	ST-Teams-Users	NONE	Disabled	NONE	Disabled	
Omar Save on demand	Saves the entire call	SAVE_ON_DEMAND	Enabled	NONE	Enabled	
racheltest3	racheltest3	NONE	Disabled	NONE	Disabled	
ST-Teams-Users	ST-Teams-Users	NONE	Disabled	NONE	Disabled	
Omar FULL Notification	Disable NOT	FULL_TIME	Disabled	NONE	Disabled	
STQATeam	STQATeam	NONE	Disabled	NONE	Disabled	
Full Time	Full Time recording profile	FULL_TIME	Disabled	NONE	Disabled	

AAD Retention Policy Mapping

This section describes how to map AAD Retention Mappings profile. The policy should be mapped to one or more of the member groups that you mapped in [AAD User and Group Mapping](#) on page 271 and therefore users assigned to these groups are associated with the new Retention policy.





- In case the retention policy of a user is mapped in two or more groups (of the same kind) then no retention policies will be mapped for the user (and an alarm will be sent). For example, user “Bill” belongs to both group A and B on Azure, and both are mapped to the same retention policy . In this case “Sharon” will not be assigned to any retention policy.
- If a user is already assigned to a local Retention Policy , then if an AAD policy is later assigned to the same user then this policy takes precedence.
- If while removing a retention group there are calls that connected to this retention policy, then the mapping will be removed however the retention policy stays local and stays attached to the calls. Example: group A on Azure is mapped to a retention policy and then after some time there are some calls that are assigned to this policy. If the user is unmapped the group then the group will be removed from the mapping, however the retention policy will still remain in the local DB including the assigned calls, however without a user assigned.

➤ To configure retention policy mapping:

1. Open the View/Modify AAD Config page (**System tab** > **AAD folder** > **Add AAD Config**).

Figure 13-46: Active Directory Providers Page

Active Directory Providers				
Name	Organization (Tenant) Id	Application (Client) Id	Modify	Delete
OmarAAD_mapping	ad41d6c3-67f0-47cc-9de3-e07fd185c1c7	00c65e7a-2064-443f-bb24-0de67025bd72		


2. Select the provider entry that you configured in [Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on page 270 and then click .

Figure 13-47: Modify Active Directory Configuration

Modify Active Directory Configuration

Name

OmarAAD_mapping

Directory (Tenant) ID

ad41d6c3-67f0-47cc-9de3-e07fd185c

Application (Client) ID

00c65e7a-2064-443f-bb24-0de67025

Client Secret

SUBMIT

▼

User Mappings

Mapping Name

omarAAD

Member Groups

ST_Test_Group, 2E5_users

Select Groups

First Name

givenName

Last Name

surname

Login

userPrincipalName

Email

mail

Alias

surname

OID

id


☐ One Level

☒ Subtree

☒ Add Groups

CANCEL

SUBMIT

	Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
🔍	omarAAD	ST_Test_Group, 2E5_users	SUB_TREE		

▶ Security Profile Mappings

▶ Recording Profile Mappings

▶ Retention Mappings

3. Select the **Retention Mappings** tab.

Figure 13-48: Retention Mappings

Add Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID

Client Secret

▸ User Mappings

▸ Security Profile Mappings

▸ Recording Profile Mappings

▾ Retention Mappings

Mapping Name

Member Groups

☒ One Level ☐ Subtree

Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
No records found.				

4. In the Mapping Name field, enter a name for the Retention Mappings Profile.
5. Select one of the following:
 - **One Level:** SmartTAP maps the user to the highest Active Directory object level (root group)
 - **Subtree:** SmartTAP maps only the root group and assigns to it, the users from the root group and subgroups.
6. Click the **Select Groups** button to browse to the relevant group.

Figure 13-49: Select Member Groups

Select Member Groups

Searched Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☒ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☒ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☒ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]

Selected Groups

7. Use the arrow buttons to assign the relevant groups.

Figure 13-50: Select Member Groups

Select Member Groups

Searched Groups

- ☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
- ☐ STloadUsers [380fac00-b5ed-41ae-b180-a3421fd701f9]
- ☐ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]
- ☐ st-subgroup1-test-rename [14a05d00-7b09-4121-a9f4-b4d2f26b79b3]
- ☐ st-subgroup2-test [8-042-1f-0c70-48d7-98da-1868886c024e]

▼ ▲

Selected Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☐ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☐ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☐ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]



The maximum number of search results is limited to "10".

- 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.

Figure 13-51: Remove Member Group Assignment

Select Member Groups

Searched Groups

- ☐ ST [104b2b0c-d1a7-46b2-a6ca-958b17b6b133]
- ☐ ST_Test_Group [845e4dd8-78aa-49cd-bd44-fbeb622ce809]
- ☐ STloadUsers [380fac00-b5ed-41ae-b180-a3421fd701f9]
- ☐ st-compliance-michal [cbc58572-7d1f-409f-bc7d-525a9718e299]
- ☐ st-subsequent-test-group [14-05f00-7500-4131-05f1-54d5f0c57053]

Selected Groups

- ☒ ST-Teams-Users [9e870e1f-0c70-48d7-98da-1868886c024e]
- ☐ ST-load-test-dynamic-rename [5e7ce8d2-412a-4886-80f3-49314e2beb60]
- ☐ STQATeam [29f34319-2230-4871-9020-d683d8a1ef2a]

CANCEL **SUBMIT**

8. Click **SUBMIT** to apply changes.

Figure 13-52: Assigned Member Groups

Modify Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID

Client Secret

SUBMIT


▶ User Mappings
 ▶ Security Profile Mappings
 ▶ Recording Profile Mappings
 ▼ Retention Mappings

Mapping Name

Member Groups **Select Groups**

☒ One Level
 ☐ Subtree

Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
No records found.				

9. Click  to add this mapping to SmartTAP 360° Live.

The new Retention Mappings Profile is displayed:

Figure 13-53: Retention Mappings Profile Successfully Added

Figure 13-54:

• Mapping successfully added.

Modify Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID


Client Secret



▶ User Mappings
 ▶ Security Profile Mappings
 ▶ Recording Profile Mappings
 ▼ Retention Mappings

Mapping Name

Member Groups

☒ One Level ☐ Subtree



Mapping Name	Member Groups	Search Scope	Modify Mapping	Delete
Central Call Center	ST, ST-Teams-Users, ST-load-test-dynamic-rename	ONE_LEVEL		

You can view the new profile in the View/Modify Retention Mappings Profiles page (see [Configuring Call Retention](#) on page 64)



By default, the newly created retention policy is set to 0 (no calls are retained) as shown in figure "Default Retention Policy"; to configure the retention policy, see [Configuring Call Retention](#) on page 64. The Figure "View New Retention Mappings Profile" below shows an example of a new mapping for ST-Teams-Users group.

The default Retention Policy is displayed in the figure below.

Figure 13-55: Default Retention Policy

Change Retention Policy Retention Policy

Retention Policy Name

Retention Policy Description

Call and Instant Message Retention Period (in days)

Figure 13-56: View New Retention Mappings Profile

View/Modify Retention Policies			
Name	Description	Days	Modify
Default	Default Retention Group	0	
STQATeam	STQATeam	0	
ST-Teams-Users	ST-Teams-Users	0	
ST-load-test-dynamic-rename	ST-load-test-dynamic-rename	0	
<div> <div>20</div> <div>< ></div> <div>1</div> <div>> ></div> </div> <div>(1 of 1)</div>			

Azure Active Directory User Authentication

For SmartTAP 360° Live version 5.1 and later users are mapped from Organizations' (Tenant) Azure Active Directory (AAD) and authenticate (login) with SmartTAP 360° Live Web using their Microsoft login credentials. SmartTAP 360° Live 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:

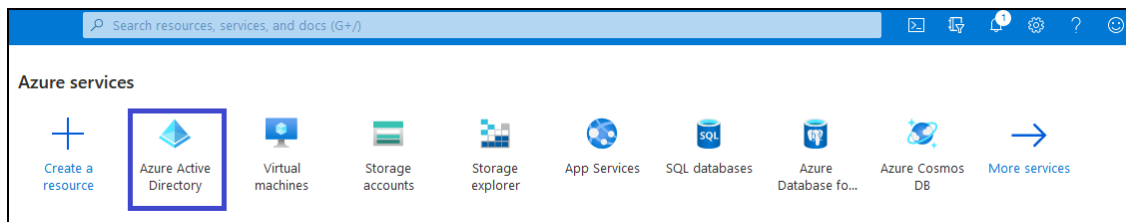
- **Step 1:** Register an web application (client) in Azure Active Directory on behalf of SmartTAP 360° Live (see [Step 1 Register App in Azure Active Directory](#) below).
- **Step 2:** Check the API permission for this app in AAD (see [Step 2 Check API Permissions](#) on page 303)
- **Step 3:** Configure Certificates & Secrets for this application in AAD (see [Step 3 Configure Certificates & Secrets](#) on page 308)
- **Step 4:** Configure this client in SmartTAP 360° Live Web as OpenID Connect (OIDC) authentication client, also known as Relying Party (see [Step 4 Configure OpenID Connect OIDC Client](#) on page 309).
- **Step 5:** Assign Security Profile to Azure Active Directory user in SmartTAP 360° Live (see [Step 5 Assign Security Profile to Azure Active Directory user in SmartTAP 360° Live](#) on page 311)

Step 1 Register App in Azure Active Directory

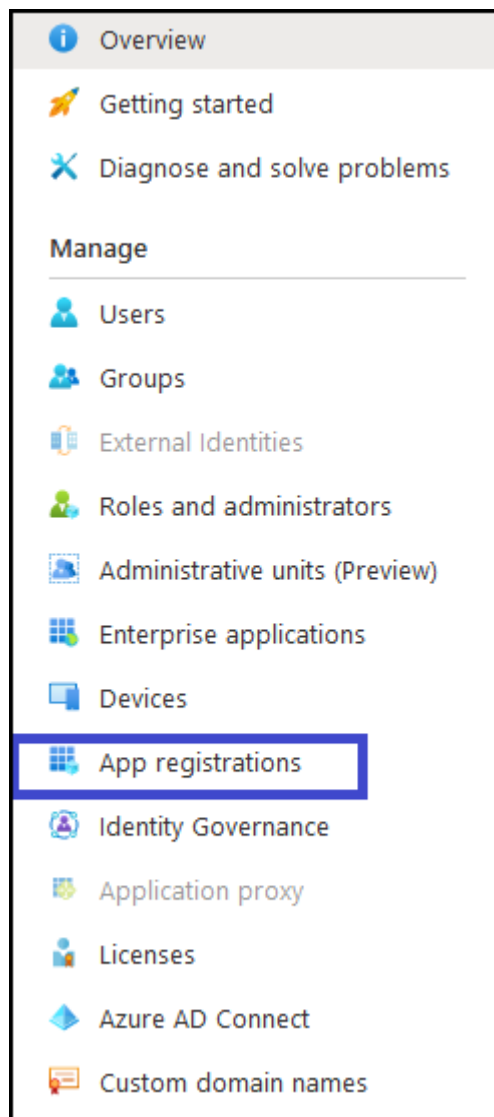
This step describes how to register the App in Azure Active Directory.

➤ To register app in ADD:

1. Login to Azure portal (<https://portal.azure.com/>)
2. Access Azure Active Directory Service.

Figure 13-57: Azure Services

3. In the Navigation pane, click "App Registration" link.

Figure 13-58: App Registrations

4. On Right side panel client "New Registration".

Figure 13-59: New Registrations

Figure 13-60: 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](#)

Register

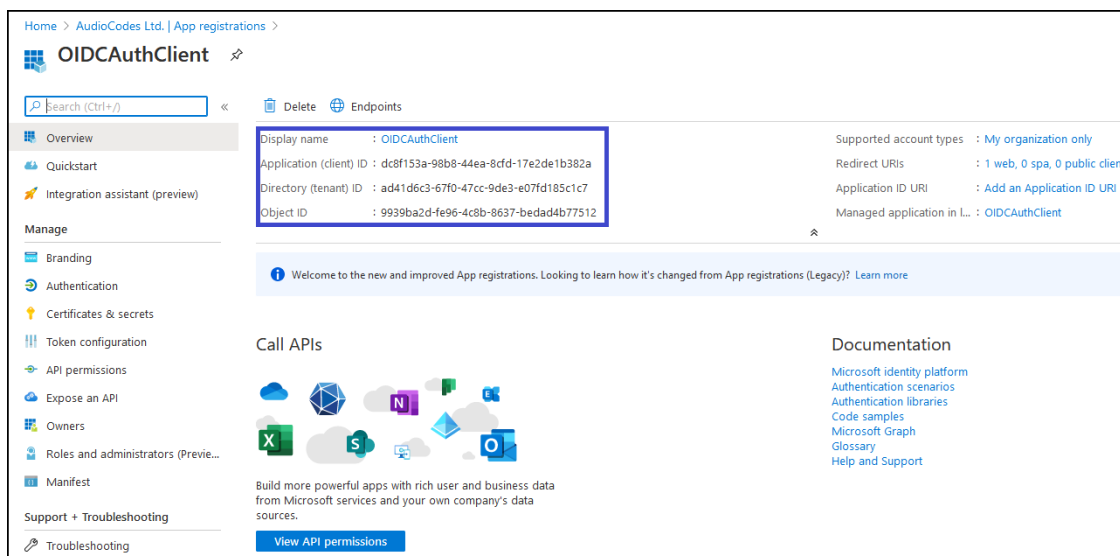
5. Enter the following details:

- 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° Live enter http://<SmartTAP FQDN>/SmartTAP/status/target_status.jsf
 - ◆ If HTTPS is configured in SmartTAP 360° Live enter https://<SmartTAP FQDN>/SmartTAP 360° Live/status/target_status.jsf

6. Click **Register** to confirm registration.

On successful registration the following details will be displayed.

Figure 13-61: OIDCAuthClient



7. Copy the value of Application (client) ID and Directory (tenant) ID for later configuration in the SmartTAP 360° Live Web (see [Step 4 Configure OpenID Connect OIDC Client](#) on page 309).

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 13-62: API permissions

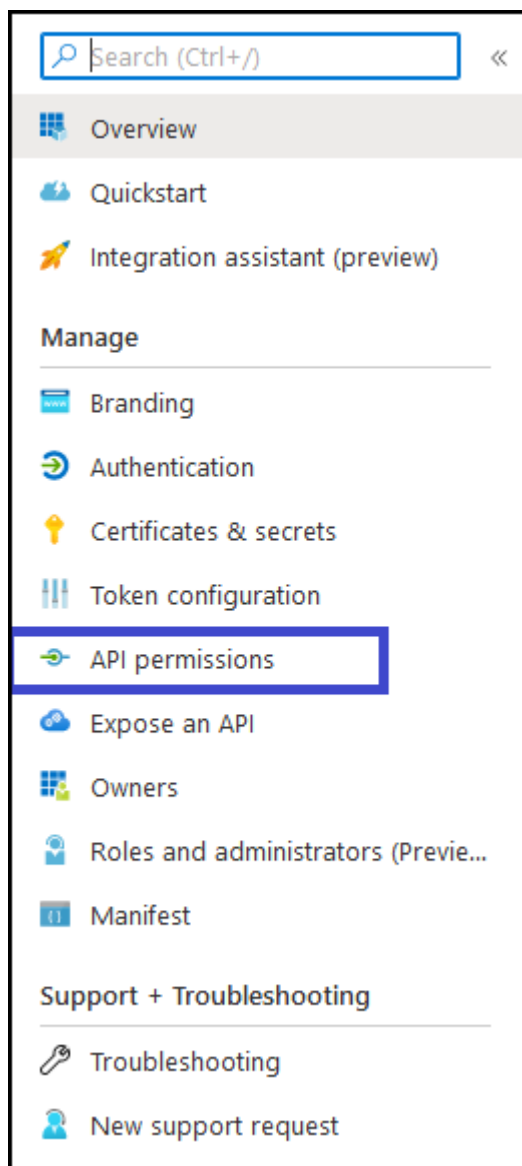


Figure 13-63: Configured Permissions

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				
<div> + Add a permission Grant admin consent for Nuera Ltd. </div>				
API / Permissions name	Type	Description	Admin consent req...	Status
<div> Microsoft Graph (1) ... </div>				
User.Read	Delegated	Sign in and read user profile	-	...

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 (1)				
User.Read	Delegated	Sign in and read user profile	-	...

2. Verify that the 'User.Read' permission is displayed.
3. Verify that allow user consent for apps is marked-Go to **Azure Ad -> Enterprise applications**

Figure 13-64: Enterprise Applications

The screenshot shows the Azure Active Directory 'AudioCodes Ltd. | Overview' page. The left sidebar contains a list of navigation options, with 'Enterprise applications' highlighted by a red rectangle. The main content area includes a top navigation bar with links like 'Switch tenant', 'Delete tenant', 'Create a tenant', 'What's new', 'Preview features', and 'Got feedback?'. Below this, there's a section for 'AudioCodes Ltd.' with a search bar. The 'Tenant information' card shows details like 'Your role: Global administrator and 7 other roles', 'License: Azure AD Premium P1', 'Tenant ID: ad41d6c3-67f0-47cc-9de3-e07fd...', and 'Primary domain: ai-logix.net'. The 'Azure AD Connect' card shows 'Status: Enabled' and 'Last sync: Less than 1 hour ago'. At the bottom, there's a 'Sign-ins' graph showing activity over time, with a large '123' indicating the total number of sign-ins.

4. Go to Consent and Permissions.

Figure 13-65: Consent and Permissions

Enterprise applications All applications			
<div> <div>Overview</div> <div> <div>Try out the new Enterprise Apps search preview! Click to enable the preview. →</div> </div> </div>			
Overview	AzureADConnectToGraph	7a4ea29e-096a-4c5a-b301-3740fae47743	1930aa07-74b1-4770-abca-9eb7e2ce3348
Diagnose and solve problems	AzureAuthIana	a0342d3-7e34-4462-a468-47b7ccade03e	ab79199e-433b-4d43-9618-1ed129ab7eb7
Manage	AzureAuthIanaLocalHost	bc603d0c-c523-4a0b-942b-1696979c3c8	41c7b241-3687-4723-a34e-f11f0fbeeec
All applications	CallDelivery-Live	8b62feb0-170d-487d-8e9e-1c95ea087515	f8fad00-dc0c-a66d-2acc0fb6067f
Application proxy	Daniel-Sharon-AAD-Test	318ed755-dedd-4010-b96c-2e13c331fa5b	2170f67f-5304-4003-a593-07bba037b07
User settings	Daniel-Sharon-Authentication-Test	333de45d-bc10-4000-8649-a273556f93cb	b6ac4882-daa3-4b6a-a504-73f1c85995a8
Collections	DebaADAppClient	0a6a09dc-46f5-4b89-92d6-7954a2ab1e32	ea58c3a6-733b-4723-a72d-7205a9b43c7
Security	Graph explorer	https://developer.microsoft.com/en-us/graph/graph-explorer	e90b0c51-1f05-4ca4-9e10-836cb1c4711b
Conditional Access	Graph Explorer	https://localhost:44328	61a915ed-1ee1-4064-b19c-647b4be94e91
Consent and permissions	IanaClientAppDev	b8837204-4b3e-407c-8425-0c79617c477d	bd1fa56e-7337-4375-a54c-fa4f8f93b457
Activity	IanaClientAppDev	53bdc267-9593-4814-902e-a0e9702d8e07	bc034a91-1b19-41f9-a09b-1e4628b79d7f
Sign-ins	IanaClientAppDev	77895cd3-c939-4ae3-810e-44644793a0c6	3d3d4dc4-f50d-48ca-89a8-8eba769e1110
Usage & insights (Preview)	IanaClientAppDev	4d520839-faf7-4fb9-aa55-ec0ed7120961	b7d9f12a-83a7-4acc-ac14-be7a1b1b53
Audit logs	IanaServerAppDev	04a5a2ec-1922-4ca0-af83-7eb0a0100edb	d1ed9374-89cb-48d3-ae7d-e82638aa5995
Provisioning logs (Preview)	IanaWebApp	4c2945f6-0803-4145-99e8-c7223fa1b08c	ca597d54-b00b-447c-b736-c7c14e820e8c
Access reviews	IntegrationM8	1b17805d-9ccb-40f5-b3f9-0e4ae7372e31	f558ff52-ef4c-41dc-bba3-4af52f0b559
Admin consent requests (Preview)	MeetingInsightsAAD	422516e-d08b-479c-bb0b-fbc092c174cc	b1e28a07-68aa-42b1-a8b2-5ae3831c09df
Troubleshooting + Support	MeetingInsightsBot	ac6e0546-f552-430e-ac54-abcb8b3f9686	20e605e5-a54c-4905-ae49-370dc8f19b0
Virtual assistant (Preview)	MeetingInsightsWebApp	6ba10234-5ae4-4e9e-a545-f46e98a2a098	1d7d2d33-c285-429e-84aa-6056eac3a29
New support request	MIADWebApp	25d31ea4-37cb-4217-a1ee-a4a35528e0ff	79fa9fb-b062-494c-9004-5a203b54a621
	mibotps	d128a05a-126d-44b9-b0cf-500ca95601b0	f7d3aeb5-e63b-461c-b076-4c5f2cb07090
	MIIntegrationRFServeApp	6a4f4f6a-7db1-4517-5a45-8aa577a81774	01a981a1-37a6-4703-807b-dcb454e61384

- Go to User Consent settings , by default the third option (Allow user consent for apps) is chosen, and it's the one used by SmartTap by default.

Figure 13-66: User Consent Settings

Consent and permissions | User consent settings

Save Discard

Manage

User consent settings

Permission classifications

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. [Learn more about consent and permissions](#)

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

☐ Do not allow user consent
 An administrator will be required for all apps.

☐ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
 All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

☒ Allow user consent for apps
 All users can consent for any app to access the organization's data.

⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. [Learn more about the risks](#)
 Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". [Learn more](#)

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

☐ Do not allow group owner consent
 Group owners cannot allow applications to access data for the groups they own.

☐ Allow group owner consent for selected group owners
 Only selected group owners can allow applications to access data for the groups they own.

☒ Allow group owner consent for all group owners
 All group owners can allow applications to access data for the groups they own.

The second option is also supported with the following configuration:

Figure 13-67: User Consent Settings

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

« Save Discard

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. [Learn more about consent and permissions](#)

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

☐ Do not allow user consent
An administrator will be required for all apps.

☒ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

[Select permissions to classify as low impact](#)

☐ Allow user consent for apps
All users can consent for any app to access the organization's data.

i You have enabled limited user consent to apps, but users can still consent to apps accessing the groups they own. You can change settings for user consent to group data below.

Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

☐ Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

☐ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

☒ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

6. Save and then "Select permissions to classify as "low impact".

Figure 13-68: Permission Classifications

Consent and permissions | Permission classifications

Manage

- User consent settings
- Permission classifications

« + Add permissions

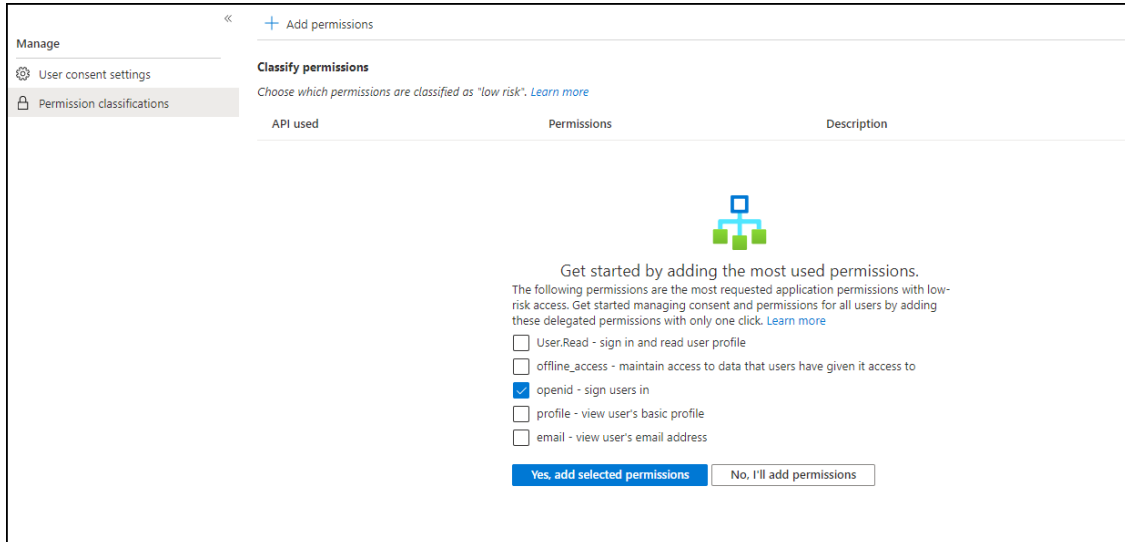
Classify permissions
Choose which permissions are classified as "low risk". [Learn more](#)

API used	Permissions	Description
	<input checked="" type="checkbox"/> openid - sign users in	Get started by adding the most used permissions. The following permissions are the most requested application permissions with low-risk access. Get started managing consent and permissions for all users by adding these delegated permissions with only one click. Learn more
	<input type="checkbox"/> User.Read - sign in and read user profile	
	<input type="checkbox"/> offline_access - maintain access to data that users have given it access to	
	<input type="checkbox"/> profile - view user's basic profile	
	<input type="checkbox"/> email - view user's email address	

[Yes, add selected permissions](#) [No, I'll add permissions](#)

7. Check the **openid-sign users in** option and **Yes, add selected permissions**.

Figure 13-69: Add Permissions--Openid



Manage < + Add permissions

Manage

- User consent settings
- Permission classifications

Classify permissions

Choose which permissions are classified as "low risk". [Learn more](#)

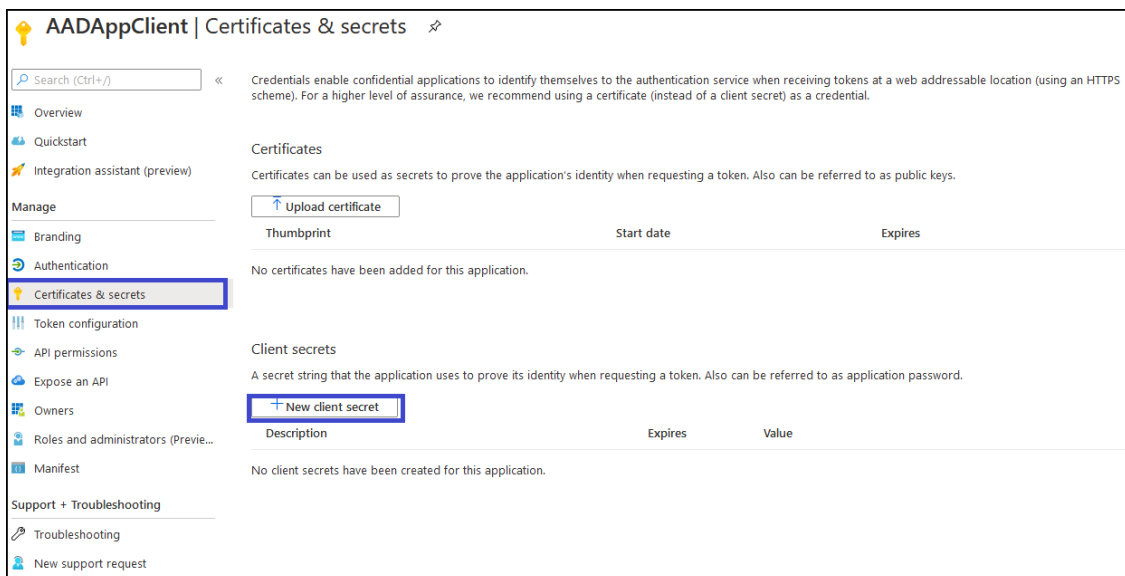
API used	Permissions	Description
	<p>Get started by adding the most used permissions.</p> <p>The following permissions are the most requested application permissions with low-risk access. Get started managing consent and permissions for all users by adding these delegated permissions with only one click. Learn more</p> <p> <input type="checkbox"/> User.Read - sign in and read user profile <input type="checkbox"/> offline_access - maintain access to data that users have given it access to <input checked="" type="checkbox"/> openid - sign users in <input type="checkbox"/> profile - view user's basic profile <input type="checkbox"/> email - view user's email address </p> <p> Yes, add selected permissions No, I'll add permissions </p>	

Step 3 Configure Certificates & Secrets

➤ Do the following:

1. In the Navigation pane, open the Certificates & Secrets page (**Manage > Certificate & Secrets**).

Figure 13-70: Certificates & Secrets



AADAppClient | Certificates & secrets ✕

Search (Ctrl+/) <

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.

[Upload certificate](#)

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.

[New client secret](#)

Description	Expires	Value
No client secrets have been created for this application.		

Navigation pane:

- Overview
- Quickstart
- Integration assistant (preview)
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - Owners
 - Roles and administrators (Previe...
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

2. Click + **New client secret** link.

Figure 13-71: Add a client secret

3. Enter a "Description", select "Expires" time and click **Add**.



The New Client Secret must be generated before the expiration time and set in SmartTAP to avoid possible issues that may arise with the recording service. Note the new client secret as it must be later configured.

A client secret is generated and displayed as below.

Figure 13-72: 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.		
+ New client secret		
Description	Expires	Value
OIDC Auth Client Secret	7/2/2021	.!s8d76uf.fl5ZA18qNqd.44kdyVHryhy

4. Copy the Value of the client secret for later configuration in the SmartTAP 360° Live Web (see [Step 4 Configure Azure Active Directory Client in SmartTAP 360° Live](#) on page 270).

Step 4 Configure OpenID Connect OIDC Client

To configure the OIDC Client in SmartTAP 360° Live, 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° Live Web with a user that has "sysAdmin" role.
2. Open the OAuth Client Config screen (**System > WEB > OAuth Client Config**).

Figure 13-73: OpenID Connect

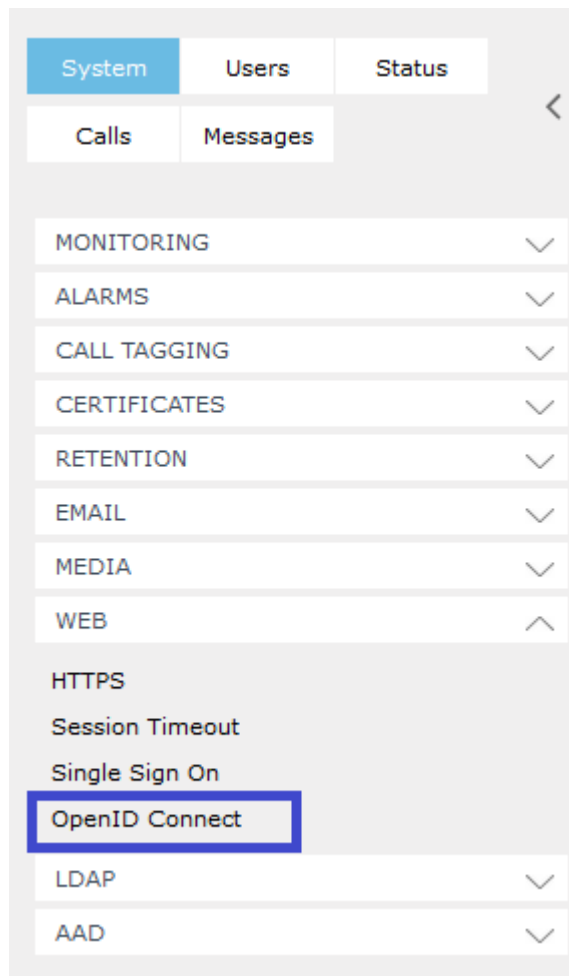
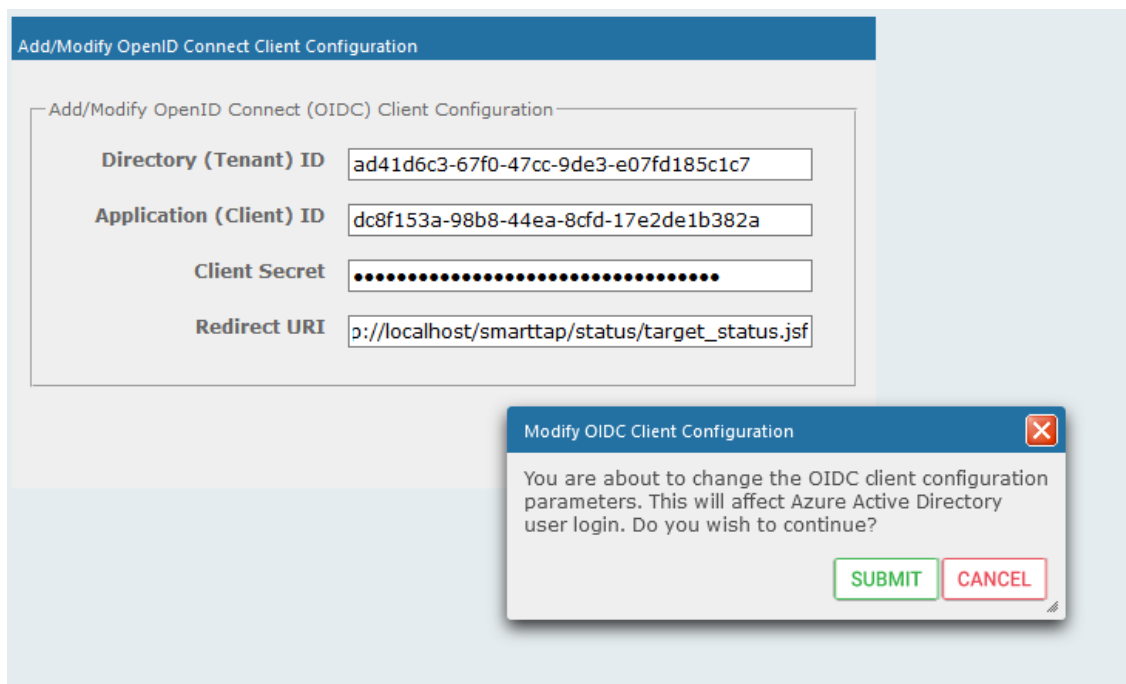


Figure 13-74: OpenID Connect Client Configuration




3. Enter the details and then click .
4. A confirmation message is displayed that the OIDC client configuration has been successfully saved to SmartTAP 360° Live.


Figure 13-75: 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	<input type="text" value="ad41d6c3-67f0-47cc-9de3-e07fd185c1c7"/>
Application (Client) ID	<input type="text" value="dc8f153a-98b8-44ea-8cf-d-17e2de1b382a"/>
Client Secret	<input type="text"/>
Redirect URI	<input type="text" value="http://localhost/smarttap/status/target_status"/>



Step 5 Assign Security Profile to Azure Active Directory user in SmartTAP 360° Live


This step describes how to assign a user to "agent" security profile in SmartTAP 360° Live.






➤ To assign a security profile:

1. Login to SmartTAP 360° Live with a user that has "userAdmin" permissions.
2. Open the View/Modify Users page (**Users** tab > **User Management** > **View/Modify Users**).

Figure 13-76: View/Modify Users

View/Modify Users

<input type="text" value="First Name"/>	<input type="text" value="Last Name"/>	<input type="text" value="Email"/>	<input type="text" value="Login ID"/>	<input type="text" value="Alias"/>	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>
Deb	Dutta		debajyotid@smarttap.onmicrosoft.com			

20    **1**   (1 of 1)



3. Assign "agent" security profile and then click . A confirmation message is displayed:

Figure 13-77: User Successfully Updated

• *User successfully updated.*

Modify User



First Name **Last Name**

Email **Login ID**

Alias **Retention Policy**


Recording Profile **Legal Hold** OFF

Security Profiles

- administrator
- agent**
- supervisor

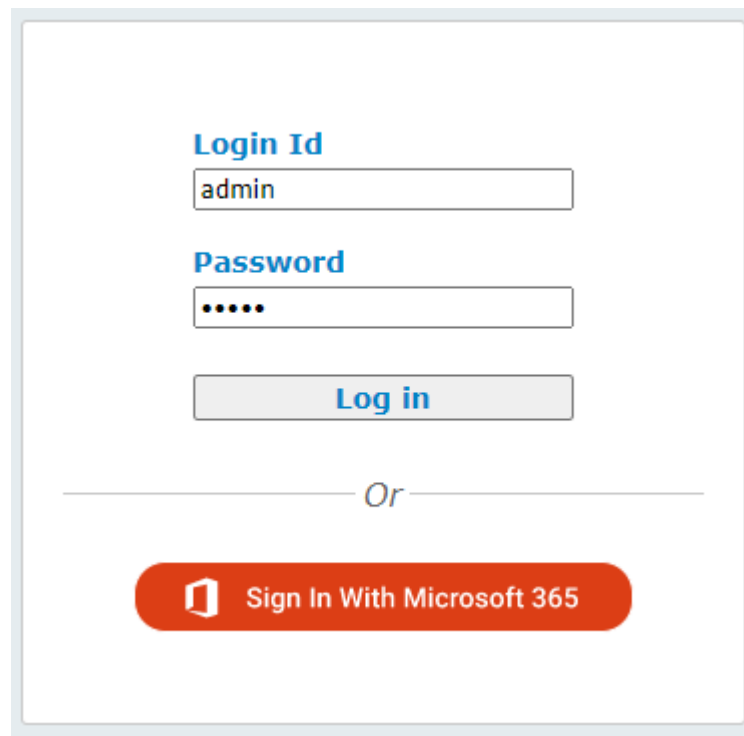
Groups

- Default
- TEST_G_1

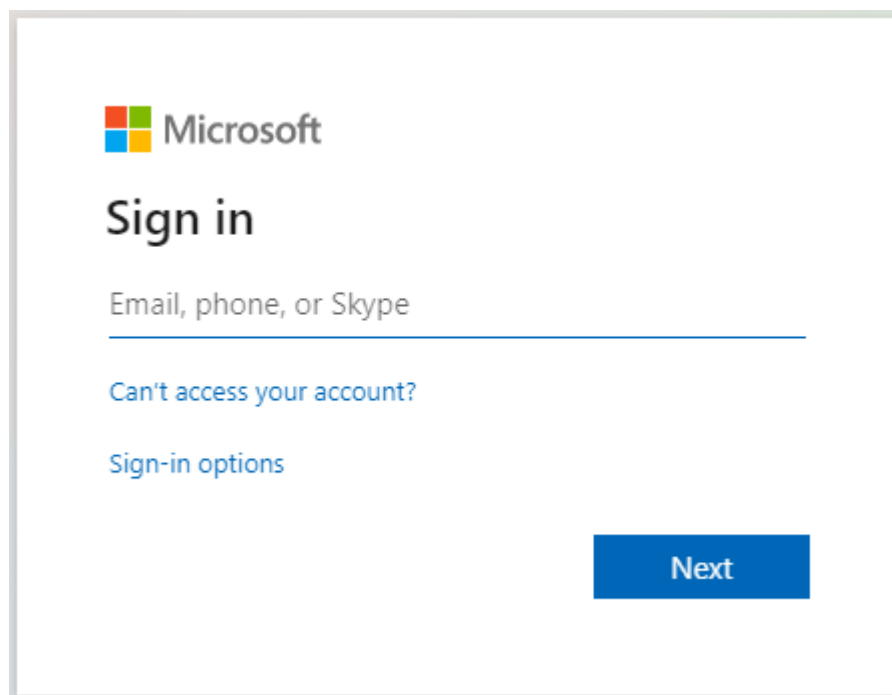


4. Login to SmartTAP 360° Live using Microsoft Login Credentials.

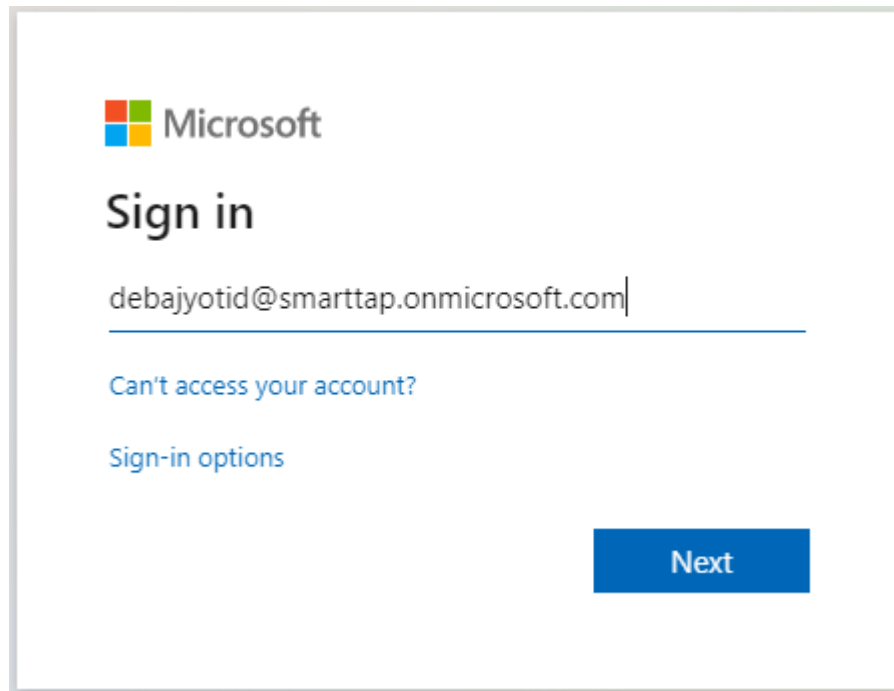
- On the SmartTAP 360° Live login page, click **Sign In With Microsoft 365**.

Figure 13-78: Microsoft Sign inA screenshot of a Microsoft sign-in form. It features two input fields: 'Login Id' with the text 'admin' and 'Password' with five dots. Below these is a 'Log in' button. A horizontal line with the word 'Or' in the center separates this from a large red button labeled 'Sign In With Microsoft 365' which includes the Microsoft 365 logo.

The user is redirected to Microsoft MFC Login page:

Figure 13-79: Microsoft MFC Login PageA screenshot of the Microsoft MFC Login page. It displays the Microsoft logo at the top left, followed by the heading 'Sign in'. Below this is a text input field labeled 'Email, phone, or Skype'. Underneath the input field are two links: 'Can't access your account?' and 'Sign-in options'. A blue 'Next' button is positioned in the bottom right corner.

- Enter the Microsoft credentials

Figure 13-80: Sign InThe image shows a Microsoft sign-in interface. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed in a large, bold font. Underneath, there is a text input field containing the email address "debajyotid@smarttap.onmicrosoft.com". Below the input field, there are two links: "Can't access your account?" and "Sign-in options". At the bottom right, there is a blue button with the text "Next".

Microsoft

Sign in

debajyotid@smarttap.onmicrosoft.com

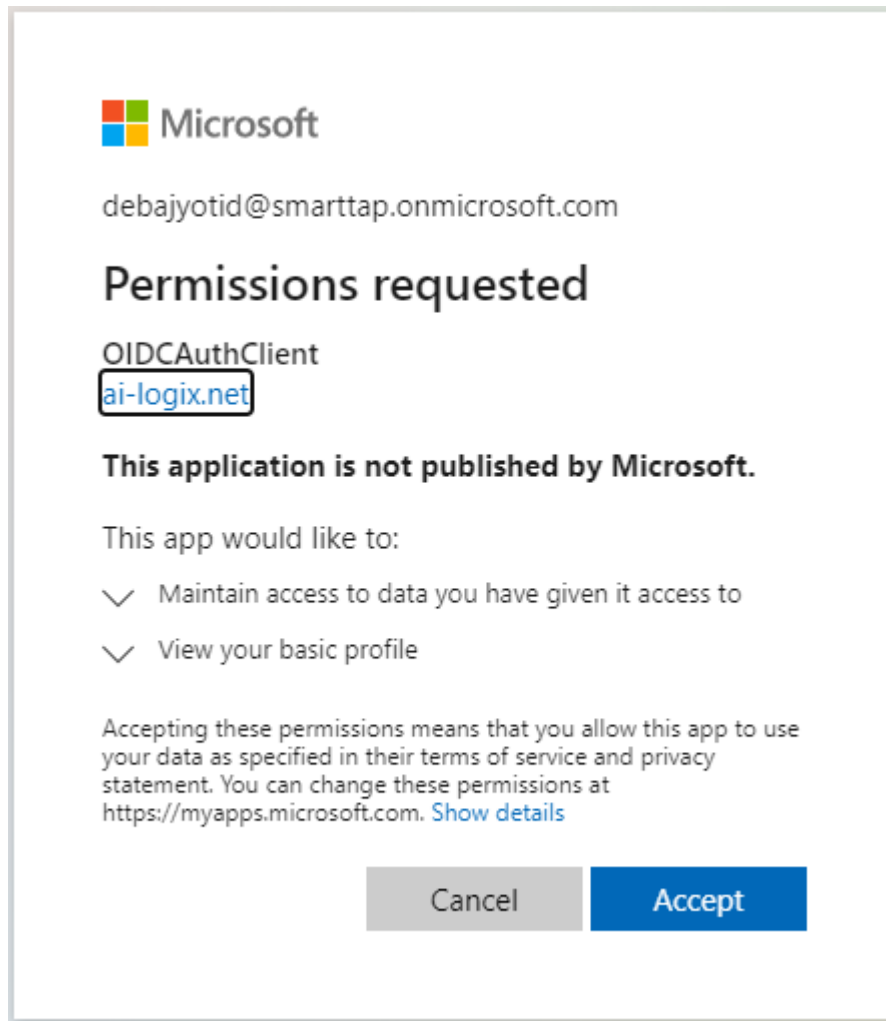
[Can't access your account?](#)

[Sign-in options](#)

Next

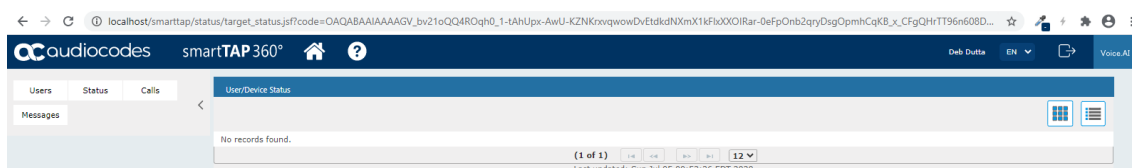
- Allow permission to the client app to use user authentication data.

Figure 13-81: Permissions Requested



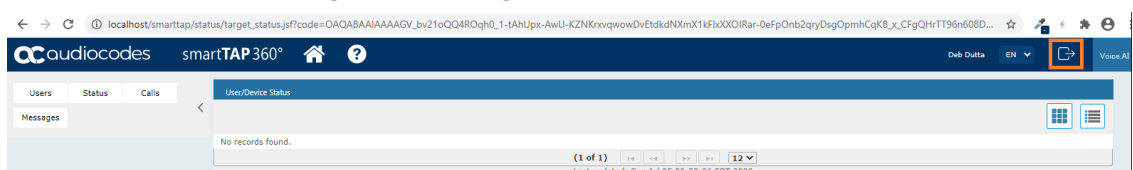
The user is re-directed to SmartTAP 360° Live URI configured in AAD (see [Step 1 Register App in Azure Active Directory](#) on page 300 i.e. http://localhost/SmartTAP 360° Live/status/target_status.jsf)

Figure 13-82: User Device Status

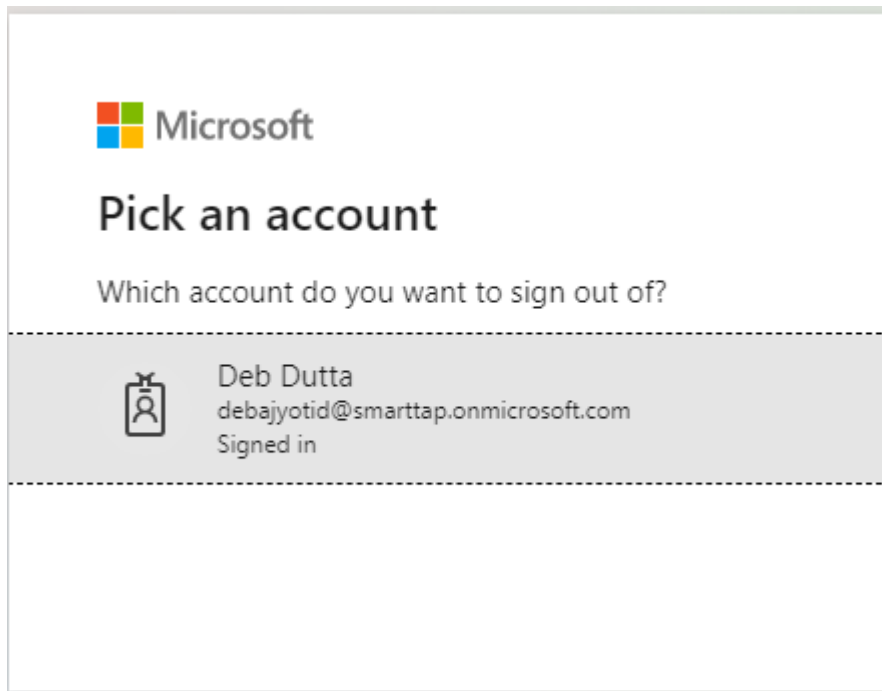


5. An Azure Active Directory user logs off from SmartTAP 360° Live Web.

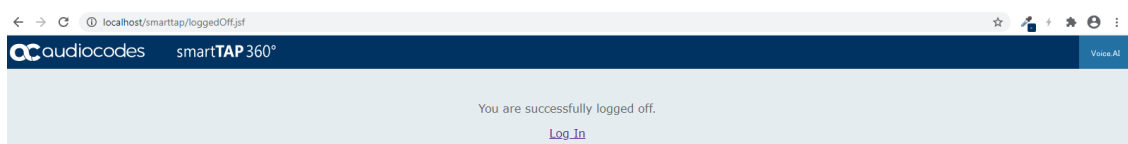
Figure 13-83: Logout



6. User is prompted to select the Microsoft account that needs to be signed out.

Figure 13-84: Pick an Account

7. When the account is selected, the user is redirected to the SmartTAP 360° Live log off page.

Figure 13-85: SmartTAP 360° Live LogOff Page

14 Integrate SmartTAP Personal App in Teams

SmartTAP for Teams can be added as a Personal App in Microsoft Teams with the main tab/page that includes On-demand buttons and an additional tab for access to the full application. This section describes how to configure the Azure Registration for this app and for the SSO login to SmartTAP Teams personal app from the Teams App client.



- The Application server supports logging in from a Teams desktop client and from a Teams mobile clients, however does not support logging in from a Teams Web Client.
- SmartTAP Teams personal app must be able to successfully connect to the SmartTAP Server on TCP: 443 port. If the SmartTAP Server is deployed in the customer environment (Azure cloud or On-premises) either the Teams client hosting the app must be running on a machine that can connect to the SmartTAP Server or a global inbound rule must be defined in the firewall to allow access to SmartTAP Server on TCP: 443 port.

This procedure includes the following procedures:



To perform the procedures below, you must have Global administrator role in Azure.

1. [Create and Register the SmartTAP Personal App](#) below
2. [Set Microsoft API Permissions for Personal App](#) on page 320
3. [Configure Connection with SmartTAP Server](#) on page 325
4. [Configure and Upload Manifest](#) on page 325

Create and Register the SmartTAP Personal App

This procedure describes how to create and register the SmartTAP Personal App.

➤ **To configure SmartTAP Teams app for SSO and Teams client:**

1. Go to Azure portal > **Azure Active Directory** > **App Registrations**
2. Select the registration app that was created for open ID connect or create a new App registration.

Figure 14-1: Register SmartTAP Personal App

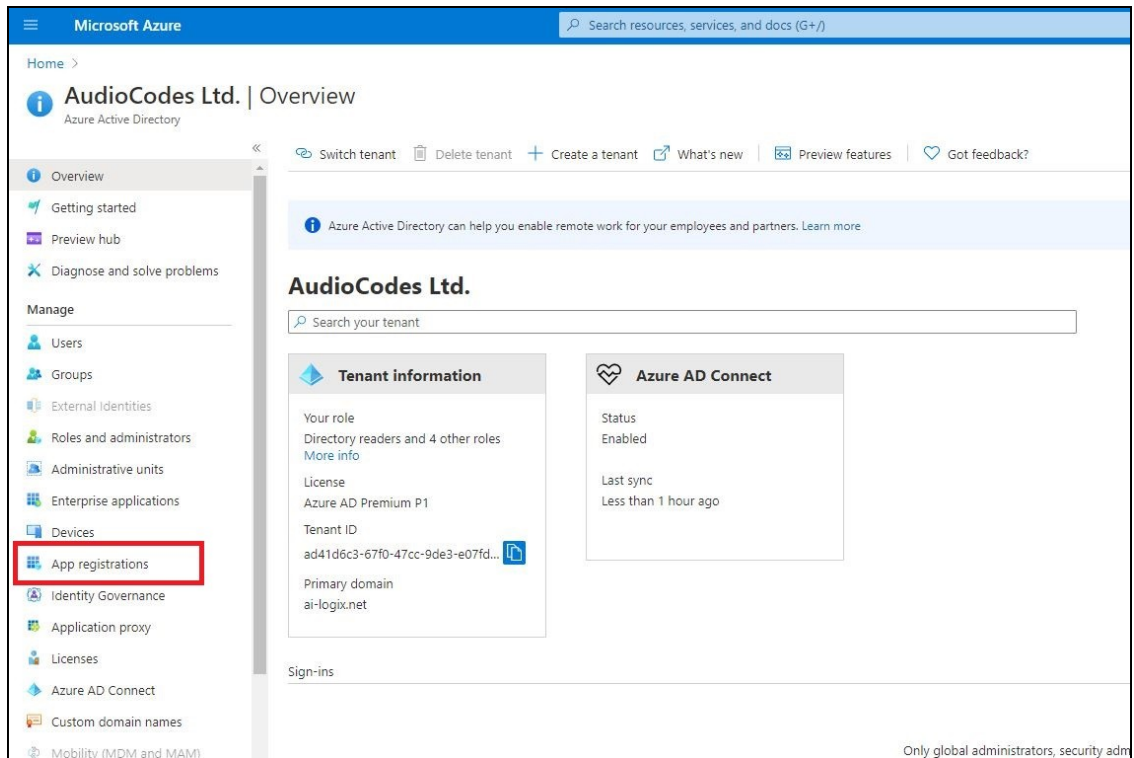


Figure 14-2: Register an application

Home > AudioCodes Ltd. >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

ST-Teams-app ✓

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)

☐ Personal Microsoft accounts only

[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.

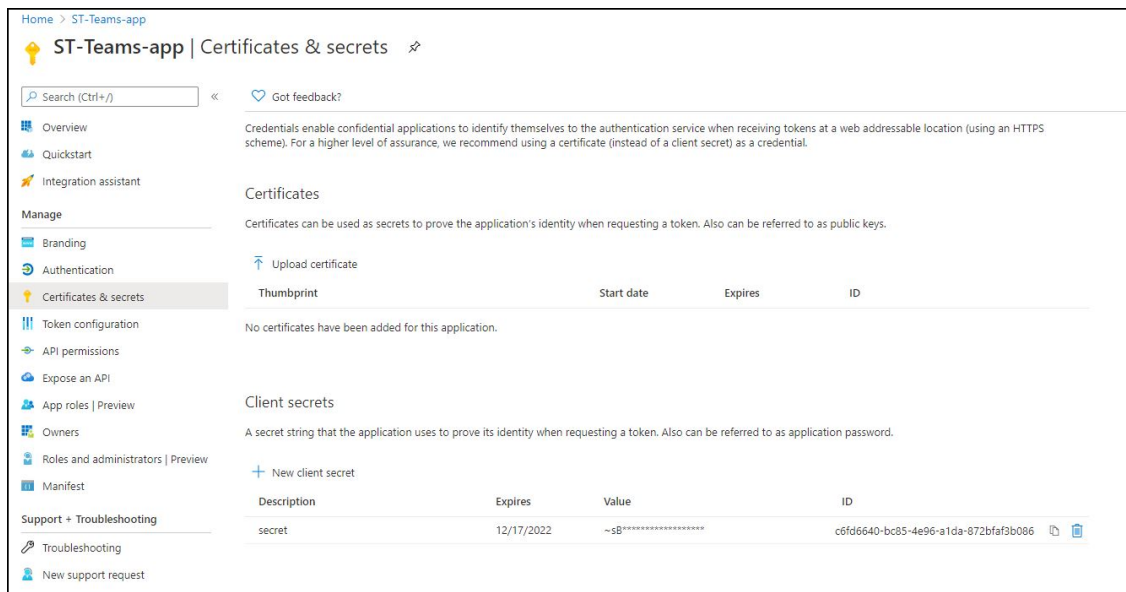
Web ▼ e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

3. Enter the Application name.
4. Select “Accounts in this organizational directory only”.
5. Click **Register**.
6. In the Navigation pane, select **Overview** and save the ‘Application (Client) ID’ as it needs to be later configured.
7. In the Application page Navigation pane, select **Certificates & secrets**.
8. Add a new Client Secret by clicking **New client secret**.

Figure 14-3: Certificates & secrets



Set Microsoft API Permissions for Personal App

This section describes how to set permissions for the Personal App.

➤ To set permissions for the personal app:

1. In the Navigation pane, select **Expose an API**.

Figure 14-4: Expose an API

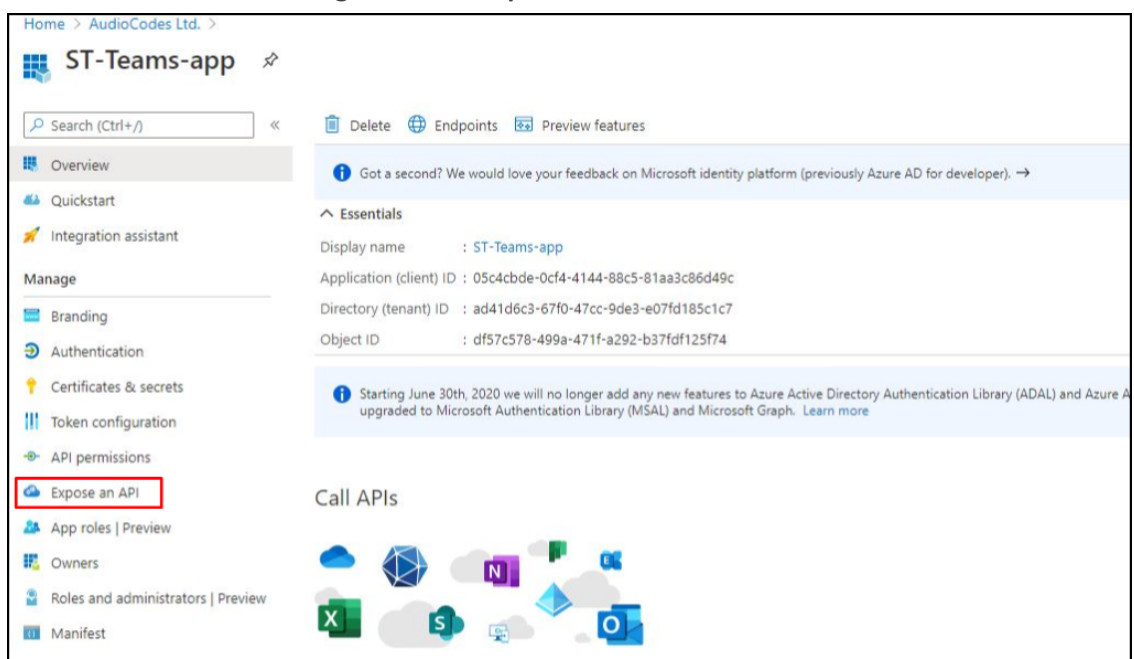
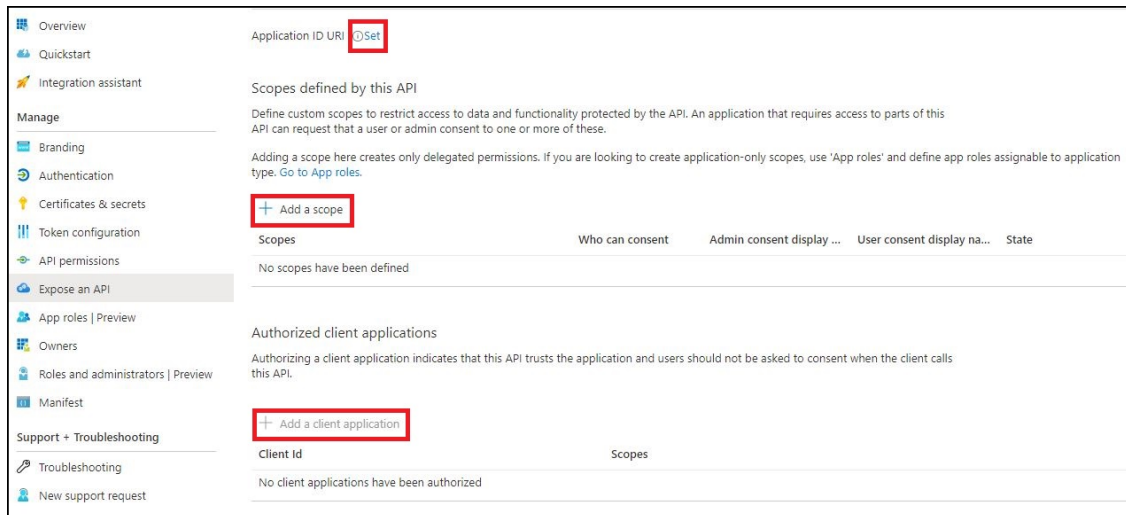


Figure 14-5: Expose an API



2. Select the **Set** link to generate the Application ID URI.
3. Insert your fully qualified domain name in the following format: `api://<fully-qualified-domain-name.com>/<AppID>`

Where

- `<fully-qualified-domain-name.com>` is the FQDN of the SmartTAP Server

Example

`api://smarttapteamspoc.bot.ai-logix.net/05c4cbde-0cf4-4144-88c5-81aa3c86d49c`

- Where {AppID} is the Application [clientID] shown in the figure above.

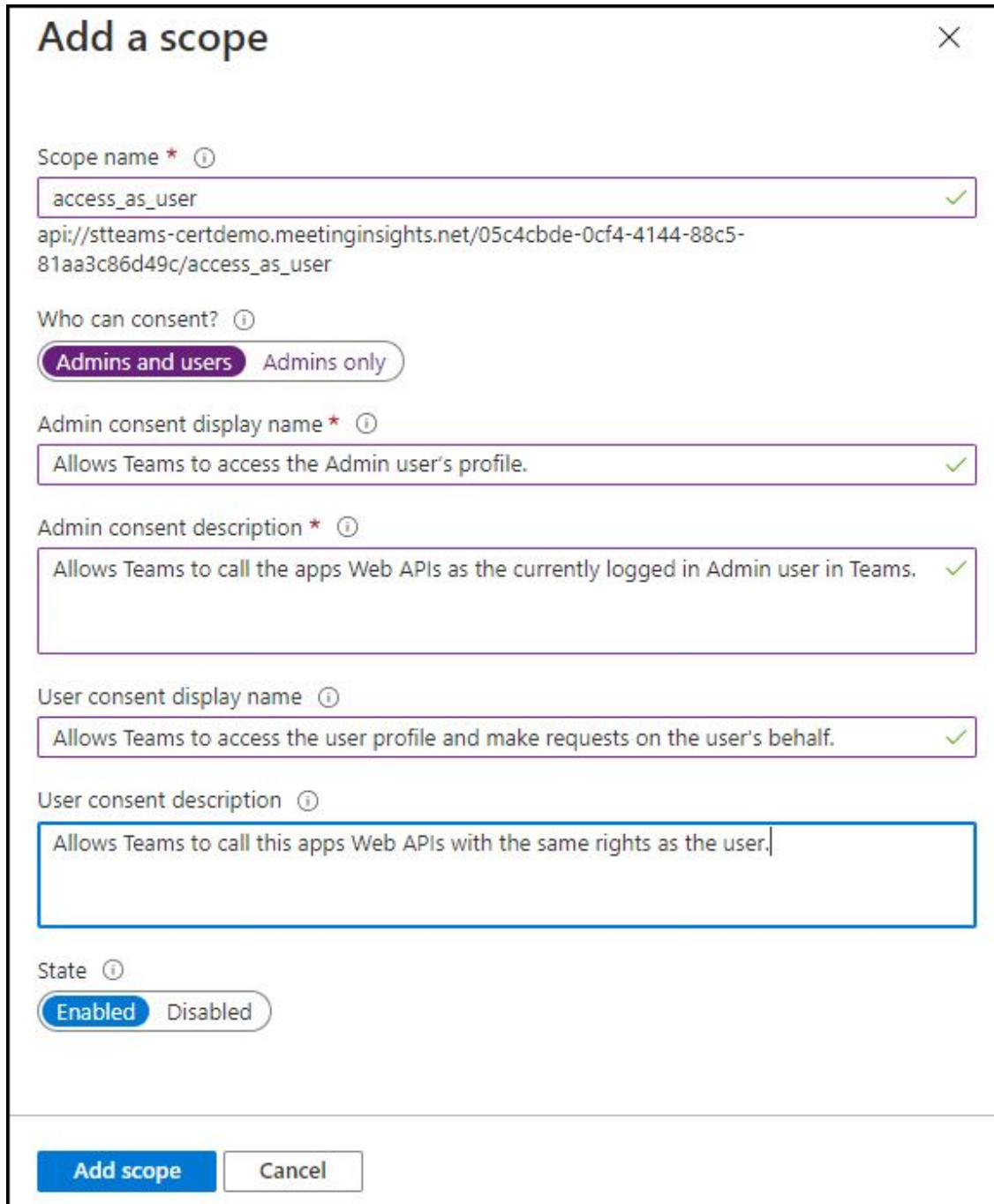
4. Select **Add a scope**. In the panel that opens, enter `access_as_user` as the **Scope name**.
5. Set **Who can consent?** to `Admins and users`.
6. Enter the following fields for configuring the admin and user consent prompts with values that are appropriate for the `access_as_user` scope:
 - **Admin consent title:** Teams can access the user's profile.
 - **Admin consent description:** Allows Teams to call the app's web APIs as the current user.
 - **User consent title:** Teams can access the user profile and make requests on the user's behalf.
 - **User consent description:** Enable Teams to call this app's APIs with the same rights as the user.
7. Ensure that **State** is set to **Enabled**.
8. Click **Add scope** to save changes.

- The domain part of the **Scope name** is displayed just below the text field and should automatically match the **Application ID** URI set in the previous step with `/access_as_user` appended:

Example

api://[smarttapteamspoc.bot.ai-logix.net](#)/05c4cbde-0cf4-4144-88c5-81aa3c86d49c/access_as_user

Figure 14-6: Add a Scope



Add a scope [Close]

Scope name * ⓘ
 ✓
 api://stteams-certdemo.meetinginsights.net/05c4cbde-0cf4-4144-88c5-81aa3c86d49c/access_as_user

Who can consent? ⓘ
☒ Admins and users ☐ Admins only

Admin consent display name * ⓘ
 ✓

Admin consent description * ⓘ
 ✓

User consent display name ⓘ
 ✓

User consent description ⓘ

State ⓘ
☒ Enabled ☐ Disabled

Add scope Cancel

9. In the Authorized client applications section, identify the applications that you want to authorize for your app's Web application.
 - a. Select **Add a client application**.

- b. Enter the following Client ID and select the Authorized scope that you created in the previous step (see selected Check box in the screen below):
- ◆ 1fec8e78-bce4-4aaf-ab1b-5451cc387264 (Teams mobile/desktop application)

Figure 14-7: Client ID

The screenshot displays a configuration interface for a client. It features two main sections: 'Client ID' and 'Authorized scopes'. The 'Client ID' section has a text input field containing the value '1fec8e78-bce4-4aaf-ab1b-5451cc387264', with a green checkmark icon to its right. The 'Authorized scopes' section shows a list of scopes, with the first one selected, indicated by a blue checkmark in a box. The selected scope is 'api://stteams-certdemo.meetinginsights.net/05c4cbde-0cf4-4144-88c5-81aa3c86d49c...'. The entire interface is enclosed in a light gray border.

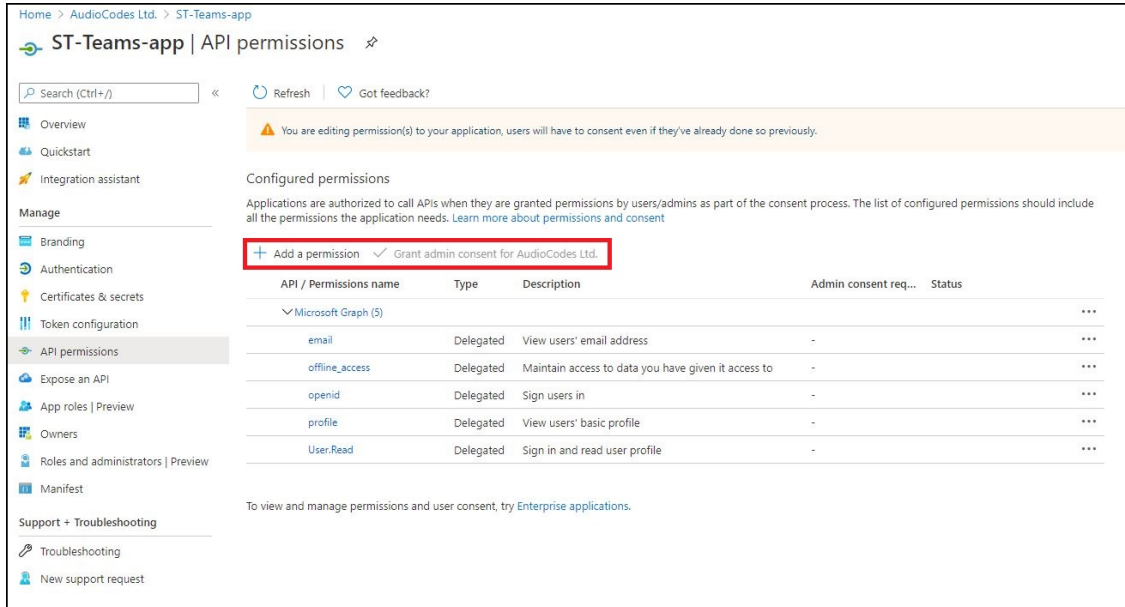
Client ID ⓘ

1fec8e78-bce4-4aaf-ab1b-5451cc387264 ✓

Authorized scopes ⓘ

☒ api://stteams-certdemo.meetinginsights.net/05c4cbde-0cf4-4144-88c5-81aa3c86d49c...

10. In the Navigation pane, select **API Permissions**, select **Add a permission > Microsoft Graph > Delegated permissions**, and then add the following permissions from the Microsoft Graph API:
- User.Read (enabled by default)
 - email
 - offline_access
 - OpenId
 - profile

Figure 14-8: Delegated Permissions


Home > AudioCodes Ltd. > ST-Teams-app

ST-Teams-app | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

Branding Authentication Certificates & secrets Token configuration

API permissions

Expose an API App roles | Preview Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

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.

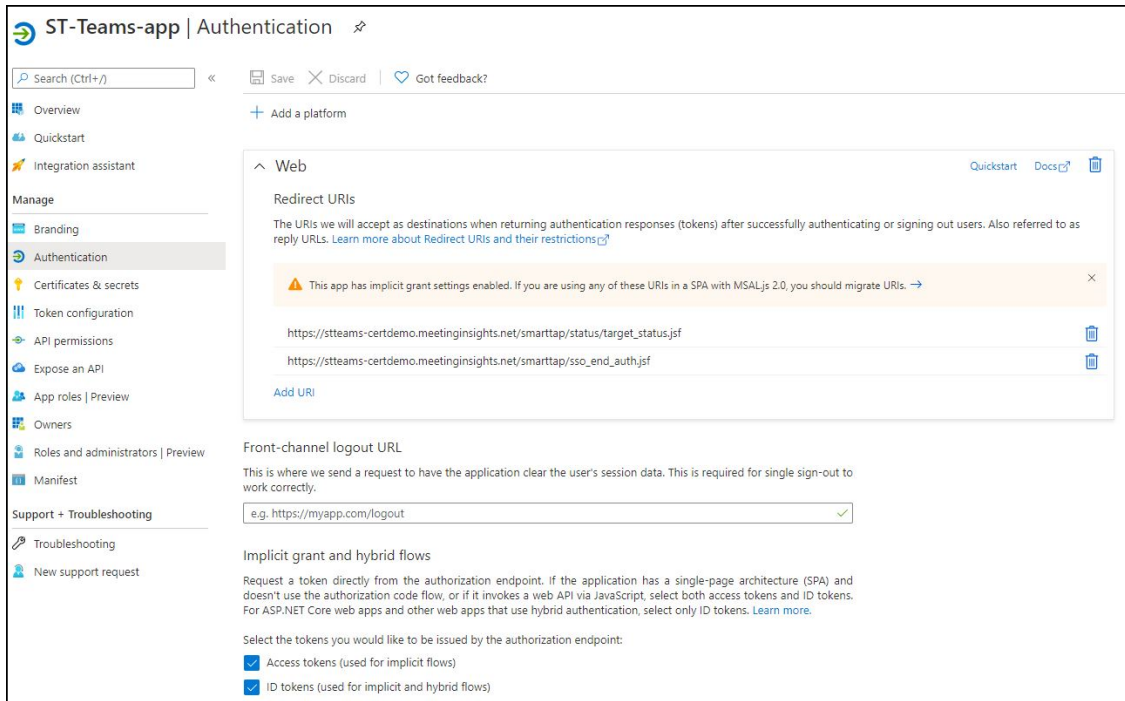
API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				...
email	Delegated	View users' email address	-	...
offline_access	Delegated	Maintain access to data you have given it access to	-	...
openid	Delegated	Sign users in	-	...
profile	Delegated	View users' basic profile	-	...
User.Read	Delegated	Sign in and read user profile	-	...

To view and manage permissions and user consent, try [Enterprise applications](#).



If the App hasn't been granted admin consent (see "Grant admin consent for AudioCodes Ltd." adjacent to the 'add a permission' button), users are prompted to grant consent the first time they use the App.

11. In the Navigate pane, select **Authentication**.

Figure 14-9: Authentication


ST-Teams-app | Authentication

Search (Ctrl+/) Save Discard Got feedback?

+ Add a platform

Web

Quickstart Docs Add

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL.js 2.0, you should migrate URIs. →

https://steams-certdemo.meetinginsights.net/smarttap/status/target_status.jsf

https://steams-certdemo.meetinginsights.net/smarttap/sso_end_auth.jsf

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://myapp.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more](#).

Select the tokens you would like to be issued by the authorization endpoint:

☒ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

12. Set a redirect URI:

- Select **Add a platform**

- Select **web**

13. Enter the redirect URI in the following format: `https://<fully-qualified-domain-name.com>/smarttap/sso_end_auth.jsf`

Where <fully-qualified-domain-name.com> is the FQDN of the SmartTAP server

Example:

`https://smarttapteams poc.bot.ai-logix.net/smarttap/sso_end_auth.jsf`

14. Enable implicit grant by selecting the following Check boxes:

- ID Token
- Access Token

Configure Connection with SmartTAP Server

This section describes how to configure the OpenID Connect (OIDC) Client Configuration.

➤ **To configure the OpenID Connect OIDC Client:**

1. In the SmartTap Web interface, under **System**, select 'OpenID Connect' and set your App details. For more information, see [Step 4 Configure OpenID Connect OIDC Client](#) on page 309

Figure 14-10: OpenID Connect

The screenshot shows a web form for configuring an OpenID Connect (OIDC) client. The form has a blue header bar with the text 'Add/Modify OpenID Connect (OIDC) Client Configuration'. Below the header, the form is enclosed in a light gray border. Inside the border, there are four labels and corresponding input fields: 'Directory (Tenant) ID', 'Application (Client) ID', 'Client Secret', and 'Redirect URI'. Each label is followed by a white input field with a thin gray border. At the bottom right of the form, there is a green button with the word 'SUBMIT' in white capital letters.

Configure and Upload Manifest

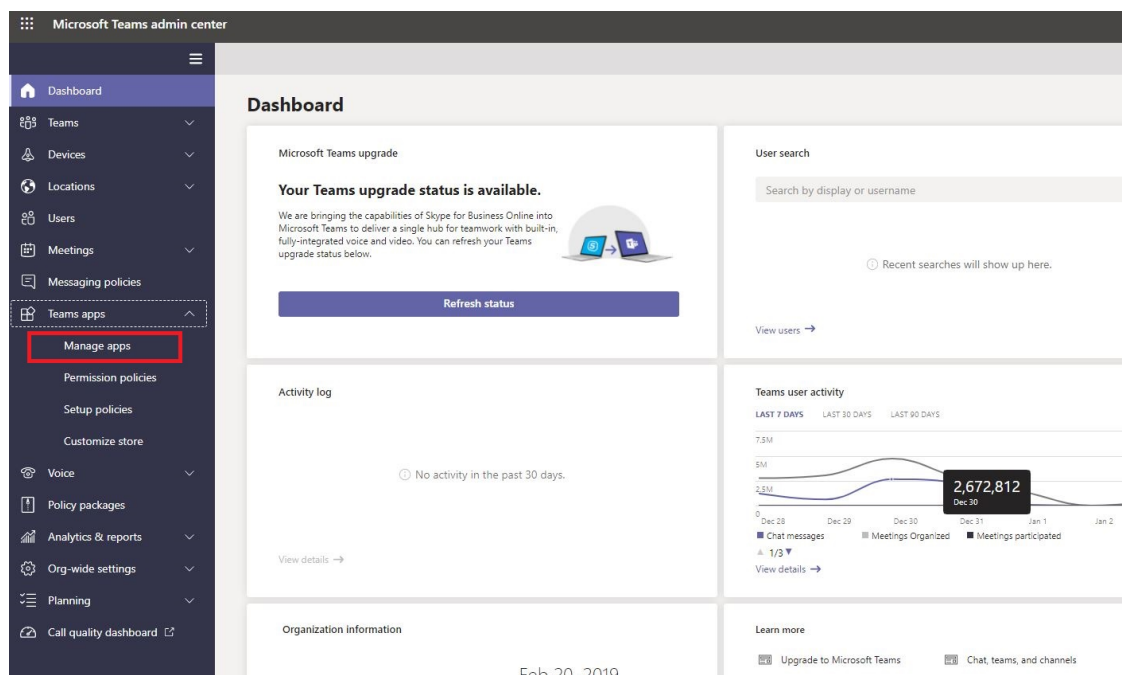
This section describes how to configure and upload the Manifest.

➤ **To configure and upload the Manifest:**

1. Update the Manifest template with the customer details. The Manifest template is located at the following path: AUDIOCODES\Tools\Teams\manifest.json
2. The following information must be added to the Tab application Manifest for each customer:
 - Under **staticTabs**:
 - i. Replace the **<customer_FQDN>** with the actual FQDN. For example, "contentUrl": "https://<customer_fqdn>/smarttap/status/call_status.jsf", should be "contentUrl": "https://smarttapteams poc.bot.ai-logix.net/smarttap/status/call_status.jsf"

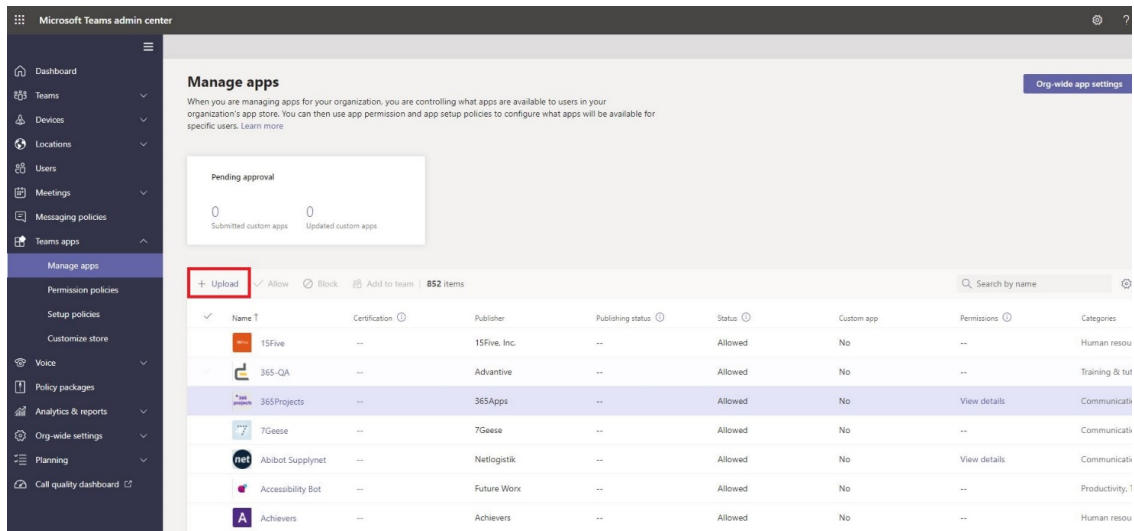
Where **<customer_FQDN>** is the FQDN of the SmartTAP server
 - Under **webApplicationInfo**:
 - i. Replace <app_id> with the Application (client) ID. For example, 05c4cbde-0cf4-4144-88c5-81aa3c86d49c
 - ii. Replace the <customer_FQDN> where **<customer_FQDN>** is the FQDN of the SmartTAP server.
3. When the updates to the Manifest template have been completed, zip the three files manifest.json, outline.png, and color.png to a single zip file to give to the customer. The customer should then upload them to their App store using the following: <https://admin.teams.microsoft.com/dashboard>
 - a. In the Navigation pane, select **Teams apps > Manage apps**.

Figure 14-11: Manage apps



- b. Click **Upload** and choose the zip file you created.

Figure 14-12: Upload Manifest



Example of manifest:

```
{
  "$schema": "https://developer.microsoft.com/en-us/json-
schemas/teams/v1.8/MicrosoftTeams.schema.json",
  "manifestVersion": "1.8",
  "version": "1.0.1",
  "id": "<bot_app_id>", where <bot_app_id> is a unique Azure Application ID
  "packageName": "\"com.audiocodes.smarttap.tabs\"",
  "developer": {
    "name": "AudioCodes",
    "websiteUrl": "https://www.audiocodes.com/solutions-
products/voiceai/meetings-and-recording/smarttap-360",
    "privacyUrl": "https://www.audiocodes.com/corporate/privacy-policy",
    "termsOfUseUrl": "https://www.audiocodes.com/library/technical-
documents?productGroup=1695"
  },
  "icons": {
    "color": "color.png",
    "outline": "outline.png"
  },
  "name": {
    "short": "SmartTAP",
    "full": "Compliance Recording for Teams"
  },
  "description": {
    "short": "SmartTAP for Teams",
    "full": "SmartTAP 360° Enterprise Interactions Recording for Microsoft
Teams\nAudioCodes SmartTAP 360° is an intelligent, fully-secured
enterprise compliance-recording solution, allowing companies to capture
and index any customer or organizational interactions across both external
and internal communication channels.\n\nCompanies using Microsoft Teams
can seamlessly apply SmartTAP 360° to record all voice, video and IMs
interactions for later-stage AI analysis and for meeting regulatory
compliance demands."
  },
  "accentColor": "#F9F9FA",
  "staticTabs": [
    {
```

```

"entityId": "RecordOnDemand",
"name": " MY Active Calls",
"contentUrl": "https://smarttapteamspec.bot.ai-
logix.net/smarttap/status/call_status.jsf",

"websiteUrl": "https://smarttapteamspec.bot.ai-
logix.net/smarttap/status/call_status.jsf",
"scopes": [
"personal"
]
},
{
"entityId": "ST",
"name": "All Calls",
"contentUrl": "https://smarttapteamspec.bot.ai-
logix.net/smarttap/welcome.jsf",

"websiteUrl": "https://smarttapteamspec.bot.ai-
logix.net/smarttap/welcome.jsf",

"scopes": [
"personal"
]
},
"permissions": [
"identity",
"messageTeamMembers"
],
"validDomains": [
"smarttapteamspec.bot.ai-logix.net",

"ai-logix.net"
],
"webApplicationInfo": {
"id": "<app_id>",
"resource": "api://smarttapteamspec.bot.ai-logix.net/<app_id>"
}
}

```

15 Enable Users with Compliance Recordings

This procedure describes how to enable users with Compliance Recordings using PowerShell scripts on the local machine that need to run with permissions on the required Teams environment. This step includes the following procedures:

- Prerequisite - Join Calls in Teams Tenant
- Create Compliance Recording Policy

Prerequisite - Join Calls in Teams Tenant

This procedure describes how to provide SmartTAP 360° with permissions to join calls in your Teams' tenant. The procedure should be performed by your Office 365 Administrator.

➤ To join calls in your Teams tenant:

1. Paste the following URL in your browser with parameters shown below:

<https://login.microsoftonline.com/common/adminconsent?>

- client_id=XXXX

Where XXXX is the SmartTAP 360° Bot app ID from BOT service that was created in Step 2-1 Configure Service Channel which can be extracted from Manage > BoT Service. This is required to authenticate your Azure subscription.

- &state=12345
- [&redirect_uri=https://login.microsoftonline.com/common/oauth2/nativeclient](https://login.microsoftonline.com/common/oauth2/nativeclient)
 - ◆ 'nativeclient' is the SmartTAP 360° Bot app ID from BOT service that was created and which can be extracted from the Manage > BoT Service page. This is required to authenticate your Azure subscription.
- &scope=
- <https://graph.microsoft.com/Calls.AccessMedia.All>
- <https://graph.microsoft.com/Calls.JoinGroupCall.All>

The Authentication Settings are displayed and the connection is authenticated.

Figure 15-1: BOT Channel Settings

sfbTeamsBotChannel | Settings
Bot Channels Registration

Search (Ctrl+/) << Save Discard

Overview
Activity log
Access control (IAM)
Tags
Bot management
Test in Web Chat
Analytics
Channels
Settings
Speech priming
Bot Service pricing
Support + troubleshooting
New support request

Upload custom icon 30K max, png only

Display name * ⓘ
sfbTeamsBotChannel

Bot handle ⓘ
sfbTeamsBotChannel

Description ⓘ

Configuration
Messaging endpoint
https URL

☐ Enable Streaming Endpoint

Microsoft App ID (Manage) ⓘ
53210052-c601-4d74-bfdc-cc3863e9b375

Analytics
Application Insights Instrumentation key ⓘ
1921024f-7141-4743-b9e4-5ce18c5e3976

Application Insights API key ⓘ
.....

Application Insights Application ID ⓘ
c65f42e0-4e73-4ddc-830f-48c1a8657bfc

OAuth Connection Settings
No settings defined

Add Setting

Create Compliance Recording Policy

This procedure describes how to create a Compliance Recording Policy:

1. Create Application Instance
2. Create New Compliance Recording Policy
3. Set Compliance Recording Policy
4. Grant Policy to a Recorded User

Create Application Instance

This procedure describes how to create an Application Instance on the local machine. This action can be performed by 'Admin' user.

➤ **To create an Application instance:**

1. Download Skype for Business module to be able to record Teams users with SmartTAP 360°. The Microsoft Teams Administrator must create a Compliance Recording Policy for SmartTAP 360° and assign it to the recorded users. Refer to the following link:

<https://docs.microsoft.com/en-us/skypeforbusiness/set-up-your-computer-for-windows-powershell/download-and-install-the-skype-for-business-online-connector>

2. Create a new session with the relevant Teams tenant:

```
PS .:\> Import-Module
SkypeOnlineConnector

PS .:\> $sfbSession = New-
CsOnlineSession

PS .:\> Import-PSSession $sfbSession
```

Refer to: <https://docs.microsoft.com/en-us/office365/enterprise/powershell/manage-skype-for-business-online-with-office-365-powershell>

3. Enter the following commands:

```
PS .:\> New-CsOnlineApplicationInstance -UserPrincipalName <User Principal
Name> -DisplayName<displayName> -ApplicationId <SmartTAPBOTID>
```

Where:

- <UserPrincipalName>: AD BOT entity - Create new Organizational user with onmicrosoft.com domain that is assigned to the BOT.
- <SmartTAPBOTID> -Application ID that was created during the creation of the BOT Service channel (see Step 2-1 Configure Service Channel). This value can be extracted from the Settings screen (see example figure below).
- <displayName>: Free text Description field

Output similar to the following is displayed:

```
RunspaceId: 15eea8f7-970e-4061-893e-3573cb5e973b
ObjectId: fd13dab0-dd31-4b58-86d6-122fa07e250f
TenantId: ad41d6c3-67f0-47cc-9de3-e07fd185c1c7
UserPrincipalName :
STTeamsbotstandartlb2@smarttap.onmicrosoft.com
ApplicationId: ff6fc00a-fc73-4062-b99f-55ff0e09b779
DisplayName: STTeamsbotstandartlb2
```


PhoneNumber:

Figure 15-2: Create Application Instance

The screenshot shows the 'StTeamsBot | Settings' page. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Bot management (Test in Web Chat, Analytics, Channels, Settings), Speech priming, Bot Service pricing, Support + troubleshooting, and New support request. The main content area has a 'Save' and 'Discard' button at the top. Below is an 'Upload custom icon' section (30K max, png only). The 'Display name' is 'STTeamsBot'. The 'Bot handle' is 'STTeamsBot'. The 'Description' field is empty. Under 'Configuration', the 'Messaging endpoint' is 'https://url'. The 'Enable Streaming Endpoint' checkbox is unchecked. The 'Microsoft App ID (Manage)' is '51c35d16-1664-494c-936b-2cc35bdcf34b'. Under 'Analytics', the 'Application Insights Instrumentation key' is '0e20465d-1c39-42b8-ab7e-46e6e44aa2d4'. The 'Application Insights API key' is masked with dots. The 'Application Insights Application ID' is '177d50a7-07db-4cf4-a2c9-1e5cc4b6799e'. At the bottom, 'OAuth Connection Settings' shows 'No settings defined' and an 'Add Setting' button.

4. Enter the following command:

```
PS .:\> Sync-CsOnlineApplicationInstance -ObjectId
<ObjectID>
```

Where <ObjectID> is the ObjectID that was generated from the above command. Note this value for procedure in Step 4-3-2 Set Compliance Recording Policy.

Create New Compliance Recording Policy

This procedure describes how to create a new Compliance Recording Policy.

➤ To create a new compliance recording policy:

1. Enter the following commands:

```
PS .:\> New-CsTeamsComplianceRecordingPolicy -Tenant <TenantID> -Enabled $true
-Description <free text> <ComplianceRecordingBot_PolicyName>
```

- <TenantID>: Azure tenant ID of customer's Microsoft Azure subscription (Microsoft App ID)

- **<ComplianceRecordingBot_PolicyName>**: User-defined name of the Compliance Recording Policy
- **Example:**

```
New-CsTeamsComplianceRecordingPolicy -Tenant ad41d6c3-67f0-47cc-9de3-e07fd185c1c7 -Enabled $true -Description "Test policy created by admin" smarttap5v3stln2
```

2. After 30-60 seconds, the policy should be displayed. Enter the following command to verify that your policy was added correctly:

```
PS ..\> Get-CsTeamsComplianceRecordingPolicy <ComplianceRecordingBot_PolicyName>
```



For more information, refer to: [Create New Compliance Recording Policy](#)

Set Compliance Recording Policy

This procedure describes how to set the Compliance Recording policy.

➤ To set the Compliance Recording Policy:

1. Enter the following commands:

```
PS ..\> Set-CsTeamsComplianceRecordingPolicy -Tenant <TenantID> - Identity <ComplianceRecordingBot_PolicyName> -ComplianceRecordingApplications ` @(New-CsTeamsComplianceRecordingApplication -Tenant <TenantID> - Parent ComplianceRecordingBot -Id <ObjectID>) -<policy-based recording application behavior> $true/false
```

- **<TenantID>**: Azure tenant ID of customer's Microsoft Azure subscription (Microsoft App ID)
- **<ComplianceRecordingBot_PolicyName>**: User-defined name of the Compliance Recording Policy that was defined in Step 4-3-1 Create New Compliance Recording Policy
- **<ObjectID>**: Object ID that was generated in Step 4-2 Create Application Instance
- **<policy-based recording application behavior>**: \$true/false

Where <policy-based recording application behavior> is one of the following:

- ◆ **RequiredBeforeCallEstablishment (default: false):** Indicates whether the policy-based recording application must be in the call before the call is allowed to establish. If this is set to True, the call will be cancelled if the policy-based recording application fails to join the call. If this is set to False, call establishment will proceed normally if the policy-based recording application fails to join the call.
- ◆ **RequiredBeforeMeetingJoin (default: false):** Indicates whether the policy-based recording application must be in the meeting before the user is allowed to join the meeting. If this is set to True, the user will not be allowed to join the meeting if the policy-based recording application fails to join the meeting. The meeting will still continue for users who are in the meeting. If this is set to False, the user will be allowed to join the meeting even if the policy-based recording application fails to join the meeting.
- ◆ **RequiredDuringCall (default: false):** Indicates whether the policy-based recording application must be in the call while the call is active. If this is set to True, the call will be cancelled if the policy-based recording application leaves the call or is dropped from the call. If this is set to False, call establishment will proceed normally if the policy-based recording application leaves the call or is dropped from the call.
- ◆ **RequiredDuringMeeting (default: false):** Indicates whether the policy-based recording application must be in the meeting while the user is in the meeting. If this is set to True, the user will be ejected from the meeting if the policy-based recording application leaves the meeting or is dropped from the meeting. The meeting will still continue for users who are in the meeting. If this is set to False, the user will not be ejected from the meeting if the policy-based recording application leaves the meeting or is dropped from the meeting.
- ◆ **Priority:** Determines the order in which the policy-based recording applications are displayed in the output of the Get-CsTeamsComplianceRecordingPolicy cmdlet.
- ◆ **ConcurrentInvitationCount:** Determines the number of invites to send out to the application instance of the policy-based recording application.
- ◆ **Example:**

```
Set-CsTeamsComplianceRecordingPolicy -Tenant ad41d6c3-67f0-47cc-9de3-e07fd185c1c7 -Identity smarttap5v3stln2 -ComplianceRecordingApplications ` @
(New-CsTeamsComplianceRecordingApplication -Tenant ad41d6c3-67f0-47cc-9de3-e07fd185c1c7 -Parent smarttap5v3stln2 -id 0535d120-cded-4305-a6ef-3e2dbb77c12e)
```

- ◆ Set application behavior to False to avoid disconnection of the calls if Bot fails to join:

```
Set-CsTeamsComplianceRecordingApplication -Identity 'Tag:smarttap5v3stln/ID' -
RequiredBeforeCallEstablishment $false -RequiredDuringCall $false -
RequiredBeforeMeetingJoin $false -RequiredDuringMeeting $false
```

2. After 30-60 seconds, the policy should be displayed. Enter the following command to verify that your policy was updated correctly:

```
PS .:\> Get-CsTeamsComplianceRecordingPolicy <ComplianceRecordingBot_  
PolicyName>
```



For more information, refer to [Set Compliance Recording Application](#)

Grant the Policy to a Recorded User

This procedure describes how to grant policies to a single recorded user and to grant policies to a Security Group containing multiple users.

➤ To grant policies to a single recorded user:

- Enter the following commands:

```
PS .:\> Grant-CsTeamsComplianceRecordingPolicy -Identity <Identity> -PolicyName  
ComplianceRecordingBot -Tenant <TenantID>
```

Where:

- Identity: UPN of recording-targeted user
- <TenantID>: Azure tenant ID of customer's Microsoft Azure subscription (Microsoft App ID)



For more information, refer to <https://docs.microsoft.com/en-us/powershell/module/skype/grant-csteamscompliancerecordingpolicy?view=skype-ps>

➤ To apply policies to a Security Group:

1. Install the following modules before applying the policy:

```
Install-Module -Name  
MicrosoftTeams
```

Or

```
Update-Module  
MicrosoftTeams
```

2. Connect to the module:

```
Connect-  
MicrosoftTeams
```

3. Retrieve Active Directory users:

```
Connect-  
AzureAD
```

4. Assign the policy to a Security group as shown in the example below:

```
New-CsGroupPolicyAssignment -GroupId cbc58572-7d1f-409f-bc7d-525a9718e299 -  
PolicyType TeamsComplianceRecordingPolicy -PolicyName "STTeamsbotstandart1b2"-  
Rank 1
```



Refer to the following link: <https://docs.microsoft.com/en-us/microsoftteams/assign-policies>

16 SmartTAP Alarms

Alarm – Component Unreachable

Alarm Field	Description		
Description	<p>This alarm is raised in the following circumstances:</p> <ul style="list-style-type: none">■ The OVOC Main Agent is unable to connect to one of the OVOC Client agents. Note that currently the Client agent is only installed on the SmartTAP application server.■ The SmartTAP Application server is unable to connect to the SmartTAP Web Admin Interface		
SNMP Alarm	acVAManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.1		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	The OVOC Main Agent is unable to connect to one of the installed OVOC Client agents. AudioCodes_CS; CallDelivery-IP; HealthMonitorSvc ; AudioCodesMPSSvc; HPXMEDIA; RemoteTransferService; AcProcDump ; CallDeliverySR; CallDelivery;CallDeliveryLD; CallDeliveryAES; SmartTapMonitoringSvc	Unable to connect to client agent on <SmartTapAS_ FQDN>	
	The SmartTAP Application server is unable to connect to the SmartTAP Web Admin interface.	Unable to Connect to Voice Application Admin	
Cleared	OVOC Client agent is re-available		

SmartTAP Event – Component Restart

Alarm Field	Description		
Description	This event is raised when the SmartTAP Application server has been restarted.		
SNMP Alarm	acVAManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.2		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	The SmartTAP Application server has been restarted. AudioCodes_CS; CallDelivery-IP; HealthMonitorSvc;	Component <SmartTap AS FQDN> restarted	-

Alarm Field	Description		
	AudioCodesMPSSvc; HPXMedia RemoteTransferService; AcProcDump CallDeliverySR; CallDelivery; CallDeliveryLD; CallDeliveryAES; SmartTapMonitoringSvc		

Event – Component Resource Failed

Alarm Field	Description		
Description	<p>This event is raised in the following circumstances:</p> <ul style="list-style-type: none"> The allocation of resources for recording licenses has been exceeded Media Server management has failed 		
SNMP Alarm	acVaCompResFailedEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.9		
Alarm Source	<p>SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following:</p> <ul style="list-style-type: none"> Licenses: <ul style="list-style-type: none"> imLicQuotaExceeded videoLicQuotaExceeded userLicQuotaExceeded mediaFwdLicQuotaExceeded licUnavailable Media Server Resource Failure: <ul style="list-style-type: none"> Hmp - channelResourceFailure Hmp createFileFailed Hmp bindingFailure Hmp rtsTransferFailed Hmp writeFileFailed 		
Alarm Title	Component Resource Error		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition (related resource indicated in parenthesis)	<text>	Corrective Action
Major	The quota for the number of users targeted for Instant Messaging has been exceeded (imLicQuotaExceeded).	IM target quota exceeded	Reduce the number of users/devices targeted for Instant Messaging recording or purchase additional licenses.
Major	The quota for the number of users targeted for video has been exceeded (videoLicQuotaExceeded).	video target quota exceeded	Reduce the number of users/devices targeted for video recording or purchase additional licenses.
Major	The quota for the number of users/devices targeted for audio recording has been exceeded (userLicQuotaExceeded).	Audio User target license exceeded	Reduce the number of users/devices targeted for audio recording or purchase additional licenses.
Major	The quota for the number of users/devices targeted for audio recording has been exceeded (mediaFwdLicQuotaExceeded).	Recording license exceeded	Reduce the number of users/devices targeted for audio recording or purchase additional licenses.
Major	No license is available. All licenses are currently consumed (licUnavailable).	-	-

Alarm Field	Description		
Major	The Media server failed to create a channel resource (Hmp - channelResourceFailure).	Media server failed to create channel resource	-
Major	The Media Server failed to write to disk (Hmp createFileFailed).	-	Check available disk space. Check that Media Server has read/write permissions on the local disk.
Major	Media Server cannot bind to ports in order to open media channels (Hmp bindingFailure).	-	Verify that other applications are not using UDP ports in the range of 40000 – 50000. Restart Media Server.
Warning	Transfer Server failed to copy files from temporary, local recording location to remote storage (Hmp rtsTransferFailed).	Transfer service failed to copy	Verify that the Remote Transfer Service is running with permissions that grant it read/write access to the media storage volume.
Major	The Media server failed to create a file with recorded media (Hmp writeFileFailed)	Media server failed to create a file	Check available disk space. Check that Media Server has read/write permissions on the local disk.

Alarm - Component Resource Threshold Exceeded

Alarm Field	Description		
Description	<p>This alarm is raised when one of the SmartTAP component resources listed below has reached its pre-defined threshold. This alarm applies for the following resources:</p> <ul style="list-style-type: none"> ■ Recording license notification thresholds (for all recording license types) triggered according to the configuration in the SmartTAP Web interface License screen. ■ Media Storage notification thresholds triggered according to the configuration in the SmartTAP Web interface Storage Statistics screen. 		
SNMP Alarm	acVaResourceThresholdAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.11		
Alarm Source	<p>SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following:</p> <ul style="list-style-type: none"> ■ SmartTAP License Threshold Notification value (for all recording license types) ■ Media Storage Notification Threshold value 		
Alarm Title	Alarm - Component Resource Threshold Exceeded		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	The media storage location threshold has been reached.	Media Storage threshold	<ul style="list-style-type: none"> ■ Verify the Notification Threshold setting configuration in the Storage Statistics screen. It's possible that there is sufficient storage and that the threshold needs to be adjusted. ■ Add additional storage capacity to the file server to support additional media files (recordings). The file server is external to SmartTAP.
	License threshold exceeded	licThresholdExceeded	<ul style="list-style-type: none"> ■ Verify the Notification Threshold setting configuration in the License screen. It's possible that there are sufficient licenses and that the threshold needs to be adjusted. ■ Purchase additional recording licenses
Cleared	When counter returns below the threshold level.	-	-

Alarm – Connection Failure

Alarm Field	Description	
Description	This alarm is raised in the following circumstances: <ul style="list-style-type: none"> ■ The connection between one of the SmartTAP components and the SmartTAP Application server is down. ■ The connection between other SmartTAP components is down. 	
SNMP Alarm	acVaConnectionFailureAlarm	
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.12	
Alarm Source	<SmartTAPComponent>@ <FQDN>: <ul style="list-style-type: none"> ■ AC-MediaProxy @<FQDN> ■ AC-Announcement @ <FQDN> ■ CS@ <FQDN> ■ CD-IP@ <FQDN> ■ CD-SIPREC@ <FQDN> ■ MediaDelivery@ <FQDN> ■ Media Server@<FQDN> ■ AC_HealthMonitor@ <FQDN> ■ AC-Plugin@ <FQDN> ■ RTS@ <FQDN> 	
Alarm Title	Alarm – Connection Failure	
Alarm Type	Other	
Probable Cause	Other	
Additional Info	-	
Alarm Severity	Condition	Corrective Action
Critical/Major/Warning	Communication between SmartTAP component and SmartTAP Application server is down	Communication Down Details: Managed Device <SmartTAPComponent>@<HostNameFQDN> failed to send heartbeat within specified time of <xxmS>. Device Infold: <SmartTAPInternalID>HostNameType: COM_SERVERDisplay Name: <HostName>Last heartbeat received on <yyyy-mm-dd> <hh:mm>
	Connection from CallDelivery to lyncPlugInServerConnDown	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to FE Plug-using TCP
	Connection from CallDelivery to lyncPlugInSWConnDown	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to SmartWorks Plug-using TCP
	Connection from CallDelivery to communication server	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to communication server Plug-using TCP
	Connection from CallDelivery to Media delivery	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to Media delivery using TCP
	Connection between Media Proxy and Calldelivery	Communication Down Details: Call Delivery at <HostNameFQDN> lost connection to AC-MediaProxy using TCP
	Connection from lync Plugin to Media Proxy	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to AC-MediaProxy using TCP
	Connection from lync Plugin to CallDelivery	Communication Down Details: AC-Plugin at

Alarm Field	Description	
		<HostNameFQDN> lost connection to Call Delivery at <HostNameFQDN> using TCP
	Connection from Lync plugin to ann	Communication Down Details: AC-Plugin at <HostNameFQDN> lost connection to Announce-ment Server at <HostNameFQDN> using TCP
Cleared	-	The connection is up again -

Call Recording Error Event

Alarm Field	Description		
Description	This event is raised when errors are reported by the Health Monitor to the SmartTAP Application server.		
SNMP Alarm	acVaCallRecordingErrorEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.13		
Alarm Title	Call Recording Error Event		
Alarm Source	SmartTAPAS_FQDN		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Major	One of the following Health Monitor services reported an error to the SmartTAP Application server	as below	
	NoMediaFile(301)	Call not recorded or recorded with errors	Check ST configuration and health
	NoFileOnDisk(302)	Call not recorded or recorded with errors	Check ST configuration and health
	TestCallWarning(303)	Call not recorded or recorded with errors	Check ST configuration and health
	TestCallNotRecorded(304)	Call not recorded or recorded with errors	Check ST configuration and health
	FileXferFailed(204)	Error: Can't upload file to blob	<ul style="list-style-type: none"> Check Media location configuration in SmartTAP Check Azure Blob accessibility and health
	ComplianceRecordedButNotAssignedToRecProfile(209)	User is targeted but has no recording profile in ST	Assign Recording Profile to user under Compliance Recording Policy
	JoinCallFailed(210)	Bot failed to join the call	<ul style="list-style-type: none"> Check Service Fabric Cluster health Verify MSFT Graph API accessibility and responsiveness
Major	CdrRecoveryFailed(450)	Call Recovery Failed, file <path> has exceeded the allowed failure threshold.	Check SmartTAP and CD-Live configuration
Major	CdrRecoveryFailed(450)	Call Recovery Failed with status	Check faulty CDR file

Alarm Field	Description		
		code <statusCode>, file <path>	

Alarm – Certificate Expired

Alarm Field	Description		
Description	This alarm is raised when one of the Microsoft Windows-certificates installed on the SmartTAP Application server is about to expire.		
SNMP Alarm	acVaCompCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.27		
Alarm Source	SmartTapAS_<FQDN>		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Raised when the certificate will expire in less than two days	Certificate will expire in <days left> days	Verify which certificate is about to expire and renew it.
Major	Raised when the certificate will expire in less than 30 days.	Certificate will expire in <days left> days	Verify which certificate is about to expire and renew it.
Cleared	When certificate is renewed	-	-

Alarm – Component Event Viewer Dropped

Alarm Field	Description
Description	This alarm is raised when events from the Event Viewer are dropped after the sending rate threshold has been exceeded; preventing a burst of events being raised for a specific component.
SNMP Alarm	acVaCompEventViewerDropped
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.26
Alarm Source	N/A
Alarm Title	Component Event Viewer Dropped
Alarm Type	Other
Probable Cause	Other
Alarm Text	Events from Event Viewer dropped due to high sent rate
Additional Info	-
Alarm Severity	Indeterminate

Alarm – Component Performance Counter General

Alarm Field	Description
Description	This alarm is raised when the generic performance counter on the SmartTAP Application server has reached a pre-defined threshold for memory/CPU/disk.

Alarm Field	Description		
SNMP Alarm	acVACompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.21		
Alarm Source	SmartTapAS_<FQDN>/<Performance Monitor Group>/<Performance Monitor Name>/<NetworkAdapterName>		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup>/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>	-
Major	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup>/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>	-
Warning	Pre-defined severity per counter type.	GeneralCounter performance counter <PerformanceCounterGroup>/<PerformanceCounterName>/<NetworkInterfaceName>is Above threshold <thresholdlevel>	-
Cleared	When counter returns below the threshold level.	-	

Alarm – Component Service Status

Alarm Field	Description
Description	This alarm is raised when a component service on the SmartTAP Application server is down. These services include SmartTAP components, for example, HealthMonitorSvc and core Windows components, for example, AcProcDump.
SNMP Alarm	acVaCompSrvAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.23
Alarm Source	SmartTapAS_<FQDN>/<servicename> is one of the following: <ul style="list-style-type: none"> ■ AudioCodes_CS ■ MySQL ■ CallDelivery-IP ■ HealthMonitorSvc ■ AudioCodesMPsSvc ■ HPXMedia ■ RemoteTransferService ■ AcProcDump ■ CallDeliverySR ■ CallDelivery ■ CallDeliveryLD ■ CallDeliveryAES ■ SmartTapMonitoringSvc
Alarm Title	Component Service Status

Alarm Field	Description		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	-
Cleared	Service is running	SERVICE_RUNNING	
Note: the severity is determined according to the service's importance to system functionality.			

Alarm – Disk Space

Alarm Field	Description		
Description	This alarm is raised when the server disk space on the SmartTAP Application Server drive is above the pre-defined threshold.		
SNMP Alarm	acVaDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.28		
Alarm Source	SmartTAPAS_<FQDN>/DriveName:\\		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.	-	-

Event – Configuration Error

Alarm Field	Description		
Description	<p>This event is raised under the following circumstances:</p> <ul style="list-style-type: none"> ■ A user is mapped to two or more Retention Policies groups via AAD mapping. In this case, the user is not assigned to any retention policy. ■ A user is mapped to two or more Recording Profile groups via AAD mapping. In this case, the user is not be assigned to any recording profile. ■ Problems with Azure Storage account configuration 		
SNMP Alarm	acVaConfigErrorEvent		
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.14		
Alarm Source	<n><un> (where n is the name of the component or ip:port and un is the user name)		
Additional Information	<ul style="list-style-type: none"> ■ User xxx will not be recorded. A user can not be assigned to two or more AAD groups that are mapped to recording profiles in SmartTAP. Please make sure the user is assigned to one AAD group that is mapped to a recording profile. ■ User xxx is not assigned to a mapped retention policy and will be assigned to the default retention policy. A user can not be assigned to two or more AAD groups that are mapped to retention policies in SmartTAP. Please make sure the user is assigned to one AAD group that is mapped only when mapping retention policies. 		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Major	A user cannot be assigned to multiple AAD groups for Recording Profiles.	Failed to assign a Recording Profile to a user	Check AAD Configuration
Major	A user cannot be assigned to multiple AAD groups for Retention Policies.	Failed to assign a Retention Policy to a user	Check AAD Configuration
Major	Failed to assign a recording location to a Teams Bot node	A recording location is not assigned for Teams Bot node <src>.	Check Recording Location Configuration
Major	Metadata Container does not exist in Storage Account	Container <containerName> was not found in <storageName> Storage.	Check Storage Account Configuration
Major	Metadata Container is Immutable and cannot be used.	Container <containerName> in Storage <storageName> is Immutable and cannot be used.	Check Storage Account Configuration

Recording Resource Failure

Alarm Field	Description
Description	This alarm is raised when the recording resource is not available
SNMP Alarm	acVaRecordingResourceFailureAlarm
SNMP OID	1.3.6.1.4.1.5003.9.40.3.2.0.15
Alarm Title	Recording Resource Failure
Alarm Source	<ul style="list-style-type: none"> ■ botNodeName@botclusterFQDN

Alarm Field	Description		
	■ botCluster@botclusterFQDN		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	Text	Corrective Action
Critical	RecordingClusterNotAvailable (Teams Bot cluster is not available): The cluster is overloaded and further calls won't be recorded.	Teams Bot cluster - no recording resource available Alarm.	Increase cluster size immediately.
Warning	RecordingNodeNotAvailable (Teams Bot node is not available): The reporting node is overloaded, bot is still might record further calls if there is another node which is not overloaded.	Teams Bot node - no recording resource available Alarm.	Monitor the system if more than 60% percent of the nodes are overloaded, consider increasing cluster size.
Cleared	Teams Bot node is available again	Teams Bot node - no recording resource available Cleared.	
Cleared	Teams Bot cluster is available again	Teams Bot cluster - no recording resource available Cleared.	

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>

©2021 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-27179

