

SmartTAP 360°

SmartTAP 360° Enterprise Recording Solution

Version 5.6

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: July-18-2023

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 are used interchangeably in this document unless specified otherwise. References to Microsoft Teams are explicitly indicated.

Related Documentation

Document Name
SmartTAP 360° Release Notes
SmartTAP 360° Installation Guide
SmartTAP 360° Hardware and Software Requirements
SmartTAP 360° for Microsoft Teams Deployment Guide
SmartTAP 360° Genesys Integration 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° 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°; 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</p>

LTRT	Description
	<p>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 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
27178	<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°; 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>
27179	Update the Server requirements.
27602	<p>Updated Section: Features Overview; Architecture; Managing Licenses; SmartTAP Alarms; Adding a Recording Profile; Configuring OVOC Connection; Managing Recording Locations; Viewing Managed Devices; Managing Certificates; Managing Security Profiles; Save on Demand Call Retention; Managing Calls; Playing Back Recorded Media; Managing Recording Profiles; Managing Users; Managing Devices; Adding an LDAP Configuration; LDAP</p>

LTRT	Description
	<p>Active Directory Mapping</p> <p>Added Section: View or Modify User Attributes; Managing Analytics Profiles; Analytics; Retrieving Recording Queue Instances; Azure Active Directory Media Location Mapping; Azure Active Directory Analytics Mapping; Downloading Call Transcripts</p> <p>Removed Section: Inter-Components Communication.(merged with Viewing Managed Devices); Configuring a Digital Signature (see Managing Certificates); Microsoft Azure Active Directory; Integrate SmartTAP Personal App in Teams; Enable Users with Compliance Recordings</p>
27603	<p>Added Section: User Settings; Call Transfer Information; Delegating Teams Calls; On-Demand Recording; Search by Analytics Category; Search by Analytics Sentiment</p> <p>Updated Section: Managing Analytics Profiles; Features Overview; Managing Calls; Searching for Calls; Retention Policies; Step 4 Configure OpenID Connect OIDC Client; Configuring Recording Format; Managing Licenses; Adding Media Storage Recording Locations; Viewing and Modifying a Recording Location; HTTPS Certificate; Loading Web Browser Certificate; Analytics; Run Recording Policy Script; Specific Considerations for Microsoft Teams Instant Messages</p>
27604	<p>Descriptions updated in Adding a Recording Profile.</p>
27605	<p>Updated Section: Features Overview; Azure Active Directory User Mapping; Azure Active Directory User Authentication; Run Recording Policy Script; Features Overview; Adding a Recording Profile; Adding a Media Storage Recording Location; Setup Microsoft Blob Storage account renamed to Setup Microsoft Azure Blob Storage Account-Recordings and updated; Monitoring Storage Statistics; Configure User Login Authentication; Managing Analytics Profiles; Analytics; Microsoft Teams Instant Messages; Microsoft Teams Integration; Updated SmartTAP Alarm Component Resource Threshold Exceeded; Upload Existing Certificates</p> <p>Removed references to Microsoft Lync</p> <p>Added Section: Setup Microsoft Azure Blob Storage Account-Analytics</p>
27606	<p>Update to Section "Adding a Recording Profile".</p>

Table of Contents

1	About SmartTAP 360°	1
	SmartTAP 360° Benefits	2
	Competitive Advantages	2
	Features Overview	3
	Architecture	12
	About this Guide	13
Part I		14
	Getting Started	14
2	Logging In	15
	Logging in with Microsoft Office 365 Credentials	15
3	Performing Initial Configuration	18
	Getting Acquainted with the Web Interface	19
	Determining User/Device Status	21
4	Testing the Initial Configuration	26
	Making Sure a Recording is in Progress	26
	Listening to a Recording and Viewing a Video	26
Part II		28
	User Configuration	28
5	Sending Email	29
6	Managing Groups	31
	Adding Recording Group	31
	View and Modify Recording Groups	32
7	Managing Security Profiles	35
	Adding a Security Profile	35
	Configure Permissions in a Security Profile	37
8	Managing Recording Profiles	40
	Adding a Recording Profile	40
	Viewing or Modifying Recording Profiles	48
	Assigning Recording Profile to User or Device	49
	Recording Profile-Call Type Configuration Examples	52
	Retrieving Recording Queue Instances	53
9	Managing Call Retention	58
	Configuring Call Retention	58
	Adding Call Retention Policy	58
	Viewing or Modifying a Retention Policy	59
	Save on Demand Call Retention	60

10	Managing Analytics Profiles	62
	Add Analytics Categories	62
	View and Modify Analytics Categories	66
	Add Analytics Profile	67
	View and Modify Analytics Profile	69
	Add Users to Analytics Profiles	70
11	Managing Devices	73
	Add Recordable Device	73
	Viewing and Modifying Recordable Devices	74
	Adding a Device Attribute	76
	Adding a Device Attribute for Recording	78
	Viewing and Modifying Device Attributes	79
12	Managing Users	81
	Adding a User	83
	View and Modify Users	85
	Update an Admin User	88
	Adding a User Attribute	90
	Adding a Microsoft Teams AAD User Attribute	92
	View and Modify User Attributes	94
	Modify a User Password	95
	Uploading a User Image	96
	Set Time and Language	97
13	Skype for Business Features	98
	SmartTAP 360° Skype for Business Toolbar	98
	Toolbar Features	98
	Announcement Server (Skype for Business)	100
	Simple Announcement	101
	IVR	101
	Configuring IVR Script Files	102
	Enabling Text-to-Speech Platform	103
	Consent to Record Calls	103
	Example Announcement Server Scenarios	106
	PSTN and Federated Calls	106
	All Inbound Calls	107
	Announcement Server Advanced Call Scenarios	108
	Announcement Server Configuration Parameters	111
14	Managing Calls	116
	Searching for Calls	119
	Search by Date	126
	Searching by Users and Devices	127
	Calling Parties Search	128
	Search by Call Tags	128

Search by Analytics Category	130
Search by SysCall ID	133
Search by Analytics Sentiment	133
Saving Search Queries	136
Deleting Calls and Instant Messages	137
Call Transfer Information	138
Delegating Teams Calls	139
Playing Back Recorded Media	141
Listening to Call and Viewing Call Video	143
Managing Microsoft Teams Video Calls	146
Viewing and Playing Back Transcripts	147
Skype for Business and Teams Video and Screen Sharing	149
Timeline View	151
Downloading Call Recordings	156
Downloading an Audio Call	156
Downloading Video Call	158
Downloading Video and Screen Sharing Call	159
Downloading Call Transcripts	162
Emailing Call Recordings	163
Using Call Tagging	165
Adding a Call Tag	166
Viewing / Deleting a Call Tag	167
Assigning Values to a Call Tag and Applying to Call	168
On-Demand Recording	169
15 Managing Instant Messages	171
Searching for Messages	173
Microsoft Teams Instant Messages	180
16 Using the Evaluation Feature	182
Adding a New Evaluation Form	183
Viewing and Copying an Evaluation Form	185
Adding a New Section [Evaluation Forms]	186
Adding Questions and Answers to an Evaluation Form	187
Finalizing Forms	190
Performing an Evaluation	191
Part III	200
System Configuration	200
17 Viewing/Searching an Audit Trail	201
Exporting an Audit Trail	203
18 Managing Licenses	204
Licenses for Other Integrations	206
License Configuration Parameters	208

Assign Licenses	209
Assign Analytics Licenses	210
19 Device Management	212
Viewing Managed Devices	212
Adding a Device Manually to the Application Server	215
20 Recording Health Monitor	216
General Configuration	216
REST API Configuration	218
Report Formats	219
21 Monitoring Storage Statistics	221
22 Configuring OVOC Connection	225
Whitelisting Certificate Files	229
23 Alarms	233
Alarm History	233
Alarm Notifications	233
Monitoring System Health	235
Windows Event Log	236
SCOM Integration	238
SmartTAP Alarms	239
SmartTAP System Alarms	239
Alarm – Component Unreachable	239
SmartTAP Event – Component Restart	239
Event – Component Resource Failed	240
Alarm - Component Resource Threshold Exceeded	241
Alarm – Connection Failure	242
SmartTAP Agent Alarms	243
Alarm – Component Performance Counter General	243
Alarm – Component Service Status	244
Alarm – Component Event Viewer Dropped	245
Alarm – Certificate Expired	246
Alarm – Disk Space	246
SmartTAP Application Server Alarms	246
Call Recording Error Event	246
Event – Configuration Error	247
Recording Resource Failure	248
24 Managing Certificates	250
Browser Connection Certificate Requirements	250
Generating New Certificates	251
Step 1: Generate Certificate Signing Request (CSR)	251
Viewing/Modifying the Certificate List	253
Step 2: Load New Certificates	254

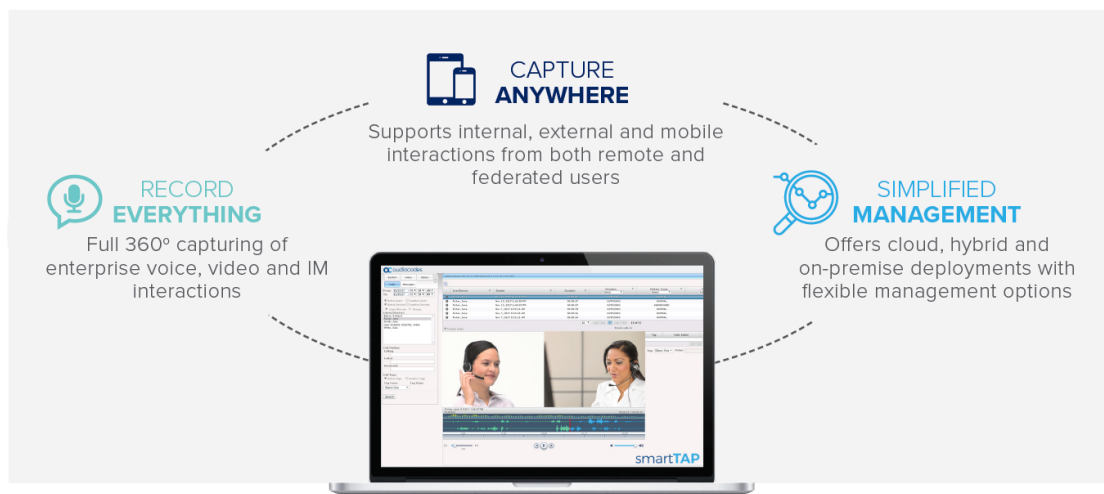
Loading Web Browser Certificate	254
Loading a Digital Signature	256
Upload Existing Certificates	260
25 Configuring Email Server Settings	263
26 Analytics	265
Configure Connection with Microsoft Cognitive Services	265
View and Modify Analytics Configurations	266
27 Managing Recording Locations	268
Adding Media Storage Recording Locations	269
Setup Microsoft Azure Blob Storage Account-Recordings	274
Setup Microsoft Azure Blob Storage Account-Analytics	282
Viewing and Modifying a Recording Location	286
Associating Users to Media Locations	289
Configuring Recording Format	291
Configuring Live Monitoring Location	292
28 Configuring Web Session Timeout	294
29 Single Sign-On for SmartTAP 360°	295
Configuring Single Sign-on in SmartTAP Web Interface	296
Validating SSO	298
Single Sign-On Client Browser Settings	298
Enabling Microsoft Edge Browser with IWA	298
Enabling Firefox Browser with IWA	301
Enabling Chrome Browser with IWA	302
Single Sign-On Variables	303
Configuring Active Directory for Single Sign-On	306
Testing Single Sign-On	309
Troubleshooting Single Sign-On	309
30 Configuring SSL	315
31 Adding an LDAP Configuration	317
32 LDAP Active Directory Mapping	319
Configuring User Mappings	319
Configuring Group Mappings	324
Configuring Security Group Mappings	327
33 Microsoft Teams Integration	331
Managing Access to Microsoft 365	332
Configure Client Secret for Role-based Access (aad-app)	333
Add Permissions for Role-based Access (aad-app)	336
Update OpenID Connect Token (OIDC) Client Configuration	337
Setup SmartTAP OpenID Connect Token Automatically (auth-app)	338
Verify Active Directory Providers Configuration	340

Configure AAD Mapping Profiles	341
AAD Analytics Mapping	342
AAD Media Location Mapping	347
AAD Retention Policy Mapping	352
AAD Recording Profile Mapping	358
AAD Security Profile Mapping	365
AAD User and Group Mapping	372
Setup Microsoft 365 User Sign-in Authentication	378
Configure Client Secret for login-app	378
Verify login-app Permissions	381
View OIDC Client User Login	385
Assign Security Profile to M365 User	386
Integrate SmartTAP Personal App in Teams	391
Create and Register the SmartTAP Personal App	392
Set Microsoft API Permissions for Personal App	394
View OIDC Client User Login	398
Configure and Load Manifest (Personal App)	399
Enable Users with Compliance Recording	408
34 Media Exporter	415
35 API Integration	421

1 About SmartTAP 360°

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° 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° anywhere and any-time they are on Skype for Business calls.

Figure 1-1: SmartTAP 360° Solution



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

System Users Status

Calls

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

☒ Active Users ☐ Inactive Users
☒ Active Devices ☐ Inactive Devices
* Users/Devices:
Users/Devices: ACD, Adir (admin), Tania, Banks (+3056), Eric, Barrett, Lorenzo, Every Phone, Huff, Rosie, Jenkins, Edgar, Somerset Conference Room, Warner, Barbara

Call Parties:
Calling:
Called:
Answered:

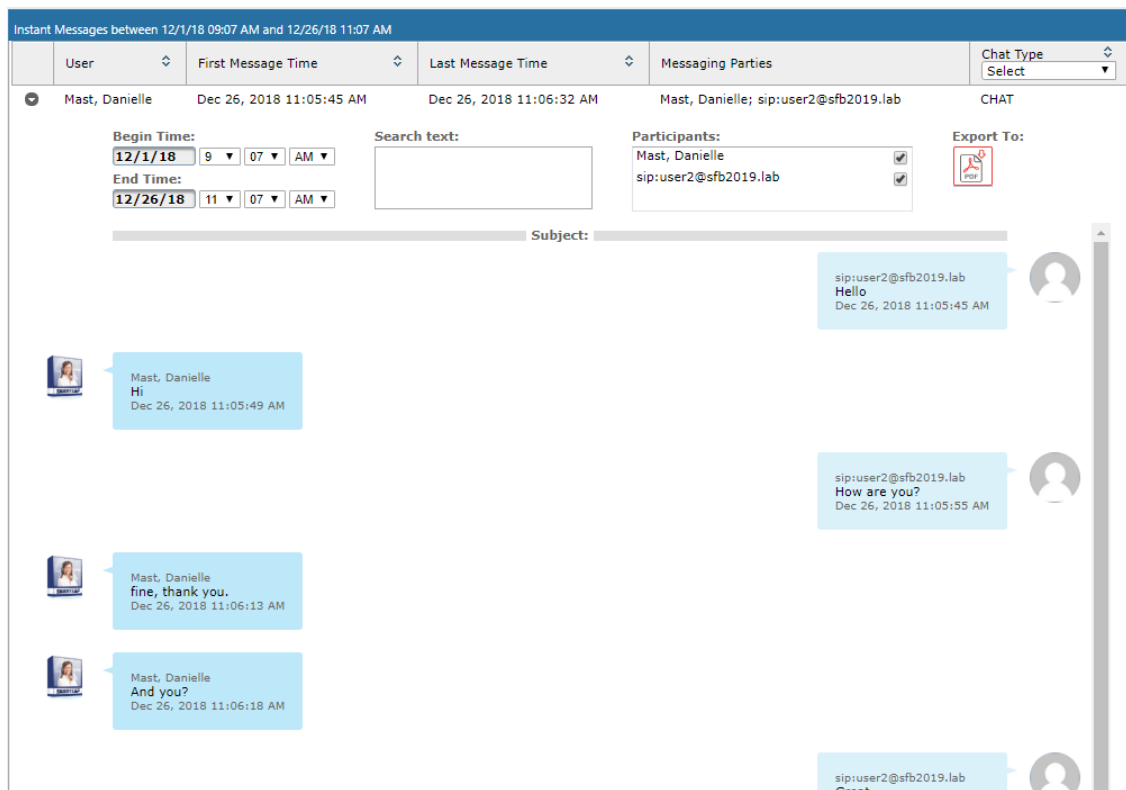
Call Tags:
☒ Active Tags ☐ Inactive Tags
Tag Name:
Tag Value:
Select One:
Search:

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			

Total calls: 4 (1 of 1)

EMEA_Oncall-1 1/19 10:37:09 AM READY

00:00:24 | 00:00:48



SmartTAP 360° Benefits

SmartTAP 360° benefits organizations and enterprises as follows:

- Captures corporate interactions including voice, video, desktop sharing 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° 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° recording features.

Table 1-1: SmartTAP 360° 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

Feature	Details
	manually trigger a recording of another user's calls.
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"> ■ Create and assign to multiple parties to define the recording method. ■ Full Time Recording – Automatic audio or video recording. ■ Record on Demand – Audio recording is manually triggered from the Status page in the Web interface or Skype for Business Conversation Window Extension (CWE) toolbar ■ Save on Demand – Audio or Video recording is manually triggered from the Status page in the GUI or from the Skype for Business CWE toolbar ■ PCI (Payment Card Industry) Pause / Resume Recording (Optional) – Audio recording is manually triggered from the Status page in the GUI or from the Skype for Business CWE toolbar. ■ IM recording – Automatic Instant Message recording.
Security Profiles	<ul style="list-style-type: none"> ■ Creation and assignment to multiple parties to define security access in SmartTAP 360°.
LDAP Integration	<ul style="list-style-type: none"> ■ Allow SmartTAP 360° 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

Feature	Details
	recordings when placed on legal hold.
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.

Feature	Details
Automatic Email Notifications	<ul style="list-style-type: none"> Automatic email notifications when Alarms are triggered or thresholds are exceeded (Recording licenses or 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: agent evaluations, review evaluations, and reports can be generated.
Distributed Architecture	<ul style="list-style-type: none"> One SmartTAP 360° may be deployed across multiple physical locations. Recording on remote locations is not interrupted even if connection to main site is down.
Multiple Call Protocols and Physical Interfaces Share the Same UI	<ul style="list-style-type: none"> One SmartTAP 360° server is capable of recording diverse call signaling and voice protocols. SmartTAP 360° records PSTN, Microsoft Teams/Skype for Business, 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° GUI or Skype for Business client toolbar after validation of their

Feature	Details
	<p>SmartTAP 360° security profile and authentication of their credentials with LDAP Active Directory.</p> <ul style="list-style-type: none"> ■ For Microsoft Team clients: Single Sign-on is supported for logging onto the SmartTAP 360° Personal App. See Integrate SmartTAP Personal App in Teams on page 391.
.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°) 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° 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° 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,

Feature	Details
	<p>allowing SmartTAP 360° to capture a copy of the SRTP conversation.</p> <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° 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°, i.e., Ext, Tel URI, Address, etc., for informational purposes only. Designates to SmartTAP 360° what to use to trigger recording, i.e., adds a SIP_URI attribute and provides a value assigned to the user. If the user makes a SIP call, SmartTAP 360° triggers a recording based on the SIP_URI. Mapping Active Directory attributes to user / device information on SmartTAP 360°. Mapping Microsoft Azure Active Directory Teams users object ID to user properties on SmartTAP 360°.
Automatic Instant Message Recording	<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° User interface design and layout has been updated to the look and feel for AudioCodes product family.
Call Type-based recording	It is now possible to define specific call types to be recorded through SmartTAP 360° recording profiles. For example, it is possible to select recording of the following call types: in domain, PSTN, external, response group calls and more.
Selective Announcement service	The Announcement service can be enabled for recording profile and activated on calls for the users that are associated with the recording profile.
Beep tone generation	Playing recording beep tone to the local call parties is possible with SmartTAP 360° Media Proxy.
Test calls 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° inter-components communication status shows the statuses reported by managed devices for its connections with other components in the system.
Malicious call recording enhancement	Enables users to save a call recording after the call was ended for a predefined time.
OVOC Management	SmartTAP 360° server components can be monitored from OVOC (starting from OVOC version 7.6.100) including the sending of alarms and statuses.
Support for Skype For Business 2019	SmartTAP 360° Announcement and Application servers can be installed on the Skype For Business 2019 platform.
Original Call Reason	Original call release reason is presented as part of the call recording meta-data.
Scalability	SmartTAP 360° SIPRec solution scalability enhancement with an option to reroute a call to another recording server when

Feature	Details
	the server is at the maximum capacity.
SmartTAP 360° low-end Profile	SmartTAP 360° 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° interface supports the following languages:</p> <ul style="list-style-type: none"> ■ English ■ German ■ Spanish ■ French
Personal App in Microsoft Teams	SmartTAP 360° 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.
Voice Call Transcriptions	SmartTAP 360° for Teams supports enables transcription of recorded voice calls to quickly retrieve important segments of the call rather than listening to the entire call. The full call transcription can be enabled for users or groups of users defined locally or mapped from AAD. Generated transcriptions can be downloaded or exported through Rest API.
Media Storage dispersed across Multiple Locations	User recordings can be stored in multiple regions or countries defined by the customer and required by local regulations while working in parallel with a centralized application for configuration and recording playback. Multiple types of storage are supported including Azure Blob storage, SMB, and local storage. Association to a media location is user-based and can be mapped to AAD groups. This ensures the local integrity of stored recorded data together with a secure connection to the central database.
Analytics	Configuration of Analytics Profiles for Interaction analytics of voice to gather business insights. For example, Speech analytics involves analyzing the voice interactions with voice recognition and other cognitive services including transcription, keyword and phrase spotting, categorization

Feature	Details
	and sentiment analysis.
On Demand Recording in Active Active Setup	SmartTAP for Teams users utilizing the double recording solution can trigger on demand recording from one system and applied it to both systems.simultaneously.
Compliance Recording Policy	Create recording policies for the users in the recording group on the customer's Azure tenant. PowerShell script automation allows the recording policy to be assigned to specific users or directly to the Azure groups. Script features include the ability to enable audio notifications for PSTN call commencement and to disable calls in case call recording functionality fails.

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

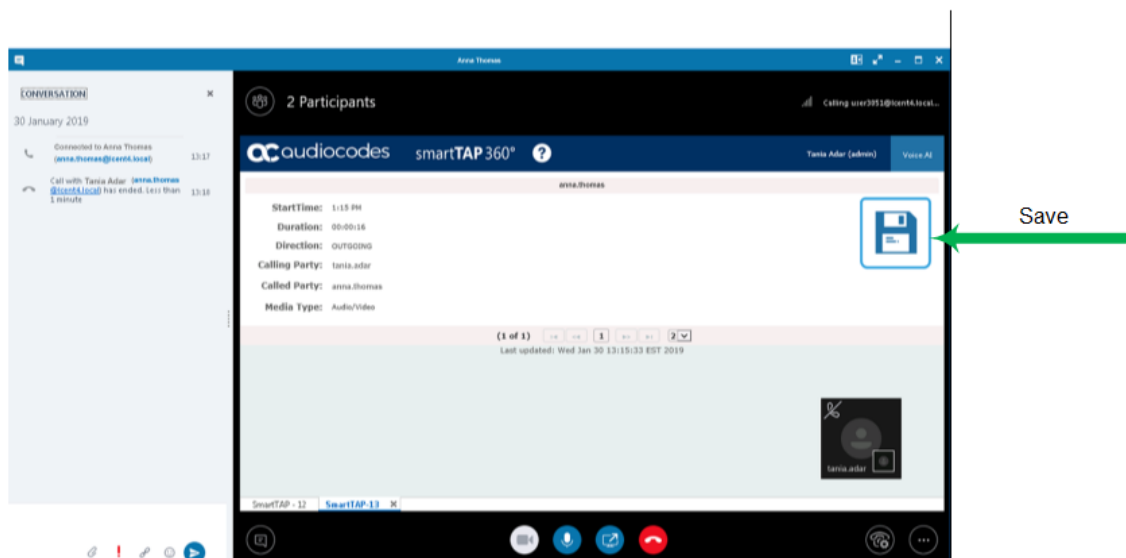


Figure 1-3: Record on Demand (ROD) in SmartTAP 360° Skype for Business Client

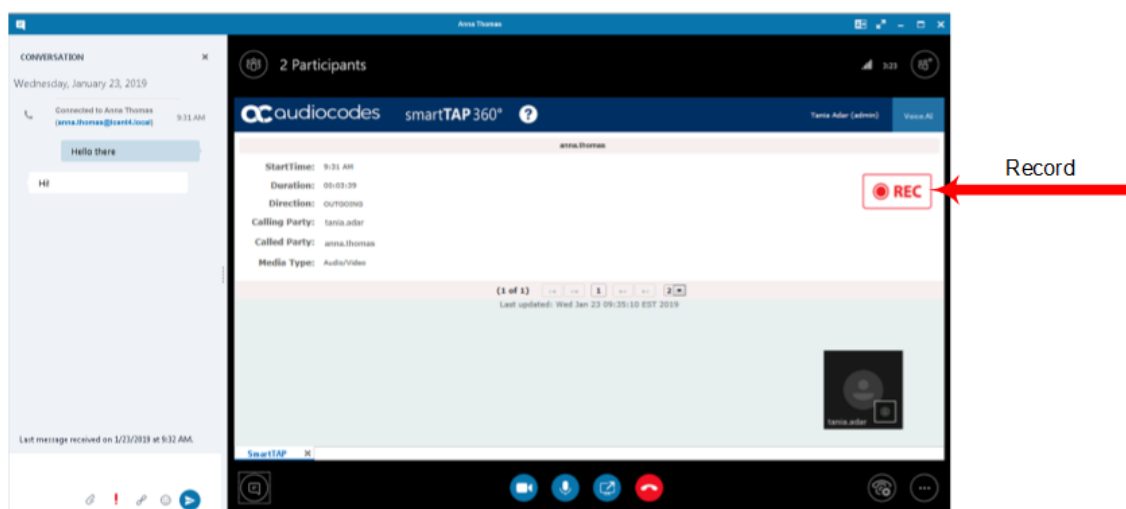
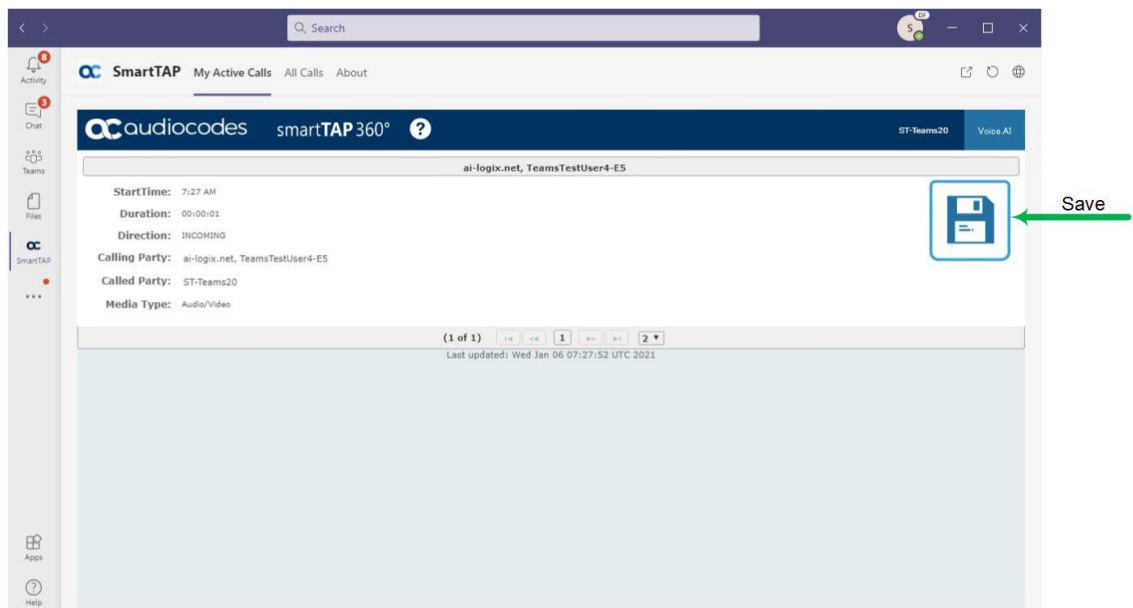
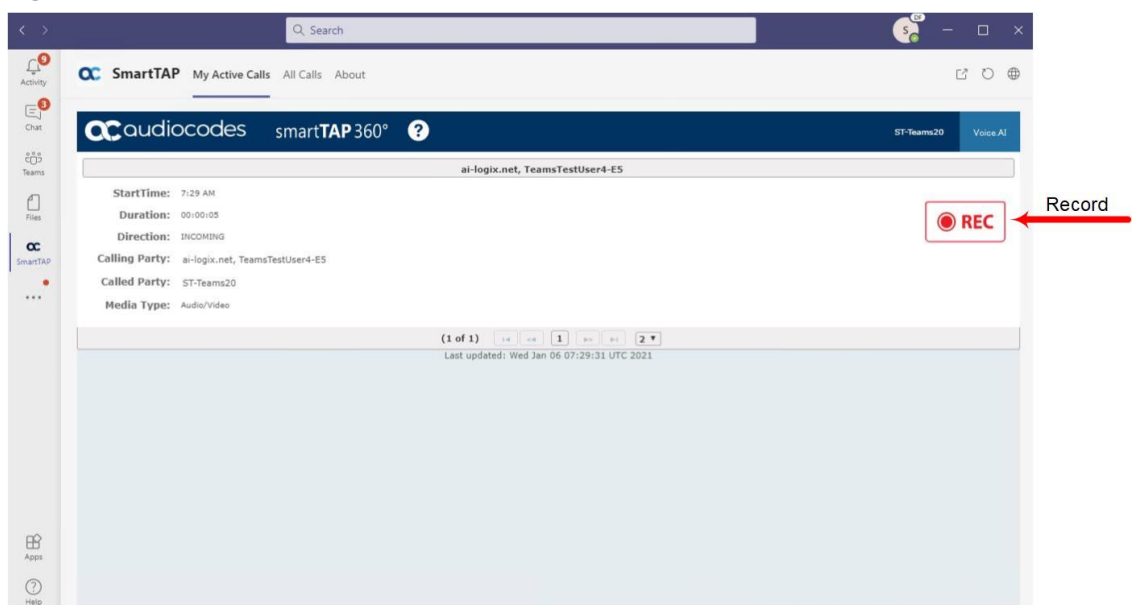
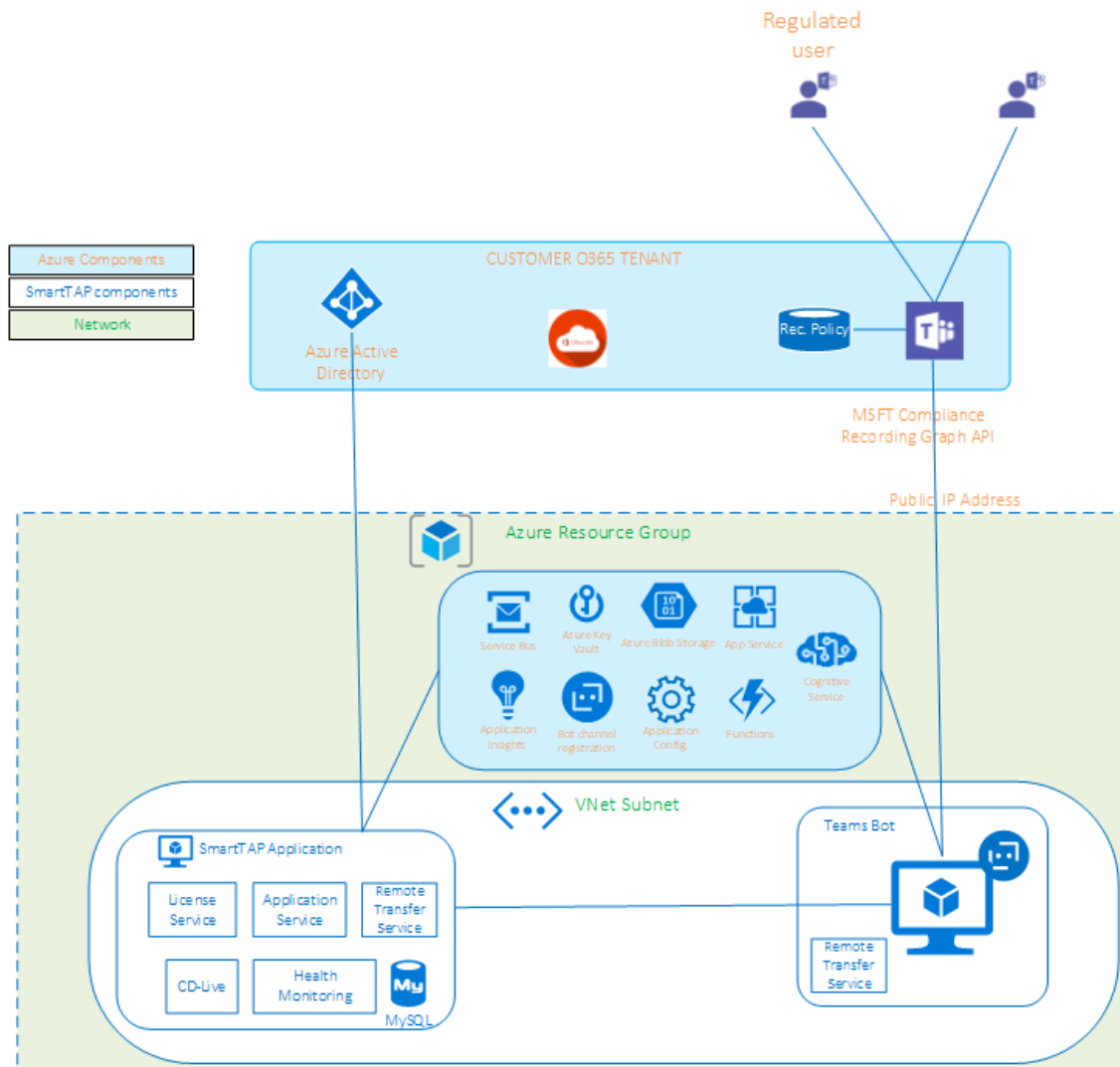


Figure 1-4: Save on Demand (ROD) in SmartTAP 360° Microsoft Teams Client**Figure 1-5: Record on Demand (ROD) in SmartTAP 360° Microsoft Teams Client**

Architecture

The figure below illustrates SmartTAP 360° architecture.

Figure 1-6: SmartTAP 360° Architecture

About this Guide

This guide helps enterprise network administrators obtain full benefit from the SmartTAP 360° Call Recording System. The guide is divided into the following parts:

- Getting Started
- User Actions
- Admin Actions

Part I

Getting Started

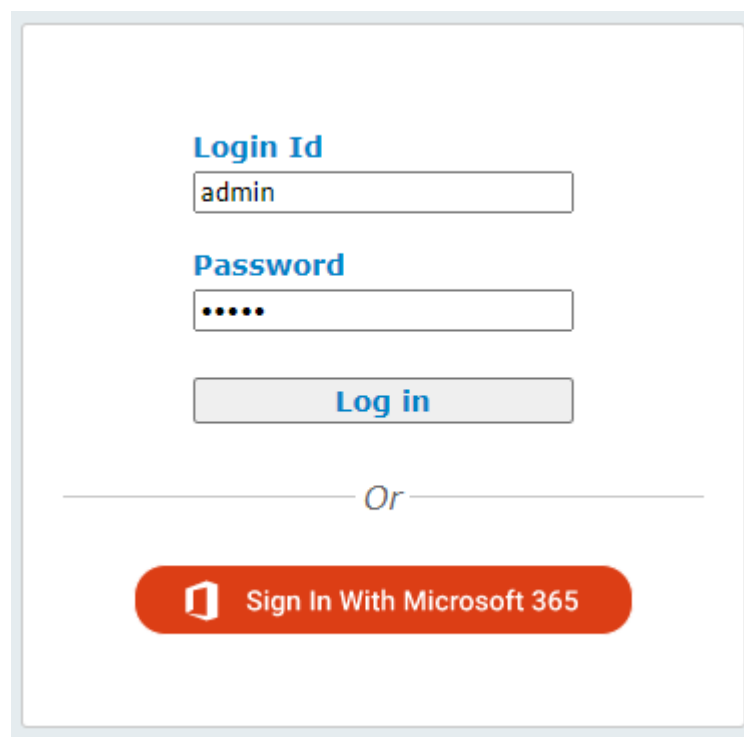
2 Logging In

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

➤ **To log in:**

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

Figure 2-1: Login Page



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

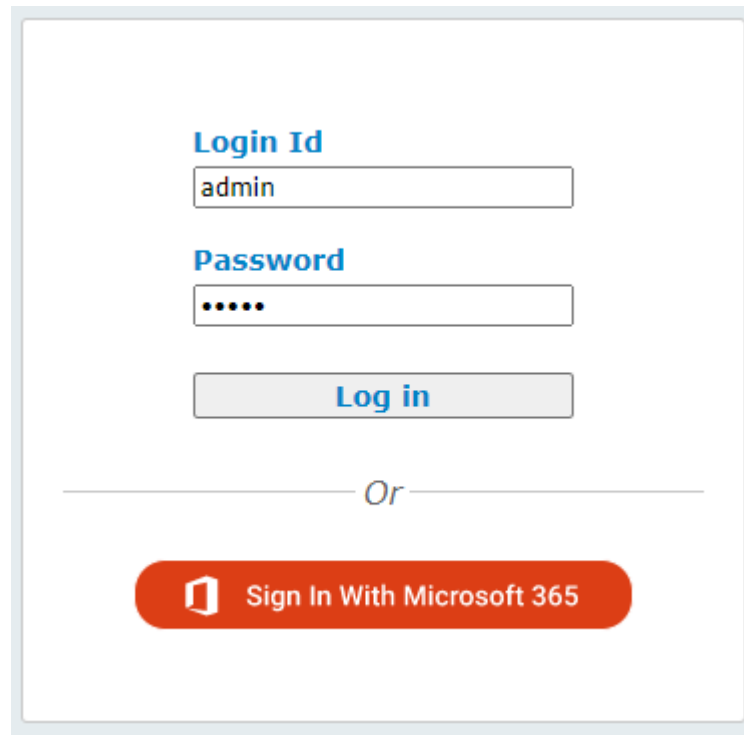
This section describes how to login with Microsoft Office 365 Credentials.



This option is disabled until the OIDC Client is configured (see [View OIDC Client User Login](#) on page 398).

➤ To login with Microsoft Office 365 credentials:

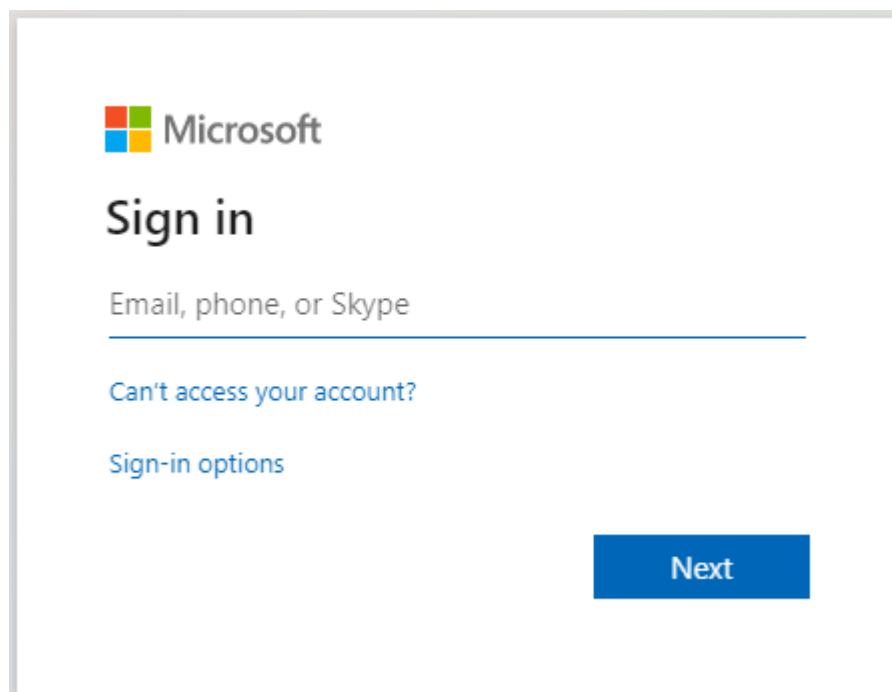
1. Click **Sign-in with Microsoft 365** button.



The image shows a login form for SmartTAP 360°. It features two input fields: 'Login Id' with the text 'admin' and 'Password' with masked characters '••••'. 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 logo.

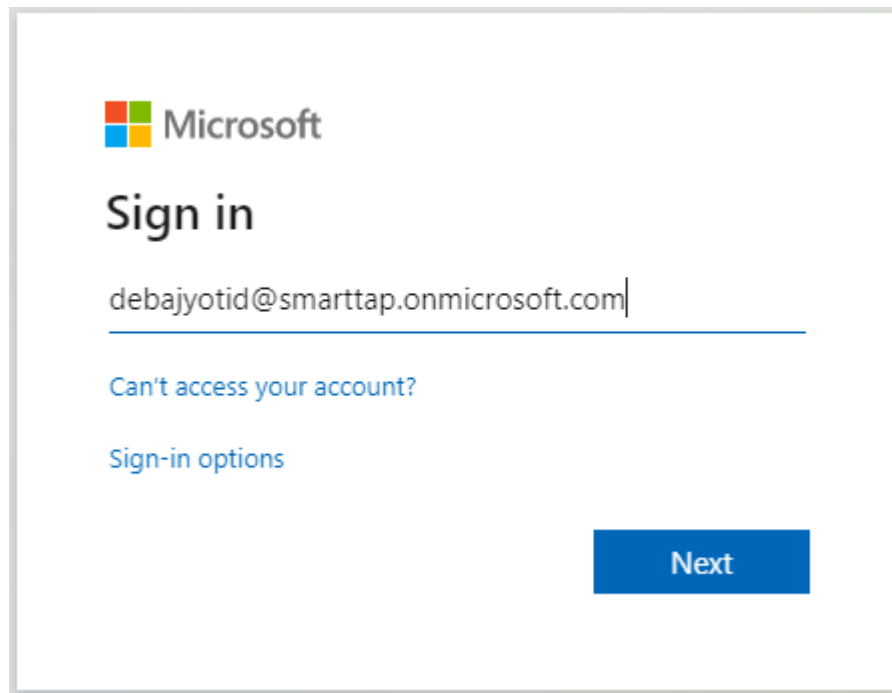
The user is redirected to Microsoft MFC Login page:


Figure 2-2: Microsoft MFC Login Page



The image shows the Microsoft MFC Login page. At the top is the Microsoft logo. Below it is the heading 'Sign in'. A text input field is labeled 'Email, phone, or Skype'. Below the input field are two links: 'Can't access your account?' and 'Sign-in options'. A blue 'Next' button is located at the bottom right of the form.

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

A screenshot of the 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?](#)

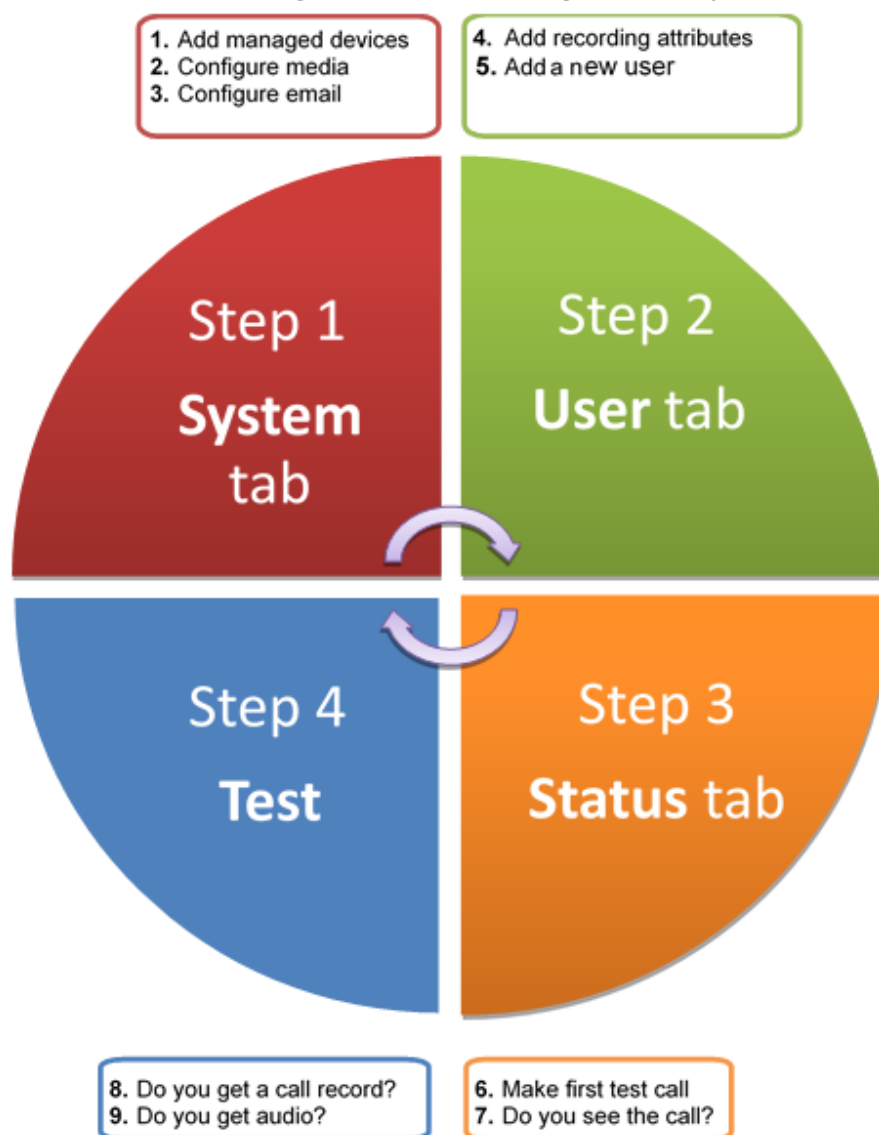
[Sign-in options](#)

Next

3 Performing Initial Configuration

The figure below shows the steps to take to perform initial SmartTAP 360° configuration (Step 1-Step 2) in order to record a call. Detailed instructions follow below it. It's assumed SmartTAP 360° software components were installed on the servers necessary for your environment, and were configured based on the SmartTAP 360° Installation Guide.

Figure 3-1: Performing Initial Setup



➤ **To perform initial setup:**

1. Log in for the first time (see Logging In)
2. Configure media (see Managing Recording Locations).
3. Configure email (see Configuring Email Server Settings).
4. Add a user attribute for recording purposes (see [Adding a Device Attribute](#) on page 76).
5. Add a user (see [Managing Users](#) on page 81).

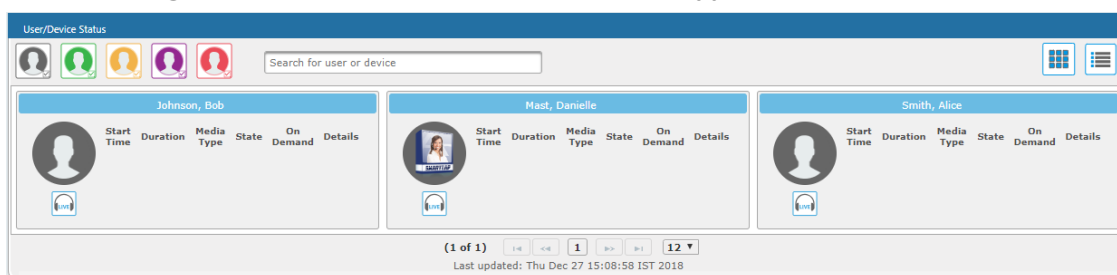
6. Make sure the new user is assigned a recording profile (see Managing Recording Profiles).
7. Make sure the user's recording attribute field is populated (see Managing Recording Profiles).

Getting Acquainted with the Web Interface

The figure below shows the main screen. The following areas are identical across all Web interface 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 3-2: SmartTAP 360° Main Screen – Upper Banner

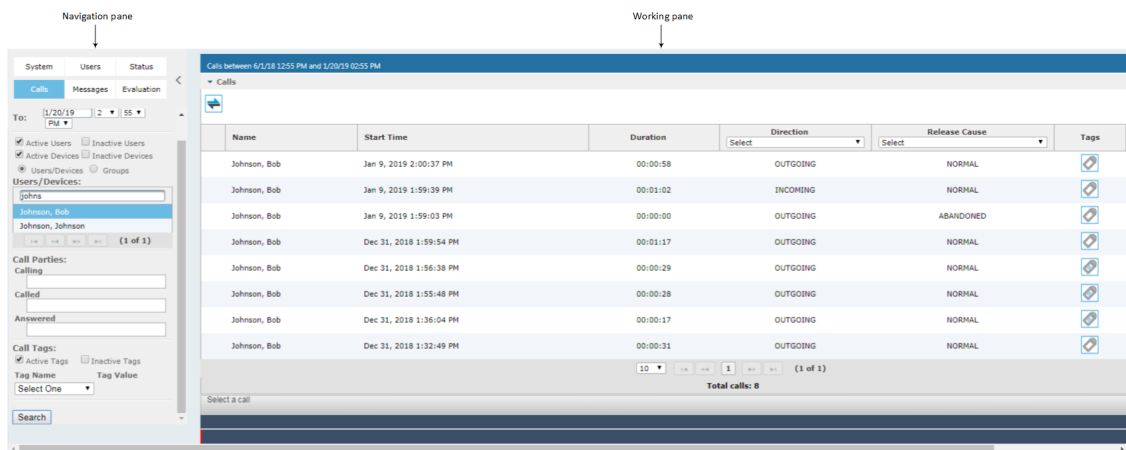


The table below describes the active buttons on the toolbar.



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

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

Figure 3-3: SmartTAP 360° Main Screen

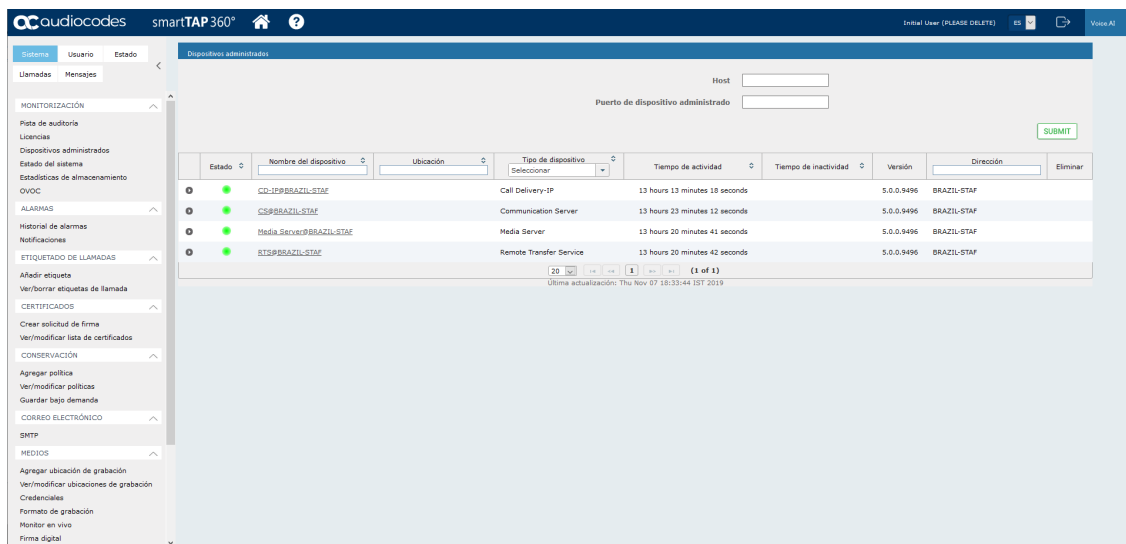
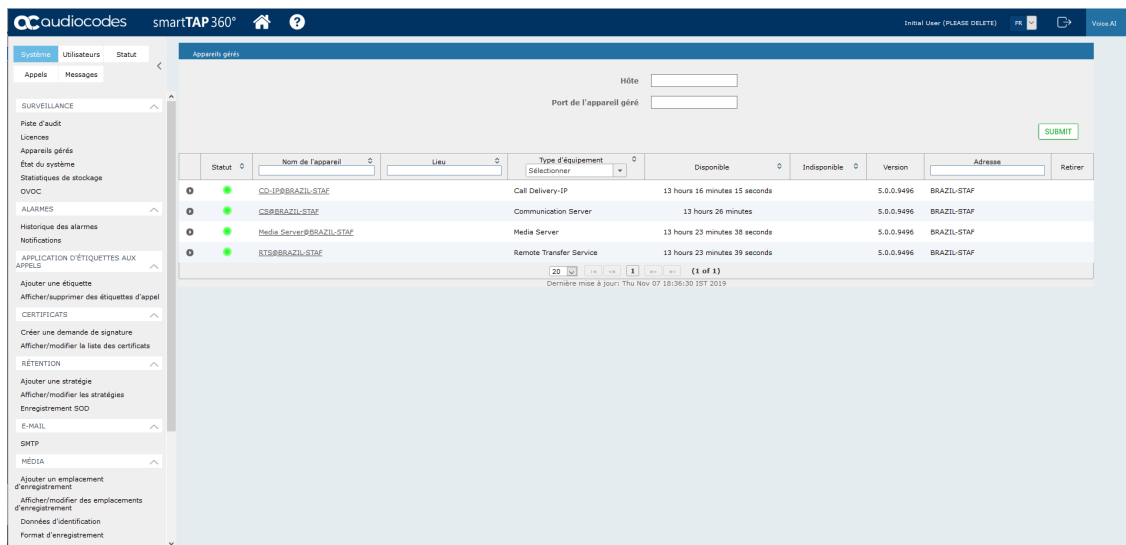
The figure above shows the following three areas below the upper banner:

- 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 3-4: 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.


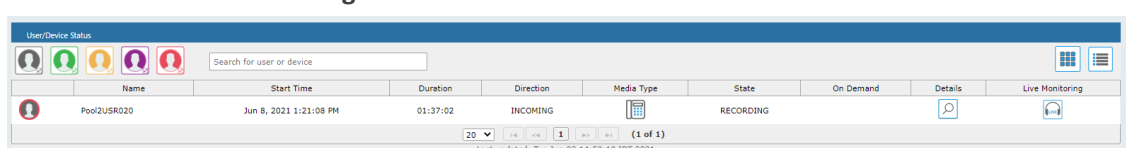
The figure below shows the List View 

Figure 3-5: List View




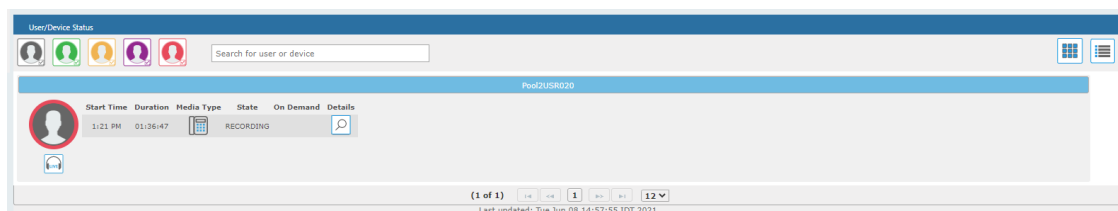
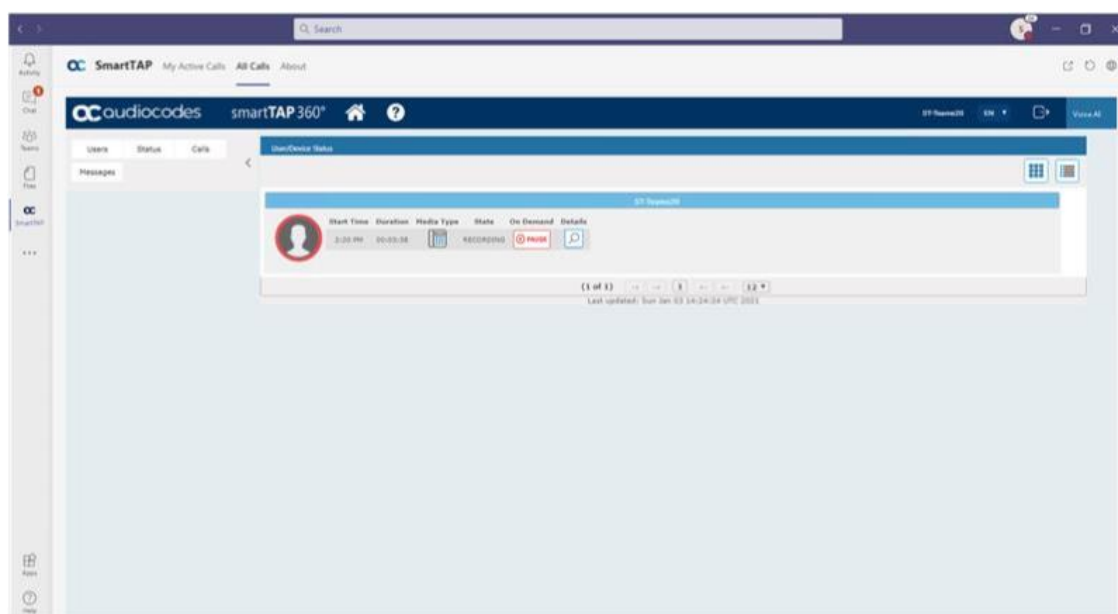
The figure below shows the Grid View 

Figure 3-6: Grid View






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












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

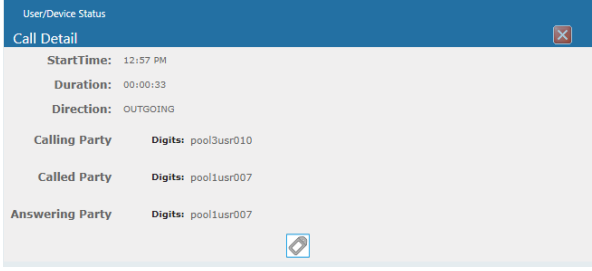










The screen provides near real-time information on the targeted users and their recording status. The table below describes the Status screen features.

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 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). The objective is to validate the configuration and the recording functionality. After making sure that the recording is functioning correctly, continue 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 or 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.

Part II

User Configuration

5 Sending Email

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



➤ **To send an Email:**

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

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

Table 5-1: Email Field Descriptions

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

Field	Description
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.

6 Managing Groups

This section describes how to manage groups:

- [Adding Recording Group](#) below
- [View and Modify Recording Groups](#) on the next page

Adding Recording Group


This section describes how to add a new recording 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**).

2. Configure fields according to the table below.
3. Click SUBMIT to apply changes.

Table 6-1: Group Screen Settings




Field	Description
Group Name	Name of group to add.
Group Description	Description of the group to add.
NonMembers	Users that are not group members. Select users by clicking the user name; multiple users while holding <ctrl>; or all within a range by clicking top user and bottom user while holding <shift>.
>>	Add all NonMembers to the Members group.
>	Add selected NonMembers to the Members group.
<	Remove selected Members from the Members group.
<<	Remove all Members from the Members group.
Available Groups	List of existing groups. Select groups by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>
Sub Groups	List of Sub-Groups of the group to add. Sub-Groups for the Group added can be optionally entered from the Add Group screen.
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>
	Delete Group – displayed only when you modify an existing group.

View and Modify Recording Groups

This section describes how to add and remove users in recording groups.


➤ To view/modify a Recording Group:

1. Open the screen View/Modify Group screen (**Users** tab > **Group Management** folder > **View/Modify Group**).

View/Modify Groups				
Name	Description	Modify	Delete	
Default	Default group			
VPNCpolicy				
yehuditv55				



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

- Click  adjacent to the group that you wish to modify.

Modify Group

Group Name

VPNCpolicy

Group Description

☐ Show Inactive Users/Devices

Non Members

Members

ST-Teams20

ST-Teams21

ST-Teams22

ST-Teams23

ST-Teams24

ST-Teams25

ST-Teams26

Available Groups

VPNCpolicy

yehuditv55

Sub Groups



- Change the Membership by moving users to/from the Members window.
- Change the Sub-Groups by moving Groups to/from the Sub-Groups window.
- Configure other fields according to the table below.
- Click  to apply changes.

Figure 6-1: View/Modify Groups – Field Descriptions

Field	Description
Group Name	Name of group to add.
Group Description	Description of the group to add.
NonMembers	Users that are not group members. Select users by clicking the user name; multiple users while holding <ctrl>; or all within a range by clicking top user and bottom user while holding <shift>.
>>	Add all NonMembers to the Members group.
>	Add selected NonMembers to the Members group.
<	Remove selected Members from the Members group.
<<	Remove all Members from the Members group.
Available Groups	List of existing groups. Select groups by clicking the group name; multiple groups while holding <ctrl>; or all within a range by clicking top group and bottom group while holding <shift>
Sub Groups	List of Sub-Groups of the group to add. Sub-Groups for the Group added can be optionally entered from the Add Group screen.
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>.
	Delete Group – displayed only when you modify an existing group.

7 Managing Security Profiles

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

- [Adding a Security Profile](#) below
- [Configure Permissions in a Security Profile](#) on page 37

Adding a Security Profile

This section describes how to add a Security Profile which sets the Call and Instant Message permissions for the user. For example, play call media or download media related to a call.

➤ To add a Security Profile:

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




2. Configure fields according to the table below.
3. Click  to apply changes.

Table 7-1: Security Profile Settings

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

Field	Description
Name	
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 calls	Select this option to allow users with this security profile to access calls for all users and devices. These users can delete any calls and instant messages.
Access calls within user's groups	Select this option to allow users with this security profile to access calls for all users within all the groups and sub groups of the group hierarchy to which they are a member. These users can delete calls and instant messages that belong to the user's groups.
Access user's own calls	Select this option to allow users with this security profile to access their calls. These users can only delete their own calls and instant messages.
Play Media Related to a call	Select this option to allow users with this security profile to play calls to which they have access.
Download Media Related to a call	Select this option to allow users with this security profile to download media for calls to which they have access.
Email Media Related to a call	Select this option to allow users with this security profile to email media for calls to which they have access.
Tag Calls	Select this option to allow users with this security profile to add Call Tags to calls to which they have access.
Live Monitor	Select this option to allow users with this security profile to live monitor calls to which they have access.
ROD/SOD	Select this option to record on demand and save on demand for calls to which they have access.
Delete Transcription	Select this option to delete transcriptions for call recordings in the Calls screen.
Evaluate Calls	Select this option to allow users with this security profile to evaluate

Field	Description
	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 137.
View Evaluations / Reports	Select this option to allow users with this security profile view completed evaluations or run reports for evaluations to which they have access.
ROD/SOD other users	Select this option to allow a user to Record or Save on Demand another user's calls. The user to be recorded must be in the same group as the initiator.
Configure System	Select this option to allow users with this security profile to view and modify system configuration settings.
Create and modify users and groups	Select this option to allow users with this security profile to create and modify users, groups, and security profiles.
Create Evaluation Forms	Select this option to allow users with this security profile access to the SmartTAP Web interface.
	Delete Security Profile – displayed only when you modify an existing profile.

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

Configure Permissions in a Security Profile

This section describes how to configure permissions in a Security Profile.

➤ **To view/modify Security Profiles:**

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

Figure 7-1: View/Modify Security Profiles

Figure 7-2:

View/Modify Security Profiles		Permissions	Modify	Delete
Name	Description			
system		Configure system		
supervisor	Supervisor	Play Media Related to a call Tag calls Email Media Related to a call Access calls within user's groups Download Media Related to a call Live Monitor		
agent	Agent	Play Media Related to a call Tag calls Access user's own calls Email Media Related to a call Download Media Related to a call		
administrator	Administrator	Configure system Play Media Related to a call Tag calls Delete transcription Email Media Related to a call ROD/SOD other users Create and modify users and groups Download Media Related to a call Live Monitor Access all calls		



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.

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
 ☐ Delete transcription

☐ Configure system
 ☐ Create and modify users and groups

3. Configure fields according to the table below.

4. Click to apply changes.

Table 7-2: 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 delete the Security Profile.

8 Managing Recording Profiles

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

■ **Call:**

- Recording Type – Full Time, Record on Demand, Save on Demand or none.
- Video – enable if video call recording is desired
- Desktop Sharing – enable if Desktop Sharing recording is desired
- Pause or Resume – enable if the 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](#) below
- [Viewing or Modifying Recording Profiles](#) on page 48
- [Assigning Recording Profile to User or Device](#) on page 49
- [Add Recordable Device](#) on page 73
- [Recording Profile-Call Type Configuration Examples](#) on page 52

Adding a Recording Profile

This section describes how to add a recording profile for different recording types for targeted users.

➤ **To add a Recording Profile:**

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

Add Recording Profile

Recording Profile Name

Recording Profile Description

Call

* 'Video' and/or 'Desktop Sharing' options are supported for Microsoft Teams and Skype for Business. 'Record On Demand' and/or 'Pause or Resume' together with 'Video' and/or 'Desktop Sharing' is supported for Microsoft Teams only

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 (transfer mode) *

Call Queues Instance Ids:

* Applicable for MSFT Teams only. Refer to the administrator guide for how to retrieve ids of call queues

Filter Calls User Receives :

List Type: **Block**
Numbers:
Regular Expression:

Filter Calls User Makes :

List Type: **Block**
Numbers:
Regular Expression:

* The Filter Calls options are limited to PSTN calls in MSFT Teams

Applicable for Skype for Business and Lync A/V Recording

☒ Referred by Response Group

Announcements

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

Call type

Internal

☐ Incoming

ANN
☐ Play to calling party

File name

☐ Play to answering party

File name

☐ Outgoing

ANN
☐ Play to calling party

File name

☐ Play to answering party

File name

PSTN

☐ Inbound

ANN
☐ Play to calling party

File name

☐ Play to answering party

File name

☐ Outbound

ANN
☐ Play to calling party

File name

☐ Play to answering party

File name

Federated

☐ Inbound

ANN
☐ Play to calling party

File name

☐ Play to answering party

File name

☐ Outbound

ANN
☐ Play to calling party

File name

☐ Play to answering party

File name

☐ Record Announcement

Don't Play Announcement Destination Numbers :

911

☐ Block Calls on Announcements 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

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

- 41 -

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







- Ensure that you have setup the Announcement server to support this functionality (see Announcement Server (Skype for Business). See [Announcement Server \(Skype for Business\)](#) on page 100 and [Example Announcement Server Scenarios](#) on page 106.
- Recording notifications in Teams environment are provided by Microsoft.

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

7. Click SUBMIT.

Table 8-1: 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: Automatic recording of complete call will begin from start of call with no user action required. ■ Record on Demand: (supported for audio in Skype For Business) recording will commence from a specific point in the call that the user decides to record. ■ Save on Demand: Recording will contain audio and/or video from the beginning 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° Skype for Business Toolbar on page 98. <p>Audio/Video recording can be triggered from the GUI Status page or from the Skype for Business CWE toolbar or Teams Client application.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>For Microsoft Teams, SmartTAP can be integrated into the Microsoft Teams client as a Personal App (see Integrate SmartTAP Personal App in Teams on page 391).</p> </div>

Field	Description
Video	Record a video call (Full Time or Save on Demand).
Pause / Resume	Select Pause / Resume audio recording during sensitive areas of the conversation with a customer, for example, when Credit Card details are given. The process is manual and executed from the Status page. Pause/Resume of a recording can be triggered from the SmartTAP 360° Web interface status page or from the Skype for Business CWE toolbar or Teams Client application.
Instant Message	Automatic Instant Message recording for both Skype for Business recordings and Microsoft Teams recordings.
Desktop Sharing Recording	Recording of Desktop Sharing sessions is supported for Skype for Business and Microsoft Teams. <div>  Record on Demand and Pause/Resume with Video or Screen Sharing are not supported for Skype for Business. </div>
	Apply the changes.
	Cancel the changes.


- **Call Type:** The Recording profile contains call types that can be selected and recorded. The call types described in the following table are supported. The options below relate to SmartTAP 360° users and devices regardless of the user or device location (intranet, internet, mobile device).




- The call types described in the table below are relevant for Microsoft Teams, Skype For Business; Audio; Video and Screen Sharing recording.
- **Skype-For-Business calls only:** When a call is escalated to a conference call by an Internal user (when an additional party(s) are added to the call), the escalated Conference part of the call (from the time the additional party(s) join) is reported as a separate call recording, and will be recorded only if "Calls with internal conference option" is enabled (see [Calls with Internal Conference](#) on the next page).
- **Teams only calls:** When one of the following Call Types is enabled: 'PSTN', 'Internal' or 'Federated', and then the call is escalated to a Conference call by an Internal user (when additional party(s) are added to the call), the escalated Conference part of the call will be recorded as part of the original peer-to-peer call recording leg. If none of the above-mentioned Call Types are enabled, then the escalated Conference part of the call will not be recorded.

Table 8-2: 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)	<p>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.</p> <p>Select the “Calls with Internal Conference” to record Internal calls that are elevated to a conference (Skype For Business only).</p>
PSTN (inbound, outbound)	<p>PSTN calls are 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.</p> <p>Select the “Calls with Internal Conference” to record PSTN calls that are elevated to a conference or conferences with PSTN participants (Skype For Business only).</p>
Federated (inbound, outbound)	<ul style="list-style-type: none"> ■ Federated calls are 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	<p>Record Skype for Business and Teams calls with an Internal conference bridge in the Enterprise domain.</p> <p>An Internal Conference is a scheduled, ad-hoc meeting (for Skype-For-Business also includes a call escalated to a conference, however not relevant for Microsoft Teams) that occurs on a bridge belonging to the targeted user organization (i.e. that is organized or escalated in Skype-For-Business by a user from the targeted user’s organization). When enabled, all user calls with internal conferences are recorded regardless of participant types on the conference (federated, PSTN, or other internal users). When disabled, none of the user calls with</p>

Field	Description
	<p>internal conferences are recorded. Select one of the following options:</p> <ul style="list-style-type: none"> ■ Conferences Calls with All Participant Types: Record all targeted user's calls with conferences (default). ■ Conference Calls with External Participants: Record only conferences with external participants. External participants are those participants who either don't have an Azure object id or it don't belong to the recording organization. For example, participants joined from PSTN, guests from Web or from Federated organization or from a Teams home client. SmartTAP starts recording the targeted user call leg to the conference when an external participant joins the conference and continues recording until the targeted user disconnects or the conference bridge disconnects the call. <div>  This option is supported by Microsoft Teams Integration and with "Full Time" Recording Type only (not supported with Pause and Resume). </div>
Teams Queue Calls (transfer 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.
Call Queues Instance ids	<p>Comma separated list of the instance ids of the relevant call queues ids which should be recorded (see Retrieving Recording Queue Instances on page 53).</p> <p>Relevant when Teams Queue Calls (Transfer mode) is configured and "All" in not selected.</p> <p>When "All" is selected, all user calls will be recording including calls from any call queue. The maximum length of the field is 2048 characters.</p>
Referred by Response Group	Record user calls that are referred by a response group. To record calls referred by a response group to any user, select this option and create a user or device with the network mapping attributes that are associated with the response group (the Response Group URI). To record all calls that a response group is involved, select this option and the "All" option and create a user or device with the network mapping attributes that are associated with the response group (the Response Group URI).

Field	Description
	This configuration is applicable to Skype for Business integrations.
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” 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>Filtering is applicable to Skype for Business integrations and to Microsoft Teams (PSTN calls only).</p> <div>  <p>The + sign should not be added in Numbers and Regular Expression fields as its not recognized by SmartTAP.</p> </div>

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

Table 8-3: Announcements

Field	Description
Internal (incoming, outgoing)	Play announcement on the Internal calls of the recorded user. To play announcement on the calls the user receives, select the “Incoming” option. To play announcement on the calls the user makes, select the “Outgoing” option. *Playing the announcement on the calls with con-

Field	Description
	ference server is currently not supported."
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).

Field	Description
	 This parameter is applicable for Teams Native Integration only.
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 example, PSTN_Inbound.wma • ANN and IVR files must be pre-saved to the StateMachineConfig folder on the ANN server: refer to the SmartTAP Installation Guide.

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



- The Announcement Server does not require to be installed to play beep tones.
- Beep tone can be played on calls 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 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 8-1:

View/Modify Recording Profiles						
Name	Description	Call Recording Type	Video Recording	IM Recording Type	Desktop Sharing Recording	Modify Delete
Full Time	Full Time recording profile	FULL_TIME	Enabled	FULL_TIME	Enabled	 
Queue		FULL_TIME	Disabled	NONE	Disabled	 
ROD		RECORD_ON_DEMAND	Enabled	FULL_TIME	Enabled	 
<div> <div>20</div> <div>1</div> <div>(1 of 1)</div> </div>						

2. Configure fields according to the table below.

Table 8-4: View/Modify Recording Profiles – Field Descriptions



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

Assigning Recording Profile to User or Device


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

➤ To assign a recording profile to a User / Device account:

- **Option method #1:** Add the recording profile to the account manually when the user account is created in SmartTAP 360°. To create a new user account and assign a Recording Profile:

- a. Under the **User** tab, select **View/Modify Users**.
- b. Click  .
- c. From the 'Recording Profile' dropdown, select the required profile (i.e., R.O.D).
- d. Click  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  to apply changes.



- By default, SmartTAP 360° includes the 'Full Time' recording profile.
- All users imported from Active Directory will not have a recording profile assigned. Use optional method # 2 above to quickly assign multiple users the appropriate recording profile.

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

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

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
- Ilyayev, 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

Navigation buttons: >>, >, <, <<

SUBMIT CANCEL

2. Configure parameter according to the table below.

Table 8-5: Add Users to Recording Profiles Screen

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



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

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

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

Retrieving Recording Queue Instances

Configuration of Teams call queues recordings (Transfer mode) in the recording profile requires the retrieval of the application instance of each call queue that is designated for recording. Each call queue is represented by a single Application Instance ID.

➤ To retrieve call queue application instances using PowerShell:

1. Enter the following PS command:

```
PS C:\Users\Admin> Get-CsCallQueue
```

```
WARNING: All the agents added to callqueue have opted out. There are no agents to call.
```

```
TenantId                                : ad41d6c3-67f0-47cc-9de3-e07fd185c1c7
```

Name	: CallQueue1
Identity 62efe4db5c16	: 361635e9-1159-43be-bdc2-
RoutingMethod	: Attendant
DistributionLists	:
Users 2f4134736e42	: 9f7309ea-a318-4ac5-92a0-
DistributionListsLastExpanded	: 11/21/2021 08:12:49 +00:00
Agents 2f4134736e42, OptOut	: 9f7309ea-a318-4ac5-92a0-
AllowOptOut	: True
ConferenceMode	: False
PresenceBasedRouting	: True
AgentsCapped	: False
AgentsInSyncWithDistributionLists	: True
AgentAlertTime	: 60
LanguageId	: en-US
OverflowThreshold	: 200
OverflowAction	: DisconnectWithBusy
OverflowActionTarget	:
OverflowSharedVoicemailTextToSpeechPrompt	:
OverflowSharedVoicemailAudioFilePrompt	:

```

OverflowSharedVoicemailAudioFilePromptFileName :
EnableOverflowSharedVoicemailTranscription      : False
TimeoutThreshold                                : 1200
TimeoutAction                                    : Disconnect
TimeoutActionTarget                             :
TimeoutSharedVoicemailTextToSpeechPrompt        :
TimeoutSharedVoicemailAudioFilePrompt           :
TimeoutSharedVoicemailAudioFilePromptFileName  :
EnableTimeoutSharedVoicemailTranscription       : False
WelcomeMusicFileName                            : caal_queue_greeting.mp3
UseDefaultMusicOnHold                           : True
MusicOnHoldFileName                             :
Statistics                                       : Current queue size = 0
ApplicationInstances                             : f17e8e19-1669-4a4c-bf13-
e9e31420edaf
ChannelId                                       :
OboResourceAccounts                             :

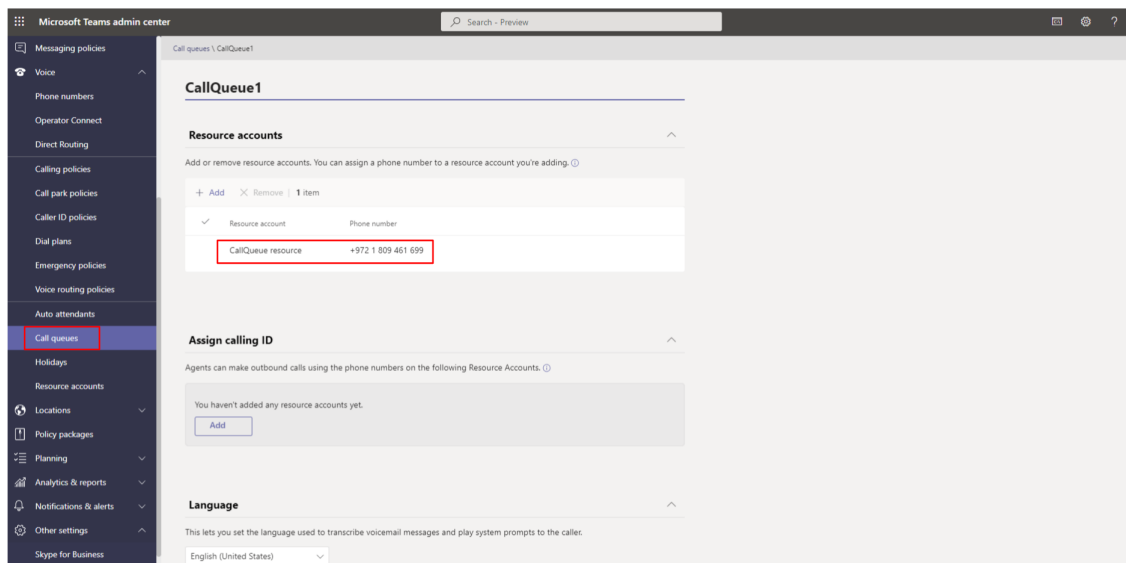
```

2. Copy the Application Instance to notepad.

➤ **To retrieve call queue application instances using Teams Administration:**

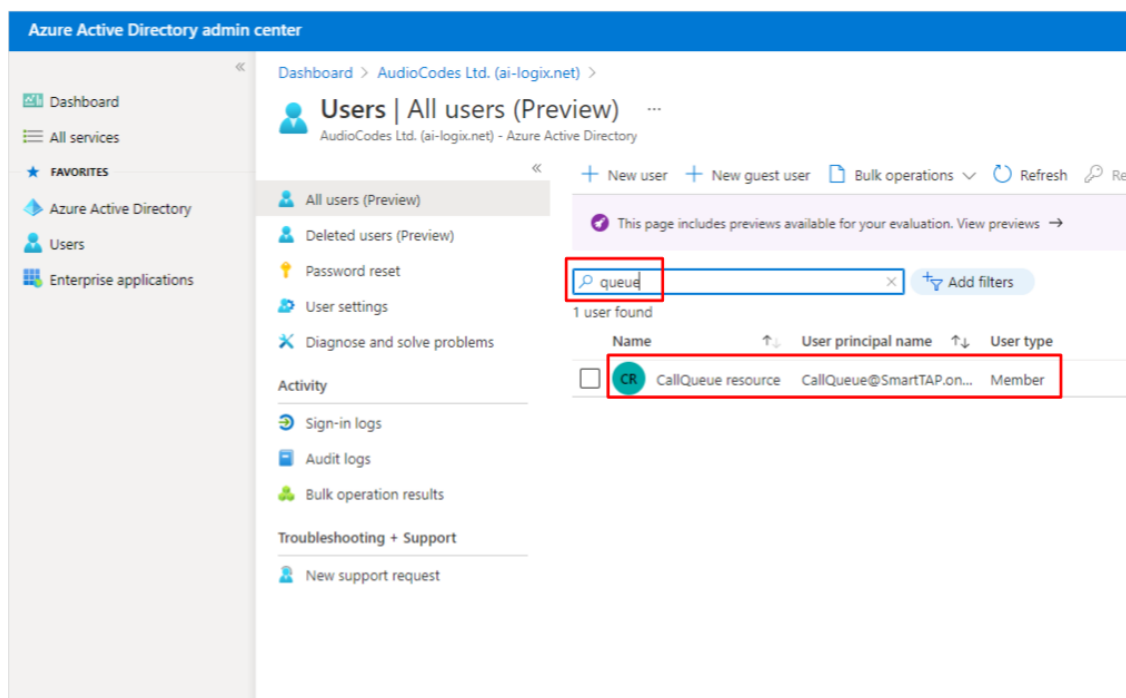
1. Open the Teams Administration portal.
2. Select the Queue.
3. Find Resource details.

Figure 8-2: Call Queues



4. In the Azure Active directory find the queue Resource.

Figure 8-3: Resources



5. Copy the Object ID (application instance) to notepad.

Figure 8-4: Call Queue Resource

The screenshot displays the Azure Active Directory admin center interface. The left-hand navigation pane includes sections for 'Dashboard', 'All services', 'FAVORITES', and 'Enterprise applications'. The main content area is titled 'CallQueue resource | Profile' and shows the following details:

- Manage** section: Includes links for 'Diagnose and solve problems', 'Edit', 'Reset password', 'Revoke sessions', 'Delete', 'Refresh', and 'Got feedback?'. Below these are links for 'Profile', 'Custom security attributes (preview)', 'Assigned roles', 'Administrative units', 'Groups', 'Applications', 'Licenses', 'Devices', 'Azure role assignments', and 'Authentication methods'.
- Activity** section: Includes links for 'Sign-in logs' and 'Audit logs'.
- Troubleshooting + Support** section: Includes a link for 'New support request'.
- CallQueue resource** details: A circular profile picture with 'CR' is shown. The email address is 'CallQueue@SmartTAP.onmicrosoft.com'. The creation time is '8/25/2020, 2:59:14 PM'. A 'User Sign-ins' chart shows zero sign-ins across a timeline from Oct 24 to Nov 21. The 'Group memberships' section shows zero memberships.
- Identity** section: A table with the following data:

Name	First name	Last name
CallQueue resource

User Principal Name	User type
CallQueue@SmartTAP.onmicrosoft.com	Member

Object ID	Issuer
f17e8e19-1669-4a4c-bf13-e9e31420edaf	SmartTAP.onmicrosoft.com
- Job info** section: A table with the following data:

Job title	Department
...	Microsoft Communication Application Instance

9 Managing Call Retention

This section describes the following:

- [Configuring Call Retention](#) below
- [Save on Demand Call Retention](#) on page 60

Configuring Call Retention

Call retention is the number of days to keep recordings in storage. Default: 0 indicates that recordings are never deleted. Use the default with caution since eventually the storage location will be completely consumed. To meet business requirements, it's highly recommended to set the retention value to a positive number. SmartTAP 360° deletes calls that exceed the retention period once a day. A network administrator with appropriate security profile credentials has the option to add / modify retention policies.

Adding Call Retention Policy

This section describes how to add a Call Retention Policy.

➤ **To add a new retention policy:**

1. Open the Add Retention Policy screen (**Users** tab > **Retention** folder > **Add Policy**).

2. Configure parameters according to the tables below.

Table 9-1: Call Retention

Field	Description
Retention Policy Name	The name of the Retention Policy. For example, Agent or Sales.
Retention Policy Description	Description of the policy and to whom it applies.

Field	Description
Call and Instant Message Retention Period (in days)	The number of days before automatically deleting Call and IM recordings. A value of zero (0) indicates that recordings are never deleted.
Video and Desktop Sharing Retention Period (in days)	The number of days before automatically deleting Video and Desktop Sharing recordings. A value of zero (0) indicates that recordings are never deleted.
SUBMIT	Applies the changes.

The Retention Evaluation options set the rules for keeping and/or deleting calls used in evaluations, as well as evaluations themselves.

Table 9-2: Evaluation Retention Rules

Rule	Description
Delete Calls and Evaluations	Evaluations based on the calls subject will be deleted along with their associated calls.
Delete Calls, Keep Evaluations	Evaluations will be kept, however associated calls are deleted. Evaluation-call relationship is eliminated.
Keep Calls and Evaluations	If an evaluation is associated with a call, both the call and its' evaluation will be permanently kept.









3. Click **SUBMIT** to submit changes.


Viewing or Modifying a Retention Policy

This section describes how to view or modify a Retention Policy.

➤ To view / modify a retention policy:

1. Open the Call Retention screen (**Users** tab > **Retention** > **View / Modify Policies**).

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>				

- Click  for a specific policy and modify the necessary fields (see [Adding Call Retention Policy](#) on page 58).

Change Retention Policy Retention Policy

Retention Policy Name

Retention Policy Description

Call and Instant Message Retention Period (in days)

Video and Desktop Sharing Retention Period (in days)

Retention Evaluation Rules

☒ Delete Calls and Evaluations
☐ Delete Calls, Keep Evaluations
☐ Keep Calls, Video, Desktop Sharing and Evaluations

SUBMIT

CANCEL

- Click

SUBMIT

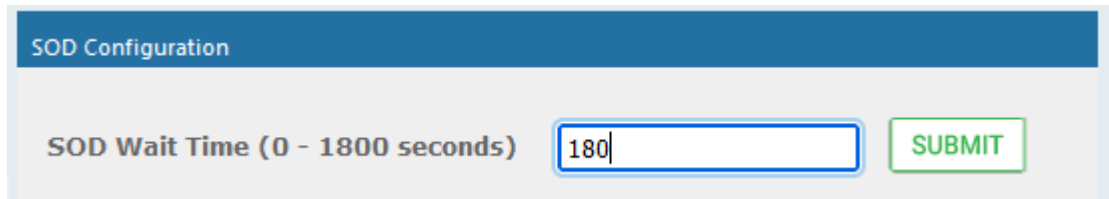
 to apply changes.

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 of up to 1800 seconds (30 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.

➤ **Do the following:**

1. Open the SOD Configuration screen (**Users** tab > **Retention** folder > **Save on Demand**).
2. Configure the SOD Threshold value in seconds (up to 1800 seconds). Default= 180 seconds (3 minutes).



The screenshot shows the 'SOD Configuration' screen. At the top, there is a blue header bar with the text 'SOD Configuration'. Below this, the main area is light gray. On the left, the text 'SOD Wait Time (0 - 1800 seconds)' is displayed. To the right of this text is a text input field with a blue border, containing the number '180'. Further to the right is a green rectangular button with the word 'SUBMIT' in green capital letters.

10 Managing Analytics Profiles

Analytics is a process of analyzing human interactions media of voice by way of speech-to-text and analysis over the related transcription. The use of analytics enables organization stake holders such as compliance officers, process managers, product managers, marketing experts and others to acquire business insights efficiently for measuring performance and progress. For example, measuring employee performance and gauging customer satisfaction and behavior. Voice call transcription can be integrated into a business intelligence system to provide holistic analytics view of all communications in the organization. SmartTAP integrates with the Microsoft cognitive services to provide the following:

- Transcription of recorded voice interactions to text.
- **Categorization and Word and phrase matching:** Recordings can be categorized and keywords can be defined for each category for phrase and word matching. For example, "Sales Improvement" category may include keywords for analyzing consumer behavior for sales cold calling to customers. In this case, you may wish to detect mentions of "discount offers". According to the number of times this phrase is mentioned, analysis can gauge whether there is a positive correlation with sales leads.
- **Sentiment Analysis:** Sentiment analysis analyzes text polarity to determine impressions of brands or other topics based on positive, negative or neutral sentiments, and their association to specific sentences in the Speech-to-text transcripts. For example, 'dreadful' would be interpreted with strong **negative** polarity, 'OK' with **neutral** polarity, and 'awesome' with **positive** polarity.



Analytics is supported for Microsoft Teams integration only.

Add Analytics Categories

Analytics categories are used to gauge different customer or call agent behavioral trends during voice conversations. Each category includes specific word-matching elements.



Its not Mandatory to define Analytics categories. Analyze can be performed on the full transcript.

- **Analytics for Compliance:** Companies recording for compliance and regulatory reasons must adhere to a very strict criteria which in many cases makes analysis of their call records mandatory. For example, set words not spoken to “recorded, "recording", "quality purposes” depending on the script. Automated analytics can be used to identify possible problem issues such as:
 - Determining whether offerings by financial advisers adhere to regulations.
 - Verifying whether staff provide a mandated regulatory statement at the start of each call.

- Ensuring employees describe promotions or offers accurately and transparently.
- Holding a complete record of all interactions to address problems before they arise.

■ **Analytics for Quality Recording:** Quality analysis from the captured calls repository including:

- Gauging customer experience including ease of reaching the personnel and identifying frequent product or support issues.
- Monitoring Call agent adherence to workflow scripts.
- Quality alerting through the identification of keywords such as “complaint” , “refund” , “escalation” or “unsatisfactory”

■ **Analytics for Sales Improvement:** Analytics to objectively assess corporate sales performance including:

- Attaining customer perspectives on pricing and service levels.
- Attaining customer perspectives on competitors.
- Identifying why customers are leaving, including which factors affect customer loyalty the most, and determine how to turn the situation around.
- Identifying keywords that indicate quality issues and determine hot topics and trends which can potentially pitch advertising campaigns.

The figure below illustrates the different categories and their respective features.



The following are examples of keywords that may be used for the "Sales Improvement" category:

- Keywords for understanding product/customer support issues such as "refunds", "returns", "its not working".
- Sales Campaigns mentioning the word "discount" "limited offer".
- Contract renewal mentioning "contract" or "contract renewal".
- Apologies, for example "we apologize for any convenience".
- Inability to help related to sales/support: "I can't help", "I'm sorry I can't help with that", "Don't support".

For example "Life Insurance Renewal campaign": an Insurance salesman insists on delivering a stern message to customers that their life insurance policy has the lowest premium in the market and that customers can save compared to competitors. Phrases in transcript may contain "lowest premium", "significant savings" and "best value-for-money policy".

For example "Paperless Campaign": Paperless Campaign to sway customer to move to digital billing with incentive of 5% off their next billing cycle.

Add Analytics Category

Analytics Category Name:

Analytics Category Description:

Must Match	<input type="text" value="Paperless"/>	
Must Match	<input type="text" value="five percent"/>	
Must Match	<input type="text" value="Digital Billing"/>	

The figure below shows a transcript between a sales representative and customer. Three categories are defined for this user (in this case, a salesperson):

- Campaign: keywords matching the names of marketing campaigns and programs. In the example, "Paperless billing" and "Digital billing".
- Competitor mention: keywords matching the names of competitors.
- No mention of recording: keywords matching

Call: before 12/09/22 5:17 AM

Call

Name	Start Time	Answered	Released	Duration	Direction	Calling Party	Called Party	Answering Party	Dialed Digits	Release Cause	Recording Type	Triggered	Calls Expires	Video and Desktop Sharing Expires	Tags	Media Type	Media Status	Media Reason	Conversation ID	Conf
Fedida, Gid(Gid@audiocode.biz)	12/6/22 8:20:13 PM	12/6/22 8:20:16 PM	12/6/22 8:20:23 PM	00:02:12	INCOMING	CONFERENCE...	Fedida, Gid(Gid@audiocode.biz)	Conference	NORMAL	FULL_TIME	Dec 6, 2022									

Display Transcript

Search text in transcript:

Sentiment: ☒ Positive ☒ Negative ☒ Neutral ☒ Auto-scroll

Categories: Campaign (2) Competitor Mention (2) No Mention of Recording (see...) (0)

00:25.740 so if you hear all that typing in the in the background i know that can be quite annoying

00:30.880 all right so uh customer michael after pulling up your account i do see that you've got a really awesome deal that that we have in place that could be really beneficial for you

00:44.120 we do see that you are, you are a you are billed via the mail and we do have a current discount happening right now that if you switch over to **paperless** billing, which is essentially our **digital billing** program, you'll be able to get a 5% discount on.

01:02.630 On services. How does that sound?

01:04.950 Oh, it sounds great. Awesome. Awesome. Really, really love having your business.

01:11.140 You know, there's a few other things i'm seeing too. Ohh, you, you did want to mention that you have a lot of other competitors that you're looking at that could potentially have some better deals. Yeah, i think we do compete really well with **verizon**

01:29.570 There's a few others out there too. You know, if you, you mentioned **apologetic** i, you know, i think that we've got better services and products there and we'd really hate for you to leave the, you know, leave our services.

01:41.390 last thing michael is i do see that you've got a contract coming up to to be renewed would you like to renew that contract

01:49.000 that would be it would be really great if you could renew the contract and you could stay part of this awesome business

01:55.690 oh, you would love to renew it for \$1,000,000. that is perfect. we love that and we love your business and we appreciate you and have a great rest of your day. we thank you, Michael. Goodbye.

For figure below displays additional categories 'Apologize', identifying apologetic keywords, Malicious, identifying threatening keywords and 'Refund' mentioning keywords identifying refunds of money.

Tag Name: Tag Value:

Analytics Categories:

Analytics Sentiment: Positive % Negative %

SysCall ID:

Search

Saved Searches

No records found. (1 of 1)

Search text in transcript:

Sentiment: ☒ Positive ☒ Negative ☒ Neutral ☒ Auto-scroll

Categories: malicious (3) paperless campaign (4) No mention of Recording (0) Apologize (1) Refund (2)

Competitor Mention (1)

00:00.560 Hi we'd like to offer you **paperless billing**, where if you are willing to switch over we will give you **five percent** off of your next bill.

00:15.660 I'm so **sorry** about your recent experience sir, let me see how i can help you.

00:25.120 I'd like to **return** this product.

00:32.170 It has been off and on from the very start.

00:38.430 So your product isn't working and you'd like me to establish a **refund** for you?

00:45.760 I may switch over to **verizon** if i keep having these issues with you guys.

00:55.980 I will **complaint** to the **police** if you keep **threatening** me.

00:00:00 | 00:01:02

➤ **To add categories:**

1. Open the Add Analytics categories page (**Users** tab > **Analytics** folder > **Add Analytics Categories**).

2. Fill in Analytics Category Name and Analytics Category Description (optional).
3. Click **+Must Match** to fill in a word or phrase that if matched during the call, aligns with the category.
4. Click **+Must Not Match** to fill in a word or phrase that if not matched during the call, aligns with the category.
5. Select AND/OR drop-down to add the Boolean logic to the matched and unmatched words.
6. Click **+Composite** to create another group that all follows AND logic or OR logic.
7. Click **SUBMIT** to apply changes.

View and Modify Analytics Categories

This section describes how to view/modify categories.

➤ **To View/Modify categories:**

1. Open the View/Modify Analytics Categories page (**Users** tab > **Analytics** folder > **View/Modify Analytics categories**).

Figure 10-1: View/Modify Analytics categories

Name	Description	Modify Analytics Categories	Delete
Paperless Campaign	Paperless Campaign to sway customer to move to paperless		
Extended Contract	Extended Contract of 3 or 5 years		
Category_1	des		
Category_REST	des		

2. Click adjacent to the Analytics category that you wish to modify.
3. Modify category (see [Add Analytics Categories](#) on page 62).
4. Click **SUBMIT** to apply changes.

Add Analytics Profile

Analytics profiles lets you define analytics criteria for applying to specific users. The profile includes the assigning of categories defined in [Add Analytics Categories](#) on page 62. You can generate reports based on the retrieved data and send the reports to a list of subscribers.

➤ **To add an analytics profile:**

1. Open the Add Analytics Profile page (**Users** tab > **Analytics** folder > **Add Analytics Profile**).

Figure 10-2:

Add Analytics profile

Analytics Profile Name

Analytics Profile Description

Configuration SmartTapAnalytics

Language English (Australia) - Sentiment supported

Sentiment Analysis Enabled ☐

Categories

hello

Enable Analytics Report ☐

Subscription For Report

Non Recipients

null
ST-Teams106, ST-Teams106
ST-Teams20
ST-Teams22
ST-Teams23
ST-Teams24
ST-Teams25

>>
>
<
<<

Recipients

Report Frequency

Daily ☐

Weekly ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Monthly ☐ 1st of the Month ☐ Mid Month ☐ Final Day of the Month

SUBMIT CANCEL

2. Configure fields according to the table below.

3. Click SUBMIT to apply changes.

Table 10-1: Analytics Profile

Field	Description
Analytics Profile Name	The name of the Analytics profile.
Analytics Profile Description	A short description of the Analytics profile.
Configuration	The name of the pre-configured analytics configuration.
Language	The language to apply to the transcript.
Sentiment Analysis Enabled	Determine whether the sentiment analysis uses Microsoft's sentiment analysis feature to provide % negative, % neutral, and % positive sentiment values for the call (based on a per phrase analysis).
Categories	Determines the categories that are applicable to the Analytical Profile. The categories are defined in Add Analytics Categories on page 62.
Enable Analytics Report	Enables the generation of Analytics reports and the sending of the reports to specific recipients.
User Subscription	The list of subscribers to receive the generated reports. Use the > >> keys to add user recipients for receiving the Analytical reports by email. Use the < << keys to remove recipients from the list.
Report Frequency/date criteria	The frequency a report is sent to a recipient(s). The higher the frequency of the report, the less data that is sent in the call period listed. Configure one of the following Report Frequencies: <ul style="list-style-type: none"> ■ Daily (Monday thru Sunday) ■ Weekly ■ Monthly

The following shows an example of a generated report sent to subscribers.

A	B	C	D	E
1	Category	Call link	# of matches	
2	cat1	http://il-sharonbi-lp.corp.audiocodes.com/smarttap/calls/calls.jsf?id=10536	3	
3	cat1	http://il-sharonbi-lp.corp.audiocodes.com/smarttap/calls/calls.jsf?id=10535	2	
4	cat2	http://il-sharonbi-lp.corp.audiocodes.com/smarttap/calls/calls.jsf?id=10536	4	

Example report data is shown below.

Subject: analytics11 Anyltics Report - Daily

analytics11 Anyltics Report: DailyReport

Total Analyzed Calls: 3

Category Name: cat1

Number of Matched Calls: 2

% Match of Analyzed Calls: 66%

Category Name: cat2

Number of Matched Calls: 1

% Match of Analyzed Calls: 33%

Category Name: cat3

Number of Matched Calls: 0





















% Match of Analyzed Calls: 0%

View and Modify Analytics Profile

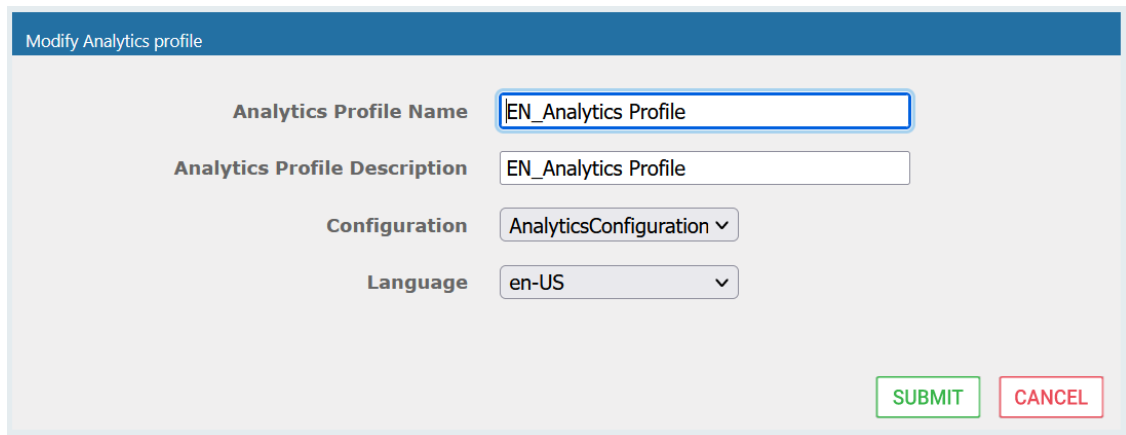
This section describes how to view and modify an Analytics profile.

➤ To view and modify an analytics profile:

1. Open the View/Modify Analytics Profiles page (**Users** tab > **Analytics** folder > **View/Modify Analytics Profile**).

View/Modify Analytics Profiles			
Name	Description	Modify Analytics Profiles	Delete
EN_Analytics Profile	EN_Analytics Profile		
rest_Analytics	rest_Analytics_desc		
prof1	des		
HE_Analytics Profile	HE_Analytics Profile		
FR_Analytics Profile	FR_Analytics Profile		
RU_Analytics Profile	RU_Analytics Profile		
AR_Analytics Profile	AR_Analytics Profile		
Managed Identity_Analytics Profile_EN	Managed Identity_Analytics Profile_EN		
<div> 20   1   (1 of 1) </div>			

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

Figure 10-3: Modify Analytics Profile

Modify Analytics profile

Analytics Profile Name

Analytics Profile Description

Configuration

Language

3. Configure fields according to the table below.

4. Click to apply changes.

Table 10-2: Analytics Profile

Field	Description
Analytics Profile Name	The name of the analytics profile.
Analytics Profile Description	A short description of the analytics profile.
Configuration	The preconfigured configuration of the analytics profile.
Language	The language to apply to the analytics configuration.

Add Users to Analytics Profiles

This section describes how to associate users to Analytics profiles configured in [Add Analytics Profile](#) on page 67. Once the users are associated to a profile, the Analytics toolbar is displayed below the selected call in the Calls list including the attached profile. In addition, when **Display Transcript** check box is selected, the words matching the configured categories are highlighted.

Call before 12/26/22 5:17 AM

Call

Name	Start Time	Answered	Released	Duration	Direction	Calling Party	Called Party	Answering Party	Dialed Digits	Release Cause	Recording Type	Triggered	Calls Expires	Video and Desktop Sharing Expires	Tags	Media Type	Media Status	Media Reason	Conversation ID	Conf
Fedida, Gid (Gid@audcode.biz)	12/26/22 5:17:13 PM	12/26/22 5:17:16 PM	12/26/22 5:17:25 PM	00:02:12	INCOMING	CONFERENCE...	Fedida, Gid (Gid@audcode.biz)	Conference	NORMAL	FULL TIME	Dec 5, 2022									

Display Transcript

Search text in transcript

Sentiment: ☒ Positive ☒ Negative ☒ Neutral ☐ Auto-scroll

Categories: Campaign (1) Competitor Mention (1) No Mention of Recording (sec... (0)

00:25:740 so if you hear all that typing in the in the background i know that can be quite annoying

00:30:880 all right so uh customer michael after pulling up your account i do see that you've got a really awesome deal that that we have in place that could be really beneficial for you

00:44:120 we do see that you are, you are a you are billed via the mail and we do have a current discount happening right now that if you switch over to **SmartTAP** billing, which is essentially our **SmartTAP** program, you'll be able to get a 5% discount on.

01:02:630 on services. How does that sound?

01:04:950 oh, it sounds great. Awesome. awesome. Really, really love having your business.

01:11:140 You know, there's a few other things i'm seeing too. Ohh, you, you did want to mention that you have a lot of other competitors that you're looking at that could potentially have some better deals. Yeah, i think we do compete really well with **SmartTAP** and

01:29:570 there's a few others out there too. You know, if you, you mentioned **SmartTAP**, i, you know, i think that we've got better services and products there and we'd really hate for you to leave the, you know, leave our services.

01:41:350 last thing michael is i do see that you've got a contract coming up to to be renewed would you like to renew that contract

01:49:000 that would be it would be really great if you could renew the contract and you could stay part of this awesome business

01:55:690 oh, you would love to renew it for \$1,000,000. That is perfect. we love that and we love your business and we appreciate you and have a great rest of your day. we thank you, michael. Goodbye.

Total calls: 1

➤ To add users to analytics profiles:

1. Open the Add Users to Analytics Profiles page (Users tab > Analytics folder > Add Analytics Profile).

Add Users to Analytics Profiles

No Analytics Profile

- ST-Teams06, ST-Teams06 (None)
- ST-Teams11, ST-Teams11 (None)
- ST-Teams12, ST-Teams12 (None)
- ST-Teams13, ST-Teams13 (None)
- ST-Teams14, ST-Teams14 (None)
- ST-Teams20 (None)
- ST-Teams21 (None)
- ST-Teams22 (None)
- ST-Teams23 (None)
- ST-Teams24 (None)
- ST-Teams25 (None)
- ST-Teams26 (None)
- ST-Teams27 (None)
- ST-Teams28 (None)
- ST-Teams29 (None)
- ST-Teams30 (None)
- ST-Teams31 (None)
- ST-Teams32 (None)
- ST-Teams33, ST-Teams33 (None)
- ST-Teams34, ST-Teams34 (None)
- ST-Teams35, ST-Teams35 (None)
- ST-Teams36, ST-Teams36 (None)
- ST-Teams37, ST-Teams37 (None)
- ST-Teams38, ST-Teams38 (None)
- ST-Teams39, ST-Teams39 (None)
- ST-Teams40, ST-Teams40 (None)
- ST-Teams41, ST-Teams41 (None)
- ST-Teams42, ST-Teams42 (None)
- ST-Teams43, ST-Teams43 (None)
- ST-Teams44, ST-Teams44 (None)
- ST-Teams45, ST-Teams45 (None)
- ST-Teams46, ST-Teams46 (None)
- ST-Teams47, ST-Teams47 (None)
- ST-Teams48, ST-Teams48 (None)
- ST-Teams49, ST-Teams49 (None)
- ST-Teams80, ST-Teams80 (None)

Analytics Profiles

AnalyticsProfile_EN

Analytics_Profile_HE

ST-load-test-dynamic-rename

SUBMIT CANCEL

2. Manage user Analytics Profiles according to the table below.

3. Click  to apply changes.

Table 10-3: Analytics Profiles

Field	Description
No Analytics Profile	Lists all users that are not assigned to any Analytics profile. Select users by clicking the username; multiple users while holding <ctrl>; or all users within a range by clicking top user and user while holding <shift>.
Analytics Profiles	Names of the configured Analytics profiles.
>>	Assign all users to a specific Analytics profile.
>	Add selected user to a specific Analytics profile.
<	Remove user from an Analytics profile
<<	Remove all users from specific Analytics profile.

11 Managing Devices

This section describes how to manage recordable devices:

- [Add Recordable Device](#) below
- [Viewing and Modifying Recordable Devices](#) on the next page
- [Adding a Device Attribute](#) on page 76
- [Viewing and Modifying Device Attributes](#) on page 79

Add Recordable Device

This section shows how to manage recordable devices.

➤ To add a Recordable Device:




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

2. Configure the fields according to table below.

3. Click  to apply changes.

Table 11-1: Recordable Device – Settings Descriptions

Field	Description
Name	Name of the new recordable device.

Field	Description
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.

Viewing and Modifying Recordable Devices

This section describes how to view and modify recordable devices.

➤ To view and modify recordable devices:

1. Open the View/Modify Recordable Devices screen (**Users** tab > **Device Management** folder > **View/Modify Devices**).

Figure 11-1:

View/Modify Recordable Devices

Name	Description	Type	Modify	Delete
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)

View/Modify Recordable Devices

Name: SIP Proxy1 Description: SIP_PROXY Type: SIP_PROXY

20 1 (1 of 1)

2. Select the Recordable Device to modify.

Figure 11-2: Modify Recordable Device

Modify Recordable Device

Name: SIP Proxy1 Description:

Device type: SIP Proxy SIP1:

Retention Policy: Default Recording Profile: None

Available Groups

Default



Assigned Groups

>> > < <<

SUBMIT CANCEL

3. Configure fields according to the table below.
4. Click **SUBMIT** to apply changes.

Table 11-2: 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. Drop down 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.
	Cancel the changes.
	Delete Device – displayed only when you modify an existing profile.

Adding a Device Attribute

This section describes how to add a SmartTAP 360° device attribute. Create device attributes and devices when you need to record common area phones, IVR numbers, or other common phone numbers. The table below describes the purposes of these attributes.

Table 11-3: SmartTAP 360° Device Attributes

Attribute Purpose	Priority	Description
Trigger Recording	Critical	Instructs SmartTAP 360° which attribute to use for triggering recording. (i.e., Add TEL_URI attribute and provide a value to be assigned to the device. If the device makes a SIP call, SmartTAP 360° will trigger a recording based on the TEL_URI).
Provide Additional device Info	Optional	Add additional information to the device account within SmartTAP 360°, for example, Ext, Tel URI, Mobile, etc. for information purposes only.

➤ **To add a device attribute:**

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

Figure 11-3: Add General Device Attribute

2. Configure fields according to the table below.
3. Click **SUBMIT** to apply new device attribute.

Table 11-4: Device Attributes

Field	Description
Attribute Name	Unique easily identifiable name to the attribute.
Attribute Description	Brief Description of the attribute.

Field	Description
Network Mapping	Indicates whether attribute mapping is required. When selected, the 'Network Mapping Type' drop-down list is displayed.
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

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 > Device Management** folder > **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. 'TEL_URI'
6. Click SUBMIT to apply new device attribute or CANCEL to exit.

Figure 11-4: Add Device Attribute - TEL_URI

The screenshot shows a web form titled "Add Device Attribute". It contains four fields: "Attribute Name" with the value "TEL_URI", "Attribute Description" with the value "TEL_URI", "Network Mapping" which is a checked checkbox, and "Network Mapping Type" which is a dropdown menu currently showing "TEL_URI". At the bottom right, there are two buttons: a green "SUBMIT" button and a red "CANCEL" button.

Viewing and Modifying Device Attributes

This section describes how to view and modify device attributes.

➤ **To view and modify recordable devices:**

1. Open the View/Modify Recordable Devices screen (**Users tab > Device Management folder > View/Modify Device Attributes**).

The screenshot shows a table titled "View/Modify Device Attributes". The table has columns for "Name", "Description", "Network Mapping", "Modify", and "Delete". There is one row with the following values: "TEL_URI", "TEL_URI", "Select One", a pencil icon, and a trash can icon. Below the table, there are pagination controls showing "20" items per page, "1" of 1 items, and a "(1 of 1)" indicator.

2. Select the Device Attributes to modify.

The screenshot shows a web form titled "Modify Device Attribute". It contains four fields: "Attribute Name" with the value "TEL_URI", "Attribute Description" with the value "TEL_URI", "Network Mapping" which is a checked checkbox, and "Network Mapping Type" which is a dropdown menu currently showing "TEL_URI". At the bottom right, there are two buttons: a green "SUBMIT" button and a red "CANCEL" button.


3. Configure fields according to the table below.
4. Click  to apply changes.

Table 11-5: Device Attributes

User Attribute	Description
Attribute Name	Unique easily identifiable name to the attribute.
Attribute Description	Brief Description of the attribute.
Network Mapping	Indicates whether attribute mapping is required. When selected, the 'Network Mapping Type' drop-down list is displayed.
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

12 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 85
- [Update an Admin User](#) on page 88
- [Modify a User Password](#) on page 95
- [Uploading a User Image](#) on page 96

➤ **To add a user:**

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

The screenshot shows the 'Add User' form with the following fields and options:

- First Name**: Text input field
- Last Name**: Text input field
- Email**: Text input field
- Login Id**: Text input field
- Id / Alias**: Text input field
- SIP URI**: Text input field
- TEL URI**: Text input field
- Retention Policy**: Dropdown menu with 'Default' selected
- Recording Profile**: Dropdown menu with 'None' selected
- Legal Hold**: Toggle switch set to 'OFF'
- Security Profiles**: List box containing 'administrator', 'agent', and 'supervisor'
- Groups**: List box containing 'APAC Sales', 'APAC Support', 'Default', 'EMEA Sales', 'EMEA Support', 'NA Sales', 'NA Support', 'Sales', and 'Support'
- SUBMIT**: Green button
- CANCEL**: Red button

2. Enter the user's First Name.
3. Enter the user's Last Name.
4. Optionally enter the user's email (SmartTAP 360° sends initial password to this email address).





5. Optionally enter ID / Alias (this is free-form text that can be used to enter the employee ID or any other data).
6. Select an appropriate retention policy for the user (Default: 'default').
7. Select an appropriate recording profile for the user (Default: 'None').
8. Select the security profile or profiles by highlighting them (see the notes on the Add User screen field descriptions, above, for how to select more than one profile).
9. Select the group or groups to which the new user is to be added.
10. Add the appropriate value to any attribute fields that are designated for recording.

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

11. Click **SUBMIT** to apply changes; a successful configuration results in a message in green font in the command execution Results area; a failed configuration results in a failure message encoded in red font in the command execution Results area. SmartTAP 360° sends an email to the user with their login and initial password, assuming that an email was provided.
12. Use the table below as reference.

Table 12-1: 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

Field	Description
	the bottom of the range.
Groups	<p>Lists the groups that the user can be a member of. Highlighted items indicate the groups that the user is a member of.</p> <p>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.</p> <p>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.</p>
	Reset Password – displayed only when modifying a user.
	Legal Hold – the retention process will not delete a user's calls or messages when the user is placed on legal hold. This feature is only available when modifying a user.
	Apply the changes.
	Cancel the changes.

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.

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

SUBMIT **CANCEL**

Table 12-2: 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.
OID	Custom OID field.

Field	Description
Security Profiles	<p>Select one of the following security profiles to attach to the user:</p> <ul style="list-style-type: none"> <input type="checkbox"/> administrator <input type="checkbox"/> agent <input type="checkbox"/> supervisor
Groups	Select a group to assign 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  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**).

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)	notausers@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> <div>20</div> <div>< << 1 2 3 4 5 >> ></div> <div>(1 of 5)</div> </div>						

Figure 12-1: 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			
<div> <div>20</div> <div>< << 1 >> ></div> <div>(1 of 1)</div> </div>						

2. Click  adjacent to the user that you wish to modify.



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








3. Configure fields according to the table below.

4. Click  to apply changes.

Table 12-3: 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.

Field	Description
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.
OID	Custom OID field.
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.
Security Profiles	<p>Select one of the following security profiles to attach to the user:</p> <ul style="list-style-type: none"> <input type="checkbox"/> administrator <input type="checkbox"/> agent <input type="checkbox"/> supervisor
Groups	Select a group to assign to 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.

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 263).


➤ **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**).

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. Click  to modify the user.

Modify User



First Name

Last Name

Email

Login ID

Alias

OID

Retention Policy

Recording Profile

Media Location

Analytics profile

Legal Hold OFF

Recording license None


Analytics license None

Security Profiles

- administrator
- agent
- supervisor
- system

Groups

- Default

SUBMIT **CANCEL** 

- Update the user information (First name, Last name, Email, Login Id).
- Make sure the email is a valid email.
- 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.
- Click **SUBMIT** to apply changes.

Adding a User Attribute

This section describes how to add a user attribute. The table below describes the purposes of these attributes.

Table 12-4: SmartTAP 360° User Attributes

Attribute Purpose	Priority	Description
Trigger Recording	Critical	Instructs SmartTAP 360° which attribute to use for triggering recording. (i.e., Add SIP_URI If the device makes a SIP call, SmartTAP 360° will trigger a recording based on the SIP_URI, for Teams add OBJECT_ID).
Provide Additional device Info	Optional	Add additional information to the user account within SmartTAP 360°, for example, Ext, Tel URI, Mobile, etc.(for information purposes only). See also Adding a General Device Attribute.

Enhance the integration by mapping SmartTAP 360° attributes to Active Directory attributes to auto-populate device information within SmartTAP 360°. To map a device attribute to an Active Directory device attribute, see [Adding an LDAP Configuration](#) on page 317.

➤ **To add a user attribute:**

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

2. Configure fields according to the table below.

Table 12-5: User Attributes

Field	Description
Name	Unique easily identifiable name to the attribute.
Description	Brief Description of the attribute.
Network Mapping	Indicates whether attribute mapping is required. When selected, the 'Network Mapping Type' drop-down list is displayed.

Field	Description
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

Adding a Microsoft Teams AAD User Attribute

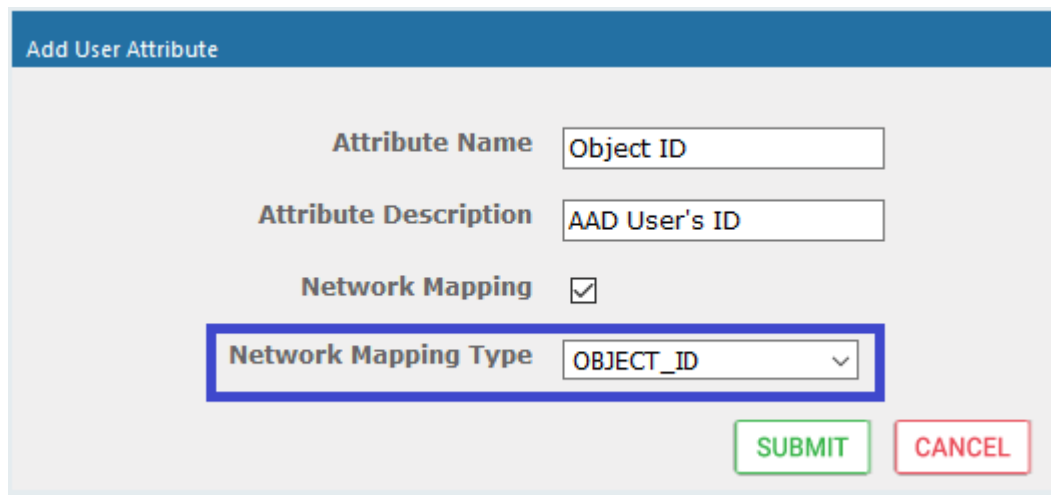
This section describes how to add a custom user attribute for mapping the Object ID of the Microsoft Teams user Active Directory attribute. When the Object_ID is assigned its mapped to the value 'id' which can then be configured in the mapping profile in the Active Directory Configuration (see Step 5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



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° user to Object ID attribute:

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



Add User Attribute



Attribute Name Object ID

Attribute Description AAD User's ID

Network Mapping ☒

Network Mapping Type OBJECT_ID

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 372).
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 12-2: 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] [Delete Icon]

10. Click **SUBMIT** to apply changes.

View and Modify User Attributes

This section describes how to view and modify user attributes.

➤ **To view and modify user attributes:**

1. Open the View/Modify User Attributes screen (**Users > User Management > View/Modify User Attributes**).

Figure 12-3: View/Modify User Attributes

View/Modify User Attributes

Name: Description: Network Mapping: Select One

Modify Delete

Object_ID: OID: OBJECT_ID: [Edit Icon] [Delete Icon]

20 [Navigation Buttons] (1 of 1)


2.  to modify a user attribute.

Figure 12-4: Modify User Attribute

Modify User Attribute

Attribute Name

Attribute Description

Network Mapping ☒

Network Mapping Type

SUBMIT **CANCEL**

3. Configure fields according to the table below.
4. Click **SUBMIT** to apply changes.

Table 12-6: View/Modify Attributes

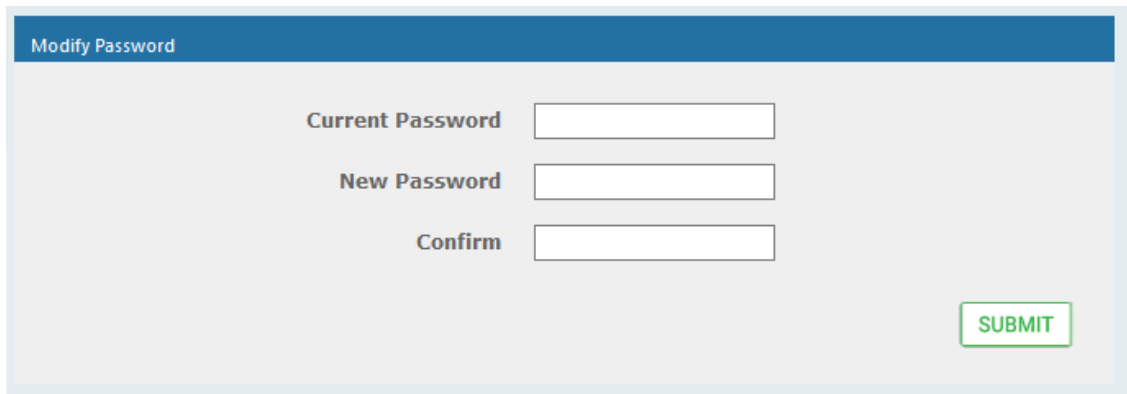
Field	Description
Name	Unique easily identifiable name to the attribute.
Description	Brief Description of the attribute.
Network Mapping	Indicates whether attribute mapping is required. When selected, the 'Network Mapping Type' drop-down list is displayed.
Network Mapping Type	Indicates the type of network mapping that is required for the user. Choose from one of the following values: <ul style="list-style-type: none"> ■ TEL_URI ■ SIP_URI ■ IP_ADDRESS ■ TERMINAL_ADDRESS ■ USERNAME ■ EXTENSION ■ TRUNK_ID ■ OBJECT_ID

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 > **My Settings** folder > **Modify 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 12-5: Change Password

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



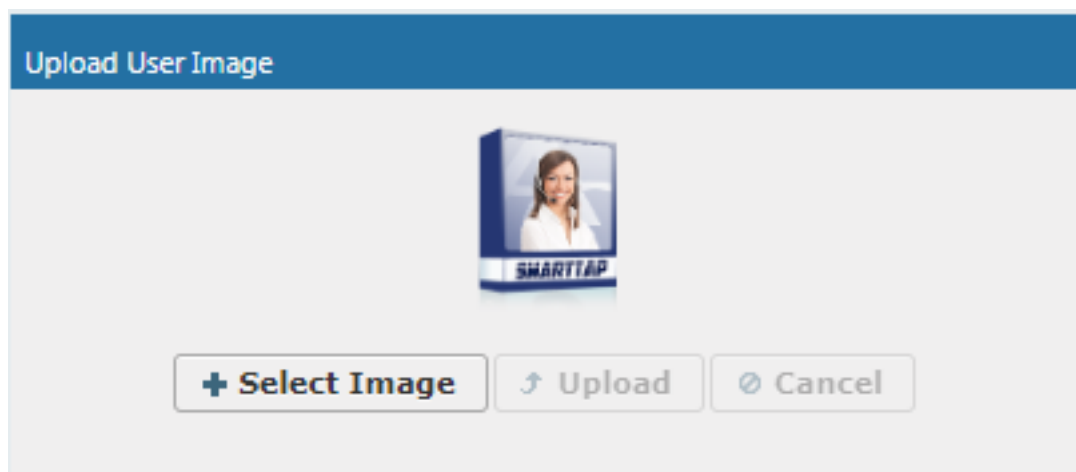
The only method to regain access to the SmartTAP 360° system after a password has been lost is to reset it (users with Add/Modify privileges can reset passwords).

Uploading a User Image

You can upload a user image to display in the passport portrait for the user.

➤ **To upload an image:**

1. Open the Upload User Image screen (**Users** tab > **My Settings** folder > **Upload User Image**).



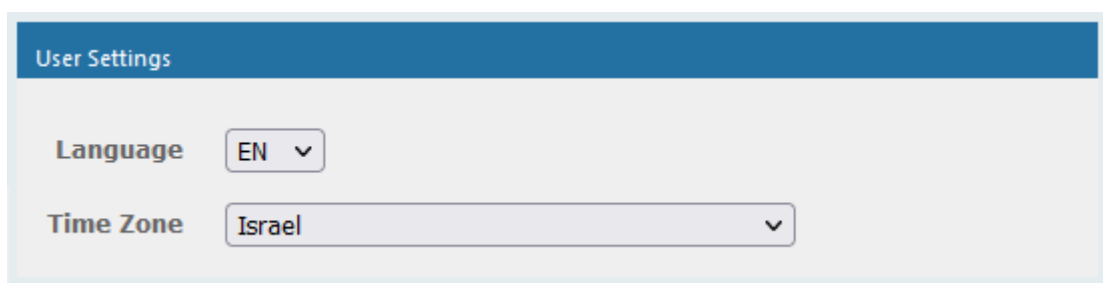
2. Click **+ Select Image** and select the desired image.
3. Click **Upload** to load the user image.

Set Time and Language

This section describes how to change the regional settings including Timezone and Language Settings for a specific user. These settings apply to data displayed in the Web interface (Calls, Alarms and Audit Trail) and in exported data.

➤ To change the language and timezone:

1. Open the Change User Settings page (**Users** tab > **User Management** folder > **Set Time & Language**).



2. From the Language drop-down list, select the required language.
3. From the Time Zone drop-down list, select the required timezone.

13 Skype for Business Features

This section describes the following Skype for Business features:

- [SmartTAP 360° Skype for Business Toolbar](#) below
- [Announcement Server \(Skype for Business\)](#) on page 100

SmartTAP 360° Skype for Business Toolbar

The SmartTAP 360° Skype for Business Toolbar functions in conjunction with the Skype for Business Conversation Window Extension (CWE) which allows the user to have access to in-call features like 'Save on Demand', 'Call Tagging', etc., without needing to open a browser window to access the SmartTAP 360° GUI separately. The toolbar is by default not enabled and must be installed / configured by AudioCodes, a certified AudioCodes Partner or by your local IT expert.



To learn more about Microsoft Skype for Business CWE, refer to:
[http://msdn.microsoft.com/en-us/library/office/jj933101\(v=office.15\).aspx](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.

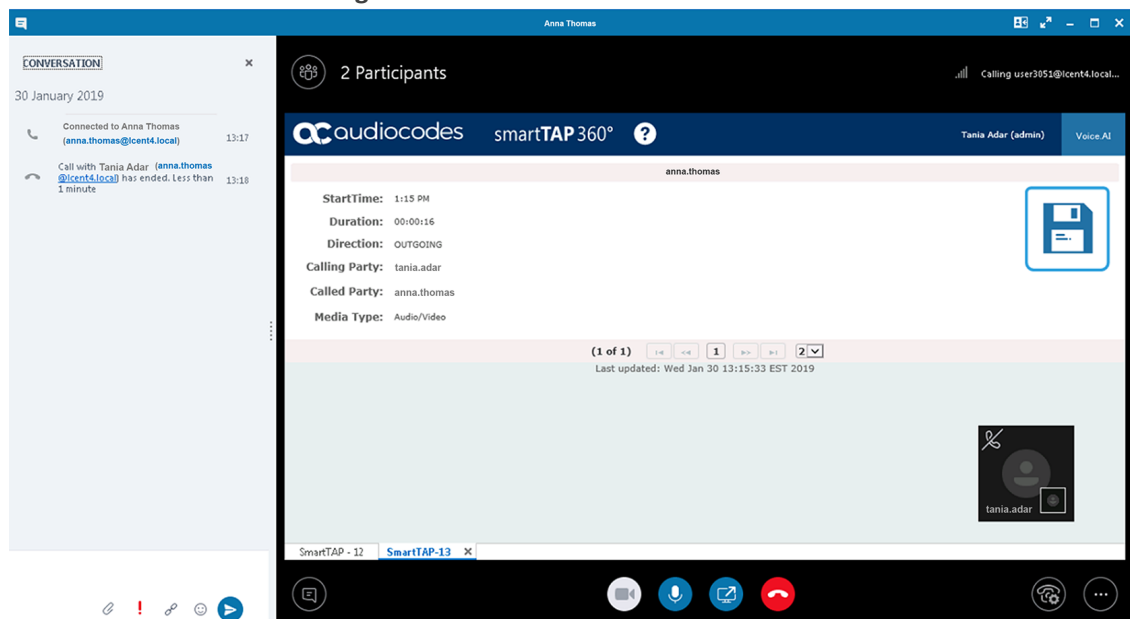
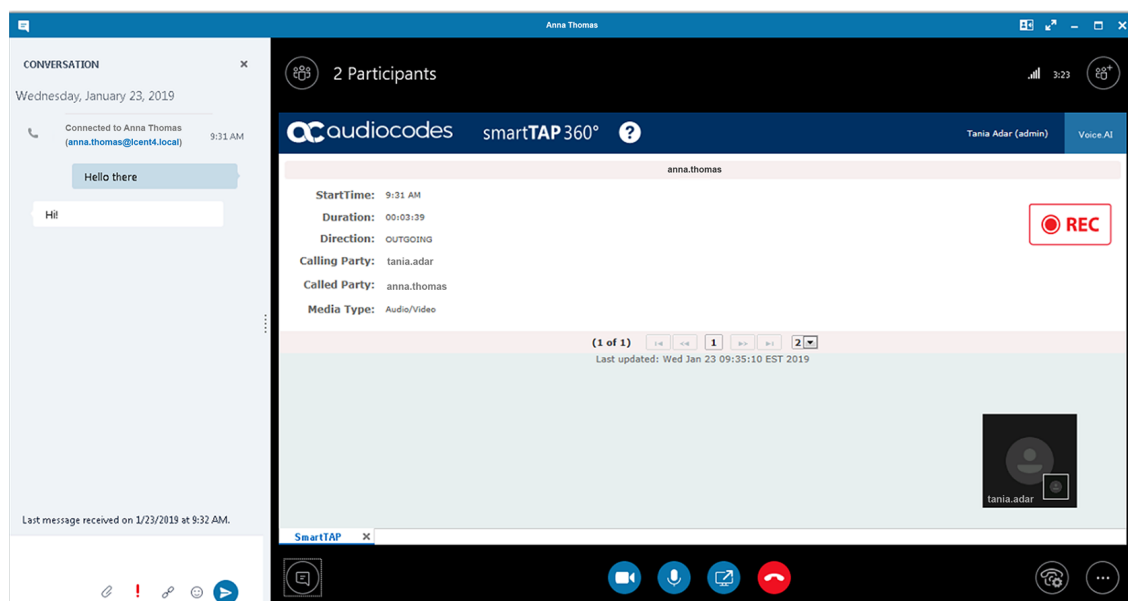
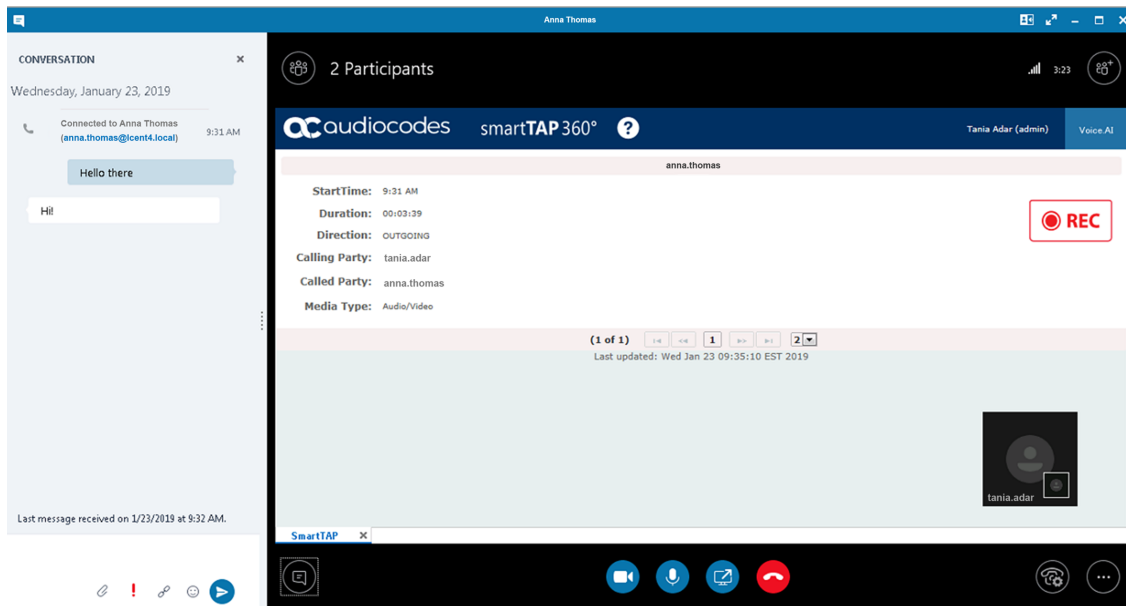
Figure 13-1: SmartTAP 360°: Save On Demand (SOD)**Figure 13-2:****Figure 13-3: Record on Demand (ROD)**

Figure 13-4: SmartTAP 360° Skype for Business CWE Toolbar (Pause / Resume)

Announcement Server (Skype for Business)

SmartTAP 360° offers Announcement Server (AN) in the Microsoft Skype for Business environment to inform the call parties that their call will be recorded. When the Announcement Server (AN) is deployed, SmartTAP 360° directs 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 40 and [Example Announcement Server Scenarios](#) on page 106). For installing and setting up the Announcement server, refer to the [SmartTAP Installation Guide](#).



- SmartTAP 360° requires two concurrent audio recording licenses to record both legs of the announcement part of the call. Make sure that the number of the system's concurrent recording licenses is equal to or higher than the number of concurrent announcements multiplied by 2.
- **For Microsoft Teams:** For Microsoft Teams recording notifications are provided by Microsoft.

This section includes the following:

- [Simple Announcement](#) on the next page
- [IVR](#) on the next page
- [Example Announcement Server Scenarios](#) on page 106
- [Announcement Server Configuration Parameters](#) on page 111

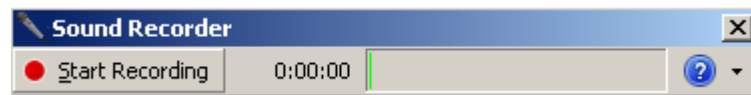
Simple Announcement

SmartTAP 360° can be configured to play announcements to the calling party and if required called parties on a call with a targeted user. The configuration enables setting of announcements to the calling party and if required called parties on a call with a targeted user.

➤ To configure a simple announcement:

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

Figure 13-5: Sound Recorder



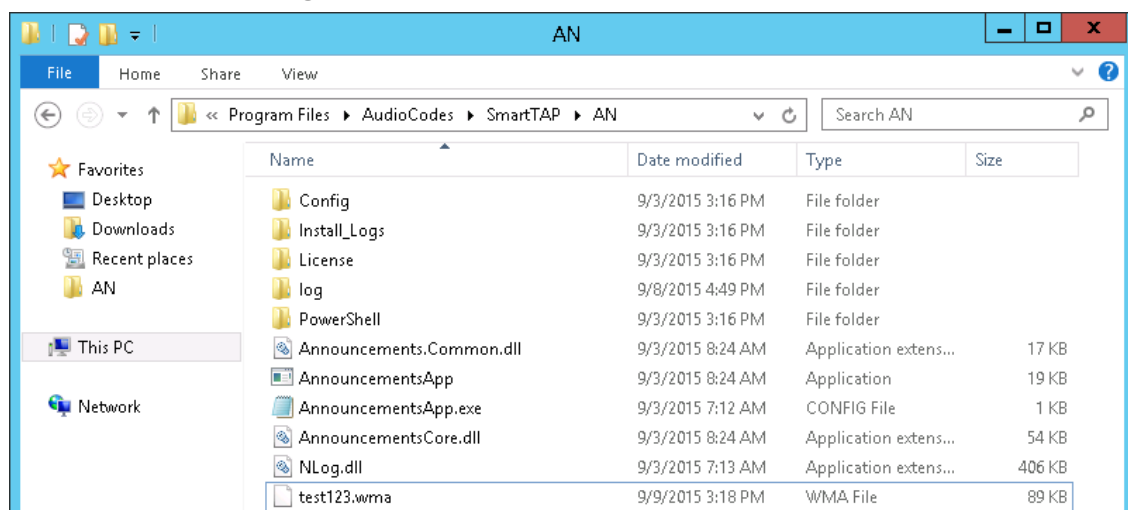
Example: “Thank you for calling Company A, your call may be recorded for quality assurance”.

2. When done, click Stop Recording and it will prompt for the new file destination.
3. Save the file to the following location:
Program Files\AudioCodes\SmartTAP 360°\AN\Config\StateMachineConfig



Ensure that you save the file in WMA format.

Figure 13-6: Announcement Server



IVR

SmartTAP 360° supports interactive voice response (IVR) announcements. The IVR menus are configured by default to request recording consent from a call party(s). These menus can be customized:

- Text-to-speech support is available in 26 languages (see [Enabling Text-to-Speech Platform](#) on page 103)
- Enable Consent to record calls (see [Consent to Record Calls](#) on page 103)

For details on configuring IVR files, see [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 40).

Configuring IVR Script Files

The IVR files are located as follows:

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



IVR scripts files must be saved in JSON format to the StateMachineConfig file in order to be configured in the Recording Profile (see [Managing Recording Profiles](#) on page 40).

- The IVR sample state machines are located under Program Files\\AudioCodes\\SmartTAP 360°\\AN\\Config\\Repo

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

The AN state machine can be fine-tuned according to requirements in the state machine file. The following shows example IVR file :

Figure 13-7: Example IVR Script File

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

Enabling Text-to-Speech Platform

The actual consent to record announcements can be played from a text-to-speech (TTS) file or from a recorded audio file. This section describes how to setup to use the TTS method.

➤ To enable text-to-speech platform:

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

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

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

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

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

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

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



- It is not recommended to install Speech Recognition (SR) files because currently AN doesn't support speech recognition. This feature may be supported in the future. If you install SR files they will not be used and AN behavior is not affected.
- Install platform and language from the same Version 11. A combination of Versions 10 and 11 is invalid.

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

Consent to Record Calls

SmartTAP 360° supports interactive voice response (IVR) announcements requesting consent from the call party to record the conversation of the call. If the call party does not consent, the conversation is not recorded. Below is an example of a call consent prompt:

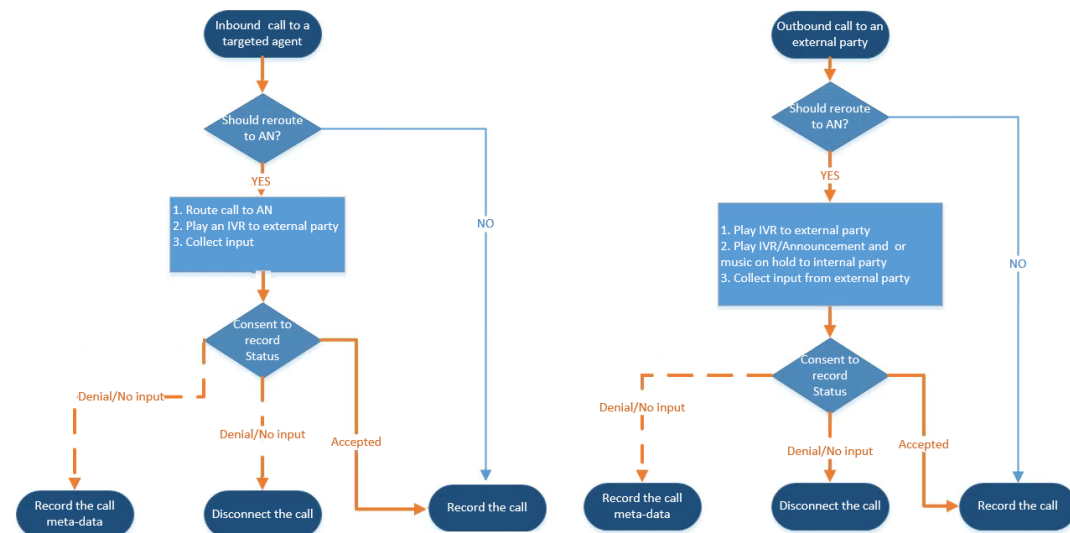
"This call may be recorded for quality assurance purposes. Press one to accept or press zero to continue without recording."



The Demo IVR files provided by SmartTAP 360°, by default, disable call consent.

The following figure illustrates the Call Consent process for Inbound and Outbound calls:

Figure 13-8: IVR Announcements



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

Figure 13-9: 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 13-10: 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 13-11: Call Parties

The screenshot shows the 'Calls' tab in the SmartTAP 360° interface. At the top, there are tabs for 'System', 'Users', and 'Status'. Below these are 'Calls' and 'Evaluation' sub-tabs. The 'Calls' sub-tab is active, showing call details for a call on 05/20/2016 from 8:05 AM to 10:05 AM. Below the call details are checkboxes for 'Active Users', 'Inactive Users', 'Active Devices', and 'Inactive Devices'. There are also radio buttons for 'Users/Devices' (selected) and 'Groups'. A list of users/devices is shown, including Adar, Tania; Admin, Local; Campos, Jose; Carosella, Gino; Conlon, Tom; Da Silva, Sandy; DCI; Dougher, Michael; Dutta, Debajyoti; and Herberger, Steven. The 'Call Parties' section is highlighted with a blue box and contains three rows: 'Calling' with the value 'Consent Declined*', 'Called' with an empty field, and 'Answered' with an empty field. Below this is the 'Call Tags' section with checkboxes for 'Active Tags' (checked) and 'Inactive Tags'. There are also fields for 'Tag Name' (a dropdown menu showing 'Select One') and 'Tag Value'. A 'Search' button is at the bottom.

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 13-12: 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 13-13: 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

☐ 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 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 13-1: Call Transfer Scenarios

Call Scenario	Targeted Users	Flow and expected results from Announcement Server*
Supervised/blind transfer	A	1. A calls B, B answers: announcement is played.

Call Scenario	Targeted Users	Flow and expected results from Announcement Server*
		<ol style="list-style-type: none"> 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 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

Call Scenario	Targeted Users	Flow and expected results from Announcement Server*
		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 13-2: Call Forwarding and Simultaneous Ringing

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

- **Conferences:** Playing announcements on the calls of targeted users with a conference bridge are not currently supported. with SmartTAP 360° team the feature status if you need it.
- **Video calls:** Video calls routed to the ANN are handled as audio-only calls, the video part of the call is stripped. Once the call is transferred to the original destination the video of the call can be re-initiated.
- **Mobile Clients and Voice Mail:** Announcements are played for calls with mobile clients as defined in previous sections with an exception to the following scenarios:
 - The AN is configured to play an announcement to the calling party only mode (AnnouncementRecipients=CallingParty). The mobile client calls to another party where the mobile client, another party or both are targeted users. In this scenario, the announcement is not played.
 - The AN is configured to play an announcement to both parties mode (AnnouncementRecipients=BothParty). The mobile client calls to another party where the mobile client, another party or both are targeted users. The call is answered by voice mail. In this scenario, the announcement is not played.

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

Announcement Server Configuration Parameters

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

Table 13-3: 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 "".
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".

Parameter	Description
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".
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 "

Parameter	Description
	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	<p>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.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ True ■ False (default)
uaReceiveReferRegex	<p>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.</p> <p>Default value:</p> <p>"PolycomVVX-VVX_500"</p>
asList	<p>Application server comma-separated list. AN sends alarms to the AS in the list.</p> <p>For example</p> <p>http://10.21.8.120:80,https://10.21.80.170:443</p>
restClientTimeoutMilliseconds	<p>Alarms timeout in milliseconds.</p> <p>Default Value: 5000</p>
normalizeNumbers	<p>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.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ True ■ False (default)

Parameter	Description
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: <ul style="list-style-type: none"> ■ True (disable) ■ False (default)
uaDontReceiveReferRegex	A regular expression (case insensitive). If the value of the UserAgent header matches the expression then the SIP REFER is not sent to that device when rerouting the call to the original destination. This solves the problem for Skype for Business clients when answering '488 not acceptable' on reception of SIP INVITE with replaces from the mobile clients. Default Value: "ucwa"
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 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

Parameter	Description
	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 Installation Guide](#).

14 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 5/30/21 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

0:00 0:30 1:00 1:30 2:00 2:30 3:00 3:30 4:00 4:30 5:00

0.2 1.0 5.0

⏮ ⏪ ⏩ ⏭ 🔊

Figure 14-1: Call Search

The screenshot displays the 'Call Search' interface. At the top, there are tabs for 'System', 'Users', and 'Status'. Below these are 'Calls', 'Messages', and 'Evaluation' tabs, with 'Calls' being the active tab. A 'Search Criteria' section includes a 'Custom Dates' dropdown, a '1' input field, and date/time pickers for 'From' (6/19/22, 1:27 PM) and 'To' (6/19/22, 2:27 PM). Checkboxes for 'Active Users', 'Inactive Users', 'Active Devices', and 'Inactive Devices' are present, along with radio buttons for 'Users/Devices' (selected) and 'Groups'. A 'Users/Devices' section has a 'Select All' checkbox and a list of 'ST-Teams07', 'ST-Teams09', and 'ST-Teams20'. Below this is a 'Call Parties' section with input fields for 'Calling', 'Called', and 'Answered'. The 'Call Tags' section includes checkboxes for 'Active Tags' and 'Inactive Tags', and a 'Tag Name' dropdown set to 'Select One'. An 'Analytics Categories' list shows 'Paperless Campaign', 'Extended Contract', 'Category_1', and 'Category_2'. A 'SysCall ID' input field is also present. The 'Analytics Sentiment' section has dropdowns for 'Positive %' and 'Negative %'. A 'Search' button is located at the bottom right of the search criteria section. Below the search results, a 'Saved Searches' section shows a list of saved searches, with the first one being 'No records found.' and a '(1 of 1)' indicator.

Figure 14-2: Search Calls Navigation Screen - Calls Tab

Field	Description
From:	Earliest date and time to search from. Click the date field for a calendar

Field	Description
	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 drop-down, change the time of day.
Active Users	Users whose accounts are enabled in the SmartTAP 360° system.
Inactive Users	Users whose accounts have been deleted from the SmartTAP 360° system.
Active Devices	Devices that are not associated with users enabled in the SmartTAP 360° system and can be targeted for recording.
Inactive Devices	Devices that have been deleted from the SmartTAP 360° system.
Users/Devices	Only Users and Devices will be listed in the search list. Either the Users/Devices or the Groups option must be selected.
Groups	Only Groups will be listed in the search list. Either the Users/Devices or the Groups option must be selected.
User/Devices: (list)	To select multiple Users/Devices, select each 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.
Analytics Categories	To select multiple categories, select each category name while holding <ctrl>; or all within a range by clicking the top category and bottom category while holding <shift>.
SysCall ID	Filter by SysCall ID
Analytics	Select whether the positive analytical sentiment must be greater or

Field	Description
Sentiment	less than a specified percent. Alternatively, select whether the negative analytical sentiment must be greater or less than a specified percent.
Saved Searches	You can save search criteria as a query and then later retrieve it.
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 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 137.

Table 14-1: Search Calls Results

Field	Description
	Launches the Add and Remove Columns dialog.
	<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.
	Silent Media – Indicates when media files associated with the call are silent; the packets were received however didn't carry audio.

Field	Description
	None – There are no reasons.
	Indicates that a tag has been associated with a recording.
	Indicates that no tags are associated with a recording
	Deletion
	Pending Deletion
Analytics Profile	Indicates the Analytics profile that has been assigned to the user.
Analytics Status	<p>Indicates the Analytics status:</p> <ul style="list-style-type: none"> ■ Not Assigned: An Analytics profile is not assigned for this user. ■ No License: The number of Analytics license hours has reached its limit. ■ No Transcription: No transcription was generated for this user. This may occur if the media file was not yet transferred to the media storage location. ■ In Progress: The transcription generation is in progress. ■ Analytics Error: An error occurred in the generation of the transcript. ■ Exists: The transcript has been successfully generated; click the entry to view the transcript. ■ Deleted: The transcript has been deleted.
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.
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
Direction	The column represents Call Direction (Incoming, Outgoing). Clicking this header sorts the search results in Ascending/Descending order alternating with each click. Drop down entry shows only the matching results.
Display Video	Displays the video screen. When you select the  button, the recorded video is replayed.
Duration	Call Duration. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
Expires Calls	<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>
Media Status Reason	Corresponding Media Reason
Media Type	<p>Indicates the media type. One of the following values:</p> <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. ■  Indicates that the call audio has been successfully recorded.

Field	Description
	<ul style="list-style-type: none"> ■  Indicates that the call video has been successfully recorded. ■  Indicates that the Video and Screen Sharing has been successfully recorded. ■ None
None	None - Indicated when there are no media files and the call was not answered i.e. Abandoned or Missed.
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>
Release Calls Details	<p>Release Cause of the Original Call. Applicable to Skype For Business. Example: "Call failed to establish due to a media connectivity...;22</p> <p>"Action initiated by user";51004;.</p>
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.
Start Time	Date and time the call recording started. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.
SysCall 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.
Tags	Identifies whether tag have been defined for the call as follows
User/Device	User/Device name. Clicking this header sorts the search results in Ascending/Descending order alternating with each click.

➤ **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 14-3: Add/Remove Columns from the Search Call Results Screen

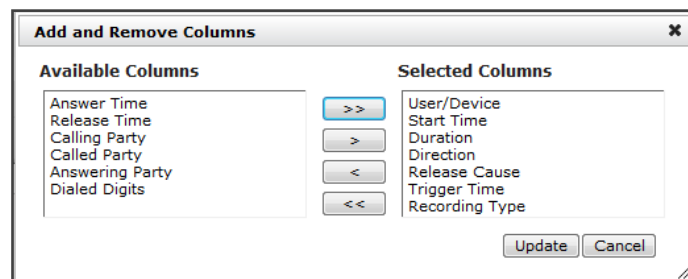
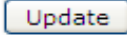
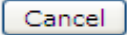


Table 14-2: Add and Remove Columns – Field Descriptions

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 14-3: Add and Remove Columns

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

Field	Description	
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	<ul style="list-style-type: none"> ■ Full Time ■ Record on Demand ■ Save on Demand 	
Expires	Call recording expiration date. The date after which the call recording is purged. The date is calculated based on the retention profile assigned to the call. If the call was put on legal hold or evaluated, the expiration date is presented along with a lock icon.	
System Call ID	Indicates the Original Call ID. Applicable to Skype For Business and other SIP-related integrations. This ID can be used to correlate call records to the original calls.	
Conversation ID	Indicates the Skype For Business Conversation ID. This ID can be used to correlate between audio/video and content sharing calls made by a user from SFB client as part of one conversation.	
Conference ID	Indicates the Skype For Business Conference ID. This ID identifies the conference to which the call was connected. It can be used to correlate between audio/video and content sharing calls made by a user from a Skype for Business client.	
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.	

Field	Description
Analytics Status	Indicates the status of the Analytics license as described above in table "Search Call Results".
Analytics Profile	Indicates the Analytics profile that has been assigned to the user.

Search by Date

This section describes how to search for calls by date.

➤ To search for calls by date:

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 14-4: 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 14-5: Calendar Search

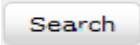
4. Click **Search**.

Searching by Users and Devices

This section describes how to search by different Calling Parties.

➤ To search by different calling parties:

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:
 - Select the type of Users and Devices.
 - Select either the Users/Devices or Groups Radio button.
 - Selecting the User/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).
 - Select one of more User/Devices or Groups by highlighting them in the list (see notes on Search Calls Navigation screen field descriptions above on how to select more than one User/Device or Group).

8. Click  to start the search for calls matching the search criteria.

Calling Parties Search

This section describes how to search by different calling parties.

➤ **To search for calls by Calling, called and/or answered party:**

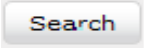
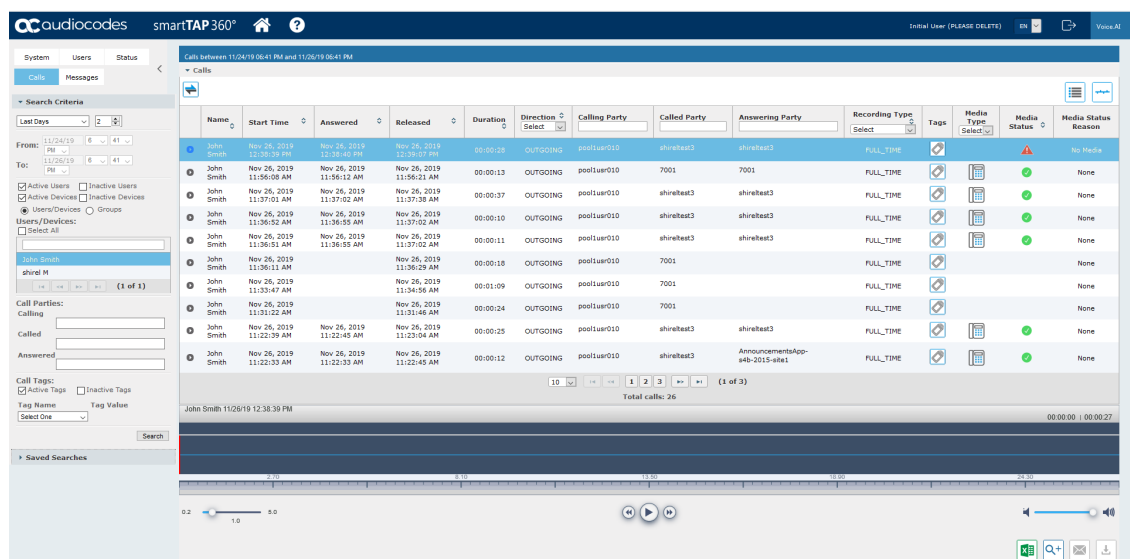
1. Open the Search Calls screen by clicking the **Calls** tab.
2. Click  to start the search for calls matching the search criteria; the Results are displayed in the Search Calls Results screen to the right. The figure below shows a search for the last two days for user "John Smith".

Figure 14-6: Retrieved Calls List for Specific User



The screenshot shows the SmartTAP 360° interface. The 'Calls' tab is selected. Search criteria are set for 'From: 11/24/19 PM' to '11/26/19 PM' and 'To: 11/24/19 PM' to '11/26/19 PM'. The 'Calling Parties' section shows 'John Smith' and 'shirley H'. The 'Call Tags' section shows 'Active Tags' and 'Inactive Tags'. The 'Call Tags' section also shows 'Tag Name' and 'Tag Value'. The 'Search' button is visible. The 'Retrieved Calls List' shows a table of calls for 'John Smith' between 11/24/19 PM and 11/26/19 PM. The table has columns: Name, Start Time, Answered, Released, Duration, Direction, Calling Party, Called Party, Answering Party, Recording Type, Tags, Media Type, Media Status, and Media Status Reason. The table shows 10 calls, all outgoing, with durations ranging from 00:00:10 to 00:00:25. The 'Media Status' column shows 'None' for all calls. The 'Media Status Reason' column shows 'No Media' for all calls. The 'Total calls: 26' is displayed at the bottom of the table.

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 11:24:19 PM	Nov 26, 2019 11:24:19 PM	Nov 26, 2019 11:24:19 PM	00:00:25	OUTGOING	pooluser010	shirleyH3	shirleyH3	FULLTIME			None	No Media
John Smith	Nov 26, 2019 11:56:08 AM	Nov 26, 2019 11:56:12 AM	Nov 26, 2019 11:56:21 AM	00:00:13	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:37:01 AM	Nov 26, 2019 11:37:02 AM	Nov 26, 2019 11:37:38 AM	00:00:37	OUTGOING	pooluser010	shirleyH3	shirleyH3	FULLTIME			None	
John Smith	Nov 26, 2019 11:36:52 AM	Nov 26, 2019 11:36:55 AM	Nov 26, 2019 11:37:02 AM	00:00:10	OUTGOING	pooluser010	shirleyH3	shirleyH3	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	shirleyH3	shirleyH3	FULLTIME			None	
John Smith	Nov 26, 2019 11:36:11 AM	Nov 26, 2019 11:36:11 AM	Nov 26, 2019 11:36:29 AM	00:00:18	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:33:47 AM	Nov 26, 2019 11:33:47 AM	Nov 26, 2019 11:34:56 AM	00:01:09	OUTGOING	pooluser010	7001	7001	FULLTIME			None	
John Smith	Nov 26, 2019 11:33:12 AM	Nov 26, 2019 11:33:12 AM	Nov 26, 2019 11:33:12 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	shirleyH3	shirleyH3	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	shirleyH3	AnnouncementsApp-44b-2015-v1at	FULLTIME			None	

Search by Call Tags

This section describes how to search by Call Tags.

➤ **To search for calls by call tags:**

1. Open the Search Calls screen by clicking the **Calls** tab.
2. Optionally, specify a Call Tag & Value.

Figure 14-7: Call Tags

Call Tags:

☒ Active Tags ☐ Inactive Tags

Tag Name	Tag Value
ActionItem	Schedule Meeting

Search

- 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 14-8: Call Tags

Call Tags:

☒ Active Tags ☐ Inactive Tags

Tag Name	Tag Value
ActionItem	Schedule Meeting

Search

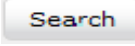
Context menu options: Insert Row, Delete Row

Call Tags:

☒ Active Tags ☐ Inactive Tags

Tag Name	Tag Value
ActionItem	Schedule Meeting
Company	AudioCodes

Search

- 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 TagAction 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 14-9: Search Calls Results

The screenshot shows the SmartTAP 360° interface. On the left, there's a sidebar with 'Search Criteria' including filters for 'Last Days', 'From', 'To', 'Active Users', 'Inactive Users', 'Active Devices', 'Inactive Devices', 'Users/Devices', and 'Groups'. The main area displays a table of call records with columns: Name, Start Time, Answered, Released, Duration, Direction, Calling Party, Called Party, Answering Party, Recording Type, Tags, Media Type, Media Status, and Media Reason. A call record for 'John Smith' is selected. A 'Call Tags' dialog box is open, showing a table with columns: Tag, Date Added, Added By, Value, and Private. The dialog shows a tag 'Personal Call' added on 'Nov 26, 2019' by 'Initial User (PLEASE DELETE)' with a value of 'true' and 'Private' set to 'true'.



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

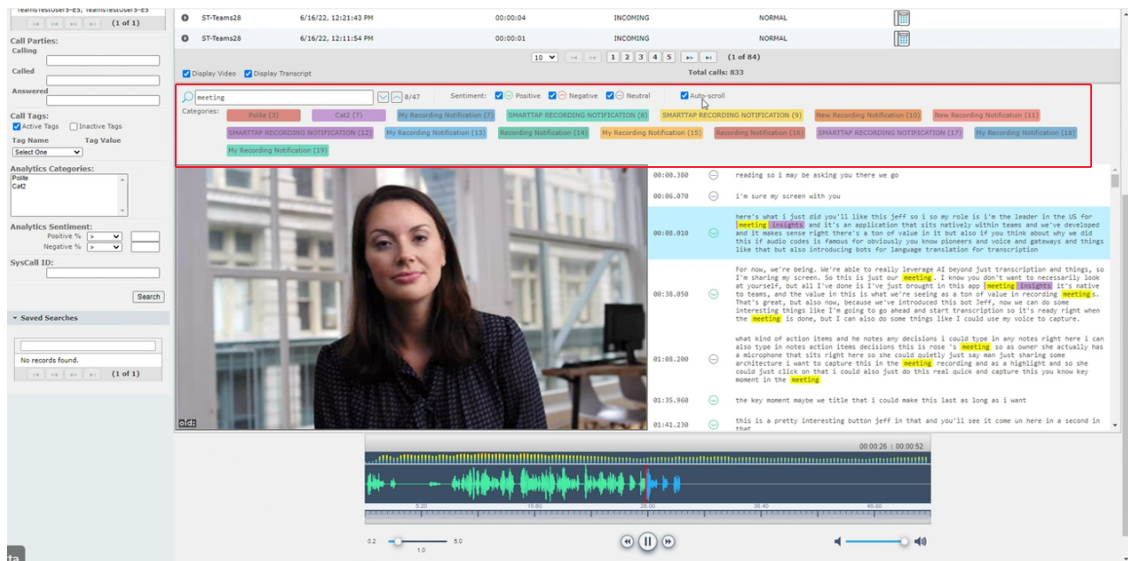
Search by Analytics Category

Searches can be refined for calls matching specific Analytics categories. In the retrieved search results, select a call record; the matching categories are displayed in the Analytics toolbar. Transcript is by default displayed.

Figure 14-10: Analytics Categories in an Audio Call

The screenshot shows the SmartTAP 360° interface with analytics categories. The sidebar on the left has 'Search Criteria' and 'Analytics Categories' (Positive, Negative, SysCall ID). The main area displays a table of call records. A call record for 'ST-Team28' is selected. The 'Display Transcript' checkbox is checked. Below the transcript, there's a section for 'Analytics Categories' showing various categories like 'SmartTAP RECORDING NOTIFICATION', 'Recording Notification', and 'New Recording Notification'. The transcript text is visible, showing a conversation between two people. At the bottom, there's an audio player with a timeline and playback controls.

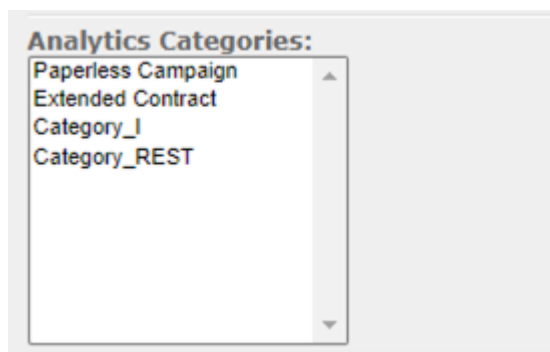
Figure 14-11: Analytics Categories in a Video Call



➤ To search for calls by Analytics categories:

1. Open the Search Calls screen by clicking the **Calls** tab.

Figure 14-12: Analytics



2. In the **Analytics Categories** section, select one or more categories.
3. Click **Search** to start the search for calls matching the search criteria.
4. Select one the retrieved call records to display the Analytics toolbar.
5. Select the **Display Transcript** check box to display the recorded text transcript. Note that keywords matching the categories configured in the Analytics profile are displayed.

Calls before 12/26/22 5:17 AM

Name	Start Time	Answered	Released	Duration	Direction	Calling Party	Called Party	Answering Party	Dialed Digits	Release Cause	Recording Type	Triggered	Calls Expires	Video and Desktop Sharing Expires	Tags	Media Type	Media Status	Media Reason	Conversation ID	Conf
Fedida, Gd (@audcode.biz)	12/26/22 5:17:13 PM	12/26/22 5:17:16 PM	12/26/22 5:17:25 PM	00:02:12	INCOMING	CONFERENCE...	Fedida, Gd (@audcode.biz)	Conference	NORMAL	FULL TIME	Dec 5, 2022									

Display Transcript

Search text in transcript

Sentiment: ☒ Positive ☒ Negative ☒ Neutral ☒ Auto-scroll

Categories: **Polite (3)** Competitor Mention (2) No Mention of Recording (sec... (0)

00:25.740 so if you hear all that typing in the in the background i know that can be quite annoying

00:30.880 all right so uh customer michael after pulling up your account i do see that you've got a really awesome deal that that we have in place that could be really beneficial for you

00:44.120 we do see that you are, you are a you are billed via the mail and we do have a current discount happening right now that if you switch over to **business** billing, which is essentially our **business** program, you'll be able to get a 5% discount on.

01:02.630 on services. How does that sound?

01:04.950 oh, it sounds great. Awesome. awesome. Really, really love having your business.

01:11.140 You know, there's a few other things i'm seeing too. Ohh, you, you did want to mention that you have a lot of other competitors that you're looking at that could potentially have some better deals. Yeah, i think we do compete really well with **business** on

01:29.570 There's a few others out there too. You know, if you, you mentioned **business** i, you know, i think that we've got better services and products there and we'd really hate for you to leave the, you know, leave our services.

01:41.350 last thing michael is i do see that you've got a contract coming up to to be renewed would you like to renew that contract

01:49.000 that would be it would be really great if you could renew the contract and you could stay part of this awesome business

01:55.690 oh, you would love to renew it for \$1,000,000. That is perfect. We love that and we love your business and we appreciate you and have a great rest of your day. we thank you, michael. Goodbye.

Each category is assigned a different color. By default, all the matching words from a category are highlighted inside the transcript using the category color.

Categories: **Polite (3)** Cat2 (7)

Search text in transcript

Sentiment: ☒ Positive ☒ Negative ☒ Neutral ☒ Auto-scroll

Categories: **Polite (3)** Cat2 (7)

00:00.380 reading so i may be asking you there we go

00:06.070 i'm sure my screen with you

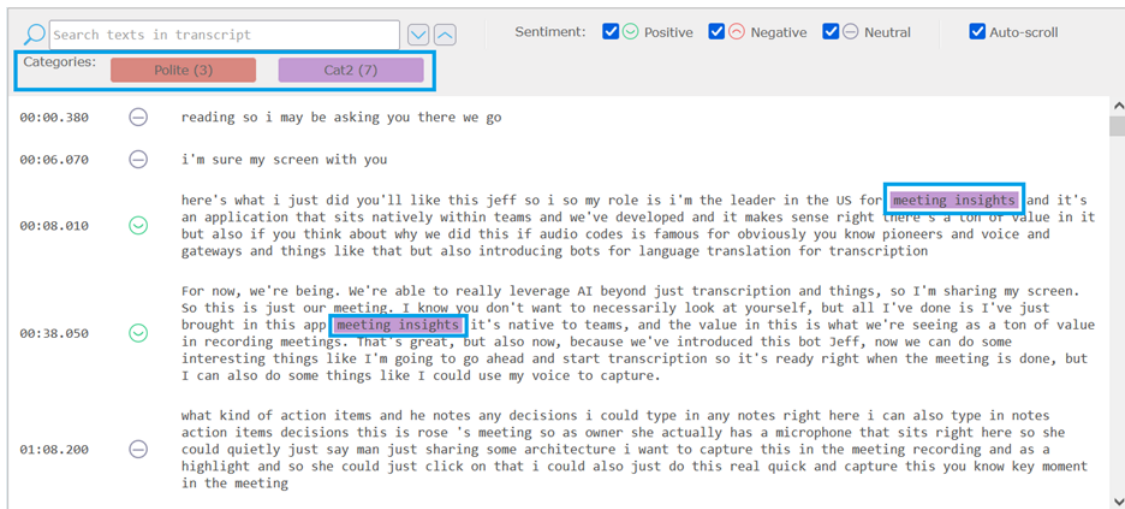
00:08.010 here's what i just did you'll like this jeff so i so my role is i'm the leader in the us for **meeting insights** and it's an application that sits natively within teams and we've developed and it makes sense right there's a ton of value in it but also if you think about why we did this if audio codes is famous for obviously you know pioneers and voice and gateways and things like that but also introducing bots for language translation for transcription

00:38.050 For now, we're being. We're able to really leverage AI beyond just transcription and things, so i'm sharing my screen. So this is just our **meeting**. I know you don't want to necessarily look at yourself, but all i've done is i've just brought in this app **meeting insights** it's native to teams, and the value in this is what we're seeing as a ton of value in recording meetings. That's great, but also now, because we've introduced this bot Jeff, now we can do some interesting things like i'm going to go ahead and start transcription so it's ready right when the meeting is done, but i can also do some things like i could use my voice to capture.

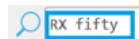
01:08.200 what kind of action items and he notes any decisions i could type in any notes right here i can also type in notes action items decisions this is rose 's meeting so as owner she actually has a microphone that sits right here so she could quietly just say man just sharing some architecture i want to capture this in the meeting recording and as a highlight and so she could just click on that i could also just do this real quick and capture this you know key moment in the meeting

When one or more categories are selected, only those phrases with matching categories are displayed. In the following screen, the user has selected category "Polite".

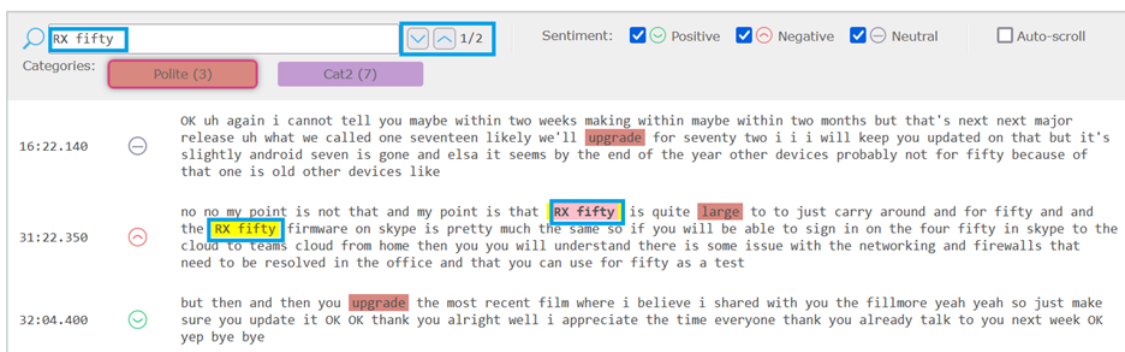
Categories: **Polite (3)** Cat2 (7)



6. In the search field, enter the phrase for which you wish to search in the transcription.



7. Use the navigation buttons  to toggle between retrieved entries of the phrase.



Search by SysCall ID

This section describes how to search by SysCall ID.

➤ To search for calls by SysCall ID:

1. Open the Search Calls screen by clicking the **Calls** tab.
2. In the SysCall ID section, type in the **SysCall** ID.
3. Click to start the search for calls matching the search criteria.

Search by Analytics Sentiment

You can filter calls to query sentiment levels. In the example shown below, the Positive sentiment is set to "20" and the Negative sentiment is set to "40". All calls matching these sentiment ranges are retrieved. The sentiments are calculated by the Microsoft Cognitive Services Speech-to-text algorithms for the call transcriptions.

➤ **To search for calls by Analytics sentiment:**

1. Open the Search Calls screen by clicking the **Calls** tab.
2. In the search criteria set the Analytics sentiment **Positive** or **Negative** sentiments as follows:
 - From the **Positive** drop-down list, select an operand value (<, = or >) and then enter a numeric value.

OR

 - From the **Negative** drop-down list, select an operand value (<, = or >) and then enter a numeric value.

In the image below, Positive Sentiment is set to **20** and Negative Sentiment is set to **40**. This search criteria is then reflected in the search results.

Call Parties:
 Calling
 Called
 Answered

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

Analytics Categories:
 Polite
 Cat2

Analytics Sentiment:
 Positive % > 20
 Negative % > 40

SysCall ID:

▼ **Saved Searches**

No records found.

3. Click to start the search for calls matching the search criteria.

Results are retrieved with the matching criteria.

Release Cause	Analytics Profile	Analytics Categories	Analytics Sentiment
Select			
NORMAL	analytics11	cat2(4), cat1(3)	<div> <input checked="" type="radio"/> 20% <input type="radio"/> 30% <input type="radio"/> 40% </div>

1 (1 of 1)

4. Select **Display Transcript** check box to display the transcript. Notice that each segment in the transcript includes a color-coded icon reflecting the degree of sentiment.

The screenshot shows a call transcript for ST-Teams28 on 6/16/22 at 12:21:43 PM. The transcript is displayed in a list format with time stamps and sentiment icons. A blue box highlights the sentiment icons for the first five segments: a green smiley face for positive sentiment and a red frowny face for negative sentiment. The transcript text includes: "We left off. That's a pretty critical. Everyone really loves. That feature is probably the right way to say that.", "And then quickly I want to show you just where this goes. You're in my team's client right now. I've just got meeting Insights pinned. This is our meeting right now. Let me go to one that I have is a favorite just to give you a quick example. So what will happen is.", "This is Anderson windows and doors are familiar with them.", "they're going to move forward with us as well and what i've done here in this meeting sorry i'm i'm on my laptop so this this is going to look a little squished the resolution is not good but here's the highlights we had for this any bookmarks here's the transcript i can search in this jeff", and "yeah so i want to see where microsoft was mentioned or meeting inside it's or anything like that here's the power of this engine what we've done is we've done some language processing to match up with content being shared so in this meeting this is pretty critical stuff a lot of people like to analytics that we gather from our meetings across our enterprise".



All sentiments are by default enabled.

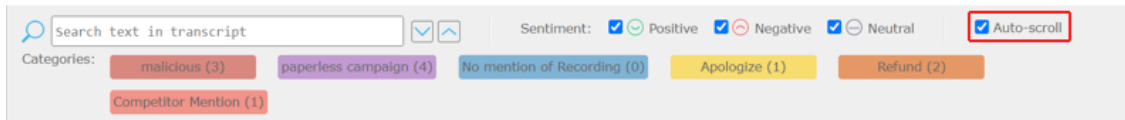
The screenshot shows a call transcript for ST-Teams28 on 6/16/22 at 12:21:43 PM. The transcript is displayed in a list format with time stamps and sentiment icons. A red box highlights the sentiment icons for the first five segments: a green smiley face for positive sentiment and a red frowny face for negative sentiment. The transcript text includes: "Hi we'd like to offer you paperless billing, where if you are willing to switch over we will give you five percent off of your next bill.", "I'm so sorry about your recent experience sir, let me see how I can help you.", "I'd like to return this product.", "It has been off and on from the very start.", "So your product isn't working and you'd like me to establish a refund for you?", "I may switch over to verizon if i keep having these issues with you guys.", and "I will complain to the police if you keep threatening me.".

The phrase level sentiments are displayed with the transcription. A sentiment filter (above the transcription) allows you to display or hide phrases in the transcription based on the selected sentiments (one or more values can be selected):

Sentiment Icon	Description
	Positive sentiment.
	Negative sentiment.


Sentiment Icon	Description
	Neutral sentiment.

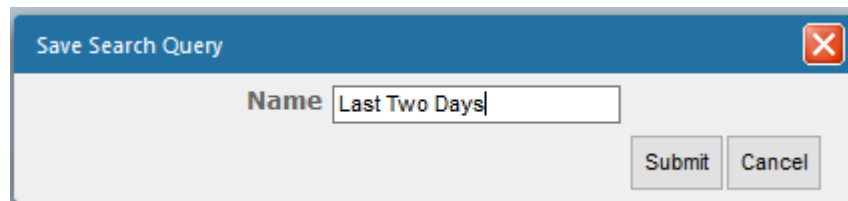
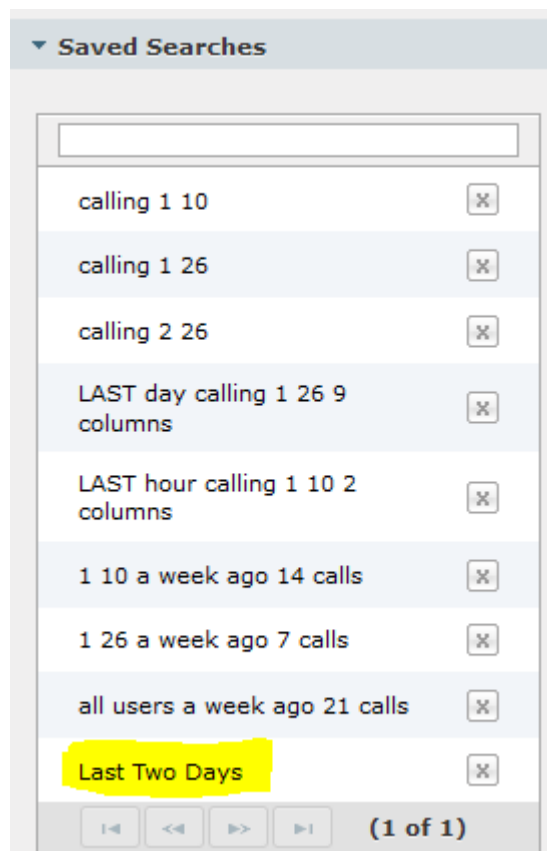
Select the **Auto-scroll** check box to enable auto-scrolling for transcript recording text.



Saving Search Queries

You can save search criteria as a query and then later retrieve it. Save the search criteria by

selecting the  located at the bottom right of the call list. 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.

Deleting Calls and Instant Messages



SmartTAP 360° is deployed in several recording scenarios such as compliance, quality monitoring and for malicious call recordings. While regulatory compliance requires that recordings are deleted automatically after a regulated time frame, quality monitoring scenarios requires the ability to manually delete recordings. Consequently, calls and instant messages conversations can be deleted on demand by users with the appropriate permissions in security profiles (see [Managing Security Profiles](#) on page 35).



- This feature is enabled through the SmartTAP 360° 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 81).
- 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 119).

2. Select the  button adjacent to each call that you wish to delete. The button becomes  red.



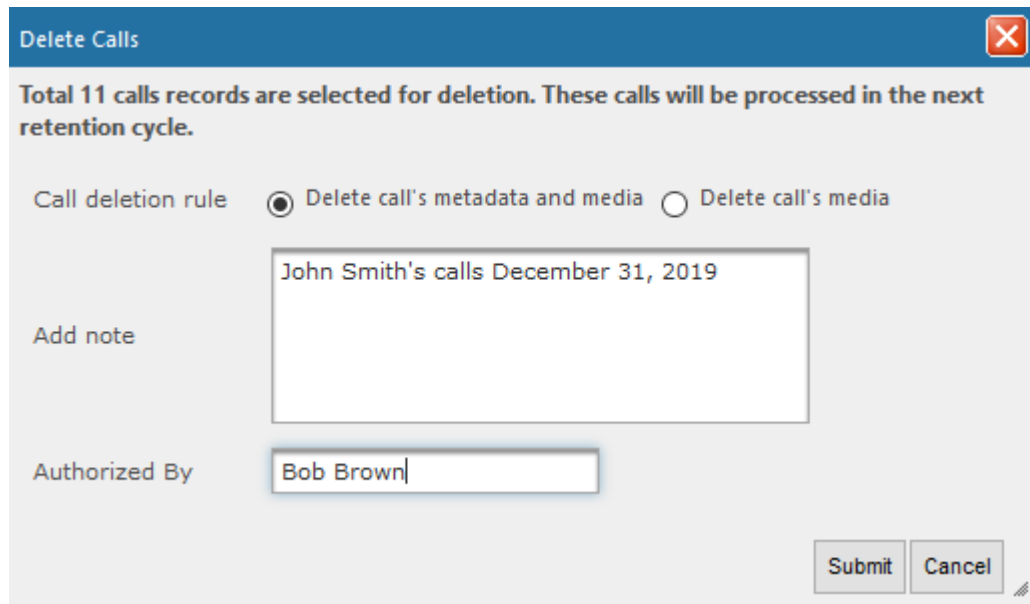
Only the filtered and selected recordings are deleted.

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

	Name	Start Time	Duration	Direction	Release Cause	Media Type
	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:



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.

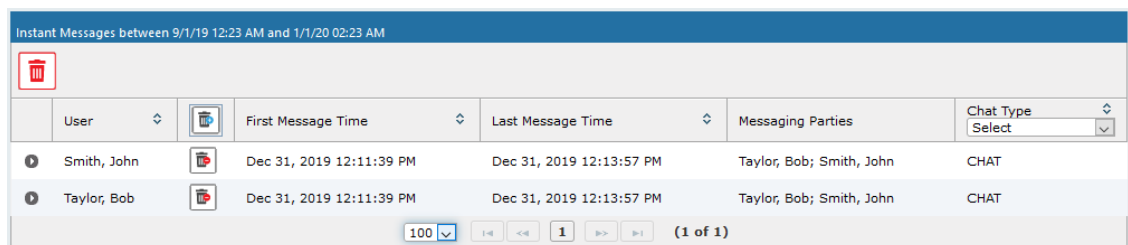
You can monitor the deletion process in the Audit Trails page:

Figure 14-13: 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 14-14: 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

100 1 (1 of 1)

Call Transfer Information

The Transferred by a Party data is displayed in the Call Details as highlighted below. Party A answers the call and then transfers to Party B (meta data displays that Party A answered the call and was transferred By Party. Party B's meta data shows that the call was transferred by Party A.

The screenshot displays the SmartTAP 360° Live interface. The top navigation bar includes 'System', 'Users', and 'Status' tabs. The main content area is titled 'Calls' and shows a detailed view of a specific call. The call details include:

- From:** MI-Team05, MI-Team05(MI-Team05)
- To:** 7/7/22, 1:56:16 PM
- Duration:** 00:00:14
- Direction:** INCOMING
- Release Cause:** MISSED
- Answer Time:** 7/7/22, 1:56:50 PM
- Release Time:** Jul 7, 2022, 1:56:50 PM
- Calling Party:** Name: +97239766000, Transferred By: Ron Miller
- Called Party:** Name: MI-Team05, MI-Team05(MI-Team05)
- Recording Type:** FULL_TIME
- Triggers:** Expires: Media Status: NONE, Media Status Reason: None, SysCall ID: 5119500-c0a-4f0c-a318-eaf5535d194, Conversation ID: Conference ID: Release Cause Details: Analytics Status: No transcription, Analytics Profile: SmartTapAnalyticsProfile, Analytics Categories: Analytics Details: Analytics was not triggered

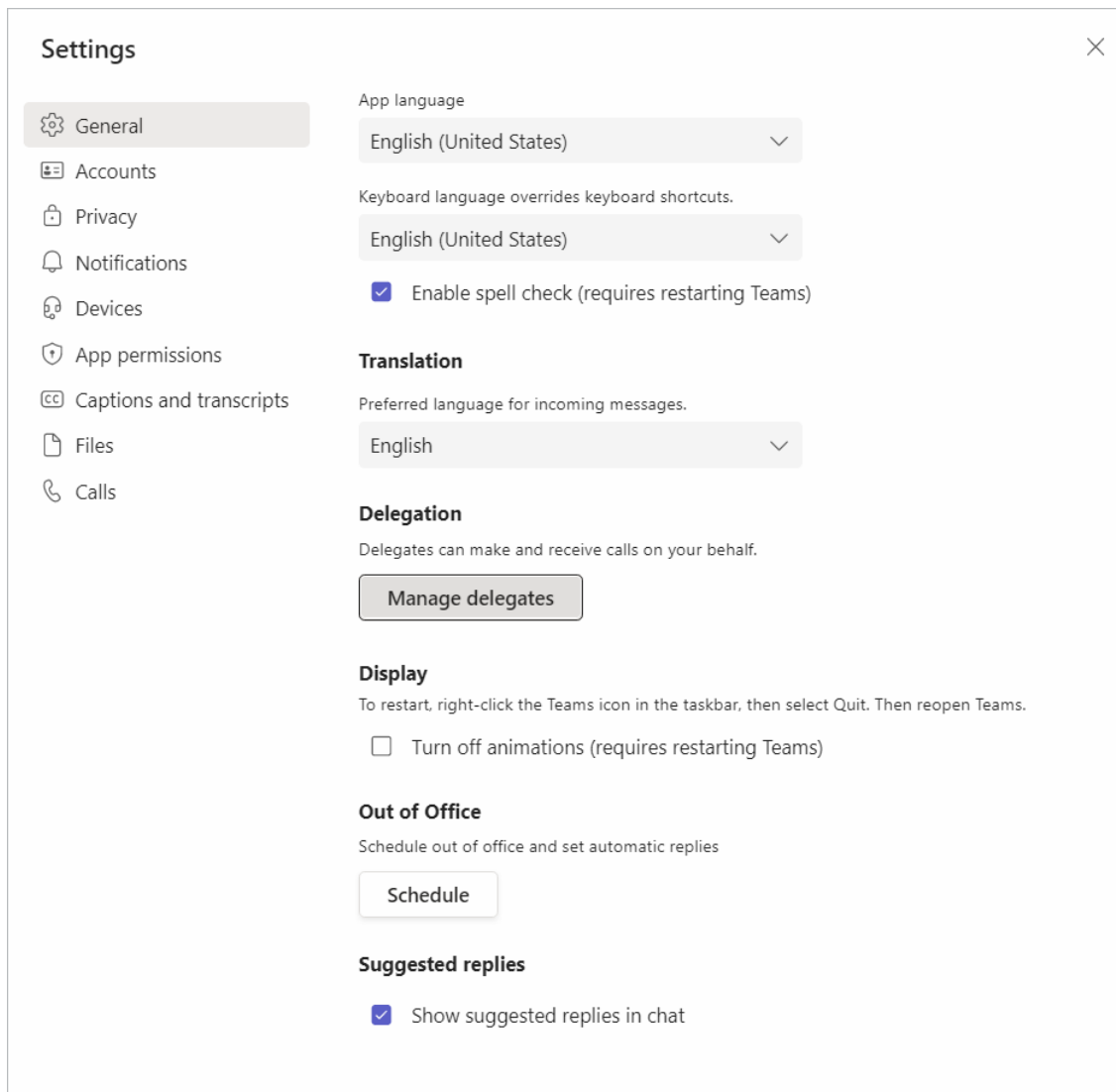
Below the call details is a table listing recent calls:

ID	From	To	Start Time	Duration	Direction	Release Cause	Media Type
1	MI-Team05, MI-Team05(MI-Team05)	7/7/22, 1:55:35 PM	00:00:06	OUTGOING	ABANDONED		
2	MI-Team05, MI-Team05(MI-Team05)	7/7/22, 1:55:35 PM	00:00:06	OUTGOING	ABANDONED		
3	teamstestuser2@a-logix.net, teamstestuser2@a-logix.net	7/7/22, 1:53:02 PM	00:02:25	OUTGOING	NORMAL		
4	MI-Team05, MI-Team05(MI-Team05)	7/7/22, 1:49:43 PM	00:03:28	OUTGOING	NORMAL		
5	teamstestuser2@a-logix.net, teamstestuser2@a-logix.net	7/7/22, 1:41:24 PM	00:00:03	OUTGOING	ABANDONED		
6	MI-Team05, MI-Team05(MI-Team05)	7/7/22, 1:38:37 PM	00:00:03	OUTGOING	ABANDONED		
7	MI-Team05, MI-Team05(MI-Team05)	7/7/22, 1:38:37 PM	00:02:52	OUTGOING	NORMAL		
8	MI-Team05, MI-Team05(MI-Team05)	7/7/22, 1:37:34 PM	00:00:19	OUTGOING	ABANDONED		
9	teamstestuser2@a-logix.net, teamstestuser2@a-logix.net	7/7/22, 1:37:33 PM	00:00:20	INCOMING	MISSED		

Delegating Teams Calls

You can set delegates to answer Teams calls. For example, an Administrative assistant makes calls on behalf of a manager.

Figure 14-15: Teams Calls Settings



Settings [Close]

General

- Accounts
- Privacy
- Notifications
- Devices
- App permissions
- Captions and transcripts
- Files
- Calls**

App language
English (United States) [v]

Keyboard language overrides keyboard shortcuts.
English (United States) [v]

☒ Enable spell check (requires restarting Teams)

Translation
Preferred language for incoming messages.
English [v]

Delegation
Delegates can make and receive calls on your behalf.
[Manage delegates](#)

Display
To restart, right-click the Teams icon in the taskbar, then select Quit. Then reopen Teams.
☐ Turn off animations (requires restarting Teams)

Out of Office
Schedule out of office and set automatic replies
[Schedule](#)

Suggested replies
☒ Show suggested replies in chat

The delegated call information is displayed in the Call Details.

Figure 14-16: Teams Call Delegate

Calls between 10/13/21 9:23 AM and 10/13/21 10:23 AM		
<div> <div>▼ Calls</div> <div> </div> </div>		
	Name	Start Time
▼	TeamsTestUser2	10/13/21 10:22:04 AM
<p>Answer Time: Oct 13, 2021 10:22:09 AM</p> <p>Release Time: Oct 13, 2021 10:22:11 AM</p> <p>Calling Party</p> <p>Name: TeamsTestUser4 on behalf of TeamsTestUser2</p> <p>Called Party</p> <p>Name: ST-User11</p> <p>Answering Party</p> <p>Name: ST-User11</p> <p>Recording Type: FULL_TIME</p> <p>Triggered:</p>		

Playing Back Recorded Media

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



The Web browser support for the SmartTAP 360° HTML5 player is listed below:

- **Audio:**

- ✓ Audio Playback: 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 14-17: Audio Player Screen

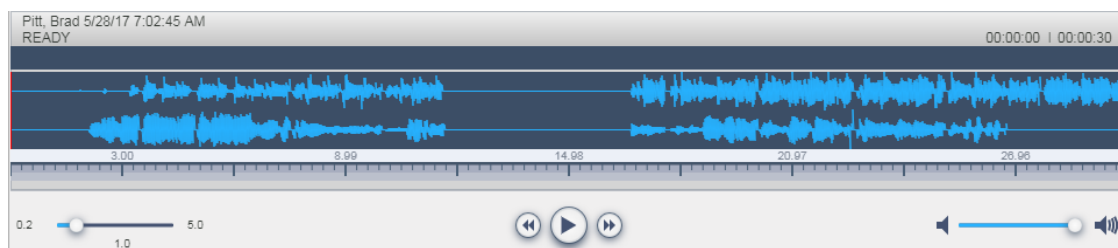






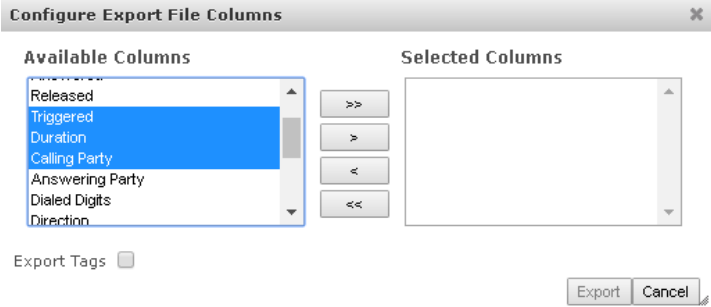







Table 14-4: Player Screen Overview

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.

Field	Description
	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 29
	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 119
	Download call information to your PC. When this option is selected, the Download Media dialog opens. See Downloading Call Recordings on page 156
	Download call transcript VTT file.
	Delete call transcript.
Rubbish bin	

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



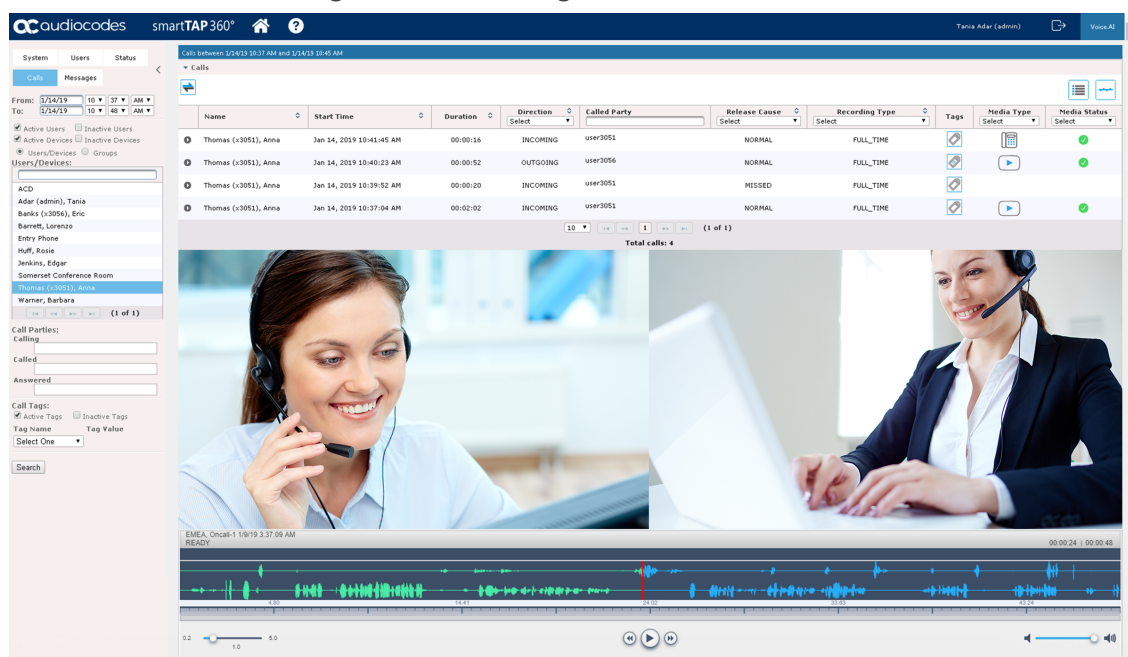
4. Click the  button to start listening to the call and/or view the video (if you selected “Display Video” check box); the button changes to  PAUSE while the call is playing, to allow the administrator to pause the player while playing the audio or video.

Figure 14-18: Viewing Video



The screenshot displays the smartTAP 360° interface. On the left, there is a sidebar with navigation tabs: System, Users, and Status. Under the Users tab, there are sections for 'Active Users', 'Inactive Users', 'Users/Devices', and 'Groups'. A list of users is shown, including 'Adar (Admin), Tania', 'Banks, Eric', 'Barrett, Lorenzo', 'Entry Phone', 'Huff, Rosie', 'Jenkins, Edgar', 'Somerset Conference Room', 'Thomas (x3051), Anna', and 'Warner, Barbara'. The 'Call Particles' section shows 'Calling' and 'Called' counts. The 'Call Tags' section shows 'Active Tags' and 'Inactive Tags' counts. The main area displays a table of calls with columns: Name, Start Time, Duration, Direction, Called Party, Release Cause, Recording Type, Tags, Media Type, and Media Status. The table shows four calls, all from 'Thomas (x3051), Anna' to 'user3051'. The first call is selected. Below the table, there is a video player showing two video feeds of a woman wearing a headset. The video player has a timeline at the bottom with a play button and a volume control. The timeline shows green segments indicating played back segments and yellow lines indicating audio signaling playback data.

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 14-19: Multiple Conference Participants

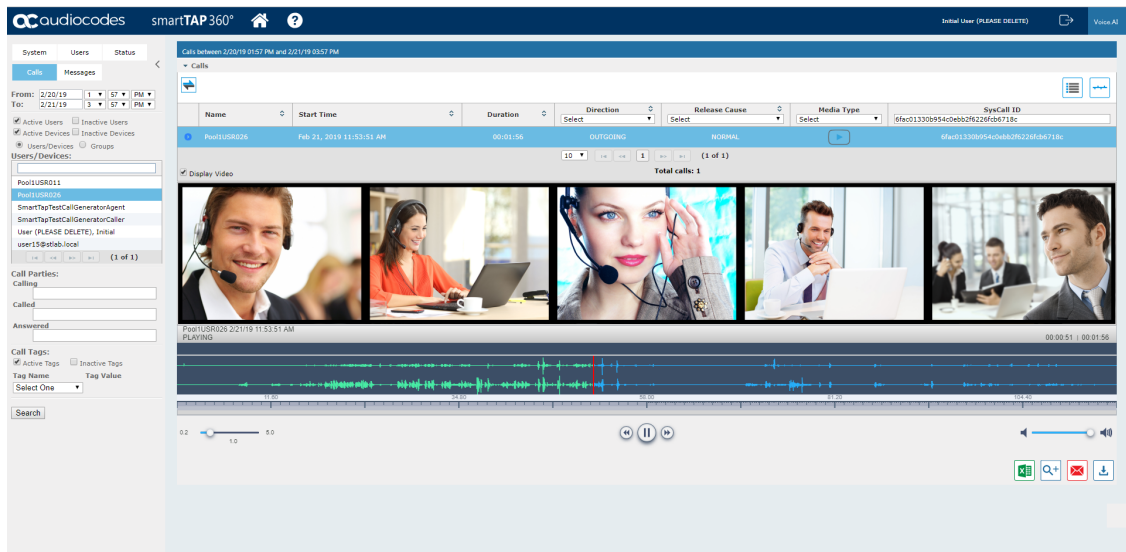
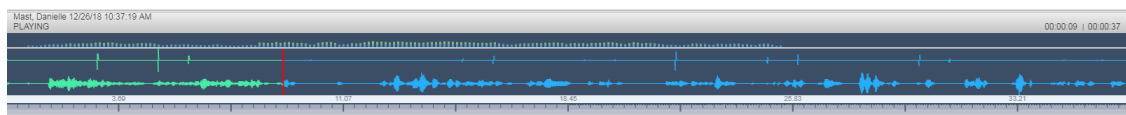


Figure 14-20: Playback Audio Signaling Data



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:


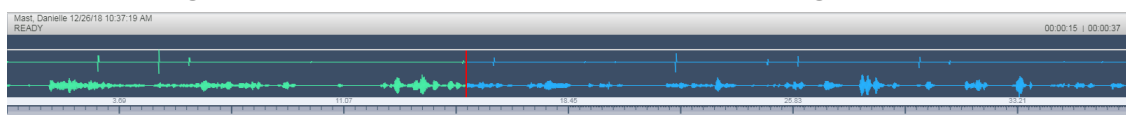
- Move the cursor to any random point in the recording and left-click and release;
- The selected segment is colored green. Click the  button; the call recording is played from the left-click selection point forward (shown by the red line in the figure below).

Figure 14-21: Random Selection Point in Call Recording




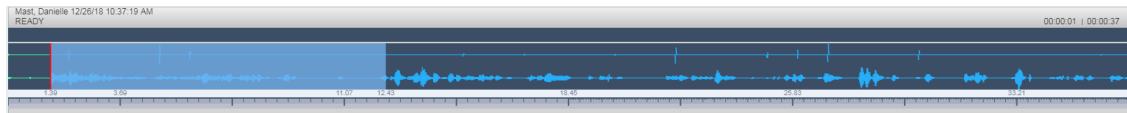



- Left-click and drag the mouse over the desired segment in the call recording and release; the selected segment is shaded blue. Click the  button; the shaded segment of the call recording is played back.

Figure 14-22: 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 (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 or download.
- In case, media is stored in Azure Blob, media files are downloaded to server and then processed.

Viewing and Playing Back Transcripts

This section describes how to view and playback Analytics transcripts.

➤ To view call transcript:

1. Follow the instructions described in [Searching for Calls](#) to search for calls.
2. In the retrieved calls list, select the call with Analytics Status 'Exists'. The transcript text is displayed.

Figure 14-23: Call Transcript

The screenshot displays the 'Call Transcript' interface. At the top, there is a table with columns: Name, Start Time, Duration, Direction, Release Cause, Media Type, Analytics Status, and Analytics Profile. The table lists several calls, with the last one, 'ST-Teams47, ST-Teams47', selected. Below the table, there are checkboxes for 'Display Transcript' and 'Auto-scroll'. The transcript text is displayed in a large text area, showing a conversation between two parties. At the bottom, there is a timeline and a playback control bar with a play button and a volume slider.

Name	Start Time	Duration	Direction	Release Cause	Media Type	Analytics Status	Analytics Profile
ST-Teams11, ST-Teams11	11/30/21 2:33:52 PM	00:00:56	INCOMING	NORMAL		Not assigned	
ST-Teams11, ST-Teams11	11/30/21 2:17:41 PM		INCOMING			Not assigned	
TeamsTestUser2	11/30/21 1:56:11 PM	00:01:08	INCOMING	NORMAL		Not assigned	
ST-Teams49, ST-Teams49	11/30/21 8:26:44 AM	00:00:55	INCOMING	NORMAL		In progress	VPNCpolicy
ST-Teams41, ST-Teams41	11/30/21 8:26:41 AM	00:00:58	INCOMING	NORMAL		In progress	VPNCpolicy
ST-Teams29	11/30/21 8:26:41 AM	00:00:56	INCOMING	NORMAL		In progress	VPNCpolicy
ST-Teams46, ST-Teams46	11/30/21 8:26:41 AM	00:00:59	INCOMING	NORMAL		In progress	VPNCpolicy
ST-Teams26	11/30/21 8:26:36 AM	00:00:04	INCOMING	MISSED		No transcription	VPNCpolicy
ST-Teams35, ST-Teams35	11/30/21 8:26:34 AM	00:00:05	INCOMING	MISSED		No transcription	VPNCpolicy
ST-Teams47, ST-Teams47	11/30/21 8:26:33 AM	00:01:08	INCOMING	NORMAL		Exists	VPNCpolicy

Display Transcript

Auto-scroll

Search texts in transcript

0:00:00.5 Then I need to talk to her. There you go. You got something in life story, so we're going to begin with their first. Let's dig in as little bit far away.

0:00:13.7 hey guys welcome back to another episode of gals today i have with me best and now you are legit and i know that because i saw a couple of videos you're a producer at mba which is the studio across the street right across the hall and feels like across this feels like a cross right million miles away so i know i've heard of you have seen you on the internet i'm like i gotta have this growing girl and i need to talk to her there you got something in life story so we're going to figure out their first little bit far away

0:00:45.7 Hey guys, welcome back to another episode of Gals Today I have with me best.

ST-Teams47, ST-Teams47 11/30/21 8:26:33 AM

00:00:00 | 00:00:54

5:10 15:20 27:30 37:50 45:50

0.2 5.0

1.0

⏮ ⏪ ⏩ ⏭

🔊 🔇

📄 🔍 📧 📄 📄 📄

3. Click  to delete a transcript.

4. Click  to download a transcript.

Figure 14-24: Transcript with Video

The screenshot shows the SmartTAP 360° interface. On the left is a sidebar with search criteria, including filters for 'From' and 'To' dates, 'Active Users', 'Inactive Users', 'Active Devices', 'Inactive Devices', 'Users/Devices', and 'Groups'. The main area displays a table of calls with columns: Name, Start Time, Duration, Direction, Release Cause, Media Type, Media Status, Analytics Status, and Analytics Profile. Below the table, there are checkboxes for 'Display Video' and 'Display Transcript'. The video player shows a woman speaking, and the transcript on the right shows the text of the call. The transcript includes a search bar and a list of text segments with timestamps.

Figure 14-25: Transcripts with Screen Sharing

The screenshot shows the SmartTAP 360° interface. On the left is a sidebar with search criteria, including filters for 'From' and 'To' dates, 'Active Users', 'Inactive Users', 'Active Devices', 'Inactive Devices', 'Users/Devices', and 'Groups'. The main area displays a table of calls with columns: Name, Start Time, Duration, Direction, Release Cause, Media Type, Media Status, Analytics Status, and Analytics Profile. Below the table, there are checkboxes for 'Display Transcript' and 'Auto-scroll'. The screen sharing area shows a presentation slide titled 'Peak bandwidth estimation. Solution 2 - PP' with a diagram of a packet pair approach. The transcript on the right shows the text of the call, including a search bar and a list of text segments with timestamps.

The screenshot shows the SmartTAP 360° interface. On the left is a sidebar with search criteria, including filters for 'From' and 'To' dates, 'Active Users', 'Inactive Users', 'Active Devices', 'Inactive Devices', 'Users/Devices', and 'Groups'. The main area displays a table of calls with columns: Name, Start Time, Duration, Direction, Release Cause, Media Type, Media Status, Analytics Status, and Analytics Profile. Below the table, there are checkboxes for 'Display Video' and 'Display Transcript'. The screen sharing area shows a presentation slide titled 'Kalman Filter, short intro' with mathematical formulas and a diagram. The transcript on the right shows the text of the call, including a search bar and a list of text segments with timestamps.

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 119 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.

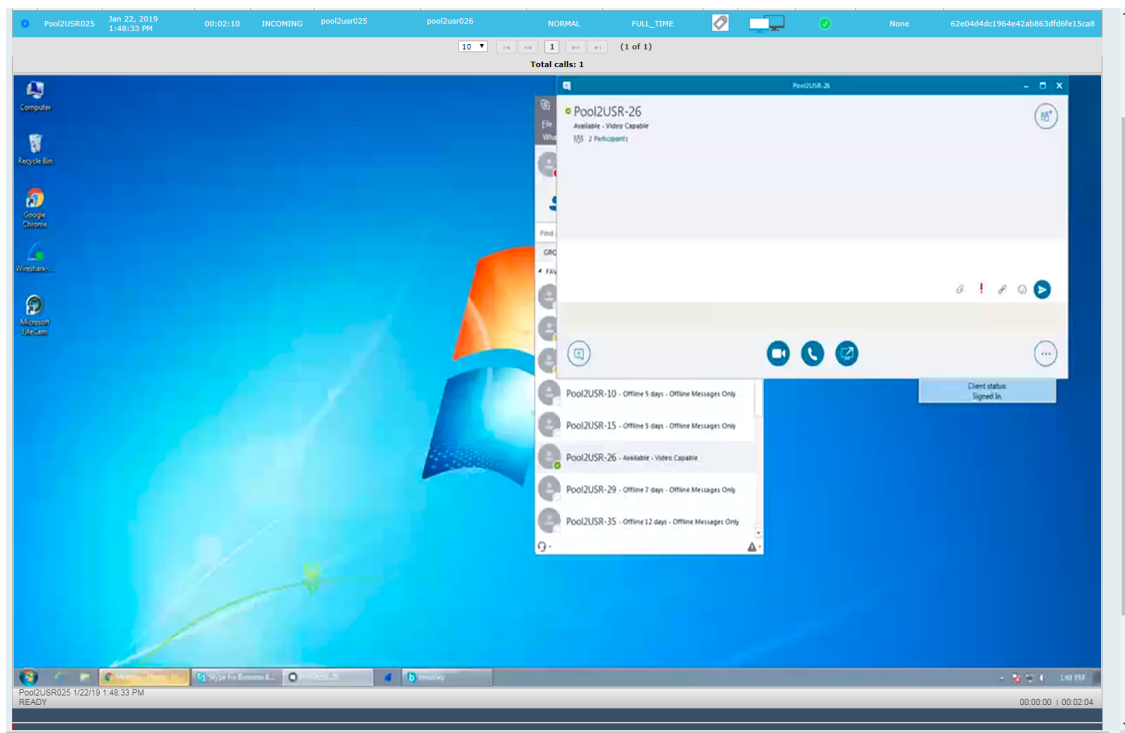
Figure 14-26: Media Type-Video and Screen Sharing with Teams


Name	Start Time	Duration	Direction	Release Cause	Media Type
ST-Teams08	Jul 16, 2020 9:50:57 AM	00:02:07	INCOMING	NORMAL	SHARING
ST-Teams35	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	SHARING
ST-Teams36	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	SHARING
ST-Teams34	Jul 16, 2020 9:50:56 AM	00:02:09	INCOMING	NORMAL	SHARING
ST-Teams39	Jul 16, 2020 9:50:56 AM	00:02:09	INCOMING	NORMAL	SHARING
ST-Teams37	Jul 16, 2020 9:50:56 AM	00:02:08	INCOMING	NORMAL	SHARING
ST-Teams33	Jul 16, 2020 9:50:55 AM	00:02:09	INCOMING	NORMAL	SHARING
ST-Teams11	Jul 16, 2020 9:32:56 AM	00:02:08	INCOMING	NORMAL	SHARING
ST-Teams13	Jul 16, 2020 9:32:56 AM	00:02:08	INCOMING	NORMAL	SHARING
ST-Teams14	Jul 16, 2020 9:32:55 AM	00:02:10	INCOMING	NORMAL	SHARING

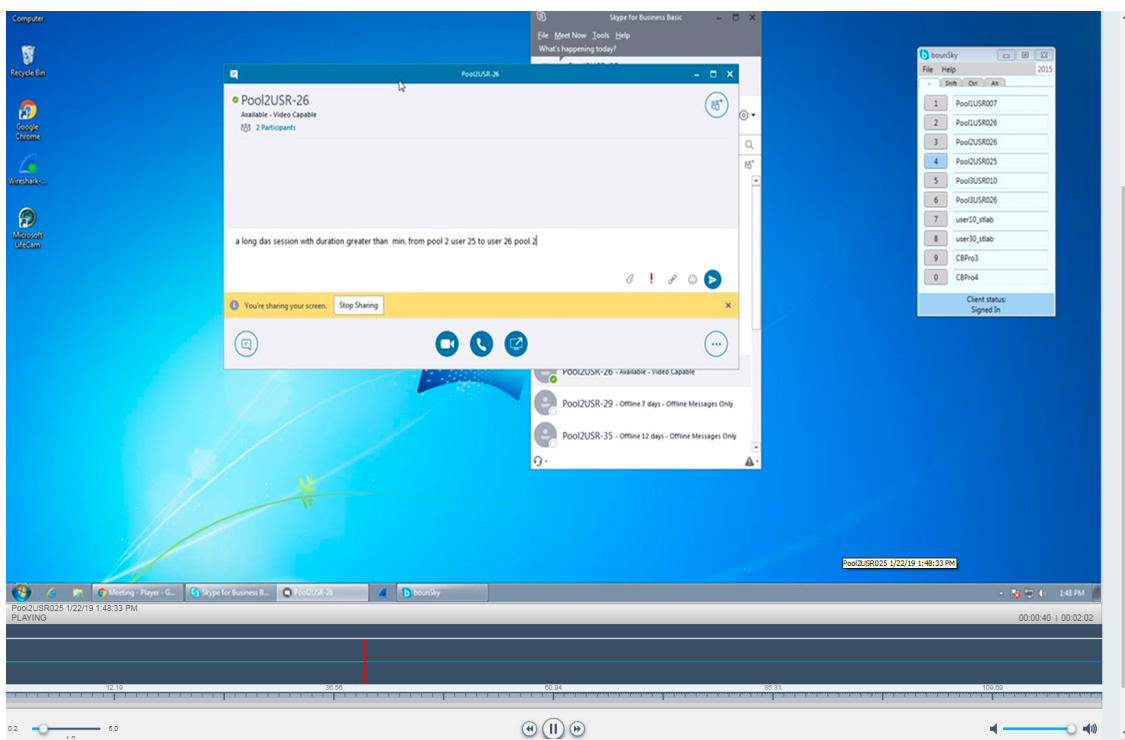
Figure 14-27: Media Type-Video and Screen Sharing with Skype for Business


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



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

Figure 14-28: 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.

Timeline View

You can view call data for a specific user/device over a timeline. 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 to search for calls.

Figure 14-29: Calls List

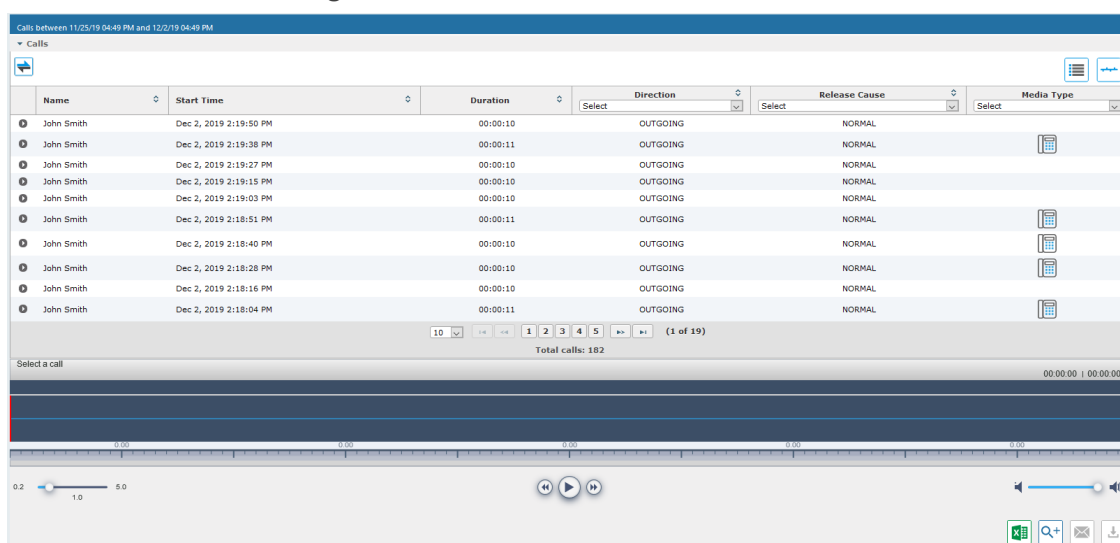


Figure 14-29 shows the 'Calls List' interface. At the top, it displays the search range: 'Calls between 11/25/19 04:49 PM and 12/2/19 04:49 PM'. Below this is a table with columns: Name, Start Time, Duration, Direction, Release Cause, and Media Type. The table lists 19 calls for 'John Smith', all outgoing, with durations ranging from 00:00:10 to 00:00:11. The interface includes a 'Total calls: 192' indicator and a 'Selected a call' section. At the bottom, there is a timeline view with a zoom slider and navigation buttons.

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

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

Figure 14-30: Select User in Timeline View

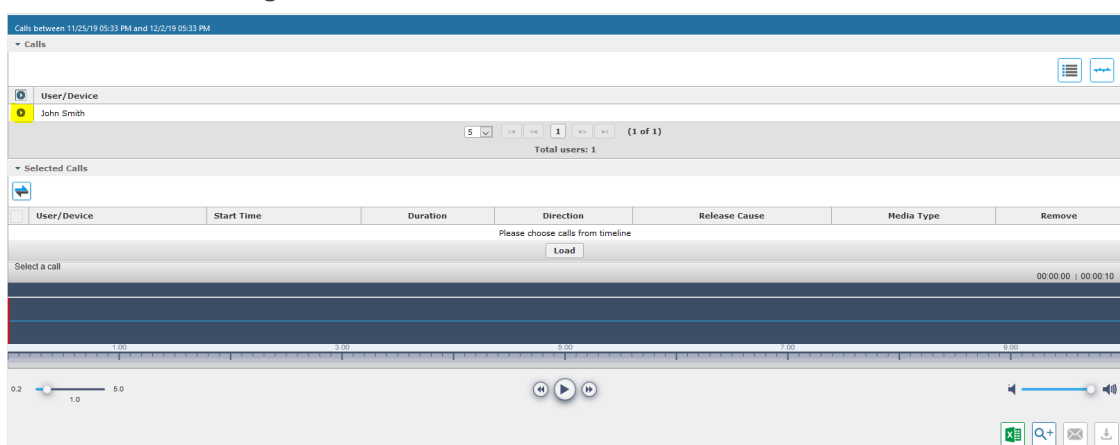
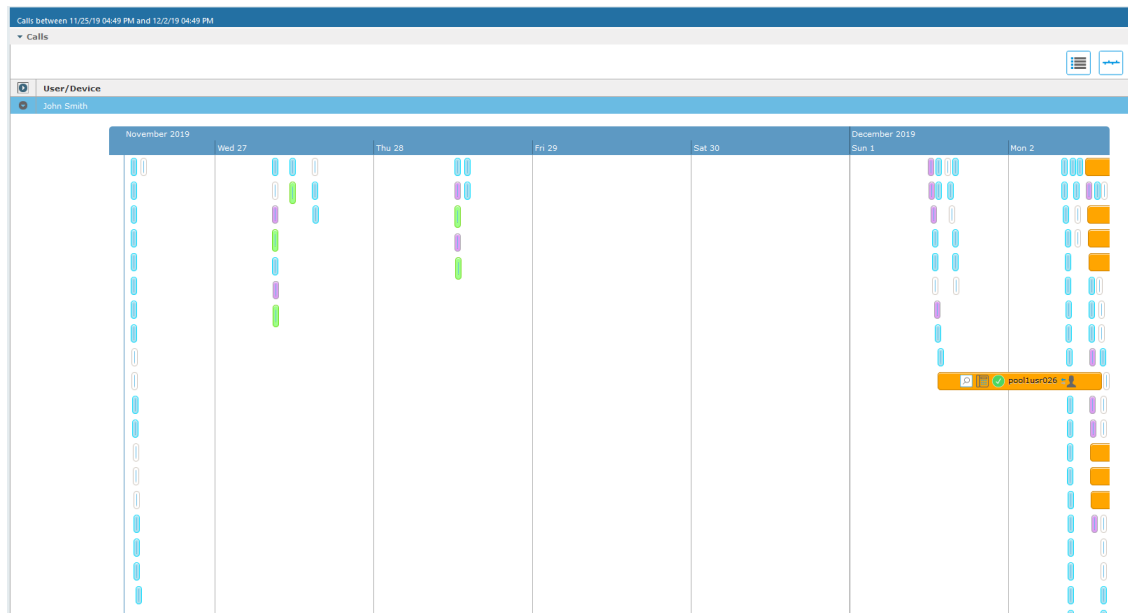


Figure 14-30 shows the 'Select User in Timeline View' interface. It displays a list of users/devices under the 'User/Device' section, with 'John Smith' selected. Below this, there is a 'Selected Calls' section with a table showing call details. The interface includes a 'Total users: 1' indicator and a 'Please choose calls from timeline' section with a 'Load' button. At the bottom, there is a timeline view with a zoom slider and navigation buttons.

User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
Please choose calls from timeline						

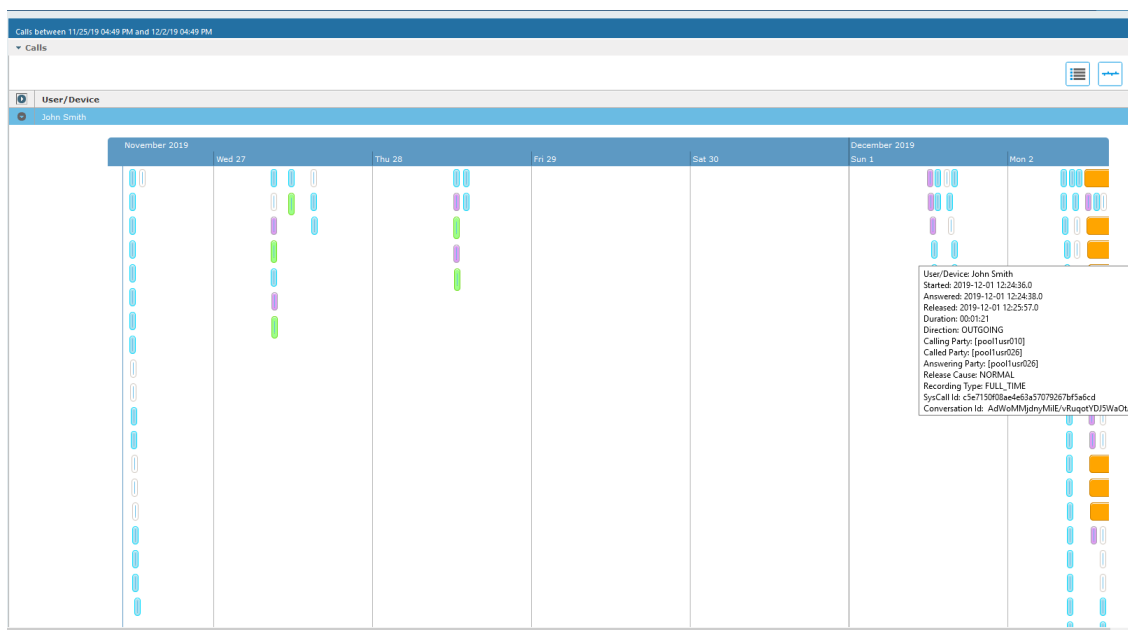
3. Select the arrow adjacent to the User/Device whose timeline you wish to view. The Calls List is displayed:

Figure 14-31: User Timeline



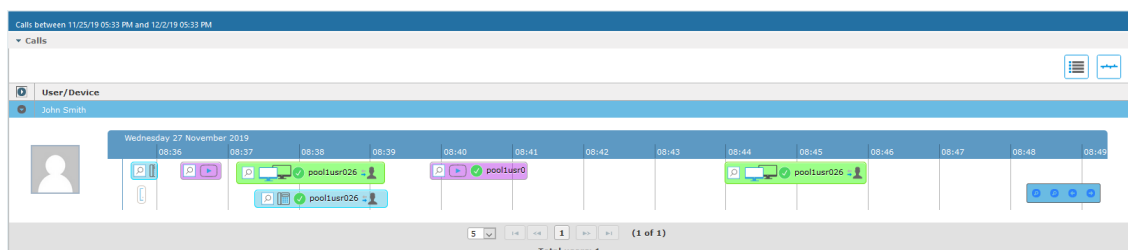
4. Hover over a call event to view details of the call.

Figure 14-32: Call Event Details

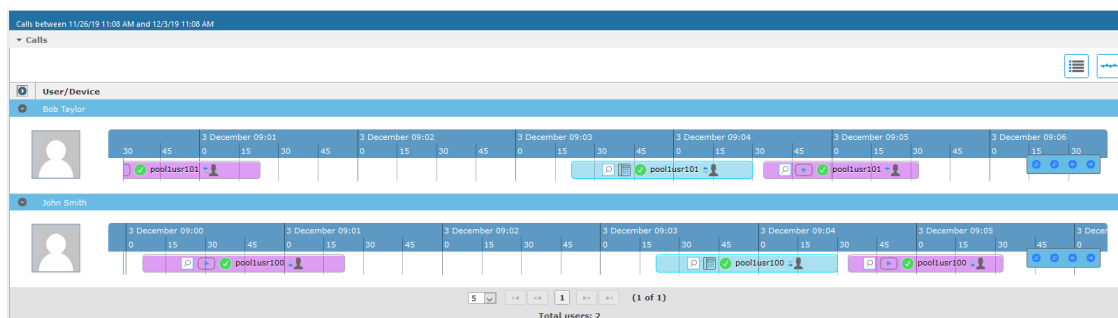


5. Zoom in on a specific day to view the details using either the mouse roller or the navigation buttons that are highlighted below.

Figure 14-33: Zoom In






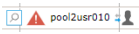
- In timeline view, the calls are grouped according to their target type. Each target type is represented by a different color (see table below). Calls for the same target type are displayed as events in a continuous timeline.
- Call events from one or more timelines can be selected to a playable table. 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 14-34: 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 14-5: Call Events Description

Media Type	Description
 pool2usr	Represents an Audio call.
 pool2c	Represents a Video call
 pool2usr027	Represents a Video and Screen Sharing call
 pool2usr010	Represents a call that has no media. When a call is abandoned or missed, this target is displayed without the red warning.

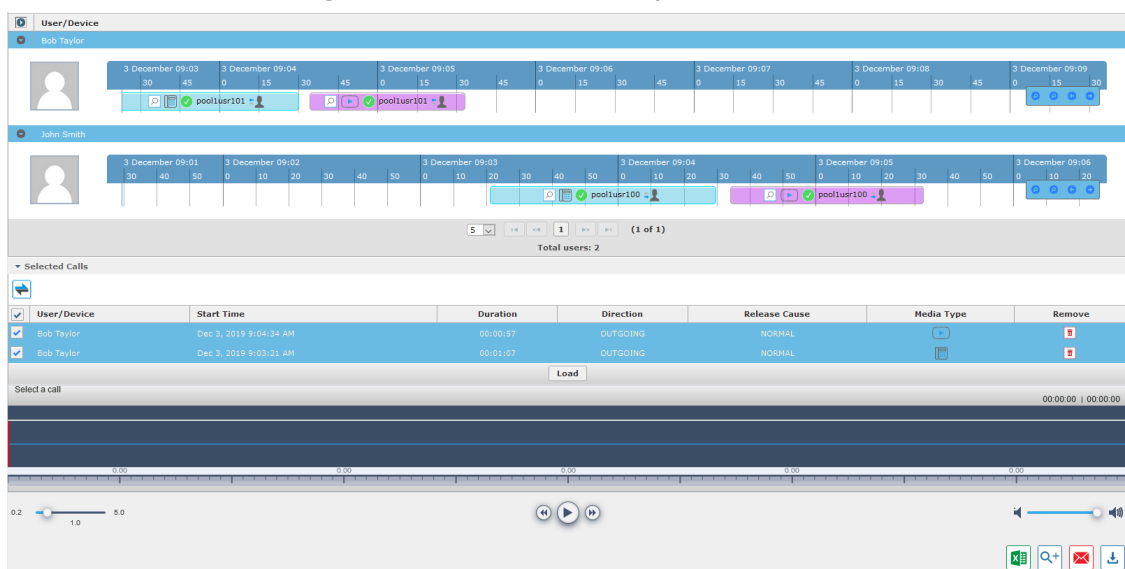
Each event includes different call information statuses as shown in the table below:

Table 14-6: 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 14-35: Load Media Player



The selected files are loaded to the Media Player.

Figure 14-36: Loading Files to Media Player

User/Device

Bob Taylor

John Smith

Display Video

Total users: 2

Selected Calls

User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
Bob Taylor	Dec 3, 2019 9:04:34 AM	00:00:07	OUTGOING	NORMAL	[Icon]	[X]
Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	[Icon]	[X]

Load

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

00:00:00 | 00:01:01

0.2 1.0 5.0

Media Player Controls: Play, Pause, Stop, Volume, Full Screen, Search, Print, Download

Figure 14-37: Files Ready to Play

User/Device

Bob Taylor

John Smith

Display Video

Total users: 2

Selected Calls

User/Device	Start Time	Duration	Direction	Release Cause	Media Type	Remove
Bob Taylor	Dec 3, 2019 9:04:34 AM	00:00:07	OUTGOING	NORMAL	[Icon]	[X]
Bob Taylor	Dec 3, 2019 9:03:21 AM	00:01:07	OUTGOING	NORMAL	[Icon]	[X]

Load

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

00:00:00 | 00:02:04

0.2 1.0 5.0

Media Player Controls: Play, Pause, Stop, Volume, Full Screen, Search, Print, Download


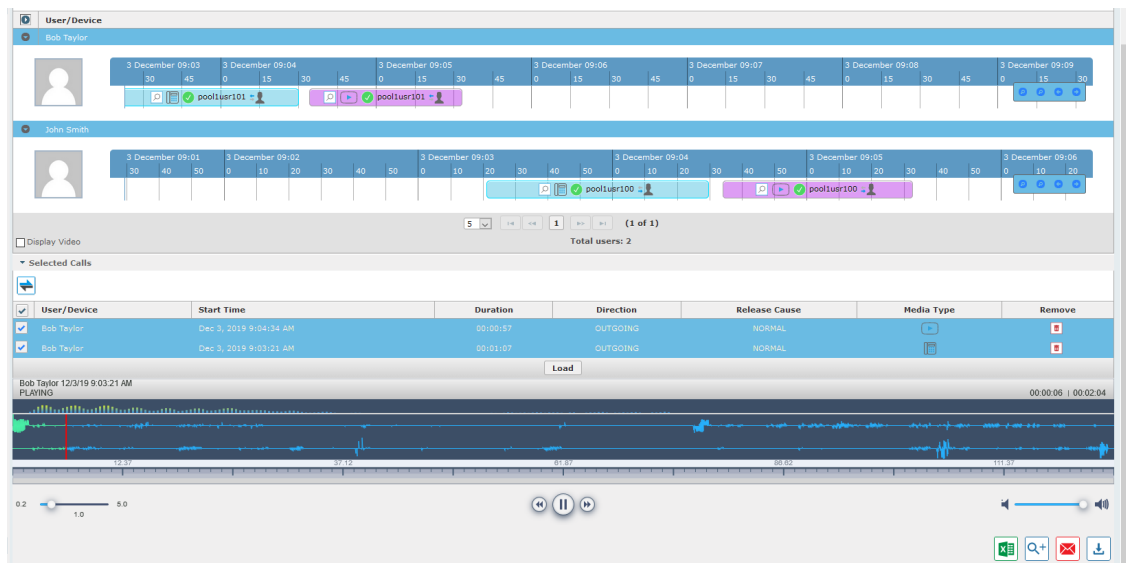
- b. Click  to play the selected call.

Figure 14-38: Play Call



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](#) 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 14-39: 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 14-40: 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**

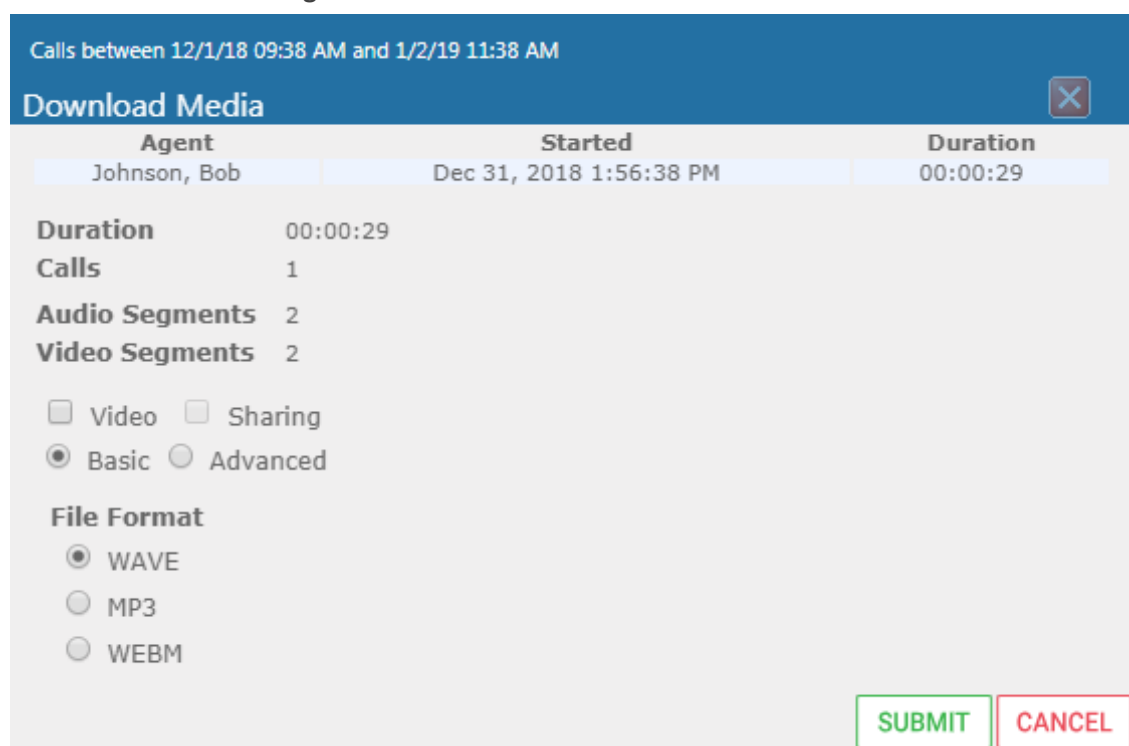
Downloading Video Call

This section describes how to download a video call.

➤ **To download a video call:**

1. Follow the instructions in Searching for Calls 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 14-41: 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 14-42: 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 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 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 14-43: 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 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 **SUBMIT** to download and save the file on the local computer.

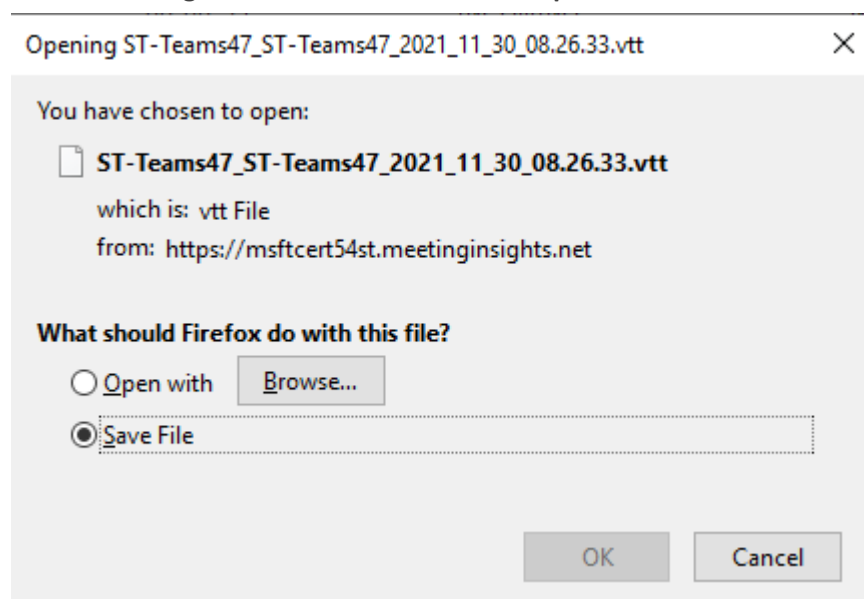
Downloading Call Transcripts

You can download call transcripts. This action requires call download permissions.

➤ To download transcripts:

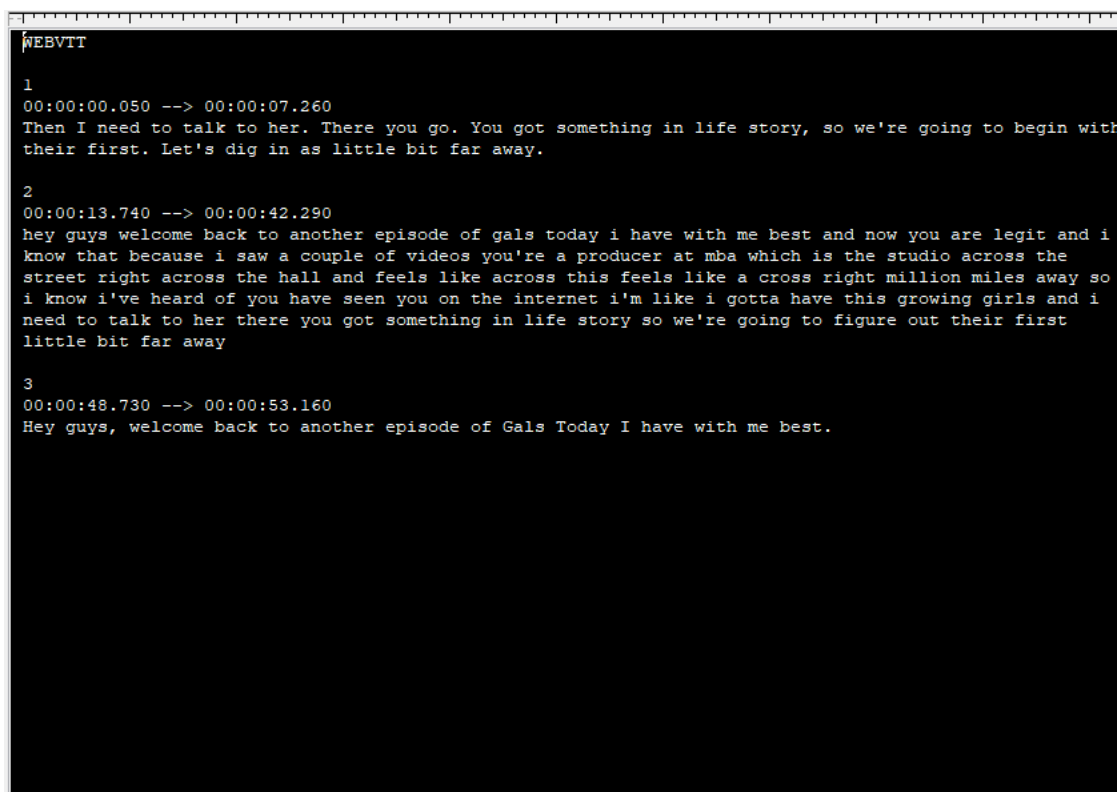
1. Click Download Transcript  to download a transcript.

Figure 14-44: Download Transcript




2. Browse to select the desired application to open the VTT file.

Figure 14-45: Example Downloaded Transcript



➤ **To delete call transcripts:**



- Click  to delete a transcript. This action requires Delete transcription permissions in the Security Profile (see [Managing Security Profiles](#) on page 35).


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

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 14-7: Email – Field Descriptions

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

Field	Description
	to the attachment removes the attachment from the email.
Body	Body of the email.
	Sends the email.
	Cancels the email.

6. Click  to send the email.

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 14-8: 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,

Field	Description
	only the specific administrator account will be able to view the tag.
SUBMIT	Applies changes.
CANCEL	Cancels changes.

Adding a Call Tag





This section describes how to add a new call tag.

➤ To add a new Call Tag

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

Table 14-9: 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)

Field	Description
	<p>■ Select_One (Define a list of options for the user to choose from, i.e., Excellent, Very Good, Good, Poor)</p> <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 accept user inputs like Sales-1234567QA OR Sales-9876543P2, etc.</p>
	Click to view tag details.
	Click to delete tag.
	Apply changes.
	Cancel changes.

Viewing / Deleting a Call Tag

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

➤ To view or delete Call Tags:

1. Open the Call Tagging screen (**System** tab > **System** folder > **CallTagging** > **View/Delete Call Tags**).

Figure 14-46: 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:


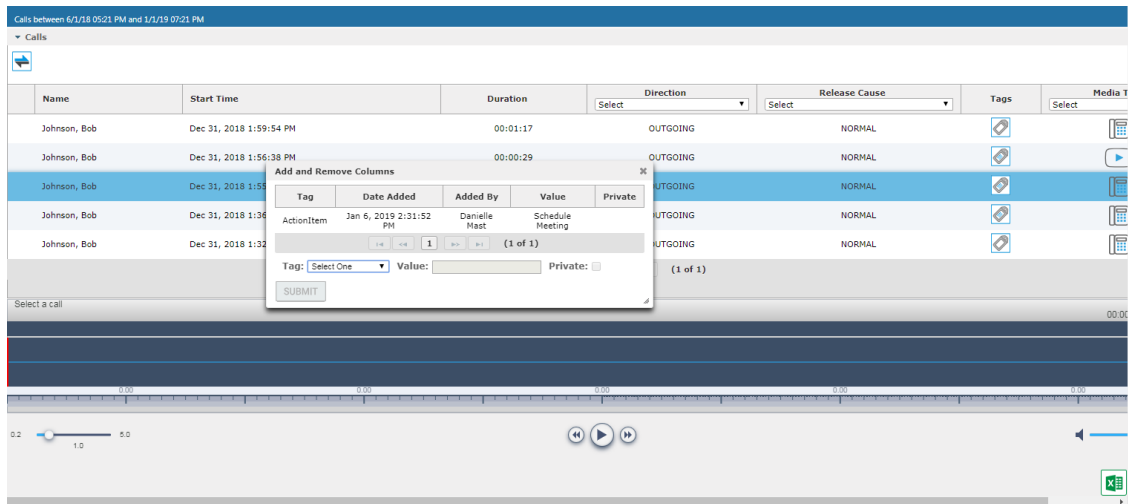
1. Search for call records (see Searching for Calls).
2. Select the call record to tag and ensure that the Tags column is displayed.
3. Double-click the Tags icon in the call record.
4. In the Tag field, select the type of tag that you wish to add and enter the desired value in the Value field.
5. Select 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 14-47: Assigning a Call Tag



On-Demand Recording

The On-Demand Recording configuration is used for synchronization between the paired Bot machines in the Microsoft Teams Active-Active setup. The On-Demand Configuration parameters are preconfigured in the automation scripts as part of the initial setup of SmartTAP on Microsoft Teams and can be updated using this menu option.

➤ To configure On-Demand:

1. Open the On-Demand Configuration page (**System** tab > **Redundancy** folder > **On-Demand Configuration**).

The screenshot shows the 'On-Demand Configuration' page. It has a blue header with the title 'On-Demand Configuration'. Below the header, there are three input fields: 'Service bus connection string Local' (with a yellow background and a dropdown menu), 'Service bus subscription Local' (with a white background and a dropdown menu), and 'Service bus connection string Remote' (with a white background and a dropdown menu). A green 'SUBMIT' button is located at the bottom right of the form.

Table 14-10: On-Demand Configuration

Parameter	Description
Service bus connection string Local	The connection string of the local Service bus in the Active Active setup.

Parameter	Description
Service bus subscription Local	The subscription that is used for sending messages from the local to the remote service bus.
Service bus connection string Remote	The connection string of the remote Service bus in the Active Active setup.

15 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 15-1: Managing Instant Messages

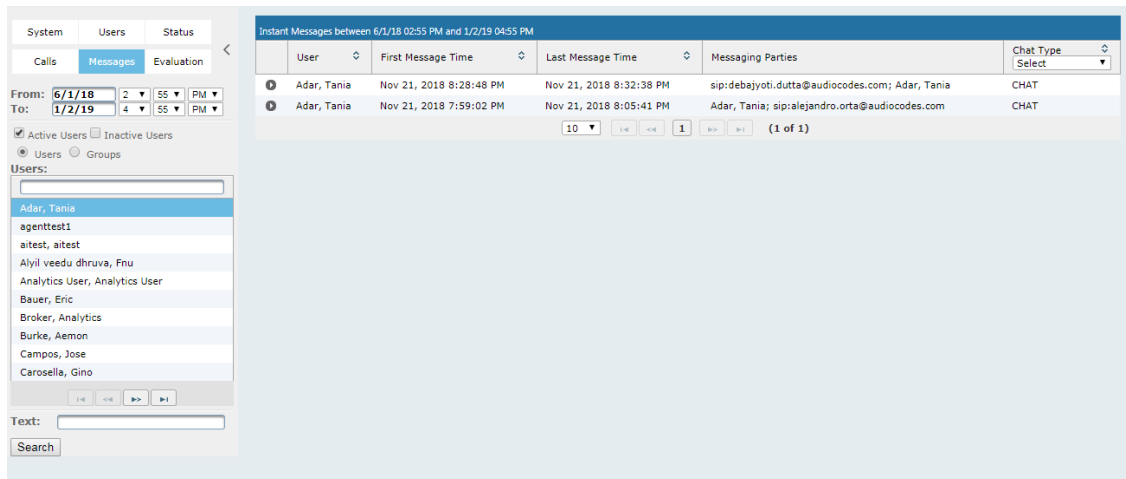


Figure 15-3:

Figure 15-2: Instant Message Display-Skype for Business

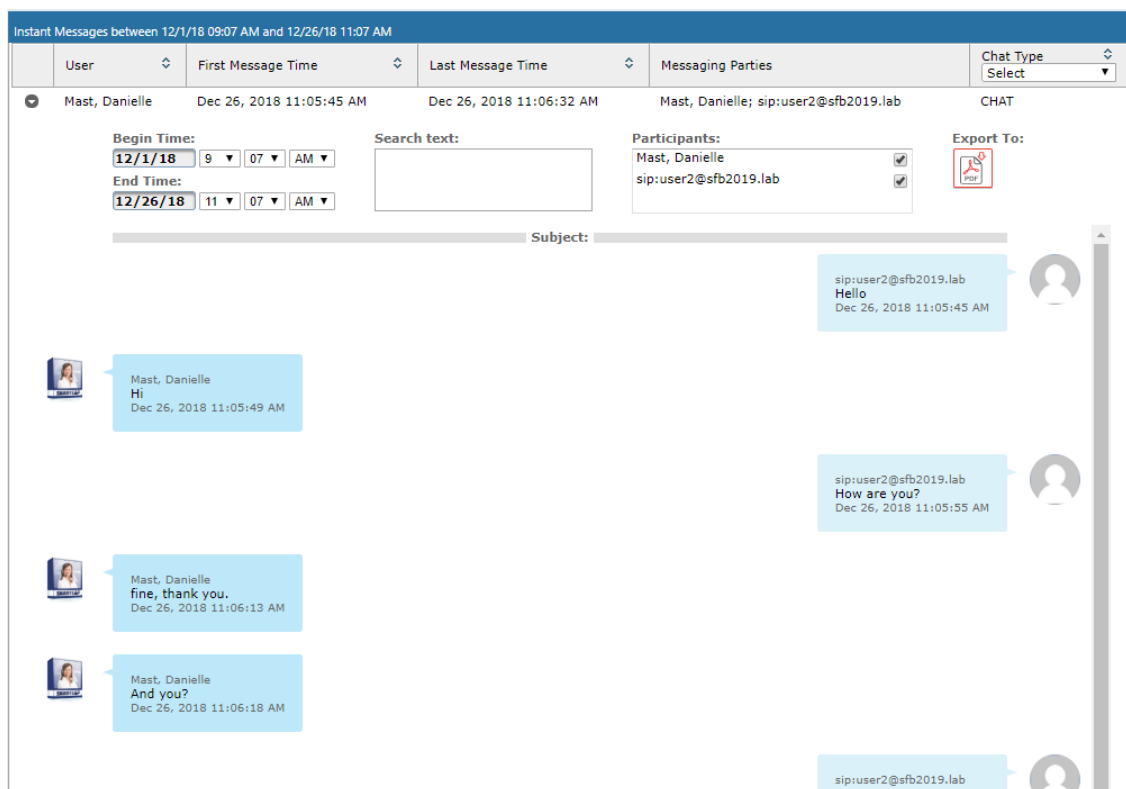


Figure 15-4: Search Messages

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 15-1: 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° application.
Inactive Users	Users whose account has been deleted from the SmartTAP 360° application.
Users	Only Users will be listed in the Search list. Either the Users or the Groups option must be selected.
Groups	Only Groups will be listed in the Search list. Either the Users option or the Groups option must be selected.

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 15-5: 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°'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).

Table 15-2: 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	""word1 word2 word3" @8' Search for matching

Operator	Description	Example
	each other, measured in words.	messages where word1, word2 and word3 are separated by a distance of 8 words from each other.
> <	These two operators are used to change a word's contribution to the relevance value that is assigned to a conversation or message. The > operator increases the contribution and the < operator decreases it.	'+apple +(>turnover <strudel)'Find messages that contain the words 'apple' and 'turnover' or 'apple' and 'strudel' (in any order), but rank 'apple turnover' higher than 'apple strudel'.
()	Parentheses group words into subexpressions. Parenthesized groups can be nested.	
~	A leading tilde acts as a negation operator, causing the word's contribution to the message's relevance to be 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°, the minimum length of the word for full-text searches is 2.

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

Figure 15-6: 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
▶	Adar, Tania	Nov 21, 2018 8:28:48 PM	Nov 21, 2018 8:32:38 PM	sip:debajyoti.dutta@audiocodes.com; Adar, Tania	CHAT
▶	Mast, Danielle	Dec 26, 2018 11:05:45 AM	Dec 26, 2018 1:34:40 PM	sip:user2@sfb2019.lab; Mast, Danielle	CHAT
▶	Mast, Danielle	Dec 26, 2018 2:04:48 PM	Dec 26, 2018 2:06:40 PM	sip:user2@sfb2019.lab; Mast, Danielle; sip:user3@sfb2019.lab	GROUPCHAT

Figure 15-7: 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
▶	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 15-3: Search Messages Results

Field	Description
User	The username. When this field is clicked, the search results are sorted 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. When this field is clicked, the search results are sorted in Ascending/Descending order, alternating with each click.
Messaging Parties	The messaging parties who sent or received the conversation messages.
Chat Type	<p>The following chat types can be filtered:</p> <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).

Figure 15-8: 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:

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 15-9: 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:
 Conference Ids: [sip:user2@sfb2019.lab;gruu;opaque=app:conf:chat:id:14W62Z79]
 Participants: sip:user2@sfb2019.lab, Mast, Danielle, sip:user3@sfb2019.lab
 Export To:

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

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

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

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

50 1 (1 of 1)

Figure 15-10: 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
 Mast, Danielle: Have a nice day
 Dec 26, 2018 11:06:32 AM
 Mast, Danielle: Thank you
 Dec 26, 2018 12:28:13 PM
 sip:user2@sfb2019.lab: Great
 Dec 26, 2018 11:06:25 AM
 sip:user2@sfb2019.lab: File: SMARTTAP_Administrator_Guide.pdf
 Size: 6150 KB
 Status: sent
 Dec 26, 2018 12:24:20 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 15-4: 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° displays a collection of messages in one conversation based on the time and participants.

Microsoft Teams Instant Messages

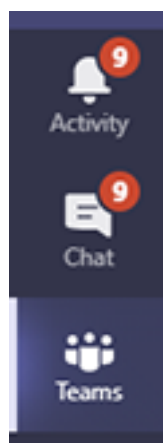
SmartTAP utilizes Microsoft Graph Teams Export API for recording Microsoft Teams Chat messages. The TerraSmart deployment script creates the "ims-app" for accessing Microsoft Teams Instant Messages. Customers using AudioCodes Azure subscription must provide consent for reading and recording Microsoft Teams user chat messages (refer to the [SmartTAP Hardware and Software Requirements](#)).

Before you can view Instant Messages, Microsoft Teams prerequisites and licenses must be installed as described at: [Prerequisites to access Teams Export APIs](#).

Instant messages are stored in the **database** and not on storage disks.

Microsoft Teams Instant Message features include:

- When editing a chat message, the new message content will be replaced with the original one, and “This message has been edited” is displayed.
- When deleting a chat message, the content of the message will still be displayed, and “This message has been deleted” is displayed.
- Clicking ‘Undo’ on deleted message will be considered as edited.
- HTML based messages, such as Formatted\Tables\Links are not supported (only the content is 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).




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

16 Using the Evaluation Feature

The Evaluation tab accesses all functions related to the SmartTAP 360° evaluation feature. From under this tab, evaluation forms to be used for evaluations are created. Later, evaluation reviews and reports can be generated. The Evaluation Forms screens, shown in the figure below, provides access to all evaluation-related features.



Figure 16-1: Evaluation Forms – New Form Subscreen


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_vest	DRAFT	N/A			
Sales	DRAFT	N/A			
test	FINAL	Sep 7, 2017			

(1 of 1) 1 10 ▾

Use the table below as reference.

Table 16-1: 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.

Field	Description
 (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 185
- [Adding a New Section \[Evaluation Forms\]](#) on page 186
- [Adding Questions and Answers to an Evaluation Form](#) on page 187
- [Finalizing Forms](#) on page 190

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 16-2: 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 16-2: 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 16-3: 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 16-4: Sections of Evaluation Form – New Section Sub-screen







Sections of Evaluation Form: Agentscoring 002

— New Section

Name:

Description:

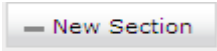
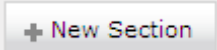
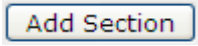
Add Section

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

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 16-3: Sections of Evaluation Form – Field Descriptions

Field	Description
	Click to close the New Section subscreen.
	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.
	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 16-5: Sections of Evaluation Form – New Questions Sub-screen

Questions of Evaluation Form: Agentscoring 002 Section: Greeting

— New Question

Question:
Description:









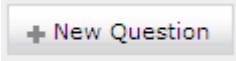
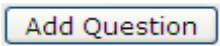


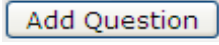
		Question (click to change)	Add Answer	Delete	Move
	Q:	The agent thanked the customer for calling a: Yes a: No			up down
	Q:	The agent mentioned their company name a: Yes a: No			up down
	Q:	The agent identified themselves to the customer a: Yes a: No			up down
	Q:	The agent stated that the call is being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

Table 16-4: 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  adjacent to the row of the Form that you wish to change.
3. Click  to open the row of the Section that you wish to change.
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 16-5: 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  adjacent to the row of the Form that you wish to change.



- Click  adjacent to the row of the Section that you wish to change.
- Click  adjacent to the row of the Question whose Answer screen you wish to launch.


Figure 16-6: Sections of Evaluation Form - New Answer Sub-screen



- Enter the new Answer information.



You must provide at least two answers for each question.

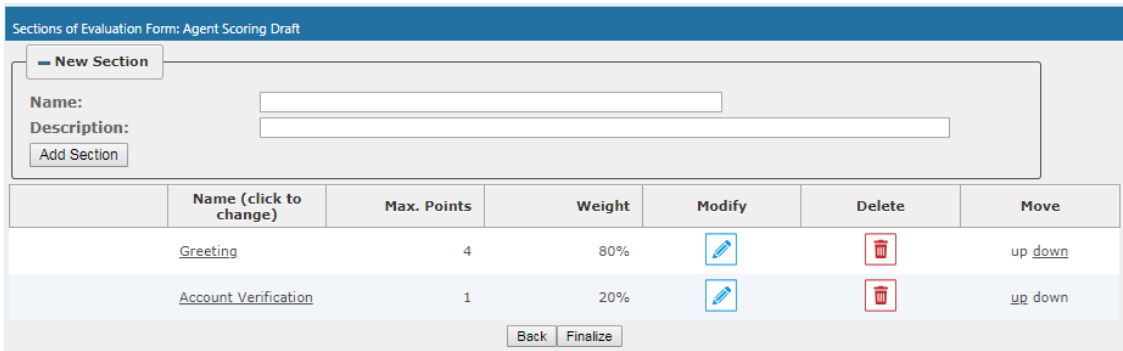
- Click  to create the new Answer; the new Answer will appear in the form with an asterisk * on the leftmost column indicating that the form is missing fields and cannot be finalized. There is a minimum of two (2) answers required before a form can be finalized.





Finalizing Forms

This section describes how to finalize forms.

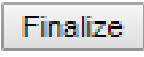
➤ To finalize a Form [Evaluation Forms]:



Figure 16-7: 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:

- Open the form (**Evaluation** tab > **Evaluation** folder > **Evaluation Forms** > **Form**).
- Click  to open the Finalize Evaluation form subscreen.

3. Click  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 16-6: Select Evaluation Form Screen

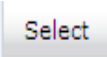
Field	Description
Name	The name of the form.
Description	Description of the form.
Select	 click to select the form.

Figure 16-8: Call Search/Selection Evaluation Form

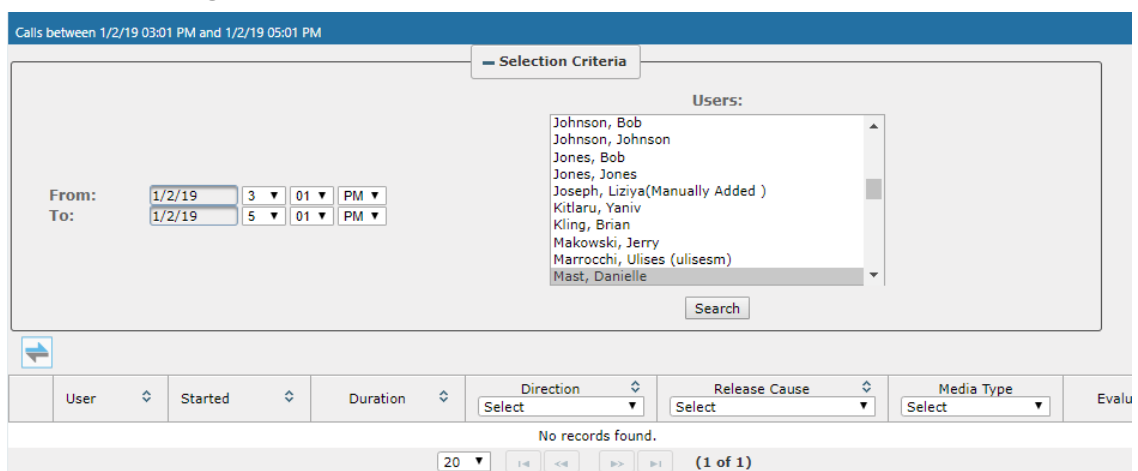
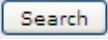



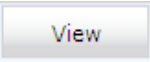

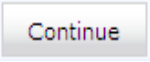


Table 16-7: Call Search/Evaluation Form – Field Descriptions

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 drop-down 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 drop-down to change the time of day.

Field	Description
Users	Users whose account is enabled in SmartTAP 360°.
	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 drop-down 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 type="checkbox"/> Audio <input type="checkbox"/> Video <input type="checkbox"/> Video and Screen Sharing <input 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.
	Continue previously started Evaluation.

Field	Description
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 16-9: Select Evaluation Form

Figure 16-10: Evaluation Form User Selection

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

Figure 16-11: 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 **New** on the row of the call to evaluate.

Figure 16-12: Perform Evaluation Screen

Perform Evaluation: Customer Service

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

00:00:00 | 00:00:12

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%)



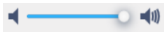






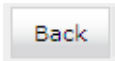
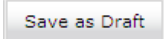
Questions	Answers	Score	Notes
How well did the agent communicate at an understandable rate and sound positive?	Choose One	0 out of 10	
How well did the agent seem to empathize with the customer?	Choose One	0 out of 10	
How well did the agent use probing questions to identify the problem?	Choose One	0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

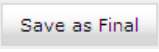
Section: Closing Section: Closing Score: 0 out of 30 (0%)

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	

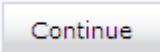
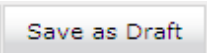
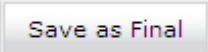
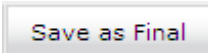
Save as Draft Save as Final

Table 16-8: 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	Drop-down 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 16-13: 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	
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	
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	
Agent Scoring	Agent Scoring Evaluation form	FINAL	Adar, Tania	Mast, Danielle	2018-04-24 15:20:57.0	
Agent Scoring	Agent Scoring Evaluation form	FINAL	Adar, Tania	Mast, Danielle	2018-04-24 15:24:44.0	

Table 16-9: 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 drop-down 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 drop-down 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 drop-down 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 drop-down 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 16-14: Average Score Report

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

— Report Filter

Customer Service ▼ From: To:

Create Report

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

Export Data



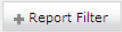
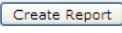
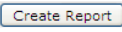
 ☒ Average ☐ All

Table 16-10: Average Score Report – Field Descriptions

Field	Description
	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°; can be changed by the user.
To:	Search before this call date(s). Automatically populated by SmartTAP 360°; can be changed by the user.
List of users	List of evaluatees. Automatically populated by SmartTAP 360°; 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="564 1305 1027 1563" data-label="Image"> </div> <ul style="list-style-type: none"> ■ Click to export data to Excel.

Part III

System Configuration

17 Viewing/Searching an Audit Trail

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

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

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



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

Figure 17-1: Audit Trail

The screenshot shows the 'Audit trail' interface. At the top, there is a blue header bar with the text 'Audit trail'. Below this, there is a section titled 'Selection criteria' which contains a list of users. To the right of the list, there are two date input fields labeled 'From:' and 'To:', both set to '12/31/18'. Below these fields is a 'Search' button.

Selection criteria	From:	To:
Adar, Tania	12/31/18	12/31/18
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		

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

Figure 17-2: Audit Trail Query Result

Name	Action	Timestamp	Description
ST-Teams100	LOGIN	01/14/2021 11:05:58 AM	User ST-Teams100@smarttap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/14/2021 11:17:25 AM	User ST-Teams100@smarttap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:11:55 PM	User ST-Teams100@smarttap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:18:58 PM	User ST-Teams100@smarttap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:21:48 PM	User ST-Teams100@smarttap.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. Click
ST-Teams100	PLAY_CALL_MEDIA	01/17/2021 02:22:06 PM	ST-Teams100 requested playback of media for call id 43. Click
ST-Teams100	PLAY_CALL_MEDIA	01/17/2021 02:23:46 PM	ST-Teams100 requested playback of media for call id 43. Click
ST-Teams100	LOGIN	01/17/2021 02:28:11 PM	User ST-Teams100@smarttap.onmicrosoft.com successfully logged in.
ST-Teams100	LOGIN	01/17/2021 02:29:44 PM	User ST-Teams100@smarttap.onmicrosoft.com successfully logged in.

Table 17-1: Audit Trail

Field	Description
	Click to hide the area
	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.
Navigation buttons under the search display: 	

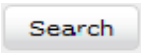
Field	Description
Buttons are shortcuts to the beginning/end, previous/next page of the displayed entries. The drop-down list allows changing the number of entries that are displayed per page.	


Exporting an Audit Trail

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

➤ **To export the audit trail:**

1. Open the Audit Trail screen (**System** tab > **Monitoring** Folder > **Audit Trail**).
2. Select the User or Users to view and date range.

3. Click  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

18 Managing Licenses

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

- **Targeted user licenses:** Enables SmartTAP 360° 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 differ for each integration type.



- Compliance Call Recording can be enabled on Microsoft 365 A3/A5/E3/E5/Business Premium and Office 365 A3/A5/E3/E5 users.
- For Microsoft Teams integrations, its possible to allocate user licenses using this interface, however for other integrations user licenses are allocated on-the-fly.

- **Targeted User Licenses:**
 - **Audio Targets:** 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:** Sets the number of users that can be assigned to a Recording Profile for recording Audio and Video, Desktop Sharing and chats. "Audio & Video Concurrent Recordings" licenses (described below) are required to record these users calls
- **Concurrent Recording Licenses:**
 - **Audio Concurrent Recordings:** 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:** 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.
- **Analytics Licenses Usage:** see descriptions below

Figure 18-1: Licenses

Licenses

Total Targets License Usage
Last Updated Tuesday, December 7, 2021 2:04:49 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Targets	2	2	0	2		
All Included Targets	4	4	0	4		

Teams Concurrent Calls Recordings License Usage
Last Updated Tuesday, December 7, 2021 2:04:49 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	2	0	2	0		
Audio & Video Concurrent Recordings	4	0	4	2		

Analytics License Usage
Last Updated Tuesday, December 7, 2021 2:04:49 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Analytics Users	2	2	0	2		
Analytics Hours	2	0	2	2		

Refresh

Licenses

Total Targets License Usage
Last Updated Wednesday, July 6, 2022, 7:06:01 PM

License	Total	Used	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Targets	10	0	10	2		
All Included Targets	10	4	6	4		

Teams Concurrent Calls Recordings License Usage
Last Updated Wednesday, July 6, 2022, 7:06:01 PM




License	Total	Used	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	10	0	10	2		
Audio & Video Concurrent Recordings	10	0	10	14		

Analytics License Usage
Last Updated Wednesday, July 6, 2022, 7:06:01 PM

License	Total	Used	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Analytics Users	15	2	13	3		
Analytics Hours Bank	14	0	14			

Analytics License Usage
Last Updated Wednesday, July 13, 2022, 3:56:18 PM

License	Total	Used	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Analytics Users	100	3	97	95		
Analytics Monthly Hours	100	0	100	0		

Analytics License Usage						
Last Updated Wednesday, July 13, 2022, 4:12:42 PM						
License	Total	Used	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Analytics Users	100	3	97	95	 0	
Analytics Hours	100	0	100		2	

This screen is divided into four sections:

- **Total License Target Usage:** Displays the total number of licenses (configured in License file) and currently consumed licenses accumulated for all integration types.
- **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.
- **Analytics License Usage:** Displays the following:
 - **Analytics Users:** Total number of analytics users licenses.
 - **Analytics Monthly Hours:** The number of hours of calls analyzed by the Analytics service (this amount is reset on a monthly basis).
 - **Analytics Hours:** The analytics hours which represents a one-time allocation for the number of hours.
- **Other Integrations:** Displays that total number and currently consumed concurrent recording licenses for other integrations (if existing). See [Licenses for Other Integrations](#) below.



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

Licenses for Other Integrations

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

- **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.
 - **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.

- **All Included Targets:** This license sets the number of users that can be assigned to a Recording Profile for recording Audio. 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 Video and Audio enabled recording profile.
- **Desktop Sharing Concurrent Recordings:** This license determines the maximum number of concurrent Desktop Sharing and Audio recordings of the users that are assigned to Desktop Sharing and Audio enabled recording profile.
- **Agent Evaluation:** This license determines the maximum number of agent evaluation licenses.

➤ **To view Managed Licenses:**

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





Figure 18-2: Licenses for Other Integrations




LICENSE_SERVER@STVM5510070

Sales Order Number 1219877
Product Key st55v
Date Issued 12/07/2021
Customer Name QA

Total Targets License Usage
Last Updated Tuesday, December 7, 2021 2:13:32 PM





License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Targets	150	2	148	2 	<input type="text" value="0"/>	
All Included Targets	150	4	146	4 	<input type="text" value="0"/>	




LICENSE_SERVER@STVM5510070

Sales Order Number 1219877
Product Key st55v
Date Issued 12/07/2021
Customer Name QA

Teams Concurrent Calls Recordings License Usage
Last Updated Tuesday, December 7, 2021 2:13:32 PM





License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	150	0	150	0 	<input type="text" value="0"/>	
Audio & Video Concurrent Recordings	150	0	150	2 	<input type="text" value="0"/>	




LICENSE_SERVER@STVM5510070

Sales Order Number 1219877
Product Key st55v
Date Issued 12/07/2021
Customer Name QA

Analytics License Usage
Last Updated Tuesday, December 7, 2021 2:13:32 PM











License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Analytics Users	150	2	148	2 	<input type="text" value="0"/>	
Analytics Hours	10	0	10	2 	<input type="text" value="1"/>	




CD-SIPREC@STVM5510070


Sales Order Number 0000000000
Product Key st55v
Date Issued 12/07/2021
Customer Name Demo

CD-SIPREC@STVM5510070 Concurrent Calls Recordings License Usage
Last Updated Tuesday, December 7, 2021 2:13:32 PM

License	Total	In Use	Available	Max. Consumed*	Notification Threshold Value	Set/Modify Threshold Value
Audio Concurrent Recordings	4	0	4	0 	<input type="text" value="0"/>	
Agent Evaluation	8	0	8	0 	<input type="text" value="0"/>	
IM Targets	4	0	4	0 	<input type="text" value="0"/>	
Video & Audio Concurrent Recordings	2	0	2	0 	<input type="text" value="0"/>	
Desktop Sharing Concurrent Recordings	2	0	2	0 	<input type="text" value="0"/>	

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.

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



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.

Assign Licenses

This section describes how to assign licenses to Teams users.

➤ To assign licenses to users:

1. Open the Assign Licenses page (**System** menu > **Monitoring** folder > **Assign Licenses**).

Figure 18-3: Assign Licenses

Licensed Targets

Audio: Used Licenses/Available Licenses: 0 / 100
All Included: Used Licenses/Available Licenses: 44 / 150

Set all None

Name	Recording Profile	Recording license
ST-Teams11, ST-Teams11	Full Time_Video_DAS	All Included
ST-Teams12, ST-Teams12	Full Time_Video_DAS	All Included
ST-Teams13, ST-Teams13	Full Time_Video_DAS	All Included
ST-Teams14, ST-Teams14	Full Time_Video_DAS	All Included
ST-Teams20	VPNCpolicy	All Included
ST-Teams21	VPNCpolicy	All Included
ST-Teams22	VPNCpolicy	All Included
ST-Teams23	VPNCpolicy	All Included
ST-Teams24	VPNCpolicy	All Included
ST-Teams25	VPNCpolicy	All Included
ST-Teams26	VPNCpolicy	All Included
ST-Teams27	VPNCpolicy	All Included
ST-Teams28	VPNCpolicy	All Included
ST-Teams29	VPNCpolicy	All Included
ST-Teams30	VPNCpolicy	All Included
ST-Teams31	VPNCpolicy	All Included
ST-Teams32	VPNCpolicy	All Included
ST-Teams33, ST-Teams33	VPNCpolicy	All Included
ST-Teams34, ST-Teams34	VPNCpolicy	All Included
ST-Teams35, ST-Teams35	VPNCpolicy	All Included

20 (1 of 3)

2. In the Name field, enter the username whose license you wish to assign.
3. From the Recording Profile drop-down list, select the name of the recording profile to assign the user license
4. From the Recording License drop-down list, select the recording license type:
 - All Included
 - None
 - Audio
 Or
5. From the Set all drop-down list, select one of the above values to apply globally to all users.

Assign Analytics Licenses

This section describes how to assign Analytics licenses.

➤ To assign licenses for analytics users:

1. Open the Assign Analytics License page (**System** tab > **Assign Analytics License**).








Figure 18-4: Licensed Targets


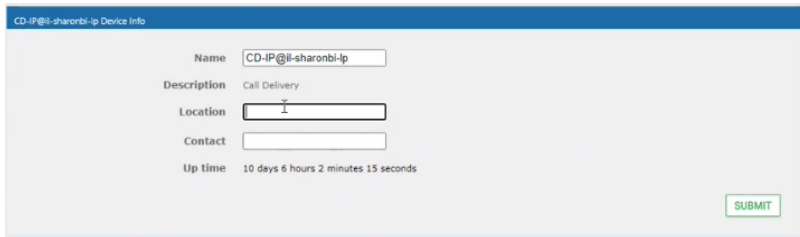


The screenshot shows the 'Licensed Targets' interface. At the top, it says 'Analytics: Used Licenses/Available Licenses: 4 / 10'. Below this is a table with columns: Name, Analytics Profile, and Analytics license. The table lists four teams: ST-Teams11, ST-Teams12, ST-Teams13, and ST-Teams14. Each team has an assigned Analytics Profile and an Analytics license. A 'Set all' button is highlighted in a red box in the top right corner.

Name	Analytics Profile	Analytics license
ST-Teams11, ST-Teams11	Managed Identity_Analytics Profile_EN	Analytics
ST-Teams12, ST-Teams12	Managed Identity_Analytics Profile_EN	Analytics
ST-Teams13, ST-Teams13	EN_Analytics Profile	Analytics
ST-Teams14, ST-Teams14	EN_Analytics Profile	Analytics

At the bottom of the table, there is a pagination bar showing '20' items per page, '1' of 1 page, and '(1 of 1)' items.

2. In the Name field, enter the username whose license you wish to assign.
 3. From the Analytics Profile drop-down list, select the name of the Analytics profile to assign the user license.
 4. From the Analytics Profile drop-down list, select the Analytics license type:
 - Analytics Users
 - Analytics Hours
- Or
- From the Set all drop-down list, select one of the above values to apply globally to all users.

Field	Description
	the type of this device is set as 'Host'.
Port	SNMP UDP Listening Port of the managed device to add.
Status	Indicates the status of the managed device.
	 Device status is UP: the device has registered and is sending heartbeats periodically at regular 30 second intervals.
	 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 device connections 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> <div>  Clicking the Device Name link opens the control panel page for this device. </div>
Device Location	<div>  Devices location information. Sorted ascending/descending by clicking header up/down arrows. If defined, the field entry displays only matching entries. Click an entry to add a device location. This configuration is relevant for all CD processes. This is a global configuration which overrides any user location configuration. </div>

Field	Description
	 
Device Type	Type of the device provided during registration. A manually added device has type 'Host'. In SmartTAP 360°, valid device types are as follows: Unknown; Host; Call Delivery-IP; Call Delivery-SIPREC; Media Server; Communication Server; Integration Specific; Health Monitor; Remote Transfer Service, Teams Bot and Media Delivery. Sorted ascending/descending by clicking header up/down arrows. The dropdown only displays matching entries. 'Unknown' devices are devices unreachable by the Application Server's Web service.
Up Time	Time elapsed since the device status became UP.
Down Time	Time elapsed since the device status became DOWN.
Version	Version of the registered device.
Address	IP address or Host name of the registered device.
	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.

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, 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 19-2: 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.

20 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 AudioCodestools folder in Program Files under Config (ex. C:\Program Files\AudioCodes\Tools\HealthMonitor\Config). Email notification with generated reports can be sent via email (requires HealthMonitor SMTP configuration).

The Health Monitor is installed automatically on SmartTAP 360° server as a part of the SmartTAP 360° installation, under the AudioCodestools 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 218

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 20-1: General Configuration

The screenshot shows the 'General' configuration tab. It includes a list of days for monitoring, a 'Report Time' field, an 'Email notification' checkbox, and a prominent 'SAVE' button.

- **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:

```
\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](#) Default: Disabled.

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

```
\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).

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

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

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

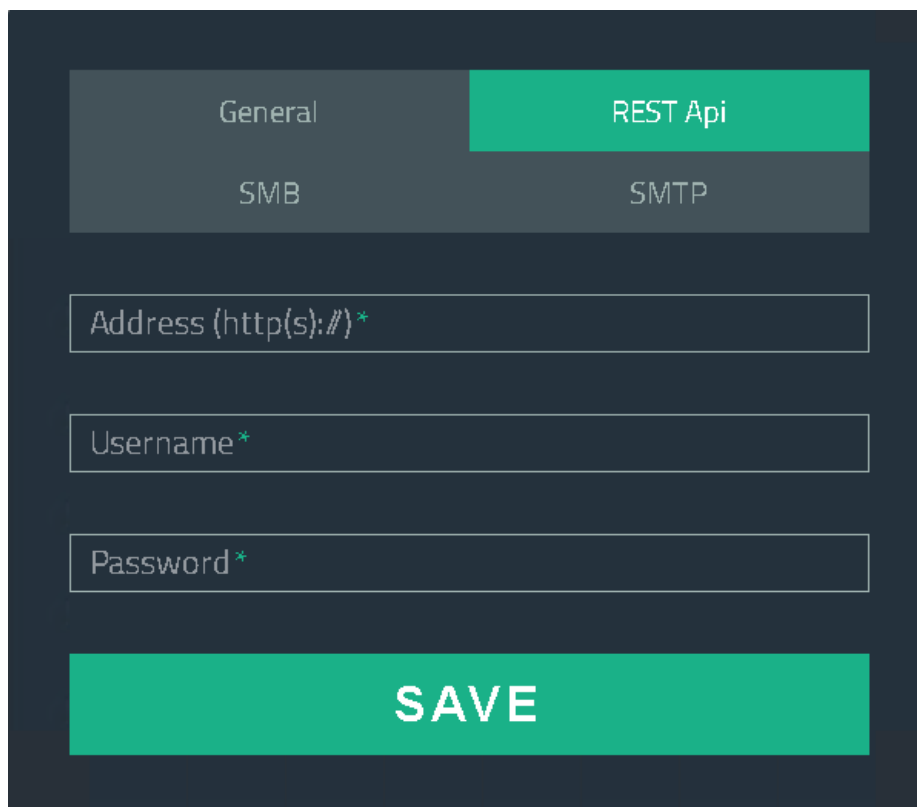
- **ReportLocaton:** Enables the storage of reports in a custom location. Default is [HM LOCATION]\Reports.

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

REST API Configuration

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

Figure 20-2: REST API Configuration



The screenshot displays the 'REST API Configuration' window. It features a dark background with four tabs: 'General', 'REST Api' (highlighted in green), 'SMB', and 'SMTP'. Below the tabs, there are three input fields: 'Address (http(s):/)*', 'Username*', and 'Password*'. A large green 'SAVE' button is positioned at the bottom of the configuration area.

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. Refer to the [SmartTAP Installation Guide](#).

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 20-3: 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

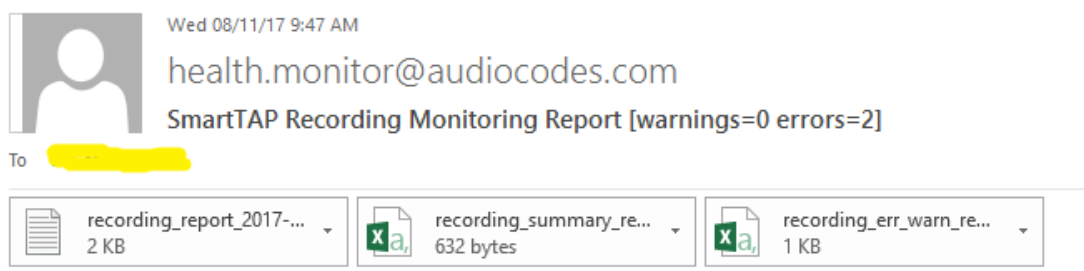
```

Figure 20-4: 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 20-5: 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 20-6: Email Format:

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

Received from: <http://172.17.127.133>

21 Monitoring Storage Statistics

The SmartTAP 360° server monitors disk utilization on File/SMB and Azure Blob disks that are used for storing recorded media. Notification thresholds can be configured to trigger an alarm when utilized storage space approaches its maximum allocation. Standalone data is collected for each managed storage disk and notifications can be configured separately for each disk.

- **File/SMB Storage Usage Statistics:** Storage utilization calculations include the free storage, the size and rate of the new recordings and also the size and rate when older recordings (exceeding the retention value) are deleted.
- **Azure Blob Storage:** Azure Blob storage is sampled once a day. Storage utilization calculations include the free storage, storage growth in the past month and the estimated number of months of free storage based on ratio of free storage to the growth in the previous month.



This feature is relevant for any Blob Azure hosted in AudioCodes Azure deployment. It is only available for AudioCodes hosting and storage setup. For Customer hosting or BYOS, consumption can be viewed in the customers' Azure tenant.

➤ To monitor storage SMB/File usage statistics:

1. Open the Storage Usage Statistics (**System** tab > **Monitoring** Folder > **Storage Statistics**).

Figure 21-1: Storage Usage Statistics

Storage Statistics								
 vision- st.kfbzxc023eujpy1td1sboh5a.ax.internal.cloudapp.net Tuesday, November 22, 2022, 3:01:21 PM	Storage Usage Statistics From Oct 23, 2022 To Nov 23, 2022							
	Media Path	Total Available Storage	Storage Left	Net Recording Rate/day	Estimated Time Left	Samples	Notification Threshold Value	Set/Modify Threshold Value
	C:/media	126.45GB	66.14GB	n/a	n/a	0	0	<input type="button" value="SUBMIT"/>


2. Set the Notification Threshold value (**GB**) for triggering notifications when storage disk capacity is approaching its limit.
 - Open the View/Modify Alarm Notifications (**System** tab > **Alarms** Folder > **Notifications** menu).
 - Click  adjacent to the **I/O Error** alarm.

Figure 21-2: I/O Error Alarm Notification

- Select the users to receive the notification when the threshold is crossed: From the 'Non-Recipients' table use the > and >> keys to select the relevant users to move to the 'Email Recipients' table.
- Click **SUBMIT**.

3. Use the table below as a reference.

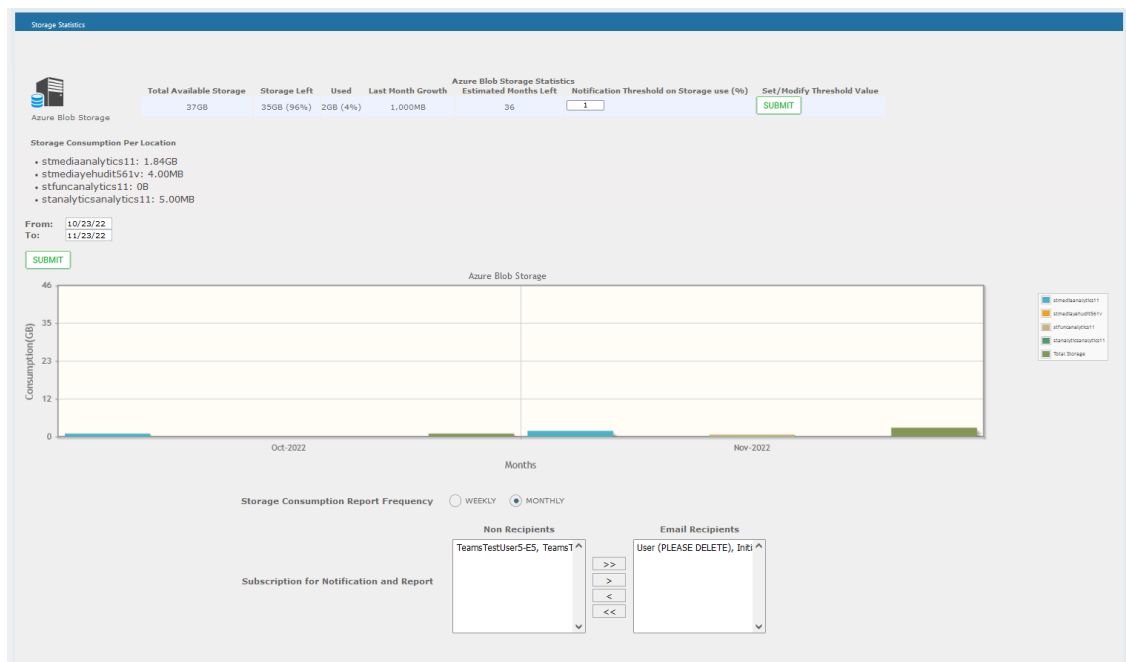
Table 21-1: File/SMB Storage Statistics Fields

Field	Description
Media Path	Saved folder location of the stored media recordings.
Total Available Storage	The total storage available (GB) for the media. Note: the drive's total storage is assumed. The storage reflects all media types (audio and video).
Storage Left	The remaining disk storage space (GB).
Net Recording Rate / day	The net average storage space (GB) consumed per day, calculating the net between the recording rate and the deletion (retention) rate.
Estimated Time Left	Estimated time remaining before the Media Path is full.
Samples	Number of days used to calculate the Net Recording Rate.
Notification Threshold Value	Specifies the threshold GB of consumed disk space/total allocated media disk space before an alarm is triggered. Default: 0 (never notify).

➤ To monitor Azure Blob usage statistics:

1. Open the Storage Usage Statistics (**System** tab > **Monitoring** Folder > **Storage Statistics**).

Figure 21-3: Azure Storage Statistics



The lower pane displays a graph which charts the average monthly disk consumption (GB) on the Azure Blob Storage device. A separate bar graph is generated for each configured storage device (indicated by unique color-coded)

2. Select the date range to filter graph for specific time range.
3. Set the Storage Consumption Report Frequency check box to **Weekly** or **Monthly**. The generated report includes table and graph data. See example report below.

[You don't often get email from mi-teams01@smarttap.onmicrosoft.com. Learn why this is important at <https://aka.ms/LearnAboutSenderIdentification>]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Storage Consumption Report: Weekly Report

The utilization of your SmartTAP Blob storage(s) can be viewed in the below table.

Total Available Storage: 20GB
Used: 12MB (0%)
Storage Left: 20GB (100%)
Notification Threshold: 1%
Last Month Growth:
Estimated Months Left:

Consumed per media location
stmediaomr561terpck: 12.00MB

Reminder that threshold values can be changed in your SmartTAP system's storage statistics settings.

4. Set the Notification Threshold value (%) for triggering notifications when storage disk capacity is approaching its limit.
 - Select the users to receive the automated notification when the threshold is crossed: From the 'Non-Recipients' table use the > and >> keys to select the relevant users to move to the 'Email Recipients' table.

- Click SUBMIT.

5. Use the table below as a reference.

Table 21-2: Azure Blob Storage Statistics

Field	Description
Total Available Storage	<p>The total storage available for the media. The Total Available storage is calculated as follows:</p> <p>■ Audio User Licenses + All Included User Licenses = Free Storage Allocation (1 GB per user) + Purchased Storage Allocation.</p> <p>For example, a customer user has 100 Audio User Licenses + 100 All Included Users Licenses = 200 GB Free Storage Allocation + Purchased Storage Allocation e.g. 500 GB. In this case, the customer has a Total Available Storage of 700 GB.</p>
Storage Left	The remaining disk storage space (GB) % that is allocated for media.
Used	Currently utilized disk space (GB) % that is allocated for media.
Last Month Growth	Growth in disk storage GB that is allocated for media in the past month.
Estimated Months Left	Estimated number of months of remaining storage calculated based on Storage Left/Last Month Growth.
Notification Threshold on Storage Use (%)	Specifies the threshold % of Used disk space reached to trigger the sending of an email notification to the customer.

An example threshold alarm is shown below.

Name	Description	Source	Date	Summary	Detail
Resource Threshold Exceeded	The threshold of a limited resource has been exceeded.	AzStorage	November 18, 2022, 6:00:06 AM	The storage space remaining for the Azure Storage is below the threshold of 1%.	Total storage space: 37.00GB Free space remaining: 34.38GB Estimated recording time remaining: 35.2 Months
Resource Threshold Cleared	The usage of a limited resource has been reduced below the threshold value.	AzStorage	November 22, 2022, 11:30:08 AM	The storage space remaining for the Azure Storage is above the threshold of 6%.	

(1 of 1)

22 Configuring OVOC Connection

This section describes how to setup the connection to the OVOC server. SmartTAP 360° 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° components and forwarded to OVOC from the SmartTAP 360° Application server. OVOC Agents are installed on the SmartTAP 360° Application server for this purpose. For more information, refer to the [SmartTAP Installation Guide](#).

➤ **To configure the connection with the OVOC server:**

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

View/Modify OVOC settings

OVOC Connection

☐ Use public OVOC

IP Address :

Trap Port :

Keep Alive Port :

SNMP

☒ SNMP v2 ☐ SNMP v3

Community Read :

Community Write :

System Info

Name :

Location :

Access Settings

Login URL :

SUBMIT **CANCEL**

Figure 22-1: OVOC Settings-Public IP

2. Configure one of the following:

- In the IP Address field, enter the OVOC On-Premises IP address
- Select **Use Public IP** to configure OVOC Public OVOC IP, and then configure the following:
 - ◆ In the OVOC Public IP field, configure the Public IP address of OVOC Cloud deployment.
 - ◆ In the Public User field, enter the Username for connecting to OVOC WebSocket Tunnel. Default: *VPN*

- ◆ In the Public Password field, enter the Password for connecting to OVOC WebSocket Tunnel (Cloud Architecture Mode only). Default: 123456 (note that after initial connection is established, you can change this password and add new users to manage this connection (refer to the OVOC IOM manual).
- 3. In the Trap Port field enter **162**.
- 4. In the Keep Alive Port field enter one of the following:
 - **1161** for Public IP connection
 - **161** for On-Premises IP connection.
- 5. Configure the SNMPv2 community strings:
 - SNMPv2 Community Read string-**public**
 - SNMPv2 Community Write string **-public**
- 6. Configure SNMPv3 settings (OVOC On-Premises deployment only):
 - Security Name-Security Name of the SNMPv3 operator
 - Authentication Protocol-the SNMPv3 authentication protocol (SHA or MD5)
 - Authentication Key- the authentication password.
 - Private Protocol-the SNMPv3 privacy protocol (AES 128 or DES)
 - Private Key-the private key



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

Figure 22-2: 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**

7. Configure System Information:
 - Name
 - Location
8. Login URL: this login is used for logging into the SmartTAP 360° Web interface from OVOC . Enter the SmartTAP Server IP address.
9. Verify that the DNS resolves for the OVOC FQDN is successful, for example Google.com:

```
C:\Users\enterprise1user>nslookup  
www.google.com
```

```
Server: tlc-ovoc.trunkpack.com
```

```
Address: 10.1.1.10
```

```
Non-authoritative answer:
```

```
Name:      www.google.com
```

```
Addresses: 2a00:1450:4006:801::2004
```

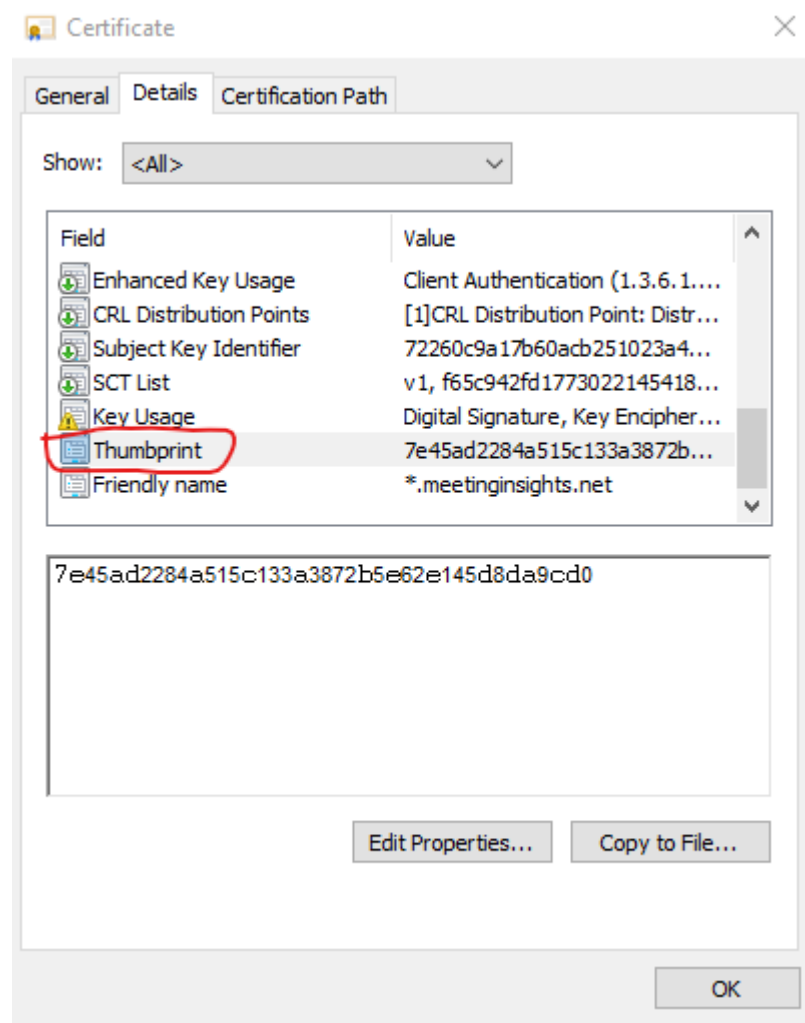
```
172.217.18.36
```

Whitelisting 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 whitelist 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 22-3: 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 ****

23 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 23-1: 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.	
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) [1] [2] [3] [4] [5] [6] [7] [8] [9] [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° 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 23-2: 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.	



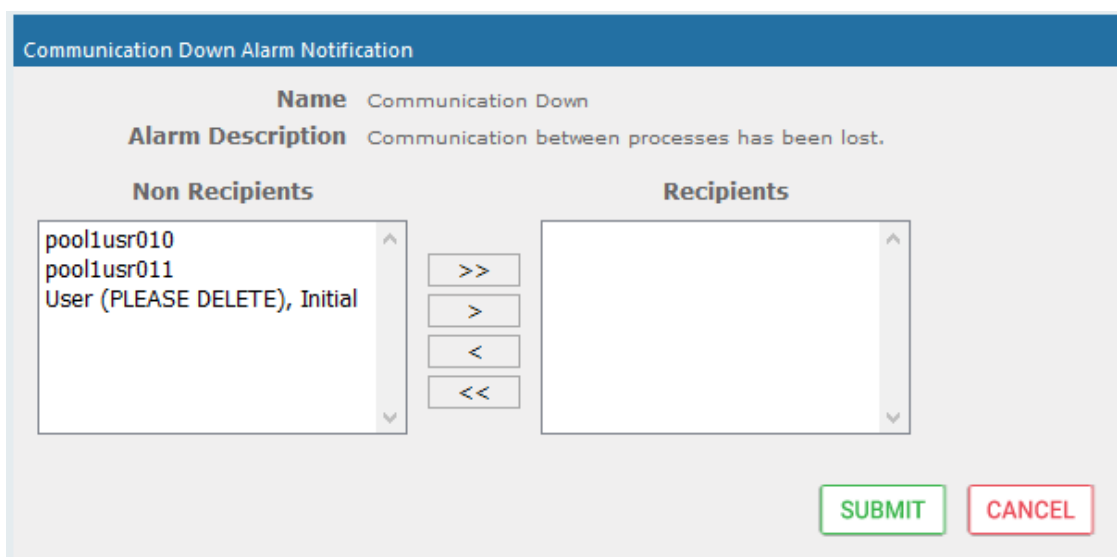

2. Click Modify  on the alarm that you wish to modify.
3. Move the users to receive Email Notifications from the 'Non Recipients' side to the 'Recipients'.
4. Use the assignment keys to assign recipients of the alarm notifications:
 - Click the >> or << keys to move all users between the Non-Recipients 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 23-3: Link Up Alarm Notification



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











Table 23-1: 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 239

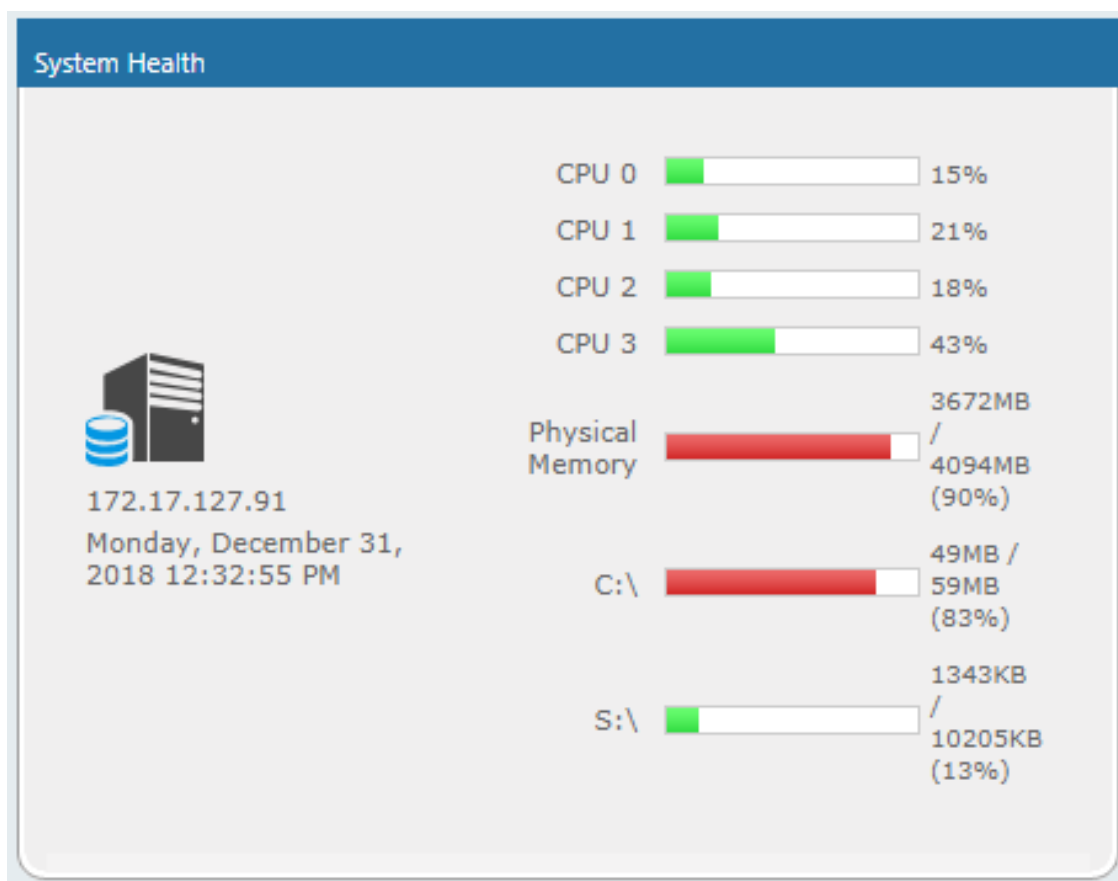
The figure below shows alarm notifications for the 'Resource Threshold Exceeded' notification; sent when the system utilization has exceeded the maximum number of available licenses. The 'Resource Threshold Cleared' notification is sent when the system license utilization falls back within the threshold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

Figure 23-4: 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° 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.



Windows Event Log

By default alarms and events raised on SmartTAP 360° are sent to the OVOC server as SNMP traps (see [Configuring OVOC Connection](#) on page 225) and are not sent by default to the Windows Event Log.

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

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

Figure 23-5: 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 receive 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 -->
145 <System httpClientMode="http" adminAccessUrl="http://localhost:80/rs/audiocodes/recorder/api/" ovocGroup="SmartTap" useEventViewer="true"/>

```

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

- **SmartTAPCalls:** this log includes all alarms and events related to call recording that were logged while running according to the logging configuration. The source attribute of these alarms is “SmartTCalls” and Event ID=<EventID> <Task Category> where 1-Alarm and 2-Event.
- **SmartTGeneral:** this log includes all 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 23-6: Event Viewer SmartTCalls

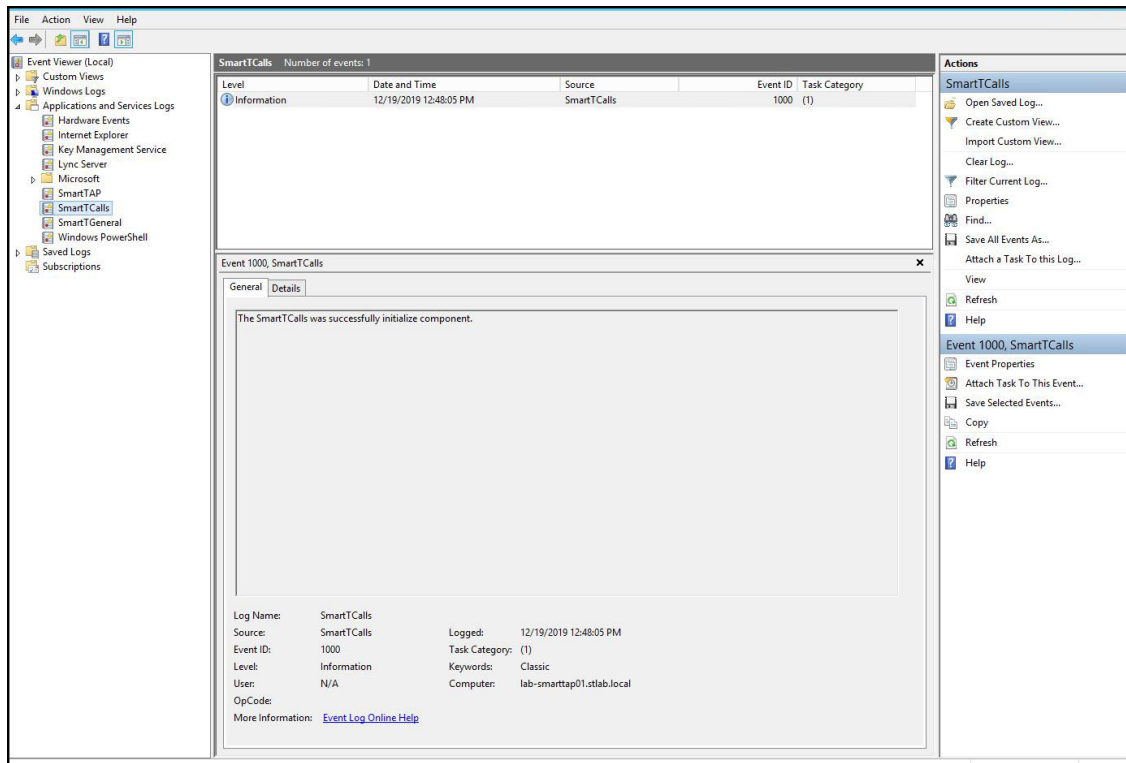
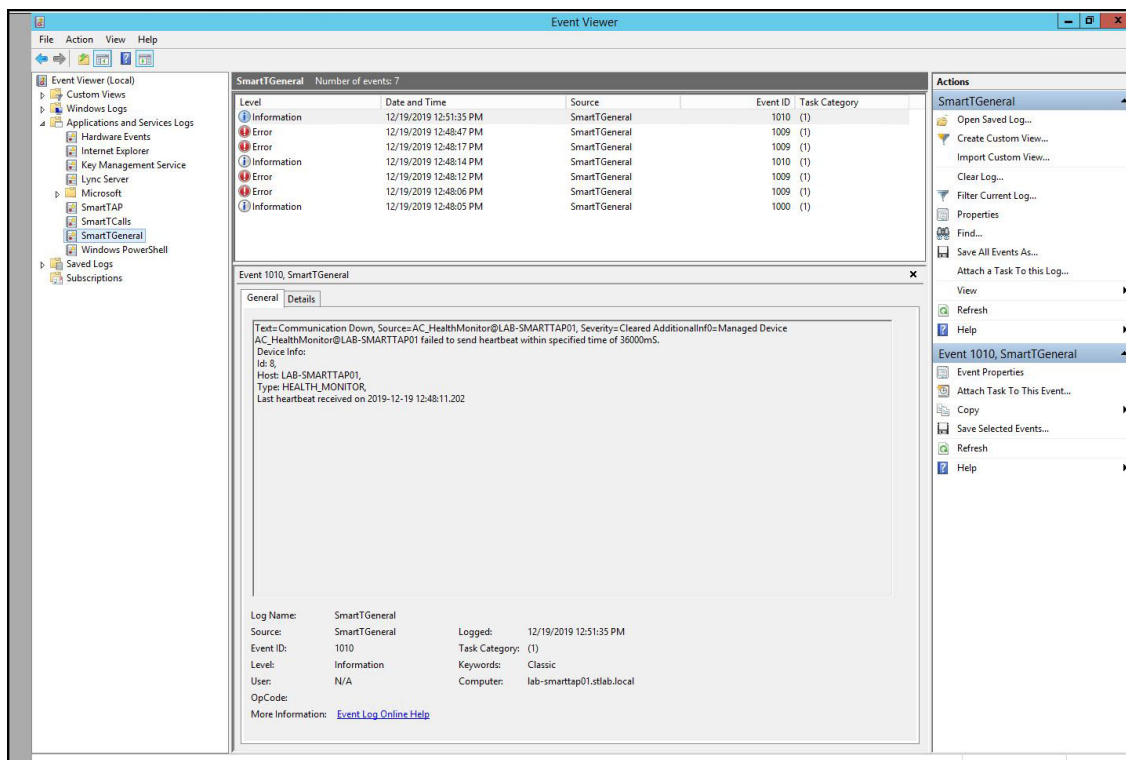


Figure 23-7: Event Viewer SmartTGeneral



SCOM Integration

The SmartTAP 360° platform can be configured to generate the event monitor or send an alert based on a Windows event to the Microsoft SCOM platform. In case of SmartTAP 360°, the

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

SmartTAP Alarms

This section describes the SmartTAP alarms.

SmartTAP System Alarms

This section describes SmartTAP Microsoft Windows Server System 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	Other

Alarm Field	Description		
Cause			
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	The SmartTAP Application server has been restarted. AudioCodes_CS; CallDelivery-IP; HealthMonitorSvc ; AudioCodesMPSSvc; HPXMEDIA RemoteTransferService; AcProcDump CallDeliverySR; CallDelivery;CallDeliveryLD; CallDeliveryAES; SmartTapMonitoringSvc	Component <SmartTap AS FQDN> restarted	-

Event – Component Resource Failed

Alarm Field	Description		
Description	This event is raised in the following circumstances: <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	SmartTapAS_<FQDN>_<resource>, where <resource> is one of the following: <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.

Alarm Field	Description		
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).	-	-
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 following: <ul style="list-style-type: none"> ✓ SMB/File Storage: Configuration in the SmartTAP Web interface Storage Statistics screen. ✓ Azure Blob Storage: Thresholds shown below for Azure Blob storage event. ■ The total hours of calls analyzed by the Analytics Service has exceeded the limit. ■ The number of licensed Analytics users has exceeded the limit.
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 ■ Analytics Hours license value ■ Analytics Users license value ■ AzStorage
Alarm Title	Alarm - Component Resource Threshold Exceeded
Alarm Type	Other
Probable Cause	Other
Additional Info	<p>AzStorage:</p> <ul style="list-style-type: none"> ■ Total Space: <amount> GB ■ Free Space Remaining: <amount> GB

Alarm Field	Description		
	■ Estimated Recording Time Remaining:- <number of months>		
Alarm Severity	Condition	<text>	Corrective Action
Critical/Major/Warning	The media storage location threshold has been reached.	Media Storage threshold exceeded	■ 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.
	Recording License threshold has been exceeded.	Recording License threshold exceeded	■ 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
	The total number of hours of analyzed calls by Analytics Service has exceeded the limit.	Analytics Hours license Threshold Exceeded	■ 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 Analytics hours
	The number of licensed Analytics users has exceeded the limit.	Analytics Users license Threshold Exceeded	■ 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 Analytics user licenses
	The threshold of a limited resource has been exceeded.	The Blob Storage usage reached 90% of available storage.	■ Purchase additional storage or transfer media to another disk.
Cleared	■ When counter returns below the threshold level. ■ The Blob Storage usage reached 80% and below.	-	-

Alarm – Connection Failure

Alarm Field	Description
Description	This alarm is raised in the following circumstances: ■ 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>: ■ AC-MediaProxy @<FQDN> ■ AC-Announcement @ <FQDN> ■ CS@ <FQDN> ■ CD-IP@ <FQDN> ■ CD-SIPREC@ <FQDN> ■ MediaDelivery@ <FQDN> ■ Media Server@<FQDN> ■ AC_HealthMonitor@ <FQDN>

Alarm Field	Description		
	<ul style="list-style-type: none"> ■ AC-Plugin@ <FQDN> ■ RTS@ <FQDN> 		
Alarm Title	Alarm – Connection Failure		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	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 <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 Annoucement Server at <HostNameFQDN> using TCP	
Cleared	-	The connection is up again	-

SmartTAP Agent Alarms

This section describes SmartTAP Microsoft Windows Server Agent alarms.

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 ■ AudioCodesMPSvc ■ 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 – 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 – 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 – 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.	-	-

SmartTAP Application Server Alarms

This section describes SmartTAP Application Server alarms.

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 Field	Description		
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 code <statusCode>, file <path>	Check faulty CDR file

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 A user is mapped to two or more media locations groups via AAD mapping. In this case the user will not be assigned to any media location. A user is mapped to two or more analytics profiles groups via AAD mapping. In that case the user will not be assigned to any analytics profile.

Alarm Field	Description		
	<ul style="list-style-type: none"> User access to Azure Cognitive Services is unauthorized. 		
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. User <username> will be assigned to the default Media Location. A user can not be assigned to multiple Media Locations. Make sure the user is assigned to only one Media Location mapped in SmartTAP. User <username> will be assigned to the default Analytics profile. A user can not be assigned to multiple Analytics profiles, make sure the user is assigned to only one Analytics profile mapped in SmartTAP 		
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	A user cannot be mapped to two or more media locations groups via AAD mapping.	Failed to assign a Media Location to a user	Check the Media Location Group assignments.
Major	A user is mapped to two or more analytics profiles groups via AAD mapping; the user will not be assigned to any analytics profile.	Failed to assign an Analytics Profile to a user	Check the analytics profiles groups assignments.
Major	Access to Azure Cognitive Services is unauthorized.	CognitiveServiceMisconfiguration	Check the permissions authorizations to Azure Cognitive Services.

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 botCluster@botclusterFQDN
Alarm Type	Other
Probable Cause	Other

Alarm Field	Description		
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.	

24 Managing Certificates

SmartTAP 360° server by default operates in non-secure (HTTP) mode. This section describes how to optionally implement SSL/TLS (HTTPS) for the following:

- Securing the connection between your Web browser and the SmartTAP 360° server
- Digitally signing audio files

SmartTAP supports the creation of new certificates and the uploading of existing certificates:

- [Generating New Certificates](#) on the next page
- [Upload Existing Certificates](#) on page 260

Before configuring certificates, note the [Browser Connection Certificate Requirements](#) below



SmartTAP 360° supports HTTPS/TLS 1.2.

Browser Connection Certificate Requirements

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

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

In addition, ensure the following:

- All SAN entries are resolvable via the DNS configured on participating servers/workstations. Make sure the “DNS Suffixes” IPv4 setting is configured correctly.
- Whenever the network is installed with Microsoft Enterprise CA (as opposed to Microsoft Standalone CA), the Domain’s root CA certificate is automatically distributed to all domain member servers and workstations. No further action is required.
- Servers/Workstations that are not members of the forest where Microsoft Enterprise CA is installed, and house SmartTAP 360° components or used to manage SmartTAP 360° via browser, should have the root CA certificate imported into Windows’ “Trusted Root Certificates” store.
- When using 3rd party Certificate Management Suite to self-issue a private certificate chain (as opposed to using a Global CA to issue a Global Certificate), the root CA certificate and intermediate certificates should be imported to certificate local store (Root certificate to 'Trusted Root Certificates', Intermediate certificate to 'Intermediate certificates') on all servers where SmartTAP 360° components reside, and all computers used to manage SmartTAP 360° via its web interface.

Generating New Certificates

New certificates are generated in the following stages:

- **Step 1: Generate Certificate Signing Request (CSR)** below
- **Step 2: Load New Certificates** on page 254

Step 1: Generate Certificate Signing Request (CSR)

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



- The CSR is listed in the Certificate list as a self-signed certificate if you choose not to get a signed certificate from a trusted authority.
- To create a CSR, SmartTAP 360° will automatically use Key type = RSA, Key size = 2048 and Cryptographic Hash = SHA-256.

➤ To generate a CSR:

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

Figure 24-1: Certificate Signing Request Screen

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

Table 24-1: 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.
Province, Region, County or State	The Province, Region, County or State in which your organization is located.
Country	<p>The country in which your organization is located.</p> <p>The following list of country codes is provided as a reference: http://www.digicert.com/ssl-certificate-country-codes.htm </p>
Email	This field is optional..
Public Key	Created automatically by SmartTAP 360°.



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

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



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

Viewing/Modifying the Certificate List

Figure 24-2: 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 24-2: 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**).


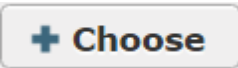
2. Click the  **Import** icon and then the Browse button  to navigate to the location of the appropriate certificate file: 'filename.cer'


Figure 24-3: 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:**


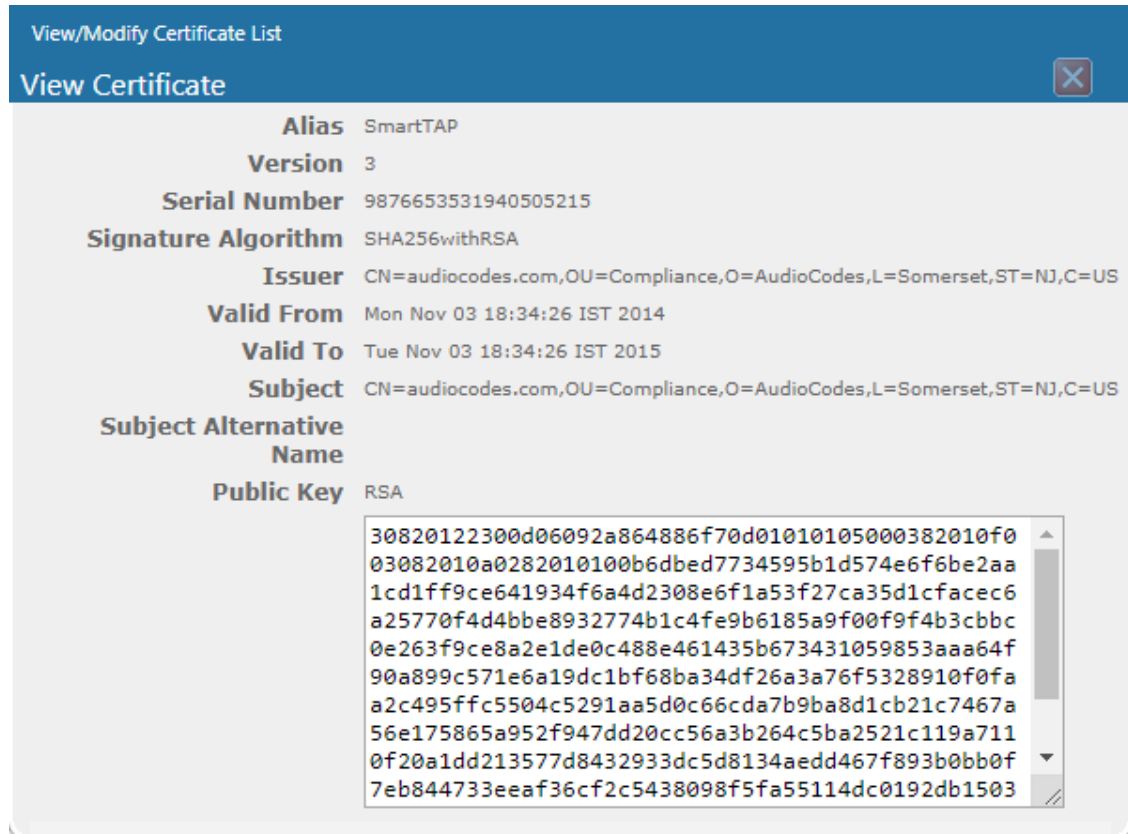
1. Open the View/Modify Certificate List page (**System** tab > **Certificates** folder > **View/Modify Certificate List**), click the  **View** icon.

Figure 24-4: View Certificate



Step 2: Load New Certificates

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

- [Loading Web Browser Certificate](#) below
- Loading Digital Files Certificate

Loading Web Browser Certificate

This section describes how to load the certificate to secure the connection between your Web browser and the SmartTAP 360° server. The following methods can be used:

- Use Local Certificate to secure connection
- Use Azure Key Vault to secure connection

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

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

Figure 24-5: HTTPS Certificate

HTTPS Certificate

Local Certificate: None

Azure Certificate: ☒

Azure Key Vault Name:

Azure Certificate Name:

SUBMIT CANCEL

2. Do one of the following:

- From the Local Certificate drop-down list, select the desired local certificate.
- Select the Azure Certificate check box and configure the parameters below:
 - ◆ Azure Key Vault Name
 - ◆ Azure Certificate Name



The above methods cannot be implemented simultaneously.

Figure 24-6: Key Vault Name

Microsoft Azure

dev-st-kv-sharon1

Overview

Essentials

Resource group: dev-st-sharon1-rg

Location: North Europe

Subscription: SmartTAP_ML

Subscription ID: c4b0174c-b110-43f6-9cf1-4a666f03688

Vault URI: https://dev-st-kv-sharon1.vault.azure.net/

SKU (Pricing tier): Standard

Directory ID: a541d6c3-67b0-47cc-9de3-e0796185c1c7

Directory Name: AudioCodes Ltd. (ai-logi.net)

Soft-delete: Enabled

Purge protection: Disabled

Tags: environment: sharon1, owner: Avi Ben-Shushan, project: SmartTap

Get started

Manage keys and secrets used by apps and services

Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.

Control access to key vault

Assign access policy and determine whether a given service principal, namely an application or user group, can perform different operations on key vault keys, secrets or certificates.

View access policies

Enable logging and set up alerts

Enable logging to monitor how, when and by whom your key vaults are accessed. Monitor performance and configure alerts for key vault metrics e.g., service API latency, error code, throttling.

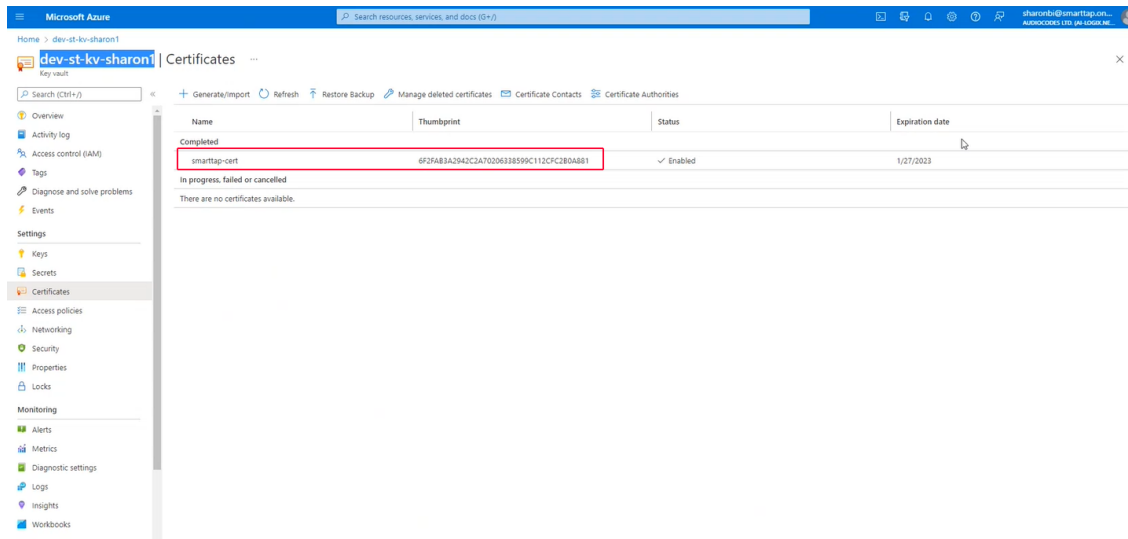
View

Turn on recovery options

For protection against accidental or malicious deletion, soft-delete is enabled. Turn on purge protection to guard against manual purging of deleted key vaults and items. Learn more

Explore

Figure 24-7: Certificate Name



- From the Local Certificate drop-down list, select the certificate that you wish to load and click **SUBMIT**.
- Restart the SmartTAP 360° server.

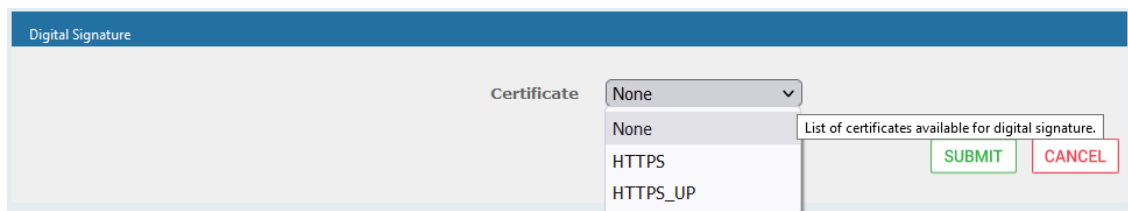
Loading a Digital Signature

A digital signature is a method 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.

➤ To load a Digital Signature:

- Open the Digital Signature page (**System** tab > **Media Locations** folder > **Digital Signature**).
- From the drop-down list, choose the appropriate certificate to use.
- Click **SUBMIT**.

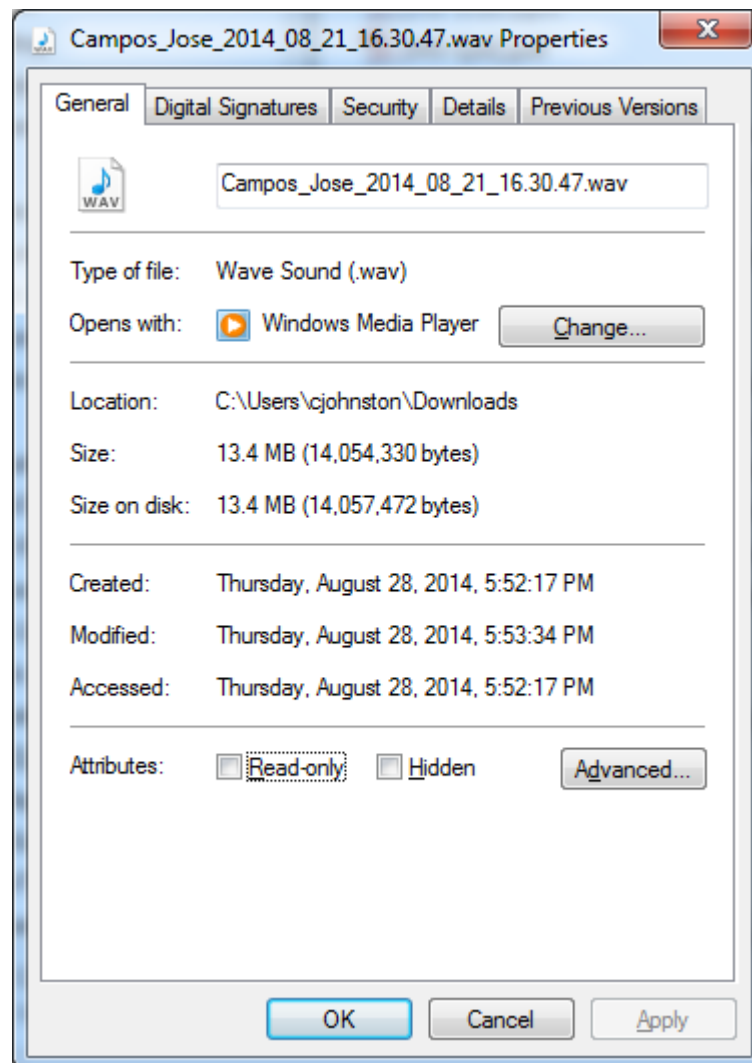
Figure 24-8: Digital Signature

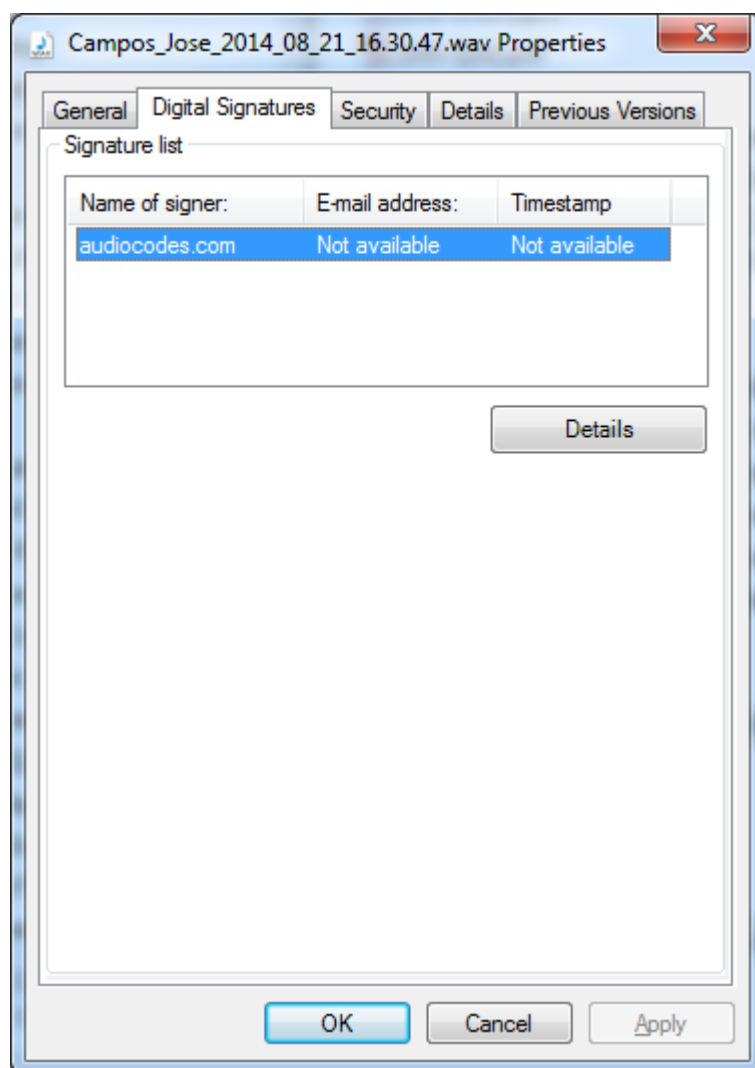


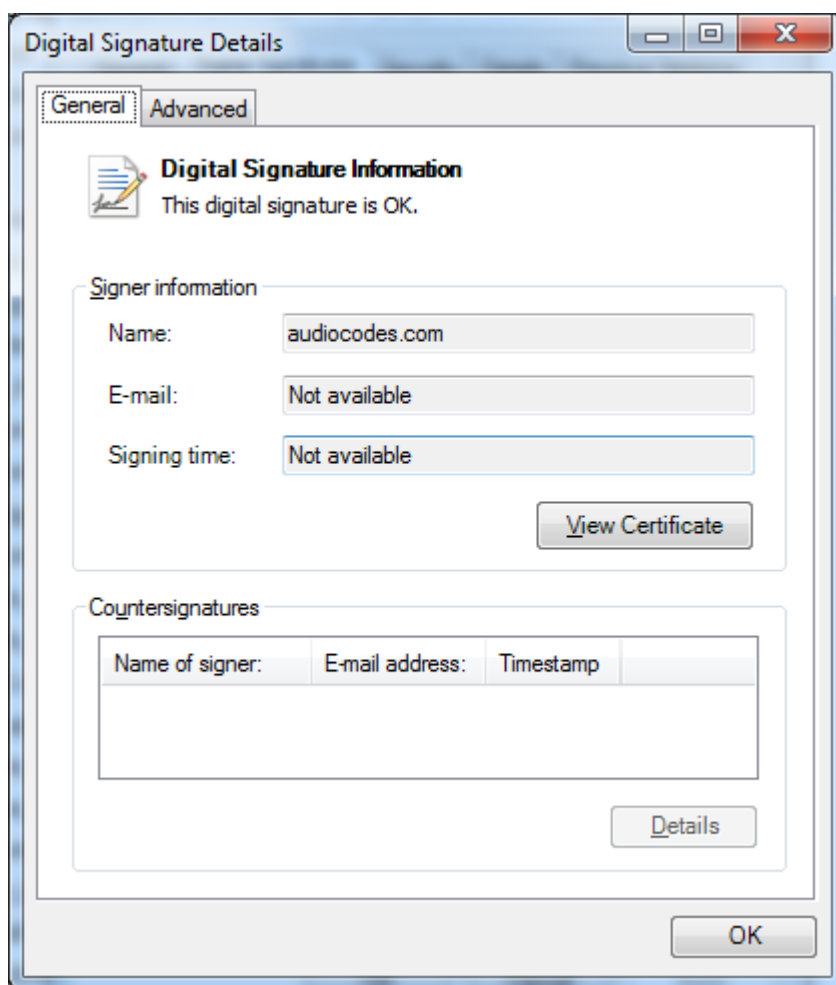
If a user 'optionally' chooses to add a Digital Signature during the download process, the configured certificate is used to digitally sign the audio file. The SmartTAP 360° Digital Signature file properties add-on must be installed on the local user PC to properly view the digital signature in the downloaded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

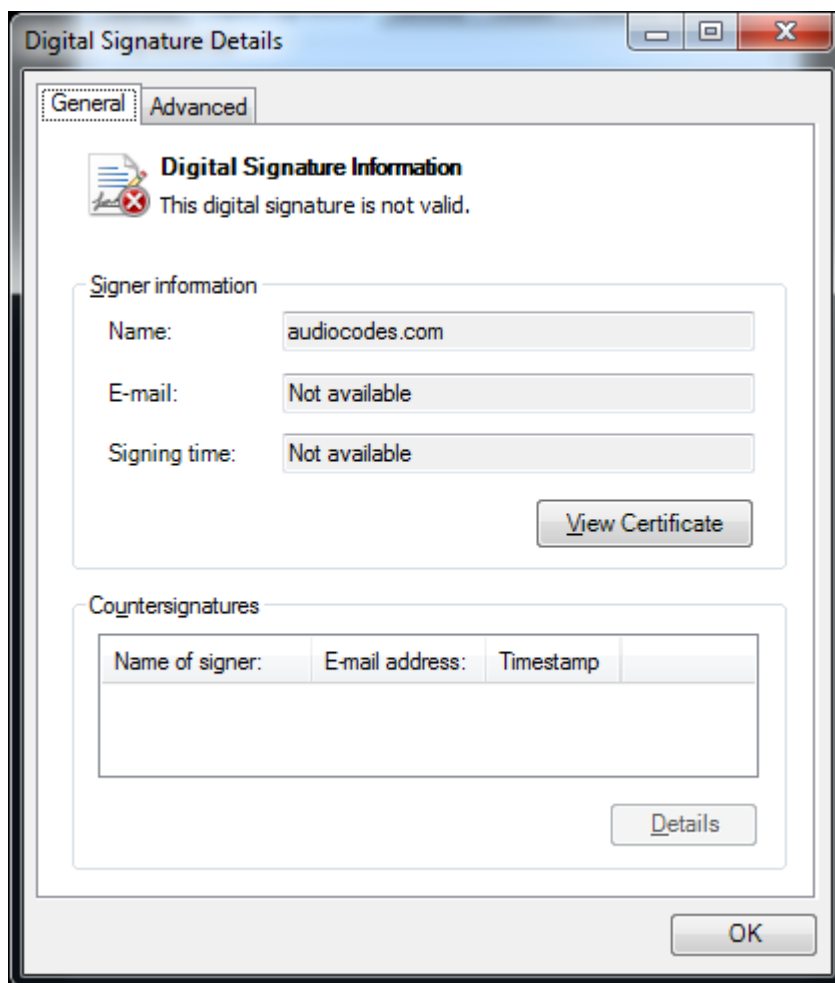
Once installed, the Digital Signatures tab appears in the file properties of the downloaded audio recording. Click it to view the certificate and make sure it's from a trusted source. The certificate must be installed on the local PC in the Trusted Root authority.

Figure 24-9: Digital Signature Details









For instructions on how to install the add-on, refer to the [SmartTAP Installation Guide](#).

Upload Existing Certificates

This section describes how to upload a signed certificate and private key from an existing key-store.

➤ To upload certificates:

1. Copy the certificate to the SmartTAP server (it can be copied to any location on the server).
2. (For Microsoft Teams **Hybrid** deployment **only**) Edit the file \Program Files\AudioCodes\SmartTap\AS\domain\configuration\host.xml as follows:

```
<!--<keystore provider="SMARTTAP_AZ_KS" keystore-
password="{mysql.ngp.pass}" alias="smarttap" />-->
```

- Open the Upload Certificates page (**System** menu > **Certificates** folder > **Upload Certificate**).

- Configure certificate parameters according to the table below.
- Click **SUBMIT** to apply changes.

Table 24-3: Certificate Parameters

Field	Description
Certificate File	The file containing the certificate and private key. For example: "C:\User-s\siprecadmin\Downloads\cert\cert.pfx"
Keystore Type	Choose from one of the following keystore types: <ul style="list-style-type: none"> ■ PKCS12 ■ PFX ■ PKCS11 ■ DKS ■ JKS ■ JCEKS
Key Alias (Optional)	The alias name of the certificate inside the keystore. You can leave this field blank if the keystore contains only one entry, otherwise it must be specified. If not sure about the key alias use the following command to find the alias of the desired certificate: <pre>keytool -list -keystore keyFile.p12 -storepass password -storetype PKCS12</pre>
Keystore	The password that enables access to a keystore. Note that not all keystores

Field	Description
Password	have passwords.
Certificate Alias (Optional)	A unique alias to help identify the certificate.

25 Configuring Email Server Settings

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

Email settings must be configured for SmartTAP 360° to send email messages/notifications, set new user passwords, reset passwords and to email recordings.

➤ **To configure email:**

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



2. Enter the SMTP server information (provided by the SMTP administrator).
3. Configure fields according to the table below.
4. Click  to apply changes.

Table 25-1: Email Screen

Field	Description
SMTP Server	Hostname or IP address of the email server.
SMTP Port	TCP port of the email server.
SMTP User	Email user for authentication. By default, SmartTAP 360° will send emails from CallRecording@<SNMPServerDomain>.com . To make sure an email is sent from your domain, set the SMTP User to username@YourDomain.com . In addition, you can instead customize an email address from which to send emails in the SMTP From field

Field	Description
	(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.

5. Apply changes (SmartTAP 360° tests the Email interface when the user clicks  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.

26 Analytics

This section describes how to configure the connection with the Analytics service.



Analytics is supported for Microsoft Teams integration only.

Configure Connection with Microsoft Cognitive Services

This section describes how to configure the connection with the Microsoft Cognitive Services. Once the connection is successfully established, SmartTAP can retrieve data output generated by the Cognitive Services. For configuration of Analytics profiles and categories and applying to users (see [Managing Analytics Profiles](#) on page 62).

➤ **To configure connection with Microsoft Cognitive Services:**

1. Open the Add Analytics Configuration page (**System** tab > **Analytics** folder > **Add Analytics Configuration**).

2. Configure fields according to the table below.

3. Click  to apply changes.

Table 26-1: Analytics Configuration

Field	Description
Analytics Configuraton Name	The name of the Analytics configuration.













Field	Description
Analytics Configuration Description	A short description of the Analytics configuration.
Storage	The name of the storage container.
Password	The password of the storage container.
Domain	The name of the storage domain.
Cognitive Service Region	The region where the Cognitive Service is applied.
Cognitive Service Key	The security key of the Cognitive Service.
Service Bus Connection String	The connection string of the Service bus.

View and Modify Analytics Configurations

This section describes how to view and modify an Analytics configuration.

➤ **To view or modify analytics configuration:**

1. Open the View/Modify Analytics Configuration page (**System** tab > **Analytics** folder> **View/Modify Configuration**).

View/Modify Analytics Configurations			
Name	Description	Modify Analytics Configurations	Delete
AnalyticsConfiguration 1	Analytics Configuration desc		
an_config	des		
Managed Identity Analytics configuration	Managed Identity Analytics configuration		
New Analytics configuration	new Analytics configuration		
<div> 20   1   (1 of 1) </div>			

2. Click  adjacent to the Analytics Configuration that you wish to modify.

Modify Analytics configuration

Analytics Configuration Name

Analytics Configuration Description

Storage

Password

Domain

Cognitive Service Region

Cognitive Service Key

Service Bus Connection String

3. Configure fields according to the table below.

4. Click to apply changes.

Table 26-2: Analytics Configuration

Field	Description
Analytics Configuration Name	The name of the Analytics configuration.
Analytics Configuration Description	A short description of the Analytics configuration.
Storage	The name of the storage container.
Password	The password of the storage container.
Domain	The name of the storage domain.
Cognitive Service Region	The region where the cognitive service is applied.
Cognitive Service Key	The security key of the cognitive service.
Service Bus Connection String	The connection string of the Service bus.

27 Managing Recording Locations

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 27-1: Managing Recording Locations

Item	Description
Adding Media Storage Recording Locations on the next page.	Defines and adds a new media storage location.
Viewing and Modifying a Recording Location on page 286	View and modify an existing media location.
Associating Users to Media Locations on page 289	Add users to media locations. Multiple media locations can be defined for each user. A default location can be configured.
Configuring Recording Format	Defines a recording format, e.g., encryption and compression.
Configuring Live Monitoring Location	The Live monitoring feature allows users to listen to calls in real time.
Extracting User Credentials from Microsoft Azure Fileshare Account	Describes how to extract the relevant credentials from the Microsoft Azure Fileshare account.
Setup	Describes how to extract the credentials from the Microsoft Azure Blob storage account.

Item	Description
Microsoft Azure Blob Storage Account-Recordings on page 274	

Adding Media Storage Recording Locations

This section describes how to configure locations for storing recorded media. Locations can be mapped to AAD groups where all users calls attached to a specific group are recorded to the mapped location.



RTS is utilized for transferring media to the remote storage (Azure Blob or SMB) and for uploading recorded media to Azure Blob for analytics processing.

The following Storage support options are offered:

■ AudioCodes hosting:

- Azure Blob Storage in AudioCodes subscription
- BYOS – Bring your own Azure Blob storage

■ Customer hosting:

- Azure Blob
- SMB
- Local File Storage

■ **Local File Storage:** Store media on a local file disk on SmartTAP server when a Single SmartTAP server is deployed (Local File Storage is not supported with distributed deployments such as RDDs with Call Delivery and is not supported for Microsoft Teams).

■ **SMB:** Store media on a network accessible drive, i.e., Windows shared drive for accessing files over the SMB protocol. Multiple storage configurations can be defined per location. Whenever the recording location is added or modified, SmartTAP 360° verifies whether this location is accessible to the user defined in this procedure.

SmartTAP supports SMB2 and SMB3 protocol with a default connection timeout of 60 seconds. The following link provides SMB3 timeout parameters in windows:

<https://learn.microsoft.com/en-us/archive/blogs/openspecification/smb-2-x-and-smb-3-0-timeouts-in-windows>.



- It's recommended to define the SMB Scheme host machine with an FQDN instead of an IP address which prevents scenarios where the System administrator changes the IP address of the SmartTAP 360° application server and as a consequence, the media files can no longer be accessed.
- If you define the media location in a different domain to the SmartTAP 360° AS, ensure that write permissions are set for the directory to which you wish to save the media files.
- Transferring the recording to the SMB – The Bot(s) connect to the SMB storage and transfer the recordings. In case of a disconnection, it attempts to reconnect while buffering/keeping the recordings locally (refer to the [SmartTAP Hardware and Software Requirements](#)).

■ **Azure Blob:** Store media on Azure Blob storage. Media files are transferred and accessed from the Azure Blob storage account. For this mode, you must configure a **remote** Host address and configure **HTTPS** scheme. When customers host SmartTAP in AudioCodes subscription (including VMs, DB, Teams Bot components) they can optionally utilize BYOS (Bring their own Azure Blob Storage account) to store call recordings. In this case, customers create the Blob storage account and provide AudioCodes with the relevant access credentials described below. Once SmartTAP is deployed, customers will be able to restrict the access to the storage drive to the IP address of SmartTAP application/ SmartTAP Server IP address and the Teams Bot IP address in case of Teams recording deployment. The following Azure Blob storage accounts can be setup:

- [Setup Microsoft Azure Blob Storage Account-Recordings](#) on page 274
- [Setup Microsoft Azure Blob Storage Account-Analytics](#) on page 282

➤ **To add a recording location:**

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

Figure 27-1: File/SMB Recording Location

Add Recording Location

Location Name	<input type="text"/>
Description	<input type="text"/>
Scheme	<input type="text" value="file"/>
Local Host IP address or FQDN	<input type="text"/>
External Host IP address or FQDN	<input type="text"/>
Path	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Domain	<input type="text"/>
Azure Subscription Id	<input type="text"/>
Azure Resource Group Name	<input type="text"/>

Figure 27-2: Blob Storage Location

Add Recording Location

Location Name

Description

Scheme

Local Host IP address or FQDN

External Host IP address or FQDN

Container

Storage

Password

Domain

Azure Subscription Id

Azure Resource Group Name

SUBMIT **CANCEL**

2. Use the table below as a reference.
3. Click **SUBMIT** to apply changes.

Table 27-2: 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"> ■ File ■ Server Message Block (SMB) Shared File

Parameter	Description
	<ul style="list-style-type: none"> ■ HTTPS (for Microsoft Blob Storage)
SMB Internal Host (SMB)	The internal/Private IP address or FQDN of the SMB Scheme host machine. For Hybrid deployment scenarios, allow VPN traffic from Microsoft Azure Bot deployment via RTS to access the storage host location using Internal/Private IP address.
SMB External Host (SMB)	The NAT IP address or FQDN of the SMB Scheme host machine. For Hybrid deployment scenarios, allow VPN traffic from Microsoft Azure Bot deployment via RTS to access the storage host location using NAT IP address.
Path	Defines the media path pattern. For example, '[filesystem]/[directory]/'yyyy'/MM'/dd'/HHmmss
Username	<ul style="list-style-type: none"> ■ File or SMB: The username for accessing shared resources. ■ Azure Blob: The storage account name where the Blob container was created.
Container (Media Container Name)	<ul style="list-style-type: none"> ■ File or SMB: not applicable ■ Azure Blob: The name of the container of the Blob account.
Storage	<ul style="list-style-type: none"> ■ File or SMB: not applicable ■ Azure Blob: The name of the Blob Storage account.
Password	<ul style="list-style-type: none"> ■ File or SMB: The password for accessing shared resources. ■ Azure Blob: The “access key” for the Blob storage account.
Domain	<ul style="list-style-type: none"> ■ File or SMB: The domain used to authenticate the username and password for accessing shared resources. ■ Azure Blob: The Azure domain used to authenticate the username and password for accessing shared resources.
Azure Subscription ID (AudioCodes Hosted Subscription only)	The Azure Subscription ID is created under the Azure tenant. It enables agreements with Microsoft to use Azure cloud services.
Azure Resource Group Name (AudioCodes Hosted)	The resource group name where all the resources related to the setup are created. Every Azure resource is associated with a Subscription ID.

Parameter	Description
Subscription only)	

Figure 27-3: Configured Blob Storage Recording Location

Modify Recording Location

Location Name

Storage

Description

Blob

Scheme

https

Local Host IP address or FQDN

External Host IP address or FQDN

Container

recordings

Storage

stmediaanalytics11

Password

••••••••

Domain

Azure Subscription Id

c4b0174c-b110-43f6-9cf1-4a666f603686

Azure Resource Group Name

analytics-11

SUBMIT

CANCEL

Setup Microsoft Azure Blob Storage Account-Recordings

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

The following containers must be created on the Customer Azure Storage account:

- Media Storage container
- Metadata Storage container (required when implementing BOT Resiliency)



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. When SmartTAP is deployed in multi-country storage (hosted by customer subscription) both SMB and Blob storage can be configured on the same deployment.

➤ **To configure Microsoft Blob:**

1. Extract the SmartTAP BLOB configuration file from installation package folder, "...\\TerraSmartTap\\TerraSmartTap\\output_data\\SmartTAP_config.txt".

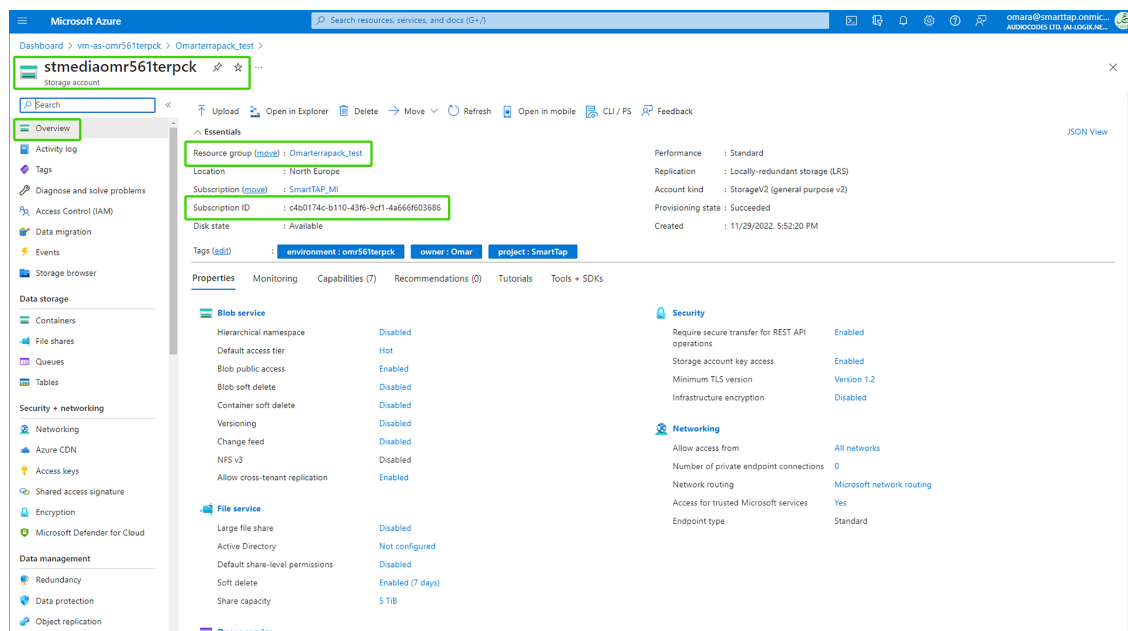
See example below:

Username: Storage account name extracted from "SmartTAP_config.txt file or from Azure portal.

2. Login to the Microsoft Azure portal with customer credentials (<https://portal.azure.com/>).
3. Open the Storage account settings page (create or use an existing storage account).
4. In the Overview page, save the highlighted credentials in notepad as they must be configured for the Storage account setup in the SmartTAP Web interface (see [Adding Media Storage Recording Locations](#) on page 269):

- Storage account name
- Resource group
- Subscription ID

Figure 27-4: New Blob Storage Accounts



5. Create a new container for the Teams recordings media storage. For example, "SmartTAPBlobStorage_Recordings".

Figure 27-5: Create New Blob Container

The screenshot shows the 'Create New Blob Container' dialog. On the left, a list of containers is visible with columns for Name, Last modified, and Public access level. The 'New container' form on the right has the following fields and controls:

- Name ***: A text input field.
- Public access level**: A dropdown menu with the option 'Private (no anonymous access)' selected.
- Create**: A blue button to create the container.
- Discard**: A button to discard the changes.

Name	Last modified	Public access level
bootdiagnostics-stteams-16806f6d-914e-44ed-ad03-2e1cc534eb65	4/23/2020, 12:35:10 ...	Private

New container ✕

Name *

recordings ✓

Public access level ⓘ

Private (no anonymous access) ▼

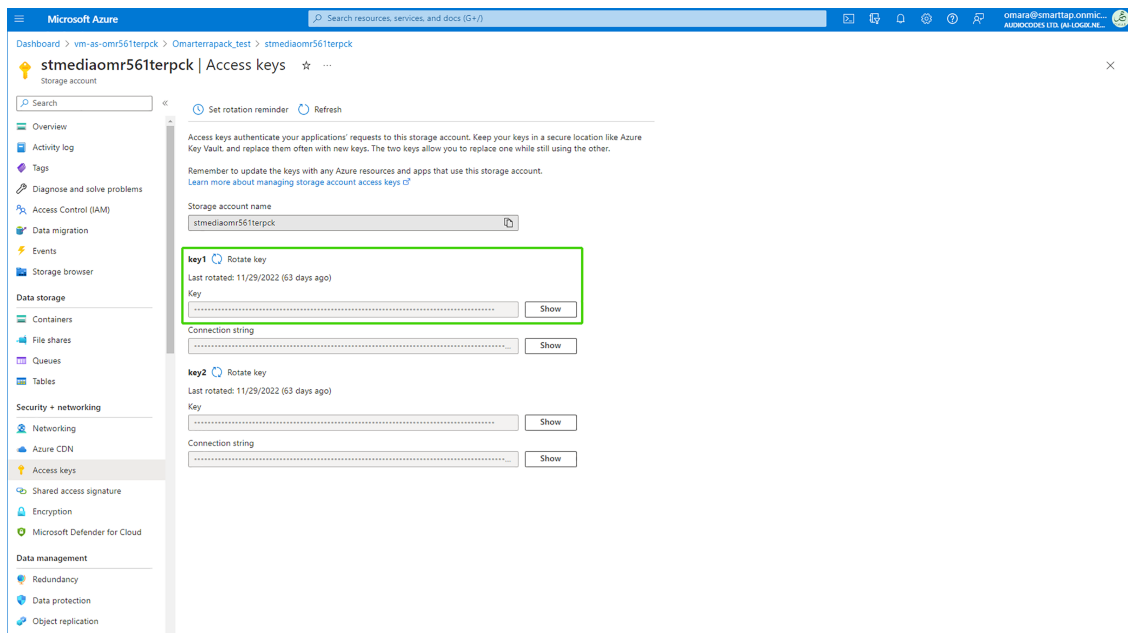
▼ Advanced

Create

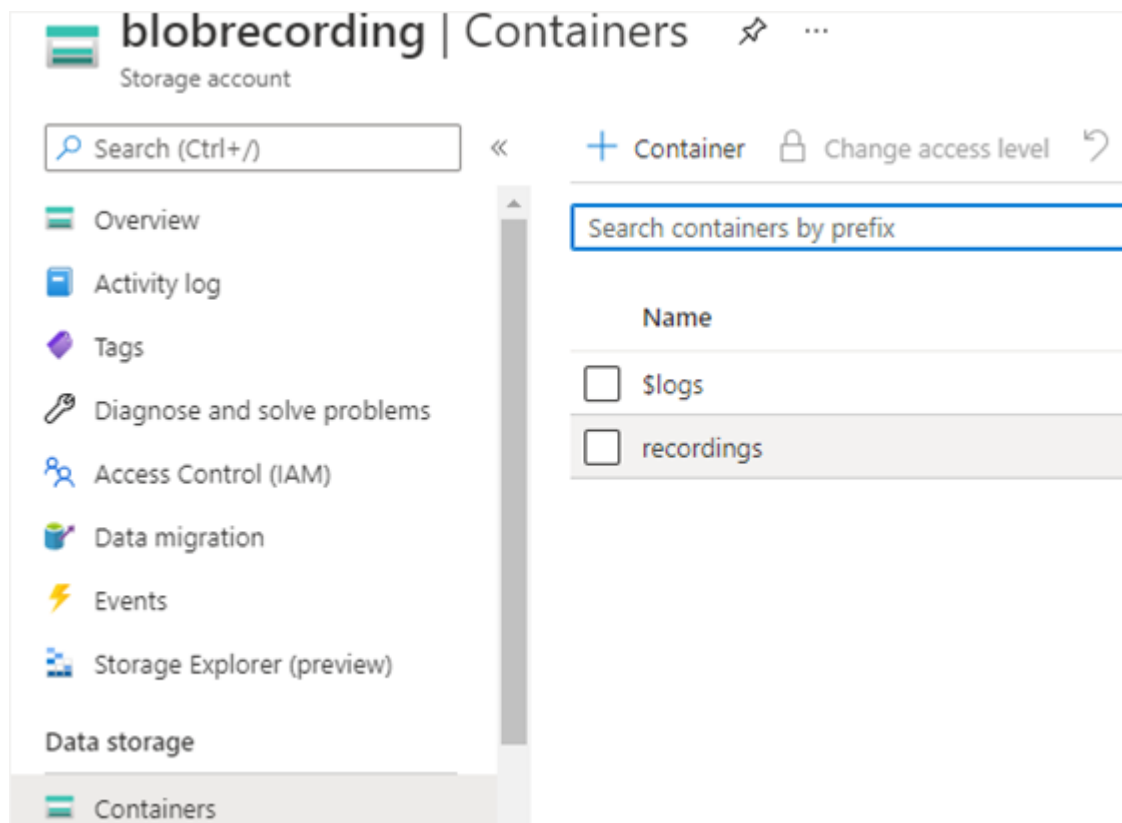
Discard

6. In the Navigation pane, select **Access keys**.
7. Copy one of the access key values to notepad.

Figure 27-6: Access Keys



8. In the same Storage account where the recorded media is stored, create container for the Teams recordings Metadata (resiliency storage). For example, "SmartTAP_BlobStorage_Metadata".



New container ✕

Name *

recordingsmetadata ✓

Public access level ?

Private (no anonymous access) ▼

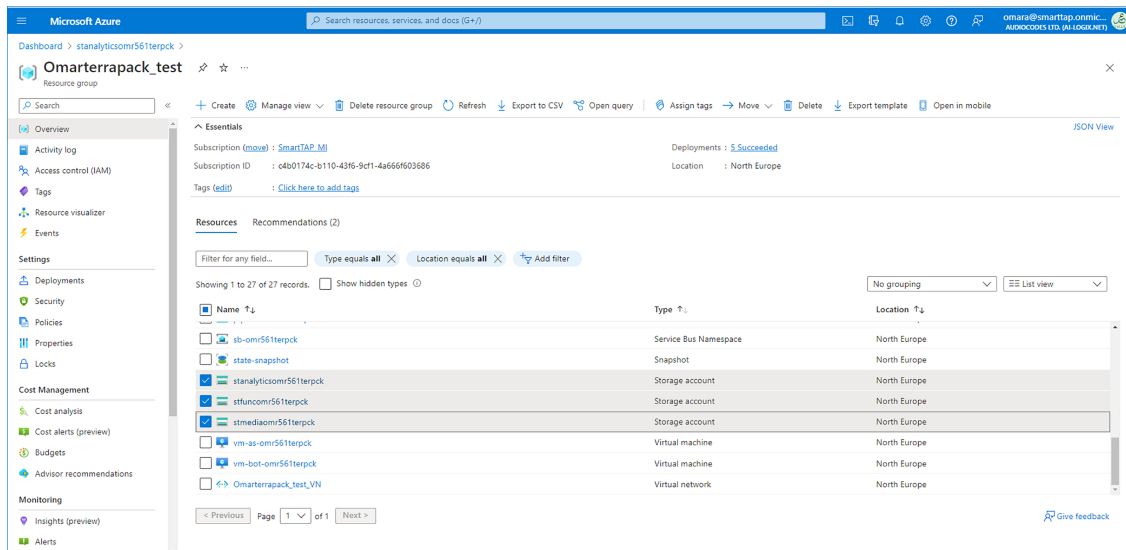
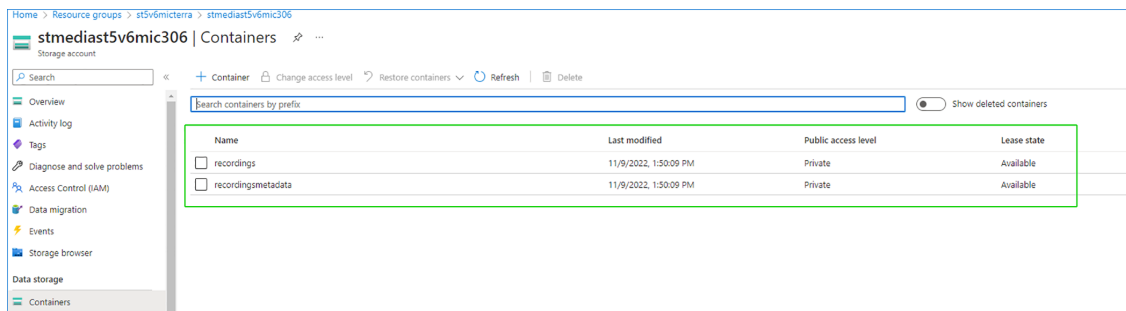
▼ Advanced

Create

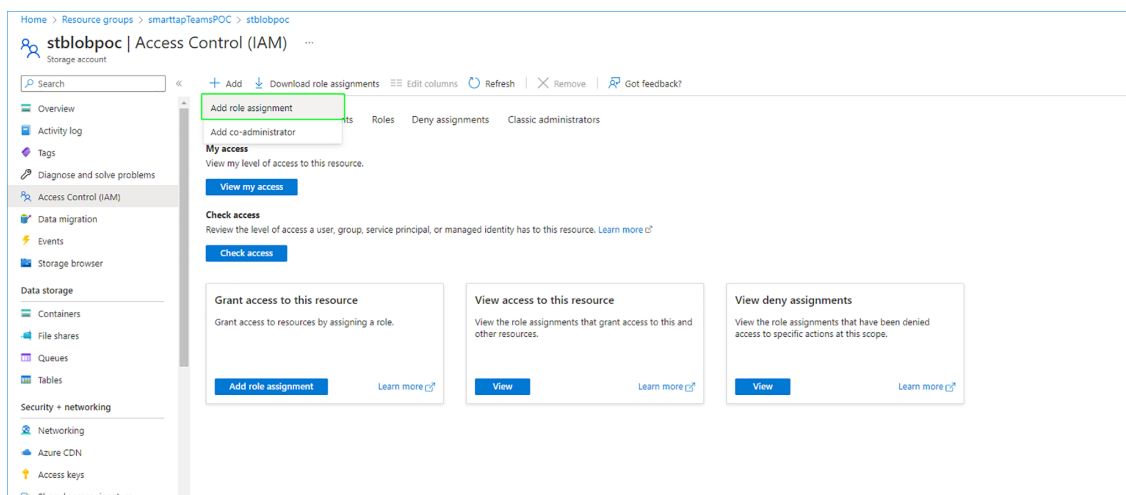
Discard

9. Enter the name **recordingsmetadata** and then click **Create**.

The following figure shows the added containers.



10. Open Access Control (IAM).



11. Click **Add > Add role assignment** and then search for 'Monitoring Reader' rule.

Home > Resource groups > smarttapTeamsPOC > stblobpoc | Access Control (IAM) >

Add role assignment

Got feedback?

Role Members Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#) >

mon

Type: All Category: All

Name ↑	Description ↑	Type ↑	Category ↑	Details
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension...	BuiltInRole	Analytics	View
Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azur...	BuiltInRole	Analytics	View
Monitoring Contributor	Can read all monitoring data and update monitoring settings.	BuiltInRole	Monitor	View
Monitoring Metrics Publisher	Enables publishing metrics against Azure resources	BuiltInRole	Monitor	View
Monitoring Reader	Can read all monitoring data.	BuiltInRole	Monitor	View

< Previous Page 1 of 1 Next >

Home > Resource groups > smarttapTeamsPOC > stblobpoc | Access Control (IAM) >

Add role assignment

Got feedback?

Role Members Review + assign

Selected role Monitoring Reader

Assign access to ☒ User, group, or service principal ☐ Managed identity

Members + Select members

Name	Object ID	Type
No members selected		

Description Optional

Review + assign Previous Next

Select members

Select

oidcauth

☒ OIDCAuthClient

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.
[Learn more about RBAC](#)

Select Close

Home > Resource groups > smarttapTeamsPOC > stblobpoc | Access Control (IAM) >

Add role assignment


[Got feedback?](#)

Role **Members** Review + assign

Selected role Monitoring Reader

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

Name	Object ID	Type
OIDCAuthClient	f3f6d2f7-8088-4f82-9eaa-e5be430d37b9	App 

Description

[Review + assign](#) [Previous](#) [Next](#)

12. Click **Next**.

13. Leave the 'Assign access to' option as default - User, group, or service principal.

14. Click **Select members** link.

15. Search for the OIDC Token app that is configured in SmartTAP Web (see Token Authentication Registration).

16. Click **Review+assign**.

Setup Microsoft Azure Blob Storage Account-Analytics

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

The following containers are created by the TerraSmartTAP Deployment script:

- azure-webjobs-hosts
- azure-webjobs-secrets
- speech-analytics-input
- speec.-analytics-output

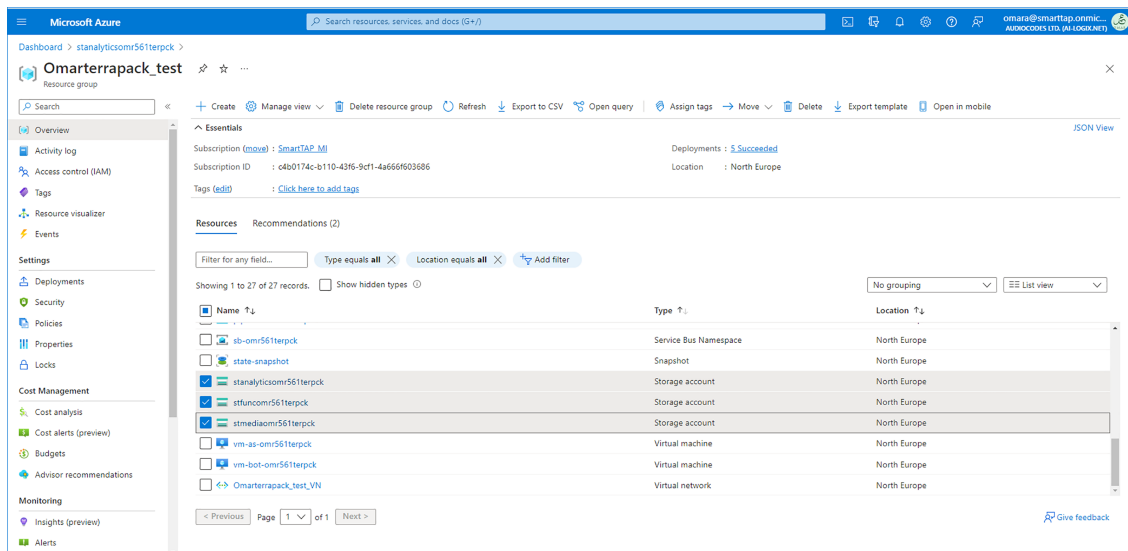


Figure 27-7:



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. When SmartTAP is deployed in multi-country storage (hosted by customer subscription) both SMB and Blob storage can be configured on the same deployment.

➤ To configure Microsoft Blob:

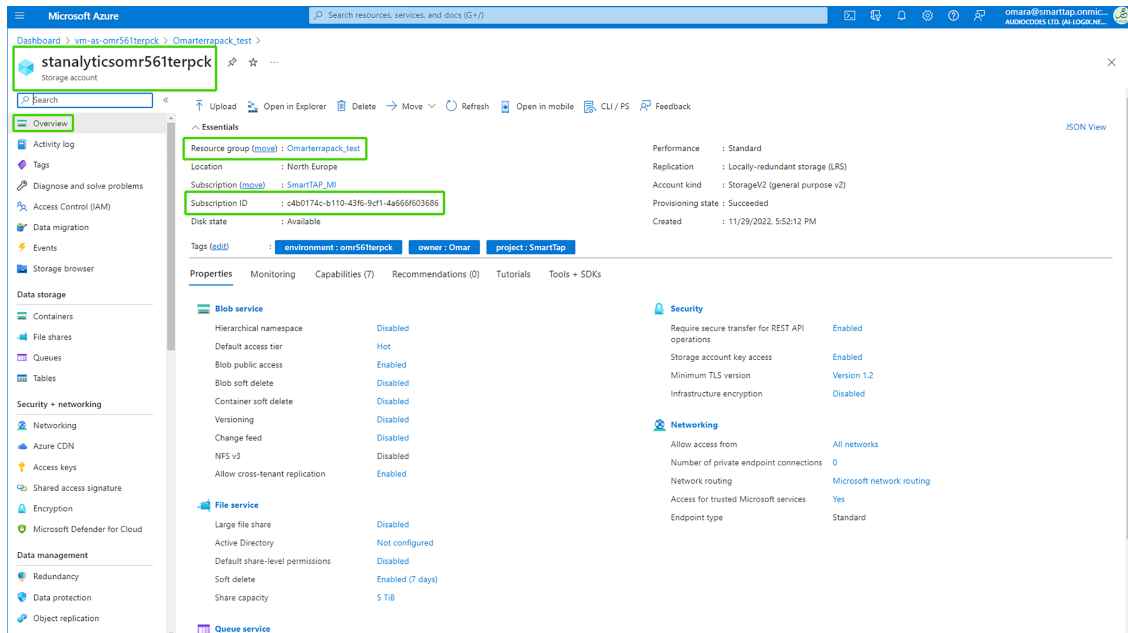
1. Extract the SmartTAP BLOB configuration file from installation package folder, "...\\TerraSmartTap\\TerraSmartTap\\output_data\\SmartTAP_config.txt".

See example below:

Username: Storage account name extracted from "SmartTAP_config.txt" file or from Azure portal.

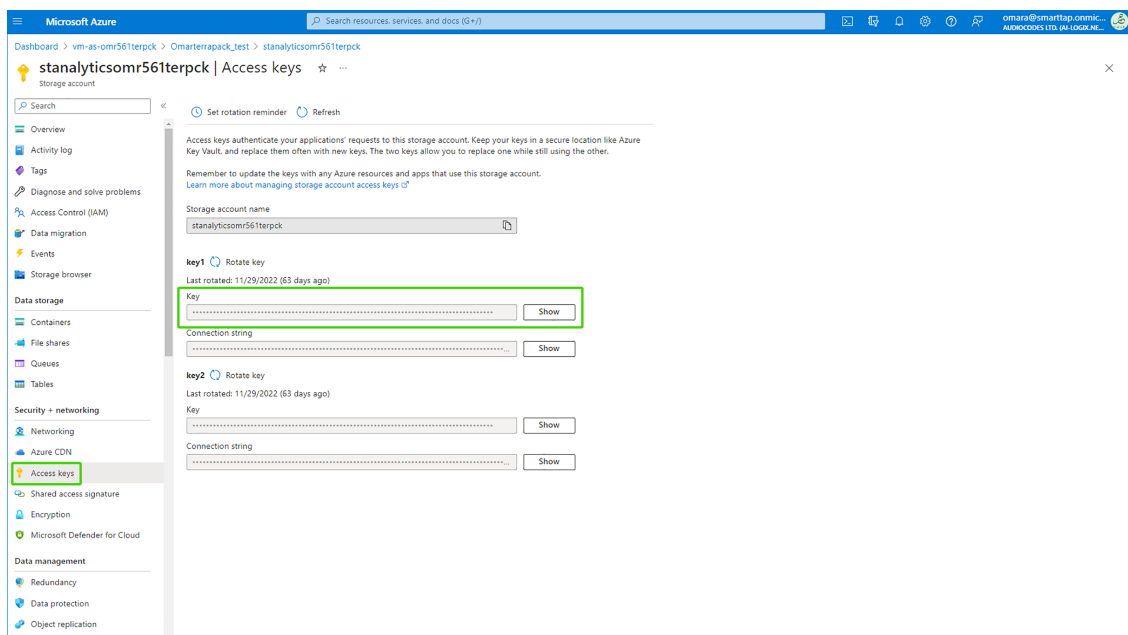
2. Login to the Microsoft Azure portal with customer credentials (<https://portal.azure.com/>).
3. Access the Analytics Storage account created by the TerraSmart script.
4. In the Overview page, save the highlighted credentials in notepad as they must be configured for the Storage account setup in the SmartTAP Web interface (see [Adding Media Storage Recording Locations](#) on page 269):
 - Storage account name
 - Resource group
 - Subscription ID

Figure 27-8: New Blob Storage Accounts



5. In the Navigation pane, select **Access keys**.
6. Copy one of the access key values to notepad.

Figure 27-9: Access Keys



The following screen displays the containers created by the TerraSmartTAP script.

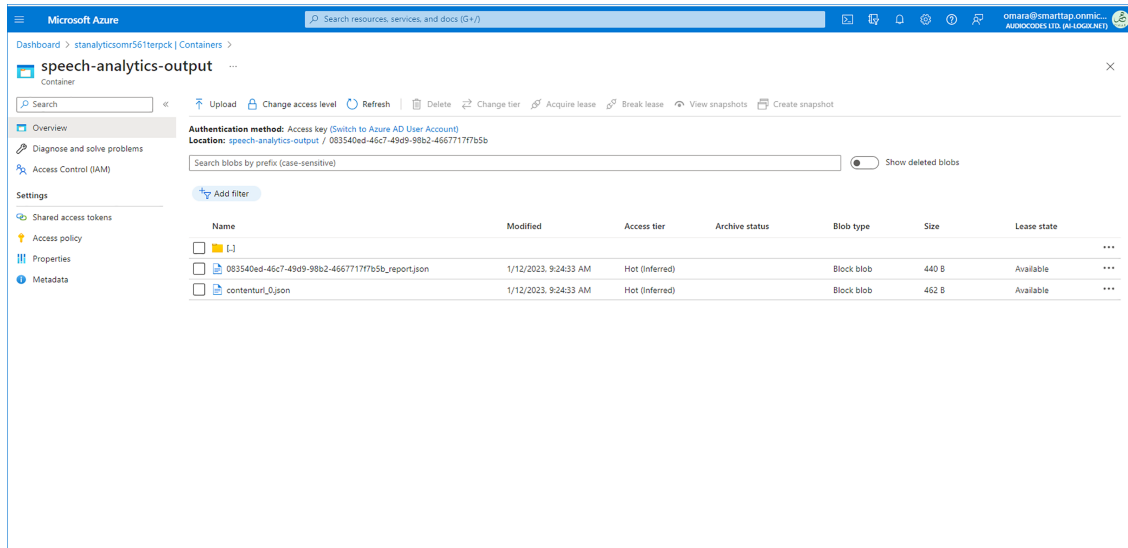
The following screen displays the recorded media files used as input by the Analytics Service.

Name	Modified	Access tier	Archive status	Blob type	Size
102335f8b6d4a1-b499-4831-a30d-a227b060a7cf--1081998339-101-XMQV22.wav	1/11/2023, 12:34:51 PM	Hot (Inferred)		Block blob	19.92 MiB
10245d5901d9a-8f63-49c7-a745-4a239ef50df7--1081998339-103-DONLS2.wav	1/18/2023, 12:25:24 PM	Hot (Inferred)		Block blob	1.75 MiB
104934b5964414-9569-4535-9773-45354caae3c9--1081998339-101-JIPBP2.wav	1/11/2023, 12:50:20 PM	Hot (Inferred)		Block blob	954.42 KiB
105144279990c-bba3-4398-95b8-100d8312aae2--1081998339-101-W1R1Z2.wav	1/11/2023, 12:51:35 PM	Hot (Inferred)		Block blob	578.79 KiB
10847cb73ad1-55b5-469a-94db-d848575d92a1--1081998339-103-SPQEU2.wav	1/18/2023, 12:09:55 PM	Hot (Inferred)		Block blob	1.21 MiB
111718e6bc365e-8464-4670-92c7-a4a8647f8c7e--1081998339-101-CZSTF2.wav	1/11/2023, 1:17:58 PM	Hot (Inferred)		Block blob	416.29 KiB
1118200b0bbdbf-229c-4f69-960a-256913abc08e--1081998339-101-1RMBW2.wav	1/11/2023, 1:18:46 PM	Hot (Inferred)		Block blob	261.92 KiB
11211721939599-c285-4800-8122-fb6f7c51deba--1081998339-101-FNQA42.wav	1/11/2023, 1:21:34 PM	Hot (Inferred)		Block blob	128.79 KiB
112158823cf967-e8ff-4e9a-92fa-a3536ea0c9ad--1081998339-101-V56YL2.wav	1/11/2023, 1:22:22 PM	Hot (Inferred)		Block blob	147.54 KiB
1122222d35e11-03a4-4614-bd8f-28c16ded4a20--1081998339-101-RV1KG2.wav	1/18/2023, 1:24:17 PM	Hot (Inferred)		Block blob	2.76 MiB
112228175d6479-6950-464e-b0e0-120cd35504f--1081998339-101-S4AL92.wav	1/11/2023, 1:27:42 PM	Hot (Inferred)		Block blob	8.71 MiB
1138203a217a33-00c3-406b-87f6-b341368600dc--1081998339-103-8QA3L2.wav	1/11/2023, 1:40:12 PM	Hot (Inferred)		Block blob	2.59 MiB
114249eb55f2-5282-4342-9c20-431e2df12b17--1081998339-101-IVV6D2.wav	1/11/2023, 1:44:14 PM	Hot (Inferred)		Block blob	2.17 MiB
114335e0b55f2-5282-4342-9c20-431e2df12b17--1081998339-103-ASFHQ2.wav	1/11/2023, 1:45:46 PM	Hot (Inferred)		Block blob	3.15 MiB
114919db0024-06eb-47f0-9485-e5c713e5da10--1081998339-101-9ISTX2.wav	1/11/2023, 1:53:32 PM	Hot (Inferred)		Block blob	7.11 MiB

The following screen displays the output media files that were analyzed by the Analytics Service.

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
00703b03-34cd-4546-acaf-add8c985f0a4						...
0460d819-2448-4b92-9743-38b81e1223a3						...
083540de-46c7-49d9-98b2-46677177b5b						...
0d478f5c-bd7a-4dec-a847-c19d99990fe						...
0e32c51a-c5fa-4278-8346-5decd532b5a						...
0f7560de-bf4a-45f6-ad23-1b632d7c8349						...
123abba9-f6a2-4a33-909f-61e7a3917f0						...
15b69ecb-1af3-41c9-a412-a3ef1ad25f01						...
2a29326a-c41c-4d2b-9d7b-aab46f0cc24d						...
2dc6765b-3cf8-4b13-9c59-fc0aef1bfe1a						...
2fddaeab-9ded-49a3-8139-129f9fa3bee						...
316d7bd6-2a73-4536-8f00-7d985b94ebef						...
327c2e11-e0b5-4b78-a170-a28a957bb296						...
352819b5-dc8a-47b0-8044-ef0d456166bd						...
36a957f4-fc4f-4569-9afb-bfa6a03299b8						...


The following displays an example output file generated by the Analytics Service.



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 Locations** folder > **View/Modify Rec. Locations**).
2. Click  to set location as the default recording location.



The default location cannot be deleted.

Figure 27-10: View/Modify Recording Locations

View/Modify Recording Locations							
Location Name	Path or Container	Description	Username	Domain	Modify	Default	Remove
Initial	recordings	Initial Recording Location	mediabxnmstfcert54				
STQATeam	recordings	STQATeam	mediabxnmstfcert54				
ST-Teams-Users		ST-Teams-Users					
ST-load-test-dynamic-rename		ST-load-test-dynamic-rename					

3. Click  to open the Modify Recording Location screen.

Figure 27-11: Modify Recording Location

• **Location STQATeam successfully updated.**

Modify Recording Location

Location Name

STQATeam

Description

STQATeam

Scheme

https

Host

Container

recordings

Storage

mediabxnmsftcert54

Password

Domain

SUBMIT

CANCEL

Modify Recording Location

Location Name

az1

Description

az1

Scheme

file

Local Host IP address or FQDN

External Host IP address or FQDN

Path

recordings

Username

stmediaqatest6

Password

Domain

Azure Subscription Id

c4b0174c-b110-43f6-9cf1-4a666f603686

Azure Resource Group Name

rg-qatest6

SUBMIT

CANCEL

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

5. Click **SUBMIT** to apply changes.

Table 27-3: 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: <ul style="list-style-type: none"> ■ File ■ Server Message Block (SMB) Shared File ■ HTTPS (for Microsoft Blob Storage)
Host	<ul style="list-style-type: none"> ■ File or SMB schemes: The IP address or FQDN of the SMB Scheme host machine. ■ Microsoft Azure Fileshare: 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
Username	<ul style="list-style-type: none"> ■ File or SMB schemes: Specifies username for accessing shared resources. ■ Microsoft Azure Fileshare: Specifies the Storage username defined for the Fileshare storage account. ■ Azure Blob: Specifies the storage account name where the Blob container was created.
Password	<ul style="list-style-type: none"> ■ File or SMB schemes: Specifies password for accessing shared resources. ■ Microsoft Azure Fileshare: Specifies the Storage Password defined for the Fileshare storage account. ■ Azure Blob: Specifies the “access key” for the Blob storage account.
Domain	<ul style="list-style-type: none"> ■ File or SMB schemes: Specifies the Azure domain used to authenticate the username and password for accessing shared resources. ■ Microsoft Azure Fileshare: Specifies 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

Parameter	Description
	<p>“core.windows.net”. This value is shown as the “EndpointSuffix” in the Azure Portal.</p> <ul style="list-style-type: none"> ■ Azure Blob: Specifies the Azure domain used to authenticate the username and password for accessing shared resources.
Azure Subscription ID	The Azure Subscription ID is created under the Azure tenant. It enables agreements with Microsoft to use Azure cloud services.
Azure Resource Group Name	The resource group name where all the resources related to the setup are created. Every Azure resource is associated with a Subscription ID.
Container	<ul style="list-style-type: none"> ■ File or SMB schemes: not applicable ■ Microsoft Azure Fileshare: not applicable ■ Azure Blob: Specifies the name of the container of the Microsoft Azure account.
Storage	<ul style="list-style-type: none"> ■ File or SMB schemes: not applicable ■ Microsoft Azure Fileshare: Specifies the name of the Azure Fileshare storage account. ■ Azure Blob: Specifies the name of the Blob Storage account.

Associating Users to Media Locations

This section describes how to associate users to recording media locations defined in [Adding Media Storage Recording Locations](#) on page 269. User recordings can be stored in multiple locations according to regions or countries defined by the customer and required by local regulations. This ensures the local integrity of stored recorded data together with a secure connection to the central database.

➤ To add users to media locations:

1. Open the Users/Devices page (**Users** tab > **Media Locations** > **Users/Devices**).

Add Users to Media Locations

Default Media Location

- ST-Teams20
- ST-Teams21
- ST-Teams22
- ST-Teams23
- ST-Teams24
- ST-Teams25
- ST-Teams26
- ST-Teams27
- ST-Teams28
- ST-Teams31
- ST-Teams32
- ST-Teams33, ST-Teams33
- ST-Teams34, ST-Teams34
- ST-Teams35, ST-Teams35
- ST-Teams36, ST-Teams36
- ST-Teams37, ST-Teams37
- ST-Teams38, ST-Teams38
- ST-Teams39, ST-Teams39
- ST-Teams40, ST-Teams40
- ST-Teams41, ST-Teams41
- ST-Teams42, ST-Teams42
- ST-Teams43, ST-Teams43
- ST-Teams44, ST-Teams44
- ST-Teams45, ST-Teams45
- ST-Teams46, ST-Teams46
- ST-Teams47, ST-Teams47
- ST-Teams48, ST-Teams48
- ST-Teams49, ST-Teams49
- ST-Teams80, ST-Teams80
- ST-Teams81, ST-Teams81
- ST-Teams82, ST-Teams82
- ST-Teams83, ST-Teams83
- ST-Teams84, ST-Teams84
- ST-Teams85, ST-Teams85
- ST-Teams86, ST-Teams86
- ST-Teams87, ST-Teams87

Media Locations

Azure Managed Identity

- ST-Teams11, ST-Teams11
- ST-Teams13, ST-Teams13

Default

SMB-Azure2

- ST-Teams29
- ST-Teams30

SUBMIT CANCEL

- Use the table below as reference.
- Click **SUBMIT** to apply changes.

Table 27-4: Media Locations

Field	Description
Default Media Locations	
Media Locations	
>>	Assign all users to a specific location.
>	Add selected user to a specific location.
<	Remove selected user from specific location.
<<	Remove all users from specific location.

Field	Description
CANCEL	Cancel changes.

Configuring Recording Format

This section describes how to define a recording format for Audio, Video and Analytics.

➤ **To define a recording format:**

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

2. Configure fields according to the table below.

3. Click **SUBMIT** to apply changes.

Table 27-5: Recording Format

Fields	Description
Audio Encoding	<p>Defines one of the following coders:</p> <ul style="list-style-type: none"> ■ G.711Ulaw -Uncompressed storage ■ G.711Alaw -Uncompressed storage ■ G.729 -Compressed storage (default)

Fields	Description
	'Encryption' check box: Select this option to encrypt media files as they are recorded. Files are encrypted using AES 128- bit key encryption.
Video Encoding	Video recordings are by default saved in MP4/H.264 format (not configurable).
Audio for analytics	Defines one of the following coders: <ul style="list-style-type: none"> ■ PCM16 16 KHz -High quality optimized coder (default) ■ G.711 -Standard quality coder

Configuring Live Monitoring Location

The Live monitoring feature allows users to listen to calls in real time. When this feature is enabled for a site, Live monitoring media files are buffered to a playlist. The playlist and files are stored in the “Live Monitoring Location” which can be configured using this procedure. The live monitoring content is constantly refreshed by the SmartTAP 360° client and can be played back by the user by clicking the Live Monitor microphone button (see Determining User/Device Status).

➤ To configure Live Monitoring file location:

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

In this page, the following can be configured:

- **Scheme:** The protocol used for storing and retrieving live monitoring files. The following scheme is used:
 - **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 for the recording location (see [Adding Media Storage Recording Locations](#) on page 269).
- 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 27-12: 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 27-13: Modify Live Monitoring Location-Update Error

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

Modify Live Monitoring Location

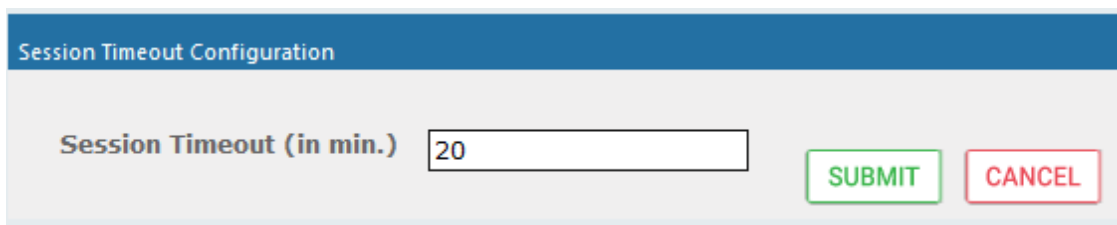
28 Configuring Web Session Timeout

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 28-1: Session Timeout



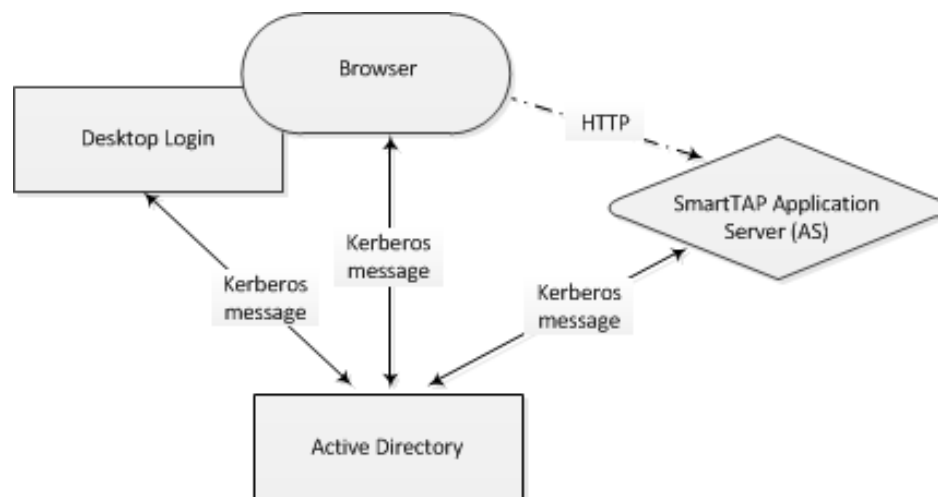
The image shows a web configuration screen titled "Session Timeout Configuration". It features a text input field labeled "Session Timeout (in min.)" with the value "20" entered. To the right of the input field are two buttons: a green "SUBMIT" button and a red "CANCEL" button.

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

29 Single Sign-On for SmartTAP 360°

This chapter describes the Single Sign-On functionality for SmartTAP 360°. Single Sign-On (SSO) simplifies the login process for domain users. The user logs into their machine using domain credentials and then attempts to access the SmartTAP 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° 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 Web interface and for quick access to different SmartTAP 360° pages.

Figure 29-1: Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Web Authentication Service



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

■ **Prerequisites:** LDAP configuration is optional if all Clients using SSO were manually added to the SmartTAP 360° database. If they were not manually added, then LDAP must be configured so that SmartTAP 360° can validate the user and find the user's Roles/Permissions (see [Configuring SSL](#) on page 315).

■ **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 29-1: Terms

Term	Description
{username}	New domain user required for SmartTAP 360° to authenticate through SSO. Referred to as the 'SSO User'. Use a different user for SSO and LDAP if possible, in order to simplify later steps and facilitate troubleshooting. In this Appendix, testUser is used.
{domain}	The complete name of the domain to be used for SSO, for example, myDomain.local.
{realm}	The security realm to be used for authenticating the SSO User. Can be different to the realm of the SmartTAP 360° server and should be the realm of the SSO User. The realm must be specified in capital letters. In the example of a single domain used in this Appendix, the realm is the same as {domain}: MYDOMAIN.LOCAL.
{kdc}	The fully qualified domain name (FQDN) of the Key Distribution Center (KDC) which must be the Active Directory server to be used to authenticate the SSO User (created in the next step). Example: ad.myDomain.local
{user password}	The password defined for the SSO User when created. In 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° server. Must be in the form {machine name}.{domain}. Example: SmartTAP 360°.myDomain.local. If a CNAME alias is used to map an unfriendly machine name to a friendlier one such as SmartTAP 360°, the original machine name must be used.
{principal}	Special string defining a service running on a host within a security realm, in this case, HTTP/{hostname}@{realm} Example: HTTP/SmartTAP 360°.myDomain.local@MYDOMAIN.LOCAL

Configuring Single Sign-on in SmartTAP Web Interface

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° server. When SSO is enabled, the administrator is authenticated in the background through Active Directory using the same domain credentials that were used to log into the machine. This bypasses the login page and immediately opens the Welcome page. Initially, SSO is disabled, so the usual login form must be used. Log in with any account with permissions such as the default administrative user admin to make system changes to SmartTAP 360°.



The SmartTAP 360° server must be added to the Domain.

➤ **To configure Single Sign-On:**


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

Figure 29-2: Single Sign-On

2. Configure the parameters described in the table below.

Table 29-2: SSO Configuration Parameters

Parameter	Description
Enable SSO	Select this option to enable Single Sign-On.
KDC	Key Distribution Center, which is probably located on the Active Directory server. Enter {kdc}. In the example shown in this Appendix, ad.myDomain.local is used.
Principal	The Service Principal Name mapped in the previous steps. Enter {principal}. Note: The principal name must include the security realm. HTTP/SmartTAP 360°.myDomain.local@MYDOMAIN.LOCAL is used in the example in this Appendix.
Password	The password set previously in Service Principal Name Mapping. Enter {user password}. testUserPassword is used in the example in this Appendix.

3. When you have completed the configuration click .
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 for other necessary steps to configure SSO.

Single Sign-On Client Browser Settings

After enabling SSO on SmartTAP 360°, 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](#) below
- [Enabling Firefox Browser with IWA](#) on page 301
- [Enabling Chrome Browser with IWA](#) on page 302

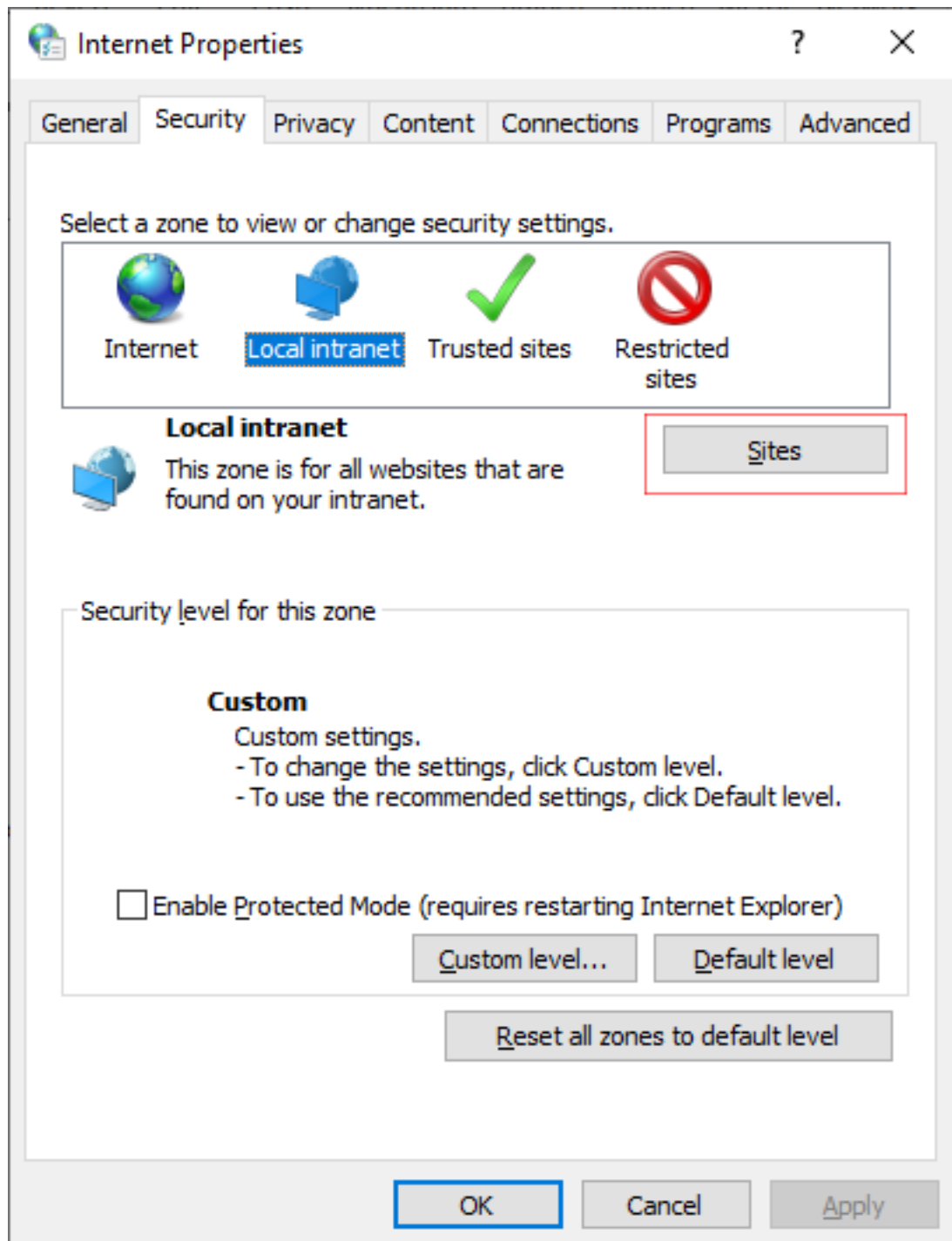
Enabling Microsoft Edge Browser with IWA

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:

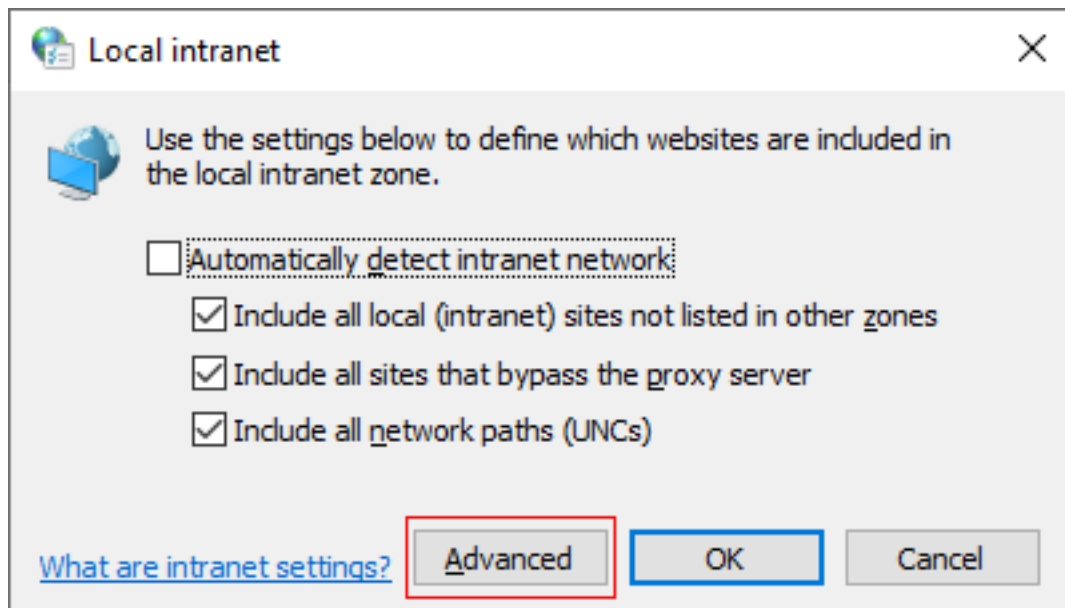
1. Open the Windows Settings and search **Internet Options**.

Figure 29-3: Internet Properties



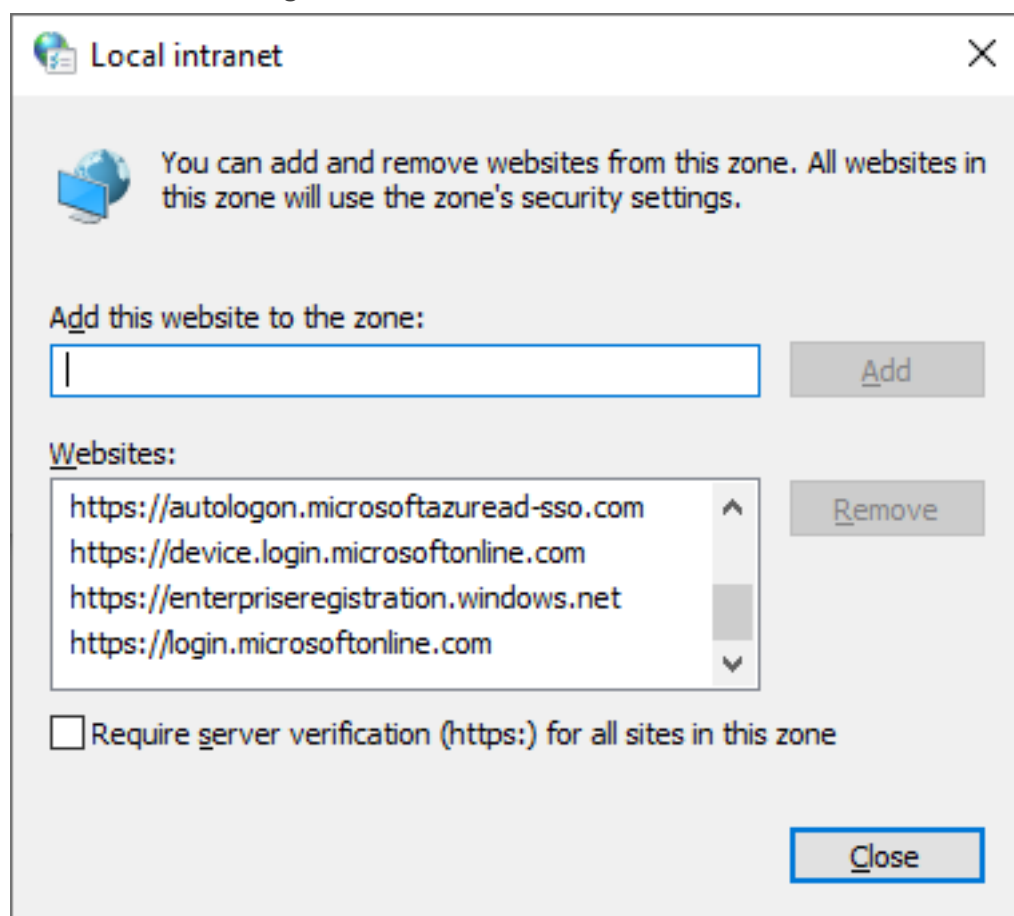
2. Click **Local intranet > Sites**.

Figure 29-4: Sites



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

Figure 29-5: Tenant URL



4. Click **Close**.

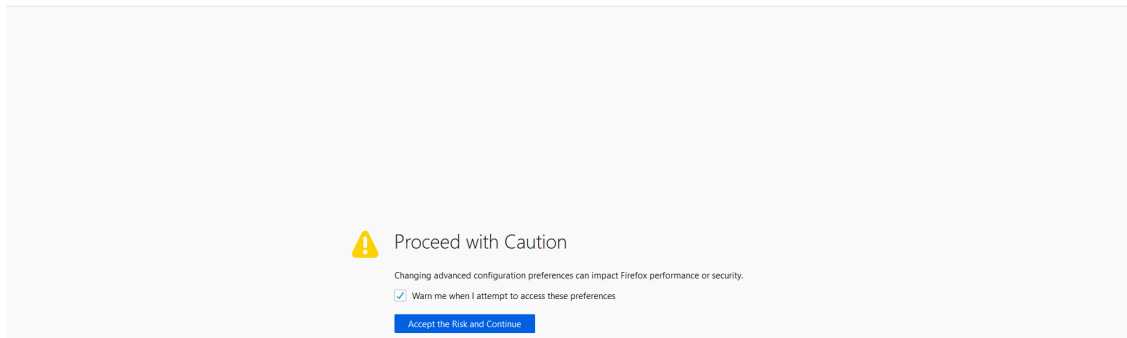
Enabling Firefox Browser with IWA

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

➤ To enable Firefox browsers with IWA:

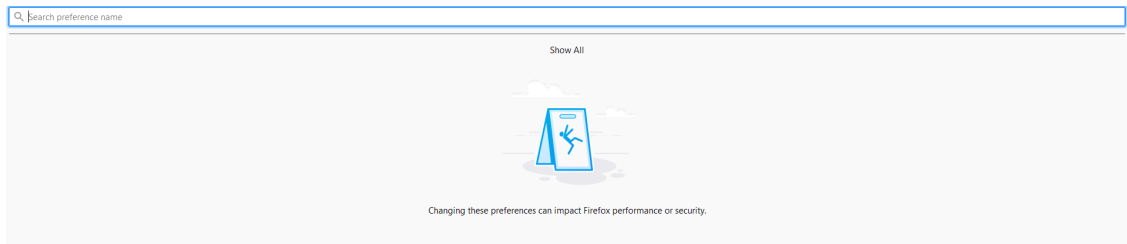
1. Open Firefox, enter the URL **about:config** and then press Enter; Firefox warns you're updating its internal settings.

Figure 29-6: 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 29-7: Firefox Negotiation Options



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

Figure 29-8: 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 29-9: Add SmartTAP 360° FQDN

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	Smarttap.myDomain.local
network.negotiate-auth.using-native-gsslib	true

network.negotiate-auth ☐ Boolean ☐ Number ☒ String

- Restart Firefox; SSO now functions on Firefox.



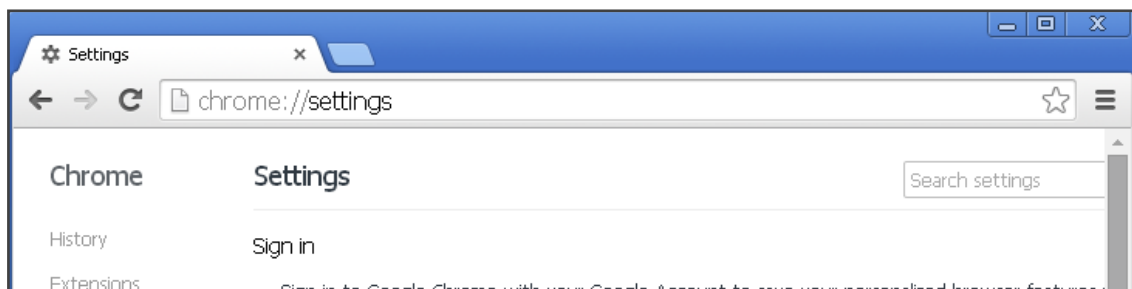
Additional changes may be required for Firefox. If SSO does not function immediately after these changes, see. [Troubleshooting Single Sign-On](#) on page 309

Enabling Chrome Browser with IWA

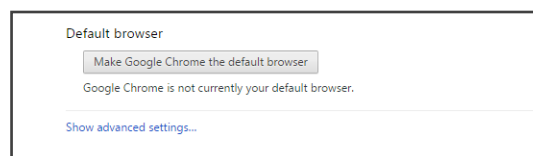
This section describes how to enable Chrome browsers with Integrated Windows Authentication (IWA) for Silent Authentication.

➤ To configure Chrome browser settings:

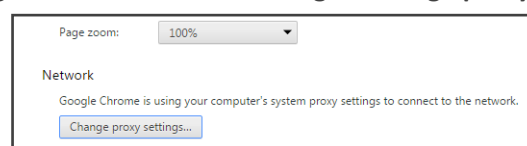
- Open the Chrome browser and click the menu icon located to the right of the address field, and then select **Settings**. Alternatively, browse to `chrome://settings`.

Figure 29-10: 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.

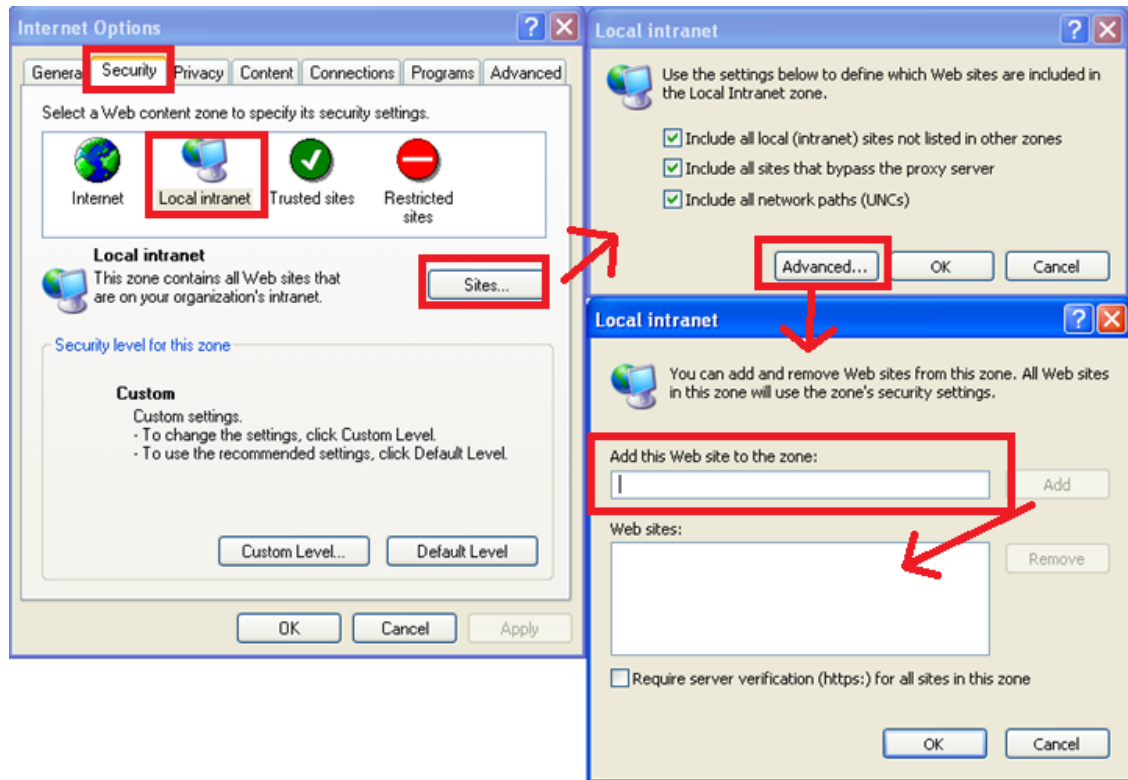
Figure 29-11: Google Chrome Browser Settings – Show advanced settings

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

Figure 29-12: Google Chrome Browser Settings – Change proxy settings

4. Select the **Security** tab > **Local Intranet zone** > **Sites** > **Advanced**.
5. Add the SmartTAP 360° FQDN to the local Intranet zone.
6. Close all Google Chrome windows and restart; SSO occurs.

Figure 29-13: Google Chrome Browser Settings – Adding a Web Site to the Zone



Single Sign-On Variables

■ Variable List:

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

{username} _____

{user password} _____

{domain} _____

{short domain} _____

{realm} _____

{hostname} _____

{kdc} _____

{principal} _____

■ Validate the Hostname to be Used for the Principal Name

A CNAME alias for the SmartTAP 360° server can cause problems when used as part of the Principal Name. A Client machine will request a Kerberos ticket for the FQDN using the

actual hostname, not the version using the CNAME. So the Principal to be used must contain the name that the Client will be requesting.

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

```
ping {hostname}
```

The command shell then prints out

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

If {ping destination name} is the same as {hostname}, then this is the correct hostname to use for the Principal. If different, then the correct hostname must be investigated further. Most likely, {ping destination name} is the correct one to use. However, SSO may have to be configured in SmartTAP 360° and Wireshark run in order to see which hostname the Client machine uses when requesting a ticket from Kerberos.

■ Windows KTPASS Command and Choice of User

Active Directory must then be commanded to map the HTTP service on the SmartTAP 360° server to the newly created user. The ktpass command included on Windows servers will be used. It must also be run on the Active Directory server.

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

ktpass most importantly creates the keytab for the Principal. SmartTAP 360° does not need this file to be exported. The Client obtains an encrypted version of the keytab and sends it to SmartTAP 360° as part of the authentication process.



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

Instead of entering the password, the domain administrator can use the -pass * option. The user is then prompted for the password. Although more secure, in some cases this changes the user's password within Active Directory. If this user is used by SmartTAP 360° for SSO only, this is acceptable. If the user is also used for LDAP, LDAP authentication will fail after the password is changed. Manually resetting the user's password in Active Directory corrects the LDAP authentication error but breaks the mapping performed by ktpass and therefore SSO fails.

The only way to use SSO and LDAP while also using the -pass * option is to use two separate users for SmartTAP 360° – one for SSO and one for LDAP. For simplicity, try to use two different users for LDAP and SSO to facilitate troubleshooting and configuration.

■ User Properties – Before and After Running ktpass

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

Figure 29-14: Before Running the ktpass Command

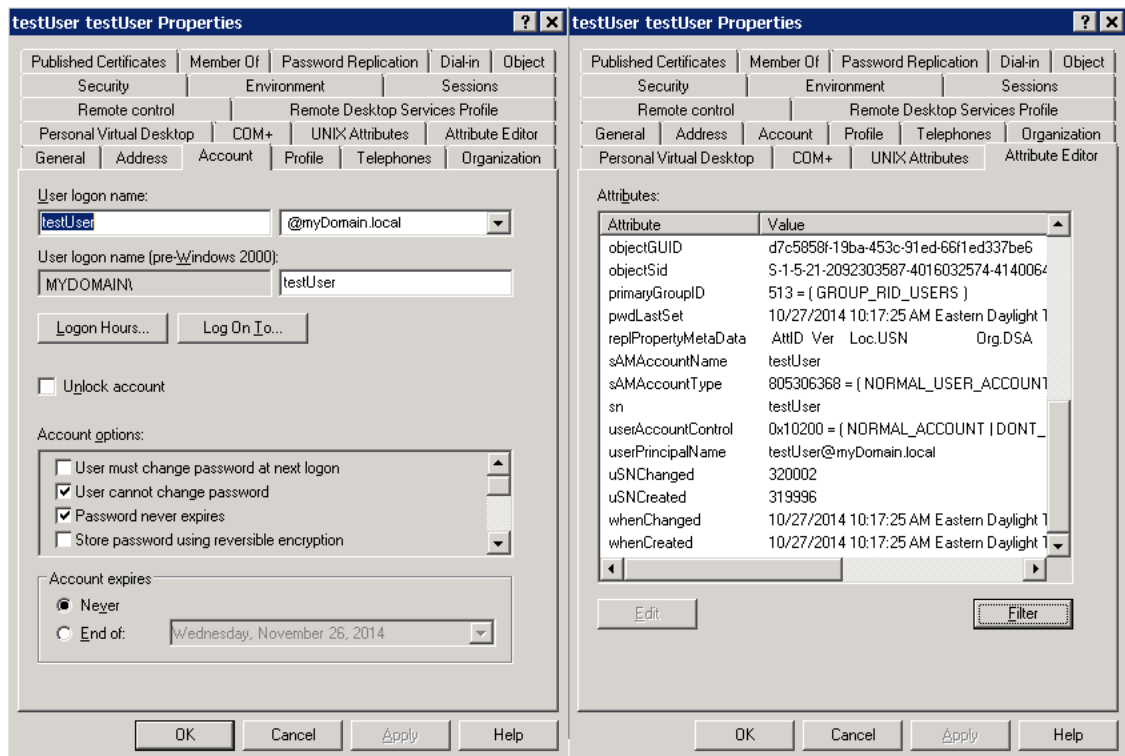


Figure 29-15: After Running the ktpass Command

The figure shows two screenshots of the 'testUser testUser Properties' dialog box in Windows. The left screenshot shows the 'General' tab with the following information:

- User logon name: HTTP/smarttap.myDomain.local @MYDOMAIN.LOCAL
- User logon name (pre-Windows 2000): MYDOMAIN\testUser
- Logon Hours... and Log On To... buttons
- Unblock account checkbox (unchecked)
- Account options:
 - User must change password at next logon (unchecked)
 - User cannot change password (checked)
 - Password never expires (checked)
 - Store password using reversible encryption (unchecked)
- Account expires:
 - Never (selected)
 - End of: Wednesday, November 26, 2014

The right screenshot shows the 'Attributes' tab with the following attributes:

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° Application Server to use for authenticating client's login attempts. The SSO User is only to be used within SmartTAP 360° and should not be used to log into any machine on the domain, including the SmartTAP 360° server. It is recommended to create this user and to select the options 'Password never expires' and 'The user cannot change password' as shown in the figure below. Assign the username a login ID of {username} and a password of {user password}.

Figure 29-16: Create a New Domain User

New Object - User

Create in: myDomain.local/Users

Password: [masked]

Confirm password: [masked]

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

■ Active Directory Commands - ktpass:

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

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



The Level of the Encryption Used: SmartTAP 360° supports encryption types as high as AES-128 though not all Windows Server OS versions support this level of encryption. It only depends on the OS version, not on the domain's Functional Level.

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

Example:

```
ktpass -princ HTTP/SmartTAP 360°.myDomain.local@MYDOMAIN.LOCAL -mapuser  
myDomain\testUser -pass testUserPassword -ptype KRB5_NT_PRINCIPAL -kvno 0 -  
crypto AES128-SHA1
```

When running flawlessly, the command outputs:

```
Targeting domain controller: <DC  
hostname>
```

```
Successfully mapped {principal} to  
{username}.
```

```
Key created.
```

The command may take a few minutes to propagate through the network. It's recommended to log out and then back in on any client machines that will attempt SSO, in order to speed up the process for laboratory testing. This ensures that the Client machine is not caching any Kerberos tickets that will be out of date after making changes to the User in Active Directory. If the Client machine used for testing has not previously accessed the SmartTAP 360° server, logging out is unnecessary.

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

■ Verify the User's Credentials

AudioCodes has observed cases in which the ktpass command changed the user's password even when explicitly defined in the ktpass command. To avoid confusion later, make sure the user's credentials are still correct. From the command prompt on either the SmartTAP 360° server or the Active Directory server, run the command:

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

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

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

valid. Other errors indicate that the user credentials are OK, but the command failed for other reasons.

Error 1326: Logon failure: unknown user name or bad password indicates that the credentials are incorrect. Make sure the username and password are correct. If this error persists it means the user's password must have been changed. If this fails to run and SmartTAP 360° is configured with the same password, then Single Sign-On will fail. Try resetting the password in Active Directory and re-running the ktpass command to make sure the password is correct. Repeat this test to validate that the user's credentials are still known before continuing.

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

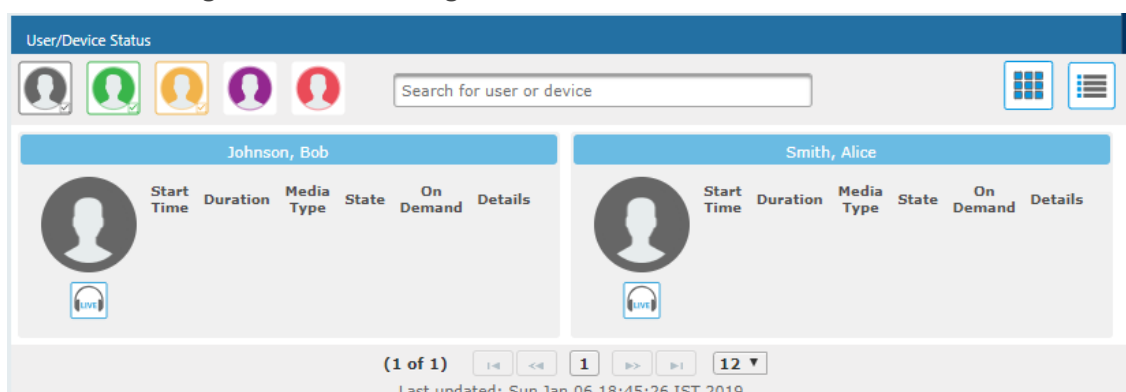
Testing Single Sign-On

After logging into the domain computer and configuring the browser to trust the SmartTAP 360° server as described in previous sections, you can browse to the SmartTAP Web server, preferably via the SmartTAP 360° server's FQDN. You may briefly see the Redirecting notification:

Redirecting

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

Figure 29-17: Browsing to the SmartTAP Web Server



If an error page is displayed, or if the normal login form for SmartTAP 360° is displayed, SSO has malfunctioned – see [Troubleshooting Single Sign-On](#) below.

Troubleshooting Single Sign-On

■ Frequently Asked Questions

When SSO is enabled, how can I log in as the default SmartTAP 360° administrative user?

SSO is enabled, so all login attempts will automatically attempt SSO as the domain user logged into the client machine. The SmartTAP 360° administrative user (default username = admin) will likely not be a user in Active Directory, so it cannot be used to log into the client machine and log in to SmartTAP 360° via SSO. The form login page of SmartTAP 360° must be accessed in order to log in as this user.

It is recommended that a domain user be given valid SmartTAP 360° permissions to make system changes so that the default SmartTAP 360° administrative user can be removed.

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

There are a few ways to do this:

- Browse to the SmartTAP 360° server using its IP address instead of the FQDN. SSO will not function this way, so the form page will be displayed. The IP address can be obtained by pinging the hostname from a command prompt.
- Access the SmartTAP 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° server hostname is not configured as an Intranet site), you may be able to access the form login page. See the next question.

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

When a client accesses the SmartTAP Web server, the server requests the client browser to negotiate authentication. If the browser can determine the credentials from the user's login, it will be used. However, if the browser does not trust the Website, or the user is not in the domain, the internet browser will often prompt the user for credentials, displaying a popup window which prompts for the client's domain credentials, not the SmartTAP 360° 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° 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 29-3: HTTP Error Codes

Error Code	Description
400 – Bad Request	Indicates that part of the HTTP Request is malformed. When using SmartTAP 360° for SSO, the likely cause is that the authentication header being sent by the client is too large. This can occur when the client has many authentication details to send. Simpler networks (such as a laboratory test domain) don't require much data for authentication. As of SmartTAP 360° Version 2.6, the default maximum header length is 8 KB, but instances in which 32 KB was required for authentication information have been observed. A system property must be added to the SmartTAP 360°.xml file for the SmartTAP 360° Application Server: <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° 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 access. Another cause is if SmartTAP 360° cannot determine the User Roles/Permissions for this user. Make sure the user performing SSO is part of the domain and that SmartTAP 360° can find this loginId through LDAP or in its own database. Make sure LDAP is configured correctly and can communicate with Active Directory.

■ SmartTAP 360° Application Server Errors

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

- **No Errors – Using Firefox browser**
 - ◆ The Firefox browser will by default just display the 401 Unauthorized error page until the configuration is changed to trust the SmartTAP 360° server though instances occur in which the Firefox browser does not attempt to authenticate

even when the SmartTAP 360° 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°.
- `Javax.security.auth.login.LoginException: Pre-authentication information was invalid (24)`
 - ◆ The likely cause of this error is that the SSO user's password does not match that configured in the SmartTAP 360° GUI.
 - ◆ Validate whether the user's password was changed or not - see Verify the User Credentials.
 - ◆ To resolve the error, reset the SSO user's password, re-enter this same password into the SmartTAP 360° GUI for the SSO credentials. You may also need to re-generate the keytab using the `ktpass` command.
- `Javax.security.auth.login.LoginException: Checksum failed`
 - ◆ Occurs when the Kerberos ticket obtained by the client is out of date. Most frequently, during SSO testing, when a client cached a Kerberos ticket for the first SSO login attempt and an attribute for the SSO user was then changed.

- ◆ To resolve this, log out on the client PC and then log back in; this immediately flushes the cache of Kerberos tickets and requires the cache to obtain a new ticket when trying to access the SmartTAP 360° server.
- Org.ietf.jgss.GSSException is thrown when authenticating with Kerberos server. Defective token detected (Mechanism level: GSSHeader did not find the right tag)
 - ◆ Indicates that the client machine did not send the correct authentication token to SmartTAP 360°. The most likely cause is that the client machine did not send any token at all.
 - ◆ Observed with a non-domain client machine accessing SmartTAP 360° from a Firefox browser, with trusted site configured.

■ Troubleshooting with More Detailed SmartTAP 360° Application Server Logging

If more detailed logging is required to troubleshoot these issues within the Application Server, configure the following loggers. Consult with AudioCodes technical support before making any changes to the SmartTAP 360° logging.

The loggers can be configured through the SmartTAP 360° Application Server Web interface - browse to <http://localhost:9990>. Note that this requires running the add_user.bat script to configure a user for accessing the Admin Console, or it can be configured in the SmartTAP 360°.xml configuration file - which requires a restart of the Application Server service.

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

■ Resetting the Configuration for Firefox Browser

In certain situations, it may be necessary to reset the configuration for the Firefox browser in order to use SSO with SmartTAP 360°. To do this, see the Mozilla guide at <https://support.mozilla.org/en-US/kb/reset-preferences-fix-problems>.





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

The following sections summarize the guide.

■ Refresh Firefox

This section instructs you how to refresh Firefox.





- a. Click the menu button , click help  and select Troubleshooting Information; the Troubleshooting Information tab opens.
- b. Click the Refresh Firefox button in the uppermost right corner of the Troubleshooting Information tab.

- c. When prompted to confirm, click the Refresh Firefox button again; Firefox closes to refresh itself. When finished, a window is displayed listing your imported information. Click Finish; Firefox reopens.
- d. If previously set, the 'Trusted URIs' configuration will be lost. Follow the steps in the Firefox Browser configuration to assign the SmartTAP 360° server as a trusted server.
- e. Attempt SSO again; if SSO still doesn't work, delete Firefox preference files as shown in the next section.

■ Delete Firefox Preference Files

This section instructs you how to delete Firefox preference files.

➤ To delete Firefox preference files:

- a. Click the menu button , click help  and select Troubleshooting Information; the Troubleshooting Information tab opens.
- b. Under the Application Basics section, click Show Folder; a window opens displaying your profile files.
- c. Click the menu button  and then click Exit .
- d. Locate and delete the file prefs.js (or rename it, for example, to prefs.jsOLD, to keep the old file as a backup. If you find more than one, a prefs.js.moztmp file or a user.js file, delete (or rename) these as well.
- e. Close the profile folder and open Firefox.
- f. If previously set, the 'Trusted URIs' configuration will be lost. Follow the steps in the Firefox Browser configuration to assign the SmartTAP 360° server as a trusted server.
- g. Attempt SSO again; if SSO still does not work, uninstall and reinstall Firefox as shown in the next section.

■ Uninstall & Reinstall Firefox

- a. Uninstall Firefox through the Windows Control Panel.
- b. Make sure all Firefox data stored in the following locations is removed:
C:\Users\<user>\AppData\Local\Mozilla\
C:\Users\<user>\AppData\Roaming\Mozilla\
[Optional] Reboot the machine.
- c. Reinstall the latest version of Firefox. It may be a good idea to download the latest version from Mozilla again, to be safe.
- d. After the installation, follow the steps in the Firefox Browser configuration to assign the SmartTAP 360° server as a trusted server.
- e. Attempt SSO again.

30 Configuring SSL

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

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

1. On the server that stores the certificate authority (typically, the domain's active directory server), run from a command prompt:

```
certutil -ca.cert
client.crt
```

2. Copy client.crt from the Active Directory server to the SmartTAP 360° server, copy from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----.

Figure 30-1: Copy Client Certificate From Active Directory

```

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

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

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>certutil -ca.cert client.crt
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIQGo4xz2d6IotAfjh/bwwxvzANBgkqhkiG9w0BAQUFADBK
MRUwEwYKCZImiZPyLGBGRYFbG9jYVWwFzAUBgoJkiaJk/IsZAEZFgdxyWxhYkUFLU
MRgwFgYDUQDEw9xYVWxhYkUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLU
MDAxMDAwMTI5WjBKMRUwEwYKCZImiZPyLGBGRYFbG9jYVWwFzAUBgoJkiaJk/Is
ZAEZFgdxyWxhYkUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLUFLU
S1b3DQEBAAQAA1BDwAwggEKAoIBAQC2dHX0Cdu4kGZX/drEv9fU+YHUtqidiDi9
A9lxeRlG8pMCnOUBUPg/+rg77zI9rMMYzvoGaw5uLImx+2oikrcY+zFpZd+gGJw2
r46YwpUwAP5jd3bqq4kbwDpxv8mSiXfw4CDYTD0oN4Gute+38mie.jzWd25vPY5qs
ki/ihUKQteAlip1FFfLY+zLmKR71yvLt5vXveZiJp8Q8DnZWw7ARQ1TtsJulQ+d3
UbfN7/c1c8a4hsUxFTp4bTSq8Uf6cv9HSoj9QD8GtFTLqc5+We6So/JS6HtK5Fr
ZTKKoTYGJD1e1jXZBj0cdOBxPfha8jyCSWCYA40S56bJQMUUC/AtAgMBAAgJUTBP
MAsGA1UdDwQEAwIBhjaPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRrh4ofriwZM
GK6kLidd8PRjsoc2nDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAAO
AQEASusysykyTuZOi+9N1MOfR+QFt0RWbjaw2goWCMUxT/Xl1Slsx2bPHIUYuJd1
M4t9b/FJWu16FU+wpWzyjK40Lp8uIPmyoBHTw6vTXnJ3wnC9fb6eDSjL1jx6dOL
rQh7XShPhNI0+zDJZ0B2ggLHUPe1T3jK3zFFi02Sjlg5wqlbA8mDdcw0pkbGqGIB
ncSZtUDhNFug500sG1QksmDUiRoXlkZ9bWau+f2zS8ESGeIfCEXX1BdfxGBfIbEC
zwUkz9MJ0/mcXcXJ0dGZ45MdLedt0maDgZhExytpFNeDWN0YpQJWhrdExsxYsfT
sZkBB6trtS7vptX72kk+hwAB/w==
-----END CERTIFICATE-----

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

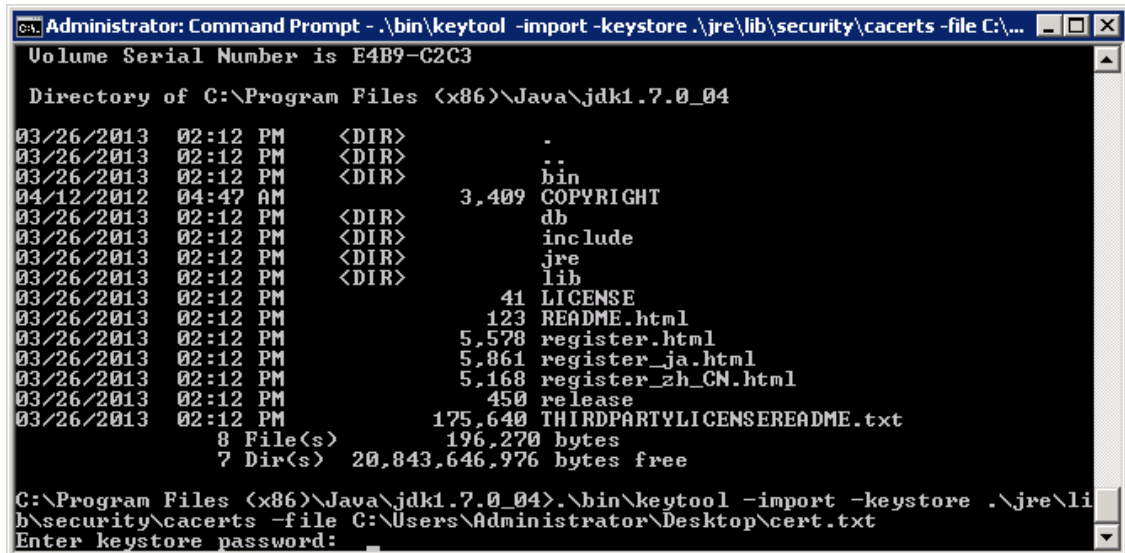
C:\Users\Administrator>

```

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

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

Figure 30-2: Copy Client Certificate to SmartTAP 360° Machine



- 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° 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 **SUBMIT** to continue (see the figure below).

Figure 30-3: LDAP SSL Configuration

31 Adding an LDAP Configuration

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



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

➤ **To add an LDAP configuration:**

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

2. Configure fields according to the table below.


3. Click  to apply changes.

Table 31-1: LDAP 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

Field	Description
	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 page 315.

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

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

➤ **To configure an LDAP connection from SmartTAP 360°:**

1. Enter the IP or Name of the domain controller in the 'Host' field.
2. Enter distinguishedName in the 'Principal' field.
3. Enter the Port number in the 'Port' field.
4. Provide the password for the distinguishedName account used.
5. Check 'Use SSL' if required (see [Configuring SSL](#) on page 315).
6. Click  to apply changes.

32 LDAP Active Directory Mapping

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 324)
- Security Group Mappings ([Configuring Security Group Mappings](#) on page 327)



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:

1. Open the View/Modify LDAP Configuration page (**System** tab > **LDAP** folder > **View/Modify LDAP Configuration**).

Figure 32-1: Modify LDAP Configuration

Host	Port	Modify	Delete
172.17.127.120	389		

2. Select the required LDAP Configuration that was configured in [Adding an LDAP Configuration](#) on page 317 and then click

[Configuration](#)

Figure 32-2: User Mappings

Modify LDAP Configuration

Host: 172.17.127.120 Principal: qalab\admin Use SSL: ☐
 Port: 389 Password:

User Mappings

Base Context:
 Mapping Filter:
 First Name:
 Last Name:
 Login:
 Email:
 Alias:
 extension:
 username:
☒ One Level ☐ Subtree

Base DN	Filter	Search Scope	Modify Mapping	Delete
CN=Users,DC=qa,DC=lab	(s(objectClass=user))	ONE_LEVEL		

Group Mappings

Security Group Mappings

3. Click to modify the User Mapping. The current mapping settings are displayed.

Figure 32-3: Modify LDAP Configuration

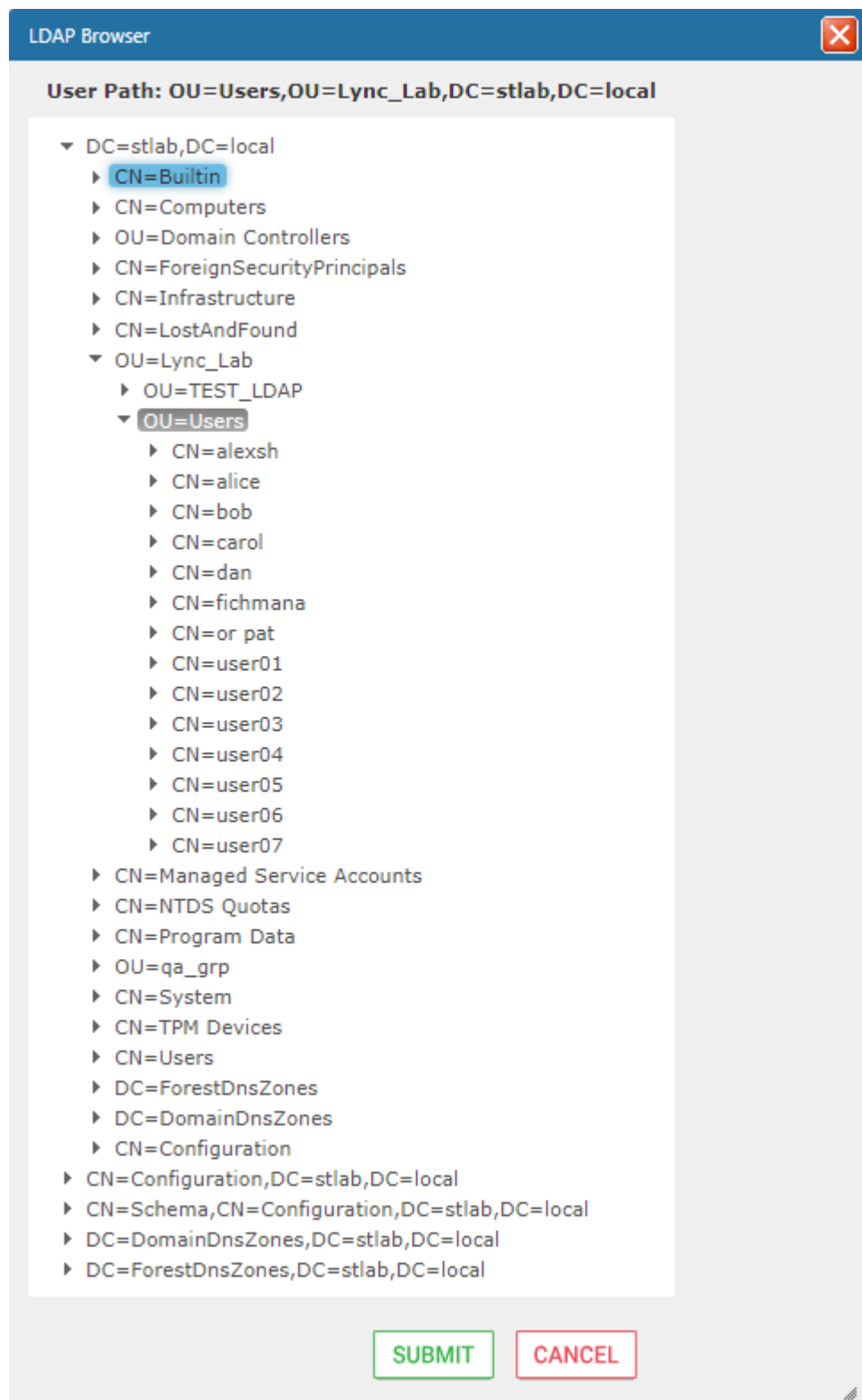
4. Configure fields according to the table below.

Table 32-1: 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

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

Figure 32-4: LDAP Browser



8. Navigate to the appropriate 'User Path' and then click SUBMIT.
9. Use filtering if you prefer not to add all users.

➤ **To add a filter:**




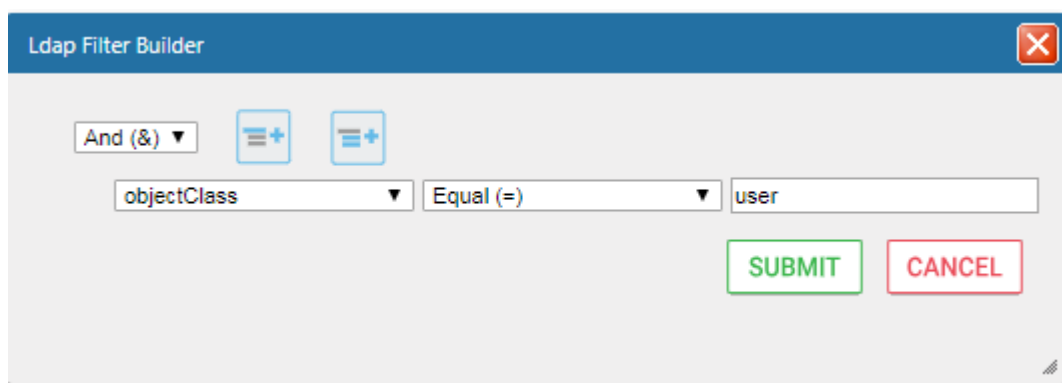
1. Select the **Create Filter** button.
2. Select the appropriate Conditional Operator (And, Or, Not)
3. Select the appropriate Attribute
4. Select the appropriate Equality Operator (>=, =, ~=, <=)
5. Specify value = (objectClass = user) recommended
6. Click  to apply changes.
7. Click the  icon to add 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 32-5: 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° Attributes, they will appear in the list of user attributes as well.
 - Those attributes that were created with 'Network Mapping' defined will be used to trigger recording.
 - 'Ext' and 'SIP URI' in the image above are examples of SmartTAP 360° User attributes added for recording purposes.
10. Map SmartTAP 360° attributes to appropriate AD user attributes.

Figure 32-6: 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 32-7: 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="Edit"/>	<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 32-8: 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	erib			
Analytics	Broker	tanial.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 the View/Modify LDAP Configuration page (**System** tab > **LDAP** folder > **View/Modify LDAP Configuration**).

Figure 32-9: Modify LDAP Configuration

Host	Port	Modify	Delete
172.17.127.120	389		

2. Select the required LDAP Configuration that was configured in [Adding an LDAP Configuration](#) on page 317 and then click

Figure 32-10: Modify LDAP Configuration

Host: 172.17.127.120, Port: 389, Principal: qalab\admin, Password: [empty], Use SSL: ☐

USER MAPPINGS

Base Context: [empty] Browse
 Mapping Filter: [empty] Create Filter
 First Name: Choose One
 Last Name: Choose One
 Login: Choose One
 Email: Choose One
 Alias: Choose One
 extension: Choose One
 username: Choose One
☒ One Level ☐ Subtree

Base DN	Filter	Search Scope	Modify Mapping	Delete
① CN=Users,DC=qa,DC=lab	(&(objectClass=user))	ONE_LEVEL		

GROUP MAPPINGS

Security Group Mappings

3. Select the **Group Mappings** tab.

Figure 32-11: Group Mappings



GROUP MAPPINGS

Base Context: [empty] Browse
 Mapping Filter: [empty] Create Filter
 Name: Choose One
 Description: Choose One
 Members: Choose One
☒ One Level ☐ Subtree

4. Configure fields according to the table below.

Table 32-2: Group Mappings Field Descriptions

Field	Description
Group Mappings	■ Group Base Context (LDAP path for groups)
	■ Group Filter (Create / Manage Group filter)
	■ Name (LDAP Attribute that maps to the group name)
	■ Description (LDAP Attribute that maps to the group description)

Field	Description
	<ul style="list-style-type: none"> 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. <p>  = expand screen  = shrink screen </p>

5. Enter the Group Mappings Information in the 'Group Mappings' screen (i.e. (Groups,DC=qalabEE,DC=local)

6. Navigate to appropriate 'Group Path' and then click .

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

➤ **To add a Group Filter:**


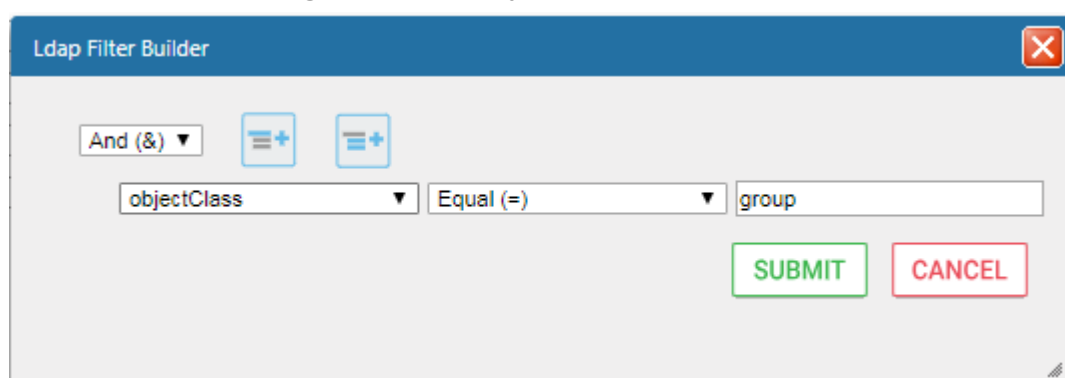



1. Select the appropriate Conditional Operator (And, Or, Not).
2. Select the appropriate Attribute.
3. Select the appropriate Equality Operator (>=, =, ~=, <=).
4. Specify a value.
5. Click  to apply changes.

Figure 32-12: 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.

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

Figure 32-13: Group Filtering Screen




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

Figure 32-14: 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. Open the View/Modify Groups page to view the mapped groups.

Configuring Security Group Mappings

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



By default, new security profiles are not granted SmartTAP 360° permissions, permissions must be configured in the Security Profiles screen once the security profile has been mapped.

➤ To configure Security Group Mappings:

1. Open the View/Modify LDAP Configuration page (**System** tab > **LDAP** folder > **View/Modify LDAP Configuration**).

Figure 32-15: Modify LDAP Configuration

Host	Port	Modify	Delete
172.17.127.120	389		


2. Select the required LDAP Configuration that was configured in [Adding an LDAP Configuration](#) on page 317 and then click .

Figure 32-16: Modify LDAP Configuration


3. Select the **Security Group Mappings** tab.

Figure 32-17: Security Group Mappings

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

Table 32-3: Security Group Mapping – Field Descriptions

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

Field	Description
	child nodes in the LDAP directory tree.
	Expand or Shrink screen

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

➤ **To add a Security Group Filter:**


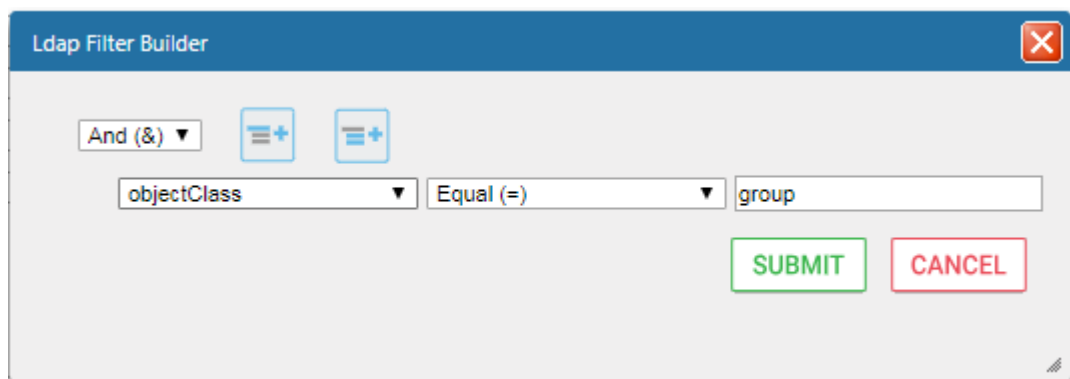
1. Select the appropriate Conditional Operator (And, Or, Not).
2. Select the appropriate Attribute.
3. Select the appropriate Equality Operator (>=, =, ~=, <=).
4. Specify a value.
5. Click  to apply changes.

Figure 32-18: Security Group Filter






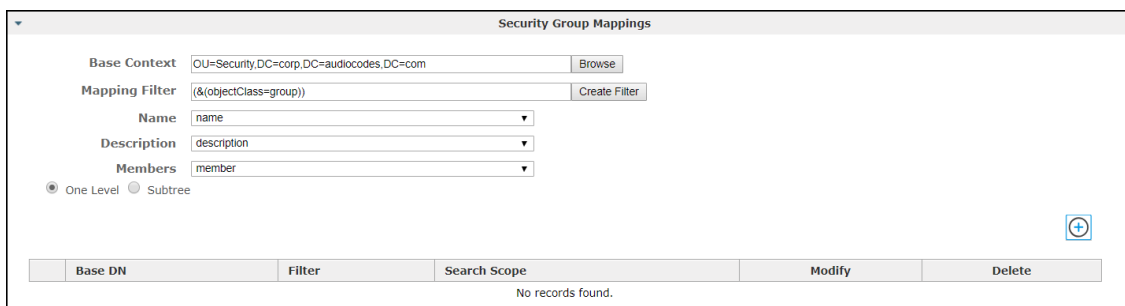
6. Click the  icon to add an additional filter condition and repeat above filter steps
7. Click the  icon to add a new Sub filter and repeat above filter steps
8. Click  to apply changes.

Figure 32-19: Security Group Filtering Screen



9. Click  to apply changes.

Figure 32-20: Security Group Configured

Security Group Mappings

Base Context Browse

Mapping Filter Create 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 add additional Security Group Mappings.
11. Open the View/Modify Security Profiles page to view the mapped groups and configure the required permissions (see [Configure Permissions in a Security Profile](#) on page 37).

33 Microsoft Teams Integration

Microsoft Teams is integrated automatically using the TerraSmartTAP for Microsoft Teams Deployment script which executes most of the required configuration. The table below summarizes the configuration actions executed by the Deployment scripts.

Table 33-1: Microsoft Teams Deployment

Description	Executed by Deployment Scripts	Reference
Registers daemon client application in Azure Active Directory on behalf of SmartTAP 360° (aad-app).	☑	Configure Client Secret for Role-based Access (aad-app) on page 333
Configures aad-app permissions for user and group mapping and for accessing Azure Blob statistics.	Configured automatically except for role-based permissions for accessing Azure Blob statistics.	Add Permissions for Role-based Access (aad-app) on page 336
Configures OpenID Connect Token (OIDC) Client Configuration used for authentication between the SmartTAP server, Bot and Remote Transfer Service (RTS).	☑	Update OpenID Connect Token (OIDC) Client Configuration on page 337
Configures auth-app permissions for authentication between the SmartTAP server, Bot and Remote Transfer Service (RTS) using the OpenID Token mechanism.	The SmartTAP OpenID Connect connection registration "auth-app" is applied for backward compatibility for customers deploying versions prior to Version 5.6. For Version 5.6 and later, these permissions are configured in the aad-app (see above).	Setup SmartTAP OpenID Connect Token Automatically (auth-app) on page 338
Creates default AudioCodes Active Directory mapping entry.	☑	Verify Active Directory Providers Configuration on page 340
Other Mapping: ■ Media Location	✕	Configure AAD Mapping Profiles

Description	Executed by Deployment Scripts	Reference
Profile Mapping <ul style="list-style-type: none"> ■ User and Group Mapping ■ Retention Policy Mapping ■ Recording Profile Mapping ■ Security Profile Mapping ■ Analytics Mapping 		on page 341
Microsoft 365 Sign-in setup	Automatically configured except for assigning Security Profile to M365 user.	Setup Microsoft 365 User Sign-in Authentication on page 378
Integrate Teams Personal app	Automatically configured except for uploading of Manifest file to customer's Teams admin center.	Integrate SmartTAP Personal App in Teams on page 391
Create Microsoft Teams Compliance Recording Policy for allowing recording of users belonging to Azure defined group.	Automatically configured using complianceRec.ps1 script. User must create group on Azure and add members to allow recording. <div>  Configuration in the SmartTAP Web is not required for this setup. </div>	Enable Users with Compliance Recording on page 408

Managing Access to Microsoft 365

The TerraSmartTAP deployment script creates the "aad-app" registration for accessing the customers' Microsoft 365 platform. A secure authenticated connection is established using OpenID Connect Token (OIDC). Customers using AudioCodes Azure subscription must provide consent for this app to access their Microsoft 365 platform (see Customer Consent for Azure Active Directory (aad-app)).

In addition to the automatic TerraSmartTAP configuration, manual configuration is required in both Azure and the SmartTAP Web for accessing Azure Blob storage statistics and for configuring user mapping profiles as detailed in the following procedures:

- [Configure Client Secret for Role-based Access \(aad-app\)](#) below
- [Add Permissions for Role-based Access \(aad-app\)](#) on page 336
- [Update OpenID Connect Token \(OIDC\) Client Configuration](#) on page 337
- [Configure AAD Mapping Profiles](#) on page 341



For more information on OIDC, refer to <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow>.

Configure Client Secret for Role-based Access (aad-app)

The aad-app registration is configured by the TerraSmart script with the following permissions:

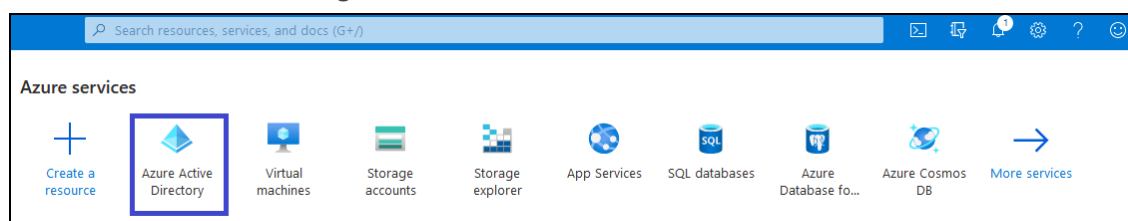
- Read users and groups of your AAD and map them to users and associated SmartTAP policies and profiles.
- Authenticate between the SmartTAP server, Bot and Remote Transfer Service (RTS) using the OpenID Token mechanism. The following permissions are required:
 - GroupMember.Read.All – Read all group memberships (Application)
 - User.Read.All – Read all users' full profiles
- Role-based access control for retrieving Azure Blob Storage statistics. The following roles are required:
 - Teams Bot
 - Remote Transfer Service
 - Call Delivery Live

You must **configure** a Client secret for **Role-based access** control for retrieving Azure Blob Storage statistics.

➤ Do the following:

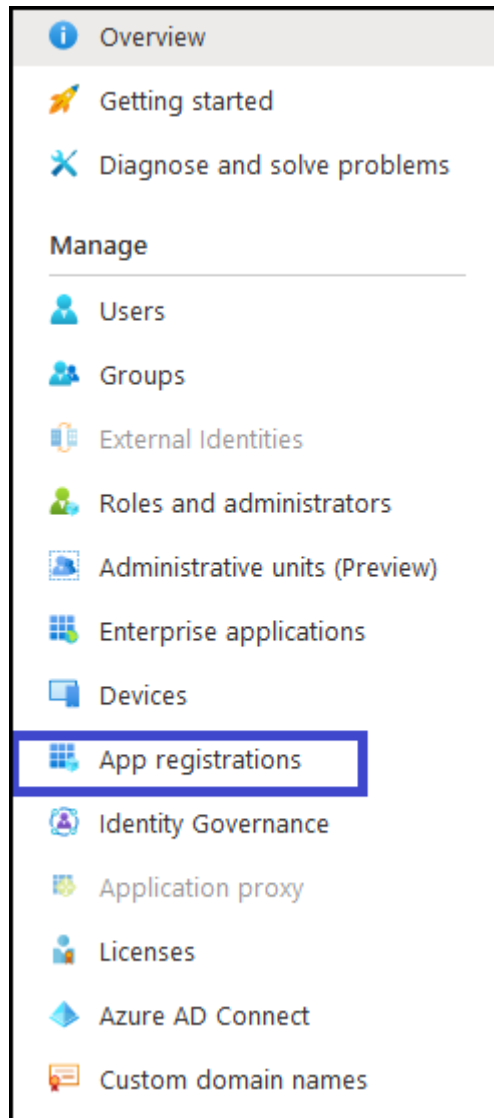
1. Login to the Microsoft Azure portal (<https://portal.azure.com/>).

Figure 33-1: Azure Services



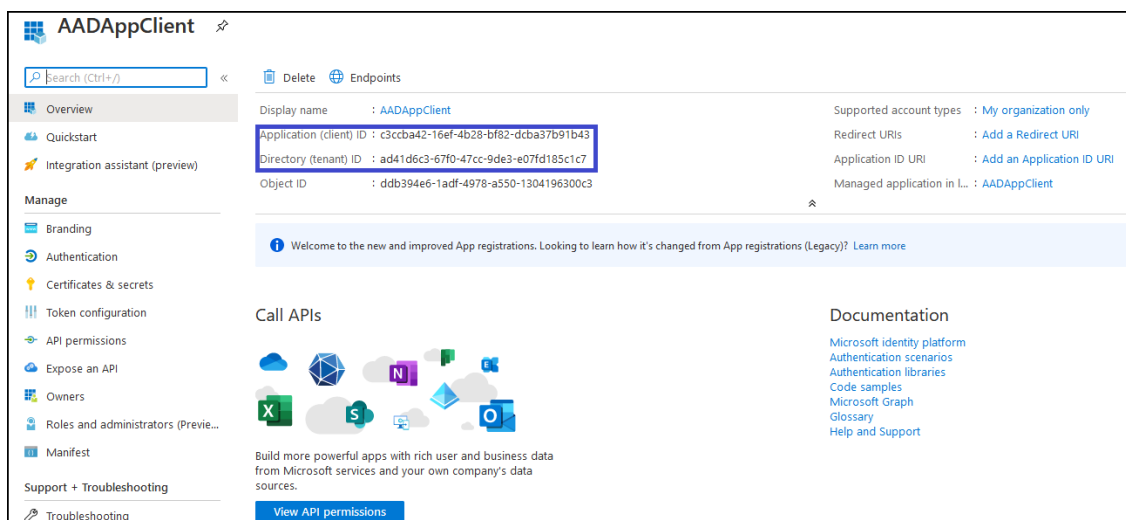
2. Click **Azure Active Directory**.

Figure 33-2: Application Registration



3. Open the aad-app registration.

Figure 33-3: AADAppClient



4. In the Navigation pane, select **Certificates & secrets**.

The screenshot shows the Microsoft Azure portal interface. The left-hand navigation pane is expanded, and 'Certificates & secrets' is selected under the 'Manage' section. The main content area displays the 'Client secrets (1)' tab. A table lists the existing client secret with the following details:

Description	Expires	Value	Secret ID
No description	1/1/2030	K95*****	0f4231bf-a164-4f78-aff2-dffa07fa4

Below the table, there is a '+ New client secret' button. A tooltip message states: 'Application registration certificates, secrets and federated credentials can be found in the tabs below.'

5. Click **+ New client secret**.

Figure 33-4: Add a Client Secret

The screenshot shows the 'Add a client secret' dialog box. It has two main fields: 'Description' and 'Expires'. The 'Expires' field is currently set to 'Recommended: 6 months'. A dropdown menu is open, showing the following options: 'Recommended: 6 months', '3 months', '12 months', '18 months', '24 months', and 'Custom'.



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 33-5: New Client Secret

The screenshot shows the 'Client secrets' page. A '+ New client secret' button is visible. Below it, a table displays the newly generated client secret:

Description	Expires	Value
AAD App Client Secret	7/2/2021	s07y53pN-V~jmW9Vyn260eNO.0_L7tlc_6

The 'Value' column contains the newly generated client secret, which is highlighted with a blue selection box.

6. Add client secret and copy value for Client Configuration (see [Verify Active Directory Providers Configuration](#) on page 340).

Add Permissions for Role-based Access (aad-app)

The aad-app deployment script configures the following permissions:

- GroupMember.Read.All – Read all group memberships (Application)
- User.Read.All – Read all users' full profiles (Application)



The Tenant's Office 365 administrator role is required to run the consent link.

You must **manually** configure the following permissions for Role-based access for Azure Blob Storage statistics:

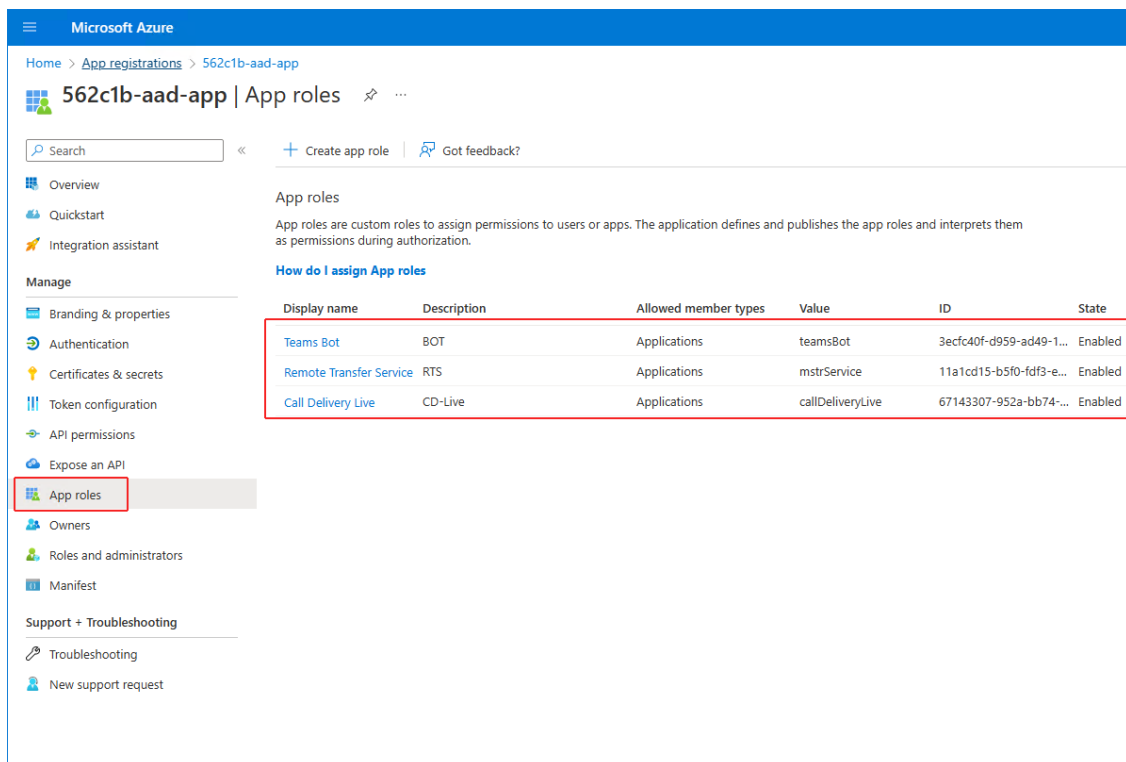
- Register web API and expose it through scopes to authorized users and client apps that access your API.
- Define roles for Teams Bot, Remote Transfer Service, Call Delivery Live.

➤ Do the following:

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

The screenshot shows the Microsoft Azure portal interface. The navigation pane on the left is expanded, and 'Expose an API' is selected. The main content area shows the configuration for the application '562c1b-aad-app'. The 'Application ID URI' is set to 'api://562c1b.smarttap.finebak.com/smarttap'. Below this, there are sections for 'Scopes defined by this API', 'Authorized client applications', and 'App roles'. The 'Scopes' section is currently empty, showing 'No scopes have been defined'. The 'Authorized client applications' section is also empty, showing 'No client applications have been authorized'. The 'App roles' section is not visible in the screenshot.

2. Enter the Application ID URI to expose.
3. In the Navigation pane, select **App roles**.



Microsoft Azure

Home > App registrations > 562c1b-aad-app

562c1b-aad-app | App roles

Search

+ Create app role | Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

[How do I assign App roles](#)

Display name	Description	Allowed member types	Value	ID	State
Teams Bot	BOT	Applications	teamsBot	3ecfc40f-d959-ad49-1...	Enabled
Remote Transfer Service	RTS	Applications	mstrService	11a1cd15-b5f0-fdf3-e...	Enabled
Call Delivery Live	CD-Live	Applications	callDeliveryLive	67143307-952a-bb74-...	Enabled

4. Define the following App roles:

- Teams Bot
- Remote Transfer Service
- Call Delivery Live

Update OpenID Connect Token (OIDC) Client Configuration

OpenID Connect Token (OIDC) Client Configuration is used for authentication between the SmartTAP server, Bot and Remote Transfer Service (RTS). SmartTAP 360° uses the Client Credential Flow to authenticate itself and access hosted resources, such as Users and Groups from Azure Active Directory.



This configuration is created **automatically** by the **Deployment script**; however, you must manually update the Client Secret generated in [Configure Client Secret for Role-based Access \(aad-app\)](#) on page 333.

➤ To update the client secret:

1. Login to the SmartTAP Web with a user that has "sysAdmin" role.
2. Open the Add/Modify OpenID Connect Token (OIDC) Client Configuration screen (**System** menu > **WEB** folder > **OpenID Connect Token**).

Add/Modify OpenID Connect Token (OIDC) Client Configuration

Add/Modify OpenID Connect Token (OIDC) Client Configuration

Hosted (Tenant) ID

Application (Client) ID

Client Secret

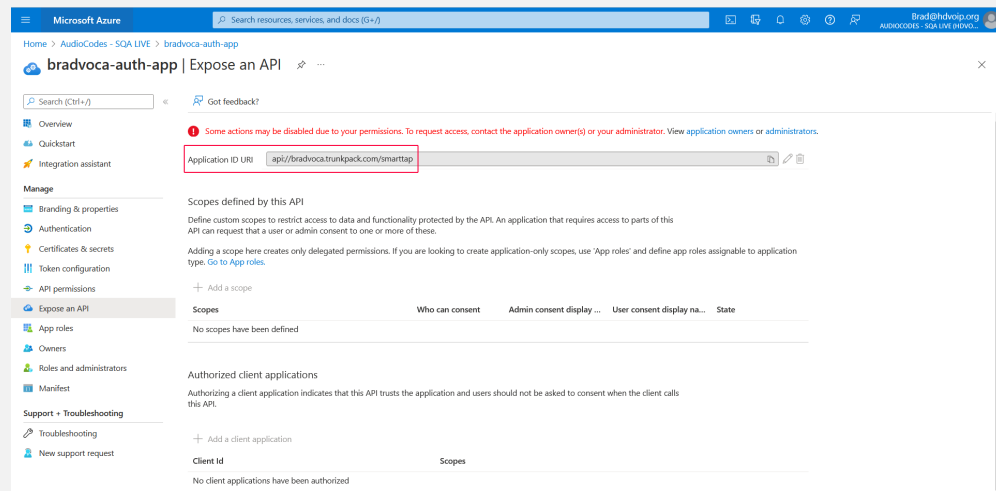
Resource ID

SUBMIT

3. Configure the Client Secret and then click **SUBMIT**.



In previous versions, the Redirect URI field was used instead of the Resource ID field. For customers upgrading from the previous version, this field is supported for Backward compatibility.



Setup SmartTAP OpenID Connect Token Automatically (auth-app)

The SmartTAP OpenID Connect connection registration "auth-app" is applied for backward compatibility for customers deploying versions prior to Version 5.6 as described in the note below.



The **auth-app** registration applies to SmartTAP versions 5.3, 5.4, 5.5 and upgrade to version 5.6. For a clean installation of version 5.6 and later versions, see Setup Azure Active Directory (aad-app)

➤ **To view the auth-app:**

1. Login to the Azure portal for the hosting or customer tenant.
2. In the Active Directory Navigation pane, select **App Registrations** and then select the **auth-app**. For example, "Bradvoca-auth-app".

Figure 33-6: auth-app

The figure consists of two screenshots from the Microsoft Azure portal.

Top Screenshot: App Registrations Overview

The top screenshot shows the 'App registrations' page in the Azure portal. The left navigation pane is open, showing 'App registrations' selected. The main content area displays a list of 20 applications found. The 'bradvoca-auth-app' is highlighted in the list.

Display name	Application (client) ID	Created on	Certificates & secrets
ARM_Terraform	30a41dca-f008-4b28-95a3-78ee29d91bf0	5/9/2022	Current
bradvoca-aad-app	6f8e1b35-2b94-4205-a34a-29d94a344894	6/14/2022	Current
bradvoca-auth-app	4e68065c-7e9c-4bb9-bd96-beae7a8f13cd	6/14/2022	-
bradvoca-calls-app	cb1e2c5-031e-41c0-8551-8739421b2a	6/14/2022	Current
bradvoca-login-app	810e8eb2-a1df-4f0e-94a8-36654e5a92d6	6/14/2022	Current
bradvoca-rtts-app	abf06f46-3145-413e-a2b6-8064a17d658f	6/14/2022	Current
changeNotificationSampleApplication	463ca8be-4c5f-44ce-8309-b1c9376aa714	7/15/2020	Current
Costi	8658d577-45d7-47a4-9425-53e7efca5295	1/17/2022	Current
DNS_Client_Provisioning	bd2e21ca-bd43-49d3-a9c1-ad0519c14e7d	10/13/2021	Current
hdvoporg-LTC-Smartap-213a96df-89c2-4bf3-9840-e99ea20ebac1	cd5d77b-5e9d-4e8c-ad96-5b074adac47e	5/11/2022	Current
LogAnalyticsMon	cc24299b-5f53-4d53-a370-707b8e0ea905	4/20/2022	Current
OV_L_DEV	bd930812-07e-4d29-ba14-640ee01ec219	10/31/2021	Current
OV_L_Rivka	b2455cb6-58db-4308-92c2-68dc368bd526	7/6/2021	Current

Bottom Screenshot: bradvoca-auth-app Overview

The bottom screenshot shows the 'Overview' page for the 'bradvoca-auth-app'. The left navigation pane is open, showing 'Overview' selected. The main content area displays the app's details.

Essentials

- Display name: bradvoca-auth-app
- Application (client) ID: 4e68065c-7e9c-4bb9-bd96-beae7a8f13cd
- Object ID: 1260f144-1952-4ec5-a7c0-b7a5c7ef2408
- Directory (tenant) ID: 6a217d07-8f6d-43da-bcd5-2cd8bdbe3b17
- Supported account types: Multiple organizations

Client credentials

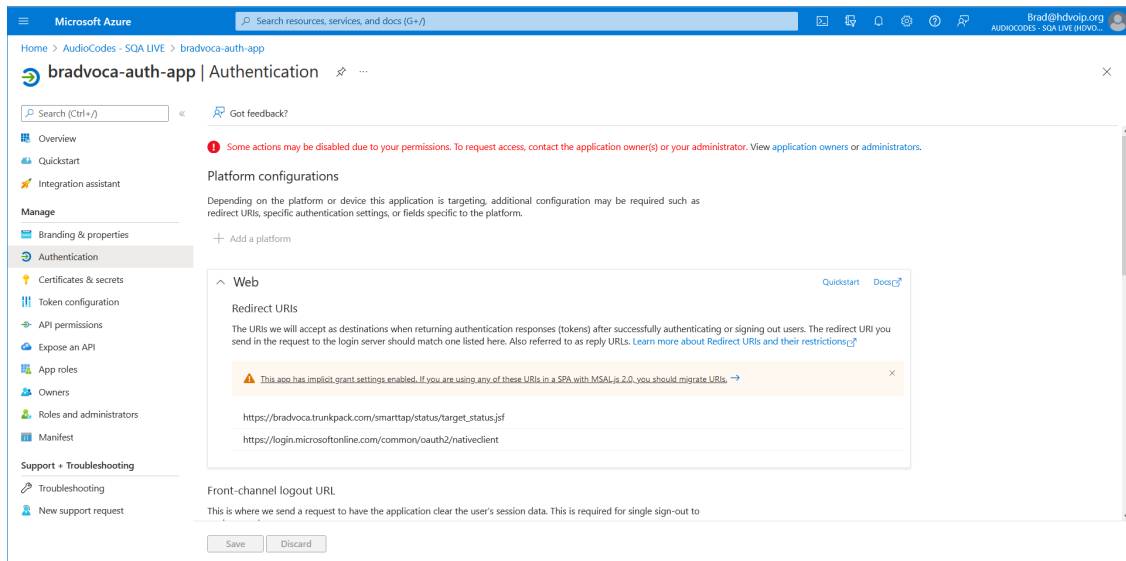
- Add a certificate or secret
- 2 web, 0 spa, 0 public client
- Application ID URI: api://bradvoca.azurewebsites.com/smarttap
- Managed application in: bradvoca-auth-app

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

3. In the Navigation pane, select **Authentication**.

Figure 33-7: auth-app Authentication

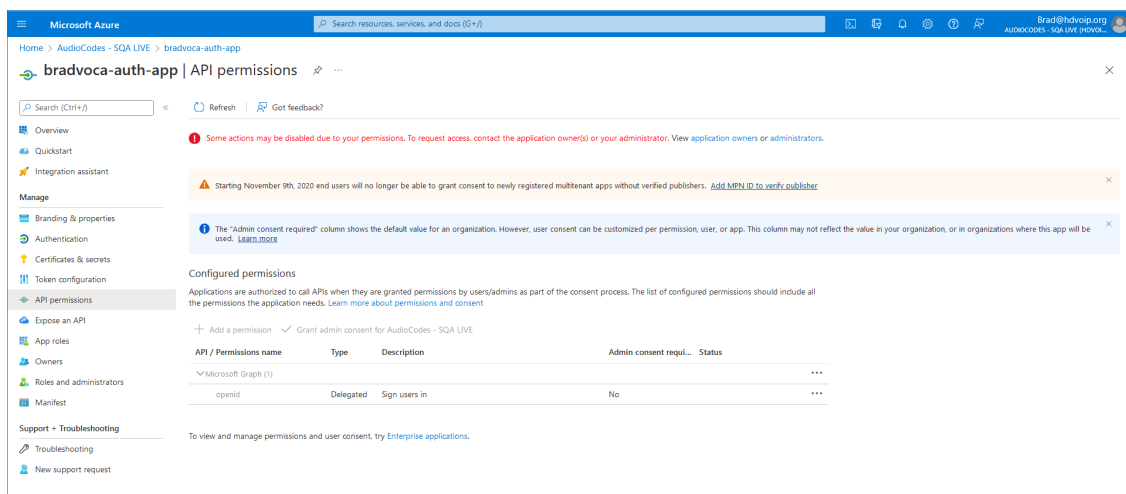


The configured Redirect URIs are used as follows:

- Customer login to SmartTAP Portal (a separate URI is created for each customer).
- Token authentication link send to customer IT administrator for requesting consent.

4. In the Navigation pane, select **Permissions**.

Figure 33-8: auth permissions



5. View that the required permissions are displayed:

- Openid-Sign in and read user profile

Verify Active Directory Providers Configuration

An AAD mapping entry is created by the SmartTAP for Teams Deployment script with the following customer tenant credentials:



- Application (Client) ID
- Directory (Tenant) ID

- Client Secret

➤ **Do the following:**

1. Login to the SmartTAP Web with Administrator role.
2. Open the View/Modify AAD Configuration screen (**System** tab > **AAD** folder > **View/Modify AAD Config**).

Figure 33-9: Active Directory Providers

Active Directory Providers				
Name	Organization (Tenant) Id	Application (Client) Id	Modify	Delete
OmarAADMapping	ad41d6c3-67f0-47cc-9de3-e07fd185c1c7	e89f56de-0f23-4d35-a639-9503caa55de4		



There is an identical corresponding mapping entry for the customer Azure tenant between the Active Directory Providers table (shown in figure above) and the OpenID Connect Token Client Configuration screen (see [Update OpenID Connect Token \(OIDC\) Client Configuration](#) on page 337).

Configure AAD Mapping Profiles

SmartTAP 360° Version 5.1 and later allows configuration of the following profiles for mapping Organizations' (Tenant) users from Microsoft Azure Active Directory (AAD Azure Active Directory objects to SmartTAP entities. It's possible to map users and profiles from **several** Azure Active Directories. The following profiles can be configured:

- **Active Directory Providers Configuration:** AAD mapping with customer tenant credentials (see [Verify Active Directory Providers Configuration](#) on the previous page).



A default mapping entry is created by the Deployment script including the credentials of the Azure customer tenant.

- **AAD User Mapping Profile:** Maps to one or more member groups. All users belonging to the mapped groups inherit the mapped profile (see [AAD User and Group Mapping](#) on page 372). Once the AAD group is mapped, it is added to the SmartTAP Groups table.
- **AAD Security Mapping Profile:** Maps to one or more member groups. All users belonging to the mapped groups inherit the mapping profile (see [AAD Security Profile Mapping](#) on page 365). Once the AAD Security Profile is mapped, it is added to the SmartTAP Security Profiles table.
- **AAD Recording Mapping Profile:** Maps to one or more member groups. All users belonging to the mapped groups inherit the mapping profile (see [AAD Recording Profile Mapping](#) on page 358). Once the Recording Profile is mapped, it is added to the SmartTAP Recording Profiles table.
- **AAD Retention Mapping Profile:** Maps to one or more member groups. All users belonging to the mapped groups inherit the mapped profile. Once the Retention Profile is mapped, it

is added to the SmartTAP Retention Policies table (see [AAD Retention Policy Mapping](#) on page 352).

- **AAD Media Location Mapping Profile:** Maps to one or more member groups. All users belonging to the mapped groups inherit the mapped profile (see [AAD Media Location Mapping](#) on page 347). Once the Media Location Mapping Profile is mapped, it is added to the SmartTAP Recording Locations table.
- **AAD Analytics Mapping Location Mapping Profile:** Maps to one or more member groups. All users belonging to the mapped groups inherit the mapped profile (see [AAD Analytics Mapping](#) below). Once the AAD Analytics Mapping Profile is mapped, it is added to the SmartTAP Analytics Profile table.



- 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 Analytics Mapping

This section describes how to map AAD Analytics profiles. The Analytics profiles should be mapped to one or more of the member groups that you mapped in [AAD User and Group Mapping](#) on page 372 and then users assigned to these groups are associated with the new Analytics profiles.



- In the event where a user is mapped to two or more Analytics profiles then it will not be assigned to any profile and an alarm will be raised.
- In case the analytics profile of a user is mapped to two groups (of the same kind,) then no analytics profile is 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 analytics profile.

➤ To configure analytics mapping:

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

Figure 33-10: 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 [Verify Active Directory Providers Configuration](#) on page 340 and then click .

Figure 33-11: Modify Active Directory Configuration

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

Mapping Name:

Member Groups:

☒ One Level
 ☐ Subtree

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

3. Select the **Analytics Mappings** tab.

Figure 33-12: Analytics Mappings

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

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 Analytics 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 33-13: 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 33-14: 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 33-15: Remove Member Group Assignment

8. Click  to apply changes.

Figure 33-16: Assigned Member Groups**Figure 33-17:**










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

Figure 33-18: Analytics Profile Mapping

10. Open the View/Modify Analytics Profiles page to view the new profile mapping and to configure it ([View and Modify Analytics Profile](#) on page 69).

Figure 33-19: View/Modify Analytics Profiles

View/Modify Analytics Profiles			
Name	Description	Modify Analytics Profiles	Delete
AnalyticsProfile_EN	rest_Analytics_desc		
VPNCpolicy	VPNCpolicy		
Analytics_Profile_HE	Analytics_Profile_HE		
STQATeam	STQATeam		
ST-load-test-dynamic-rename	ST-load-test-dynamic-rename		

AAD Media Location Mapping

This section describes the AAD Media Location mapping. The media locations should be mapped to one or more of the member groups that you mapped in [AAD User and Group Mapping](#) on page 372 and then users assigned to these groups are associated with the new media location.





- In the event where a user is mapped to two or more media locations then it will not be assigned to any location and an alarm will be raised.
- In case the media location of a user is mapped to two groups (of the same kind,) then no media location is 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 media location.

➤ To configure media location mapping:

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

Figure 33-20: 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 [Verify Active Directory Providers Configuration](#) on page 340 and then click .

Figure 33-21: Modify Active Directory Configuration

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

[SUBMIT](#)

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

Mapping Name:

Member Groups: [Select Groups](#)

☒ One Level
 ☐ Subtree

[+](#)

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

▶ Analytics Mappings

3. Select the **Media Location Mappings** tab.

Figure 33-22: Location Mappings

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

[SUBMIT](#)

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

Mapping Name:

Member Groups: [Select Groups](#)

☒ One Level
 ☐ Subtree

[+](#)

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

▶ Analytics Mappings

4. In the Mapping Name field, enter a name for the Media Location 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 33-23: 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 33-24: 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 33-25: Remove Member Group Assignment

8. Click  to apply changes.

Figure 33-26: Assigned Member Groups

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

The new Location Mappings profile is displayed:

Figure 33-27: Media Location Mapping

10. Open the View/Modify Recording Locations page to view the media location mapping and configure it ([Viewing and Modifying a Recording Location](#) on page 286).

Figure 33-28: View/Modify Recording Locations

View/Modify Recording Locations							
Location Name	Path or Container	Description	Username	Domain	Modify	Default	Remove
Initial	recordings	Initial Recording Location	mediabxmsftcert54				
STQATeam		STQATeam					
ST-Teams-Users		ST-Teams-Users					
ST-load-test-dynamic-rename		ST-load-test-dynamic-rename					

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 372 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, 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 33-29: 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 [Verify Active Directory Providers Configuration](#) on page 340 and then click .

Figure 33-30: 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 33-31: 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 33-32: 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 33-33: 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 33-34: Remove Member Group Assignment

8. Click  to apply changes.

Figure 33-35: Assigned Member Groups

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

The new Retention Profile mapping is displayed:

Figure 33-36: Retention Profile Mapping

10. Open the View/Modify Retention Policies page to view the new profile mapping and configure it according to requirements (see [Configuring Call Retention](#) on page 58).

Figure 33-37: View/Modify Retention Policies

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	



By default, the newly created retention policy is set to 0 (no calls are retained) as shown in figure "Default Retention Policy".

Figure 33-38: Default Retention Policy

Change Retention Policy Retention Policy	
Retention Policy Name	<input type="text" value="st-subgroup1-test"/>
Retention Policy Description	<input type="text" value="st-subgroup1-test"/>
Call and Instant Message Retention Period (in days)	<input type="text" value="0"/>

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 372 and then 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 204).

➤ **To configure recording profile mapping:**

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

Figure 33-39: 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 [Verify Active Directory Providers Configuration](#) on page 340 and then click .

Figure 33-40: 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 33-41: 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 33-42: 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 33-43: 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 33-44: 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-subnet1-test-group [14-05d00-7500-4131-0f4-54d5f3c570b3]

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 33-45: 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°.

The new Recording profile is displayed:

Figure 33-46: Recording Profile

• Mapping successfully added.

Modify Active Directory Configuration

Name: OmarAAD_mapping

Directory (Tenant) ID: ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Application (Client) ID: 00c65e7a-2064-443f-bb24-0de67025bd72

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
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		

9. Open the View/Modify Recording Profile page to view the new profile mapping and configure it (see [Viewing or Modifying Recording Profiles](#) on page 48).

Figure 33-47: View/Modify 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	

100% 1 (1 of 1)



By default, the newly created recording profiles are mapped with all options disabled as shown in figure "Default Recording Profile" below.

Figure 33-48: 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	<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 type="checkbox"/> Inbound	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"/> Outbound	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
Federated	<input type="checkbox"/> Inbound	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"/> Outbound	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

☐ 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

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 372 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 33-49: 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 [Verify Active Directory Providers Configuration](#) on page 340 and then click .

Figure 33-50: 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 33-51: 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 33-52: 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

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

Figure 33-53: 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 33-54: 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 33-55: Assigned Member Group

Modify Active Directory Configuration

Name

Directory (Tenant) ID

Application (Client) ID

Client Secret

SUBMIT

User Mappings

Security Profile Mappings

Mapping Name


Member Groups **Select Groups**

☒ One Level ☐ Subtree

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

Recording Profile Mappings

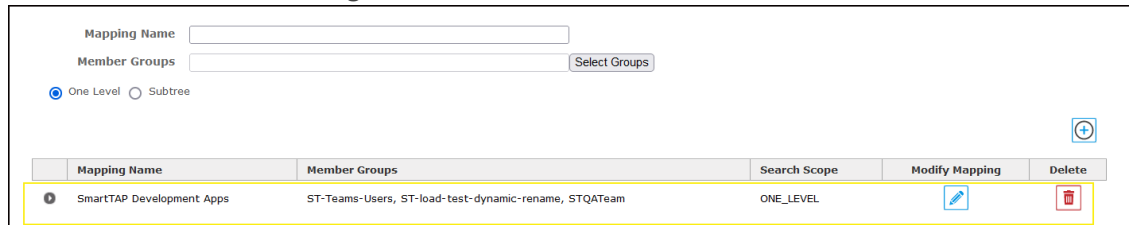
Retention Mappings

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

The new Security profile mapping is displayed.

Figure 33-56: Security Profile Mapping



Figure 33-57:



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		

10. Open the View/Modify Security Profile page to view the new profile mapping and configure it (see [Configure Permissions in a Security Profile](#) on page 37).

Figure 33-58: View/Modify Security Profile

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



By default, the security profiles are mapped with all permissions disabled (see figure "Default Security Profile" below).

Figure 33-59: Default 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

AAD User and Group Mapping

SmartTAP 360° 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° 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 92 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 92).
2. Open the Add AAD Config page (**System** tab > **AAD** folder > **Add AAD Config**).

Figure 33-60: Add Active Directory Configuration

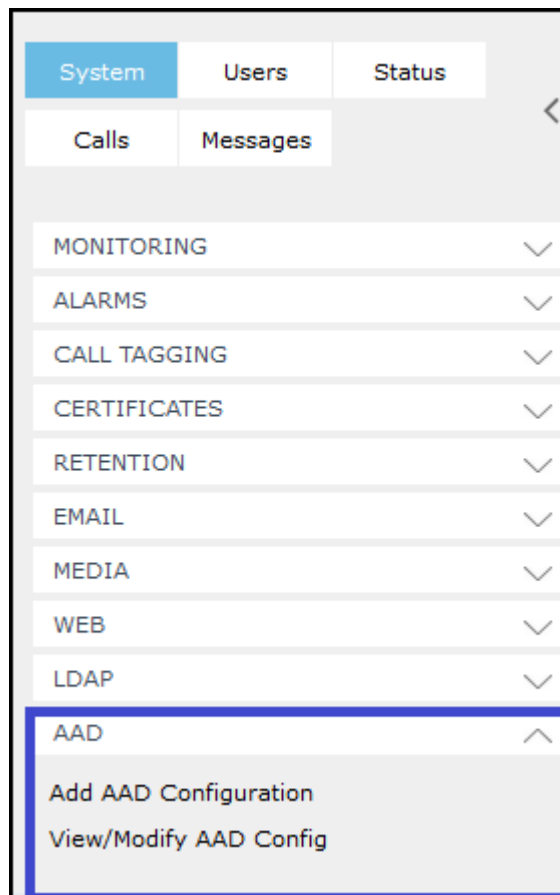


Figure 33-61: Active Directory Providers

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 [Verify Active Directory Providers Configuration](#) on page 340 and then click .

Figure 33-62: 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

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 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.

Figure 33-63: Select Member Groups

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 33-64: Select Member Groups

- Click ▼ to move selected groups from the 'Search Groups' section to the 'Selected Groups' section.
- Click ▲ to remove selected groups from the 'Selected Groups' section, and in case the search results should contain those groups, they are moved back to the 'Search Groups' section.



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



7. Click  to apply the changes.
8. Click  to add this mapping to SmartTAP 360°.

Figure 33-65: Member Groups

Mapping Name:

Member Groups:

First Name:

Last Name:

Login:

Email:

Alias:

Object ID:

Mapping Name	Member Groups	Modify Mapping	Delete
No records found.			

Successful user mapping is displayed under the User Mapping table.

Figure 33-66: Mapping Successfully Added

• Mapping successfully added.

Modify Active Directory Configuration

Name:

Directory (Tenant) ID:

Application (Client) ID:

Client Secret:

User Mappings

Mapping Name:

Member Groups:

First Name:

Last Name:

Login:

Email:

Alias:

Object ID:

Mapping Name	Member Groups	Modify Mapping	Delete
ST AAD Users	ST_Test_Group, SmartTapAgents	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

- Open the View/Modify Users page (Users > View/Modify Users page) (see [View and Modify Users](#) on page 85).

Figure 33-67: Mapped Users

First Name	Last Name	Email	Login ID	Alias	Object ID	Modify	Delete
TeamsTestUser4-E5		TeamsTestUser4-E5@ai-logix.net	TeamsTestUser4-E5@ai-logix.net		3b47f7f8-bd88-4cd7-a963-5c24a0f0cd03	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
ST-Teams20		ST-Teams20@SmartTAP.onmicrosoft.com	ST-Teams20@SmartTAP.onmicrosoft.com		f0ef13b3-b9e7-428d-97c2-4d80692080b4	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
ST-Teams32		ST-Teams32@smarttap.onmicrosoft.com	ST-Teams32@smarttap.onmicrosoft.com		23030c8b-81de-4cfe-95c9-a8f33b2f0e12	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
ST-Teams24		ST-Teams24@smarttap.onmicrosoft.com	ST-Teams24@smarttap.onmicrosoft.com		3d811607-c0c0-471d-8ab8-8766102a3366	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
ST-Teams23		ST-Teams23@smarttap.onmicrosoft.com	ST-Teams23@smarttap.onmicrosoft.com		85291d87-392e-4415-b453-4219ac8330e1	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

- When the "Add Groups" check box is selected, Mapped Groups can be viewed in the Groups page (see [View and Modify Recording Groups](#) on page 32).

Figure 33-68: Mapped Groups

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

Setup Microsoft 365 User Sign-in Authentication

For SmartTAP 360° version 5.1 and later, users can be mapped from Organizations' (Tenant) Azure Active Directory (AAD) and authenticated with SmartTAP Web using their Microsoft 365 login credentials. SmartTAP 360° uses the OpenID Connect Authorization Code Flow) to authenticate users with Microsoft Identity Platform. The "login-app" registration created by the Deployment script is used to manage the Microsoft 365 User Sign-in authentication.



- This feature supports logging in to the SmartTAP Web for users from a **single** organizational tenant as an alternative to local user authentication.
- Ensure that the **login-app** includes a Client Secret which is required for accessing Azure Blob storage statistics.
- Except for the assigning of a **Security profile** to the M365 user, this setup is performed **automatically** by the SmartTAP for Microsoft Teams **deployment script**.

This section includes the following procedures:

- View the login-app API permissions (see [Verify login-app Permissions](#) on page 381).
- View OIDC Client User Login Authentication (see [View OIDC Client User Login](#) on page 398).
- Assign Security Profile to Azure Active Directory user in SmartTAP 360° (see [Assign Security Profile to M365 User](#) on page 386).

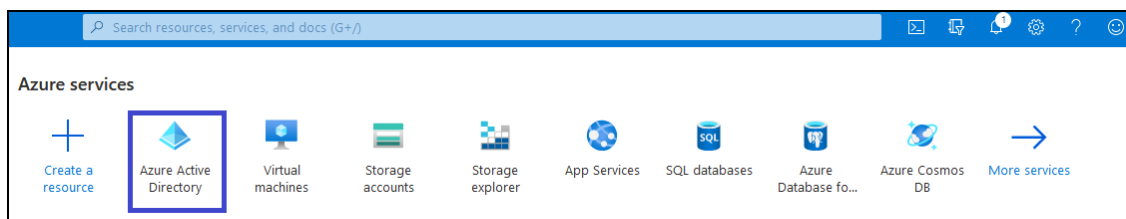
Configure Client Secret for login-app

A client secret must be configured for the login-app ?.

➤ To configure a client secret:

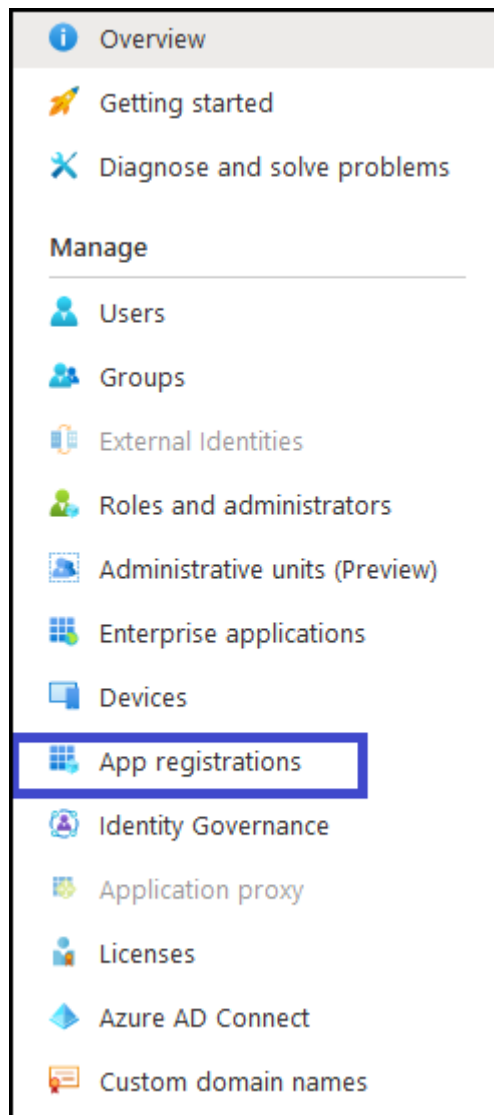
1. Login to Azure portal (<https://portal.azure.com/>)
2. Access Azure Active Directory Service.

Figure 33-69: Azure Services



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

Figure 33-70: App Registrations



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

Figure 33-71: Certificates & Secrets

AADAppClient | Certificates & secrets

Search (Ctrl+/) «

Certificates
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 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.		

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

Figure 33-72: Add a client secret

Add a client secret

Description:

Expires: Recommended: 6 months

- Recommended: 6 months
- 3 months
- 12 months
- 18 months
- 24 months
- Custom

6. 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 33-73: 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

7. Copy the Value of the client secret for later configuration in the SmartTAP Web (see [View OIDC Client User Login](#) on page 398).

Verify login-app Permissions

This step describes how to verify the login-app permissions are correctly set.

➤ To check API permissions:

1. Open the API Permissions screen (**Manage > API permissions**).

Figure 33-74: API permissions

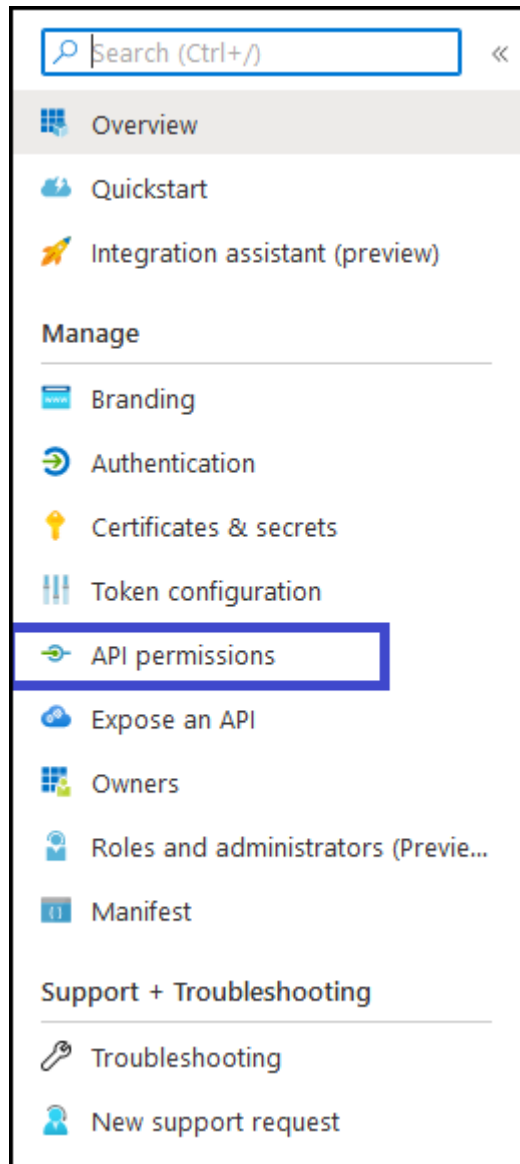


Figure 33-75: Configured Permissions

Refresh

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [Grant admin consent for Nuera Ltd.](#)

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
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 selected. Navigate to **Azure Ad ->Enterprise applications**.

Figure 33-76: Enterprise Applications

Home > AudioCodes Ltd. | Overview

Azure Active Directory

Switch tenant Delete tenant Create a tenant What's new Preview features Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

AudioCodes Ltd.

Search your tenant

Tenant information

Your role
Global administrator and 7 other roles
[More info](#)

License
Azure AD Premium P1

Tenant ID
ad41d6c3-67f0-47cc-9de3-e07fd...

Primary domain
ai-logix.net

Azure AD Connect

Status
Enabled

Last sync
Less than 1 hour ago

Sign-ins

2,000
1,500
1,000
500
0

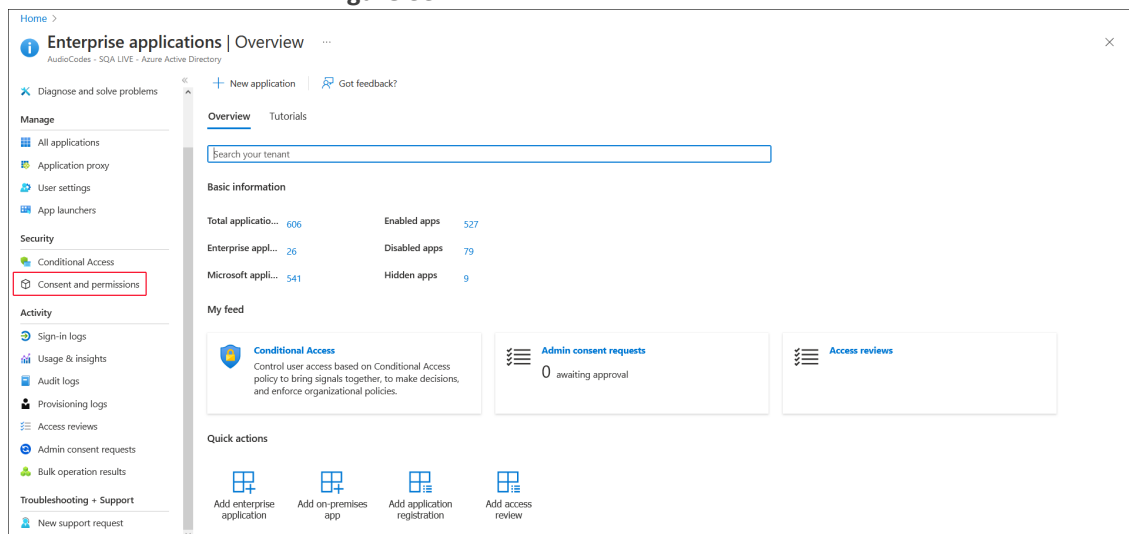
November Nov 8

Sign ins
123

Create

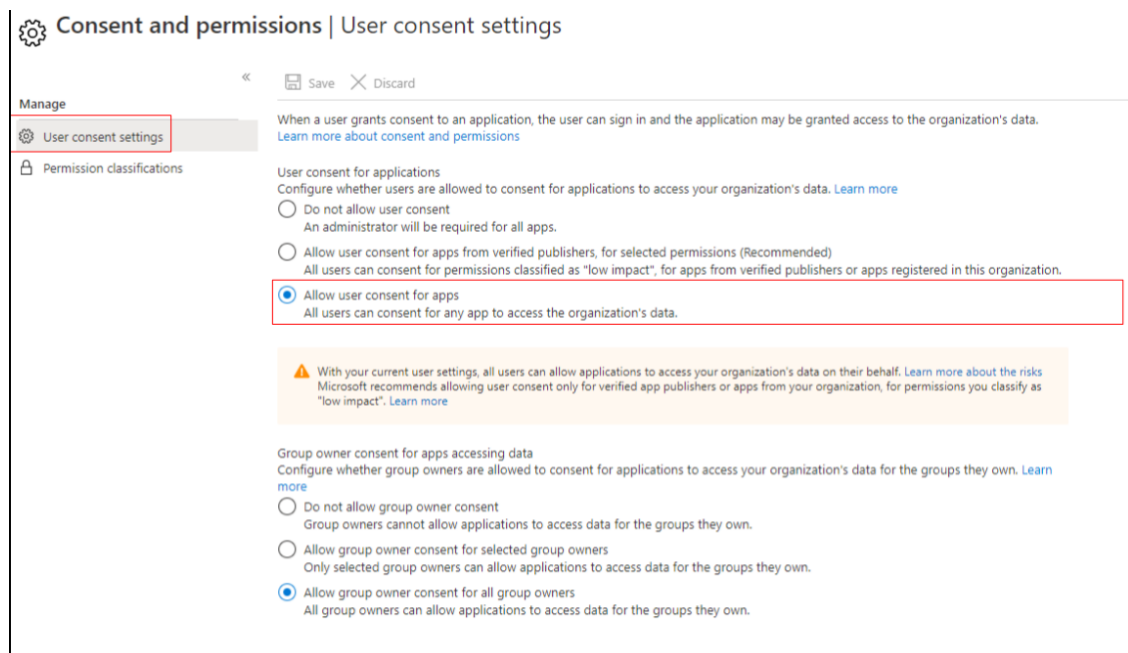
4. Navigate to **Consent and Permissions**.

Figure 33-77:



5. By default, the third option (**Allow user consent for apps**) is chosen, and it's the one used by SmartTap by default.

Figure 33-78: User Consent Settings



The option **Allow user consent for apps from verified publishers** is also supported with the following configuration:

Figure 33-79: 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.

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. Click Save and then **Select permissions to classify as low impact**.

Figure 33-80: 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 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	

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](#)

Yes, add selected permissions **No, I'll add permissions**

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

Figure 33-81: Add Permissions--Openid

Manage

« + Add permissions

User consent settings

Permission classifications

Classify permissions

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

API used	Permissions	Description

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](#)

- ☐ User.Read - sign in and read user profile
- ☐ offline_access - maintain access to data that users have given it access to
- ☒ openid - sign users in
- ☐ profile - view user's basic profile
- ☐ email - view user's email address

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

View OIDC Client User Login

OpenID Connect Login (OIDC) Client Configuration is used for configuration of the login-app. This app is used for the SmartTAP application for Microsoft 365 User Sign-in and for logging into SmartTAP using the Teams Personal app utilizing Microsoft Open ID Connect (Oauth 2). The app enables SmartTAP to reroute users accessing the SmartTAP application either from a browser or from the SmartTAP's Teams application to be authenticated according to your organizational M365 policy.



The OpenID Connect Login (OIDC) configuration is created **automatically** by the Deployment script. For more information on OIDC, refer to <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow>.

➤ To view the OpenID Connect OIDC Client:

1. In the SmartTap Web interface, open the Add/Modify OpenID Connect Login (OIDC) Client Configuration page (**System** tab > **Web** folder > **OpenID Connect Login**).

Figure 33-82: OpenID Connect

Add/Modify OpenID Connect Login (OIDC) Client Configuration

— Add/Modify OpenID Connect Login (OIDC) Client Configuration —

Directory (Tenant) ID
ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Hosted (Tenant) ID
ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Application (Client) ID
663786d3-823b-4dac-8666-f5906886cda1

Client Secret
••••••••

Redirect URI
https://omr561terpckst.ai-logix.net/smarttap/status/

SUBMIT

The OIDC Client Web Application registration (login-app) includes the following customer tenant credentials:

- Directory (Tenant) ID
- Hosted (Tenant) ID
- Application (Client) ID
- Client Secret
- Redirect URI

Assign Security Profile to M365 User

This step describes how to assign M365 user to "agent" security profile in SmartTAP 360°.

➤ To assign a security profile:

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

Figure 33-83: View/Modify Users

View/Modify Users

First Name	Last Name	Email	Login ID	Alias	Modify	Delete
Deb	Dutta	debajyotid@smarttap.onmicrosoft.com	deb			


20 1 (1 of 1)

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

Figure 33-84: User Successfully Updated

• *User successfully updated.*

Modify User



First Name

Email

Alias

Recording Profile

Last Name

Login ID

Retention Policy


Legal Hold

Security Profiles

- administrator
- agent**
- supervisor

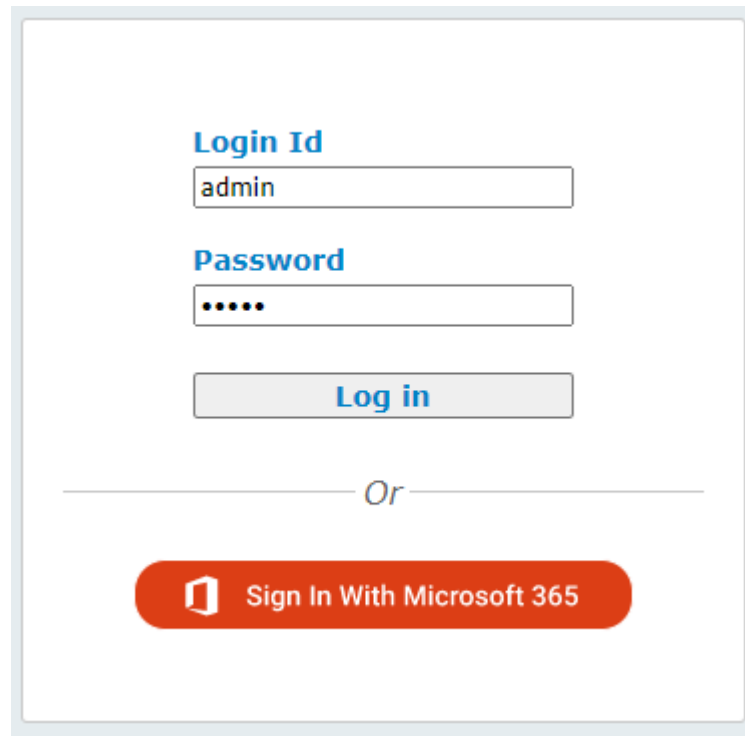
Groups

- Default
- TEST_G_1

SUBMIT **CANCEL** 

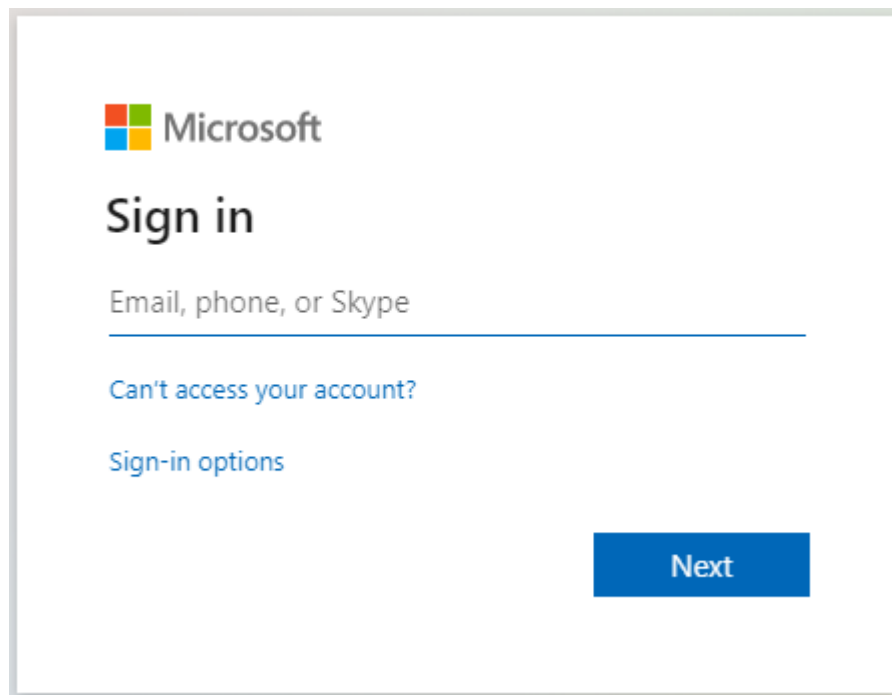
4. Login to SmartTAP 360° using Microsoft Login Credentials.
- On the SmartTAP 360° login page, click **Sign In With Microsoft 365**.

Figure 33-85: Microsoft Sign in

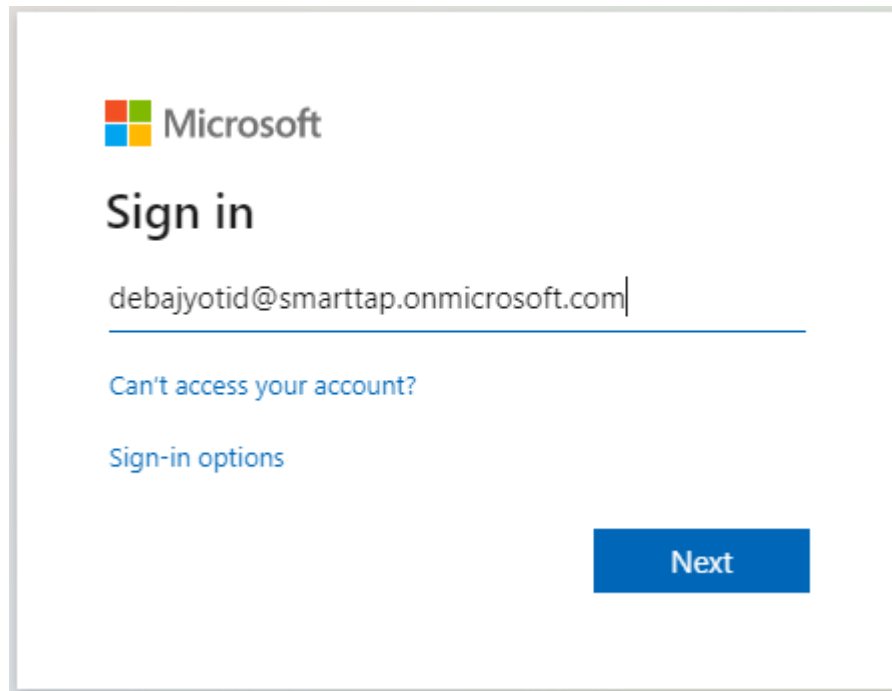
A screenshot of a Microsoft login form. It features two input fields: 'Login Id' with the text 'admin' and 'Password' with five dots. Below these is a 'Log in' button. A horizontal line with the word 'Or' in the center separates this from a large red button labeled 'Sign In With Microsoft 365' which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

The user is redirected to Microsoft MFC Login page:

Figure 33-86: Microsoft MFC Login Page

A 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 33-87: Sign InA screenshot of the 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

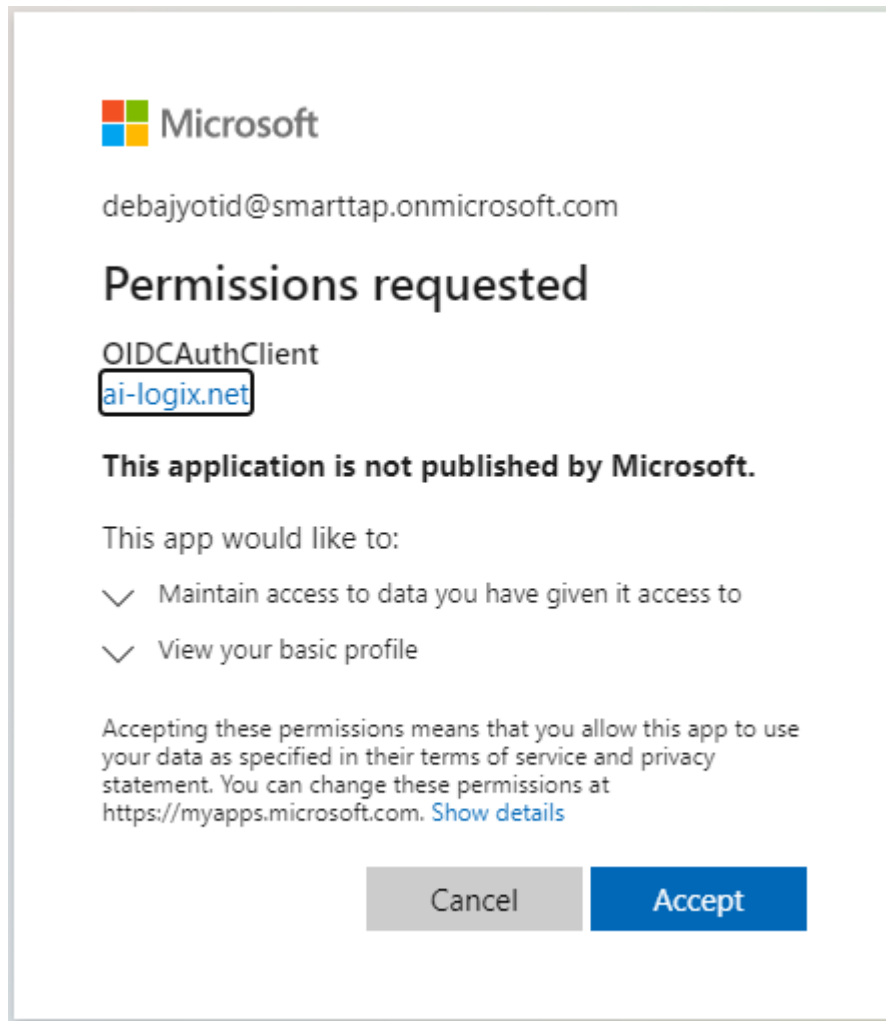
[Can't access your account?](#)

[Sign-in options](#)

Next

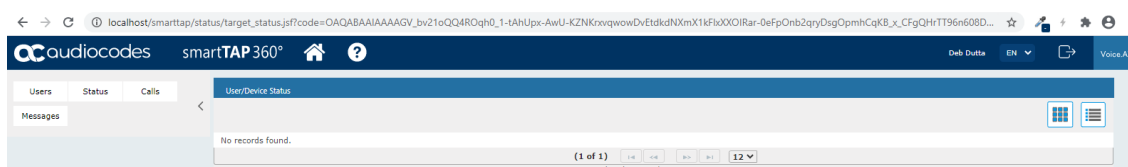
- Allow permission to the client app to use user authentication data.

Figure 33-88: Permissions Requested



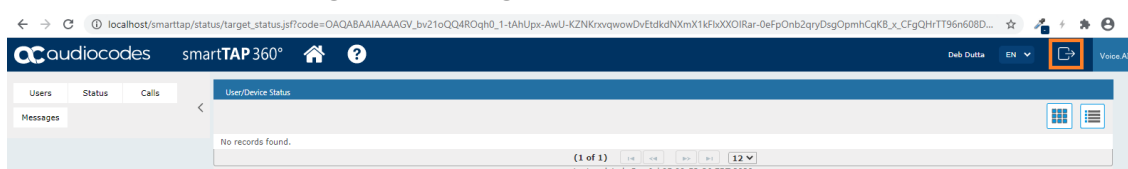
The user is re-directed to SmartTAP 360° URI configured in AAD (see [Configure Client Secret for login-app](#) on page 378 i.e. http://localhost/SmartTAP 360°/status/target_status.jsf

Figure 33-89: User Device Status



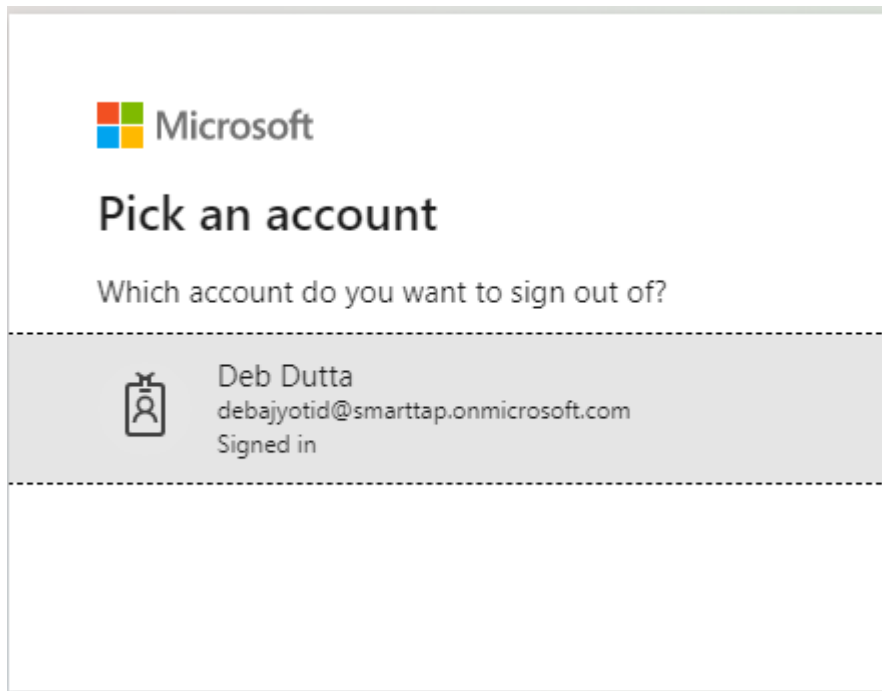
5. An Azure Active Directory user logs off from SmartTAP Web.

Figure 33-90: Logout



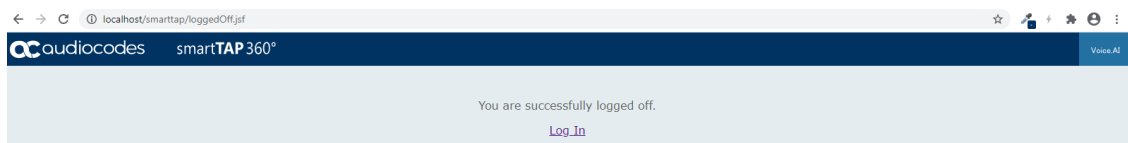
6. User is prompted to select the Microsoft account that needs to be signed out.

Figure 33-91: Pick an Account



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

Figure 33-92: SmartTAP 360° LogOff Page



Integrate SmartTAP Personal App in Teams

SmartTAP for Teams can be added as a Personal App in Microsoft Teams with the main tab/page including On-demand buttons and an additional tab for accessing the full application.

- 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.
- Global administrator role in Azure is required to perform the above procedures.
- Except for the loading the manifest file to Customer Teams admin center (see [Configure and Load Manifest \(Personal App\)](#) on page 399), this setup is performed **automatically** by the SmartTAP for Microsoft Teams **deployment script**. The script uses the **login-app** registration (also used for Microsoft 365 Sign-in to apply Open ID Connect (Oauth 2) authentication (see [View OIDC Client User Login](#) on page 398). If you wish to use a separate

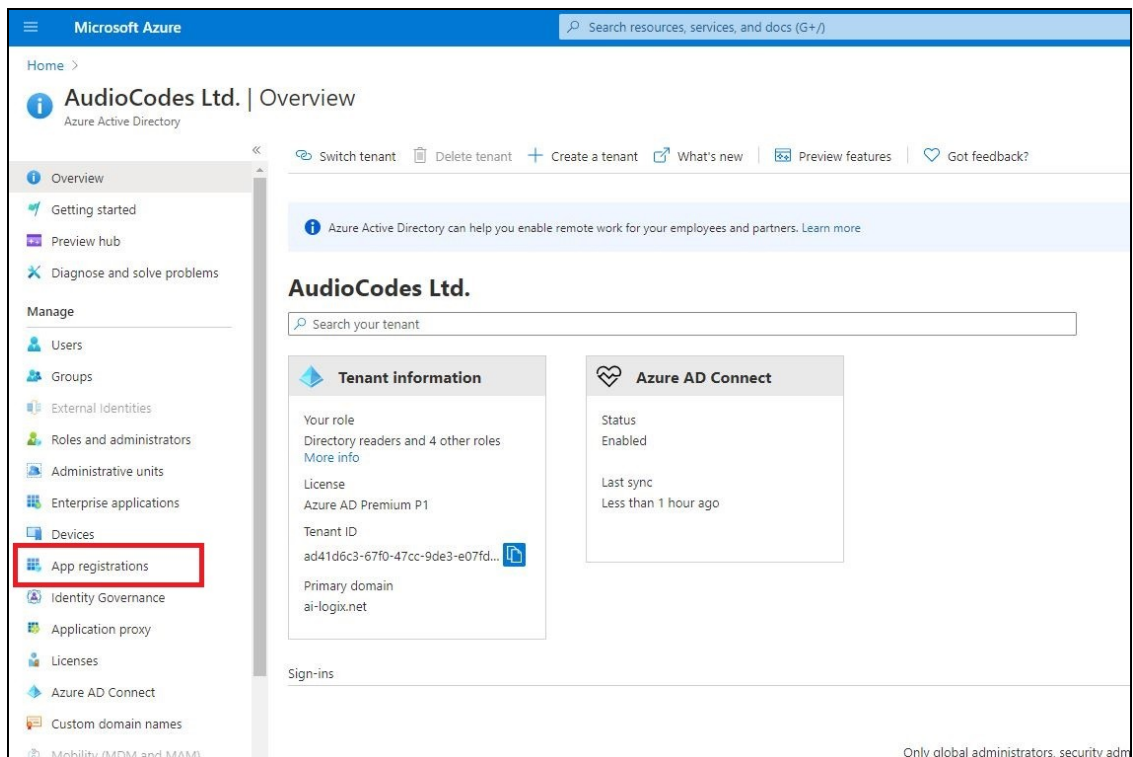
registration, create as described in [Create and Register the SmartTAP Personal App](#) below. For both scenarios, ensure that a client secret has been configured for the registration.

Create and Register the SmartTAP Personal App

This procedure describes how to create and register the SmartTAP Personal App. The same registration can be used for SmartTAP Web login authentication of the Microsoft 365 user and the Personal App user.

➤ To register the Personal app:

1. Go to Azure portal > **Azure Active Directory** > **App Registrations**.
2. Do one of the following:
 - Create a new App registration (proceed to next step).
 - Select the registration app that was created for **login-app**. In this case, ensure that you have configured a client secret and proceed to [Set Microsoft API Permissions for Personal App](#) on page 394.



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**.

The screenshot shows the 'ST-Teams-app | Certificates & secrets' page. The left navigation pane includes sections like Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, etc.), and Support + Troubleshooting. The main content area has a search bar and a 'Got feedback?' link. Below this, there's a section for 'Certificates' with an 'Upload certificate' button and a table for certificates. A message states 'No certificates have been added for this application.' Below that is a section for 'Client secrets' with a 'New client secret' button and a table for client secrets. The table has columns for Description, Expires, Value, and ID. One secret is listed with Description 'secret', Expires '12/17/2022', Value '~sB*****', and ID 'c6fd6640-bc85-4e96-a1da-872bfaf3b086'.

Set Microsoft API Permissions for Personal App

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

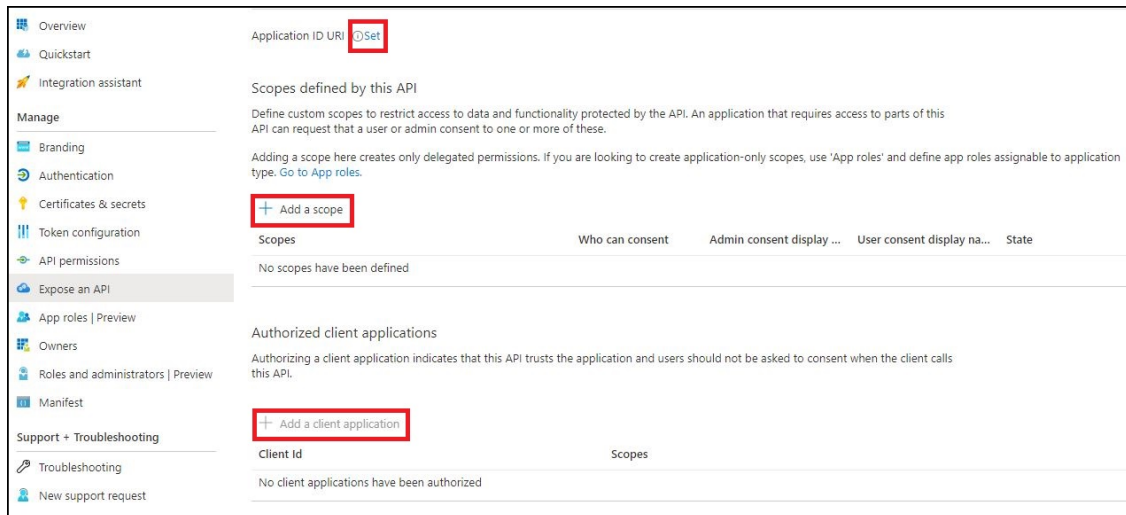
➤ To set permissions for the personal app:

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

Figure 33-93: Expose an API

The screenshot shows the 'ST-Teams-app' page with the 'Expose an API' option highlighted in the left navigation pane. The main content area displays the app's details under the 'Essentials' section, including Display name, Application (client) ID, Directory (tenant) ID, and Object ID. Below this, there's a message about the upgrade from ADAL to MSAL. At the bottom, there's a 'Call APIs' section with icons for various Microsoft services like OneDrive, SharePoint, and Teams.

Figure 33-94: 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.

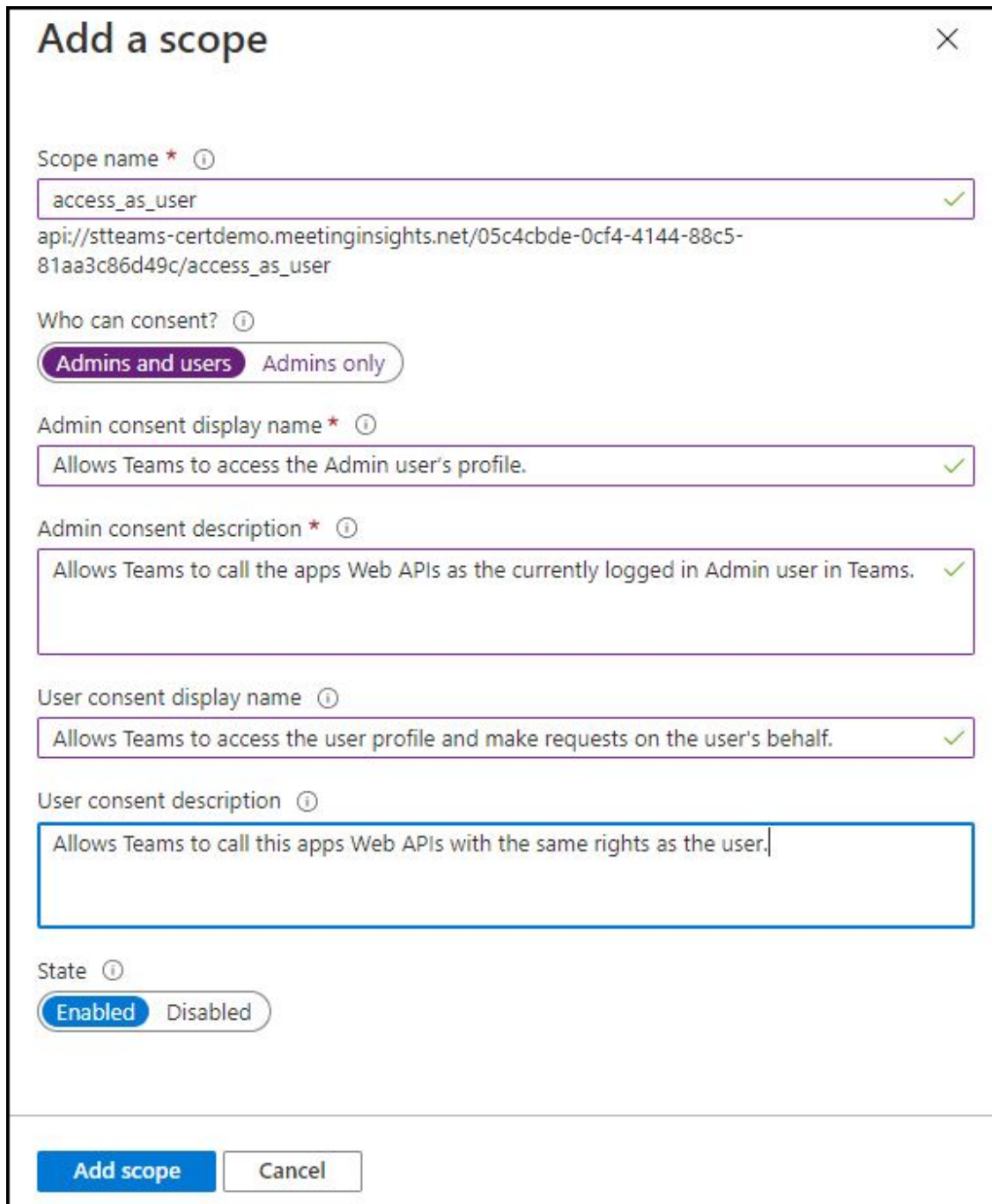
4. Select **Add a scope**. In the panel that opens, enter `access_as_user` as the **Scope name**.
5. Set **Who can consent?** to `Admins and users`.
6. Enter the following fields for configuring the admin and user consent prompts with values that are appropriate for the `access_as_user` scope:
 - **Admin 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://[smarttapteams poc.bot.ai-logix.net](#)/05c4cbde-0cf4-4144-88c5-81aa3c86d49c/access_as_user

Figure 33-95: 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

- In the Authorized client applications section, identify the applications that you want to authorize for your app's Web application.
 - 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 33-96: Client ID

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 33-97: Delegated Permissions

Home > AudioCodes Ltd. > ST-Teams-app

ST-Teams-app | API permissions ✕

Search (Ctrl+/) « Refresh Got feedback?

⚠ 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	-	...

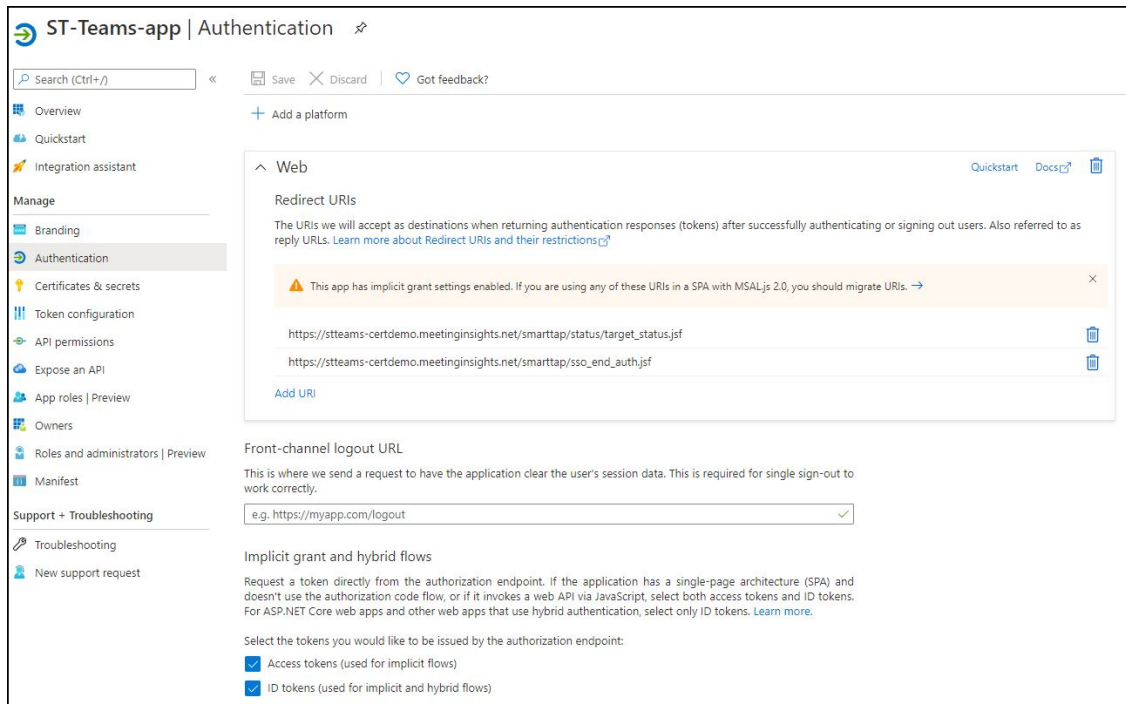
To view and manage permissions and user consent, try [Enterprise applications](#).



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 33-98: Authentication



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**

View OIDC Client User Login

OpenID Connect Login (OIDC) Client Configuration is used for configuration of the login-app. This app is used for the SmartTAP application for Microsoft 365 User Sign-in and for logging into SmartTAP using the Teams Personal app utilizing Microsoft Open ID Connect (Oauth 2). The app enables SmartTAP to reroute users accessing the SmartTAP application either from a browser or from the SmartTAP's Teams application to be authenticated according to your organizational M365 policy.



The OpenID Connect Login (OIDC) configuration is created **automatically** by the Deployment script. For more information on OIDC, refer to <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow>.

➤ **To view the OpenID Connect OIDC Client:**

1. In the SmartTap Web interface, open the Add/Modify OpenID Connect Login (OIDC) Client Configuration page (**System** tab > **Web** folder > **OpenID Connect Login**).

Figure 33-99: OpenID Connect

Add/Modify OpenID Connect Login (OIDC) Client Configuration

Add/Modify OpenID Connect Login (OIDC) Client Configuration

Directory (Tenant) ID
ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Hosted (Tenant) ID
ad41d6c3-67f0-47cc-9de3-e07fd185c1c7

Application (Client) ID
663786d3-823b-4dac-8666-f5906886cda1

Client Secret
.....

Redirect URI
https://omr561terpckst.ai-logix.net/smarttap/status/

SUBMIT

The OIDC Client Web Application registration (login-app) includes the following customer tenant credentials:

- Directory (Tenant) ID
- Hosted (Tenant) ID
- Application (Client) ID
- Client Secret
- Redirect URI

Configure and Load Manifest (Personal App)

This procedure describes how to upload the Manifest file to the customer tenant Teams admin center. The Deployment script uses the login-app for authentication for logging into

SmartTAP Web.



For manual setup of the SmartTAP Personal app, see [Integrate SmartTAP Personal App in Teams](#) in the SmartTAP Admin Guide. [Integrate SmartTAP Personal App in Teams](#) on page 391.

➤ **To upload the Manifest file:**

1. Extract the Zip file from the following path ...\\TerraSmartX\\TerraSmartX\\output_data\\xxx_app.zip to your deployment platform.
2. Upload the Zip file to the Customer App store using the following:
<https://admin.teams.microsoft.com/dashboard>

Example 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",
```

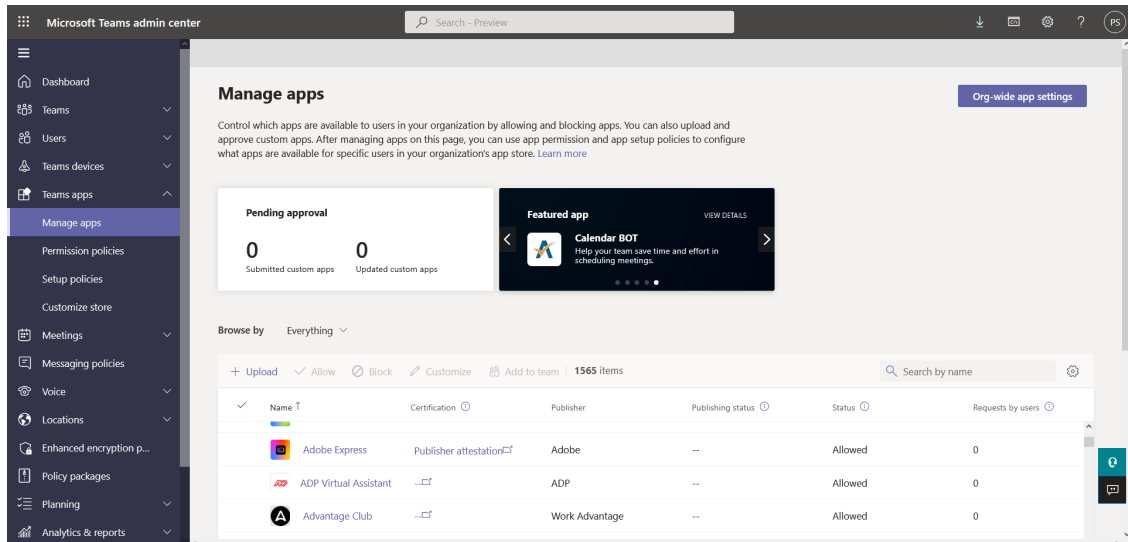
```
"websiteUrl": "https://smarttapteamspec.bot.ai-
logix.net/smarttap/status/call_status.jsf", "scopes": [ "personal" ] },
{ "entityId": "ST", "name": "All Calls", "contentUrl":
"https://smarttapteamspec.bot.ai-logix.net/smarttap/welcome.jsf",
```

```
"websiteUrl": "https://smarttapteamspec.bot.ai-
logix.net/smarttap/welcome.jsf",
```

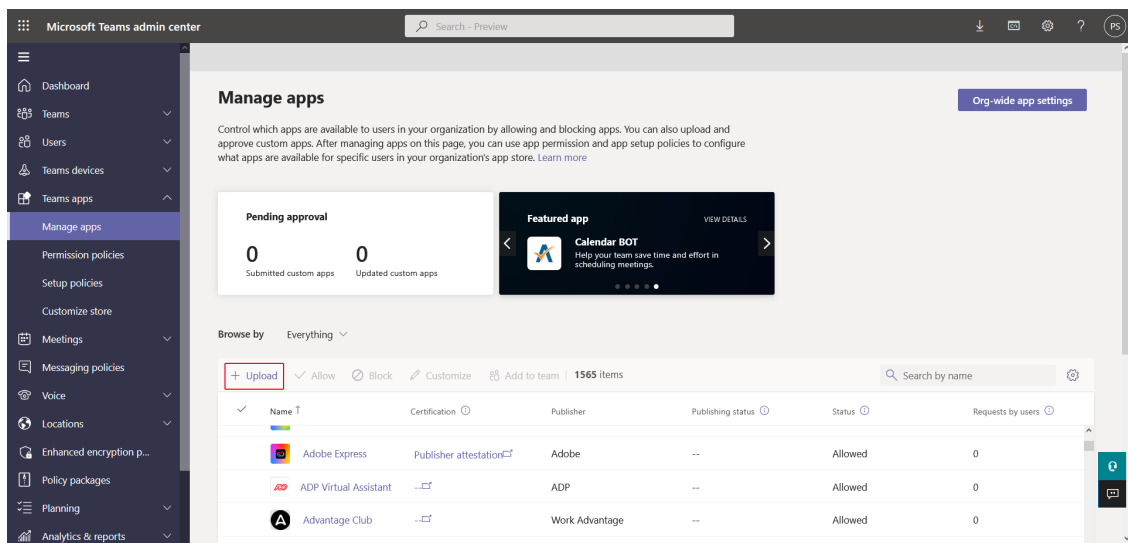
```
"scopes": [ "personal" ] } ], "permissions":
[ "identity", "messageTeamMembers", "validDomains": [ "smarttapteamspec.bot.ai-
logix.net",
```

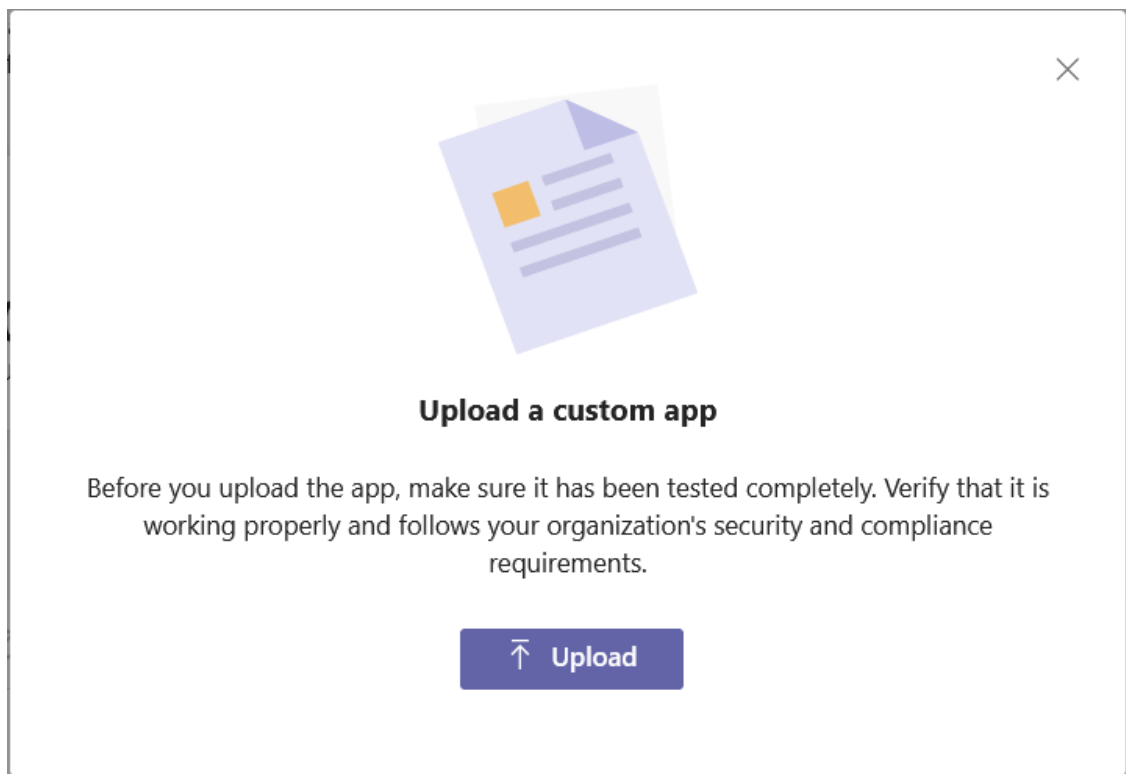
```
"ai-logix.net"], "webApplicationInfo": { "id": "<app_id>", "resource":
"api://smarttapteams poc.bot.ai-logix.net/<app_id>" }}
```

3. In the Navigation pane, select **Teams apps > Manage apps**.



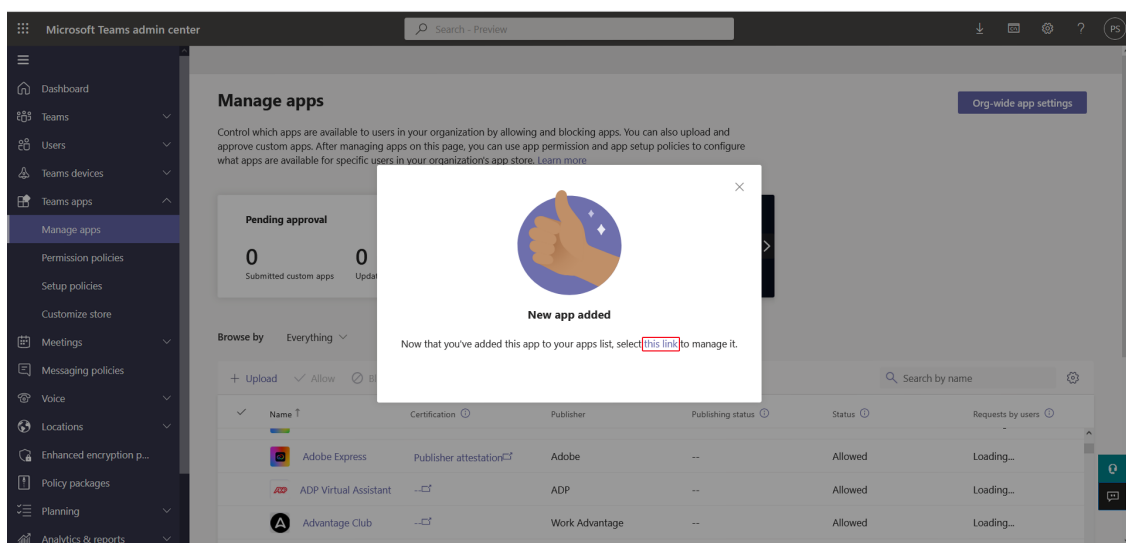
4. Click **Upload**.





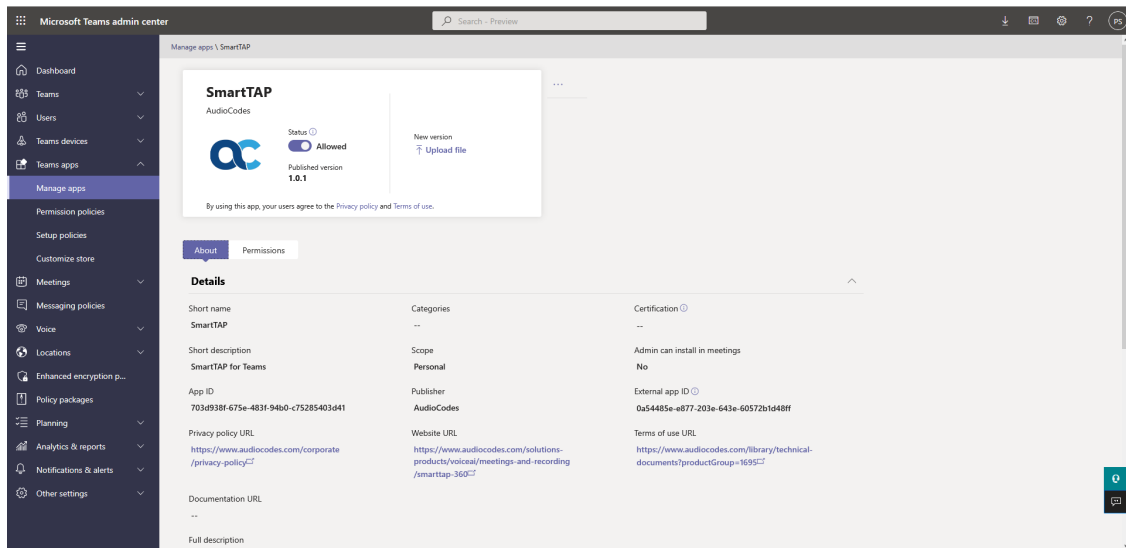
5. Browse to the saved location for **voca1_app.zip** and then click **Upload**.

The following confirmation is displayed.

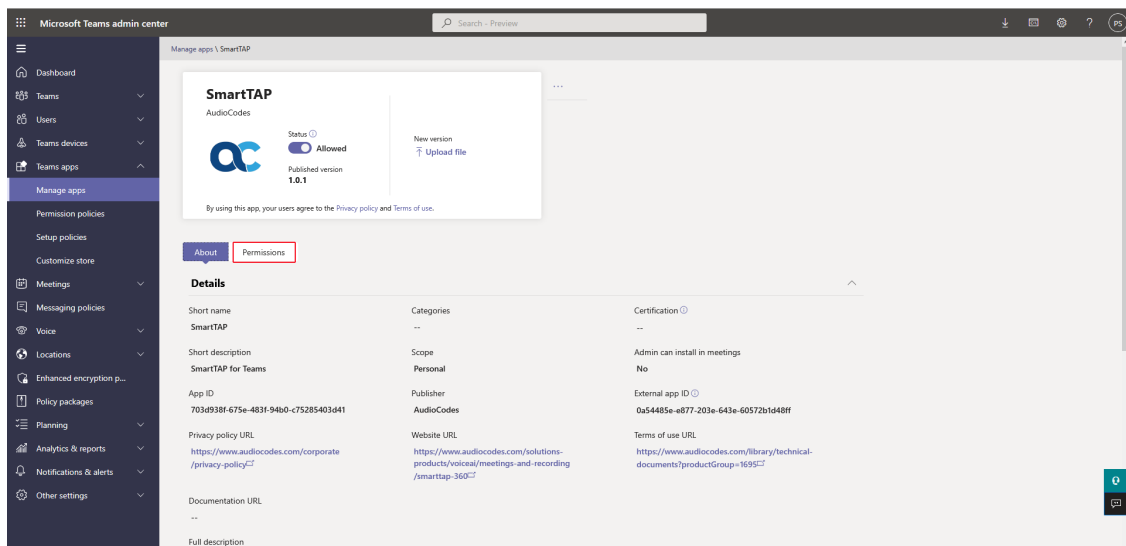


The SmartTAP Personal App is displayed.

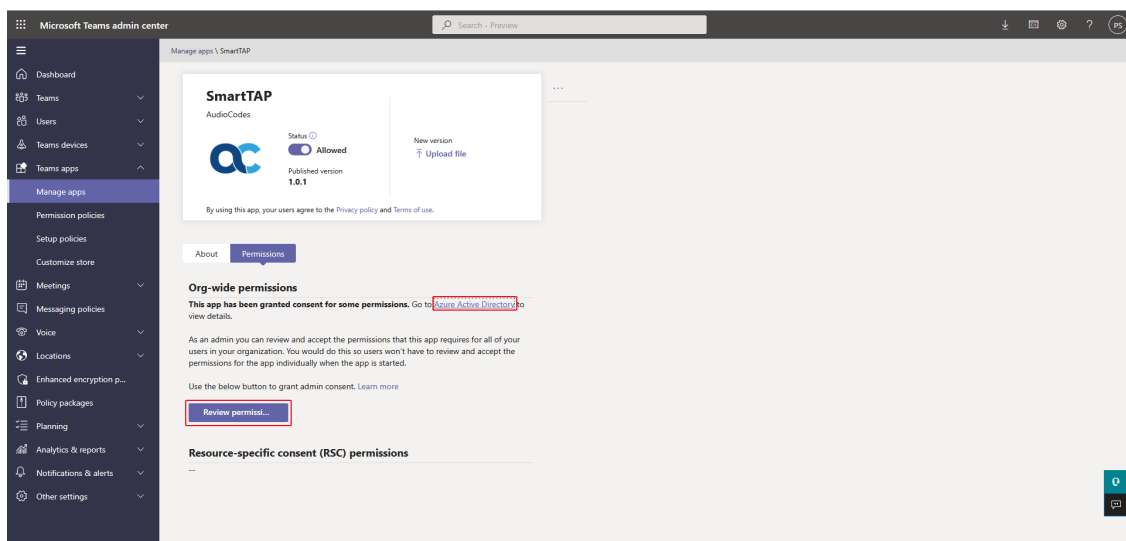
Figure 33-100 SmartTAP Personal App



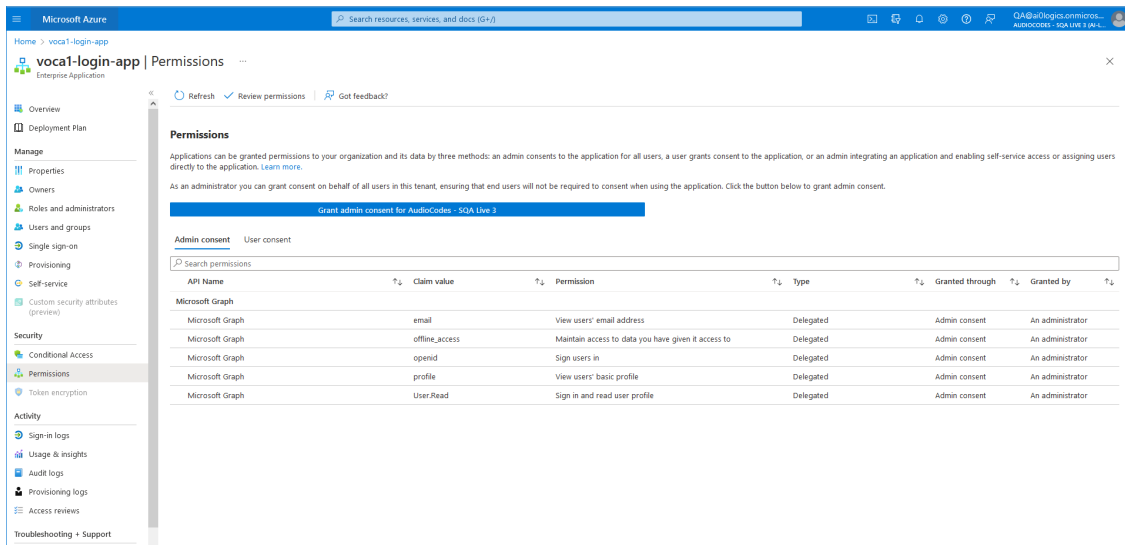
6. Click the **Permissions** tab.



7. Click the **Azure Active Directory** or **Review permissions** link.



A list of permissions for the **login-app** are displayed.



The screenshot shows the Microsoft Azure portal interface for the 'vocal1-login-app' (Enterprise Application). The 'Permissions' tab is selected, displaying a list of permissions granted to the application. A blue button at the top of the permissions list reads 'Grant admin consent for AudioCodes - SQA Live 3'.

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more.](#)

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

Grant admin consent for AudioCodes - SQA Live 3

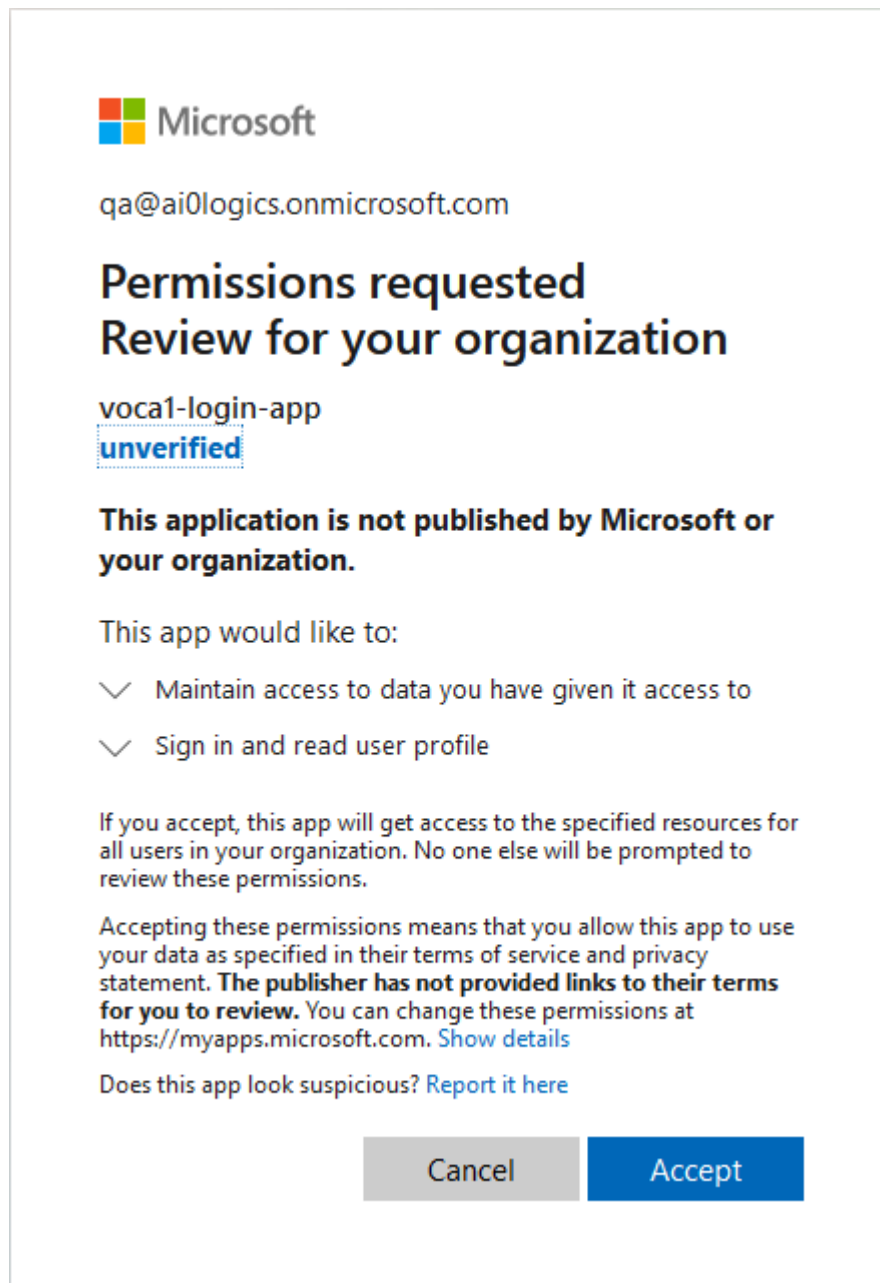
Admin consent User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	email	View users' email address	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read	Sign in and read user profile	Delegated	Admin consent	An administrator

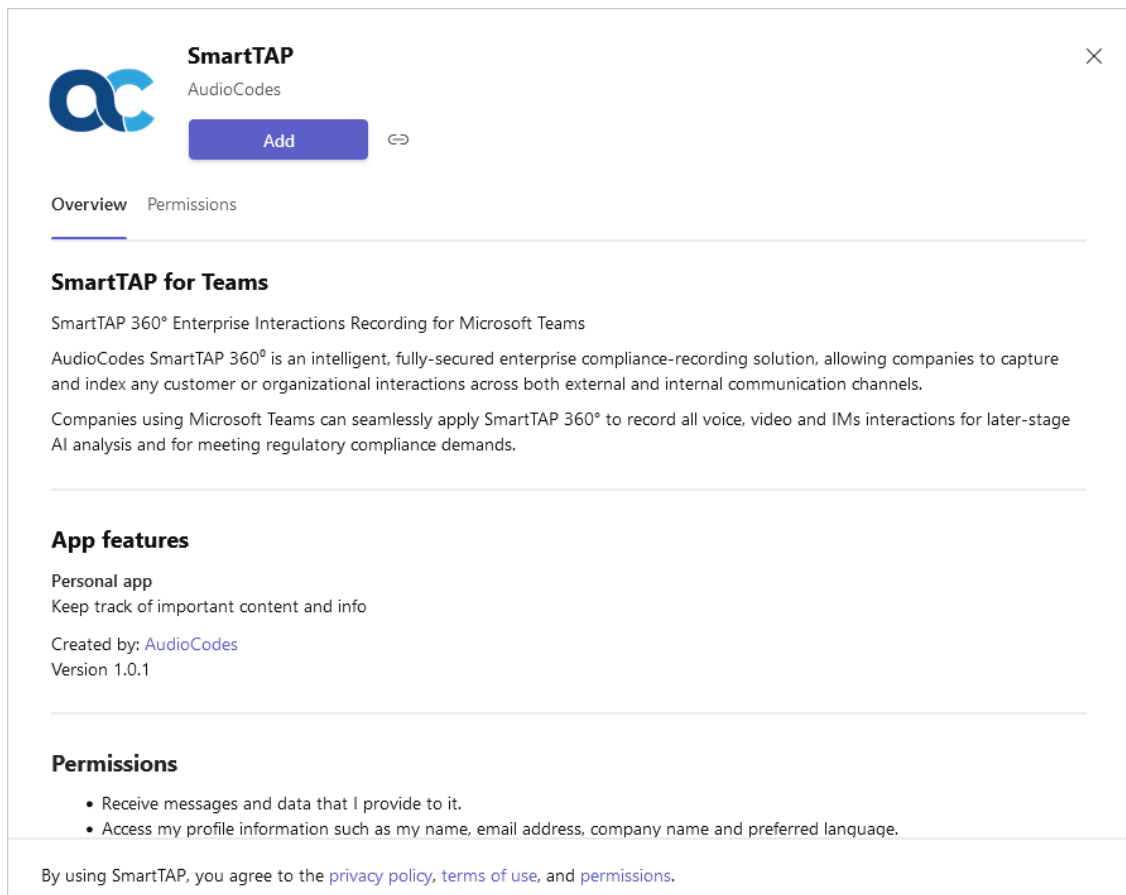
- Click Grant admin consent for <Service Provider Operator>. In the example above **AudioCodes – SQA Live 3**.

Figure 33-101 Login-app Permissions



9. Click **Accept** to provide consent.
10. Open the Microsoft Teams Customer Tenant (using Desktop application only) and search for the SmartTAP app.

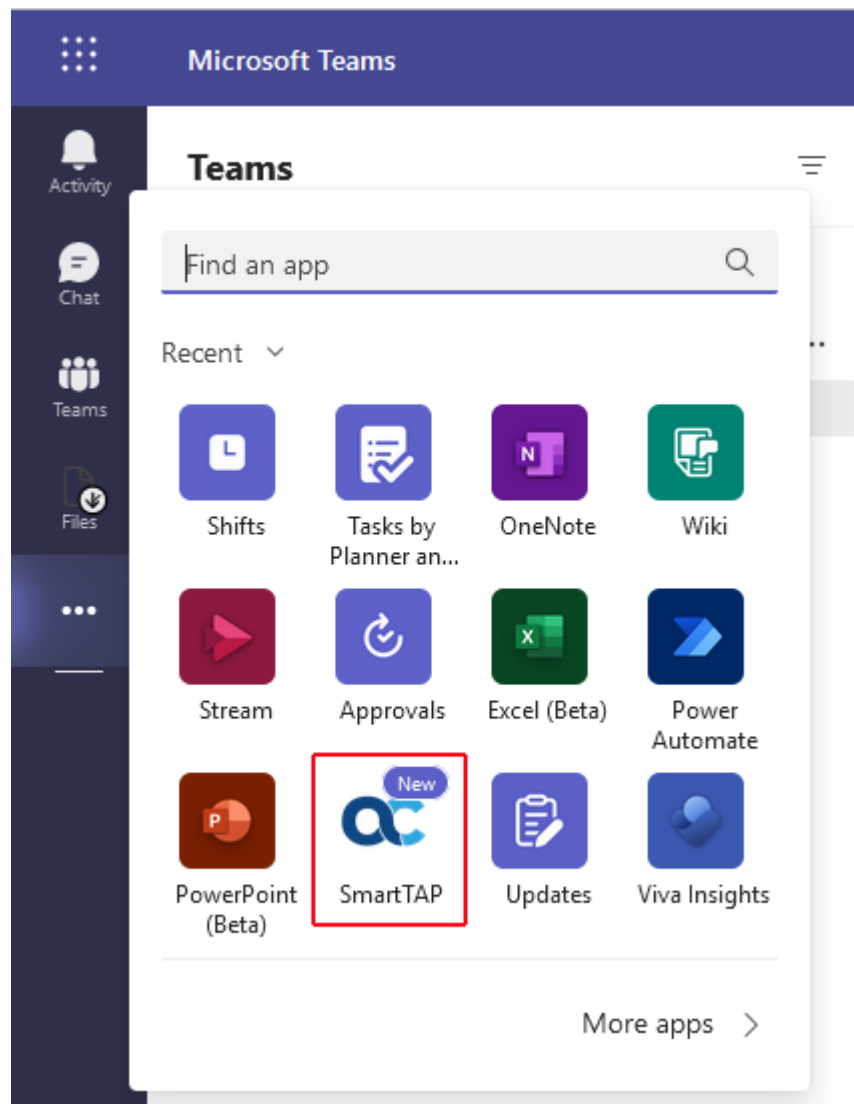
Figure 33-102 Add SmartTAP App



11. Click Add.

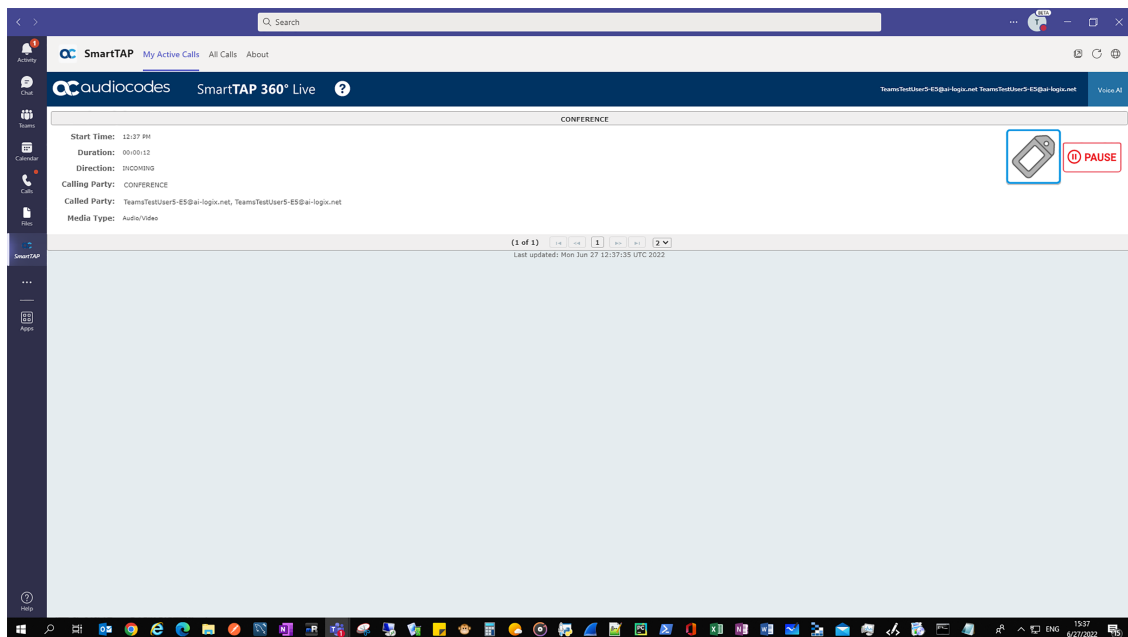
Once successfully added, the SmartTAP app is displayed in the list of apps.

Figure 33-103 SmartTAP App



12. Click the SmartTAP app, the SmartTAP Web interface opens displaying the **My Active Calls** tab.

Figure 33-104 SmartTAP Web



Enable Users with Compliance Recording

This step describes how to configure User Compliance Recording Policy which allows the recording of the users belonging to the group configured in Create Recording Group on Azure. The Microsoft Teams deployment script complianceRec.ps1 assigns M365 users and groups for recording on Microsoft Teams.

➤ To enable users with Compliance Recording:

1. Take the complianceRec.ps1 file from the folder-
..\TerraSmartTap\ComplianceRecPolicy\createRecPolicy.ps1 file.
2. In PowerShell, right-click the script and run "createRecPolicy.ps1".
3. Login to Azure account using the Teams Users Tenant Administrator's credentials.



Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? [Create one!](#)

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

Back

Next

The Compliance tool interface opens displaying a list of existing recording policies.

AudioCodes Recording Compliance Configurator v1.0

Current State of Recording Policies under Teams tenant:

☐ Show paired secondary policies

[Refresh Table](#) [Search By User/Group](#)

Name	Description	Policy Enabled	Azure Bot App ID	Linked SPN User	RequiredDuringCall	RequiredBeforeMeetingJoin	RequiredBeforeCallEstablishment	RequiredDuringMeeting	Audio Notifications
crsrecordingbotpolicy	crs policy	False	08447a53-17ca-4	crs@SmartTap.com	True	True	True	True	True
ComplianceRecordingBot1	Test policy created by admin	True			True	True	True	True	True
ComplianceRecordingBot1	Test policy created by sergein	True			System.Object[]	System.Object[]	System.Object[]	System.Object[]	True
ComplianceRecordingBot1	Test policy created by sergein	True	53210052-c601-4	stteamscompliance	True	True	True	True	True
BotLabPolicyRecordingBot1	Bot lab recording policy	True	a0603c5-d4fb-4	msd.labCompliance	True	True	True	True	True
ComplianceRecordingBot1	Test policy created by michaladnr	True	51c35d6-1664-4	STteamsbotlata@sm	True	True	True	True	True
ComplianceRecordingBot1	Test policy created by michaladnr	True	14c77b2d-b0bc-4	STteamsbotAl@sm	True	True	True	True	True
ComplianceRecordingBot1	Test policy created by michaladnr	True	e9ab82e8-3493-4	STteamsbotQa2@sm	True	True	True	True	True
ComplianceRecordingBot1	Test policy created by michaladnr	True			True	True	True	True	True
STteamsbottestcomp	Test policy created by michaladnr	True	ad41d6c3-670d-4	STteamsbottest@sm	True	True	True	True	True
STteamsbotqa3t	Test policy created by michaladnr	True	e9ab82e8-3493-4	STteamsbotqa3@sm	True	True	True	True	True
STteamsbotstandarb2	Test policy created by michaladnr	True	016c00a-6c73-40	STteamsbotstandar	True	True	True	True	True
STteamsbotcert	Test policy created by michaladnr	True	80f06d8f-c874-4	STteamsbotcert@sm	True	True	True	True	True
STteamsbotapp	Test policy created by michaladnr	True	ebe35ed8-d000-4	STteamsbotapp@sm	True	True	True	True	True
?		True			True	True	True	True	True
TeamsCompliancePolicy	TeamsCompliancePolicy	True			True	True	True	True	True
STteamsbotvsn	Test policy created by michaladnr	True	a7249d32-6335-4	STteamsbotvsn@sm	True	True	True	True	True
STteamsbotqcert	Test policy created by michaladnr	True	f3c0a2d2-b0ec-4	STteamsbotqcert@sm	True	True	True	True	True

[New Policy](#) [Policy Users/Groups Assignment](#) [Exit](#)

4. Click New Policy.

Compliance Policy

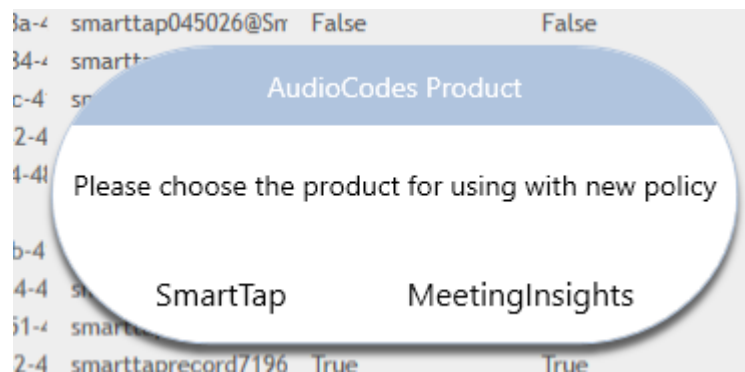
Recording Policy Name:

test for brad

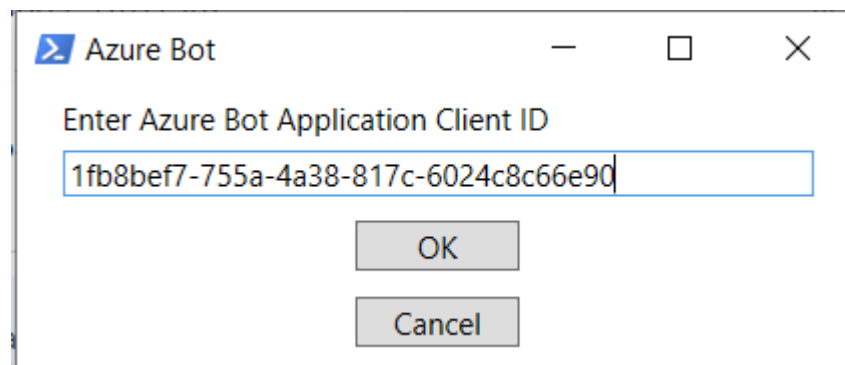
OK

Cancel

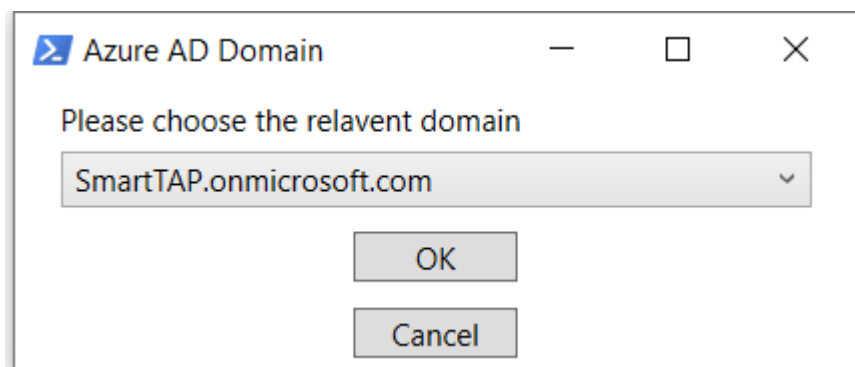
5. Enter a meaningful name and then click OK.



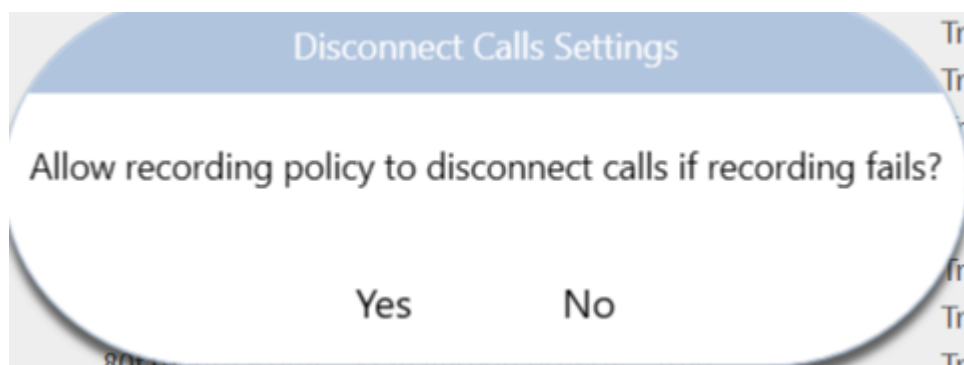
6. Select **SmartTap** as a product.



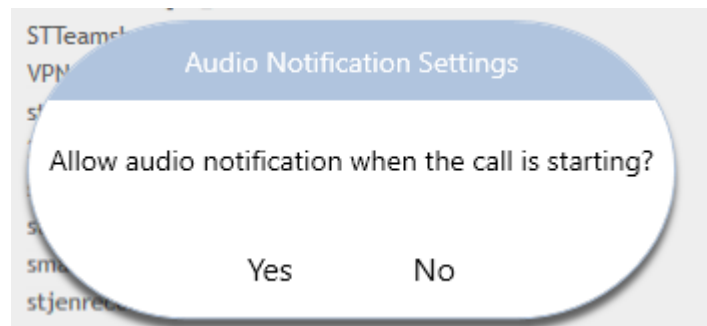
7. Enter the BOT App ID that can be found in file app_registrations.txt "devops5v5-calls-app"...\Ter- raSmartTap\TerraSmartTap\output_data\app_registrations.txt. and then click **OK**.



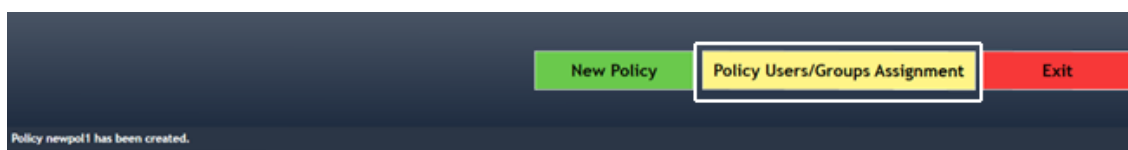
8. Select a tenant where the targeted Teams users resides.



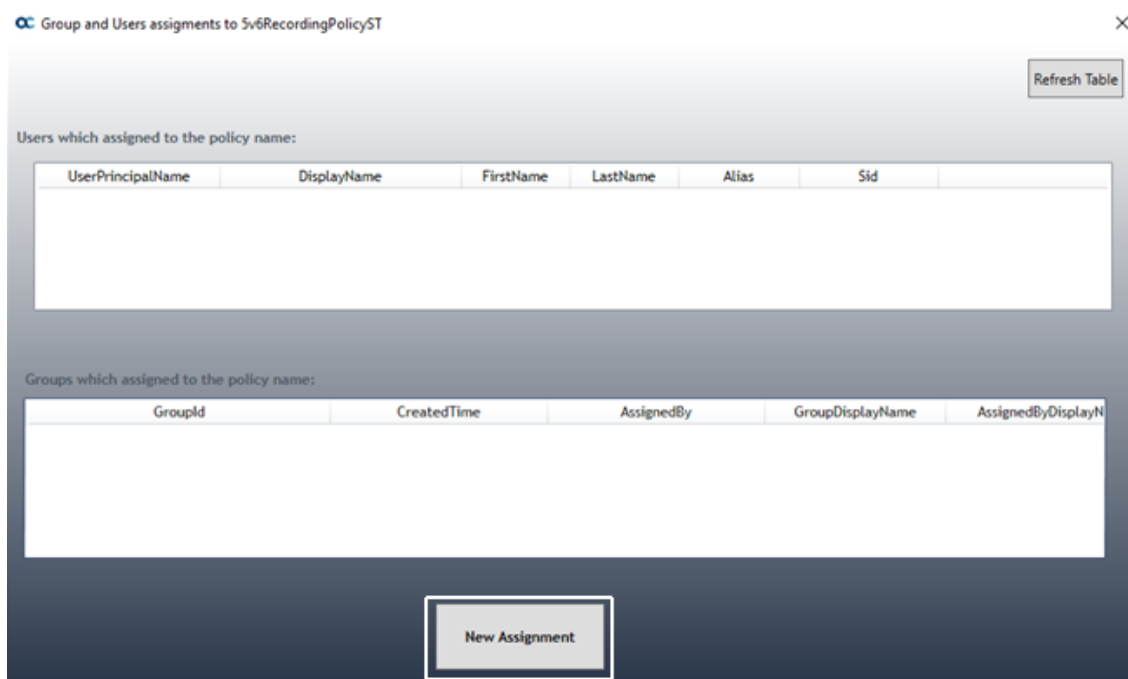
9. Click **Yes** to Allow Recording Policy to automatically disconnect the call if the recording functionality fails.



10. Click **Yes** to play Recording Notification announcement on PSTN calls.
11. Wait for confirmation on policy creation.



12. Select your new policy and click **Policy Users/Groups Assignment** to assign a new policy to Group or Users.



13. Click **New Assignment**.

Figure 33-105 New Assignment

Group and Users assignments to RecPol1

Refresh Table

Users which assigned to RecPol1:

UserPrincipalName	DisplayName	FirstName	LastName	Alias	Sid
-------------------	-------------	-----------	----------	-------	-----

Groups which assigned to RecPol1:

GroupId	CreatedTime	AssignedBy	GroupDisplayName	AssignedByDisplayName
---------	-------------	------------	------------------	-----------------------

Add New Assignment

Please choose the assignment type to policy RecPol1

Users groups

New Assignment

14. Select either **Users** or **groups**.

- **Users:**
 - a. Select **Users**.
 - b. Enter the user principal names.

Figure 33-106 User Principal Names

Add User to Policy

Type user principal names,for multiple user use ","

OK

Cancel

Add User to Policy

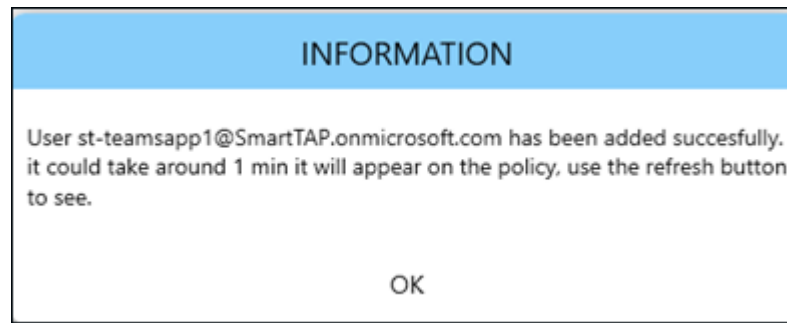
Type user principal names,for multiple user use ","

st-teamsappmi1@meetinginsights.net,st-teamsappmi2@

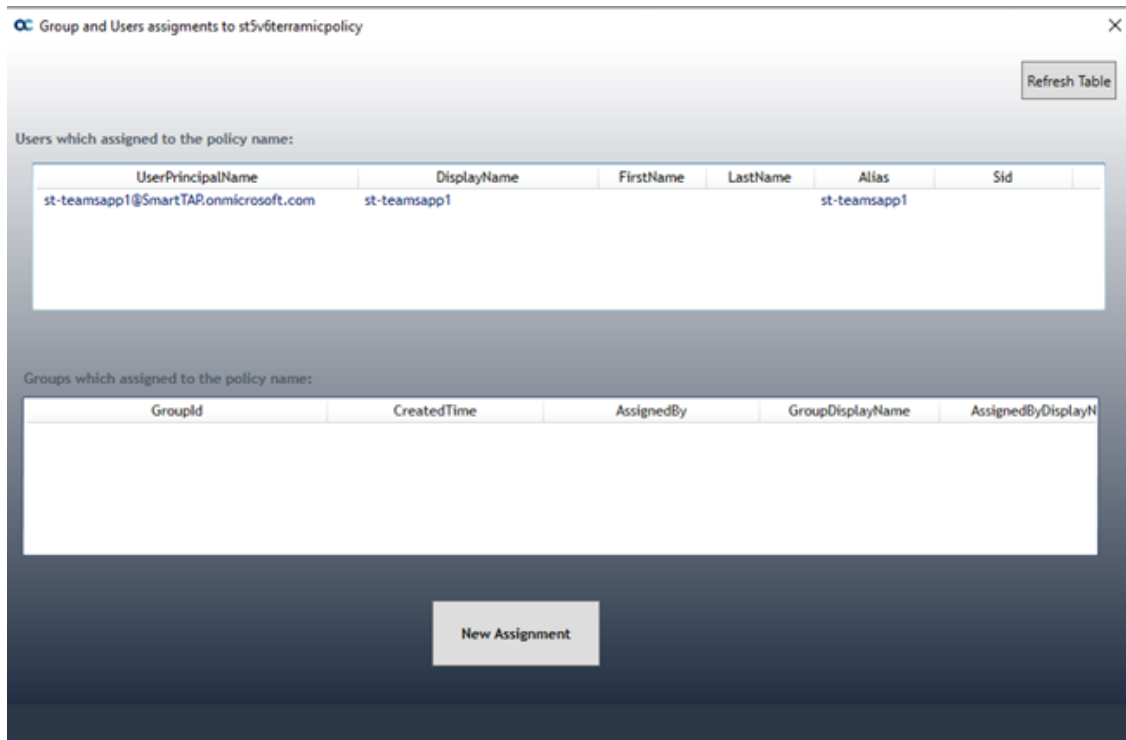
OK

Cancel

- c. Click **OK**, the following confirmation message is displayed.

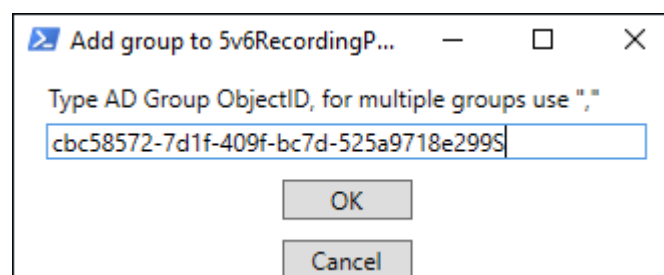
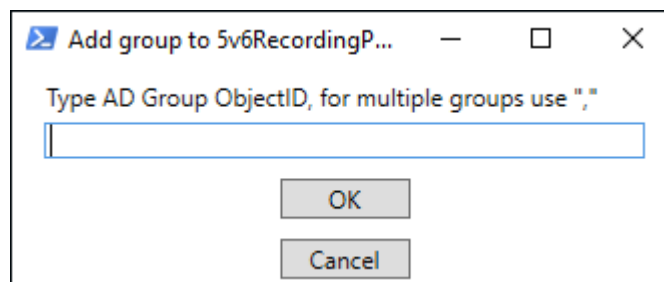


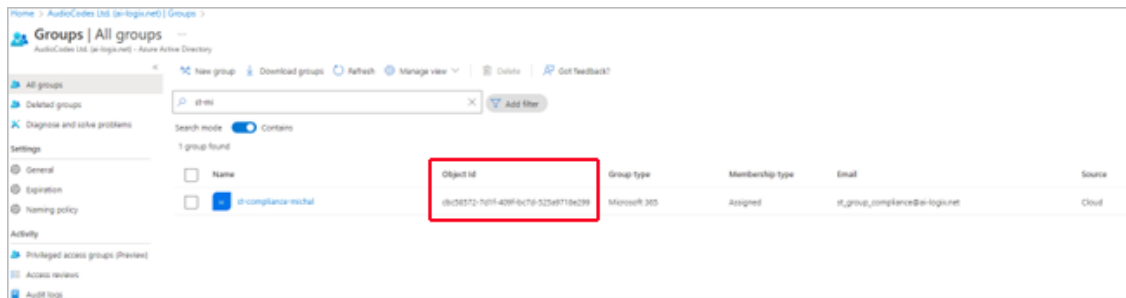
Once refreshed, the new user is visible under Users:



Groups:

- d. Select Groups.





- e. Enter group Object ID extracted from the Group's properties in Azure.
- f. Click **OK**, a confirmation message is displayed.

34 Media Exporter

Media Exporter is a separate desktop application useful for compliance officers or for those who need to download bulk calls from SmartTAP 360° for a specific user or for all users within a date/time range.



The number of exported recordings is limited to 1500. The download time depends on the system specifications and load. It takes approximately 10-15 minutes to download 100 call recordings with an average duration of 5 minutes on an idle system with 4 cores. It is not recommended to export a higher number of records during system working hours.

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

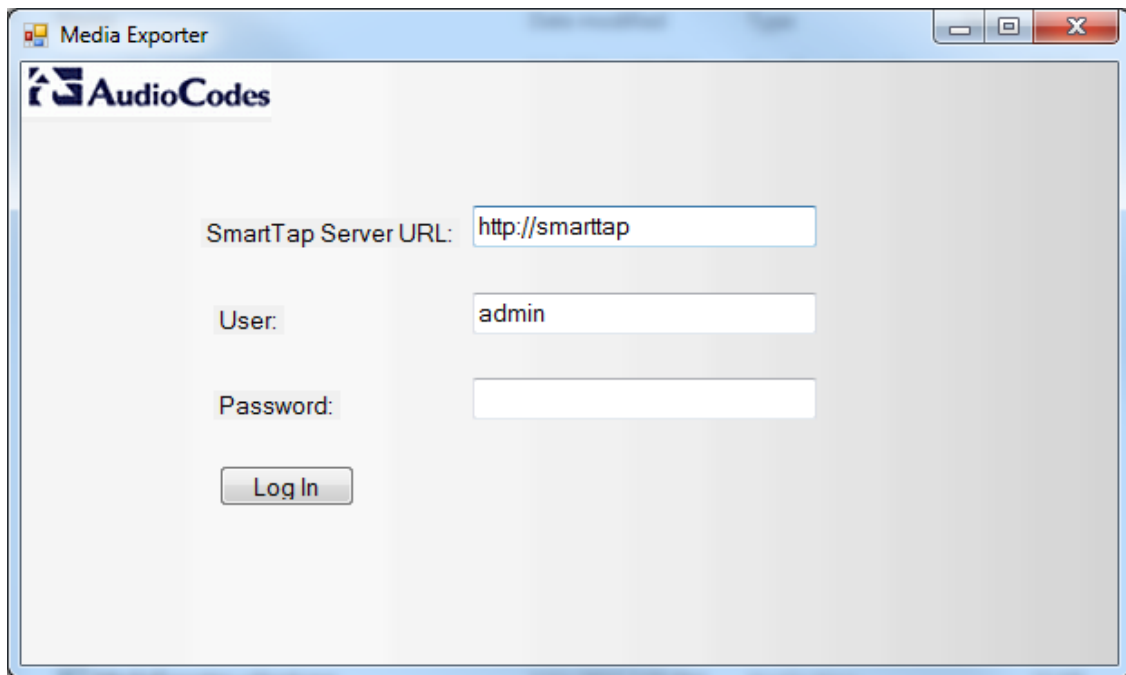


Currently both audio and video call types can be exported together. The video component of video calls is not exported in the current version. Alternatively, only the audio of video calls is exported in this version.

➤ To run the Media Exporter:

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

Figure 34-1: Credentials



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

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

3. Enter the Search Criteria.

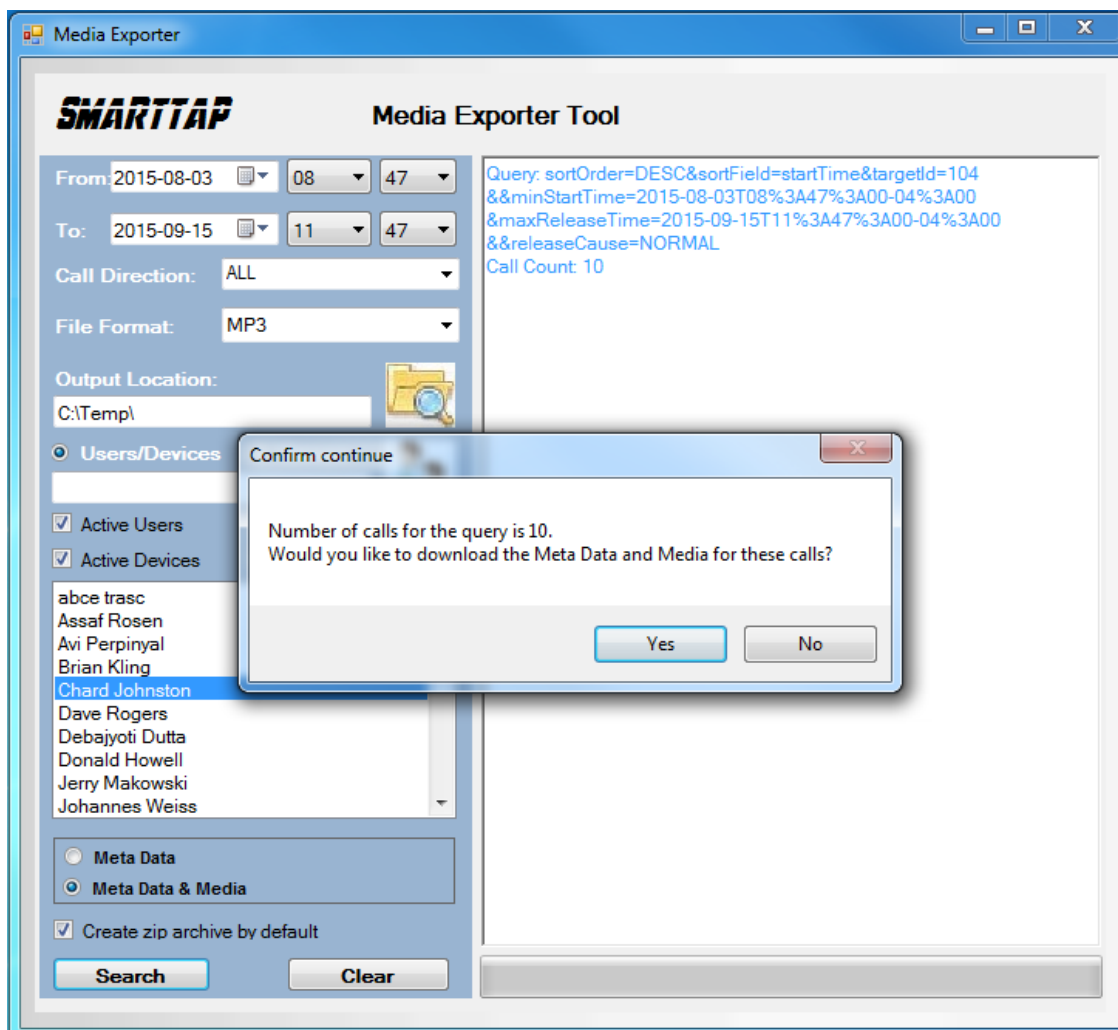
Figure 34-2: Enter the Search Criteria

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
- Search Criteria:**
 - ☒ 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

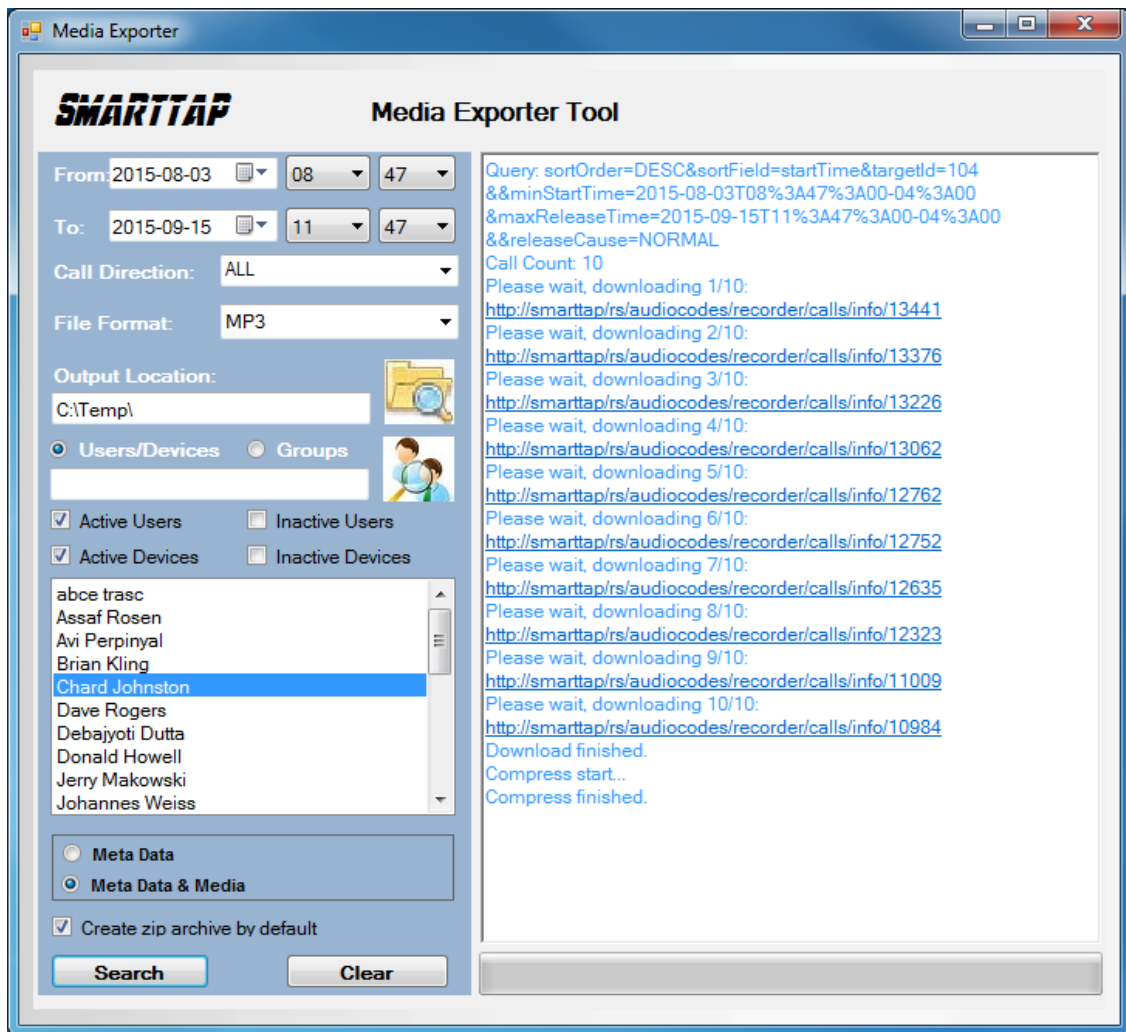
- The following search criteria definitions are identical to those of the SmartTAP Web interface:
 - ◆ File Format (MP3, WAV) Either format can be played using standard Media Player
 - ◆ Output location: Where do you want the zip file and contents to be saved?
 - ◆ Meta Data or Meta Data & Media: Download 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 34-3: Search Results



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

Figure 34-4: Downloading



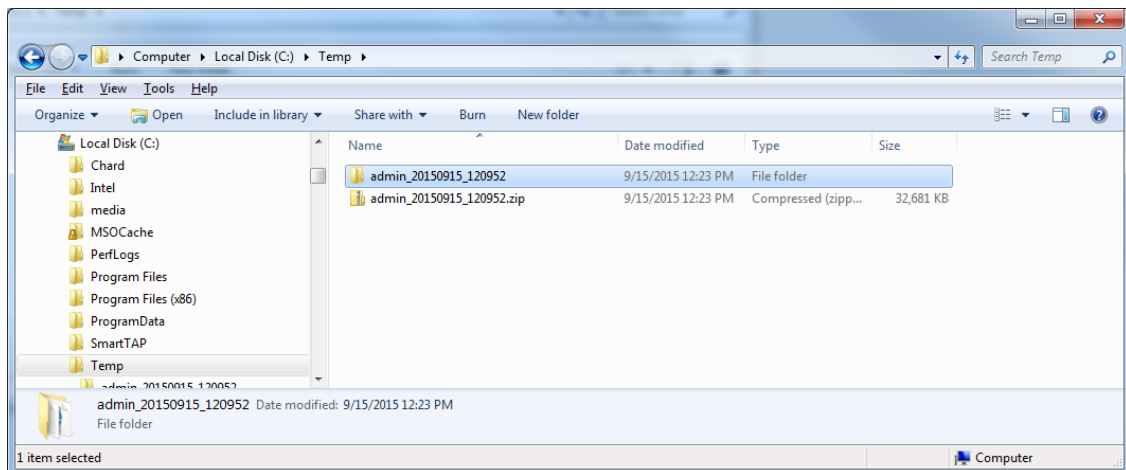
After the download completes, the default browser automatically opens presenting the Call Manifest for the calls from the search results.

Figure 34-5: Call Manifest

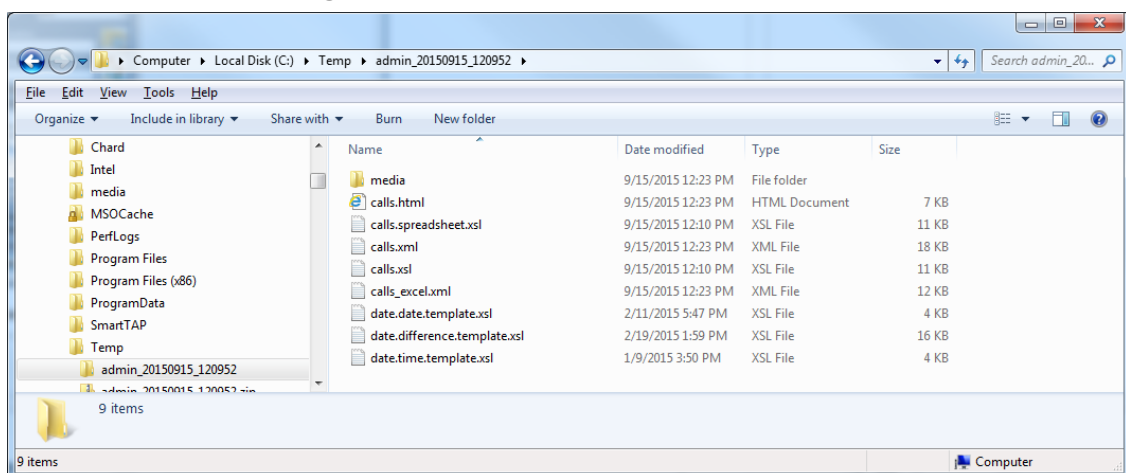
The screenshot shows a web browser window displaying the 'Call Manifest' table. The table lists call details for Chard Johnston, including dates, times, durations, directions, and parties. The 'Play' column contains links to audio files.

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 Blancquart	conf-Philippe Blancquart		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 34-6: Output Location

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

Figure 34-7: Contents of Folder

- **Calls.html:** Call Manifest
- **Calls.xml:** Call Meta Data exported from SmartTAP 360° loaded with Calls.html
- **Calls_excel.xml:** Open file in Excel. Once in, Excel can be used to generate statistics and reports.

35 API Integration

The SmartTAP 360° API is a RESTful Web Services API that provides complete access to and control over the SmartTAP 360° platform. The API provides:

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

Try the following example from your browser. Enter in the address bar:

<http://url/rs/audiocodes/recorder/calls/info>



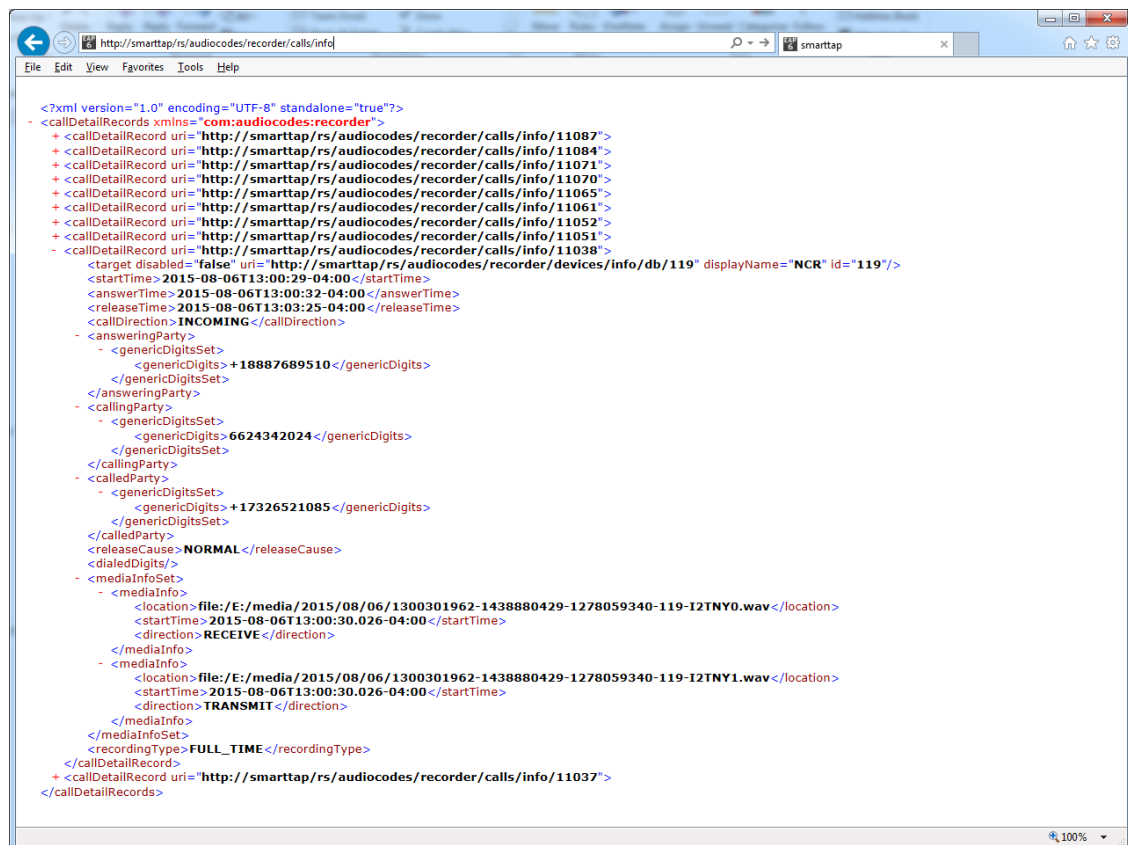
Change 'URL' to the IP address or the name of your SmartTAP 360° product.

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

/calls - SmartTAP 360° Rest API resource

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

Figure 35-1: API Integration



To learn more about the SmartTAP 360° REST API, see the HTML documentation included with the SmartTAP 360° software distribution.

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.

80 Kingsbridge Rd
Piscataway, NJ 08854, USA
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>

©2023 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, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience 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-27606

