AudioCodes SmartTAP[™] 360°

SmartTAP 360°

SmartTAP 360° Enterprise Recording Solution

Version 5.1



Notice

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

This document is subject to change without notice.

Date Published: August-03-2020

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

Related Documentation

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

Document Revision Record

LTRT	Description		
27191	Added Sections: Enabling Opus Recording on the SmartTAP 360° Media Server; Configuring Opus in SIPREC; Example for Creating a Self-signed Certificate; Installing the Application Service; Installing SmartTAP 360° Application Server; Example for Creating a Self-Signed Certificate for CD-SIPREC and SBC Connection (Create a Certificate Signing Request (CSR); Sign the Certificate at the Certificate Authority (CA); Import Certificate to CD_SIPREC Certificate Store); Generating Certificates Automatically; Generated Certificates Manually Updated Sections: Verify the Target List in Each Call Delivery; Media Delivery (MD); Configuring Gateway & SBC for SIP Recording; Windows Event Log; Editing Media Proxy Server Parameters; Step 3-Configuring Announcement Server (Skype for Business); Active / Standby Resiliency Configuration (Optional); Microsoft Hyper-V; Supported Microsoft Windows Platforms; Media Server and Remote Transfer Service with HTTPS; Installation Prerequisities		
27192	Updated figure in Section Skype for Business Recording; Updated table SmartTAP Server - INBOUND Firewall; Updated table Edge, Mediation or Conference Server(s) - Outbound Firewall		
27193	Added Section: Microsoft Teams Deployment Specifications Updated Sections: Active / Standby Resiliency Configuration (Optional); Installing the Remote Transfer Service; Skype for Business Recording Firewall; Edge, Mediation or Conference Server(s); SmartTAP 360° Server (Firewall); SmartTAP 360° Media Proxy Server; Manual Disabling of HTTP		

Table of Contents

1	Hardware and Software Requirements	1
	Server Configurations	. 1
	Microsoft Teams Deployment Specifications	4
	Network Adapter Configuration	. 5
	General Configuration	5
	VMWare Specific	. 5
	Telephony Integration Hardware	. 6
	Add-On Blades	. 6
	Power Requirements	. 6
	Antivirus Software	6
		. (
	Supported Microsoft Windows Platforms	. (
	Windows Updates	(
	Installing Windows Updates	. (
	Supported Virtual Machine (VM) Environments	. /
	Miwale ESA	. / g
	Active / Standby Resiliency Configuration (Ontional)	0
	HTMI 5 Media Player Browser Support	. 0
2		10
2		10
	License File Creation and Installation	.10
	License File Creation	. 10
	License File Installation and Ventication	.11
-	Smartrar 500 Opgrades	
3	Before Installing SmartTAP 360°	.13
	SmartTAP 360° Software Package Contents	.13
	Installation Prerequisites	13
	Installation Wizard Methods	15
	All-In-One	.15
	Distributed	.15
	Post Installation Actions	.15
4	Installation Wizard - All-In-One Method	17
	Database Service	.19
	Installing the Application Service	.20
	Installing the Communication Service	.24
	Installing the Call Delivery Service	.25
	Installing the Media Server	.27
	Installing the Remote Transfer Service	.28
	Completing Wizard Installation	.30
	Post-Installation Integration	.31

5	Installation Wizard - Distributed Method	
	Installing SmartTAP 360° Database Server	34
	Database Service Configuration	
	Installing SmartTAP 360° Application Server	
	Installing SmartTAP 360° Communication Server	
	Installing SmartTAP 360° Media Server	
	Media Server Configuration	
	Network File Server	
	Media Server	41
	Installing SmartTAP 360° Call Delivery Server	
	SmartTAP 360° File Server Installation	43
	Firewall Configuration	
	Domain Controller Configuration	
6	Uninstalling SmartTAP 360°	
7	Firewall Configuration	51
	Skype for Business Recording Firewall	51
	Front End Server(s)	
	Edge, Mediation or Conference Server(s)	
	SmartTAP 360° Server	
	SmartTAP 360° Media Proxy Server	
	SmartTAP 360° Announcement Server	
	Automated Firewall Exception Scripts for Windows Firewall	
	Distributed SmartTAP 360° Firewall	56
	Application Server (AS)	
	Communications Server (CS)	
	Database Server (DB)	58
	File Server (FS)	58
	Media Server (MS)	58
	Remote Transfer Service (RTS)	
	Call Delivery(CD)	
	Media Delivery (MD)	60
	Media Proxy (MP)	60
	Announcement Server (AN)	61
	Example	61
8	Microsoft Skype for Business Deployment	62
	Skype for Business Remote Branch Site	63
	Before Installing Microsoft Skype for Business Components	65
	Annoucement Server-Specific Requirements	
	Firewall Configuration	
	SmartTAP 360° Monitoring Service-Specific Requirements	
	Installing Skype for Business Plugin	67
	Skype for Business Plugin-Pre-install Setup on AD Domain Controller	67
	Skype for Business Plugin Pre-install Setup on each Front End, SBS or SBA	71

	Skype for Business Plugin Installation Procedure	80
	Installing Call Delivery for Skype for Business (IP-based Recording)	87
	Monitoring	89
	Edge	94
	Firewall Exceptions	96
	Configuring Media Proxy for Call Delivery-IP	96
	Configuring Call Delivery for Skype for Business	99
	Installing Media Proxy Server for Skype for Business	.100
	Editing Media Proxy Server Parameters	.107
	Installing Media Delivery Server for Skype for Business	.108
	Installing Announcement Server	109
	Announcement Server Preinstall of Core Components and Local Replica Configuration Store	.110
	Announcement Server Software Installation Procedure	.114
	Annoucement Server-Post Installation Procedures	119
	Step 1-Activate Annoucement Services	. 119
	Step 2-Add Annoucement Servers to DNS	. 120
	Step 3-Configuring Announcement Server (Skype for Business)	. 120
	Installing SmartTAP 360° Monitoring Service	121
	SmartTAP 360° Monitoring Service Installation Procedure	. 122
	Activating the SmartTAP 360° Monitoring Service	123
	Configuring the SmartTAP 360° Monitoring Service	.124
9	Integration Configuration	127
	VoIP Port Mirroring	127
	VoIP Port Mirroring Inbound / Outbound	.127
	VoIP Port Mirroring Inbound / Outbound Station to Station	. 127 127 . 127
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror)	. 127 127 . 127 . 128
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring	.127 .127 .127 .127 .128 131
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces	. 127 . 127 . 127 . 128 . 131 . 133
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio	.127 .127 .127 .128 .131 .133 .134
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap)	.127 .127 .127 .128 .131 .133 .134 .136
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio	.127 .127 .127 .128 .131 .133 .134 .136 .138
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 141
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec)	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 141 142
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec?	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 141 142 .142
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS)	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 141 142 .142 .142
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS) Session Recording Client (SRC)	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 .141 142 .142 .143 .143
	VoIP Port Mirroring . Inbound / Outbound . Station to Station . Call Delivery Install for VoIP (Port Mirror) . Additional Configuration for VoIP Port Mirroring . Setting Up Monitoring Interfaces . Analog Trunk / Radio . Call Delivery Install for Analog Recording (Passive Tap) . Additional Configuration for Analog Trunk and Radio . Activity Detection . SmartCONTROL . SIP Recording (SIPRec) . What is SIPRec? . Session Recording Server (SRS) . Session Recording Client (SRC) . Configuring Gateway & SBC for SIP Recording .	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 141 142 .142 .142 .143 143 .143
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS) Session Recording Client (SRC) Configuring Gateway & SBC for SIP Recording Configuring Load Balancing on the SBC Device	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 .141 142 .142 .143 .143 .143 .143
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS) Session Recording Client (SRC) Configuring Gateway & SBC for SIP Recording Configuring Load Balancing on the SBC Device Configuring Alternative Routing on the SBC	.127 .127 .127 .128 .131 .133 .134 .134 .136 .138 .140 .141 142 .142 .142 .143 .143 .143 .144 .145
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS) Session Recording Client (SRC) Configuring Gateway & SBC for SIP Recording Configuring Load Balancing on the SBC Device Configuring Alternative Routing on the SBC Installing SmartTAP 360° for SIP Recording	.127 .127 .127 .128 .131 .133 .134 .133 .134 .136 .138 .140 .141 142 .142 .142 .143 .143 .143 .143 .144 .145 .146
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS) Session Recording Client (SRC) Configuring Gateway & SBC for SIP Recording Configuring Load Balancing on the SBC Device Configuring Alternative Routing on the SBC Installing SmartTAP 360° for SIP Recording Configuring Call Delivery for SIP Recording	.127 .127 .127 .128 .131 .133 .134 .136 .138 .138 .140 .141 142 .142 .142 .143 .143 .143 .144 .145 .146 .147
	VoIP Port Mirroring Inbound / Outbound Station to Station Call Delivery Install for VoIP (Port Mirror) Additional Configuration for VoIP Port Mirroring Setting Up Monitoring Interfaces Analog Trunk / Radio Call Delivery Install for Analog Recording (Passive Tap) Additional Configuration for Analog Trunk and Radio Activity Detection SmartCONTROL SIP Recording (SIPRec) What is SIPRec? Session Recording Server (SRS) Session Recording Client (SRC) Configuring Gateway & SBC for SIP Recording Configuring Load Balancing on the SBC Device Configuring Alternative Routing on the SBC Installing SmartTAP 360° for SIP Recording Configuring Call Delivery for SIP Recording Configuring Call Delivery for SIP Recording	.127 .127 .127 .128 .131 .133 .134 .136 .138 .140 .141 142 .142 .142 .143 .143 .143 .143 .143 .144 .145 .146 .147 .148

_		
Co	nto	nt.
CU	IILE	:110

	Adding SmartTAP 360° to the Genesys PureCloud Contact Center User Interface	151
10	Additional Configuration Options	154
	Configuring Digital Signatures	154
	Configuring the SmartTAP 360° Web Interface	
	Configuring the PC Client	154
	Configuring LDAP	155
	Pre-Requisites	
	Configuring SSO	155
	Configuring HTTP/S	156
	Disabling HTTP Communications on Application Server (Optional)	
	Automatic Disabling of HTTP	
	Manual Disabling of HTTP	157
	Configuring SmartTAP 360° Components for HTTPS	
	Communication Server with HTTPS	158
	Call Delivery with HTTPS	
	Media-Proxy with HTTPS	159
	Announcement Server with HTTPS	159
	Remote Transfer Service with HTTPS	
	Health Monitor with HTTPS	
	Media Delivery with HTTPS	161
	Configuring Syslog Server Connection	
	Skype for Business Plug-in	161
	Location-Based Targeting in SmartTAP 360°	
	Assign a Location Attribute to each Call Delivery Component	
	Create a Location Attribute in the SmartTAP 360° GUI	165
	Assign a Location to Each User/Device in the SmartTAP 360° GUI	166
	Verify the Target List in Each Call Delivery	
	CD-SIPREC Configuration	
	CD-SIPREC Support in TLS Transport	170
	Generating Certificates Automatically	
	Generating Certificates Manually	172
	Example for Creating a Self-Signed Certificate for CD-SIPREC and SBC Connection	173
	Create a Certificate Signing Request (CSR)	173
	Sign the Certificate at the Certificate Authority (CA)	
	Import Certificate to CD-SIPREC Certificate Store	174
	Enabling OPUS Codec Recording in SmartTAP 360°	174
	Configuring Opus on Media Server	175
	Configuring Opus for CD-SIPREC	
11	Backup and Restore	177
	Prerequisites	177
	Backup	178
	Call Delivery Service	
	Media Service	

	Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server	170
	Communication Service	179
	Application Service	180
	Database	180
	SmartTAP 360° Skype for Business Plug-in (FE_SBS_SBA)	180
	SmartTAP 360° Announcement Server	181
	SmartTAP 360° Media Proxy	181
	Media	181
	System Profile Tool	182
	Restore	182
	Call Delivery Service	
	Media Service	183
	Media Delivery Service	184
	Database	184
	SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA)	184
	Announcement Server	185
	Media Proxy	
	Restoring Media	185
12	Troubleshooting	187
	How To Validate Port Mirror for Recording Skype for Business Calls	187
	Prerequisites	187
	Introduction: SmartTAP 360° Recording Concepts	
	SmartTAP 360° Processing of Skype for Business Signaling	
	SmartTAP 360° Media Processing	188
	Procedure	189
	Setup Skype for Business Logging	189
	Setup Sniffer	
	Capture a Test Call	190
	Analysis	191
	Locate Test Call in Skype for Business Log	191
	Compare Call Information with Sniffer Trace	193
	Determine Whether SmartTAP 360° will Record this Call	193
	Troubleshooting Skype for Business Plugin Installation	193
	Enable the Browser Service	193
	Use "net view" to Verify	194
	Troubleshoot Skype for Business Recording	194
	No Records for the Calls	194
	Calls with No Audio	195
	Enabling Promiscuous Mode on VMWare ESXi	195
13	Known Issues	196
	Internet Explorer Security Messages and SmartTAP 360° not Running on Server \dots	196
14	Configure Microsoft SNMP Service	197

Automatic SNMP Setup	197
Manual SNMP Setup	.198

1 Hardware and Software Requirements

This chapter describes the hardware and software requirements for installing SmartTAP 360°.

Server Configurations

The following table lists the maximum available resources for three different SmartTAP 360° server profiles and for the Media Proxy and Announcement servers.

Resources refers to Audio, Video, Announcement and Desktop Sharing licenses.

Server	Specification	Available Resources
SmartTAP 360°	2 Core 2.5 GHz	50 resources (audio only)
server (Low Profile)	6 GB Memory	25 resources when Media
	2 SATA 7200 RPM HDD* PCIe slots FL / FH2**	the same server (audio
		only)
SmartTAP 360° server (Medium Pro-	6 Cores 2 GHz****	150 resources
file)	8 GB Memory	50 resources when Media
	PCIe slots FL / FH2**	the same server (audio
		only)
SmartTAP 360° server*** (High Pro-	12 Core 2 GHz****	300 resources 500 audio resources
file)	2 SATA 7200 RPM HDD*	
	PCIe slots FL / FH2**	
Media Proxy	Quad Core 2 GHz (300	300 resources
	 8 Core 2 GHz (500 audio resources) 	Sou audio resources
	8 GB Memory	
	SATA 7200 RPM HDD	
Announcement server***	Quad Core 2 GHz	300 resources (assuming the announcement length
	8 GB Memory	

Figure 1-1: SmartTAP 360° Server

Server	Specification	Available Resources
	SATA 7200 RPM HDD	does not exceed 20% of an average call length)

* SmartTAP 360° server requires two dedicated HDDs - one for the Windows OS, SmartTAP 360° software and DB and another for the recorded media. The media HDD is required for both local or remote media storage (in the case of remote storage it is used for intermediate storage of the media). When running the SmartTAP 360° Server in a virtual environment, the HDDs has to be dedicated and mapped to SmartTAP 360° server VM.

** PCIe Full Length / Full Height slots. The number of slots required is determined by the number of Analog Stations required to record. Each card can record 24 channels (i.e., 56 Phones will require three PCIe card slots).

*** A group of these servers can be deployed when more than the supported recording capacity in one server is required. An additional high-end server is required to be deployed for the Application Server and Database.

**** Higher CPU speed (higher than 2.0 GHz) is recommended to accelerate download and playback for Video and Desktop sharing recorded calls.

- When running in a virtual environment, all specification resources in the table above must be reserved for all servers of SmartTAP 360°.
 - Dual GB NIC interfaces are required for VoIP Port Mirroring Integration Configuration (this is not relevant for Skype for Business and SIP Recording)

To determine the server specification, calculate the required available resources. The calculation of the required resources is based on the number of licenses multiplied by one of the factors specified in the table below.

License Type	Factor
Audio Recorder License	1
Video Recorder License	10
Announcement License	1
Desktop Sharing	5

Figure	1-2:	License	Factors
--------	------	---------	---------

Calculate the required number of resources on the SmartTAP 360° server and the Media Proxy server according to the following formula:

Required Number of Resources = (Number of Audio Recorder Licenses)*(Audio Recorder License Factor) + (Number of Video Recorder Licenses)*(Video Recorder License Factor) + (Number of Desktop Sharing Recorder Licenses)*(Desktop Sharing Factor) Choose the SmartTAP 360° server and Media Proxy server with the number of available resources equal or higher than the required recording resources.

Calculate the required number of resources on the Announcement server according to the following formula:

Required Number of Resources = (Number of Announcement Licenses)*(Announcement License Factor)

Example 1: 100 Audio Recorder Licenses

- Required Number of Resources = (100 Audio Recorder Licenses)*(1 Audio Recorder License Factor) = 100
- Choose Medium Profile SmartTAP 360° server and one Media Proxy server

Example 2: 30 Video Recorder Licenses

- Required Number of Resources = (30 Video Recorder Licenses)*(10 Video Recorder License Factor) = 300
- Choose High Profile SmartTAP 360° server and one Media Proxy server

Example 3: 50 Audio Recorder Licenses and 20 Video Recorder Licenses

- Required Number of Resources = (50 Audio Recorder Licenses)*(1 Audio Recorder License Factor) + (20 Video Recorder Licenses)*(10 Video Recorder License Factor)= 50 + 200 = 250
- Choose High Profile SmartTAP 360° server and one Media Proxy server

Example 4: 40 Audio Recorder Licenses

- Required Number of Resources = (40 Audio Recorder Licenses)*(1 Audio Recorder License Factor) = 40
- Choose either of the following:
 - Medium Profile SmartTAP 360° server with Media Proxy service installed on the SmartTAP 360° server
 - Low Profile SmartTAP 360° server and separate Media Proxy server

Example 5: 200 Audio Recorder Licenses with Announcement

- For SmartTAP 360° server and Media Proxy servers:
 - Required Number of Resources = (200 Audio Recorder Licenses)*(1 Audio Recorder License Factor) = 200
 - Choose High Profile SmartTAP 360° server and one Media Proxy server
- For Announcement server:
 - Required Number of Resources = (200 Announcement Licenses)*(1 Announcement License Factor) = 200
 - Choose one Announcement server

Example 6: 50 Audio Recorder Licenses and 50 Desktop Sharing Recorder Licenses

- For SmartTAP 360° server and Media Proxy servers:
 - Required Number of Resources = (50 Audio Recorder Licenses)*(1 Audio Recorder License Factor) + (50 Desktop Sharing Recorder Licenses)*(5 Desktop Sharing Recorder License Factor) = 300
 - Choose High Profile SmartTAP 360° server and one Media Proxy server

Microsoft Teams Deployment Specifications

This section describes the recommended specifications for the Microsoft Teams BOT Cluster and the SmartTAP 360° Recording solution.

- SmartTAP 360° Server:
 - Operating System: Microsoft Windows Server 2016 or Microsoft Windows Server 2019
 - SmartTAP 360° server with the specifications below can handle up to 3000 targeted users and 500 audio call recordings:
 - Virtual Machine: Tier=Standard, Instance=DS2 v2 (2 vCPUs, 7 GB RAM, 14 GB Temporary storage)
 - SmartTAP 360° server with the specifications below can handle up to a 3000 targeted users and a combination of 500 audio/DAS call recordings.
 - Virtual Machine: Tier=Standard, Instance=F8s v2 (8 vCPUs, 16 GB RAM, 64 GB Temporary storage)
- Microsoft Teams BOT Cluster:
 - Service Fabric Cluster with Silver Durability with a minimum of 5 nodes (for testing or POCs, Bronze Durability with 1 or 3 nodes can be used). For more information, refer to Microsoft Service Fabric Cluster.
 - Single BOT node with the specifications below can handle up to 40 concurrent DAS calls or up to 50 concurrent audio calls. For example, the recording of 150 DAS and 150 audio calls requires 7 nodes:
 - Virtual Machine: Tier=Standard, Instance=D2 v2 (2 vCPUs, 7 GB RAM, 100 GB Temporary storage)
 - Windows Server 2016 Datacenter with Containers
 - Additional mandatory Azure resources:
 - Load Balancer for BOT Service Fabric Cluster
 - Public IP address for the Load Balancer
 - Virtual Machine ScaleSet VMs for BOT Service Fabric Cluster
 - Key Vault to store BOT Service Fabric Cluster certificates
 - Microsoft Azure Blob Storage
 - Optional Azure resources:

- Application Insights to store BOT logs
- App Configuration to store BOT configuration
- SmartTAP 360° for Microsoft Teams availability: SmartTAP 360° for Microsoft Teams availability is based on Azure Virtual Machines (VM) Service Level Agreement (SLA):
 - SmartTAP 360° Server on Azure VM SLA is 99.9% for one instance and 99.99% can be achieved by deploying the two servers in different Availability Zones (optionally available at extra cost). Refer to Azure VM SLA.
 - SmartTAP 360° Teams BOT on Azure VM SLA 99.9%. Refer to Azure VM SLA.
 - SmartTAP 360° Media on Azure BLOB SLA is 99.9% for Hot tier, and 99% for Cool Tier. Refer to <u>Azure Blob Storage SLA.</u>
 - The durability of Azure BLOB using Locally Redundant Storage (LRS) is 11 nines. Refer to Azure Blob Storage Durability.
- SmartTAP 360° for Microsoft Teams Backup/Restore: Azure Virtual Machines (VM) backup/restore procedures are highly recommended.



Network Adapter Configuration

To provide optimal media quality for audio/video (A/V) calls and to cope with unexpected spikes in traffic and increased usage over time, additional network requirements for SmartTAP 360° and MediaProxy servers must be implemented.

General Configuration

- Increase Network Adapter Resources:
 - Receive and Send buffers increase the allocated resources. For receive-intensive scenarios, it is recommended to increase the receive buffer value to at least 8 MB.
- Enable Receive Side Scaling (RSS)
- Offload Features disable Offload operations to ease the load on network adapter
- Suggested Reference:
 - https://technet.microsoft.com/en-us/library/jj574151

VMWare Specific

- Install VMWare tools
- Set network interface adapter type to vmxnet3
- Edit network adapter advanced options:

- Enable "Receive Side Scaling"
- Set "Large Rx Buffer" to at least 8 MB
- Set "Small Rx Buffers" to at least 8MB
- Set "Rx Ring #1/#2 Size" to at least 4MB
- Disable all Offload settings
- Suggested References:
 - https://kb.vmware.com/s/article/2008925
 - https://kb.vmware.com/s/article/2039495

Telephony Integration Hardware

Add-On Blades

Table 1-1: Add-On Blades

Interface	Description	Connector	Gender
Analog	24 channel PCIe Full Length Full Height Card	RJ21x	Female
	6' 180 degree Male to 90 degree female cable included		

- Connect male end of 6' cable to card and female end to in-house wiring.
- All cards are x1 PCI 3.0 compliant. The cards will also function in x4, x8, x16 and Gen 2.0 PCI Express slots.

Power Requirements

Table 1-2: Power Requireme

Interface	+3.3Vdc	+5Vdc	-12Vdc	+12Vdc	Watts
Analog	2.3A	n/a	n/a	n/a	7.6W

Ensure the Power Supply is adequate to support ALL the devices installed in the server not just the Add-On Blades.

Antivirus Software

- No virus software is included with SmartTAP 360°
- No specific virus software is tested or certified
- If installed, do not scan the following folders and contents to prevent performance impact.

Media path: (i.e., Local D:\Media, SAN or NAS)

- …\Ai-Logix\
- ...\AudioCodes\
- ...\MySQL\

Windows Defender

It is similar to Virus software. Please disable scanning same file types and folders.

Supported Microsoft Windows Platforms

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2

Windows Updates

- It is recommended to disable Automatic Windows Updates to prevent unknown side effects.
- AudioCodes only certifies major version Service Pack updates.



Before applying Windows updates, ensure that a system backup is performed.

Installing Windows Updates

- Schedule a maintenance window. SmartTAP 360° does not record during this timeframe.
- Download and install Windows updates.
- Reboot the server, even if Windows does not ask you to reboot to finish installing updates.
- Windows may continue installing updates after the system restart which may cause instability within SmartTAP 360°.
- Once the Windows updates are complete, reboot the server again.

Supported Virtual Machine (VM) Environments

VMware ESXi

- Version 4.1 and higher (IP-based integrations only)
- See the Troubleshooting section for instructions on how to enable promiscuous mode required for a SmartTAP 360° system that is monitoring (tapping) the network.

Microsoft Hyper-V

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 64bit



Hyper-V does not support promiscuous mode. Do not use in Passive integration environments.

Active / Standby Resiliency Configuration (Optional)

AudioCodes supports Microsoft Windows Clustering in the failover configuration, which provides high available service to the SmartTAP 360° application. To support this type of install, the following is required:

- Two identical Windows servers which meet the minimum specifications mentioned above.
- A SAN (Storage Area Network) with iSCSI support. The SmartTAP 360° cluster requires at least 2 Internet Small Computer System Interface (iSCSI) targets one for the disk witness/quorum, and another for the DB and shared application data. A 3rd iSCSI target "Optional" is required for the media storage. SmartTAP 360° should not be configured to write the media directly to the 3rd media target; instead, it should be set as Media Transfer Service destination.

HTML5 Media Player Browser Support

The following table describes the SmartTAP 360° HTML5 player functionality support for web browsers.

The following table describes the supported browser features for each Player function.

SmartTAP 360° HTML5 Player function	Browser Features
Playback	Canvas 2D graphics, AudioElement with MP3 or WebM/Opus support
Wave form rendering	Canvas 2D graphics, AudioElement/ Media Source Extensions with MP3 or WebM/Opus support, Web Audio API
Stereo wave form rendering	Canvas 2D graphics, AudioElement/Media Source Extensions with MP3 support, Web Audio API
Streaming	Canvas 2D graphics, AudioElement/Media Source Extensions with

Table 1-3: HTML5 Media Player Browser Support

SmartTAP 360° HTML5 Player function	Browser Features
	MP3 or WebM with VP8 and Opus support, Web Audio API, Readable streams



The web browser has to support the media framework (browser feature) that SmartTAP 360° utilizes for streaming media as well as for rendering the audio wave forms as described in the table above.

2 SmartTAP 360° License Management

This chapter describes how to calculate the required SmartTAP 360° licenses according to system specifications.

License File Creation and Installation

This section describes how to collect the files that are required for SmartTAP 360° license creation and how to install the license files on the target system. This process applies to SmartTAP 360° 4.0.0 and above.





License File Creation

Two SmartTAP 360° components require licensing: Call Delivery-IP and Call Delivery-SIPREC. Call Delivery-AES, which is no longer supported, also requires licensing. When Call Delivery is installed, it installs a program "GetSystemIdentifier.exe" in the installation directory. This program is automatically run and generates a file called "System-[MachineName].dat", which can be found in the installation directory. This file must be retrieved and sent to AudioCodes to create a license file that is keyed to the customer's hardware.

The default installation directory is found here: C:\Program Files (x86)\AudioCodes\SmartTAP 360°\CD-xx

where xx represents which type of Call Delivery is installed.

If the customer's installation environment changes significantly, it may affect the validation of the license file. If it becomes necessary to generate a new license file, the "GetSystemIdentifer.exe" program can generate a new "System.dat" file simply by double-clicking on the program. No other action is required.

Once the "System.dat" file is delivered to AudioCodes, an authorized employee will create a license file using the purchased license counts from the Purchase Order.

A license file must be generated for each copy of each type of Call Delivery that supports licensing. For example, if the customer requires both CD-IP and CD-SIPREC for their SmartTAP

360° recorder, two license files must be generated. If the customer has 3 sites, each with a copy of Call Delivery-IP installed, then each of the three will require a separate license file.

License File Installation and Verification

Once a license file is generated, it is installed in the Call Delivery installation directory. This is the same location as the "System.dat" file. The default installation directory is found here:

C:\Program Files (x86)\AudioCodes\SmartTAP 360°\CD-xx

where xx represents which type of Call Delivery is installed.

If there are multiple license files, it is important that each one is installed in the location where its corresponding "System.dat" file is found.



Do not mix up the licenses. There is a one-to-one relationship between "System.dat" and "license.lic".

The license file must be named "license.lic". If it has been renamed to help clarify which system it belongs to, the name must be changed back to "license.lic" before Call Delivery can load it.

Call Delivery must be restarted after the license file has been copied into the installation directory. From this moment, the license will take effect (if it has been generated correctly).

To verify the contents of the license file, refer to section "Managing Licenses" in the SmartTAP 360° Administrator Guide. The "Licenses" page under the "System" tab in the SmartTAP 360° User Interface will display the license quantities and meta-data for each license file that is active in the system. If the Customer Name is reported as "Demo", then this indicates that the license has not taken effect.

SmartTAP 360° Upgrades

In general, SmartTAP 360° components are designed to be backward compatible regarding license files. Therefore, when performing an upgrade from one SmartTAP 360° version to another, it is generally not necessary to make any licensing changes with the following exceptions:

- If you are moving any licensed component (like Call Delivery) to another server or virtual machine, you will need to collect a new system.dat file and regenerate the license file. This might occur if you are changing the type of recording solution or the type of PBX being recorded.
- When adding one or more additional RDDs (Remote Data Delivery) as part of the upgrade, treat the additional RDD(s) as new installations and generate license files as described for new installations.

Prior to SmartTAP 360° 4.0, Call Delivery was licensed through SmartWORKS Service. For such systems, the license file was stored in the SmartWORKS installation directory. During the upgrade, the license file is automatically copied into the Call Delivery installation directory with

no changes, and Call Delivery will function as it did prior to the upgrade. There is no intervention required in this case. License files located in the SmartWORKS installation directory for SmartTAP 360° 4.0 and higher are ignored.

A special case occurs if the upgrade involves a SmartTAP 360° solution that includes Media Delivery from a version prior to version 4.0. Before SmartTAP 360° 4.0, Media Delivery relied on SmartWORKS Service, which required a license file. Beginning with SmartTAP 360° 4.0, Media Delivery no longer uses SmartWORKS Service and does not require a license file. Media Delivery will ignore a license file if one is present. Its behavior is controlled by the licenses residing with Call Delivery-IP. A new license file must be generated for CD-IP with sufficient licenses for all of the Media Delivery components to which it communicates. The exact license counts will depend on the customer's existing solution.



Figure 2-2: SmartTAP 360° Upgrades

For upgrades of CD-SIPREC prior to SmartTAP 360° 4.0, a new license file must be generated according to the license quantities originally purchased by the customer. This is done in the same manner as for the CD-IP, which is described above.

3 Before Installing SmartTAP 360°

This chapter describes important information that you should note prior to installing SmartTAP 360°.

SmartTAP 360° Software Package Contents

The installation package must be copied to a directory on the server where the SmartTAP 360° software is to be installed.

Contents	Description
Microsoft Lync and Skype for Business	Includes Microsoft Lync 2013, and Skype-for-Business plugin installers for Front End Server or SBA
REST API Documentation	Contains web based reference material for REST API
RESTApiWrapperLibrary	Contains C# library and web based reference. Use instead of native REST
Suite	Describes the main SmartTAP 360° installation package folder
Tools	Contains various utilities for installing and troubleshooting SmartTAP 360°
SmartTAP 360° Release Notes.pdf	Describes the new features, issues resolved and any known issues for the SmartTAP 360° software release.
SmartTAP 360° InstallationGuide.pdf	Defines the Installation setup for the SmartTAP 360° software.

Figure 3-1: Package Contents (Root Folder)

Installation Prerequisites

Before running the installation wizard, the following prerequisites must be met:

F

For each machine with a Database or Communication Server installed, there must have at least 12 GB on the drive where "mysql" is installed. View the installation path for "mysql" by opening the Services window and viewing the executable path.

- Base Windows 64 bit operating system installation complete without any additional software or features enabled
- Specific SmartTAP 360° hardware must be plugged into the server
- "Optional" PCI cards for Analog Station recording

- Specific SmartTAP 360° network tapping hardware/software must be setup:
 - Depending upon the integration method, Port SPAN/Port Mirror configured and cable with spanned/mirrored traffic connected to the NIC(s) ports that will be recording
 - "Optional" PCI card with cabling connected to the tapping hardware on the customer premises
- Host Server Microsoft SNMP Agent must be installed on the Storage server if different from the SmartTAP 360° server for storage statistics and on the servers in branches (RDD) for system health presentation (for more information, see Configure Microsoft SNMP Service on page 197 below).
- Ensure that the Windows PowerShell script execution policy is set as follows on all of the servers where SmartTAP 360° components are installed:
 - Group Policy "Unrestricted"
 - If Group Policy is not defined, the execution policy of the logged CurrentUser or LocalMachine should be either Unrestricted or RemoteSigned .
 - To check the execution policy, run the following command:

PS> Get-ExecutionPolicy -list

• To change the execution policy, you can run the following commands:

PS> Set-ExecutionPolicy -scope CurrentUser Unrestricted

PS> Set-ExecutionPolicy Unrestricted

PS> Set-ExecutionPolicy -scope LocalMachine Unrestricted

If the permissions are insufficient, the following message is displayed during the installation:

Figure 3-2:	PowerShell	Script	Execution	Policy
-------------	------------	--------	-----------	--------



Do one of the following:

- a. If you are sure that you have set the correct execution policy, click Yes to continue.
- b. If you would like to test your policy settings, click No and restart the installation.

Installation Wizard Methods

The installation package is divided into multiple elements and typically installed on one server; however, can be installed on multiple servers depending upon customer requirements. An Installation Wizard is provided to install SmartTAP 360° with one of these configuration as follows:

- All-In-One installation for a Single server installation platform
- Distributed installation for a Multi-server installation platform

All-In-One

This method installs the following default SmartTAP 360° components in a single Wizard process, including recording and integration components. For more information, proceed to Chapter Installation Wizard - All-In-One Method on page 17 (recording components and Chapter Integration Configuration on page 127 (integration components).

Distributed

The Distributed method allows you to perform Stand-alone installations of the separate installation components. You may wish to use a Distributed installation for any of the following reasons:

- If you need to add/remove a specific component
- If you need to setup survivable recording at SBA location (SmartTAP 360° RDD)
- If you need to install SmartTAP 360° Media Proxy or Announcement Server for Skype for Business.
- If some SmartTAP 360° elements will reside on different servers.
- If you are installing Analog Station Integration.
- If you are installing SIPRec.



This installation method assumes that each SmartTAP 360° component will be installed on a separate physical or virtual server.

Proceed to Chapter Installation Wizard - Distributed Method on page 32.

Post Installation Actions

After you have successfully installed SmartTAP 360° using one of the methods described above, there are additional actions required to fully setup the SmartTAP 360° network.

- Configure Firewall rules: The deployment of the SmartTAP 360° servers may have to comply with customer security policies, which require the implementation of firewall rules. You need to configure these rules in the Enterprise. See Chapter Firewall Configuration on page 51.
- Integrate SmartTAP 360° with other network components:
 - Skype for Business (see Microsoft Skype for Business Deployment on page 62)
 - SIPRec (see Section)SIP Recording (SIPRec) on page 142
 - Analog trunk/radio (see Analog Trunk / Radio on page 134
- VoIP Port Mirroring to receive the unencrypted Signaling and RTP from different IP PBX station side-tapping configurations using a mirror port or network tap appliance (see VoIP Port Mirroring on page 127
- Additional Configuration options:
 - Configuration Digital Signatures (see Configuring Digital Signatures on page 154)
 - Configuring LDAP (see Configuring LDAP on page 155)
 - Configuring SSO (see Configuring SSO on page 155)
 - Configuring HTTP/S (see Configuring HTTP/S on page 156)
- At the end of a clean installation, upgrade or maintenance update, the installer process goes to the "PostInstallation" folder, scans the files with the extensions exe,bat and ps1and runs each one of them in alphabetical order. AS host.properties automatically includes multicast IP addresses in _PostInstallation folder.

 \times

4 Installation Wizard - All-In-One Method

The installation package is divided into multiple elements and typically installed on one server; however, can be installed on multiple servers depending upon customer requirements. This chapter describes the most common SmartTAP 360° installation on a single server.



- Refer to Chapter Installation Wizard Distributed Method on page 32 for installations that involve more than one SmartTAP 360° server.
- If you are running a clean installation or upgrade, you may be prompted to restart the server. In this case, the installer prompts for a server restart; perform this action and then upon completion, run the installation script again.

> To install SmartTAP 360°:

- **1.** Verify all prerequisites for the installation are met before moving forward with the installation.
- 2. Launch install.bat from the "Suite" folder.
- 3. Click Next to continue.

Figure 4-1: Installation Wizard

\sub AudioCodes SmartTAP

Welcome to the InstallShield Wizard for
AudioCodes SmartTAP

The InstallShield(R) Wizard will install AudioCodes SmartTAP on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Next >

Cancel

v4.1.0

InstallShield

- 4. Click **Next** after accepting SmartWORKS license.
- 5. Click Next after accepting SmartTAP 360° license.

	Figure 4-2: Setup Type	
C AudioCodes	SmartTAP	×
Setup Ty	pe	SMARTTAP
	All-In-One AudioCodes Database Server, Application Server, Communication Server, Media Server and Call Delivery IP will be installed.	
	Distributed Choose which components you want installed and where they will be installed.	
InstallShield	- Sack	Cancel

6. Select All-In-One:

Refer to the following sections:

- Installing Database Service (see Section Database Service on the next page)
- Installing Application Server (AS) (see Section Installing the Application Service on page 20)
- Installing Communication Server (CS) (see Section Installing the Communication Service on page 24)
- Installing Media Server (MS) (see Section After upgrading SmartTAP 360°, make sure that the Call Delivery configuration is set to the actual IP address of the servers. Using local host, or 127.0.0.1, will no longer work correctly, although it was valid in previous versions of SmartTAP 360°. on page 26)
- Installing Call Delivery-IP (CD-IP) (see Section Installing the Call Delivery Service on page 25)

For the installation of these components, unless otherwise specified, accept defaults shown.

Database Service

The Database installation starts in the proper sequence when all or multiple services are selected on the installer menu.

> To install the database service:

1. When the Database Server Installation wizard starts, click Next to install.

岁 AudioCodes Inc.	Database Server - InstallShield Wizard	x
3	Welcome to the InstallShield Wizard for AudioCodes Inc. Database Server	1
	The InstallShield(R) Wizard will install AudioCodes Inc. Database Server on your computer. To continue, dick Next.	
	WARNING: This program is protected by copyright law and international treaties.	
	< Back Next > Cancel	

Figure 4-3: Database Server Installation Wizard

- 2. Accept ALL defaults.
- 3. Click Install.
- 4. Click Finish.
 - For setting up clustered configurations of the database, please contact AudioCodes Technical Support for further information.
 - When upgrading from SmartTAP 360° 1.8.x through SmartTAP 360° 2.2.x, you need to manually check for the following registry key and add it if it is not present:

HKLM\SOFTWARE\Wow6432Node\Audiocodes\SmartTAP 360°\DB\InstallDirectory= ...\MySql\MySql Server 5.0\

This is a value of type "String". You must replace the path to MySql with the real path on the existing system. It is important to leave the trailing backslash in place. Once this is done, the upgrade of the database can proceed successfully.

Installing the Application Service

The Application Service is essentially a Web server responsible for user access, management and database control.

- The database must be installed first before continuing.
- This procedure also runs a silent installation of the OVOC Main Agent and OVOC Client Agent. For more information, refer to the Administrator Guide.

SNMP Trap Service must be disabled on SmartTAP 360° servers running the Application Server component.

> To install the Application service:

- **1.** The Application Service installation starts in the proper sequence when all or multiple services are selected on the installer menu.
- 2. When the Application Server installation wizard starts, click Next to install.



Figure 4-4: Application Server Installation Wizard

If you are installing from a Suite, then the following screen may not be displayed.

Figure 4-5: License Agreement

😸 AudioCodes Inc. Application Server - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	
SOFTWARE LICENSE AGREEMENT	
LICENSE AGREEMENT AUDIOCODES USA, INC. (AudioCodes) provides the following License Agreement (the Agreement) to the original purchaser only: 1. PLEASE READ THIS LICENSE AGREEMENT. The enclosed AudioCodes software/firmware program (collectively, "SOFTWARE") is licensed by AudioCodes for use only on the terms and conditions set forth herein. By opening this peakers you (LICENSEE) agree to and do hereby	-
I accept the terms in the license agreement Print I do not accept the terms in the license agreement	
InstallShield < Back Next > Cancel	

3. Select the "I accept the terms in the license agreement" check box and click Next.

If you are performing an upgrade, the screen below is not displayed.

HaudioCodes Inc. Application Se	erver - InstallShield Wizard	×
Application Information Please enter your information		と
Local IP address:	172.17.127.30	•
Database IP address:	172.17.127.30	•
InstallShield	< Back Nex	xt > Cancel

Figure 4-6: Application Information

 Enter the IP address of the Application Server location and the IP address of the Database location. The IP addresses should be external i.e. not the IP address of the local host. Click Next to proceed.

🔡 AudioCodes Ind	c. Application Server - InstallShield Wizard
Setup Type Choose the setup type that best suits your needs.	
Please select a	setup type.
Complete	All program features will be installed. (Requires the most disk space.)
© Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield	< Back Next > Cancel

Figure 4-7: Setup Type

- 5. Select one of the following setup types and click Next:
 - **Complete:** Install to the default location: C:\Program Files\AudioCodes\SmartTAP 360°\AS
 - **Custom:** Change the destination location

😸 AudioCodes Inc. Application Server - InstallShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
InstallShield < Back Install Cancel	

Figure 4-8: Ready to Install

6. Click Install.





7. Click Finish.

Installing the Communication Service

The Communication Service acts like a SIP proxy and registrar to control connectivity and load balancing between the Call Delivery devices and the Media Servers.

For setting up an HTTPS connection between the SmartTAP 360° Application server and the Communication Service, see Configuring SmartTAP 360° Components for HTTPS on page 157.

> To install the Communication Service:

- **1.** The database must be installed first before continuing.
- 2. The Communication Service installation starts in the proper sequence when all or multiple services are selected on the installer menu.
- 3. When the Communication Server installation wizard starts click **Next** to install.

Figure 4-10: Communication Server

😥 AudioCodes Inc. Communication Server - InstallShield Wizard 🗙	
2	Welcome to the InstallShield Wizard for AudioCodes Inc. Communication Server
	The InstallShield(R) Wizard will install AudioCodes Inc. Communication Server on your computer. To continue, click Next.
	WARNING: This program is protected by copyright law and international treaties.
	< Back Next > Cancel

- 4. Accept ALL defaults.
- 5. During the installation you are prompted to enter the IP address of the Application server.
- 6. Click Install.
- 7. Click Finish.

Installing the Call Delivery Service

The Call Delivery is responsible for passively tapping or actively connecting to the telephony environment and then determining which calls to record using the dynamic state machine and target list. A separate Call Delivery Service will be installed for each telephony environment.

The All-In-One SmartTAP 360° install will automatically install the CD-IP Call Delivery for IP PBX recording environments like Skype for Business, Cisco, SIP, NEC, Siemens, etc.

For setting up an HTTPS connection between the SmartTAP 360° Application server and the Call Delivery Service, see Configuring SmartTAP 360° Components for HTTPS on page 157.

> To install the Call Delivery Service:

1. When the Call Delivery Service installation wizard starts click **Next** to install.



Figure 4-11: Call Delivery Service

2. Select Network Integration Type - (Skype for Business or Other).

岁 AudioCode	s Inc. Call Delivery-IP
Select Network Type	ん
Choose the type of phone network to b	e recorded
Network Type: Microsoft Lync ✓ Microsoft Lync Other	
InstallShield	< Back Next > Cancel

Figure 4-12: Select Network Type

3. Click Next

- 4. To finish the CD-IP installation, choose one of the following:
 - Skype for Business– See Section Installing Call Delivery for Skype for Business (IPbased Recording) on page 87
 - Other (VoIP Port Mirror) See Section Call Delivery Install for VoIP (Port Mirror) on page 128

<u>/</u>

After upgrading SmartTAP 360°, make sure that the Call Delivery configuration is set to the actual IP address of the servers. Using local host, or 127.0.0.1, will no longer work correctly, although it was valid in previous versions of SmartTAP 360°. The "localIp" parameter should be set to the IP address of the Call Delivery server where this software is installed.

The "trapDestIP" and "recorder ip" parameters should be set to the IP address where the Application Server is installed, which may or may not be the same server. Manually edit this section of the calldeliveryconfig.xml file:

<snmp>

```
<network locallp="CDRealIP" port="11161" name="SWCallDelivery" oid-
d="1.3.6.1.4.1.5003.9.40.1.1.2" trapDestIp="ASRealIP" />
</snmp>
<applicationServer>
<recorder ip="ASRealIP" port="80">
<protocols>
```

<protocol>http</protocol> </protocols> </recorder> </applicationServer> This note applies to CD-IP only.

Installing the Media Server

The Media Server is responsible for writing to file storage the incoming RTP stream from the Call Delivery, encrypting and compressing the data.



For setting up an HTTPS connection between the SmartTAP 360° Application server and the Media Server, see Configuring SmartTAP 360° Components for HTTPS on page 157

To install the Media Server:

- 1. The Media Server installation starts in the proper sequence when all or multiple services are selected on the installer menu.
- 2. When the Media Server installation wizard starts, click Next to install.

H AudioCodes I	nc. Media Server - InstallShield Wizard	
	Welcome to the InstallShield Wizard for AudioCodes Inc. Media Server	
	The InstallShield(R) Wizard will install AudioCodes Inc. Media Server on your computer. To continue, dick Next.	
	WARNING: This program is protected by copyright law and international treaties.	
< Back Next > Cancel		

Figure 4-13: Media Server

3. Select the IP Address of the SmartTAP 360° Server from the "Monitoring IP Address" dropdown box.
- **4.** In the Distributed or Remote Branch deployment, enter the real IP address for the Communication and Application Servers.
- 5. In the all-in-one deployment you can leave the default 127.0.0.1 address or type in the server IP address.

🖞 AudioCo	des Inc. Media Server - InstallShield Wizard			
Media Server Configu Specify the network in	uration Iformation in the given fields.			
Monitoring IP Address	This is the IP address that listens for RTP traffic			
Communication Server IP Address	127.0.0.1 This is the IP address for the Communication Server			
Application Server IP Address	127.0.0.1 This is the IP address for the SNMP trap destination			
REMINDER: Host and edge firewall rules may require updating to pass RTP traffic. Also, make sure to re-check your Windows firewall settings after installing Windows Updates.				
InstallShield	< Back Next > Cancel			

Figure 4-14: Media Server Configuration

- 6. Click Next.
- 7. Click Install.
- 8. Click Finish.

Installing the Remote Transfer Service

This section describes how to install the Remote Transfer Service (RTS).



> To install the RTS:

- 1. The RTS installation starts in the proper sequence when all or multiple services are selected on the installer menu.
- 2. When the RTS installation wizard starts, click **Next** to install.

😸 AudioCodes	Remote Transfer Service - InstallShield Wizard			
RTS Configuration Specify the network inf	ormation in the given fields.			
Monitoring IP Address	This is the IP address that listens for RTP traffic			
Application Server IP Address	This is the IP address for the SNMP trap destination			
Transfer file location	C:\Program Files(x86)\AudioCodes\SmartTap\MS\Server\Bin This is the path where transfer file is located			
Application Server Protoco				
REMINDER: Host and edge firewall rules may require updating to pass RTP traffic. Also, make sure to re-check your Windows firewall settings after installing Windows Updates.				
InstallShield				
	< Back Next > Cancel			

Figure 4-15: RTS Configuration

- 3. Enter the following parameters and then click Next.
 - Monitoring IP address (Public IP address)
 - Application Server IP address
 - Transfer File Location (Location of Bin folder of installed RTS component)
 - Application Server Protocol (HTTP or HTTPS)

Figure 4-16: Setup Type

	Figure 4-17:
😼 AudioC	Codes Remote Transfer Service - InstallShield Wizard
Setup Type Choose the set	tup type that best suits your needs.
Please select a	setup type.
 Complete 	All program features will be installed. (Requires the most disk space.)
O Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield ———	< Back Next > Cancel

4. Click **Next** to complete the installation.

Completing Wizard Installation

When the installer completes the installation of all the software components, a dialog window appears indicating that the installation has completed.

1. When the installer completes the following screen appears:

🗙 AudioCodes SmartTAP	\times
InstallShield Wizard Completed	
•	
The InstallShield Wizard has successfully installed AudioCodes SmartTAP. Click	
InstallShield	

- 2. Click Finish to exit the installer.
- **3.** Proceed to Integration Configuration on page 127 to complete the integration configuration steps required before the server is ready to record calls.

Post-Installation Integration

At this point in the installation, the software is running on the server. However, the SmartTAP 360° recorder needs additional integration specific configuration before it is capable of recording calls. This integration is described in Chapter Integration Configuration on page 127.

 \times

5 Installation Wizard - Distributed Method

This Chapter describes the Distributed method for installing SmartTAP 360°.

- This installation method assumes that each SmartTAP 360° component will be installed on a separate physical or virtual server.
 - If you are running a clean installation or upgrade, you may be prompted to restart the server. In this case, the installer prompts for a server restart; perform this action and then upon completion, run the installation script again.

> To install the distributed method:

- **1.** Launch install.bat from the "Suite" folder.
- 2. Click Next to continue.

Figure 5-1: InstallShield Wizard SmartTAP 360°

🗴 AudioCodes SmartTAP

	Welcome to the InstallShield Wizard for AudioCodes SmartTAP					
	The InstallShield(R) Wizard will install AudioCodes SmartTAP on your computer. To continue, click Next.					
	WARNING: This program is protected by copyright law and international treaties.					
v4.1.0						
		Connect				

- 3. Click Next after accepting SmartWORKS license.
- 4. Click **Next** after accepting SmartTAP 360° license.



5. Select the Distributed installation option.



Figure 5-3: Custom Setup

6. Select the software elements that you wish to install.

Refer to the following sections:

- Installing SmartTAP 360° Database Server (see Section Installing SmartTAP 360° Database Server below)
- Installing SmartTAP 360° Application Server Installation (see Section Installing SmartTAP 360° Application Server below)
- Installing SmartTAP 360° Communication Server (see Section Installing SmartTAP 360° Communication Server on the next page)
- Installing SmartTAP 360° Media Server (see Section Installing SmartTAP 360° Media Server on page 36)
- Installing SmartTAP 360° Call Delivery Server (see Section Installing SmartTAP 360° Call Delivery Server on page 43)

Installing SmartTAP 360° Database Server

This section describes the database service software installation.



It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.

> To install the database service software:

- 1. Run the Install.bat from the SmartTAP 360° "Suite\" folder.
- 2. Select the Distributed software Custom Setup type.
- 3. Select the AudioCodes Inc. Database Server option.
- 4. Click Install.
- 5. Click Next to continue.
- 6. Select Complete, and then click **Next** to continue.
- 7. Click Install.
- 8. Click **Finish** to complete the installation.

Database Service Configuration

The database is configured automatically during the installation of the AS.

Installing SmartTAP 360° Application Server



During an upgrade of the Application Server, the installers may mistakenly stop



- It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51
- This procedure also runs a silent installation of theOVOC Main Agent and OVOC Client Agent. For more information, refer to the Administrator Guide.

> To install the Application Service:

- 1. Verify that the (DB) Database Server is installed and the MySQL service is running.
- 2. Run the Install.bat from the SmartTAP 360° "..\Suite\" folder.
- 3. Select the Distributed software Custom Setup type.
- 4. Select the AudioCodes Inc. Application Server option.
- 5. Click Next.
- 6. Change the Database Server IP from "127.0.0.1" to the IP of the Database Server.
- 7. Click Next.
- 8. Select **Complete**, and then click **Next** to continue.
- 9. Click Install.
- **10.** Click **Finish** to complete the installation.

Installing SmartTAP 360° Communication Server

- During an upgrade of the Communication Server, the installers may mistakenly stop and ask the user to choose between a "Complete" and "Custom" installation. If the component was installed to a custom location, make sure the correct location is still set in the "Custom" dialog box."
 - It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51

To install the Communication Server:

- 1. Run the Install.bat from the SmartTAP 360° "Suite\" folder.
- 2. Select the Distributed software Custom Setup type.
- 3. Select the AudioCodes Inc. Communication Server option.
- 4. Click Install button to continue.
- 5. Click **Next** to continue.
- 6. Enter the "Application Server Name or IP" when prompted.

- 7. Enter the "Media Server Name or IP" when prompted.
- 8. Enter the "Database Server Name or IP" when prompted.
- 9. Since the Master DB is remote, the CS installation will install a local Slave DB with the CS.
- 10. The Slave DB will automatically connect to the Master DB.
- **11.** Select Complete, and then click **Next** to continue.
- 12. Click Install.
- **13.** Click **Finish** to complete the installation.

Installing SmartTAP 360° Media Server

- The transfer of the media files between the Media Server, Application Server, and File Server (SAN/NAS) is accomplished by using the windows SHARE (SMB) facilities. Therefore, all servers must be part of the same windows domain.
 - It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.

> To install the Media Server:

- 1. Run the Install.bat from the SmartTAP 360° "Suite\" folder.
- 2. Select the Distributed software Custom Setup type.
- 3. Check on AudioCodes Inc. Media Server option.
- 4. Click Install to continue.
- 5. Click **Next** to continue.
- 6. Select the Monitoring IP Address from the drop-down list.
 - Typically the IP of the physical or virtual server.
 - The Monitoring IP Address is the IP address of the interface that listens for the RTP media to be recorded. This RTP media is sent from the Call Delivery Server, Media Delivery or Media Proxy depending upon deployment solution.
- 7. Enter the Communication Server IP Address when prompted.
- 8. Enter the Application Server IP Address when prompted.
- 9. Select Complete, and then click Next to continue.
- 10. Click Install to continue.
- **11.** Click **Finish** to complete the installation.

Media Server Configuration



This procedure is not relevant if the media files are stored on the same server as the Media Server.

Network File Server

This section describes how to create a user account for SmartTAP 360° on the domain. For example "SmartTAPUser" for the Network File server.

> To setup the network file server accounts:

1. In the Active Directory Users and Computers folder, select the Users folder and then rightclick **New** > **User**.

		Active Dir	ecto	ory Users and Co	mputers	_ 🗆 🗙
File Action	View Help					
🗢 🔿 🙍	T & 🗉	🗙 🗐 🧟 🖻	2	l 🖬 🙎 🐮 🛍	7 🗾 🐍	
📃 Active Direct	tory Users and	Name			Туре	Description 🔨
👂 🧮 Saved Qu	ueries	🚨 Abraham			User	
⊿ 🚔 S4B.inter	op	💄 Administrat	tor		User	Built-in account for a
þ 📔 acs		용 Allowed RC	DC P	assword Replicati	Security Group	Members in this group \equiv
D Euiltin	n	🚨 Anatoly1			User	
Comp	puters	🚨 Anatoly2			User	
Doma Doma Doma	ain Controller	🚨 Anatoly3			User	
p — Foreig ⊳ [™] LostA	undFound	👗 Anatoly4			User	
b 🦳 Mana	aged Service A	👗 Burolo User			User	
⊳ 🗊 Micro	osoft Exchang	🔏 Cert Publisł	ners		Security Group	Members of this grou
⊳ 💼 OfirTe	est	🚜 Cloneable [)oma	in Controllers	Security Group	Members of this grou
👂 🦳 Opera	ationsManage	SAdminist 🚓	trator		Security Group	Members of this grou
🛛 👌 🧰 OpsN	/IgrLatencyMi	🚜 CSArchivin	ng Administrator sk		Security Group	Members of this grou
⊳ 🧮 Progr	ram Data	🚜 CSHelpDesi			Security Group	Members of this grou
⊳ 🧰 Syster	m	CSLocation	Administrator		Security Group	Members of this grou
	Delegate Co	ntrol	#Chat	tAdministrator	Security Group	Members of this grou
	Pelegate Co		Grou	apAdministrator	Security Group	Members of this grou
	Find		Grou	ipManager	Security Group	Members of this grou
	New	•		Computer		mbers of this grou
	All Tasks	+		Contact		
Crustu a num	View	۲		Group		
Create a new	Refresh			InetOrgPerson		
	Export List		msDS-ResourcePropertyList msExchDynamicDistributionList			
	Properties			msImaging-PSPs		
Help				MSMQ Queue Alias		
				Printer		
				User		
				Shared Folder		

Figure 5-4: Active Directory Users and Computers

Figure 5-5:	New SmartTAP 360° User		
	New Object - User	x	
🧏 Create in:	S4B.interop/Users		
<u>F</u> irst name:	SmartTAPUser <u>I</u> nitials:		
Last name:			
Full n <u>a</u> me:	SmartTAPUser		
<u>U</u> ser logon name:			
SmartTAPUser	@S4B.interop 🗸		
User logon name (pre	- <u>W</u> indows 2000):		
S4B\	SmartTAPUser		
	< <u>B</u> ack <u>N</u> ext > Car	ncel	

2. Enter the name of the SmartTAP 360° user in the First Name and User logon name fields and click **Next**.

Figure 5-6: Password Never Expires

New Object - User
Create in: S4B.interop/Users
Password:
User cannot change password Password never expires Account is disabled
<u>≺B</u> ack <u>N</u> ext≻ Cancel

 Enter a password, select the "Password never expires" check box and click Next. The following confirmation dialog is displayed:

New Object - User	x
Create in: S4B.interop/Users	
When you click Finish, the following object will be created:	
Full name: SmartTAPUser User logon name: SmartTAPUser@S4B.interop The password never expires.	×
< <u>B</u> ack Finish	Cancel

Figure 5-7: User Add Confirmation

- 4. Click Finish.
- 5. Right-click the newly created user, choose Properties and click the Security tab.

	:	SmartTAPU	Jser Pro	operties	5	? X
Published 0	ertificates	Member Of	Passwo	rd Replica	ation	Dial-in Object
Remote	Desktop Se	ervices Profile	(COM+ Attribute Editor		tribute Editor
General	Address	Account	Profile	Telepł	nones	Organization
Security	Er	nvironment	Ses	sions	Re	emote control
<u>G</u> roup or u	iser names:					
🚨 Eivery	one					^
SELF 🕺						≡
Autho	enticated U:	sers				
🦓 SYS 🧕 🧟 мету	NUBK SEE	VICE				
	Jniversall Is	erReadOnluGri	oup (S4R	RTCUniv	ersalUs	erRead
RTCI	JniversalUs	erAdmins (S4B	\RTCUni	versalUse	rAdmins	s) V
-						
			L	A <u>d</u> d		<u>H</u> emove
Permissions for Everyone Allow Deny						
Full con	trol					
Read					/	
Write					/	
Create	all child obje	ects				
Delete	all child obje	ects		L	4	
Allowed	to authenti	cate		L	_	
For special permissions or advanced settings, click Advanced						
	0	K C	ancel	Ap	ply	Help

Figure 5-8: Assign Read and Write Permissions

- 6. Assign "Read" and "Write" permissions and click OK.
- 7. Log in to the Media server as user "SmartTAP 360°".
- 8. Access the SmartTAP 360° shared media storage in the File server.
- 9. Create, edit, and delete a test file in the storage directory.
- **10.** Log off.

Media Server

This section describes how to add the SmartTAP 360° domain user to the local Administrators Group and to assign it to the SmartTAP 360° MS-TR service.

> Do the following:

- 1. Add SmartTAP 360° user to local Administrators Group:
 - a. In the Active Directory Users and Computers, right-click the newly created SmartTAP 360° user and choose Add to a group.

2	Active Directo	ry Users and Co	mputers	- 🗆 X
File Action View Help				
🗢 🔿 🙍 🚮 🕄	🗙 🗐 🖻 📑 👔	1 🖬 🗏 🐮 🛍	7 🗾 🔽	
Active Directory Users and Saved Queries SAB.interop SAB.interop Saved Queries SAB.interop Saved Queries Saved Qu	Name RAS and IAS Servers RAS and IAS Servers Read-only Domain Controllers RTCComponentUniversalServices RTCHSUniversalServices RTCProxyUniversalServices RTCDniversalServices RTCUniversalConfigReplicator RTCUniversalGlobalReadOnlyGroup RTCUniversalGlobalWriteGroup RTCUniversalSeadOnlyAdmins RTCUniversalSBATechnicians RTCUniversalServerAdmins RTCUniversalServerAdmins RTCUniversalServerAdmins RTCUniversalServerAdmins		Type Security Group Security Group	Description Servers in this group c Members of this grou Members can be used Members can be used Members can be used Members can particip Members have read a Members have read a Members have write a Members have read a Members have read a Members have read a Members have read a
 ▶ System ■ Users ▶ ■ Microsoft Exchang ■ MTDS Quotas ▶ ■ TPM Devices 	RTCUniversaluse RTCUniversaluse RTCUniversaluse Schema Admins SmartTAP Use SystemMai SystemMai SystemMai SystemMai SystemMai	Copy Add to a group Name Mappings Disable Account	Security Group	Members can manage Members have read a Designated administra E
< III >	< Tol Solidor	Reset Password		>
Allows you to add the selected	objects to a gro	Move Open Home Page Send Mail All Tasks	•	
		Cut Delete Rename		
		Properties		
		Help		

Figure 5-9: Add SmartTAP 360° user to Administrators Group

Figure 5-10: Add Smart TAP User to Administrator

Select Groups	x
Select this object type: Groups or Built-in security principals	Object Types
From this location:	
S4B.interop	Locations
Enter the object names to select (<u>examples</u>): Administrators	Check Names
Advanced OK	Cancel

- **b.** Enter Administrator and then click Check Names. The successfully recognized entry is underlined.
- c. Click OK. A confirmation screen is displayed.
- 2. Assign the SmartTAP 360° user to the SmartTAP 360° MS-TR service:
 - a. Open the Services (Local) application (services.msc).
 - Select the service "SmartTAP 360° MS-TR", right-click Properties and click the Logon tab.
 - c. Select the 'This account' check box.
 - **d.** Click Browse to search for the domain user who has permissions for the shared media directory in the file server.

This user may be the SmartTAP 360° user or any other user defined for this purpose.

Figure 5-11: Assign User to SmartTAP 360° MS-TR Service Account

Select Users, Computers, Service Accounts, o	or Groups 🛛 🗙
Select this object type:	_
Users, Service Accounts, or Groups	Object Types
From this location:	
S4B.interop	Locations
Enter the object names to select (<u>examples</u>):	
SmartTAPUser (SmartTAPUser@S4B.interop)	Check Names
Advanced OK	Cancel

- e. Click Check Names. The successfully recognized entry is underlined.
- f. Restart the service.

Installing SmartTAP 360° Call Delivery Server

Note: It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.

> To Install the Call Delivery server:

- 1. Run the "Install.bat" from the SmartTAP 360° "Suite\" folder.
- 2. Select the Distributed Software Custom Setup type.
- 3. Click AudioCodes Inc. Call Delivery Server.
- 4. Click Install to continue.
- 5. Select "Microsoft Lync" or "Other" when prompted.
 - Other: (NON Microsoft LYNC)
- 6. Server IP Setup Screen:
 - Specify the IP of the Communication & Application Servers.
 - Specify the IP of the Local Machine.
- 7. Click link to install Skype for Business. See Section Plugin Configuration.
 - Return here once the configuration has completed.
 - No additional CD-IP configuration should be necessary.
- 8. Click link to install the Other (IP). See VoIP Port Mirroring on page 127.
 - Return here once the configuration has completed.
 - Once the installation of the CD-IP has completed, an additional configuration is required. See Section 1.3.4 Additional Configuration.
- 9. Click link to install Analog Trunk/Radio. See Section Analog Trunk / Radio on page 134 :
 - Return here once the configuration has completed.
 - Once the installation of the CD-AL has completed, an additional configuration is required. See Section 1.5.2 Additional Configuration .
- **10.** Click **Next** to continue.
- **11.** Click **Install** to complete the installation.

SmartTAP 360° File Server Installation



It is preferable, that the File Server is installed and configured before installation of the (MS) Media Server and the (AS) Application Server.

Firewall Configuration

It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.

Domain Controller Configuration

This configuration is an example of what must be performed in a windows environment to allow the SmartTAP 360° software running on a different server to read and write to the file server directory where the recordings are stored. Alternatively, in the absence of a domain controller, the same can be achieved by the configuration of windows file sharing feature.

- > To configure the SmartTAP 360° user on the Windows server Domain Controller:
- 1. Create a user account for SmartTAP 360° on the Domain Controller. For example "SmartTAP 360° User":
 - a. In the Active Directory Users and Computers folder, select the Users folder and then right-click **New** > **User**.

	Active Dir	ecto	ry Users and Co	mputers	_ D X
File Action View Help					
🗢 🔿 🙍 🖬 🤞 🗎	🗙 🗐 🧟 🗟	?	51 🕺 🐮 🛅	7 🗾 🐍	
📃 Active Directory Users and	Name			Туре	Description 🔥
▷ 🚞 Saved Queries	🚨 Abraham			User	
🔺 🚔 S4B.interop	🔱 Administrat	or		User	Built-in account for ac
þ 🖬 acs	& Allowed RO	DC P	assword Replicati	Security Group	Members in this grou
⊳ 🧮 Builtin	🙎 Anatoly1			User	
Computers	🙎 Anatoly2			User	
Domain Controller	👗 Anatoly3			User	
Foreign SecurityPri	👗 Anatoly4			User	
p EuseAndround N C Managed Service /	🙎 Burolo User			User	
Managed Service A Microsoft Exchanged	🎎 Cert Publisł	hers		Security Group	Members of this grou
D Gi OfirTest	🎎 Cloneable 🛙)omai	in Controllers	Security Group	Members of this grou
DerationsManaqui	🎎 CSAdminist	trator		Security Group	Members of this grou
D DpsMgrLatencyMi	& CSArchiving	gAdm	iinistrator	Security Group	Members of this grou
👂 🚞 Program Data	& CSHelpDesk	ĸ		Security Group	Members of this grou
þ 🧮 System	& CSLocation	Admi	nistrator	Security Group	Members of this grou
Care Leave	SPersisten	+Chat	Administrator	Security Group	Members of this grou
Delegate Co	introl	Grou	pAdministrator	Security Group	Members of this grou
▶ 🛄 📔 Find		Grou	pManager	Security Group	Members of this grou
New	•		Computer		mbers of this grou
All Tasks	•		Contact		mbers of this grou 🗸
< III View	•		Group		>
Create a new Refresh			InetOrgPerson		
Export List			msDS-ResourcePro	opertyList	
Depending			msExchDynamicDi	stributionList	
Properties			msImaging-PSPs		
Help			MSMQ Queue Alia	s	
			Printer		
			User		
			Shared Folder		

Figure 5-12: Active Directory Users and Computers



	New Object - User	x
🤱 Create in:	S4B.interop/Users	
<u>F</u> irst name:	SmartTAP User	
Last name:		
Full n <u>a</u> me:	SmartTAP User	
<u>U</u> ser logon name:		
SmartTAP User	@S4B.interop 🗸	
User logon name (pre	ə- <u>₩</u> indows 2000):	
S4B\	SmartTAP User	
	< Back Next > Cancel	

- 2. Click Next, enter a password and then configure the following settings:
 - a. Clear the User must change password at next logon check box.
 - b. Select the User cannot change password check box.
 - c. Select the Password never expires check box.

Figure 5-14: User Settings

New Object - User
Create in: S4B.interop/Users
Password: •••••• Confirm password: ••••••
 User must change password at next logon ✓ User cannot change password ✓ Password never expires Account is disabled
< <u>B</u> ack <u>N</u> ext > Cancel

The following confirmation dialog is displayed:

Figure 5-15: User Add Confirmation

New Object - User		
Create in: S4B.interop/Users		
When you click Finish, the following object will be created:		
Full name: SmartTAP User User logon name: SmartTAP User@S4B.interop The user cannot change the password. The password never expires.		
< <u>B</u> ack Finish Cancel		

- 3. Click Finish.
- 4. Add the File Server to the Domain:
 - a. Right-click **Start** > **System**.

19			System	_ _ X
0	💿 💿 🔹 🕇 📴 🕨 Control P	anel 🕨 System and Security 🕨 Sy	stem	Search Control Panel
	Control Panel Home	View basic information	about your computer	0
	Device Manager	Windows edition		
	Remote settings	Windows Server 2012 R2 St	andard	_
9	Advanced system settings	© 2013 Microsoft Corporat	ion. All rights reserved.	Windows Server 2012 R2
		System		
		Processor:	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz 2.67 GHz	
		Installed memory (RAM):	4.00 GB	
		System type:	64-bit Operating System, x64-based processor	
		Pen and Touch:	No Pen or Touch Input is available for this Display	
		Computer name, domain, and	workgroup settings	
		Computer name:	DC	😗 Change settings
		Full computer name:	DC.S4B.interop	
		Computer description:		
		Domain:	S4B.interop	
		Windows activation		
		Windows is not activated.	Read the Microsoft Software License Terms	
		Product ID: 00252-40260-3	3000-AAOEM	Activate Windows
	See also			
	See also			
	Action Center			
	windows opdate			

Figure 5-16: System Properties

- b. Select Change settings in the Computer name, domain, and workgroup settings.
- c. Click Change.. in the Computer Name tab.
- d. Select the Domain radio button and enter the name of the domain.
- e. When prompted, enter the domain administrator user and password.

The Welcome to the <domain name> domain dialog confirms that the server is now joined to the domain.

f. Restart the File Server.

	System Properties
Computer Name Hardwa	are Advanced Remote
Windows uses on the network	s the following information to identify your computer k.
Computer <u>d</u> escription:	
	For example: "IIS Production Server" or "Accounting Server".
Full computer name:	DC.S4B.interop
Domain:	S4B.interop
To rename this computer workgroup, click Change	r or change its domain or <u>C</u> hange
Note: The identification of - The Certification Author	of the computer cannot be changed because: ity Service is installed on this computer.
	OK Cancel Apply

Figure 5-17: System Properties

- 5. Log in into the file server as user "SmartTAP 360°" in the domain.
- 6. Create the media storage directory (...\media) on the file server.
- 7. Share the media storage:
 - a. Right-click the storage directory and select Properties.
 - Select the Sharing tab and click share... in the Network File and Folder Sharing section.
 - Click the Share button and enter the domain administrator user and password when prompted.

6 Uninstalling SmartTAP 360°

The following describes how to uninstall SmartTAP 360°.

➤ To uninstall SmartTAP 360°:

- **1.** Launch install.bat from the "Suite" folder.
- 2. From the Program Maintenance screen, click Remove to remove the SmartTAP 360° component from the PC.

Figure 6-1: Program Maintenance - Remove

AudioCodes SmartTAP

Program Maintenance



	Modify Change which program features are installed or removed. This option displays the Custom Selection dialog in which you can change the way features are installed or removed.	
Û	Remove Remove AudioCodes SmartTAP from your computer.	
InstallShiak	P	Cancel

3. When the InstallShield Wizard Completed screen appears, click Finish.

Х

AudioCodes SmartTAP

	InstallShield Wizard Completed	
	The InstallShield Wizard has successfully uninstalled AudioCodes SmartTAP. Click Finish to exit the wizard.	
InstallShield		Finish

7 Firewall Configuration

The deployment of the SmartTAP 360° servers may have to comply with customer security policies, which require the implementation of firewall rules. This section provides the basic information required by the Windows administrator to configure the Windows firewall, to ensure the required connectivity between the SmartTAP 360° applications and services.

All Firewall ports listed are default ports.

Skype for Business Recording Firewall



Figure 7-1: Skype for Business Recording Firewall

Front End Server(s)

The following Inbound firewall exceptions are required.

Table 7-1: Front End Server(s) - Inbound Firewall

Protocol	Allow Port	Allowed Network
ТСР	9901	DOMAIN/INTERNAL (from SmartTAP 360° to FE)

Protocol	Allow Port	Allowed Network
ТСР	12171	DOMAIN/INTERNAL (from SmartTAP 360° Announcement Server to FE)

The following Outbound firewall rule may be required if the FE has a particularly restrictive firewall configuration (non-Default).

Protocol	Allow Port	Allowed Network
ТСР	9090	DOMAIN/INTERNAL (from FE to SmartTAP 360° CD)
ТСР	80	DOMAIN/INTERNAL (from FE to SmartTAP 360° AS)
ТСР	443	DOMAIN/INTERNAL (from FE to SmartTAP 360° AS when AS is configured with HTTPS)
ТСР	10123	DOMAIN/INTERNAL (from FE to SmartTAP 360° MP)
ТСР	10124	DOMAIN/INTERNAL (from FE to Announcement server)

Table 7-2: Front End Server(s) - Outbound Firewall

Edge, Mediation or Conference Server(s)

The following Inbound firewall exceptions are required.

Table 7-3: Edge, Mediation or Conference Server(s) - Inbound Firewall

Protocol	Allow Port	Allowed Network
ТСР	9080	DOMAIN/INTERNAL (from SmartTAP 360° CD)

The following Outbound firewall rules are required if the Edge Server has a particularly restrictive firewall configuration:

Table 7-4:	Edge, Mediation	or Conference	Server(s)	- Outbound	Firewall
------------	-----------------	---------------	-----------	------------	-----------------

Protocol	Allow Port	Allowed Network
UDP	40000- 45000	DOMAIN/INTERNAL (towards SmartTAP 360°)
ТСР	80	DOMAIN/INTERNAL (from SmartTAP 360° MD to SmartTAP 360° AS)
ТСР	443	DOMAIN/INTERNAL (from SmartTAP 360° MD to SmartTAP 360° AS

Protocol	Allow Port	Allowed Network	
		when SmartTAP 360° AS is configured with HTTPS)	

To record calls traversing Edge Server (with remote users, federated users) enable A/V/STUN.MSTURN communication with Edge Server Pool on the UDP port 3478 for compliance with MSFT port and planning requirements.

SmartTAP 360° Server

The following Inbound firewall exceptions are required.

Protocol	Allow Port	Allowed Network	
ТСР	80	DOMAIN/INTERNAL (from FE servers)	
		DOMAIN/INTERNAL (from Edge servers)	
		EXTERNAL (Web Browser Access for end-users)	
ТСР	443	DOMAIN/INTERNAL (from FE to AS when AS is configured with HTTPS)	
		DOMAIN/INTERNAL (From Edge servers to AS when AS is configured with HTTPS)	
ТСР	9090	DOMAIN/INTERNAL (from FE servers)	
UDP	40000-	DOMAIN/INTERNAL (from MD)	
	45000'	DOMAIN/INTERNAL (from MP servers)	
ТСР	10125	DOMAIN/INTERNAL (from AS) Note: The port is only required for CD when AS is installed on another server.	

Table 7-5:	SmartTAP	360°	Server -	INBOUND	Firewall
------------	----------	-------------	----------	---------	----------

The following Outbound firewall exceptions are required.

Table 7-6: SmartTAP 360° Server - Outbound Firewall

Protocol	Allow Port(s)	Allowed Network
ТСР	9080 ¹	DOMAIN/INTERNAL (to MD)
ТСР	9901	DOMAIN/INTERNAL (to FE servers)

Protocol	Allow Port(s)	Allowed Network	
ТСР	10123	DOMAIN/INTERNAL (to MP servers)	

¹Required when Media Delivery resides on Edge, Mediation or Conference server.

SmartTAP 360° Media Proxy Server

The following Inbound firewall exceptions are required.

 Table 7-7:
 SmartTAP 360° Media Proxy Server - Inbound Firewall

Protocol	Allow Port	Allowed Network
ТСР	10123	DOMAIN/INTERNAL (from FE and SmartTAP 360° servers)
UDP	37000- 39999	DOMAIN/INTERNAL (from Skype for Business clients to MP) (Audio)
UDP	33000- 36999	DOMAIN/INTERNAL (from Skype for Business clients to MP) (Video)

The following Outbound firewall exceptions are required.

Table 7-8: SmartTAP 360° Media Proxy Server - Outbound Firewall

Protocol	Allow Port	Allowed Network
UDP	37000- 39999	DOMAIN/INTERNAL (from MP to Skype for Business or Lync clients) (Audio)
UDP	33000- 36999	DOMAIN/INTERNAL (from Skype for Business clients to MP) (Video)
UDP	40000- 45000	DOMAIN/INTERNAL (from the MP to the MS)
ТСР	80	DOMAIN/INTERNAL (from MP to AS)
ТСР	443	DOMAIN/INTERNAL (from MP to AS when AS is configured with HTTPS)

SmartTAP 360° Announcement Server

The following Inbound firewall exceptions are required.

Protocol	Allow Port	Allowed Network
ТСР	12171	DOMAIN/INTERNAL (from FE servers)
ТСР	10124	DOMAIN/INTERNAL (from FE servers)

Table 7-9: SmartTAP 360° Announcement Server- Inbound Firewall

The following Outbound firewall exceptions are required.

Table 7-10: SmartTAP 360° Announcement Server - Outbound Firewall

Protocol	Allow Port	Allowed Network	
ТСР	80	DOMAIN/INTERNAL (from ANN to SmartTAP 360° AS)	
ТСР	443	DOMAIN/INTERNAL (from ANN to SmartTAP 360° AS when AS is configured with HTTPS)	

For further information regarding Skype for Business port requirements, refer to the following.

http://technet.microsoft.com/en-us/library/gg398798.aspx

Automated Firewall Exception Scripts for Windows Firewall

PowerShell scripts are installed to facilitate in adding firewall exceptions to all of the SmartTAP 360° and Lync components. They are installed by default in the following location:

...\AUDIOCODES\SmartTAP 360°\Install\EnableFWRules

The following file needs to be modified before it can be used: EnableSmartTAPFWRules.ps1. The configuration section is at the beginning of the Powershell script.

> To use the script, do the following:

- 1. Populate all of the fields for your installation. Save the file.
- Copy the entire directory to each component that needs to have firewall exceptions added (SmartTAP 360°, Skype for Business Edge, Mediation or Conference Server and the Skype for Business Front Ends).
- On each server, modify the \$machine_type line to match the machines functionality (SmartTAP 360°, edge or fe)
- 4. Run the EnableSmartTAPFWRules.bat to run the script, either by double clicking on it, or running it from a command prompt.
- 5. You can now confirm that the firewall exceptions have been added. If there was an error that you need to correct, just remove the exceptions that the script added, and rerun the script. All SmartTAP 360° firewall exceptions start with the word "SmartTAP 360°".

Distributed SmartTAP 360° Firewall

The following firewall rules are required in the event that you install each component of the SmartTAP 360° installation on a physically separate machine (as described in Chapter Installation Wizard - Distributed Method on page 32Installation Wizard - Distributed Method on page 32). Under normal circumstances, when all of the components are on the same machine you would only need to add an exception for port 80 or 443 (see Section Application Server (AS) on the next page).



The Windows firewall must be setup to allow INBOUND connections on the specified ports.





Application Server (AS)

Table 7-11:	Firewall	- Application	Server	(AS)
-------------	----------	---------------	--------	------

Protocol	Allow Port	Allowed Network
ТСР	80	EXTERNAL (Web Browser Access for end-users) DOMAIN/INTERNAL (from other SmartTAP 360° servers)

Protocol	Allow Port	Allowed Network
ТСР	9001	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
UDP	162	DOMAIN/INTERNAL (from other SmartTAP 360° servers)

Communications Server (CS)

Table 7-12: Firewall - Communications Server (CS)

Protocol	Allow Port	Allowed Network
UDP	161, 1161, 5060	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
ТСР	554	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
ТСР	9000	DOMAIN/INTERNAL (from other SmartTAP 360° servers)

Database Server (DB)

Table 7-13: Firewall - Database Server (DB)

Protocol	Allow Port	Allowed Network
ТСР	3306	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
UDP	161	DOMAIN/INTERNAL (from other SmartTAP 360° servers)

File Server (FS)

Table 7-14: Firewall - File Server (FS)

Protocol	Allow Port	Allowed Network
SMB	Windows Network File Sharing (see File Server installation)	DOMAIN/INTERNAL (from Application and Media servers)
UDP	161	DOMAIN/INTERNAL (from other SmartTAP 360° servers)

Media Server (MS)

Table 7-15: Firewall - Media Server (MS)

Protocol	Allow Port	Allowed Network
UDP	161, 5064, 10161, 40000-	DOMAIN/INTERNAL (from other SmartTAP 360°

Protocol	Allow Port	Allowed Network
	45000	servers)
ТСР	6023	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
TCP REST	10131	DOMAIN/INTERNAL (from other SmartTAP 360° servers)

Remote Transfer Service (RTS)

Table 7-16: Remote Transfer Service (RTS)

Protocol	Allow Port	Allowed Network
TCP REST	10132	Remote Transfer Service (RTS)

Call Delivery(CD)

Table 7-17: Firewall - Call Delivery(CD)

Protocol	Allow Port	Allowed Network
UDP	161, 40000- 45000	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
UDP (Add any	12161 – All VoIP	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
required)	14161 – Analog	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
	15161 – SIPRec	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
	5066 – All VoIP	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
	5067 – Analog	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
	5068 – SIPRec	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
ТСР	9090	DOMAIN/INTERNAL (from other SmartTAP 360° servers)

Protocol	Allow Port	Allowed Network
	10125 – All VoIP	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
TCP (REST)	10125	DOMAIN/INTERNAL (from other SmartTAP 360° servers)
TCP (REST)	10126	DOMAIN/INTERNAL (from SIP Recording server)
TCP (REST)	10127	DOMAIN/INTERNAL (from Analog Trunk / Radio)

Media Delivery (MD)

This applies to Skype for Business Edge, Mediation or Conference servers.

Table 7-18: Firewall - Media Delivery (MD)

Protocol	Allow Port	Allowed Network				
ТСР	9080	DOMAIN/INTERNAL (from other SmartTAP 360° servers)				
TCP REST	10133	DOMAIN/INTERNAL (from other SmartTAP 360° servers)				
TCP REST	80	DOMAIN/INTERNAL (from other SmartTAP 360° servers)				

Media Proxy (MP)

This applies to SmartTAP 360° Proxy servers exclusively in a Microsoft Skype for Business environment.

Protocol	Allow Port	Allowed Network
ТСР	10123	DOMAIN/INTERNAL (from FE servers)
UDP	37000 - 39999	DOMAIN/INTERNAL (from MP to Skype for Business Skype for Business clients)
UDP	37000 - 39999	DOMAIN/INTERNAL (from Skype for Business clients to MP)
UDP	40000 - 45000	DOMAIN/INTERNAL (from MP to MS servers)

Table 7-19: Firewall - Media Proxy (MP)

Announcement Server (AN)

This applies to SmartTAP 360° Announcement servers only in a Microsoft Skype for Business environment.

Protocol	Allow Port	Allowed Network
ТСР	12171	DOMAIN/INTERNAL (from FE servers to SmartTAP 360° Announcement servers).
ТСР	10124	DOMAIN/INTERNAL (from FE servers to SmartTAP 360° Announcement servers).

Table 7-20:	Firewall - Announcement Serve	er (AN)
-------------	-------------------------------	---------

Example

In this example, we are setting up the Windows server firewall for the Media Server UDP connections. The Media Server firewall must allow inbound connections from the Domain and Internal servers on UDP ports 161, 5064, 10161, and in the range 40000-45000.

- > To setup the firewall for the MS:
- **1.** Start > Administrative Tools > Windows Firewall with Advanced Security.
- 2. Select Inbound Rules > New Rule.
- 3. Select the Port radio button and click Next.
- 4. Select UDP Specific local ports and type in the UDP ports separated by commas and a dash separating the range (161, 5064, 10161, 40000-45000).
- 5. Select the Allow the connection and click **Next**.
- 6. Check "Domain" and "Private" and click Next.
- 7. Name the rule and click **Finish** (the rule will be active immediately).

8 Microsoft Skype for Business Deployment

In a Skype for Business environment, SmartTAP 360° will deploy a trusted plugin application on the standard or enterprise Front End Server (Pool). The configured plugin sends the necessary signaling from the FE, SBS or SBA to the SmartTAP 360° server(s) so that SmartTAP 360° is aware of call states only for recorded calls. Using the call signaling, SmartTAP 360° can then correlate the SRTP data to record the complete call. The SRTP data is captured in various ways depending upon what call types need to be recorded. See table below for details.

	Capture Ca	III Signaling	Capture Call Audio					
Criteria	Front End Server	SBA Appliance	Proxy Server	Edge Server	Mediation Server	Conference Server	Mirror Port	
Requires SmartTAP software	YES	YES	YES	YES	YES	YES	n/a	
Data Captured	SIP	SIP	SRTP	SRTP	SRTP	SRTP	SRTP	
Mirror Port Required	n/a	n/a	n/a	n/a	n/a	n/a	YES	
Media Path Routing	n/a	n/a	YES	YES	n/a	n/a	n/a	
Llient to Client	 Image: A second s	×	×	×	n/a	n/a	×	
📧 PSTN – Media Bypass Disabled	 Image: A second s	✓	×	×	×	n/a	×	
PSTN - Media Bypass Enabled	 Image: A second s	×	 Image: A second s	×	n/a	n/a	×	
Conferencing	 Image: A second s	n/a	 Image: A second s	✓	n/a	✓	✓	
Remote / Federated	 Image: A second s	n/a	n/a	×	n/a	n/a	n/a	
Nobile Mobile	×	n/a	n/a	×	n/a	n/a	n/a	
🚹 Home User	×	n/a	n/a	×	n/a	n/a	n/a	

Figure 8-1:	Capture	Call	Signaling	-	1
-------------	---------	------	-----------	---	---

= Call Type Supported | n/a = Not Applicable

The following table lists the SmartTAP 360° software components and the appropriate deployment server.

	Capture Call Signaling		Capture Call Audio						
Software	SmartTAP Server	Front End Server	SBA Appliance	Proxy Server	Edge Server	Mediation Server	Conference Server	Hirror Port	And a second sec
S4B / Lync plug-in	n/a	×	×	n/a	n/a	n/a	n/a	n/a	n/a
Application Server	×	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Communication Server	 Image: A second s	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Database	×	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Media Server	×	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Call Delivery	×	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Media Delivery	n/a	√ 1	√ 1	n/a	×	×	×	n/a	n/a
Media Proxy	n/a	n/a	n/a	√ 2	n/a	n/a	n/a	n/a	n/a
SmartTAP CWE Toolbar	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	√ 3

Figure 8-2: Capture Call Signaling - 2 Capture Call Signaling Captu

¹ Assumes Mediation or Conference server are co-located.

² Proxy Server must be installed on dedicated physical or virtual server.

³ Requires configuration of Microsoft Skype for Business client. No software is installed.

Unlike other IP Station side IP PBX, Skype for Business recording requires the installation of the AudioCodes Microsoft trusted plugin on the Front End (FE) servers, and the Skype for Business specific configuration on the Call Delivery.

This chapter describes the following procedures for installing and configuring SmartTAP 360° to Record Skype for Business:

- Installing SmartTAP 360° Skype for Business plugin (see Installing Skype for Business Plugin on page 67 Installing Skype for Business Plugin on page 67)
- Installing SmartTAP 360° Call Delivery, choose Microsoft Lync as network type (see Installing Call Delivery for Skype for Business (IP-based Recording) on page 87
- Installing Media Proxy in case of utilizing the Media Proxy solution (see Installing Media Proxy Server for Skype for Business on page 100)
- Installing SmartTAP 360° Media Delivery (see Installing Media Delivery Server for Skype for Business on page 108)
- Installing Annoucement Server (see Installing Announcement Server on page 109)
- Installing SmartTAP 360° Monitoring Service (see Installing SmartTAP 360° Monitoring Service on page 121)

Skype for Business Remote Branch Site

The Remote site is typically a branch location that connects back to the main data center. The branch site may or may not have survivable telephony services if the WAN goes down. SmartTAP 360° deployed in the branch location can record user/device calls regardless of WAN up/down.


Figure 8-3: Skype for Business Remote Branch Site

Survivable Branch Site

In the main datacenter, you may deploy an All-In-One solution or distributed. In the branch, you will typically use the Distributed configuration setup because not all components are required in the branch site.

In the branch, the following components are required:

Microsoft SBA:

- Install Skype for Business plugin on SBA (Separate installer not part of the distributed setup package). See Section Microsoft Skype for Business Deployment on page 62Microsoft Skype for Business Deployment on page 62.
- (Optional) Install Media Delivery to record PSTN calls. See Section Installing Media Proxy Server for Skype for Business on page 100.

SmartTAP 360° Server:

- Install Communication Server. See Section Installing SmartTAP 360° Communication Server on page 35.
- Install Media Server. See Section Installing SmartTAP 360° Media Server on page 36.
- Install Call Delivery Server. See Section Installing SmartTAP 360° Call Delivery Server on page 43.

Media Proxy: (Optional):

Install Media Proxy (Optional method to record Internal IP-to-IP and PSTN calls). See Section Installing Media Proxy Server for Skype for Business on page 100.

Before Installing Microsoft Skype for Business Components

This section lists the Microsoft requirements for the SmartTAP 360° components for different Skype for Business deployments.

Unified Communications Managed API (UCMA):

- For Annoucement server, SmartTAP 360° Monitoring Service, Microsoft Lync Server 2013 Plugin, Skype for Business 2015 Plugin and Skype for Business 2019 Plugin, this component must be pre-installed with the following versions:
 - Skype for Business 2019: UCMA 6.0
 - Skype for Business 2015: UCMA 5.0
 - Lync Server 2013: UCMA 4.0
- For Media Proxy server, installation is not required
- UCMA6 Windows Server Updates:
 - Windows Server 2016 with the latest update
 - Windows Server 2019 with the latest update
- UCMA6 Runtime requirements:
 - The target platform must be a 64-bit computer
 - Microsoft .NET framework 4.7 or later service packs
 - For details on the latest UCMA6 updates, see: <u>https://www.microsoft.com/en-us/download/details.aspx?id=57507</u>

Windows Server 2016:

- The Annoucement Server, SmartTAP 360° Monitoring Service and the Skype for Business 2019 Plugin must run on Windows Server 2016 when running on the Skype for Business 2019 platform.
- Anti-virus software If the Windows server run anti-virus software, then SmartTAP 360° components should be included in the anti-virus software's exception list.
- HTTPS: several of the installation setups includes an option to enable an HTTPS connection between the SmartTAP 360° Application server and the Announcement server. These settings, do not entirely complete the HTTPS setup, therefore you must also run the procedures described in Configuring HTTP/S on page 156.
- For Annoucement server-specific requirements, see Annoucement Server-Specific Requirements on the next page
- For SmartTAP 360° Monitoring Service-specific, see SmartTAP 360° Monitoring Service-Specific Requirements on the next page
- For details on configuring a remote branch site in a Skype for Business deployment, see Skype for Business Remote Branch Site on page 63

Annoucement Server-Specific Requirements

- Ensure the Annoucement installation server platform is joined to the domain
- Stand-alone Physical or Virtual server
- Microsoft Windows Server 2012/R2 and Microsoft Windows Server 2016
- Microsoft Windows Server 2012 and Microsoft Windows Server 2016 features:
 - Windows Server Media Foundation
 - Windows Identify Foundation
- Windows Server 2016 is required when recording on the Skype for Business 2019 platform.
- From the Skype for Business Installation Media:
 - Skype for Business Local Config Store (Skype for Business Install CD) Core components
 - Skype for Business Administration Tools (Skype for Business Install CD)

Firewall Configuration

It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. See Chapter Firewall Configuration on page 51.

SmartTAP 360° Monitoring Service-Specific Requirements

The SmartTAP 360° Monitoring Service-Specific requirements are described below:

- Should be installed on a server that is joined to the domain
- Media Foundation
- Health Monitor installed locally or on a remote machine.
 - For the Skype for Business 2015 and 2019 deployment:
 - Skype for Business Local Config Store (Skype for Business Install CD) Core components
 - Skype for Business Administration Tools (Skype for Business Install CD)
 - For the Lync 2013 deployment:
 - Lync 2013 Local Config Store (Lync 2013 Install CD) Core components
 - Skype for Business Administration Tools (Lync 2013 Install CD)
 - Make sure UCMA 4.0 is installed.

Installing Skype for Business Plugin

The Skype for Business plugin is a Microsoft trusted application that communicates with the Front End Software and provides the SmartTAP 360° server with the signaling and metadata of calls to record. The Skype for Business plugin must be installed on every Front End Server, SBA or SBS that may process calls to record.

The following pre installation actions must be performed:

- Skype for Business Plugin-Pre-install Setup on AD Domain Controller below
- Skype for Business Plugin Pre-install Setup on each Front End, SBS or SBA on page 71

The installation procedure is described in Section Skype for Business Plugin Installation Procedure on page 80

- It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.
 - Install the Skype for Business plugin described in this section on every Front End Server processing calls to record.
 - Before proceeding, ensure that you have noted the installation requirements (see Before Installing Microsoft Skype for Business Components on page 65.

Skype for Business Plugin-Pre-install Setup on AD Domain Controller

This section describes the pre-install setup for the Skype for Business Plugin on the Active Directory Domain Controller.

Do the following:

- 1. Create a user account for SmartTAP 360° on the domain. For example "SmartTAPUser":
 - In the Active Directory Users and Computers folder, select the Users folder and then right-click New > User.

	Active Dir	ecto	ry Users and Co	mputers	_ 🗆 🗙
File Action View Help					
♦ ♦ 2 🖬 ¾ 🗉	🗙 🗐 🖬 🗟	?	53 🕺 📷	7 🗾 🐍	
📃 Active Directory Users and	Name			Туре	Description 🔨
▷ 🚞 Saved Queries	🚨 Abraham			User	
⊿ 🏥 S4B.interop	💄 Administrat	or:		User	Built-in account for a
þ 🖬 acs	용 Allowed RO	DC P	assword Replicati	Security Group	Members in this grou
▷ Builtin	🚨 Anatoly1			User	
Computers	👗 Anatoly2			User	
Domain Controller	🚨 Anatoly3			User	
ForeignsecuntyPri SecurityP	🚨 Anatoly4			User	
D CostAnd Odna D CostAnd Odna D Managed Service 4	💄 Burolo User			User	
Microsoft Exchange	🎎 Cert Publisł	ners		Security Group	Members of this grou
▷ 3 OfirTest	🎎 Cloneable D)omai	in Controllers	Security Group	Members of this grou
OperationsManage	🎎 CSAdminist	rator		Security Group	Members of this grou
▷ CpsMgrLatencyMi	8 CSArchiving	gAdm	iinistrator	Security Group	Members of this grou
👂 🧮 Program Data	8 CSHelpDesk	<		Security Group	Members of this grou
þ 🚞 System	& CSLocation	Admi	nistrator	Security Group	Members of this grou
Leave Data acts Co	Nervisten 👷 👷 👷	tChat	Administrator	Security Group	Members of this grou
	introl	GroupAdministrator		Security Group	Members of this grou
▶ 🛄 [Find		GroupManager		Security Group	Members of this grou
New	•		Computer		mbers of this grou
All Tasks	۲		Contact		mbers of this grou 🗸
< III View	•		Group		>
Create a new Refresh			InetOrgPerson		
Export List			msDS-ResourcePro	pertyList	
P			msExchDynamicDi	stributionList	
Properties			msImaging-PSPs		
Help			MSMQ Queue Alia	s	
			Printer		
			User		
			Shared Folder		

Figure 8-4: Active Directory Users and Computers



	New Object - User	x
👗 Create in:	S4B.interop/Users	
<u>F</u> irst name:	SmartTAPUser Initials:	
Last name:		
Full n <u>a</u> me:	SmartTAPUser	
User logon name:		
SmartTAPUser	@S4B.interop 🗸	
User logon name (pre	- <u>W</u> indows 2000):	
S4B\	SmartTAPUser	
	< <u>B</u> ack <u>N</u> ext > Cance	I

b. Enter the name of the SmartTAP 360° user in the First Name and User logon name fields and click **Next**.

New Object - User
Create in: S4B.interop/Users
Password:
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 8-6: Password Never Expires

c. Enter a password, confirm the new password, select the "Password never expires" check box and click **Next**.

The following confirmation dialog is displayed:

Figure 8-7: User Add Confirmation

New Object - User	×
Create in: S4B.interop/Users	
When you click Finish, the following object will be created:	
Full name: SmartTAPUser	^
User logon name: SmartTAPUser@S4B.interop	
The password never expires.	
	~
< <u>B</u> ack Finish	Cancel

- d. Click Finish.
- 2. (Optional) Add the account to the "CSAdministrator" group. This membership is not mandatory; however, may be required for running the Plugin installation. The account can be removed from the group after the installation:

a. Right-click the newly created SmartTAP 360° user and choose Add to a group.

				0 1-
	Active Directo	ory Users and Co	mputers	_ D X
File Action View Help				
🗢 🔿 🖄 📅 🤾 🗎	🗙 🗐 🖻 📑 🚺	1 🖬 🕺 🐮 🛍	7 🛛 🔕	
📔 Active Directory Users and	Name		Туре	Description ^
Saved Queries	💐 RAS and IAS Sen	vers	Security Group.	Servers in this group c
⊿ 🙀 S4B.interop	🚨 Read-only Dom:	ain Controllers	Security Group.	Members of this grou
þ 🖬 acs	& RTCComponent	:UniversalServices	Security Group	Members can be used
Builtin	& RTCHSUniversal	Services	Security Group.	Members can be used
Computers	& RTCProxyUniver	salServices	Security Group.	Members can be used
b EoreignSecurityPri	RTCSBAUniverse	alServices	Security Group.	Members have read a
b StandFound	Sector Representation Representatio Representatio Representation Representation Representation R	nfigReplicator	Security Group	Members can particip
þ 📔 Managed Service A	RTCUniversalGlo	balReadOnlyGroup	Security Group	Members have read a
Microsoft Exchang	RTCUniversalGlo	balWriteGroup	Security Group.	Members have write a
þ 🧊 OfirTest	RTCUniversalRea	ad Only Admins	Security Group.	Members can only rea
þ 📔 OperationsManag	RTCUniversalSB/	4 lechnicians	Security Group.	Members have read as
D DpsMgrLatencyMi	RTCUniversalSer	verAdmins	Security Group.	Members can manage Members have avoid a
þ 📔 Program Data	RTCUniversalser	verkeadUniyGroup	Security Group.	Members have read a
System	RTCUniversalus	erAamins erPeadOoluGroup	Security Group.	Members can manage
Users	Scheme Admine	erkeauoniyoroup	Security Group.	Merribers riave reau a
p Microsoft Exchang Microsoft Exchang	Securit TAD Harm	•	Security Group.	Designated administra
TPM Devices	& SystemMai	Copy		-
, <u> </u>	& SystemMai	Add to a group		
	💁 System Mai	Name Mappings		
	🛃 System Mai	Disable Account		
	Tal Shlidar	Pacat Daccound		~
	<	Reset Password	_	>
Allows you to add the selected	objects to a gro	Move		
		Open Home Page		
		Send Mail		
		All Tasks	•	
		Cut		
		Delete		
		Rename		
		Properties		
		Help		

Figure 8-8: Add SmartTAP 360° user to CSAdministrators group

b. Enter CSAdministrator and then click Check Names. The successfully recognized entry is underlined.

Select Groups	X
Select this object type: Groups or Built-in security principals	Dbject Types
Erom this location: S4B.interop	Locations
Enter the object names to select (<u>examples</u>): CSAdministrator	Check Names
Advanced	Cancel

Figure 8-9: Add Smart TAP User to CSAdministrator

- c. Click **OK**. A confirmation screen is displayed.
- Add the SmartTAP 360° account to the RTCUniversalReadOnlyAdmins group. This account must be part of "RTCUniversalReadOnlyAdmins" group. This group membership enables the Plug-in to retrieve the Skype For Business topology:
 - a. Right-click the newly created SmartTAP 360° user and choose Add to a group.
 - b. Enter RTCUniversalReadOnlyAdmins and then click Check Names. The successfully recognized entry is underlined.

Figure 8-10: Add Smart TAP User to RTCUniversalReadOnlyAdmins

Select Groups	x
Select this object type:]
Groups or Built-in security principals	Object Types
From this location:	
S4B.interop	Locations
Enter the object names to select (<u>examples</u>):	
<u>RTCUniversalReadOnlyAdmins</u>	<u>C</u> heck Names
Advanced OK	Cancel

c. Click **OK**. A confirmation screen is displayed.

Skype for Business Plugin Pre-install Setup on each Front End, SBS or SBA

This section describes the setup on the Front End, SBS or SBA.

> Do the following:

- 1. Add new "SmartTAP 360° User" to the local "Administrators" group:
 - a. Log in to the machine using a local administrator or a domain administrator account.
 - b. Open the Computer Management window.

- c. Open the Local Users and Groups folder.
- d. Select the Groups folder and then select the Administrators entity.
- e. Right-click and choose Add to Group.

Figure 8-11: Add SmartTAP 360° user to the Administrators group

*	Action View Help Action View Help Task Scheduler Task Scheduler Action View Partonson Action View Partonson Computer Management (Local System Tools Task Scheduler Action View Partonson Computer Management (Local System Tools Task Scheduler Action View Partonson Computer Management (Local Computer (Local (Local Read-only (Local) Computer (Local (Local) (Local) Computer (Local)					3 X
File Action View Help						
← ⇒ 2	?					
🜆 Computer Management (Local	Name	Description		^	Actions	
⊿ 🎁 System Tools	🕭 Access Contr	ol Assist Members of	this group can remot		Groups	
þ 🕑 Task Scheduler	Admini		have complete an		Groups	
Event Viewer	🜆 Backup	Add to Group	ors can override se		More Actions	,
▷ 3 Shared Folders	🕭 Certifica	All Tasks 💦	is group are allowe		Administrators	
⊿ A Local Users and Groups	🕭 Cryptog	Delete	uthorized to perfor		More Actions	۰.
Users	🕭 Distribu	Panama	llowed to launch, a		more rectorio	
Groups Derformance	🕭 Event Lo	Trename	is group can read e			
Device Manager	🕭 Guests	Properties	e same access as m			
4 Ge Storage	🕭 Hyper-\	Help	is group have com			
Storage Mindows Server Backur	🌆 IIS_IUSR 🛛 🚽	Built-in grou	ap used by Internet Inf			
🚔 Disk Management	🌆 Network Con	figuratio Members in	this group can have s			
⊿ Services and Applications	🌆 Performance	Log Users Members of	this group may sche			
Internet Information Sei	🌆 Performance	Monitor Members of	this group can acces			
Routing and Remote Ac	🕭 Power Users	Power Users	are included for back	=		
🔍 Services	🌆 Print Operato	ors Members ca	ın administer printers			
🗃 WMI Control	🌆 RDS Endpoin	t Servers Servers in th	is group run virtual m			
▷ If SQL Server Configuratic	🌆 RDS Manager	ment Ser Servers in th	is group can perform			
🔈 🖙 Message Queuing	🌆 RDS Remote .	Access S Servers in th	is group enable users			
	🌆 Remote Desk	top Users Members in	this group are grante			
	🌆 Remote Man	agement Members of	this group can acces			
	🜆 Replicator	Supports file	e replication in a dom			
	🜆 Users	Users are pre	evented from making			
	🌆 RTC Compor	nent Loca Skype for Bu	isiness Server Web Co			
	🜆 RTC Local Ad	lministra RTC domair	n Server Administrator			
	🜆 RTC Local Co	onfig Rep Skype for Bu	isiness Server replicati			
	🜆 RTC Local Re	ad-only RTC domain	n Read-only Administr			
	🜆 RTC Local Us	er Admi RTC domair	u User Administrators			
	🌆 RTC Server A	pplications Skype for Bu	isiness Server Server a			
	🌆 RTC Server Lo	ocal Group Skype for Bu	isiness Server service			
	🧟 SQL Server 2 0 0	5SQLBro Members in	the group have the re			
× III >	A CAP I PI	· . · · · · · · ·	and a second	×	<u> </u>	
Change Group membership.						

f. In the Administrator Properties window, click Add.

Figure 8-12:	Adminis	trators P	roperties		
	Adminis	trators Pro	perties	?	x
General					
Adminis	strators				
D <u>e</u> scription:	Administrato to the comp	rs have comp uter/domain	ete and unrestricte	d acces	s
Members:					
S4B\Domain & S4B	Admins				
A <u>d</u> d	<u>R</u> emove	Changes are not eff user logs	to a user's group m fective until the nex on.	embersł «t time tł	nip ne
	ОК	Cancel	Apply	Hel	p

g. Enter the name of the SmartTAP 360° user (that you created on the Domain Controller) and then click Check Names. The successfully added entry is highlighted.

Figure 8-13: SmartTAP 360° User Added to Administrators

Select Users, Computers, Service Accounts, o	or Groups 🛛 🗙
Select this object type: Users, Service Accounts, or Groups	Dbject Types
Erom this location: S4B.interop	Locations
Enter the object names to select (<u>examples</u>): SmartTAPUser (SmartTAPUser@S4B.interop)	<u>C</u> heck Names
Advanced	Cancel

- **h.** Click OK. A confirmation screen is displayed.
- 2. Add the SmartTAP 360° user to the RTCServerApplications group. The group membership enables the Plug-in to register and operate as a Skype For Business Trusted application:
 - a. Select the RTCServerApplications entity, right-click and choose Add to Group.

File Action View Help Image: Computer Management (Local System Tools Description Name Description Image: Computer Management (Local Description Name Description Image: Computer Management (Local Description Market Social Description Market Social Market Social Description Access Computer Management Description Market Social Description Market Social Description Image: Description Description Market Social Description Market Social Description Market Social Description Market Social Description Image: Description Description Market Social Description Market Social Description Market Social Description Market Social Description Image: Description Description Description Market Social Description M	2		Computer M	anagement		_ D X
Image: Struct Tods Image: Struct Tods Actions Image: Struct Tods Image: Struct Tods Image: Struct Tods Image: Struct Tods	File Action View Help					
Computer Management (Local Version System Tools System Tools System Tools System Tools System Tools System Tools Sector Version <	🗢 🔿 🖄 🖬 🔀 🛛	? 🗊				
Image: System Tools Access Control Assist Members of this group can remot Administrators More Actions P Image: Users Users Oscie Amarger Subscie Confluence Confluence Guests Members of this group can read e More Actions	🌆 Computer Management (Local	Name	Description		^	Actions
Image: Control Viewer Administrators Administrators Administrators Administrators Administrators Backup Operators More Actions Price Image: Comparise on the comparise on the communication of this group rane and end on the communication operators Deparise on the communication operators Members of this group rane and end More Actions Price Image: Stratege on the communication operators Members of this group rane access Price Price Price Price Image: Stratege on the communication operators Price Price Price Price Price Image: Stratege on the communication operators Price Price Price Price Price Image: Stratege on the communication operators Price Price P	⊿ 🎁 System Tools	🕭 Access Control Assist	Members of this group can	remot		Groups
b Event Viewer Backup Operators Members of this group operators Members of this group operators Members of this group operators More Actions <	▷ (④) Task Scheduler	Administrators 🔬	Administrators have comple	ete an		010003
b gills Shared Folders Certificate Service DC Members of this group are allowed b Users Users Cryptographic Operat Members are authorized to perform b Over Performance Service Managerent Members are allowed to launch. a More Actions c Over Stars Services and Applications Members are allowed to launch. a More Actions c Over Stars Services and Applications Members of this group can read e More Actions c Over Users Built-in group used by Internet Infr Members of this group can acces Members of this group can acces c Over Users Power Users Power Users Power Users Power Users c Services Power Users Power Users Power Users Services in this group can perform c Services Power Users Power Users Services in this group can perform c Services Power Users Services in this group can perform c Mill Control Members of this group can perform Services in this group person c Ros Management Ser Services in this group can acces Services in this group can acces c Will Control Members of this group can acces Services in this group can acces c Will Control Members in this group can acces Service in this group	Event Viewer	🜆 Backup Operators	Backup Operators can over	ride se		More Actions 🔹 🕨
Image: Construction Cryptographic Opertu. Members are authorized to perform Image: Construction Distributed COM Users Members are authorized to perform Image: Construction Distributed COM Users Members are authorized to perform Image: Construction Distributed COM Users Members of this group ner red e Image: Construction Guests Guests Image: Construction Members of this group ner red e Guests Image: Construction Members of this group ner red e Guests Image: Construction Members of this group ner red e Members of this group ner red e Image: Construction Members of this group ner red e Members of this group ner red e Image: Construction Members of this group ner red e Members of this group ner softe Image: Construction Performance Log Users Members of this group ner ner de Image: Construction Performance Log Users Members of this group ner ner de Image: Construction Performance Log Users Members of this group ner ner de Image: Construction Performance Log Users Members of this group ner ner de Image: Construction Performance Log Users Performance Log Users Image: Construction Performance Log Users Servers in this group ner ner de	▷ 101 Shared Folders	🜆 Certificate Service DC	Members of this group are a	allowe		RTC Server Applicatio 🔺
Users © istributed COM Users Members are allowed to launch, a © Orepsile Event Log Readers Members of this group can reade © Sorge Device Manager © Windows Server Backur Members of this group have com © Disk Managernent Sorge © Sorge Network Configuration P Windows Server Backur Network Configuration P Members of this group nave com Members of this group nave com Disk Managernent Network Configuration P Members of this group nave com Members of this group can acces P Mintomstanders Performance Log Users Power Users Power Users are included for back P Mintomstanders Performance Monitor Members of this group ran perform Power Users are included for back P Mintomstanders Performance End Users Members of this group ran perform Power Users Power Users are included for back P Message Queuing RDS Remote Access S Servers in this group ran perform P RDS Endpoint Servers Servers in this group ran acces Servers in this group ran acces Replicator Supports file replication in a dom Servers in this group ran acces Replicator Supports file replication in a dom Server Administrator	⊿ A Local Users and Groups	🌆 Cryptographic Operat	Members are authorized to	perfor		More Actions
Image: Structure Event Log Readers Members of this group can read e Image: Structure Guests Guests have the same access as m Image: Structure Guests Guests have the same access as m Image: Structure Flyper-V Administrators Built-in group used by Internet Inf Image: Structure Flyper-V Administrators Built-in group used by Internet Inf Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Flyper-V Administrators Members of this group can access Image: Structure Structure Members of this group can access Image: Structure Structure Members of this group can acces	Users	🜆 Distributed COM Users	Members are allowed to lau	inch, a		More Actions
Image: Construct of the series of this group have com. Image: Construct of the series of thi	Groups	🜆 Event Log Readers	Members of this group can	read e		
 Bevice manager Hyper-V Administrators Members of this group have com Built-in group used by Intermet Inf Built-in group used by Intermet Inf Bevices and Applications Performance Log Users Members of this group may sche Performance Monitor Members of this group may sche Power Users Power Users are included for back Pomore Users Privers in this group run virtual m SQL Server Configuration RDS Endpoint Servers Rervers in this group enable users Servers in this group enable users Servers in this group are grante Members of this group are grante Remote Desktop Users Rervers this group enable users Renote Desktop Users Rervers this group enable users Renote Desktop Users Members of this group are acces Renote Management Rerote Management Rerote Component Loca Skype for Business Server Web Co RTC Local Config Rep Skype for Business Server replicati RTC Local Read-only RTC Compin User Administrators RTC Core Applicators Convertions and Skype for Business Server replicati RTC Local Read-only RTC Core Administrators RTC Core Administrators RTC Server Local Grap Administer Server Administrators RTC Server Local Grap Administer Server Administrators RTC Serv	Performance	🜆 Guests	Guests have the same acces	is as m		
> Windows Server Backur, Built-in group used by Internet Inf > Disk Management Network Configuration. > Services and Applications Performance Log Users > Rower Users Power Users > Power Users Power Users > WMI Control Performance Konitor > Wintows Server Configuration Performance Monitor > WMI Control Performance Monitor > WMI Control Performance Servers > WMI Control RDS Endpoint Servers > WMI Control RDS Remote Access S > WMI Source Log Users Servers in this group can perform > WMI Source Configuration Remote Magement > WMI Source Configuration Remote Magement > Wessage Queuing Remote Magement Remote Magement Members of this group can acces Remote Magement Members of this group can acces Replicator Supports file replication in a dom Wessage Queuing RTC Local Administra Replicator Supports file replication in a dom Replicator Supports file replication in a dom RTC Local Administra RTC Local Administra	a 🖙 Storage	🜆 Hyper-V Administrators	Members of this group have	e com		
Image: Services and Applications Network Configuratio Members of this group may sche Image: Services and Applications Performance Log Users Members of this group may sche Image: Services Performance Monitor Members of this group may sche Image: Services Power Users are included for back Power Users are included for back Image: SQL Server Configuration RDS Endpoint Servers Services Image: SQL Server Configuration RDS Renate Access S Servers in this group run virtual m Image: SQL Server Configuration RDS Renate Access S Servers in this group run virtual m Image: Remate Access Server Sint Server Sint Server Sint Server Sint Server Sint Server Sint Server Server Web Co Remate Access S Replicator Supports file replication in a dom Server Server Publicator Image: Ret Local Config Rep Skype for Business Server replicat Skype for Business Server replicat RTC Local Config Rep RTC Coll Read-only RTC domain Read-only Administrum. RTC domain Read-only Administrum. RTC Server Applicationc Change Group membership. Add to Group vice vice Image: Solu Server 200SQLBr All Tasks Her rem Vice<	Mindows Server Backur	A IIS_IUSRS	Built-in group used by Inter	net Inf		
Services and Applications Services and Applications Services and Applications Services WMI Control Sources and Applications WMI Control Sources and Applications Services WMI Control Sources and Minister Sour	Disk Management	🌆 Network Configuratio	Members in this group can	have s		
Internet Information Set Performance Monitor Members of this group can acces Routing and Remote Ac Power Users Power Users are included for back Power Users WMI Control Power Users Members can administer printers Power Users WMI Control RDS Endpoint Servers Servers in this group can perform Power Users Members Queuing RDS Endpoint Servers Servers in this group can perform Power Users Remote Maagement Ser Remote Desktop Users Servers in this group can acces Power Users Remote Maagement Members of this group can acces Remote Maagement Members of this group can acces Remote Maagement Supports file replication in a dom Users Users Users are prevented from making RTC Local Administram. RTC domain Server Administrator Skype for Business Server Web Co RTC Local Config Rep Skype for Business Server replicati RTC Local Config Rep RTC domain Serve Administrator RTC Concil Read-only RTC domain User Administrators RTC Server Local Grop Add to Group Ver To Ver To Ver To RTC Server Local Grop Add to Group <td>A Services and Applications</td> <td>🜆 Performance Log Users</td> <td>Members of this group may</td> <td>/ sche</td> <td></td> <td></td>	A Services and Applications	🜆 Performance Log Users	Members of this group may	/ sche		
Routing and Remote Ac Services WMI Control RDS Endpoint Servers Remote Desktop Users Remote Desktop Users Remote Desktop Users Remote Management. Members of this group can acces Replicator Supports file replication Users Users Users RTC Local Administra RTC Local Config Rep Stype for Business Server replicati RTC Local Config Rep RTC Local User Admin. RTC Conver 2005QUBr RTC Server Application Collect	Internet Information Sei	🜆 Performance Monitor	Members of this group can	acces		
Services WMI Control RDS Endpoint Servers Servers in this group run virtual m RDS Management Servers Revers in this group can perform Remote Desktop Users Remote Management Members of this group can acces Replicator Supports flie replication in a dom Replicator Supports flie replication in a dom Residence of the representation of the representation of the representation Replicator Supports flie replication in a dom Replicator Supports flie replication in a dom Residence of the representation of th	Routing and Remote Ac	🜆 Power Users	Power Users are included fo	r back	Ξ	
WMI Control RDS Endpoint Servers Servers in this group run virtual m RDS SQL Server Configuratic RDS Remagement Servers Servers in this group an ap le users RDS Remote Access S Servers in this group an ap le users RDS Remote Access S Servers in this group are grante RDS Remote Access S Servers in this group are grante Remote Desktop Users Members in this group are grante Replicator Supports file replication in a dom Users Users or uspont toca RTC Local Administra RTC Component Loca RTC Local Administra RTC domain Read-only Administra RTC Local Read-only RTC domain Read-only Administra RTC Call User Admin RTC domain luser Administrators RTC Server Application: Extra domain Read-only Administrators RTC Server Application: Change Group membership. Vice Vice Add to Group Vice Sol_Server200SQLBr All Tasks He re Vice	🔍 Services	🜆 Print Operators	Members can administer pr	inters		
Image: SQL Server Configuratic Description Image: RDS Management Servers in this group can perform Description of the servers in this group can bable users Description of the servers in this group can bable users Description of the servers in this group can bable users Description of the server server the server and t	🗃 WMI Control	🜆 RDS Endpoint Servers	Servers in this group run vir	tual m		
Image: Solution of the state of the stat	Ig SQL Server Configuratic	🌆 RDS Management Ser	Servers in this group can pe	rform		
Remote Desktop Users Members in this group are grante Remote Management Members of this group can acces Replicator Supports file replication in a dom Users Users are prevented from making RTC Component Loca Skype for Business Server Web Co RTC Local Administra RTC domain Server Administrator RTC Local Config Rep Skype for Business Server replicati RTC Local Config Rep Skype for Business Server replicati RTC Local Config Rep RTC domain Read-only Administrators RTC Corol User Admin RTC domain User Administrators RTC Server Application Chomain Read-only Administrators SQLServer200SQLBr Add to Group Vice Line	🔈 🖙 Message Queuing	🜆 RDS Remote Access S	Servers in this group enable	users		
Remote Management Members of this group can acces Replicator Supports file replication in a dom Users Users are prevented from making RTC Component Loca Skype for Business Server Web Co RTC Local Administra RTC domain Server Administrator RTC Local Config Rep Skype for Business Server replicati RTC Local Config Rep RTC domain Read-only Administrator RTC Local User Admin RTC domain Read-only Administrator RTC Local User Admin RTC domain Read-only Administrator RTC Server Application: Choma for Business Canage		🜆 Remote Desktop Users	Members in this group are g	grante		
Replicator Supports file replication in a dom Users Users are prevented from making RTC Component Loca Skype for Business Server Web Co RTC Local Administra RTC Local Config Rep RTC Local Config Rep Skype for Business Server replicati RTC Local Config Rep RTC domain Read-only Administra RTC Local User Admini RTC domain Read-only Administrators RTC Server Application: School User Administrators Seaver Server 7 an RTC Server Local Gro Add to Group Vice Vice SQLServer200SSQLBr All Tasks Change Group membership. Delete		🌆 Remote Management	Members of this group can	acces		
Users Users are prevented from making RTC Component Loca Skype for Business Server Web Co RTC Local Administra RTC Local Config Rep RTC Local Config Rep RTC Local Config Rep RTC Local User Administrators RTC Local User Administrators RTC Local User Administrators RTC Server Applications Server replications RTC Server Applications RTC Server Local Gro Add to Group Vice RTC Server 2005OLBr All Tasks the re Delete		🜆 Replicator	Supports file replication in a	a dom		
RTC Component Loca Skype for Business Server Web Co RTC Local Administra RTC domain Server Administrator RTC Local Config Rep Skype for Business Server replication RTC Local Read-only RTC domain Read-only Administrators RTC Local User Admin. RTC domain Read-only Administrators RTC Local User Admin RTC domain Read-only Administrators RTC Server Applications: Store for Business Cerver 3 RTC Server Local Gro Add to Group Vice SOLServer200SOLBr All Tasks the re Delete		🜆 Users	Users are prevented from m	aking		
RTC Local Administra RTC domain Server Administrator RTC Local Config Rep Skype for Business Server replication RTC Local Read-only RTC Local Read-only RTC Administrators RTC Server Applications RTC Server Applications RTC Server Applications RTC Server Local Gro Add to Group Vice RTC Server 2005SQLBr All Tasks the re Delete		🌆 RTC Component Loca	Skype for Business Server W	′eb Co…		
RTC Local Config Rep Skype for Business Server replicati RTC Local Read-only RTC domain Read-only Administr RTC Local User Administ. RTC domain User Administrators RTC Server Local Gro Add to Group RTC Server Local Gro Add to Group Vice Change Group membership.		🌆 RTC Local Administra	RTC domain Server Admini:	strator		
RTC Local Read-only RTC domain Read-only Administr RTC Jocal User Admin. RTC domain User Administrators RTC Server Application: Stowns for Purimetry Stow		🌆 RTC Local Config Rep	Skype for Business Server re	plicati		
RTC Local User Admi RTC domain User Administrators RTC Server Applications: Strong Acceleration Server a RTC Server Local Gro Add to Group Vice Change Group membership. Delete		🌆 RTC Local Read-only	RTC domain Read-only Adr	ninistr		
Change Group membership. All Tasks the rem.		🜆 RTC Local User Admi	RTC domain User Administ	rators		
Image: Construction of the co		RTC Server Applications	Shuna for Rusinass Sanvar Sa	rver a		
K MI > SQLServer2005SQLBr All Tasks the re Change Group membership. Delete		🌆 RTC Server Local Gro	Add to Group	vice		
Change Group membership. Delete	< III >	SQLServer2005SQLBri	All Tasks 🔹 🕨	the re	$\overline{}$	
	Change Group membership.		Delete			



Figure 8-15: RTC Server Applications Properties

RTC	C Server Applications Properties 2	
General		_
🔊 RTC Se	erver Applications	
D <u>e</u> scription:	Skype for Business Server Server applications are granted appropriate local permissions through this group	
<u>M</u> embers:		
A <u>d</u> d	Changes to a user's group membership are not effective until the next time the user logs on.	
	OK Cancel Apply Help	

- **b.** In the RTC Server Applications Properties screen, click **Add**.
- c. Enter the name of the SmartTAP 360° user (that you created above on the Domain Controller) and then click Check Names. The successfully added entry is highlighted.

0			
Sel	ect Users, Computers, Servic	e Accounts, or	Groups 🛛 🗙
<u>S</u> elect this ob	ject type:		
From this loca	tion:		Delect Types
S4B.interop	ect names to select (examples):		Locations
SmartTAPUs	er [SmartTAPUser@S4B.interop]		<u>C</u> heck Names
Advanced		ОК	Cancel

Figure 8-16: Add RTC Server Applications User

- d. Click OK. A confirmation screen is displayed.
- 3. Assign "logon as service" privileges to the "SmartTAPUser" account:
 - a. Open Administrative Tools > Local Policies > User Rights Assignment.
 - **b.** Select the Log on as a service entity.
 - c. Enable the Computer Browser service.

Figure 8-17:	Local	Security	Policy
--------------	-------	----------	--------

1	Local Security Policy		x
<u>File Action View H</u> elp			
🗢 🄿 🞽 🖬 🗙 🖬 😫 📝 🖬			
 Security Settings Account Policies Local Policies Local Policy Audit Policy Security Options Windows Firewall with Advanced Security Options Public Key Policies Public Key Policies Software Restriction Policies Software Restriction Policies Mplication Control Policies P Security Policies on Local Compute Advanced Audit Policy Configuration 	Policy • Image: Create permanent shared objects Image: Create symbolic links Image: Create symbolic links Image: Create symbolic links Image: Debug programs Image: Debug programs Image: Deny log on as a batch job Image: Deny log on as a batch job Image: Deny log on as a batch job Image: Deny log on locally Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Deny log on through Remote Desktop Services Image: Desktop Service Image: Desktop Service Image: Desktop Service	Security Setting Administrators Administrators LOCAL SERVICE,NETWO LOCAL SERVICE,NETWO LOCAL SERVICE,NETWO Users,Window Manager Administrators Administrators Administrators Administrators Administrators Administrators	
< III >	iiiiiii Pertorm volume maintenance tasks iiiiii Profile single process	Administrators Administrators	~

Log on as a service Properties	?	x
Local Security Setting Explain Log on as a service		
IIS APPPOOL\.NET v4.5 IIS APPPOOL\.NET v4.5 Classic IIS APPPOOL\Classic .NET AppPool NETWORK SERVICE NT SERVICEVALSERVICES NT SERVICEVMSSQL\$LYNCLOCAL NT SERVICEVMSSQL\$RTC NT SERVICEVSQLQsRTCLOCAL NT SERVICE\SQLAgent\$LYNCLOCAL NT SERVICE\SQLAgent\$RTC NT SERVICE\SQLAgent\$RTC NT SERVICE\SQLAgent\$RTCLOCAL SQLServer2005SOLBrowserUser\$FE		
Add <u>U</u> ser or Group <u>R</u> emove		
OK Cancel	Ar	ply

Figure 8-18: Log on as a service Properties

- Assign the SmartTAP 360° user account with at least RemoteSigned execution policy. RemoteSigned execution policy is required for executing PowerShell scripts during the Plugin's installation and run time.
 - a. Run PowerShell as the "SmartTapUser" that you defined on the Domain Controller using one of the following methods:
 - Command line:

Enter the following command and press enter:

Runas /user:[domain]\SmartTapUser powershell.exe



Figure 8-19: SmartTAP 360° User

Enter the SmartTAP 360° User password that you defined for the user defined on the Domain Controller and press enter.

If the SmartTAP 360° username contains spaces, ensure that you insert quotation marks at the beginning and end of the user name string in the command line e.g. "SmartTAP 360° User".

Using PowerShell:

-On the Domain Controller in the Start menu, right-click the Windows PowerShell icon and choose Run as different user:



-Enter the credentials for the "SmartTapUser" that you defined on the Domain Controller:

Figure 8-21: Windows Security	
Windows Security	x
Run as different user Please enter credentials to use for C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.	
Password Domain: S4B	
Connect a smart card	
OK Cancel	

-Open the Windows PowerShell and set the following Execution Policy for this user:

Set-ExecutionPolicy -Scope CurrentUser RemoteSigned

Figure 8-22: Windows PowerShell



A Domain Admin account may be required to perform Plug-in installation; however, the created "SmartTAPUSer" account is recommended to be used to run the Plug-in service.

Skype for Business Plugin Installation Procedure

This section describes the procedure for installing the Skype for Business plugin.

- > To install the plugin:
- 1. Copy the Skype for Business installation application SmartTAP 360° <Plugin_type> Plugin Setup to the FE, SBS or SBA desktop.
- Where <Plugin_type> is one of the following:
 - Lync2010
 - Lync2013
 - Skype for Business



AudioCodes recommends enabling the "Computer Browser" service prior to running the installer. Once the installation is complete, the "Computer Browser" service can be disabled.

1. Right-click on the file and select Run as Administrator.

1

Т

Documents library	Arrang	ge by: Folder 🔻
Name *	Date modified	Туре
readme	3/22/2012 2:59 PM	TXT File
SmartTap Lync Plug-in Setup	Open Run as administrator Troubleshoot compatibility Share with Restore previous versions Send to Cut Copy Create shortcut Delete Rename Open file location Properties	Application

Figure 8-23: Documents Library

- 2. If you see the warning, "Computer Browser" service is not running as shown below it is highly recommended to cancel the install. Enable the Computer Browser Service then restart the install. You can disable the "Computer Browser" service once install is complete.
- **3.** If you are performing an upgrade and have changed the default values for the following parameters, an informative message is displayed.
 - RecordExternalCallsOnly If exists and value is true then we prompt
 - recordPSTNCallsOnly If exists and value is true then we prompt
 - EnableAnnouncements If exists and value is true then we prompt





😸 AudioCodes Inc. Lync Plug-in Server - InstallShield Wiza 💻 🗖 🗙		
Welcome to the InstallShield Wizard for AudioCodes Inc. Lync Plug-in Server AudioCodes Inc. Lync Plug-in Server Setup is preparing the InstallShield Wizard which will guide you through the program cotup pressors. Plazes upit		
AudioCodes Inc. Lync Plug-in Server - InstallShield Wizard		
The "Computer Browser" service is not running. You may not be able to complete the install successfully.		
ОК		
< Back Next > Cancel		

- 4. Click Next to continue.
- 5. Click the I accept the terms in the license agreement radio button, and then click **Next**.

Figure 8-25: Software License Agreement

AudioCodes Inc. Lync Plug-in Server - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	
SOFTWARE LICENSE AGREEMENT]
LICENSE AGREEMENT AUDIOCODES USA, INC. (AudioCodes) provides the following License Agreement (the Agreement) to the original purchaser only: 1. PLEASE READ THIS LICENSE AGREEMENT. The enclosed AudioCodes software/firmware program (collectively, "SOFTWARE") is licensed by AudioCodes for use only on the terms and conditions set forth herein. By opening	
I accept the terms in the license agreement Print I do not accept the terms in the license agreement	
<pre>A Sack Next > Cancel</pre>	

- 6. Enter the user account that the service will use to log:
 - This user must be the "SmartTAPUser" account created previously on the domain.
 - The user account must be in the form DOMAIN\Username.
 - Optionally click the Browse... button to locate the user in the Active Directory.

Figure 8-26: Browse for a User Account

Browse for a User Account	x
Use the browse buttons to select a domain\server and a user na	ame.
Domain or server:	
	Browse
User name:	
	Browse
<u>O</u> K	<u>C</u> ancel

7. Click **Next** to continue.

Figure 8-27: Logon Information
Here and the AudioCodes Inc. Lync Plug-in Server - InstallShield Wizard
Logon Information Specify a user name and password
Specify the user name and password of the user account that the service will logon as. The user account must be in the form DOMAIN\Username.
User name: LCENT4\Administrator Browse
Password:
InstallShield

8. Select the host or pool that the Plug-in will use to register, and then click Next.

Figure 8-28: Lync Plug-in Registrar Select

閿	AudioCodes Inc. Lync Plug-in Server	x
Lync Plug	-in Registrar Select	さ
Your according the servi	ount information has been validated, please select the host or pool that ce will register with.	
 Registra	uppelt logal	~
Registra	:pool1.icent4.iocal	
InstallShield	< Back Next >	Cancel

9. Click Next.

10. Enter IP addresses of Media Proxy servers in case the Media Proxy recording method is utilized for the SmartTAP 360° installation, otherwise leave the fields empty.

Figure 8-29:	Media Proxy Server Configuration	

岁 AudioCodes In	nc. Lync Plug-in Server
Media Proxy Server Configuration If you plan or have Media Proxy servers, enter their details here. Otherwise dick Next.	
Add all Media Proxy Server IP addresses to	list IP Addresses:
Media Proxy Server IP address	
InstallShield	Back Next Cancel

- 11. Click Next.
- **12.** Enter IP addresses of Announcement servers in case SmartTAP 360° Announcement servers are installed, otherwise leave the fields empty.

岁 AudioCo	des Inc. l	Lync Plug-in Server	X
Announcement Server Configuration If you plan or have Announcement servers, enter their details here. Otherwise dick Next.			と
Add all Announcement Server IP ac	dresses to l	IP Addresses:	
Announcement Server IP address	>>		
InstallShield		Back Next	Cancel

Figure 8-30: Announcement Server Configuration

13. Click **Next**. Click the Complete installation to install the plugin in the default path on C: drive, otherwise click Custom to change the install path.

🖞 Audio	Codes Inc. Lync Plug-in Server - InstallShield Wizard		
Setup Type Choose the se	Setup Type Choose the setup type that best suits your needs.		
Please select a	a setup type.		
• <u>Complete</u>	All program features will be installed. (Requires the most disk space.)		
O Cu <u>s</u> tom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.		
InstallShield ———	< <u>B</u> ack <u>N</u> ext > Cancel		

Figure 8-31: Setup Type

- 14. Click Next.
- **15.** Click **Install** to install the plugin.
- **16.** Click **Finish** to complete installation.

If the plugin installation fails, refer to the Skype for Business plugin section in the Troubleshooting chapter.

Installing Call Delivery for Skype for Business (IP-based Recording)

It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. See Firewall Configuration on page 51.

> To install IP-based recording (Skype for Business):

1. Click Next to continue.



Figure 8-32: Call Delivery-IP

Assuming you are setting up for a Skype for Business installation, select "Microsoft Lync" when prompted for the network type.

2. Click Next on the Server IP Setup.

Figure 8-33: Network Type

👸 AudioC	Codes Inc. Call Delivery-IP
Select Network Type	4.
Choose the type of phone netwo	rk to be recorded
Network Type:	
Microsoft Lync	✓
InstallShield	
<u>ווכות</u>	< Back Next > Cancel

- Add each of your Skype for Business Front End IP addresses to the "Lync Front End IP Address" field, and click on the right arrow, to add it to the Front Ends list on the right.
- 4. Under "Public Call Delivery IP Address", type in the IP address of the computer you are currently installing the Call Delivery component on.
- 5. Click **Next** on the Server IP Setup.

퓛	Audio	Codes Inc	. Call Delive	erv-IP	X
Lync Confi Microsoft	Lync Configuration Microsoft Lync-specific configuration parameters			と	
Create a	list of all the Lync Front	End IP Addre	esses.		
Lync Fron	it End IP Address	>>	Front Ends:		
Public Cal	l Delivery IP Address				
InstallShield —			< Back	Next >	Cancel

Figure 8-34: Lync Configuration

- 6. To capture the audio:
 - See Section Monitoring below:
 - Local Port Mirroring
 - Remote Conference or Mediation Server
 - See Section Edge on page 94
 - See Section Configuring Media Proxy for Call Delivery-IP on page 96.
- 7. Click Next to select the Recording Type.

Monitoring

This section describes how to configure the location for capturing monitored recording:

- **Local** is typically used with Port Mirroring in a Skype for Business environment.
- Remote is typically used when Media Delivery is installed on Mediation or AV Conferencing server to capture SRTP.

> To capture monitored recordings locally:

1. From the Recording Type drop-down list, select **Monitoring**.

Figure 8-35: Choose Recording Mode

閿	AudioCodes Inc. Call Delivery-IP
Ch	oose Recording Mode
R N T (0 1 2 3	Anitoring Type Anitoring Mode: he monitoring method is used to record in any one of the following environments: Necessary software will be installed on Lync Server for methods 1 & 2) . Mediation Server (To record PSTN calls) 2. AV Conferencing Server (To record Conference calls) 3. Port Mirroring
Install	Shield < Back Next > Cancel

2. From the Media Tap Location drop-down list, select Local.

H AudioCode	es Inc. Call Delivery-IP
Choose Media Tap Location	と
Media Tap Location Local Y	
InstallShield	< Back Next > Cancel

Figure 8-36: Choose Media Tap Location

3. Select the appropriate interfaces from the dropdown menu in the Interface Setup screen.

Figure 8-37: Interface Setup

AudioCodes Inc. Call Delivery-IP	x
Interface Setup Configure Monitoring Ports and RTP Timeout	と
Monitoring Port 0 Disabled	~
Monitoring Port 1 Disabled	~
✓ Enable RTP Timeout RTP Timeout Value 120	
InstallShield Car	icel

In case of distributed or remote branch deployment, enter the IP address of the Application Server (AS), Communication Server (CS), and IP address of the Host Machine.

In case of all-in-one deployment, use the drop down list and choose the SmartTAP 360° IP address.

₿	AudioCodes Inc. Call Delivery-IP	x
Server IP Se Configure the	etup ne names or IP addresses of the servers	3
Communcation :	Server IP Address:	
172.26.144.23	3	~
Application Serv 172.26.144.23	ver IP Address: 13 Host Machine:	~
172.26.144.23	3	~
InstallShield	< Back Next > Cance	el

Figure 8-38: Server IP Setup

- 4. Click **Next** on the Server IP Setup.
- 5. Click Next on the Setup Type screen.
- 6. Click Install on the install screen.
- 7. Click **Finish** to finish.

> To capture monitored recordings remotely:

1. From the Media Tap Location drop-down list, select **Remote**.

岁 Aud	lioCodes Inc. Call Delivery-IP
Choose Media Tap Location	ん
Media Tap Location Remote	✓
InstallShield	< Back Next > Cancel

Figure 8-39: Choose Media Tap Location

- Specify the IP Address of the Media Delivery Host machine and click >> to add it to the IP Address list.
- 3. Repeat for each Host machine where Media Delivery is installed.

Figure 8-40: Media Delivery Configuration

🖞 AudioCo	Codes Inc. Call Delivery-IP	x
Media Delivery Configuration		ع
Create a list of Media Delivery IP add	ldresses	
	IP Addresses:	_
Media Delivery IP Address	>>	
InstallShield		
	< Back Next > Cancel	

In case of distributed or remote branch deployment, type in the real IP address of the Application Server (AS), Communication Server (CS), and IP address of the Host Machine (don't type in 127.0.0.1). In case of all-in-one deployment use the AS, CS, and the Host machine parameters drop down list and choose the SmartTAP 360° IP address.

H AudioCode	es Inc. Call Delivery-IP
Server IP Setup Configure the names or IP addresses o	of the servers
Communcation Server IP Address:	
172.26.144.23	×
Application Server IP Address: 172.26.144.23 IP Address of Host Machine:	<u> </u>
172.26.144.23	×
InstallShield	< Back Next > Cancel

Figure 8-41: Server IP Setup

- 4. Click **Next** on the Server IP Setup.
- 5. Click Next on the Setup Type screen.
- 6. Click Install on the install screen.
- 7. Click Finish.

Edge

The Media Delivery component is installed on each Edge server in the Pool. Use the Edge solution to record any call scenario in a Microsoft environment.

> To install the Edge server:

Figure 8-42: Choose Recording Mode

H AudioCodes Inc. Call Delivery-IP	x
Choose Recording Mode	4)
Recording Type Edge Notes on Monitoring Mode: The monitoring method is used to record in any one of the following environments: (Necessary software will be installed on Lync Server for methods 1 & 2) 1. Mediation Server (To record PSTN calls) 2. AV Conferencing Server (To record Conference calls) 3. Port Mirroring	
InstallShield < Back Next > Can	cel

1. Click Next to select Record Type "Edge".

Figure 8-43: Lync Edge Servers Configuration

븅 Aud	lioCodes Inc. Call Delivery-IP	x
Lync Edge Servers Configur Microsoft Lync-specific config	ration uration parameters	と
Create a list of the Edge internal	and external IP addresses	
Internal IPv4 IP address	Internal, External, NAT-enabled:	
A/V Edge service External IPv4 IP address	>>	
A/V Edge service NAT - enabled public IPv4 IP address		
InstallShield	(Bad No. 1	Creat
	<back next=""></back>	Cancel

- 2. Specify the Internal, External & NAT IP then click the >> to add to list.
- 3. Repeat for each Edge server in the pool.

In case of distributed or remote branch deployment, type in the real IP address of the Application Server (AS), Communication Server (CS), and IP address of the Host Machine

(don't type in 127.0.0.1). In case of all-in-one deployment use the AS, CS, and the Host machine parameters drop down list to choose the SmartTAP 360° IP address.

Figure 8-44: Server IP Setup

뻻	AudioCodes Inc. Call Delivery-IP
Serve Con	er IP Setup Infigure the names or IP addresses of the servers
Commu	Incation Server IP Address:
172.2	6.144.23
Applica	tion Server IP Address:
172.2	×6.144.23
IP Addr	ress of Host Machine:
172.20	6.144.23
InstallShie	d

- 4. Click **Next** on the Server IP Setup.
- 5. Click **Next** on the Setup Type screen
- 6. Click Install on the install screen
- 7. Click Finish.

Firewall Exceptions

Firewall exceptions are REQUIRED for this solution to work. Please refer to Chapter Firewall Configuration on page 51 Firewall Configuration on page 51 for the required exceptions.

Configuring Media Proxy for Call Delivery-IP

The SmartTAP 360° Media Proxy is a stand-alone server designed to relay the SRTP "Voice" to the final destination providing SmartTAP 360° with a centralized point to capture the audio. The SmartTAP 360° Skype for Business plugin on the FE / SBA will pin the media through the proxy so SmartTAP 360° has a central point to capture the SRTP for Internal, PSTN, and Conference calls.

> To configure Media Proxy for Call Delivery-IP:

1. Select the Media Proxy recording type.

闄	AudioCodes Inc. Call Delivery-IP
c	hoose Recording Mode
	Recording Type Media Proxy Notes on Monitoring Mode: The monitoring method is used to record in any one of the following environments: (Necessary software will be installed on Lync Server for methods 1 & 2) 1. Mediation Server (To record PSTN calls) 2. AV Conferencing Server (To record Conference calls) 3. Port Mirroring
Insta	allShield

Figure 8-45: Choose Recording Mode – Media Proxy

- 2. Specify the IP Address of the Media Proxy server.
- 3. Specify the Media proxy port to use (default 10123).

Figure 8-46: Media Proxy Configuration

Here and the second sec
Media Proxy Configuration
Add all Media Proxy IP addresses to list
IP Addresses:
Media Proxy IP address >> <<
InstallShield

You can combine the Media proxy model that records Internal, PSTN and Conference calls with the Edge recording model, which will record (Remote, Federated and Mobile calls). If you intend to use the Edge model in conjunction with the Media proxy, provide the Edge details in the following screen and install the Media Delivery software on the Edge server:

- 1. Provide the Internal & External Edge IP.
- 2. Add the NAT IP if configured.



👸 Audio	Codes Inc. Call Delivery-IP	
Lync Edge Servers Configurati Microsoft Lync-specific configurat	tion parameters	
Create a list of the Edge internal and external IP addresses		
Internal IPv4 IP address	Internal, External, NAT-enabled:	
I		
A/V Edge service External IPv4 IP address	>>	
	<<	
A/V Edge service NAT - enabled public IPv4 IP address		
InstallShield		
	< Back Next > Cancel	

- Specify the real IP addresses of the SmartTAP 360° Communication Server and Application Server.
- 4. Select the NIC interface of the local server.

AudioCodes Inc. Call Delivery-IP
Server IP Setup Configure the names or IP addresses of the servers
Communcation Server IP Address:
172.26.144.23
Application Server IP Address:
IP Address of Host Machine:
172.26.144.23 🗸
InstallShield

Figure 8-48: Server IP Setup

- 5. Select Complete setup type, and then click **Next** to continue.
- 6. Click Install to complete installation.

Configuring Call Delivery for Skype for Business

The Voip.cfg file located in the target path of the Call Delivery, will automatically be configured during the SmartTAP 360° software installation. Remember to restart the service if any changes are made manually to the voip.cfg file.

Default Path:\AUDIOCODES\SmartTAP 360°\CD-IP\Config\Voip.cfg

Do not make changes to the Voip.cfg unless the IP address assigned to the FE/SBA or the SmartTAP 360° server has changed.

Field	Default	Description
MICROSOFT=[]	N/A	The MICROSOFT field defines the CD configuration specific to Skype for Business recording. The # must be removed from every line starting with MICROSOFT line and the matching] at the end of the definition
SWSERVERPORT	TCP, 9090	

Figure 8-49: Description of the Skype for Business Specific Changes
Field	Default	Description
СС	ON	
PLUGINLIST	blank	Add list of Front End Server IP Addresses in the pool separated by "," connecting to this Call Delivery service. Each server in pool should be listed.
SWSERVER	blank	Set to SmartTAP 360° server IP where Call Delivery resides
RECORDINGTYPE	0	0 = Mediation, Conference server or Port Monitoring 3 = Use with Edge 4 = Use the Media Proxy and Edge (Optional)
MEDIAPROXYURL	blank	IP Address:Port of Media Proxy server (Port default 10123)

Voip.cfg changes in bold below:

```
MICROSOFT =
[
SWSERVERPORT=TCP,9090
CC=ON
PLUGINLIST=Front End / SBA IP:9901
SWSERVER=SmartTAP 360° Server IP
RECORDINGTYPE=# #0 - monitoring(default), 3 - EdgeProxy (used on the
Edge server), 4 - MediaProxy
MEDIAPROXYURL=http://IP:10123 # required if RECORDINGTYPE=4
(MediaProxy)
```

Installing Media Proxy Server for Skype for Business

The Media Proxy (MP) is used specifically in Microsoft Skype for Business environment as a voice media proxy. The SmartTAP 360° Skype for Business plugin on the FE will redirect the targeted SRTP "voice" only to the Media Proxy, which then sends the voice on to the original destination. A copy of the SRTP "voice" call that traverses the MP is sent to the SmartTAP 360° server for long-term storage.

- It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.
 - Before proceeding, ensure that you have noted the installation requirements (see Before Installing Microsoft Skype for Business Components on page 65

> To install the Media Proxy:

1. When the Media Proxy installation wizard starts, click **Next** to install.



Figure 8-50: Media Proxy Welcome

If you are installing from a Suite, the following screen may not be displayed.

Figure 8-51: License Agreement

AudioCodes Inc. Media Proxy	×
License Agreement Please read the following license agreement carefully.	5
SOFTWARE LICENSE AGREEMENT LICENSE AGREEMENT AUDIOCODES USA, INC. (AudioCodes) provides the following License Agreement (the Agreement) to the original purchaser only: 1. PLEASE READ THIS LICENSE AGREEMENT. The enclosed AudioCodes software/firmware program (collectively, "SOFTWARE") is licensed by AudioCodes for use only on the terms and conditions set forth herein. By opening	*
I accept the terms in the license agreement Print I do not accept the terms in the license agreement InstallShield	
< Back Next > Cancel	

2. Select the "I accept the terms in the license agreement" radio button and click Next.

Audio	Codes Inc. Media Proxy	×
Choose Media-Proxy IP Address Please Choose the IP address asso Media-Proxy communications.	s ociated with the network interface used for	と
Media-Proxy local IP address:	192.168.1.5	
InstallShield	< Back Next >	Cancel

Figure 8-52: Choose Media Proxy IP Address

3. Enter the external Media-Proxy local IP address i.e. do not enter the IP address of the local host, and click Next.

AudioCodes Inc. Media Proxy	×
Choose Application Server IP Address	4
Please Choose the IP address associated with the network interface used fo Application Server communications.	
Add all Application Server IP addresses to list	
Application Server IP address:	
● HTTP <<	
Онттря	
InstallShield	
< Back Next >	Cancel

Figure 8-53: Choose Application Server IP Address

4. Configure the external Application Server IP address . Click >> to add the IP address to the list of Application Servers. Use the << button to remove an entry from the list. Click the entry that you wish to remove. At least one entry should be configured. Click Next to proceed.</p>

An example configuration is shown in the figure below:

ø		AudioC	odes Inc.	Media P	roxy	×
(Choose Applicat Please Choose th Application Serve	ion Server IP Ad ne IP address asso er communications.	Idress ciated with t	ne network	interface used fo	r Z
	Add all Application	Server IP address	es to list			
	Application Server	IP address:		http://192 https://19	2.168.1.5:80 92.168.1.5:443	
	10.0.0.8	¥	>>	http://10. https://10	.0.0.8:80).0.0.8:443	
	● HTTP		<<			
Insta	llShield					
IIISto			< B	ack	Next >	Cancel

Figure 8-54: Choose Application Server IP Address

5. When you have completed the configuration, click Next to proceed.

If you are performing an upgrade, the following screen may not be displayed.

17		AudioCodes Inc. Media Proxy	×
Setup Choo	Type ose the set	tup type that best suits your needs.	と
Plea	se select a	setup type.	
	omplete	All program features will be installed. (Requires the most disk space.)	
⊖¢	ustom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.	
InstallShie	eld	< Back Next > Ca	incel

Figure 8-55: Media Proxy Setup Type

- 6. Choose one of the following setup types and click Next:
 - Complete: Install to the default location: C:\Program Files\AudioCodes\SmartTAP 360°\MP
 - Custom: Change the destination location.

AudioCodes Inc. Media Proxy
Ready to Install the Program The wizard is ready to begin installation.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield

Figure 8-56: Media Proxy Install

7. Click Install.

Editing Media Proxy Server Parameters

This section describes how to edit MP parameters after installation has been performed.

To edit MP parameters:

- 1. Edit the System.config file at Program Files\AudioCodes\SmartTAP 360°\MP\Config\.
- 2. If there is more than one interface in this machine, the Media Proxy server will use this interface.

<System key: locallpInterfaceAddress ="<local IP address>"



Where ="<local IP address> refers to the IP address of the IP interface when the installed machine has multiple IP interfaces.

3. Add option asList ="< Application Server Web Address>" to specify the list of Application servers for the Media Server.

```
<System
key: asList =" "http://172.26.144.23:80, "http://172.26.144.24:80"/>
<System
key: asList =" "https://172.26.144.23:443, "https://172.26.144.24:443"/>
```

Where < list of Application Server IP Web addresses>contains a comma separated list of the Application servers for the Media Proxy server in the SmartTAP 360° Active/Active Configuration.

4. (Optional) Modify the following Beep tone parameters (see table below for details):

<System beepEnabled="true" beepDurationMs="1000" voiceGain="1" beepGaindBm="15"intervalDurationSeconds="15"/>



Beep tones can also be enabled to play in the Recording Profile in SmartTAP 360° Web interface.

Parameter	Description	Default
beepEnabled	Set true to play beep during calls. Default : true	beepEnabled
beepDurationMs	Beep duration in milliseconds, valid range [1- 30000].	1000
voiceGain	0 – voice is removed, 1 – voice is added to tone as is, valid range [0-1].	1
beepGaindBm	Beep gain in -dBm units. range [3-31] (-3dBm to -31dBm), 3-Loudest, 31-Quietest	15
intervalDurationSeconds	Interval between each beep.	15

Table 8-1: Beep Tone Parameters

5. Restart Media Proxy Service.

Installing Media Delivery Server for Skype for Business

The Media Delivery is used specifically in Microsoft Skype for Business environment. The SmartTAP 360° CD-IP will instruct the MD running on the Skype for Business Mediation, Conference or Edge server to capture a copy of the SRTP "voice" call that is traversing the Skype for Business server and send the copied SRTP "voice" to the SmartTAP 360° server for long-term storage.

- The Media Delivery is only required for deployments that involve Microsoft Skype for Business when utilizing the Edge, Mediation or Conference server to capture the SRTP.
 - It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51.

> To Install Media Delivery (Skype for Business only):

- **1.** Run the Install.bat from the SmartTAP 360° "Suite\" folder.
- 2. Select the Distributed software Custom Setup type.
- 3. Click AudioCodes Inc. Media Delivery Server.
- 4. Click Install to continue.
- 5. Select Recording Type Monitoring or Edge.
- 6. Select Monitoring when utilizing the Mediation or Conference server.
 - Specify the physical NIC interfaces to monitor. In a NIC teaming environment do not select the virtual NIC.
- 7. Select Edge when utilizing the Edge server.
 - Specify the Edge Internal & External NIC interface to monitor. Select the physical NIC interfaces.
- 8. Select Complete, click **Next** to continue.
- 9. Click Install.
- 10. Click Finish to complete installation.

Installing Announcement Server

The Announcement Server (AN) is used specifically in the Microsoft Skype for Business environment as a call recording announcement service to let PSTN callers know their call will be recorded.

The SmartTAP 360° Skype for Business plugin on the FE will redirect the inbound PSTN calls to the targeted to be recorded users to the AN to play the announcement. Once the announcement is played, the call will be redirected to the original destination.

If you need to setup a group of Announcement Servers for redundancy or scalability, make sure to execute the following steps on each Announcement Server.

Do the following:

- 1. Announcement Server Preparation: Install Core Components & Local Replica Configuration Store
- 2. Announcement Server Software Installation Procedure on page 114

3. Annoucement Server-Post Installation Procedures on page 119

Before proceeding, ensure that you have noted the installation requirements (see Before Installing Microsoft Skype for Business Components on page 65.

Announcement Server Preinstall of Core Components and Local Replica Configuration Store

This section describes ther installation of the Core components & Local Replica Configuration store using the Deployment wizard as a prerequisite for installation of the Annoucement Server.

> To install the Deployment wizard:

1. Start the Skype for Business Server 2015 Deployment Wizard.

	Figure 8-57:	Skype for	⁻ Business	Server	2015 -	Deploy
--	--------------	-----------	-----------------------	--------	--------	--------

ត	Skype for Business Server 2015 - Deploy	ment Wizard	x
Welco	me to Skype for Business Server 2015 deployment		
Deploy			2
	Prepare Active Directory Prepares the Active Directory schema, forest, and domain for Skype for Business Server. Help >	Prepare first Standard Edition server Prepares a single Standard Edition server to host Central Management Service. Note: This task requires local administrator rights. This task does not apply to Standard	^
	Install or Update Skype for Business Server System Install or update a Skype for Business Server Server deployment member system. This option installs Skype for Business Server core components, and a local replica configuration store. Note: Before installing a server, you need to have a valid topology created and published. Help ►	Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition. Install Administrative Tools Installs the Administrative Tools to the current system. Your deployment requires at least one installation of the Topology Builder. Deploy Monitoring Reports	н
		Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances. Call Quality Dashboard Skype for Business Server 2015, Call Quality Dashboard is a portal that provides OLAP	
		reports to Skype for Business Server administrators to help troubleshoot Call Quality issues.	
		Click to view getting started videos. Back Exit	~

2. Select Install Administrative Tools and click Next.

5	Install Administrative Tools	x
S	Install Administrative Tools	
Installs t	he Administrative Tools to the current system. Your deployment requires at least one installation opology Builder.	١
Help	<u>B</u> ack <u>N</u> ext Cancel	

Figure 8-58: Install Administrative Tools

When completed, the following is displayed:

Figure 8-59: Install Status

Install Administrative Tools Installs the Administrative Tools to the current system. Your deployment requires at least one installation of the Topology Builder.

3. Click Next to continue.

Figure 8-60: Install Local Configuration Store

5	Skype for Business Server 2015 - Deployment Wizard	x
Install or up	pdate member system	
<u>Deploy</u> > Insta	ll or update	2
Step 1: <u>I</u> nst Inst Prer Help	tall Local Configuration Store alls local configuration store and populates with data from Central Management Store. requisites > p >	
Step 2: S <u>e</u> tu Insta defi Not	up or Remove Skype for Business Server Components all and activate, or deactivate and uninstall Skype for Business Server Components based on the topology inition.	=
Prer	requisites >	
Help	P > Run	
Step 3: Req This this Not	uest, Install or Assign Certificates s step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for system based on the topology definition. : Available: Local configuration store not available.	
Prer	requisites Run	
Step 4: Star Manual Afte You To s	rt Services er you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. I can start the services in a pool with the Skype for Business Server cmdlets. start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All Back	

4. Choose option Step 1: Install Local Configuration Store and click Run.

Installs core components & local replica configuration store.

Figure 8-61: Configure Local Replica of Central Management Store Store

5	Install Local Configuration Store	x
S	Configure Local Replica of Central Management Store	
Data can	be retrieved directly from the Central Management store or imported from a file.	
<u>R</u> etri <u>Mana</u>	eve directly from the Central Management store (requires read access to the Central agement store)	
◯ <u>I</u> mpo	rt from a file (recommended for Edge Servers)	
To g acce	enerate a configuration file, run the Export-CsConfiguration cmdlet on a computer that has ss to the Central Management store.	
	Browse	
Help	<u>B</u> ack <u>N</u> ext Cancel	

5. Click Next to continue.

Once completed, a screen similar to the following is displayed:

Figure 8-62: Executing Commands	
Install Local Configuration Store	x
Executing Commands	
Enable replica service for the Skype for Business Server computer. Creating new log file "C:\Users\admin.SPAIN\AppData\Local\Temp\Enable-CSReplica-[2016_09_05] [16_46_33].html". "Enable-CSReplica" processing has completed successfully. Detailed results can be found at "C:\Users\admin.SPAIN\AppData\Local\Temp\Enable-CSReplica- [2016_09_05][16_46_33].html". > Replicate-CsCmsCertificates Logging status to: C:\Users\admin.SPAIN\AppData\Local\Temp\ReplicateCMSCertificates- [2016_09_05][16_46_33].html	~
Task status: Completed.	
Bootstrap local machine	og
	_1

6. Click Finish.

Announcement Server Software Installation Procedure

This section describes the installation of the Annoucement server using the wizard.

> To install the announcement server using the wizard:

1. Launch the Installation wizard.



Figure 8-63: Announcement Server Installation Wizard

The following screen may appear if the .NET Framework 4.7 is not installed.

2. Click Install to continue.

AudioCode	es SmartTAP Announcement Server - InstallShield Wizard
ځ	AudioCodes SmartTAP Announcement Server requires the following items to be installed on your computer. Click Install to begin installing these requirements.
Status	Requirement
Pending	Microsoft .NET Framework 4.7 Full
	Install Cancel

3. Click Next.

If you are installing from a Suite, then the following screen may not be displayed.

Figure 8-64: License Agreement

😸 AudioCodes Inc. SmartTAP Announcement Server - Installation Wi
License Agreement Please read the following license agreement carefully.
SOFTWARE LICENSE AGREEMENT ^ LICENSE AGREEMENT AUDIOCODES USA, INC. (AudioCodes) provides the following License Agreement (the Agreement) to the original purchaser only: 1. PLEASE READ THIS LICENSE AGREEMENT. The enclosed AudioCodes software/firmware program (collectively, "SOFTWARE") is licensed by AudioCodes for use only on the terms and conditions set forth herein. By opening * I accept the terms in the license agreement
I do not accept the terms in the license agreement InstallShield

4. Click **Next** to agree to the license.



虔	AudioCodes SmartTAP Announcement Server	x
Plea Ch	ase choose Annoucement Server version to install hoose the Annoucement Server version appropriate to your environment	•
	 Announcement Server for Lync 2013 Announcement Server for Skype for Business 2015 Announcement Server for Skype for Business 2019 	
InstallS	5hield	

- 5. Select the type of Announcement server and click Next:
 - Announcement Server for Lync 2013

- Annoucement Server for Skype for Business 2015
- Annoucement Server for Skype for Business 2019

Figure 8-66:	Choose	Application	Server	IP	Address
i iguie 0-00.	Choose	Application	Jeivei	IF.	Audicss

岁 Au	dioCodes Inc. SmartTAP Announcement Server
Choose Appli Please Choos Application S	cation Server IP Address se the IP address associated with the network interface used for erver communications.
Add all Applicatio	n Server IP addresses to list
Application Serv	er IP address:
• HTTP	<<
InstallShield	< Back Next > Cancel

6. Configure external Application Server IP address and select either the HTTP or HTTPS protocol. Click >> to add the IP address to the list of Application Servers. Use the << button to remove an entry from the list. Click the entry that you wish to move. At least one entry should be configured. An example configuration is shown in the figure below.</p>

	0 -		
1	Audi	oCodes Inc. SmartTAP Announcement Server	×
	Choose Applica Please Choose Application Service	tion Server IP Address the IP address associated with the network interface used for ver communications.	と
	Add all Application	Server IP addresses to list	
	Application Server	IP address:	
		<<	
	HTTPS		
Insta	allShield	< Back Next >	Cancel

Figure 8-67: Application Server IP Address

Figure 8-68: Setup Type

😸 AudioCode	s Inc. SmartTAP Announcement Server - Installation Wi 🗴
Setup Type Choose the set	tup type that best suits your needs.
Please select a	setup type.
Complete	All program features will be installed. (Requires the most disk space.)
O Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield	< Back Next > Cancel

- 7. Choose the Setup Type and click **Next**:
 - Complete: Install to the default location: C:\Program Files\AudioCodes\SmartTAP 360°\ANN
 - Custom: Change the destination location.

If you are performing an upgrade, this screen may not be displayed.

Figure 8-69: Install Commences

Image: Comparison of the program

The wizard is ready to begin installation.

Click Install to begin the installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShied

Image: Comparison of your installation of the wizard.

- 8. Click Install to commence the installation process.

Do not install on the SmartTAP 360° server.

The Announcement Service will not start automatically. It needs to be started manually after configuring the Announcement Services (see below).

Annoucement Server-Post Installation Procedures

This section describes the following procedures required following the installation of the Annoucement server:

- Step 1-Activate Annoucement Services below
- Step 2-Add Annoucement Servers to DNS on the next page
- Step 3-Configuring Announcement Server (Skype for Business) on the next page

Step 1-Activate Annoucement Services

This section describes how to configure Announcement Services.

To activate announcement services:

1. Start the PowerShell console as an Administrator user with the following permissions:

- The user must be a member of RTCUniversalServerAdmins for creating the trustedapplication.
- In addition, for creating a certificate to use by AN service, the account must be a local administrator and have rights to the specified certification authority.

The CA is sometimes configured to not allow creating certificates online, and in that case, the activation will always fail regardless of the account. In this case it is required to create and assign a certificate using the Skype for Business deployment wizard and re-run the activation script. The activation script will detect an installed certificate and continue execution.

- 2. Change the working folder to the PowerShell folder in the Announcement Server installation folder: SmartTAP 360°\AN\PowerShell\.
- 3. Run the .\Activate.ps1 command.
- 4. Enter port 12171 when prompted.
- 5. Save the AnnouncementsApp application endpoint name. It should be logged in the PowerShell command line window as shown in red color below:
- 6. "...AnnoucementsApp application endpoint name sip:NAME@domain.com..."
- Save the NAME string and use it in the "Steps to add Announcement Servers to DNS" section.
- 8. Start AudioCodes Announcement Service.

Step 2-Add Annoucement Servers to DNS

- To Add Announcement Servers to DNS
- Add DNS 'A' record to the appropriate zone on the configured DNS server per Announcement server against the AnnouncementApp name that was saved in "Steps to activate Announcement Services" section (NAME, example: AnnouncementsApp-pool-2013-1, AnnouncementsApp-pool-2015-1).

Step 3-Configuring Announcement Server (Skype for Business)

This section describes how to setup the Annoucement server for recording annoucements and attaching audio files.

To configure the Announcement Server:

1. Copy all ANN files and IVR files that you wish to configure for Announcements to the following location:

Program Files\AudioCodes\SmartTAP 360°\AN\Config\StateMachineConfig

•	•		
Name	Date modified	Туре	Size
\mu Config	9/7/2016 3:04 PM	File folder	
🅌 Languages	9/7/2016 3:04 PM	File folder	
腸 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	

Figure 8-70: StateMachineConfig File Location



This action enables you to attach ANN and IVR files to the Recording Profile in the SmartTAP 360° Web interface.

All ANN files must be saved in the WMA format and all IVR files must be saved in JSON format. For more information, refer to the *SmartTAP 360° Administrators Guide*.

- Edit the System.config file from the following location: Program Files\AudioCodes\SmartTAP 360°\AN\Config\.
- **3.** Add option 'normalizeNumbers="true" when normalization of called numbers for the Announcement Server is required.

```
<System
normalizeNumbers ="true"
/>
```

4. Add option asList ="< Application Server Web address>" to specify the Web address of the Application server (AS) for the Announcement server.

```
<System
key: asList ="<Application Server IP address>"
/>
```

5. Restart AN Service.

Installing SmartTAP 360° Monitoring Service

SmartTAP 360° Monitoring Service(STMonitoringSvc) is designed to test SmartTAP 360° recording functionality using AudioCodes HealthMonitor (HM) and Microsoft UCMA. It will generate a test call between two trusted application endpoints and will update the results to the Health Monitor . The Health Monitor will then validate the recording metadata and the call media and send an alarm or emailto SmartTAP 360° if required. For more information on the Health Monitor, refer to the *SmartTAP 360° Administrator Guide*.



The CA is sometimes configured to not allow creating certificates online, and in

- this case, the activation will always fail regardless of the account and users are required to create and assign a certificate using the Skype for Business deployment wizard and re-run the activation script. The activation script will detect an installed certificate and continue execution.
- One additional Target and Recorder license is is required for the test endpoints.

Do the following:

- 1. Install the SmartTAP 360° Monitoring Service (SmartTAP 360° Monitoring Service Installation Procedure below
- 2. Activate the SmartTAP 360° Monitoring Service (Activating the SmartTAP 360° Monitoring Service on the next page
- Configure the SmartTAP 360° Monitoring Service (Configuring the SmartTAP 360° Monitoring Service on page 124)

SmartTAP 360° Monitoring Service Installation Procedure

This section describes the SmartTAP 360° Monitoring Service Installation procedure.

> To install the SmartTAP 360° Monitoring service:

- "SmartTAP 360° Monitoring Service" can be installed using SmartTAP 360° Installation Suite or dedicated installer inside Suite folder (Suite\Monitoring Service\SmartTapMonitoringService Setup.exe).
- 2. Choose Accept and continue with Next.

Figure 8-71: Monitoring Service Skype for Business Platform

Ch	pose the Monitoring service version appropriate to your environment	
	○ Monitoring Service for Lync 2013	
	○ Monitoring Service for Skype for Business 2015	
	○ Monitoring Service for Skype for Business 2019	

- 3. Select the Lync/Skype for Business platform that you wish to install.
- 4. Specify the machine's IP address where the Health Monitor is installed.

It is possible to choose from the drop-down menu or write manually.



If the Health monitor is configured to localhost, then enter the Health Monitor IP address..

- 5. Choose complete for installation on a default drive or custom to change it.
- 6. Click Next.

The installation folder is found at the following path: <rootDrive>:\Program Files\AUDIOCODES\Tools\SmartTapMonitoringService

Activating the SmartTAP 360° Monitoring Service

This section describes how to activate the SmartTAP 360° Monitoring Service.

To activate SmartTapMonitoringService service:

- 1. Start the PowerShell console as an Administrator user with the following permissions:
 - The user must be a member of RTCUniversalServerAdmins for creating the trustedapplication.
 - In addition, for creating a certificate to be used by SmartTapMonitoringService, the account must be a local administrator with rights to the specified certification authority.
- 2. Change the working folder to the PowerShell folder in the SmartTapMonitoringService installation folder.
- **3.** Run the .\Activate.ps1 command.
- 4. Enter custom port when prompted (ex. 10145).
- 5. Save the SmartTapMonitoringService application endpoint names caller and agent. It should be logged in the PowerShell command line window as below:

"...application endpoint name sip:SmartTapTestCallGeneratorAgent@domain..." "...application endpoint name sip:SmartTapTestCallGeneratorCaller@domain..."

6. Save the Trusted application name, ex.:

"Creating SmartTapTestCallGenerator trusted application on SmartTapTestCallGeneratorpool-2015-1"

7. Add DNS 'A' record of saved in previous step to the appropriate zone on the configured DNS server.

example: SmartTapTestCallGenerator-pool-2015-1.

8. Start the service.

Configuring the SmartTAP 360° Monitoring Service

This section describes how to configure the SmartTAP 360° Monitoring Service. The configuration file is found in <STMonitoringSvc root>\Config\System.config. The SmartTAP 360° Monitoring service retrieves its configuration from the HealthMonitor (REST), therefore the Health Monitor's IP address is required. If this IP address was not configured in installation, it can be configured as follows:

```
<System
healthMonitoringRestServerBaseUrl="http://localhost:10101/"
/>
```

All the configuration default values are remarked in the System.config, for example:

key: restClientKeepAliveInterval

Default Value: 30 Description: Time in seconds for Rest client to send keep alive message.

key: callerMediaFilePath

Default Value: "Music\callerMusic.wma" Description: caller media file path.

key: agentMediaFilePath

Default Value: "Music\agentMusic.wma" Description: agent media file path.

In addition, these parameters can be added to the 'System' section if they need to be overwritten:

<System

callerMediaFilePath ="Music\OtherCallerFile.wma"

agentMediaFilePath ="Music\OtherAgentFile.wma" restClientKeepAliveInterval="40" />

UcmaMonitoringConfig section Example

<UcmaMonitoringConfig>

<IsActivationMode>true</IsActivationMode>

<Endpoints/>

<ActionTimes>15:30,15:40</ActionTimes>

<KeepAliveTimeoutSec>60</KeepAliveTimeoutSec> -> NEW Field.

</UcmaMonitoringConfig>

In case the caller is created by the above script sip:SmartTapTestCallGeneratorCaller@anw365.lab , and the Agent is sip:SmartTapTestCallGeneratorAgent@anw365.lab ,

The test call scenario is a Basic call wherethe Caller calls the Agent and the Agent answers automatically. Both partiesplay 'callerMediaFilePath'\'agentMediaFilePath' media files accordingly, with default values of 'Music\callerMusic.wma' and 'Music\agentMusic.wma'.

STMonitoringSvc informs the Health Monitor when the call is has ended, and the Health Monitor validates that the call has been recorded.

In case the call was not recorded or recorded with silent media, the Health Monitor sends an alarm to the ApplicationServer and will notify by email to the list of recipients configured in <smtpProperties> section.

- The above users must be targeted users in the SmartTAP 360° system (one additional target and recorder license should be available for this purpose)).
- Also Call retention policy for one day is required in order not to overload the Database.

ActionTimes

ActionTimes configures the time of the day to generate the test call (generated daily).

<ActionTimes>15:30, 15:40, 15:50</ActionTimes>

KeepAliveTimeoutSec

A Keep Alive mechanism between the Health Monitor and STMonitoringSvc was added to theHealth Monitor. If you already have installed the Health Monitor, add the <Keep-AliveTimeoutSec> field under the <UcmaMonitoringConfig> section as is shown in the example below. This field is for the purpose of maintaining communication between the

STMonitoringSvc and the Health Monitor. The KeepAliveTimeoutSec configures the time in seconds that the Health Monitor receives a Keep-alive message from STMonitoringSvc. If this time is exceeded, the Health Monitor sends a Communication Down alarm.

<KeepAliveTimeoutSec>60</KeepAliveTimeoutSec>

9 Integration Configuration

SmartTAP 360° supports several telephony integration options. Go to the appropriate integration to configure Call Delivery for your environment:

- Microsoft Skype for Business See Section Microsoft Skype for Business Deployment on page 62
- SIPRec See SIP Recording (SIPRec) on page 142
- Voip Mirror Port (SIP, H.323, Avaya, Cisco, etc.) seeVoIP Port Mirroring below
- Analog Trunk, Station & Radio see Analog Trunk / Radio on page 134

VoIP Port Mirroring

The SmartTAP 360° software supports many different IP PBX station side-tapping configurations using a mirror port or network tap appliance to receive the unencrypted Signaling and RTP.

Inbound / Outbound

This is the easiest configuration as seen in the following image because you can mirror the traffic at the highest-level switch before the PBX. Tapping between the PBX and the phone is crucial to determining the call Initiator and Recipient.





Station to Station

To record station-to-station calls, it is important to understand that once the call is established between two endpoints that reside on the same switch, the RTP "Voice" will travel directly

between them. The recorder will miss the RTP, if you tap at the highest-level switch as in the diagram above. To avoid missing the RTP, mirror the traffic from the lower level switch with endpoints connected that need to be recorded.



Figure 9-2: Station to Station

Call Delivery Install for VoIP (Port Mirror)

This section describes how to install Call Delivery Install for VoIP (Port Mirror).

> To install Call Delivery Install for VoIP (Port Mirror)

1. Click Next to continue.



Figure 9-3: Call Delivery IP

Assuming you are NOT setting up for a Skype for Business installation, select "Other" when prompted for the network type.

2. Click Next on the Server IP Setup.

Figure 9-4: Select Network Type

闄	AudioCodes Inc. Call Delivery-IP
s	elect Network Type
	Choose the type of phone network to be recorded
	Network Type:
	Microsoft Lync 🗸
	Microsoft Lync
	Other
Insta	allShield
	< Back Next > Cancel

Assuming the Call Delivery Service is on the same machine as the Application and Communication service leave the default below settings.

3. Click Next on the Server IP Setup.

ligure 5-5. Server if Serup
AudioCodes Inc. Call Delivery-IP
Server IP Setup Configure the names or IP addresses of the servers
Communcation Server IP Address:
172.26.144.23
Application Server IP Address: 172.26.144.23 V IP Address of Host Machine:
172.26.144.23 🗸
InstallShield

Figure 9-5: Server IP Setup

SmartTAP 360° passive IP integration supports monitoring up to 8 NIC interfaces. In a typical server, there are a minimum of two NIC interfaces. NIC 1 is used to connect the SmartTAP 360° server to the LAN for user access. The 2nd NIC is connected to the mirror port on the switch to receive the signaling and RTP.

From the Monitoring Port 0 drop down list, select the appropriate NIC interface that is connected to the mirror port on the switch. Monitoring Port 1 is used in the event a 3rd NIC is required to connect to a different mirror port on a 2nd switch.

4. Select the appropriate Monitoring Port 0/1 interfaces from the dropdown menu in the Interface Setup screen

AudioCodes Inc. Call Delivery-IP
Interface Setup Configure Monitoring Ports and RTP Timeout
Monitoring Port 0 Disabled
Monitoring Port 1 Disabled
Image: Second Secon
InstallShield Cancel

Figure 9-6: Interface Setup

- 5. Click **Next** on the Setup Type screen.
- 6. Click Install on the install screen.
- 7. Click **Finish** to finish.

Additional Configuration for VoIP Port Mirroring

This section describes addition configuration for VoIP Port mirroring.

> To perform additional configuration:

- 1. Configure VoIP.cfg file to match IP PBX.
- 2. Configure mirror port on switch to mirror traffic to SmartTAP 360° server.
- 3. Configure SmartWORKS Control Panel.

The following files located in the target path of the Call Delivery are the most common files that are required for the IP environment:

Default Path:\AudioCodes\SmartTAP 360°\CD-IP\Config\Voip.cfg

Table 9-1:	Description	of the A	Avaya H.323	Specific	Changes
------------	-------------	----------	-------------	----------	---------

Field	Default	Description
Avaya_ H323=[]	N/A	Changes specific to Avaya H.323 recording. Uncomment section by removing hashes (#) at the beginning of each line

Field	Default	Description
H225CS	1720,TCP	H.323 Call Control port
H225RAS	1719,UDP	H.323 RAS port
SERVERIPS	N/A	IP address of Avaya PBX

VoIP.cfg changes for recording Avaya H.323 (unencrypted) are shown below:

#Avaya_H323 =
#[H225CS=1720,TCP
H225RAS=1719,UDP
SERVERIPS=
DCH=ON
DCH=ON
DCHFILTER=OFF
CC=ON
SUBTYPE=CM]

Table 9-2: Description of the SIP Recording Specific Changes

Field	Default	Description
SIP=[]	N/A	Changes specific to SIP recording. Uncomment section by removing hashes (#) at the beginning of each line.
SERVERIPS	N/A	IP address of PBX, or list of IP addresses of PBXs (separated by comma).
TRANSPORT	UDP,5060	SIP signaling.
ADD_ TRANSPORTS	(optional field)	Additional transports such as (TCP,5060) when SIP uses TCP for signaling in addition to UDP.

Voip.cfg changes for recording SIP (unencrypted) are shown below:

```
SIP =
[
SERVERIPS=192.168.70.6,10.250.0.5,192.168.70.5
TRANSPORT=UDP,5060
ADD_TRANSPORTS=TCP,5060
CC=ON]
]
```

Setting Up Monitoring Interfaces

This section describes how to manually setup the monitoring interfaces.

SmartControl is no longer available for CD-IP.

> To setup the monitoring interfaces:

 Run the System Profile Tool, C:\Program Files\AudioCodes\SmartTAP 360°\tools\system_ profile.exe.

This tool generates a report file called report.txt. This file contains a list of network interfaces. Choose the interfaces you wish to monitor and then extract the respective GUIDs and interface names from the data provided in the report.

2. Open the C:\Program Files\AudioCodes\SmartTAP 360°\tools\report.txt file and extract the GUIDs and interface names for those interfaces that you wish to monitor (example values are indicated in red in the extract below):

 Fri Mar 31 13:19:31 2017: Details of network interfaces.

 Fri Mar 31 13:19:31 2017: 0x000000e:

 Fri Mar 31 13:19:31 2017: Link encap:Ethernet

 Fri Mar 31 13:19:31 2017: HWaddr 02:00:4c:4f:4f:50

 Fri Mar 31 13:19:31 2017: name:\DEVICE\TCPIP_{65E31628-075A-4DEB

 A09E-C4041EC5F750}

 Fri Mar 31 13:19:31 2017: MTU:1500 Speed:1215.75 Mbps

 Fri Mar 31 13:19:31 2017: Admin status:UP Oper status:OPERATIONAL

 Fri Mar 31 13:19:31 2017: RX packets:0 dropped:0 errors:0 unknown:0

 Fri Mar 31 13:19:31 2017: TX packets:0 dropped:0 errors:0 txqueuelen:0

 Fri Mar 31 13:19:31 2017: Descr: "Microsoft KM-TEST Loopback Adapter"

- Edit the C:\Program Files (x86)\AudioCodes\SmartTAP 360°\CD-IP\config\calldeliveryconfig.xml file:
 - a. Add the extracted GUID and interface name:

<monitoringInterfaces> <interface enabled="1" guid="{65E31628-075A-4DEB-A09E-C4041EC5F750}" adapterName="Microsoft KM-TEST Loopback Adapter" /> </monitoringInterfaces>

b. Set "enabled" to 1 for all those interfaces that you wish to monitor.

Analog Trunk / Radio

The SmartTAP 360° software supports analog loop start phone line trunk or station side and VOX activity based recording. The SmartWORKS LD card is designed for high impedance tapping.

Loop Start Trunk / Station

The battery voltage of the analog line may be different between Trunk and Station side. Adjusting SmartTAP 360° to match the environment is easily achieved and discussed in the next chapter.

The 24-channel card is a Hi-Impedance tap card designed to passively tap the phone line. In the event of a card or server hardware failure, there will be no impact to normal operation of the phone or analog line.

The figure below represents a typical passive tap implementation using a 66 block. The maximum distance tested from PBX to Analog phone while tapping is 2200'.





The image in Figure 1 represents the female connector on the Analog board. The pin-out follows industry standard wiring. The image in Figure 2 is typical color coded wiring used in 25 pair telco grade CAT 3 or higher cables.

Figure 9-8: Color-Coded Wiring-RJ21x Female Connector


Figure 9-9: Color Coded Wiring-25-Pair Color Coding

Call Delivery Install for Analog Recording (Passive Tap)

The Call Delivery Install for Analog Recording is executed when an LD card is detected on the server. The LD card records Analog phones.

The screens shown in the procedure below are specific to the installation when a LD card is detected on the server.

> To install Call Delivery for Analog Recording (Passive Tap):

1. Click Next to continue on the Wizard for Call Delivery LD screen.



Figure 9-10: Call Delivery LD

In case of distributed or remote branch deployment, type in the real IP address of the Application Server (AS), Communication Server (CS), and the Local IP address machine (don't type in 127.0.0.1). In case of all-in-one deployment use the AS, CS, and the Local IP address parameters drop down list to choose the SmartTAP 360° IP address.

2. Click Next on the Server IP Setup.

뻻	AudioCodes Inc. Call Delivery-AL
Server IP Se Configure th	e names or IP addresses of the servers
Communca	tion Server Name or IP Address:
172.26.144.2	3 v
Application	Server Name or IP Address:
172.26.144.2	3 v
Local (non	-monitoring) IP Address:
172.26.144.2	3 ~
InstallShield ——	< Back Next > Cancel

Figure 9-11: Server IP Setup

- 3. Click Next on the Setup Type screen.
- 4. Click Install on the install screen.
- 5. Click Finish to finish.

Additional Configuration for Analog Trunk and Radio

The LD.xml file located in the target path of the Call Delivery is the most common file that needs to be configured for the analog environment. There is only one LD.xml file for all Analog cards. Using XML, you can specify in the LD.xml specific board and channel configurations. For example, board 0, channels 0-7 are voltage trigger based recording and 8-16 are VOX based recording.

Default Path:\AUDIOCODES\SmartTAP 360°\CD-AL\Config\

- LD.xml Configuration file
- LD.xsd Contains parameter definition and valid values.



Figure 9-12: LD.xml Basic Structure Diagram

Most Common Values that may need to be adjusted per board or channel.

Element Name	Attribute Name	Description	Default
deglitch	loopDeglitchTime	Min = 10ms, Max = 2550ms. Ignore Voltage signal bounce on line during hang-up to avoid false call records. Recommend 500ms minimum.	250ms
	ringDeglitchTime	Min = 10ms, Max = 2550ms. Ignore ringing signal bounce on line on incoming call. Avoid false start of recording.	250ms
voltage	thresholdHigh	Min = -60vdc, Max = 60vdc. On Hook voltage must be greater than thresholdHigh.	16vdc
	thresholdLow	Min = -60vdc, Max = 60vdc. Off Hook voltage must be greater than thresdholdLow and below thresholdHigh.	4vdc
Polarity	type	Normal, will cosmetically	normal

Eiguro 0.12	Most Common	Values to	ho Adjusted	nor Roard	or Channel
FIGULE 3-13.		values lu	DE AUIUSIEU	DEI DUALU	

Element Name	Attribute Name	Description	Default
		change line polarity to positive. Reversed, will cosmetically change line polarity to negative.	
alertTone	enable	True = Audible tone will be played on line for both callers to hear to indicate call is being recorded.	false
stateMachine	file	ldgeneric.scxml = User for analog loop start lines activitydetection.scxml = Used for Vox or radio lines	ldgeneric.scxml
CallerID	sensitivity	Min = 2, Max = 128	2
activityDetection	enable		
	thresholdLow	Min = -60, Max = 0dBm, Must be less than thresholdHigh by 3dBm.	-51dBm
	thresholdHigh	Min = -60, Max = 0dBm, Must be greater than thresholdHigh by 3dBm.	-48dBm
	minActivity	Min = 40ms, Max = 2000, Used to trigger recording.	40ms
	maxActivity	Min = 40ms, Max = 20000	10000ms
	minSilence	Min = 500, Max = 20000	5000ms
	maxSilenece	Min = 500, Max = 20000	5000ms
boardID		0-31	All
lineID		0 – 23, 24 channels per board	All

Activity Detection

The Activity detector measures input signal energy in 20 ms samples. The energy measurement is then converted to average power and the result is compared against two

programmable thresholds:

- The silence threshold thresholdLlow
- The activity threshold thresholdHigh

Whenever the detector is in the silence state and the measured input signal energy remains above threshold High for the minActivity duration, the detector changes to the activity state.

Whenever the detector is in the activity state and the measured input signal energy remains below thresholdLow for the minSilence duration, the detector changes to the silence state.



Figure 9-14: Activity Detection

SmartCONTROL

Use the applet in the Windows control panel to configure the Analog card using the Board tab. The only setting that requires configuration is TDM Encoding:

- U-LAW = North America
- A-LAW = Europe, APAC, etc...

nformation For Boa	ard 0				
Board Type	SmartTAP LD:	2409 PCle			
Total Channels	24				
Serial Number	211/1/9				
DateCode	1024				
Firmware Version	05.05.00	Build	1034		
OEM Info	AudioCodes l	JSA, Inc.			
Copyright	Copyright @ 2	007 AudioCodes US	A, Inc. All Rights Re	served.	
Copyright	Copyright @ 2	007 AudioCodes US	A, Inc. All Rights Re	served.	
TDM Encoding	Copyright © 2	007 AudioCodes US	A, Inc. All Rights Re	served.	
TDM Encoding	Copyright © 2	007 AudioCodes US	A, Inc. All Rights Re	served.	
TDM Encoding	Copyright © 2	007 AudioCodes US	A, Inc. All Rights Re	served.	
TDM Encoding © µ-law CT Bus Type © H.100 CT Mode	Copyright © 2	007 AudioCodes US	A, Inc. All Rights Re	served.	
TDM Encoding	Copyright © 2	007 AudioCodes US	A, Inc. All Rights Re	served. autts	
TDM Encoding	Copyright © 2	007 AudioCodes US	A, Inc. All Rights Re	served. auts	

Figure 9-15: Board Tab

SIP Recording (SIPRec)

This section describes the SIP Recording (SIPRec) integration with SmartTAP 360°. In reference to the IETF Charter: The Session Recording Protocol (SIPREC) working group is chartered to define a SIP-based protocol for controlling a session (media) recorder.

https://datatracker.ietf.org/doc/draft-ietf-siprec-protocol/

The scope of the activity includes:

- Recorder Control
- Session metadata content and format
- Security mechanisms, including transport and media encryption
- Privacy concerns, including end-user notification
- Negotiation of recording media streams

What is SIPRec?

The Session Recording Protocol is used for establishing an active recording session and reporting of the metadata of the communication session.

Session Recording Server (SRS)

A Session Recording Server (SRS) is a SIP User Agent (UA) that acts as the sink of the recorded media. An SRS is a logical function that typically archives media for extended durations of time and provides interfaces for search and retrieval of the archived media.

Session Recording Client (SRC)

A Session Recording Client (SRC) is a SIP User Agent (UA) that acts as the source of the recorded media, sending it to the Session Recording Server. In practice, a Session Recording Client could be a personal device (such as a SIP phone), a SIP Media Gateway (MG), a Session Border Controller (SBC), Media Server, or an Application Server. The Session Recording Client is also the source of the recorded session metadata.





To configure SIPRec:

- Ensure the Gateway / SBC (SRC) is properly configured to send call data to SmartTAP 360° (SRS).
- 2. Configure Call Delivery to receive from SRC.

Configuring Gateway & SBC for SIP Recording

You must configure the AudioCodes E-SBC for interworking between the SBC and the SIP Recording Server for the following entities:

- Skype for Business Server environment
- SIP Trunking environment
- SIP Recording server

For configuring Load Balancing between multiple SmartTAP 360° servers, see Configuring Load Balancing on the SBC Device on the next page

For configuring alternative routing, see Configuring Alternative Routing on the SBC on page 145

• For implementing the SBC SIP Recording configuration, the AudioCodes SBC must be installed with an appropriate License Key. For more information, contact your AudioCodes sales representative.

- For detailed information on configuring the SBC for SIP Recording, refer to the appropriate device User's Manual.
- For deploying SmartTAP 360° from the Azure Marketplace with SIPRec-based recording of calls, refer to <u>https://www.audiocodes.com/media/14106/SmartTAP</u> 360°-siprec-in-azure-marketplace-configuration-guide.pdf

Configuring Load Balancing on the SBC Device

This step describes how to configure the SBC for load balancing. This configuration is required when SmartTAP 360° is deployed on multiple servers to balance the load.

To configure Gateway & SBC for SIP Recording:

- Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder>Proxy Sets).
- Add all the CD-SIPREC servers to the SRS's Proxy Set under 'CORE ENTITIES > Proxy Sets > [Index###] > Proxy Address'.



This step is only necessary when there is more than one SmartTAP 360° server deployed.

C TOPOLOGY VIEW	Proxy Sets (7)							
CORE ENTITIES			Date	laft the second second	-			
SRDs (2)	+ New Edit		Page 1	or i == == show _10 •	 records per page 			
SIP Interfaces (3)	INDEX 1	NAME	SRD	SBC IPV4 SIP INTE	ERFACE PROXY KEE	P-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
Media Realms (3)	0	Proxy_SRS	SR1 (#1)	SIPinterface_0	60			Disable
Proxy Sets (7)								
iP Groups (7)	#0[Proxy_SRS] = #	# [SR1]						Edit
CODERS & PROFILES								
⊿ SBC	GENERAL				REDUNDANCY			
Classification (0)	Name	 Proxy_SRS 			Redundancy Mode			
▲ Routing	SBC IPv4 SIP Interface	 # [SiPinterface_0] 		View	Proxy Hot Swap	Disa	ble	
Routing Policies (1)	TLS Context Name	#[-]		View	Proxy Load Balancing M	eth = Rou	nd Robin	
IP-to-IP Routing (7)					Min. Active Servers for L	oad 1		
Alternative Reasons (1)	1000 1100							
IP Group Set (0)	REEP ALIVE							
SBC General Settings	Proxy Keep-Alive	Disable			ADVANCED			
Call Admission Control Profile (0)	Proxy Keep-Alive Time [[sec] 60			Classification Input	1P A	ddress only	
Malicious Signature (12)	Keep-Alive Failure Resp	onses			DNS Resolve Method			
External Media Source (0)	Success Detection Retri	es 1						
SIP DEFINITIONS	Success Detection Inter	val 10			PROXY ADDRESS	TYPE		
	Failure Detection Retrai	nsmi1			<srs01_ip_addr>:5068</srs01_ip_addr>	UDP		
MESSAGE MANIPULATION					<sr502_ip_addr>:5068</sr502_ip_addr>	UDP		
MEDIA					<srs03_ip_addr>:5068</srs03_ip_addr>	UDP		
INTRUSION DETECTION	Proxy Address 3 items >>							

Figure 9-17: Proxy Set

TOPOLOGY VIEW	Proxy Sets [#0] > Proxy Ad	dress (3)		
CORE ENTITIES				2
SRDs (2)	+ New Edit	Page 1 of 1 Show 10 • recon	ds per page	4
SIP Interfaces (3)	INDEX 🕆	PROXY ADDRESS	TRANSPORT TYPE	
Media Realms (3)	0	<srs01_ip_addr>:5068</srs01_ip_addr>	UDP	
Proxy Sets (7)	1.	<\$R\$02_IP_ADDR>:5068	UDP	
IP Groups (7)	2	<\$R\$03_IP_ADDR>:5068	UDP	
CODERS & PROFILES				
⊿ SBC				
Classification (0) Routing Routing Policies (1)	#2			Edit
IP-to-IP Routing (7)	GENERAL			
Alternative Reasons (1)	Brown Address	CODE ID ADDR-SOER		
IP Group Set (0)	Floxy Adultess	- 100		
Manipulation	Transport Type	- 00P		
SBC General Settings	Proxy Priority	0		
Call Admission Control Profile (0)	Proxy Random Weight	0		
Malicious Signature (12)				
External Media Source (0)				
I SIP DEFINITIONS				
MESSAGE MANIPULATION				
▶ MEDIA				
INTRUSION DETECTION				

Figure 9-18: Proxy Set IP Addresses

 After adding the SIPREC servers to the list, edit the Proxy Set's configuration under Core Entities > Proxy Sets > [Index###] > Edit' and set 'Proxy Load Balancing Method' to 'Round Robin'.

Figure 9-19: Proxy Load Balancing Method

	SRD	#1	[SR1] •		
GENERAL			REDUNDANCY		
Index	0		Redundancy Mode		
Name	Proxy_SRS		Proxy Hot Swap	Disable	•
SBC IPv4 SIP Interface	 #0 [SiPInterface_0] 	+ View	Proxy Load Balancing Method	Round Robin	•
TLS Context Name	1	• View	Min. Active Servers for Load Balancing	1	
KEEP ALIVE			ADVANCED		
Proxy Keep-Alive	Disable	•	Classification Input	IP Address only	•
Proxy Keep-Alive Time [sec]	60		DNS Resolve Method		÷
Keep-Alive Failure Responses					
Keep-Alive Failure Responses					

Configuring Alternative Routing on the SBC

This step describes how to configure an alternative reason (reject messages). The RELEASE CAUSE should match the reason configured in CD-SIPREC config file (see .CD-SIPREC Configuration on page 169). This configuration is required when SmartTAP 360° is deployed on multiple servers as a load.

> To configure alternative routing:

 Open the Alternative Reasons page (Setup tab > SBC folder > Routing > Alternative Reasons).

TOPOLOGY VIEW	Alternative Routing Reasons (2)		
CORE ENTITIES		Data in of 1	Q
SRDs (2) SIP Interfaces (3)		RELEASE CAUSE	
Media Realms (3)	0	486 Busy	
Proxy Sets (7) IP Groups (7)		4xx	
CODERS & PROFILES			
⊿ SBC			
Classification (0) Classificatio	#0		Edit
IP-to-IP Routing (7)	GENERAL		
Alternative Reasons (2) IP Group Set (0)	Release Cause • 486 Bu	usy	
Manipulation			
SBC General Settings			
Call Admission Control Profile (0)			
Malicious Signature (12)			
SIP DEFINITIONS			
MESSAGE MANIPULATION			
▶ MEDIA			
INTRUSION DETECTION			
IP SIP RECORDING			

Figure 9-20: Alternative Routing Reasons

Installing SmartTAP 360° for SIP Recording

This sections describes how to install SmartTAP 360° for SIP Recording.

➤ To install SmartTAP 360° recording:

- **1.** Launch install.bat from the "Suite" folder with "administrator" privileges.
- 2. Select the check boxes for the components as shown in the figure below.

AudioCodes SmartTAP	×
Custom Setup	
Select the program features you want to be installed or upgraded. Unselect the program features you want to be uninstalled.	
■ Recording Components	
AudioCodes Application Server	
☑AudioCodes Communication Server	
☑AudioCodes Database Server	
☑AudioCodes Media Server	
■ Integration Components	
AudioCodes Announcement Server	
AudioCodes Call Delivery AL	
AudioCodes Call Delivery IP	
✓AudioCodes Call Delivery SIPREC	
AudioCodes Media Delivery	5 5
AudioCodes Media Proxy	0
Monitoring Service	
InstallShield < <u>B</u> ack Install	Cancel

Figure 9-21: Install SIP Recording

- 3. Click **Install** and then choose the default configuration.
- 4. Proceed to Configuring Call Delivery for SIP Recording below.

It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter Firewall Configuration on page 51..

Configuring Call Delivery for SIP Recording

During the software installation, configure the CD with the necessary information to connect to the SRC. Configure the Local SIPRec listener IP Address and Port on the SmartTAP 360° server that will be used to receive from the SRC as in the following image. In case of distributed or remote branch deployment, type in the real IP address of the Application Server (AS), Communication Server (CS), and the local IP (don't type in 127.0.0.1). The Local IP and The SIPREC listener IP should be of the server the CD-SIPREC component is running on. In case of all-in-one deployment use the drop down list and choose the SmartTAP 360° IP address.

5	
AudioCodes Inc.	Call Delivery-SIPREC
Server IP Setup Configure the names or IP addresses of the	servers
Communcation Server Name or IP Addres	s:
172.26.144.23	~
Application Server Name or IP Address:	
172.26.144.23	· · · · · · · · · · · · · · · · · · ·
Local IP Address:	Local UDP Port:
172.26.144.23	✓ 5069
Local SIPREC listener IP Address:	Local SIPREC listener UDP Port:
172.26.144.23	5068
InstallShield	< Back Next > Cancel

Figure 9-22: Server IP Setup

Assuming the default parameters are insufficient, additional configuration options are available in the following configuration files.

Table 9-3: SIP Recording – Additional Configuration Files

Configuration File	Purpose
CdSipRecConfig.xml	Sets the IP & Port to receive the SIPRec data. Typically the SmartTAP 360° server.
Calldeliveryconfig.xml	Sets the IP of the SmartTAP 360° Application server. The default value is 127.0.0.1 assuming that the AS and CD are installed on the same server.
	Configures the Regular Expressions to match the specific needs of each customer network. Refer to Target Attributes for more information (see Verify the Target List in Each Call Delivery on page 168).

Recording Genesys PureCloud Contact Center Calls Locally

SmartTAP 360° can record PureCloud Contact Center calls and save them on the SmartTAP 360° server or on a local storage device. The following diagram illustrates the solution architecture.



Figure 9-23: Genesys PureCloud Contact Center Calls

This solution requires termination of the PSTN calls on-premises and requires a Bring Your Own Carrier (BYOC) Premises telephony connection. The BYOC Premises makes it possible to use a premises-based trunk and requires the installation of a PureCloud Edge server. AudioCodes SBC provides the connectivity between a service provider's network and the PureCloud Edge server and integrates with SmartTAP 360° to record these calls. SmartTAP 360° records the Contact Center calls while persisting and presenting the associated call's "interaction id" as part of the recording meta-data in the SysCall ID field.

- The SBC device must be configured to ensure seamless integration of the call recordings mechanism (see Configuring Message Manipulation Rules Genesys PureCloud Contact Center Calls below
- The SmartTAP 360° device can be added to the PureCloud Contact Center (see Adding SmartTAP 360° to the Genesys PureCloud Contact Center User Interface on page 151)

Configuring Message Manipulation Rules Genesys PureCloud Contact Center Calls

This section describes the configuration of message manipulation rules on the SBC device for supporting the Geneys PureCloud Contact Center solution. These message manipulation rules are for SIP messages recorded and saved by the SmartTAPRecording server.

Ensure that you have configured the device for SIP Recording (see Configuring Gateway & SBC for SIP Recording on page 143) and have configured all other relevant SIP entities, including IP Groups for PureCloud and the SmartTAP 360° server. For further assistance, contact AudioCodes support.

> To configure message manipulation rules on the SBC:

- Open the Message Manipulations table (Setup tab > Signaling & Media folder > Message Manipulations).
- 2. Configure Message manipulation rules as shown in the following table:

Table 9-4: Message Manipulation Rules

Configure the following rules (Manipulation Set IDs are examples only):

- Index 0: Verifies the inbound request from the PureCloud IP Group to determine whether SBC call leg should be recorded. If true, stores header.x-inin-cnv in var.session.0".
- Index 1: Verifies the Var.Session.0 value from Index 0, inserts in Header.x-audc-call-id and sends to the SmartTAP 360° Call Recording server IP Group.

Ind- ex	Manip- ulation Name	M- an Se- t ID	Message Type	Condition	Action Subject	Acti- on Type	Action Value	Row Role
0	Store x- header in var.ses- sion	11	Any	Head- er.header.x- inin- cnv con- tentexists And Header header.x- inin-cnv content != "	Var.Ses- sion.0	2 (Mo- dify)	Head- er.x-inin- cnv	0 (Use Cur- rent Condi- tion)
1	Send x- header to SIPRec	12	Invite.Re- quest	Var.Ses- sion.0 != "	Head- er.x- audc- call-id	0 (Add)	Var.Ses- sion.0	0 (Use Cur- rent Condi- tion)

3. Open the IP Group page (Setup tab > Signaling and Media folder > IP Groups).

- 4. Add an IP Group for PureCloud.
- 5. Set Inbound Manipulation Set to 11.

	MESSAGE MANIPULATION		
	Inbound Message Manipulation Set	11	
6.	Add and IP Group for the SmartTAP 3	60° Server.	
7.	Set Outbound Message Manipulation	on Set to 12.	

MESSAGE MANIPULATION	
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	12

Adding SmartTAP 360° to the Genesys PureCloud Contact Center User Interface

This section describes how to add the SmartTAP 360° application to the PureCloud Contact Center user interface.

> To add SmartTAP 360° to Genesys PureCloud :

1. Open the PureCloud Admin interface.

Figure 9-24:	Genesys	PureCloud	Admin

0	Overview / Admin Home				
		PureCloud Admin	n		
					٩
		Account Settings	People & Permissions	Directory	Integrations
		Subscription	Authorized Organizations	Groups	Actions
		Organization Settings	People	Locations	Integrations
			Roles / Permissions	Profile Fields	Bridge
					Single Sign-on
					OAuth
		Documents	Contact Center	Routing	Outbound Dialing
		Workspaces	Co-browse	Scheduling	Campaign Management
		Search Audits	Analytics	Call Routing	List Management
			ACD Skills	Emergencies	Callable Time Sets
			Utilization	Disconnect Interactions	Call Analysis Responses
			Queues	Architect	Rule Management
			Wrap-Up Codes	Data Tables	Wrap-up Code Mappings
			Email		Search Audits
			Canned Responses		Event Viewer
			Web Chat		Outbound Settings
			Contrato.		

2. From the Integrations menu, choose Integrations, select to add an integration and choose to install on the Custom Client Application tile.



3. In the Integrations menu, name the application SmartTAP 360°.

Figure 9-26: Application Name

00			Coff Queue	
0	Integrations / Integration	ns / SmartAP		
\$	Integrations	Details Configuration Support		
Q	Actions		Inactive	
G	Single Sign-on	Embeds third-party web pages in the PureCloud UI.		
¢	OAuth	SmartTAP		
8		Notes		
9				
â				
		Last Updated: Today at 457 PM		

4. Under the **Configuration** tab paste the SmartTAP 360° URL in the Application URL field:

				Q & Oll Good
0	Integrations / Integratio	ns / SmartTAP		
\$	Integrations	Details Co	figuration Support	
	Actions			
ρ	Bridge	Properties	Properties	
C4	Single Sign-on	Advanced	O 144 Presente	
	OAuth	Credentials		16km
&			Property Name	value
A			Application URL * The URL of the Application PureCloud should load.	https://smarttap.audiocodes.com/smarttap/welcome.jsf
			Application Type *	standalone
Q			Dictates the way the application will appear and function inside of Purecioud	
ළු			Application Category Tailors application behavior to a specialized purpose.	·
			Iframe Sandbox Options Comma-separated list of limited HTML5 iframe sandbox options to control application permissions	allow-scripts, allow-same-origin, allow-forms, allow-modals
			Group Filtering List of Groups whose members can see this application. Hidden if no group is selected.	Weakers Select Groups

4. Save and Activate the application.

Figure 9-27: Save the Application

00	Activity Directory -	Documents Performance 👻	Reports Apps 🕶 Admin			Q 👃 🔿 Off Queue
0	Integrations / Int	rations				
~	Integrations					Integrations
~	Actions		٩			
D	Bridge	Name 🔺	Category	Status	Last Updated	Actions
	Single Sign-on	SmartTAP	Client Anns	Active	11/12/2018	
¢	OAuth		onen rappe			
~						
₽						
Ø						

5. To open the SmartTAP 360° Web, from the Toolbar choose Apps.



							Q Off Queue
Caudiocodes sm	nartTAP 🔞 Home 🧕	Нир					Initial User (PLEASE DELETE)
Gurtern Litrare Ctatur	Calls before 12/17/18 08:56 PM						
System Cours Status ()							
Calls Messages	2						
From: 6 * 56 * PM *				Direction	C Palazca Cauca	Media Turse	SurCall ID
To: 12/17/18 8 • 56 • PM •	User/Device	Started	Ouration	0 Select	Select	Select	System to
Active Users	Aharonov, Ofer	Nov 21, 2018 3:58:28 PM	00:00:30	INCOMING	NORMAL		b0b369a5-de99-4d6d-9c72-5ab218c9d62b
Active Devices Inactive Devices	Aharonov, Ofer	Nov 21, 2018 3:57:03 PM	00:00:44	INCOMING	NORMAL	4)	4823ed4d-d265-424f-8c88-271f233ce3c5
 Users/Devices Groups 	Aharonov, Ofer	Nov 21, 2018 3:55:22 PM	00:01:06	INCOMING	NORMAL	40	e5ab0a8a-179a-4b63-8ecf-b9c90a6a7c66
Abaronov Ofer	Aharonov, Ofer	Nov 21, 2018 3:44:44 PM	00:00:26	INCOMING	NORMAL	40)	a0051ed9-55f1-4517-9462-b3f3ecc11b48
Test2, Test2	Aharonov, Ofer	Nov 21, 2018 3:42:26 PM	00:00:32	INCOMING	NORMAL	43)	55f6aa49-04d5-418e-a464-e9ccad631e45
User (PLEASE DELETE), Initial	O Test2, Test2	Nov 13, 2018 5:36:38 PM	00:01:08	INCOMING	NORMAL	\$)	b5d49c3d-cb66-4906-bce8-38f8837dfcab
	O Test2, Test2	Nov 13, 2018 5:35:41 PM	00:00:38	INCOMING	NORMAL	40)	bc0c6efb-f520-4e63-9938-b9721cc8c49e
	Aharonov, Ofer	Nov 13, 2018 5:29:54 PM	00:00:45	INCOMING	NORMAL	40)	8afe79c1-74be-4420-8211-67adfad01a08
	Aharonov, Ofer	Nov 13, 2018 5:29:33 PM	00:00:13	OUTGOING	NORMAL	43)	6e9c487e-74ac-44f9-a1bf-1042ef90c283
	Aharonov, Ofer	Nov 13, 2018 5:29:03 PM	00:00:23	INCOMING	NORMAL		8f1820f8-a725-45dd-ae58-b2e9ba73c119
×				10 7 14 44 1	2 3 🗪 🖬 (1 of 3)		
Call Parties: Calling				То	tal calls: 26		
0-8-4	READY						00:00 00:00:00
Called							
Answered							the second se
							a non in an in a
Call Tags:	•					<u>─</u> ──-{ ₩ { > ¶···─-	- ₩ · · ·!+ ·!++ ·₩₩ +++ ·1
Active Taos Inactive Taos	4.40		13.20		22.00	30.80	30.60
Tag Name Tag Value							
Select One				~	000		
Durant	0.2 -0 5.0			(• • •		
Starch							Excel Ensit Dov

10 Additional Configuration Options

This chapter describes the following additional configuration options:

- Configuring Digital Signatures below
- Configuring LDAP on the next page
- Configuring SSO on the next page
- Configuring HTTP/S on page 156

Configuring Digital Signatures

Configuring Digital Signature is a two-stage process:

- Setup in the SmartTAP 360° Web interface Refer to SmartTAP 360° User's Guide
- Setup at the Client PC (each client PC)

Configuring the SmartTAP 360° Web Interface

Refer to the Certificate and Digital Signature sections in the SmartTAP 360° Administrator Guide.

Configuring the PC Client

This section describes how to configure the PC client.

> To configure the PC client:

- Open SmartTAP 360° installer root folder and navigate to Tools\DigitalSignaturesPropertySheet\
- 2. Right-click the install.bat file and select Run as administrator.
- **3.** Once installed, the Digital Signatures tab is displayed in the file properties of the downloaded audio recording.
- 4. Click the Digital Signatures tab to view the certificate and verify it is from a trusted source.

igure to t	
Johnston_Ch	nard_2014_07_15_16.35.51.wav Properties
General Digita	al Signatures Security Details Previous Versions
WAV	Johnston_Chard_2014_07_15_16.35.51.wav
Type of file:	Wave Sound (.wav)
Opens with:	🜔 Windows Media Player 🛛 <u>C</u> hange
Location:	C:\Users\cjohnston\Desktop
Size:	933 KB (956,083 bytes)
Size on disk:	936 KB (958,464 bytes)
Created:	Today, July 17, 2014, 4 minutes ago
Modified:	Today, July 17, 2014, 4 minutes ago
Accessed:	Today, July 17, 2014, 4 minutes ago
Attributes:	Read-only Hidden Advanced
	OK Cancel Apply

Figure 10-1: Digital Signatures



You may need to reboot the PC to complete the installation.

Configuring LDAP

The SmartTAP 360° LDAP feature allows you to use your Windows Active Directory users and groups in SmartTAP 360°, and map them into users, groups and security groups in SmartTAP 360°. The users and groups are not imported. SmartTAP 360° represents is the real time view of what is in Active Directory. For example, if something changes on the AD, such as the user name, that change is reflected almost instantly in SmartTAP 360°.

Refer to the SmartTAP 360° Administrator Guide for LDAP configuration details.

Pre-Requisites

- Create or provide a user account with read-only access to Active Directory. Should be part of read-only domain controller group]
- The password for this service account should be set to "never expire"

Configuring SSO

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

in the background through Active Directory using the same domain credentials that were used to log into the machine. This bypasses the login page and immediately opens the Welcome page.



The SmartTAP 360° server must be added to the Domain. For information on configuring SSO, refer to the *SmartTAP 360° Administrators Manual*.

Configuring HTTP/S

This section describes how to configure HTTP/S.

Disabling HTTP Communications on Application Server (Optional)

This section describes how to disable non-encrypted HTTP communication on SmartTAP 360° Application Server. This ensures that all communications with the Application Server are encrypted. This can be done automatically or manually. If you are implementing SSL (HTTPS), then this action ensures that all incoming traffic to the Application Server is over HTTPS.

Configuring SmartTAP 360° Application Server for HTTPS does not automatically disable the HTTP (non-encrypted) interface. While the SmartTAP 360° management Web page would be available over HTTPS, SmartTAP 360° components would continue to communicate with SmartTAP 360° Application Server over HTTP. To convert the entire application to encrypted communications (over SSL), after disabling HTTP in Application Server as described below, SmartTAP 360° components must be configured as described in Section Configuring SmartTAP 360° Components for HTTPS on the next page (Configuring SmartTAP 360° Components for HTTPS).

Automatic Disabling of HTTP

This section describes the automatic procedure. This method requires a mandatory username and password to access Wildfly management console.

> Do the following:

- 1. Go to the Application Server Install directory.
- Locate the PowerShell directory. For example C:\Program Files\AUDIOCODES\SmartTAP 360°\AS\PowerShell.
- 3. Run the DisableHttp.ps1 script (located in the "Tools" folder of SmartTAP 360° installation) with the following parameters:
 - [Mandatory] managementIP IP address of HTTP Management interface (Application Server IP)
 - Management user credentials:
 - [Mandatory] username

- [Mandatory] password input prompt will be displayed as a part of the current run
- [Optional] jbossCliPath Full path to jboss-cli.bat (Command Line Interface)

For example:

DisableHttp.ps1-managementIP 192.168.1.100-username username - - jbossCliPath C:\Program Files\AUDIOCODES\SmartTAP 360°\AS\Bin\jboss-cli.bat

4. Restart the requested service.

Manual Disabling of HTTP

This section describes how to manually disable HTTP.

> Do the following:

- **1.** Stop the SmartTAP 360° Application Server service.
- 2. Edit ../AudioCodes/SmartTAP 360°/AS/Domain/Configuration/domain.xml
- 3. In urn:jboss:domain:undertow:4.0, comment out the listener element:

Remove http-listener

- 4. Under urn: jboss: domain: messaging-active mq: 2.0 subsystem:
 - Change element http-connector attribute Value socket-binding from "http" to "https"
 - Change http-connector-throughput socket-binding from "http" to "https"
 - Change http-acceptor http-listener from "default" to "https"
 - Change http-acceptor-throughput http-listener from "default" to "https"
- 5. Under subsystem urn:jboss:domain:remoting:4.0 change http-remoting-connector connector-ref from "default" to "https".
- 6. Restart the SmartTAP 360° Application service.

Configuring SmartTAP 360° Components for HTTPS

This section describes how to configure HTTPS on SmartTAP 360° components. CA Root Certificate/s used to sign the Application Server certificate must be installed on each machine where SmartTAP 360° components are installed. SmartTAP 360° supports HTTPS/TLS 1.2.



For generating and loading certificates, refer to Section 'Generating and Loading Certificates' in the *SmartTAP 360° Administrators Guide*.

Communication Server with HTTPS

This section describes how to configure the Communication server.

Do the following:

- On every host where CS is installed, check file "<CS_installation_Dir>\server-\ngp\data\mbeans\managedDeviceProperties.properties" and note that the entry "HOST=..." contains a value which is present in the SAN part of the AS certificate. If it is not, change it accordingly.
- 2. Find the entry "port=-1" and change it to "port=443".
- 3. Change the entry "scheme=http" to "scheme=https".
- 4. Restart the CS service for the changes to take effect.

Call Delivery with HTTPS

This section describes how to configure the Call Delivery server.

> Do the following:

- Edit the following file: "...\AudioCodes\SmartTAP 360°\CD-IP\Config\calldeliveryconfig.xml"
- Use an FQDN in the certificate SAN field in the Call Delivery configuration file calldeliveryconfig.xml (and make sure that DNS resolution is working correctly for this FQDN).

An example of calldeliveryconfig.xml HTTPS settings is shown below:

```
<applicationServer>
<recorder ip="SmartTAP 360°.company.com" port="443">
<protocols>
<protocol>https</protocol>
</protocols>
</recorder>
</applicationServer>
```

- 3. Edit the following file: "...\AudioCodes\SmartTAP 360°\CD-IP\Config\persistence.xml
- 4. Use a FQDN in the certificate SAN field in the Call Delivery configuration file persistence.xml (and make sure that DNS resolution is working correctly for this FQDN).

url="https://SmartTAP 360°.company.com:443"

Where "SmartTAP 360°.company.com" is the FQDN of the SmartTAP 360° AS

5. Restart the service to apply changes.

Using an entry not present in the SAN section of the certificate will lead to a communications failure between the Plugin and Application Server (AS):

An error occurred while sending the request.

---> System.Net.WebException: The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel. ---> System.Security.Authentication.AuthenticationException: The remote certificate is invalid according to the validation procedure.

Media-Proxy with HTTPS

This section describes how to configure the Media Proxy server.

> Do the following:

1. Edit file System.config in "..\MP\Config" and change asList attribute's value in the following section of the Media Proxy Service file:

<System asList="http://AS_FQDN:80"/>

2. Modify to the following

<System asList="https://AS_FQDN:443"/>

- 3. Make sure AS_FQDN is included in the certificate SAN field and is resolvable by DNS.
- 4. Restart the service to apply changes.

Announcement Server with HTTPS

This section describes how to configure the Announcement server.

> Do the following:

1. Manually edit asList attribute's value in "..\AS\Config" and change the following section of the Announcement Service System.config file:

<System asList="http://ASIP:80"/>

2. Change to the following:

<System asList="https://AS_FQDN:443"/>

- 3. Make sure AS_FQDN is included in the certificate SAN field and is resolvable by DNS.
- **4.** Restart the service to apply changes.

Remote Transfer Service with HTTPS

This section describes how to configure the Remote Transfer Service.

> Do the following:

1. Edit file System.config in "..\RTS\Config" and change asList attribute's value in the following section of the Remote Transfer Service file:

<System asList="http://AS_FQDN:80"/>

2. Modify to the following:

<System asList="https://AS_FQDN:443"/>

3. Use the FQDN that is found in the certificate SAN field in these files.

url="https://SmartTAP 360°.company.com:443"

Where "SmartTAP 360°.company.com" is the FQDN of the SmartTAP 360° AS



Make sure DNS resolution is working correctly for this FQDN.

4. Restart the RTS service to apply changes.

Health Monitor with HTTPS

This section describes how to configure the Health Monitor.

> Do the following:

- 1. Edit the file Tools\HealthMonitor\Config\RecordingHealthMonitor.config
- 2. Find this section in the configuration file:

<RestApi> <Address>http://[address which is present in the SAN </Address> <Username></Username> <SecurityToken></SecurityToken> </RestApi>

- 3. Make the highlighted changes:
 - <RestApi>
 - <Address>https://SmartTAP 360°.company.com]</Address>
 - <Username></Username>

<SecurityToken></SecurityToken> </RestApi>

Where "SmartTAP 360°.company.com" is the FQDN of the SmartTAP 360° AS

Media Delivery with HTTPS

This section describes how to configure Media Delivery with HTTPS.

- > Do the following:
- 1. Edit the following file: ".....\AudioCodes\SmartTAP 360°\MD\Configpersistence.xml
- Use a FQDN present in the certificate SAN field in Media Delivery configuration file persistence.xml (and make sure that DNS resolution is working correctly for this FQDN. Media Delivery may be connected to multiple SmartTAP 360° servers, so each of these connections must be edited in the file.

3. Restart the service to apply changes.

Configuring Syslog Server Connection

This section describes how to setup the connection with a syslog server.

Skype for Business Plug-in

This section describes how to setup the syslog server connection between the Skype for Business Front End and a syslog server. This procedure must be setup on every Front End machine in the managed pool.

> To setup connection:

1. Obtain the machine ip that runs the system viewer, EX: 172.17.127.XXX.

2. In the front-end machine, edit the C:\Program Files\AudioCodes\SmartTAP 360°\Lync Plug-in\LyncPlugIn.exe.config

Add / Edit required syslog appender. Example : Log and Error logs are defined in the <log4net debug="true"> section (this section does not include a MAC address)

```
<appender name="RemoteSyslogAppender"
type="log4net.Appender.RemoteSyslogAppender">
  <facility value="Local7" />
  layout type="log4net.Layout.PatternLayout" value="LPI: %d{dd MMM yyyy
HH:mm:ss,fff } %-5p %m\r\n" />
  <remoteAddress value="172.17.127.XXX "/>
  <RemotePort value="514" />
 </appender>
<appender name="RemoteSyslogAppenderError"
type="log4net.Appender.RemoteSyslogAppender">
  <facility value="user" />
  layout type="log4net.Layout.PatternLayout" value="LPI: %d{dd MMM yyyy
HH:mm:ss,fff } %-5p %m\r\n" />
  <param name="Threshold" value="ERROR" />
  <remoteAddress value="172.17.127.XXX "/>
</appender>
```

 On the front-end machine, edit the C:\Program Files\AudioCodes\SmartTAP 360°\Lync Plug-in\LyncPlugIn.exe.config

Edit the <root> section

Add

<appender-ref ref="RemoteSyslogAppender"></appender-ref> <appender-ref ref="RemoteSyslogAppenderError"></appender-ref>

4. Save the file and restart the Plug-in.

Location-Based Targeting in SmartTAP 360°

This section describes how to assign targets to specific Call Delivery components by assigning a location attribute to each instance of the Call Delivery server and then mapping targets to those locations.

By assigning targets to specific Call Delivery components, the physical location of the recording can be controlled. In addition, the loads on each Call Delivery can be minimized. By default, when no location attributes are set, Call Delivery tracks all targets. In systems with large numbers of targets, this can affect the performance of SmartTAP 360°.

Assign a Location Attribute to each Call Delivery Component

Each Call Delivery instance must be manually assigned a value, which is generally referred to as a location attribute, although it does not technically have to refer to a location. The location attribute should be something meaningful within the system topology, which is often a location.

In the first example below, there are three Remote Data Delivery (RDD) installations, all managed by a central Application server. Each Call Delivery in the RDD is assigned a location attribute: "Tasmania", "London", and "New York".



Figure 10-2: Location Attribute for each Call Delivery Component

In the second example below, there are two different Call Delivery components installed on the same server. Their "location attribute" references the intended functionality rather than a physical location. In this case, One Call Delivery handles "Skype" targets and the other handles "SIPREC" targets.

Figure 10-3: Skype and SIPREC Targets



In the case of SmartTAP 360° systems configured in the active/active mode, where Call Delivery components are organized into pairs for redundancy, both components in the pair must share the same location attribute value.

The location attribute must be set manually for each Call Delivery instance. This value is not displayed in the SmartTAP 360° GUI.

> Do the following:

- 1. Stop the Call Delivery service(s) in the service manager.
- Open the calldeliveryconfig.xml file for editing. By default, the configuration file is located in "C:\Program Files (x86)\AudioCodes\SmartTAP 360°\CD-xx\config\calldeliveryconfig.xml", where xx represents which type of Call Delivery was installed.

Within this file is an XML element called <targeting>:

<targeting></targeting>
<attributes></attributes>
<targetconversions></targetconversions>
<converter <="" format="\2" regex="(sips?:)?([^@]*)(@.*)?" td=""></converter>
type="SIP_URI">
<pre><converter format="\1" regex="(\d+)" type="TRUNK ID"></converter></pre>
<converter <="" format="\5" regex="(tel:)?(\+?)(\d+)(;ext=)(\d+)" td=""></converter>
type="EXTENSION">
<converter <="" format="\2" regex="^(\+?)(\d+)" td=""></converter>
type="EXTENSION">
<pre><converter regex="(tel:)?(\+?)(\d+)(;ext=)(\d+)" type="TEL_URI"></converter></pre>
<target format="\3"></target>
<target format="\5"></target>
<target format="\3\4\5"></target>
<converter <="" format="\3" regex="^(tel:)?(\+?)(\d+)\$" td=""></converter>
type="TEL_URI">

If no location attribute has been set, then you will see that the <attributes> element is empty, as shown above. The <targetConversions> element is not relevant for the purposes of setting a location attribute.

Add a new entry in the <attributes> element as shown. From the first example, the first RDD has a location attribute with the value of "Tasmania", so that is what is shown in the example.

```
<targeting>
<attributes>
<attribute name="Location">
<value>Tasmania</value>
</attribute>
</attribute>
```

The attribute name should be set as "Location". This is a convention that makes it easier to understand what is being configured and how to troubleshoot it. The attribute name can have any value, though it must be at least one character long.

Call Delivery can support multiple <attribute> elements under the <attributes> element and multiple <value> elements under each <attribute>. However, the use cases for doing so are extremely rare.

The entries for the attribute name and <value> are case-sensitive, so it is important to make a note of exactly how they were entered into the configuration file. These values will be needed again in a later step.

Once the location attribute is set up, save the configuration file and use the Service Manager to start up the Call Delivery component. Remember to do this for each Call Delivery within the SmartTAP 360° system.

Multiple Call Delivery components can use the same location attribute value. This means that targets that match this value will be tracked by multiple Call Delivery components. This is another example of a rare use case.

Create a Location Attribute in the SmartTAP 360° GUI

To assign a location to each target, a new attribute must be created. Attributes are a way to assign meta-data to each targeted user or device. In this case, we are creating an attribute that Call Delivery will specifically look at in order to match its location attribute with the targets'.

> To create a Location Attribute for a user:

1. Click Users > User Management > Add User Attribute

Figure 10-4: Add User Attribute

Add User Attribute			
Attribute Name	Location		
Attribute Description	Location Attribute		
Network Mapping			
		\bigotimes	\oslash
		Submit	Cancel

2. For the "Attribute Name" enter "Location". If you decided to use a different attribute name in the Call Delivery configuration file, then enter that name here instead. You must enter the value exactly as it appears in the Call Delivery configuration file.

- **3.** Enter a useful description under "Attribute Description". This field does not need to match any specific value.
- 4. Leave the "Network Mapping" checkbox unchecked.
- 5. Click Submit to add the new user attribute.

If there are devices targeted in addition to (or instead of) users, then create the same attribute under Users > Device Management > Add Device Attribute. User attributes and Device attributes do not conflict with each other, therefore they can use the same "Attribute Name".

Assign a Location to Each User/Device in the SmartTAP 360° GUI

The last step is to assign a location to each user and/or device that is targeted for recording. The idea is to associate each target with a specific Call Delivery.

Below is an example of adding a new user and setting its location attribute at the same time. To add a user, click on "User" -> "User Management" -> "Add User". Following the first example, by setting the "location" field to "Tasmania" as shown below, this new user will only be tracked by RDD #1. RDD #2 and RDD #3 will disregard this user because its location attribute doesn't match what was configured in the Call Delivery configuration file.

Add User				
	First Name	John	Last Name	Smith
	Email	John.Smith@acme.com	Login Id	jsmith
	Id / Alias	jsmith	Extension	5555
	Location	Tasmania	TelNo	18005551234
	UserName	JohnS	Retention Policy	Default 💌
	Recording Profile	Full Time	Legal Hold	OFF
Security Profiles			Groups	
administrator		<u> </u>	Default	
supervisor				
		x		-
1				
				Sudawita Canada
				Submit CarlCer

Figure 10-5: Add User

> To update the location attribute for existing users:

- 1. Click Users > User Management > View/Modify Users.
- 2. Click the "pencil" icon in the "Modify" column for the user you wish to edit. Enter the location attribute value in the "Location" field similar to the screen above.



When SmartTAP 360° is configured to map its users and their attributes from the Active Directory, the SmartTAP 360° location attribute can be mapped to the LDAP attribute that holds the appropriate location information through the SmartTAP 360° LDAP Configuration page.

*				User Mappings			
Base Context	OU+LyncUsers,DC+lcent4,DC+local		Browse				
Mapping Filter	(&(objectClass=user))		Create Filter				
First Name	givenName	•					
Last Name	sn	•					
Login	sAMAccountName	•					
Email	mai	•					
Alias	Choose One	•					
Location	location	•					
SIP_URI	lastContentIndexed lastKnownParent	•					
TEL_URI	lastLogoff lastLogon						
	lastLogonTimestamp						~
	lastSet line lasti IndateSequence	-				S	$\mathbf{\nabla}$
	IDAPAdminLimits					Concer	SUMILE
Base DN	DAPDisplayName D&PIDpanel int			Filter	Modify	Delete	
OU=LyncUsers,DC=	leggovExchangeDN			(&(objectClass=user))	1		
	InkTrackSecret	-		Group Mannings			
	ImPwdHistory			aroup ruppings			
•	localeD		Sei	curity Group Mappings			
	localizedDescription						
	locaPolicyFlags						
	locaPolicyReference						
	location	<u> </u>					

Figure 10-6: SmartTAP 360° LDAP Configuration page

Once the location attribute has been set/changed and submitted, each Call Delivery component is updated with the new targeting information. For those Call Delivery components that have a location attribute set, they will ignore any target that does not precisely match their location attribute.

Verify the Target List in Each Call Delivery

It is possible to optionally check to make sure that each Call Delivery component has been updated with the intended target list. Open the file call TargetList.xml. By default, the file is located in "C:\Program Files (x86)\AudioCodes\SmartTAP 360°\CD-xx\TargetList.xml", where xx represents the type of installed Call Delivery instance.

Be sure not to edit or save this file as its 'read only'.

The following is an example of the contents of the file:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<targeting>
<version>2</version>
<targets>
<target caseId="105" mediaType="15" targetIndex="531" type="CALLSTRING"
value="johns"></target>
</targeting>
```

In this example, John Smith is targeted by his user name, which was configured to "JohnS". This value is found in the TargetList.xml file, if the user's location attribute matches the equivalent entry in the Call Delivery configuration file. For example, John has the location attribute 'New York' and there is a CD with the location attribute 'New York'. Target attributes are not case-sensitive so the value appears as lowercase "johns" in the TargetList.xml file. You may need to wait up to one minute for the file to be updated after setting the location attribute in the SmartTAP 360° GUI.

If the expected target is not present in this file, double-check the location attribute value in the Call Delivery configuration file and in the SmartTAP 360° Web interface. Both the attribute name and its value are case-sensitive. The user or device may also fail to appear in the list if it is not targeted for other reasons, such as a lack of licenses or missing targeting attributes.

CD-SIPREC Configuration

The CdSipRecConfig.xml configuration file is displayed as follows:

<SipRecStack> <Listen IP="127.0.0.1" UDP="5068" /> <!--> NoLicenseRejectMsg - Reject message in case no licenses are available <---> <!--> NotTargetedRejectMsg - Reject message for untargeted calls (200Ok with a=inactive) <---> <SRS ExtSysCallIdHeader="x-audc-call-id" NoLicenseRejectMsg="486" NotTargetedRejectMsg="200"/> </SipRecStack>

CD-SIPREC Behavior:

- Available Licenses will be checked for incoming call:
 - CD-SIPREC will reject the call with the configured 'NoLicenseRejectMsg' status code or with the default '486 Busy Here' if the configured code is not valid.
- Regarding calls without any targeted participant, the call will be rejected with 'NormalRejectMsg' OR with 2000K(a=inactive) if the code is not valid, in which case CD will keep the call and record a possible transfer to a targeted user.
- In case None of the CDs have an available license, the call will be rejected by all CDs and multiple alarms will be sent to ST.



'NotTargetedRejectMsg' should be configured to a different reject message than the one configured in the SBC ('Alternative Reason') Note the following regarding the SBC configuration:

- The SBC should support Load Balancing between a group of SRSs (Session Recording Servers)
- A 'rule' to refer a call to another SRS (in the list) can be configured, it is the 'Alternative Reason' I mentioned, in our case it is a custom reject message and should match the one configured in 'NoLicenseRejectMsg'.
- CD-SIPREC supports parsing of external custom headers that are found in the SDP and use them as the call's SysCallId.
 - ExtSysCallIdHeader Configurable external header that will be parsed and used as SysCallId (Original call ID), SBC configuration is also required.

Example

INVITE sip:[field1]@[remote_ip]:[remote_port] SIP/2.0 Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch] From: sipp <sip:[field0]@[local_ip]:[local_port]>;tag=[call_number] To: sut <sip:[field1]@[remote_ip]:[remote_port]> Call-ID: [call_id] CSeq: 1 INVITE Contact: sip:sipp@[local_ip]:[local_port] Max-Forwards: 70 Subject: Performance Test Content-Type: multipart/mixed; boundary=unique-boundary-1 Content-Length: [len] x-audc-call-id: 545362a9-4cb3-4a55-85b8-b33ca83a6517



The x-audc-call-id header will be parsed and the 545362a9-4cb3-4a55-85b8b33ca83a6517 value will be the sysCallId that is displayed in the User Interface.

CD-SIPREC Support in TLS Transport

CD-SIPREC uses the Certificate and the Private Key to maintain a secured, encrypted connection with the SRC (SBC). In case a certificate-chain is used, all the certificates in the chain MUST be stored in one of the 'Trusted Root Certification Authorities' or 'Intermediate Certification Authorities' certificate stores on the CD-SIPREC platform. CD-SIPREC imports the certificates that are found in these stores into its local store. You can also provide a path to the CA certificates folder and CD then loads the certificate files from this location. You can generate the certificates automatically based on the Common Name 'TLSCertCN' or manually from the CertPEMFile\KeyPEMFile:

Generating Certificates Automatically below

- Generating Certificates Manually on page 172
 - Load a matching certificate to the SRC (SBC) that is signed by the same Trusted Root CA.
 - Configure a matching port on both the SRC (SBC) and the CD-SIPREC for securing TLS communication.

Generating Certificates Automatically

This section describes how to generate certificate files automatically based on the Common Name TLSCertCN.



TLS transport is associated with only one Certificate and PrivateKey i.e. the TLSCertCN, therefore ensure that the PEM files CertPEM and KeyPEM files are



empty or deleted in the CdSipRecConfig.xml file.

Do the following:

- 1. Open the CdSipRecConfig.xml file.
- 2. Configure the following:

```
<Listen
IP="0.0.0.0"
TLS="5069"
SSLType="SSLv23"
TLSVerificationMode="None"
TLSCertCN="AudcTLS"
/>
```

Where "AudcTLS" is an example Common Name.



Multiple transports can be configured (UDP\TCP\TLS), for example: <SipRecStack> <Listen IP="0.0.0.0" UDP="5068"/> <Listen IP="0.0.0.0" TLS="5069"<params>....../> <Listen ... </SipRecStack>

- 3. Configure SSLType transport type to one of the following:
 - "NoSSL"
 - "TLSv1" for TLS 1.0 version
 - "SSLv23" for TLS 1.2 and above.
- **4.** Configure TLSVerificationMode (Certificate verification as a part of the TLS handshake) to one of the following:
 - "None"
 - "Optional": certificate verification will be performed only when requested
 - "Mandatory": verification will always be performed
- Configure TLSCertCN a Certificate CommonName that is imported and used for the TLS transport.

CD-SIPREC searches for the certificate in the Local Machine's Personal certificate store. If the store cannot be accessed, CD searches in Current User's Personal store instead.



The certificate MUST contain an exportable Private Key.
Generating Certificates Manually

This procedure describes how to generated certificates manually using the CertPEM and KeyPEM files.

TLS transport is associated with only one Certificate and PrivateKey, therefore ensure that the TLSCertCN entry is empty or deleted in the CdSipRecConfig.xml file.

> Do the following:

- 1. Open the CdSipRecConfig.xml file.
- 2. Configure the following:

```
<Listen
IP="0.0.0.0"
TLS="5069"
SSLType="SSLv23"
TLSVerificationMode="None"
CertPEMFile=".....\<Path>\cert.pem"
KeyPEMFile= ".....\<Path>\key.pem"
CADir="....\<Path>\ Certificates \CA\"
/>
```

Where <Path> is the location of the certificate files on the local machine.

Multiple transports can be configured (UDP\TCP\TLS), for example: <SipRecStack> <Listen IP="0.0.0.0" UDP="5068"/> <Listen IP="0.0.0.0" TLS="5069"<params>...... /> <Listen ... </SipRecStack>

- 3. Configure SSLType transport type to one of the following:
 - "NoSSL"
 - "TLSv1" for TLS 1.0 version
 - "SSLv23" for TLS 1.2 and above.
- Configure TLSVerificationMode (Certificate verification as a part of the TLS handshake) to one of the following:
 - "None"
 - "Optional": certificate verification will be performed only when requested
 - "Mandatory": verification will always be performed
- 5. Configure CertPEMFile- the path to .pem certificate file to be used for the TLS transport.
- 6. Configure KeyPEMFile the path to .pem PrivateKey file to be used for the TLS transport.

These files must NOT be protected with a password (PassPhrase).

 Configure CADir - path to CA certificates that is loaded into CD's local store (for chain certificates).

Delete this text and replace it with your own content.

Example for Creating a Self-Signed Certificate for CD-SIPREC and SBC Connection

This section describes how to create a Self-Signed Certificate for CD-SIPREC and SBC Connection. Perform the following procedures:

- 1. Create a Certificate Signing Request (CSR) below
- 2. Sign the Certificate at the Certificate Authority (CA) below
- 3. Import Certificate to CD-SIPREC Certificate Store on the next page

Create a Certificate Signing Request (CSR)

This section describes how to create a Self-Signed certificate for the TLS connection between the Call Delivery server and the SBC.

> Do the following:

- Enter the Local Machine's certificate store (Action > All Tasks > Advanced Operations > Create Custom Request).
- 2. Click Next on 'Select Certificate Enrollment Policy'.
- 3. Click **Details** and then **Properties**.
- 4. In General tab, enter Friendly Name, for example "AudcTLS"
- 5. In Subject tab, choose 'Common name' from the drop-down list and Add a value:

Figure 10-7: Certificate Properties

- 6. In Private Key tab, check "Make private key exportable".
- 7. Click Apply > Next.
- 8. Choose a file name\directory and save the certificate request.

Sign the Certificate at the Certificate Authority (CA)



Ensure that the Certificate is appropriately signed by the Certificate Authority (CA).

Import Certificate to CD-SIPREC Certificate Store

This section describes how to import the newly generated certificate to the CD-SIPREC Certificate Store.

> To import the certificate to the Certificate Store:

- 1. Return to the Local Machine's certificate store (Action > All Tasks > Import).
- 2. Enter the certificate's path and click Next.
- 3. Under 'Import Options', check "Mark this key as exportable..." and click Next.

Figure 10-8:	Certificate	Import	Wizard
--------------	-------------	--------	--------

← 🧬 Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

l	Display Password
mp	ort options:
[Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
And a	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
ļ	Protect private key using virtualized-based security(Non-exportable)
Į	Include all extended properties.

- Choose 'Place all certificates in the following store', select Personal store and click Next > Finish.
- 5. Try to export the certificate's and validate that the Private Key is exportable.

Enabling OPUS Codec Recording in SmartTAP 360°

This section describes how to enable OPUS Codec Recording for SmartTAP 360°. The OPUS coder must be configured as follows:

- Configuring Opus on Media Server on the next page
- Configuring Opus for CD-SIPREC on the next page

Configuring Opus on Media Server

The SmartTAP 360° Media Server by default does not record audio encoded with the Opus codec. This is because there is no predefined RTP payload type for Opus, or even an informal standard value. To enable the recording of audio encoded with Opus, the Media Server's configuration must be edited with the RTP payload type for Opus, which will depend on the environment where SmartTAP 360° is recording.

> To enable Opus Recording in the SmartTAP 360° Media Server:

- Open the Media Server's configuration file: C:\Program Files (x86)\AudioCodes\SmartTAP 360°\MS\server\bin\ac-hmp20.ini
- If the [RTPMAP] section doesn't exist, add it at the bottom, along with the "Opus48000" parameter, as shown below:

[RTPMAP] Opus48000=x

- **3.** Substitute 'x' with the value of the RTP payload type for Opus. If this parameter is not present in the configuration file, the Media Server uses a default value of 120.
- 4. Save the configuration file and restart the "AudioCodes MS" service using the Windows Service Manager.

Configuring Opus for CD-SIPREC

This section describes how to add support for the OPUS codec in the CdSipRecConfig.xml file under the SipRecStack section.

To configure Opus:

- 1. Open the CDSipRecConfig.xml configuration file.
- 2. Add the following under the SipRecStack section:

<CodecList>

```
<Audio PayloadType="0" Value="PCMU/8000" />
<Audio PayloadType ="3" Value="GSM/8000" />
<Audio PayloadType ="4" Value="G723" />
<Audio PayloadType ="8" Value="PCMA/8000" />
<Audio PayloadType ="9" Value="G722" />
<Audio PayloadType ="18" Value="G729A" />
<Audio PayloadType ="97" Value="RED/8000" />
<Audio PayloadType ="103" Value="SILK/8000" />
<Audio PayloadType ="104" Value="SILK/16000" />
```

<Audio PayloadType ="111" Value="SIREN/16000" />

```
<Audio PayloadType ="112" Value="G7221/16000" />
<Audio PayloadType ="114" Value="x-msrta/16000" />
<Audio PayloadType ="115" Value="x-msrta/8000" />
<Video PayloadType ="122" Value="X-H264UC/90000" />
</CodecList>
</SipRecStack>
</CdSipRec>"
```

The audio codec used by Teams is OPUS and the codec PayloadType and the Value are dynamic and can be changed from one environment to another, therefor it should be configured according to the actual signaling of the call. For example, if OPUS codec **'OPUS/48000/2'** with the id **'111'** is being used, the matching entry in the configuration file should be modified:

```
"...
<Audio PayloadType="111" Value="OPUS/48000/2" />
..."
```

If the CodecList section is empty or does not exist in the configuration file, CD-SIPREC will use its default codec list.



Any new or modified codec must be also supported by the Media Server (see Configuring Opus on Media Server on the previous page).

11 Backup and Restore

This chapter describes the backup and restore procedures

Prerequisites

This section describes actions that you need to perform before running backup and restore procedures.

> Do the following:

1. Go to the control panel and run SmartCONTROL.



2. Make note of the configuration of the Board tab, take screen shots if necessary.

Figure 11-1: Board Tab Configuration

	Board Type	HPX 05.05.00	Server Name	SmrtWrksSrvc	
	Board Build	0023.	Server Build	0023.	
	Copy reser	right (c) 2008-2009 ved.	9 AudioCodes, Inc. All ri	ghts	
-Monitoring Port ()				
C Disable 🙃	Enable A	dapter: Intel(R) 83	2574L Gigabit Network	Connection #2	•
-Monitoring Port 1					
O Disable C	Enable A	dapter: Intel(R) 82	2574L Gigabit Network (Connection #2	v.
Passive Networ	k Settings	Frank ID F	<u>`</u>		_
Passive VLAN	C Disable C	Crable ID: J	~		_
RTP Timeout	C Disable (•	Enable Time: jt	50		
NAT Topology	Disable C	Enable			
. an ropology					
		Linenee	Information		
		License	information		

- Run services.msc (Start->Run->type "services.msc" enter), and stop all SmartTAP 360° services.
 - AudioCodes AS (SmartTAP 360° Server)
 - AudioCodes CS (SmartTAP 360° Server)
 - AudioCodes MS (SmartTAP 360° Server)
 - AudioCodes MS-TR (SmartTAP 360° Server)
 - AudioCodes CD-XX (SmartTAP 360° Server)
 - AudioCodes MD (Skype for Business Edge, Mediation or Conference Server)

- AudioCodes AN (SmartTAP 360° AN Server)
- AudioCodes MP (SmartTAP 360° MP Server)
- AudioCodes Skype for Business plug-In (Skype for Business FE or SBA
- MySQL (SmartTAP 360° Server)
- SmartWORKS Service (SmartTAP 360°, Edge, Mediation or Conference Server)

Backup

This section describes how backup the following components from the command prompt:

- Call Delivery Service (see Call Delivery Service below)
- Media Service (see Media Service on the next page)
- Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server (see Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server on the next page)
- Communication Service (see Communication Service on the next page)
- Application Service (see Application Service on page 180)
- Database (see Section Database on page 180)
- SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA) (see SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA) on page 180)
- SmartTAP 360° Announcement Server (see SmartTAP 360° Announcement Server on page 54)
- SmartTAP 360° Media Proxy (see SmartTAP 360° Media Proxy on page 181)

Call Delivery Service

Configuration	Path	\AudioCodes\SmartTAP 360°\CD-XX\
	Instructions	Copy\AudioCodes\SmartTAP 360°\CD-XX\Config to \$backup_dir\CD-XX\
Logs	Path	\AudioCodes\SmartTAP 360°\CD-XX\
	Instructions	Copy\AudioCodes\SmartTAP 360°\CD-XX\Logs to \$backup_dir\CD-XX\

Table 11-1: Backup - Call Delivery Service



Replace XX with IP, DS or AL depending upon the type of CallDelivery service installed. The SmartTAP 360° server must be added to the Domain.

Media Service

Configuration	Path	\AudioCodes\SmartTAP 360°\MS\Server\
	Instructions	Copy\AudioCodes\SmartTAP 360°\MS\Server\bin\ac- hmp20.ini to \$backup_dir\MS\Server\bin\
Logs	Path	\AudioCodes\SmartTAP 360°\MS \
	Instructions	Copy\AudioCodes\SmartTAP 360°\MS\Log to \$backup_dir\MS\

Table 11-2: Backup - Media Service

Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server

Configuration	Path	\AudioCodes\SmartTAP 360°\MD\Config\
	Instructions	Copy\AudioCodes\SmartTAP 360°\MD\Config\ to \$backup_dir\MD\
Logs	Path	\AudioCodes\SmartTAP 360°\MD \
	Instructions	Copy\AudioCodes\SmartTAP 360°\MD\Logs to \$backup_dir\MD\

 Table 11-3: Backup - Media Delivery Service

Communication Service

Table 11-4: Backup - Communication Service

Configuration	Path	\AudioCodes\SmartTAP 360°\CS\bin\
	Instructions	Copy\AudioCodes\SmartTAP 360°\CS\bin\service.bat to \$backup_dir\CS\bin\
Logs	Path	\AudioCodes\SmartTAP 360°\CS \Server\NGP\
	Instructions	Copy\AudioCodes\SmartTAP 360°\CS\Server\NGP\Log to \$backup_dir\CS\Server\NGP\

Application Service

Configuration	Path	\AudioCodes\SmartTAP 360°\AS\bin\		
	Instructions	Copy\AudioCodes\SmartTAP 360°\AS\bin\service.bat to \$backup_dir\AS\bin\		
Logs	Path	\AudioCodes\SmartTAP 360°\AS\standalone\		
	Instructions	Copy\AudioCodes\SmartTAP 360°\AS\standalone\log to \$backup_dir\AS\standalone\		

Table 11-5: Backup - Application Service

Database

Table	11-6:	Backup	-	Database
-------	-------	--------	---	----------

Configuration	Path	\MySql\MySql Server 5.6\
	Instructions	Stop SmartTAP 360° AS & MySQL service Copy\MySql\MySql Server 5.6\data directory to \$backup_dir\ MySql_PF\MySql Server 5.6\
	Path	C:\ProgramData\MySQL\
	Instructions	Copy C:\ProgramData\MySQL\MySql Server 5.6 directory to \$backup\MySQL_PD\ Start MySQL & SmartTAP 360° AS service

SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA)

Configuration	Path	\AudioCodes\SmartTAP 360°\SmartTAP 360° Lync Client\
	Instructions	Copy\AudioCodes\SmartTAP 360°\SmartTAP 360° Lync Client\ SmartTapLyncSvc.exe.config to \$backup_ dir\SmartTAP 360° Lync Client\FE#\
Logs	Path	\AudioCodes\SmartTAP 360°\SmartTAP 360° Lync Client\
	Instructions	Copy\AudioCodes\SmartTAP 360°\SmartTAP 360° Lync Client\Logs to \$backup_dir\SmartTAP 360° Lync Client\

Table 11-7: SmartTAP 360° Skybe for Business Plug-in (FE, SBS, SI	Table 11-7:	SmartTAP 3	360° S	Skype for	Business	Plug-in	(FE. SBS.	SBA)
---	-------------	------------	--------	-----------	----------	---------	-----------	-----	---



Replace # in instructions above to the actual ID # of the FE server. Repeat above instructions for each FE in Pool.

SmartTAP 360° Announcement Server

Table 11-8: Backup - SmartTAP 360° Announcement Server

Configuration	Path	\AudioCodes\SmartTAP 360°\AN\Config	
	Instructions	Copy Config folder to \$backup_dir\AN\	
Logs	Path	\AudioCodes\SmartTAP 360°\AN\Logs	
	Instructions	Copy Log folder to \$backup_dir\AN\	

SmartTAP 360° Media Proxy

Table 11-9: Backup - SmartTAP 360° Media Proxy

Configuration	Path	\AudioCodes\SmartTAP 360°\MP\Config	
	Instructions	Copy Config folder to \$backup_dir\AN\	
Logs	Path	\AudioCodes\SmartTAP 360°\MP\Logs	
	Instructions	Copy Log folder to \$backup_dir\AN\	

Media

Copy the directory structure and media files from the path defined in the SmartTAP 360° Web interface (See example screen below). Make sure you retain the same directory structure when backing up media to the backup location. We recommend that you save the screen capture of the recording location to retain your Media file settings.

Add Recording Location	
Location Name	Prime Media Storage
Description	Storage Location for Media Storage
Scheme	file 🗸
Host	
Path	'/C:/media/'MMMMM"/'dd'/'HHmmss'
Path	'/C:/media/'MMMMM"/'dd'/'HHmmss' SUBMIT CANCEL

Figure 11-2: Add Recording Location

System Profile Tool

The System Profile Tool provides a convenient method to capture all the log files for the SmartTAP 360° services on a specific server.

Configuration	Path	\AUDIOCODES\Tools\
	Instructions	 Go to the command prompt Run SystemProfile.exe The system_profile.exe tool will automatically run and capture the results to the SystemProfile.zip file in the same folder
		Before you run a test, you must go to the folder of the SmartTAP 360° service and set the appropriate log level

Table 11-10:System Profile Tool

Restore

This section describes how to restore the SmartTAP 360° components.

To restore the SmartTAP 360° components:

- 1. Install SmartTAP 360° on the new server.
- Run services.msc (Start > Run > type "services.msc" enter), and stop all SmartTAP 360° services.

You MUST restore to the same version of SmartTAP 360° that was backed up (with the same major and minor versions).

This section describes how to restore the following components:

- Call Delivery Service (seeCall Delivery Service on page 178)
- Media Service (see Media Service on page 179)
- Media Delivery Service (see Media Delivery Service on the next page)
- Database (seeDatabase on page 180)
- SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA) (see SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA) on page 180
- Announcement Server (see Announcement Server (AN) on page 61)
- Media Proxy (see Media Proxy on page 185)
- Media (see Media)

Call Delivery Service

Table 11-11:Restore – Call Delivery Service

Configuration	Path	\AudioCodes\SmartTAP 360°\CD-XX\
	Instructions	Rename\AUDIOCODES\SmartTAP 360°\CD-XX\Config to Config.orig Copy \$backup_dir\CD_XX\Config to \AUDIOCODES\SmartTAP 360°\CD-XX\

Replace XX with IP, DS or AL depending upon the type of CallDelivery service installed.

Media Service

Table 11-12:Restore – Media Service

Configuration	Path	\AudioCodes\SmartTAP 360°\MS\Server\bin\
	Instructions	Rename\AUDIOCODES\SmartTAP 360°\MS\Server\bin\ac-hmp20.ini to ac-hmp20_orig.ini Copy \$backup_dir\MS\Server\bin\ac-hmp20.ini to \AUDIOCODES\SmartTAP 360°\MS\Server\bin\

Media Delivery Service

Configuration	Path	\AudioCodes\SmartTAP 360°\MD\
	Instructions	Rename\AudioCodes\SmartTAP 360°\MD\Config\ folder to \Config.orig Copy \$backup_dir\MD\Config to \AudioCodes\SmartTAP 360°\MD\

Table 11-13:Restore – Media Delivery Service

Database

Configuration	Path	\MySql\MySql Server 5.6\
	Instructions	Stop SmartTAP 360° AS service Stop MySQL service Rename\MySql\MySql Server 5.6\data directory to data.orig Copy \$backup_dir\ MySql\MySql Server 5.6\data directory to\MySql\MySql Server 5.6\
	Path	C:\ProgramData\MySQL\
	Instructions	Rename C:\ProgramData\MySQL\MySql Server 5.6 directory to MySql Server 5.6.orig Copy \$backup_dir\MySql_PD\MySql Server 5.6 directory to C:\ProgramData\MySQL\ Start MySQL service Start SmartTAP 360° AS service

Table 11-14:Restore – Database

SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA)

This step is only required if the FE, SBS or SBA was rebuilt

Table 11-15:Restore – SmartTAP 360° Skype for Business Plug-in (FE, SBS, SBA)

Configuration	Path	\AudioCodes\SmartTAP 360°\Lync Plug-in\
	Instructions	Copy \$backup_dir\ Lync Plug- in\\FE#\LyncPlugIn.exe.config to \AudioCodes\SmartTAP 360°\Lync Plug-in\



Replace # in instructions above to the actual ID # of the FE server. Repeat above instructions for each FE in Pool.

Announcement Server

Table 11-16:Restore – Announcement Server

Configuration	Path	\AudioCodes\SmartTAP 360°\AN\
	Instructions	Rename\AudioCodes\SmartTAP 360°\AN\Config\ folder to \Config.orig Copy \$backup_dir\AN\Config to \AudioCodes\SmartTAP 360°\AN\

Media Proxy

Table 11-17:Restore – Media Proxy

Configuration	Path	\AudioCodes\SmartTAP 360°\MP\
	Instructions	Rename\AudioCodes\SmartTAP 360°\MP\Config\ folder to \Config.orig Copy \$backup_dir\MP\Config to \AudioCodes\SmartTAP 360°\MP\

Restoring Media

This section describes how to restore media.

To restore media:

 Copy the directory structure and media files from the path defined in the SmartTAP 360° Web interface (See example screen below).

Make sure you retain the same directory structure when backing up media to the backup location. We recommend that you save the screen capture of the recording location to retain your Media file settings.

Modify Recording Location		
Location Name	SMD-E-drive]
Description	SMD-E-drive]
Scheme	smb 🗸	
Host	172.17.127.130]
Path	'/media/'yyyy'/'MM'/'dd'/'HHmmss]
	SUBMIT	CANCEL

Figure 11-3: Add Recording Location

- Its recommended to define the SMB Scheme host machine with an FQDN instead of an IP address. This prevents situations where the System administrator changes the IP address of the SmartTAP 360° application server and as a consequence, the media files can no longer be accessed.
 - If you define the media location in a different domain to the SmartTAP 360° AS, ensure that write permissions are set for the directory to which you wish to save the media files.
- 2. Reboot the SmartTAP 360° machine
- 3. Check SmartTAP 360° board info using SmartCONTROL, compared with saved board info screen shots if necessary
- **4.** System should be restored and functioning. Verify you can play old calls and that the system can record new calls.

12 Troubleshooting

This chapter is for technical personnel who are responsible for the installation and maintenance of the SmartTAP 360° product.

The AudioCodes support team may refer to the sections in the troubleshooting chapter of this document when assisting customers to resolve technical issues pertaining to the SmartTAP 360° product.

This chapter provides the most common troubleshooting information and procedures; however, does not preclude the need for the customer to contact the AudioCodes support group for further assistance.

How To Validate Port Mirror for Recording Skype for Business Calls

- This section provides a procedure to verify that a proposed or existing SPAN/RSPAN/Mirrored port location (also referred to as the tapping location) meets the SmartTAP 360° recording requirements for Skype for Business.
- The document is not intended as a tutorial. It is assumed that the personnel involved in this activity will be able to examine a basic SIP call flow, to configure SPAN/RSPAN Mirroring on the switches/routers, and to administer the Skype for Business servers.

Prerequisites

The following tools and Administrative privileges are required to perform the procedure in this document:

- Wireshark or IP sniffer tool on SmartTAP 360° server or Testing PC
- Access to Skype for Business server to enable and collect logs
- Access to IP Switch/Router to configure port SPAN/MIRROR
- Ability to place test calls

Introduction: SmartTAP 360° Recording Concepts

The SmartTAP 360° recorder relies on a Microsoft Certified Skype for Business plugin to process the call signaling and on the availability of the MEDIA for the call at the recording NIC interface (s).

The Skype for Business plugin resides on the Front End Server(s) and provides the call details to the SmartTAP 360° recorder which records the MEDIA for the call through the recording NIC interface.

SmartTAP 360° Processing of Skype for Business Signaling

The SmartTAP 360° Skype for Business recorder requires the installation of a plugin for every Skype for Business server that is involved in call forwarding/routing decisions. Typically, these are the (FES) Front End Servers; however, could also be a (SBS) Small Business Server, or a (SBA) Survivable Branch Appliance. The SmartTAP 360° plugin is responsible for collecting the call information (signaling) and sending it to the SmartTAP 360° recorder as shown in the figure below.





Whether the SmartTAP 360° Skype for Business plugin is installed, the Skype for Business Administrator has access to logging facilities that enables the logging of SIP signaling and saving these logs to a text file. This log file contains the Skype for Business call information and the MEDIA information that correlates with the call information that the plugin sends to the SmartTAP 360° recorder.

SmartTAP 360° Media Processing

The SmartTAP 360° recorder uses the call information received through the plugin to locate the MEDIA associated with the call to record. The MEDIA to record MUST appear on the recording NIC interface (or interfaces if two recording NICs are used). The recording NIC interface is connected to the switch/router interface that forwards the mirrored data.



Figure 12-2: SmartTAP 360° Media Processing

Procedure

This procedure includes a step-by-step sequence to guide the user from the setup of Skype for Business and network environment, gathering of data, and finally to the analysis of the data collected.

Setup Skype for Business Logging

This section describes how to setup Skype for Business Logging.

> To setup Skype for Business Logging:

- 1. Log in to the server (FES, SBS, or SBA) as user with Administrative privileges.
- 2. Open the Lync Server Logging Tool:
 - Start > All Programs > Microsoft Lync Server 2010 > Lync Server Logging Tool
- 3. In the Components list, select SIPStack only.
- 4. In the Flags list, select **TF_PROTOCOL only**.
- 5. In the Level, select All.

😌 LYNC2010 - Re	emote Desktop Connection Manager	v2.2						- • •
File Edit Sessi	ion View Remote Desktops Too	ls Help						
🖃 🖓 Plano	Server Manager							
- 🛱 💆	File Action View Help							
	🗢 🔿 🙍 📅 📴 🙆	🛛 🖬 🕨 🖬 🖬 🕨						
- S	Server Manager (LYNC2010)	Services					Actions	
	💽 🜓 Roles						Services	<u>^</u>
-2	Features Disconction	M Services					More Actions	•
- <u>S</u>	Configuration	SmartTAP Lync Servic	e Name	e ^		Description		
	🗄 🥑 Task Scheduler			letwork Store Interface Service		This service delivers network	SmartTAP Lync Serv	vice A
- Č	Windows Firewa	: Server 2010 Logging To	bl					
- 6	WMI Control	ging Options				Global Options		
	🕀 🎊 Local Users and 🔤	omponents		Level		Log File Options		
- 2	🕀 🚰 Storage	BgsDeploymentLibrary		C Fatal Errors		Туре	Maximum Size:	
- <u>S</u>		Routing Data Sync Agen	t i	C Errors		Circular	20 MB	
≧		RtcHost		C Warnings		C Sequential	Accend to log file	
ii - 🛃 D		_ RTCSPL T S4		C Information		C New File		
<u> (</u>		ServerAgent		C Verhose				
		ServerConfiguration		④ AII		Real Time Options		
3.6		ServiceFederationPerf				Enabled	🗖 Display only	
		SIPEPSS4		Elags		- Film Online		
		SIPStackPerf			_	Filter Uptions		
		TranslationApplication		TF_CONNECTION		Enabled	Edit Liear	
		UserServices		TF_SECURITY		Include Filters		
		UserServicesPerf		TF_AUTH				
		_ Webinfrastructure □ WebRelav		TF_PARSE				
		WebRelayPerf		TF_STACKTRACE		Exclude Filters		
		WPP_OC_RDP_APPSHAF	а м	TF_XMLSERIALIZER				
		XDS_File_Transfer_Agent	•	All Flags				
	Log F	le Folder:	C:\Development\L	.ogs			Brow	wse
		Start Logging	View Log Files	Analyze Log Files	Adv	ranced Options	Exit Help	
	No activ Start Lo	e log session. Check the con aging button to start logging th	nponents you wish to lag e checked components	g in the list on the left. For each cl with the configured level and flags.	hecked comp	ponent, configure the log level an	d flags for that component.	Click
		-				2000		
		1	🧛 SI	PP Notification Service		Provides Software Licensing		
			0), S (0), S	QL Active Directory Helper Service OL Server (RTC)		Enables integration with Acti Provides storage, processing		
		1	0.5	OL Server (RTCLOCAL)		Provides storage, processing Provides storage, processing		
			Q. 5	QL Server Agent (RTC)		Executes jobs, monitors SQL		
			Q. 5	QL Server Agent (RTCLOCAL)		Executes jobs, monitors SQL	1	
			<u>. </u>			Þ		
		Extended / Standard	/				1	
			1 1 1					1 00 011
	ಶ 🛃 🛃 🎽	- Celer	🔉 🤍 📈	Þ 💦				* 🕞 👘 🎲 12(14/2011 💻
			N885					

Figure 12-3: Skype for Business Logging

Setup Sniffer

This section describes how to setup the sniffer.

To setup the sniffer:

- 1. Log into the test PC (or SmartTAP 360° Server).
- 2. Start the sniffer software (Wireshark).
- 3. Select the recording NIC interface to monitor.

Capture a Test Call

This section describes how to capture a test call.

> To capture a test call:

- **1.** On the Skype for Business server click "Start Logging" button.
- 2. On the test PC click "Start" to start capturing traffic.
- 3. Place a Skype for Business test call.
- 4. On the Skype for Business server click "Stop Logging" button.

- 5. Click "Analyze" and "Browse" to save the log file.
- 6. On the test PC click "Stop" to stop capturing traffic.
- 7. Save the capture (File -> Save As...).

Analysis

To verify that the MEDIA for the test call is present on the sniffer log, you must first find the signaling for the test call in the Skype for Business log. Once you have found the test call signaling, you must extract the MEDIA information for the call and then examine the sniffer log and see if in fact there was traffic present on the recorded IP and PORT.

Locate Test Call in Skype for Business Log

A strategy to find the test call quickly is to search the log backwards for the string "INVITE sip" which corresponds to the initial SIP message associated with the call as shown in the extract below.

TL_INFO(TF_PROTOCOL) [0]08B8.11C4::12/13/2011-22:14:16.164.0000bab2 (SIPStack,SIPAdminLog::TraceProtocolRecord:SIPAdminLog.cpp(125))\$begin_record

Trace-Correlation-Id: 1066643171

Instance-Id: 000010F8

Direction: outgoing

Peer: 10.133.11.71:1081

Message-Type: request

Start-Line: INVITEsip:10.133.11.71:1081;transport=tls;msopaque=f265f30ed4;ms-received-cid=FB00;grid SIP/2.0

From: <sip:ocs_ client3@planolab.audiocodes.com>;tag=79882da9cf;epid=518fe1de1d

To: <sip:ocs_ client2@planolab.audiocodes.com>;epid=ad43a533af;tag=e63e42b63f

CSeq: 3 INVITE

Call-ID: 3c5eed8dfdc748729bd72ad2c64bf510

... (removed text here)

o=-00 IN IP4 10.133.11.73

s=session

c=IN IP4 10.133.11.73

b=CT:99980

t=0 0

m=audio 1462 RTP/SAVP 114 9 112 111 0 8 116 115 4 97 13 118 101

a=ice-ufrag:E385

a=ice-pwd:x7t5IzxDgQExybbhBdRG1H0F

a=candidate:11UDP 2130706431 10.133.11.73 1462 typ host

a=candidate:1 2 UDP 2130705918 10.133.11.73 1463 typ host

a=crypto:2AES_CM_128_HMAC_SHA1_80 inline:94jUIdYJL2x94mTvmABNbD1cjkxywrN77mP4JQ1T|2^31|1:1

a=remote-candidates:1 10.133.11.71 26064 2 10.133.11.71 26065

... (removed text here)



It is possible that the media information shown in the INVITE message (above) is modified in a later message exchange. If this is the case, further analysis is required.

Compare Call Information with Sniffer Trace

Open the captured sniffer file and search for data to/from the media ports identified in the Skype for Business log.

Mync call	for paul.pcap	Wireshark 1.6.2 (S	VN Rev 38931 from /trunk-1.6)]							
Eile [dit	Yiew Go	Capture Analyze	Statistics Telephony Tools	Internals Help						
	* * *	🖹 🛛 🗶 🕲	📇 🔍 🔶 🔶 🐺 :		ର୍ ର୍ ଷ୍ 📰	a 🗹 🥵	* 8			
Filter ip.	edidr == 10.13	3.11.71 and ip.addr = i	10.133.11.73	Expression	Clear Apply					
No. 1	Time	Source	Destination	Protocol	Length Info					
485	9.200563	10.133.11.71	10.133.11.73	STUN	146 Binding	Request I	user: E385:I//2			
537 1	9.229705	10.133.11.71	10.133.11.73	CLASSIC-5	86 Message	Binding	Request			
540	9.280358	10.133.11.71	10.133.11.73	STUN	146 Binding	Request	user: E385:1//2			
542	9.200429	10.133.11.71	10.133.11.71	STUN	130 Binding	Success I	DISTRICT ESOSIA//2	PPED-ADOPESS:	10 133 11 71-2606	A user: E38
554	9.331301	10,133,11,71	10,133,11,73	STUN	146 Sinding	Request i	ser: E385:1//2	1100-10042-001		
558	9.355431	10,133,11,73	10,133,11,71	STUN	130 sinding	Success I	Response XDR-MA	PPED-ADORESS:	10.133.11.71:2606	5 user: E38
559	9.355528	10.133.11.73	10.133.11.71	STUN	146 Binding	Request I	user: 1//2:E385			
560 1	9.355572	10.133.11.73	10.133.11.71	STUN	146 Binding	Request i	user: I//2:E385			
561	9.381954	10.133.11.71	10.133.11.73	STUN	130 Binding	Success I	Response XOR-MA	PPED-ADORESS:	10.133.11.73:1462	user: I//2:
562 1	9.382162	10.133.11.71	10.133.11.73	STUN	130 Binding	Success I	Response XOR-MA	PPED-ADORESS:	10.133.11.73:1463	user: I//2:"
859 3	13.852980	10.133.11.73	10.133.11.71	CLASSIC-5	86 Message	Binding	Request			
861 3	13.911661	10.133.11.73	10.133.11.71	STUN	150 Binding	Request i	user: 1//2:E385			
862	13.911/51	10.133.11.73	10.133.11.71	STUN	150 Binding	Request	user: 1//2:E385		10 133 11 73-1463	
864	13.932921	10.133.11.71	10,133,11,73	STUN	130 Binding	Success I	Response XOR-MA	PPED-ADDRESS:	10.133.11.73:1402	USEF: 1//2.
870	14.093031	10.133.11.71	10.133.11.73	LIDP	85 Source I	success i	65 Destination	port: nucleur	40.133.11.73:1403	user: 1//2.
871	14.093103	10.133.11.71	10,133,11,73	LIDP	197 Source	ort: 260	65 Destination	port: nucleu		
902	15. 522599	10.133.11.71	10.133.11.73	UDP	85 Source	ort: 260	65 Destination	port: nucleu:	5	
903 1	15.522701	10.133.11.71	10.133.11.73	UDP	217 Source	port: 260	65 Destination	port: nucleu:	5	
925 1	17.521083	10.133.11.73	10.133.11.71	UDP	85 Source	port: nuc	leus Destinati	on port: 2606	5	
926 3	17.521114	10.133.11.73	10.133.11.71	UDP	233 Source	port: nuc	leus Destinati	on port: 2606	5	
928 3	17.878241	10.133.11.71	10.133.11.73	UDP	85 Source	port: 260	65 Destination	port: nucleu:	5	
929 1	17.878440	10.133.11.71	10.133.11.73	UDP	217 Source	port: 260	65 Destination	port: nucleu:	5	
932	18.081266	10.133.11.71	10.133.11.73	UDP	85 Source	port: 260	55 Destination	port: nucleu:	5	
933	18.081358	10.133.11.71	10.133.11.73	UDP	217 Source	port: 260	5 Destination	port: nucleu:	5	
930 /	18 284442	10 133 11 71	10,133,11,73	LIDE	217 Source	OFT: 260	5 Destination	port: nucleur	5	
919	18.593043	10.133.11.71	10.133.11.73	LIDP	SS Source	oort: 260	55 Destination	port: nucleu	<u></u>	
940 1	18.593148	10.133.11.71	10.133.11.73	UDP	217 Source	port: 260	5 Destination	port: nucleu:	5	
¥										
· Frane	939: 85	bytes on wire	(680 bits), 85 bytes c	aptured (680	bits)					
Ethern	net II, S	rc: Dell_4a:b8	:78 (00:14:22:4a:b8:78), Dst: Dell_	4b:4f:ef (00:1	4:22:4b:4	f:ef)			
® Intern	net Proto	col version 4,	Src: 10.133 11.71 (10	.133.11.71),	Ost: 10.133.11	.73 (10.1	33.11.73)			
⊛ User 0	Datagram I	Protocol, Src I	Port: 26065 (26065), D	st Port: nucl	eus (1463)					
🗷 Data ((43 bytes))								
1	0	0					* (1000 C		1 40 11 1 1 10

Figure 12-4: Sniffer Trace

Determine Whether SmartTAP 360° will Record this Call

If there is a correlation between the call information gathered from the Skype for Business protocol log and the sniffer data collected for the recording NIC interface (or switch port forwarding the mirrored traffic), the call meets the SmartTAP 360° recording requirements for Skype for Business.

Troubleshooting Skype for Business Plugin Installation

This section describes the troubleshooting options when the Skype for Business installation plugin fails.

Enable the Browser Service

The Enable the Browser Service service automatically stops if your registry settings are not configured to maintain the browse list.

> To verify your settings:

- 1. Navigate to Start > Run
- 2. Type regedit and click Enter

3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters

The MaintainServerList value should be set to Yes or Auto

If this Value is set to No the computer browser service will not start.

Use "net view" to Verify

Normally you do NOT have to enable "net view" service to run the install; however, sometimes it makes a difference. The reason why entering user credentials sometimes does not work is that the Front End can't see the domain in order to authenticate the user.

A simple test is to run "net view" from the command line. If the command returns a list of servers like is shown in the example below, the install should work. If not, then this indicates that there is a problem with the machine (because it can't currently see the domain).

C:\Users\Administrator.QALABEE>net view Server Name Remark

\\EDGE
\\FE1
\\OCS-CLIENT3
\\OCSCLIENT1
\\QA-USER2
\\SmartTAP 360°
The command completed successfully.

Troubleshoot Skype for Business Recording

This section describes troubleshooting for Skype for Business Recording.

No Records for the Calls

When there are no records for calls, verify the following:

- Make sure the firewall is open for in traffic on port 9901, for out traffic to 9090 on the plugin machine. Also, open for in traffic on port 9090 and out traffic to port 9901 on SmartTAP 360° machine.
- If there are messages in the Skype for Business plugin logs stating "no SIP messages are seen", check for errors and exception in the log files.
- If the Skype for Business plugin failed to register to the Front End, recheck with the customer if the pool name that was provided during Skype for Business plugin installation is correct.

When the Skype for Business plugin is installed on SBA machine, plugin fails to register to FE until the SBA synchronizes with the main FE. It may take 30 minutes or more. It might need to restart the Skype for Business plugin to trigger registration again.

Calls with No Audio

Run Wireshark to capture the tapping interface and make a call. Make sure there are UDP packets in Wireshark and if decoded as RTP they appear as RTP instead of RTP unknown version.

Enabling Promiscuous Mode on VMWare ESXi

- Using the vSphere client, promiscuous mode needs to be enabled in the following locations:
- Configuration -> Networking->Properties (on the applicable vSwitch) ->
 - In the Ports tab, vSwitch Configuration, click edit > Policy Exceptions -> Promiscuous Mode > Change to Accept
 - In the Ports tab, VM Network (applicable network name), click edit > Security > Promiscuous Mode > Change to Accept

13 Known Issues

This chapter describes known issues.

Internet Explorer Security Messages and SmartTAP 360° not Running on Server

Sometimes when configuring SmartTAP 360° on its machine, IE pops-up security messages and/or avoids SmartTAP 360° running in the browser. It might help to go to Server Manager, click Configure IE ECS and turn off enhanced security at least for administrators.

Disable IE ESC by selecting Off or On as shown in the figure below:

Server Manager		
File Action View Help		
🗇 🔿 🛛 🖬 🔹		
Server Manager (OCS) Server	er Manager (OCS)	
E P Roles		
Teacures Teacures Teacures	Get an overview of the status of this server, perform top management tasks, and add or remo	ve server roles and features.
🕀 🎆 Configuration	11 11 11 11 11 11 11 11 11 11 11 11 11	
Storage		
\odot	Server Sum Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.	Server Summary Help
	Computer Internet Explorer Enhanced Security Configuration is enabled by	🔛 Change System Properties
	Full Compu	View Network Connections
	Administrators:	Configure Remote Desktop
	QA Networ On (Recommended)	Management
	Remote De 😵 C Off	
	Server Mar Anageme Isers:	
	Product ID	
	Do not	
	😵 C Off	
6	Security]	🗑 Go to Windows Firewall
	Windows F	Configure Updates
	Windows II	Check for New Roles
	OK Cancel	Run Security Configuration Wizard
		To Contigure IE ESC
	Last installed updates: 2/17/2012 5:24 PM	
	IE Enhanced Security Configuration On for Administrators (ESC): On for Users	
		_
1 Q L	ast Refresh: Today at 9:44 AM Configure refresh	

Figure 13-1: Enhanced Security Configuration

14 Configure Microsoft SNMP Service

The SmartTAP 360° system optionally uses the Microsoft SNMP agent for configuration and alarms. All Windows servers that are part of a SmartTAP 360° installation can have the SNMP feature enabled and configured. This service must can be configured on the following servers:

- SmartTAP 360° Communication Server Installation
- SmartTAP 360° Media Server Installation
- SmartTAP 360° Call Delivery Server Installation

The service must be configured for the SmartTAP 360° Storage Server Installation if different from the SmartTAP 360° server for storage statistics and on the servers in branches for system health presentation.

- SNMP Trap Service must be disabled on SmartTAP 360° servers running the Application Server component.
 - For each SmartTAP 360° software component, it is only necessary to setup the SNMP service once per server.
 - For Call Delivery Server Installation, additional manual configuration is required (see Section Installing the Call Delivery Service on page 25Installing the Call Delivery Service on page 25).

You can install Microsoft SNMP Agent using one of the following methods:

Automatic

Manual

Automatic SNMP Setup

Starting from SmartTAP 360° Version 2.2, there is an automated installer for setting up SNMP on a system. If a system does not have SNMP services installed, this is a simple and easy way to setup SNMP without performing the manual procedure described in Section Configure Microsoft SNMP Service above.

By default, the installer is located within the install package as is not installed to the local drive with the SmartTAP 360° installer.

> Do the following:

- **1.** In your SmartTAP 360° distribution directory, locate the following file in either of the following locations:
 - .\Program Files\AUDIOCODES\SmartTAP 360°\Install\EnableSNMPOnServer.bat
 - .\installation suite\tools\EnableSNMPOnServer.bat
- 2. Right-click and choose "Run as administrator".

Manual SNMP Setup

The procedure below describes how to install the SNMP Server feature.

> Do the following:

- 1. Open Turn on Windows features on or off (Control Panel > Programs and Features > Turn on Windows features on or off).
- 2. Click Features, and click Add Features.
- 3. Select SNMP Services.

Figure	14-1:	Add	Features	Wizard
---------------	-------	-----	-----------------	--------

Add Features Wizard		×
Select Features		
Features Confirmation Progress Results	Select one or more features to install on this server. Eeatures: Multipath I/O Network Load Balancing Peer Name Resolution Protocol Quality Windows Audio Video Experience Remote Differential Compression Remote Differential Compression Remote Server Administration Tools (Installed) RPC over HTTP Proxy Simple TCP/IP Services SMTP Services SMTP Services SMTP Service Storage Manager for SANs Subsystem for UNIX-based Applications Telnet Client Telnet Server TFTP Client Windows Biometric Framework More about features	Simple Network Management Protocol (SNMP) Services includes the SNMP Service and SNMP WMI Provider. > Instell
	- Devices	Cancol

- 4. Open Services (Start > Run... > services.msc).
- 5. Right click over the SNMP Service listing.

Services							- 0 -
<u>File Action View</u>	<u>H</u> elp						
♦ ♦	à 🗟 🛛 📷 🕨 🔳 💷 🕨						
Services (Local)	Services (Local)						
	SNMP Service	Name		Description	Status	Startup Type	Log On As 🔺
	Stop the service Restart the service Description: Enables Simple Network Management Protocol (SNMP)	Secure So Security A Security C Server Shell Harc Smart Car	cket Tun Accounts Center dware De rd	Provides su The startup The WSCSV Supports fil Provides no Manages a	I D Started / Started I Started D Started c Started	Manual Automatic Automatic (D Automatic Automatic Automatic Manual	Local Service Local Syste Local Service Local Syste Local Syste Local Syste
	requests to be processed by this computer. If this service is stopped	Smart Car	d Kemo	Carlana Cia	o Started	Automatic	Local Syste
	computer. If this service is stopped, the computer will be unable to process SNMP requests. If this service is disabled, any services that explicitly depend on it will fail to start.	SNM Softv SpP I SSDF SSDF Supe Syste Syste Tabl Syste Tabl Task TCP/ Telep Telep Ther Ther	Start Stop Pause Resume Restart All Tasks Refresh Help	Es	n Started a b Started b Started c Started b Started b s Started c Started b started b started b started minimized miniminimized minimized minimized minimized minimi	Automatic Manual Automatic (D Manual Manual Automatic Automatic Automatic Automatic Manual Automatic Manual Automatic	Local Syste Local Service Network S Local Service Local Service Local Syste Local Syste Local Syste Local Syste Local Syste Local Service Network S Local Syste
	Extended Standard						

Figure 14-2: SNMP Service

6. Select **Properties** > **Security**; the following screen appears:

SNMP Service Pro	perties (Loc	al Comp	uter)		×					
General Log On	Recovery	Agent	Traps	Security	Dependencies					
Send auther	tication trap									
- Accepted cor	Accepted community names									
Community			Righ	nts						
	dd	Edit		Remo	ve					
C Accept S	NMP packets	from any	host							
Accept S	NMP packets	from the	se hosts							
localhost										
	dd	Edit]	Remo	ve					
Learn more abo	ut <u>SNMP</u>									
		OK		Cancel	Apply					

Figure 14-3: SNMP Service Properties

- 7. In the Accepted community names window, add the following;
 - public Community with READ ONLY rights
 - private Community with READ WRITE rights

The community names must be in lower case.

SNMP Service Properties (Lo	ocal Computer)
General Log On Recover	y Agent Traps Security Dependencies
Send authentication trap	p
Accepted community nam	mes
Community	Rights
public	READ ONLY
private	READ WRITE
Add	Edit Remove
Accept SNMP packet	ets from any host
Accept SNMP packet	ets from these hosts
localhost	
Add	Edit Remove
Learn more about SNMP	
	OK Cancel Apply

Figure 14-4: SNMP Service Properties - Security

- 8. In the Accept SNMP packets from these hosts window, click Add... to add the following:
 - If this is a standalone SmartTAP 360° server, leave localhost as the only entry
 - If this is for a SmartTAP 360° installation that involves more than one server, add the IP address of the Application Server (AS) instead
- 9. Click Apply.
- 10. Select the Traps tab.
- **11.** From the 'Community name' drop-down list, select **public**.
- 12. Click Add to list.

SNMP Service Prop	erties (Loca	al Comp	uter)		×
General Log On	Recovery	Agent	Traps	Security	Dependencies
The SNMP Serv and IPX/SPX pr community name host names, IP a	ice provides otocols. If tra s must be sp addresses or	network aps are re becified. IPX add	manager equired, o Trap dest resses.	ment over ne or more tinations ma	TCP/IP ay be
Community nam	e		-	۸dd	ta list
Trap destination	ns:			Remove	e from list
Add.		Edit		Remove	
Learn more about	SNMP			Canad	
		Oł		Cancel	Apply

Figure 14-5: SNMP Service Properties - Traps

- **13.** Click Add... to add Trap destinations as follows:
 - If this is a standalone server enter localhost
 - If this is for a SmartTAP 360° installation that involves more than one server add the IP address of the Application Server (AS) instead

SNMP Ser	vice Prop	erties (Loca	al Comp	uter)		×		
General	Log On	Recovery	Agent	Traps	Security	Dependencies		
The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.								
	ıblic	-		-	Add	to list		
<u>T</u> rap	<u>Remove from list</u> <u>Iocalhost</u>							
	A <u>d</u> d.		<u>E</u> dit		Re <u>m</u> ove			
Learn n	nore about	<u>SNMP</u>						
			0	(Cancel	Apply		

Figure 14-6: SNMP Service Properties – Traps – Add Trap Destinations

14. Click OK.

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

©2020 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, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-27193

