

SmartTAP

Call Recording Solution

Version 4.2

Table of Contents

1	Hardware and Software Requirements.....	13
1.1	Minimum System Requirements.....	13
1.1.1	Server Configurations.....	13
1.2	Network Adapter Configuration.....	15
1.2.1	General Configuration.....	15
1.2.2	VMWare Specific.....	16
1.3	Telephony Integration Hardware.....	16
1.3.1	Add-On Blades.....	16
1.3.2	Power Requirements.....	16
1.4	Antivirus Software.....	16
1.5	Windows Defender.....	17
1.6	Supported Operating Systems.....	17
1.7	Windows Updates.....	17
1.7.1	Installing Windows Updates.....	17
1.8	Supported Virtual Machine (VM) Environments.....	17
1.8.1	VMware ESXi.....	17
1.8.2	Microsoft Hyper-V.....	17
1.9	Active / Standby Resiliency Configuration (Optional).....	18
1.10	HTML5 Media Player Browser Support.....	18
2	SmartTAP License Management.....	19
2.1	License File Creation and Installation.....	19
2.1.1	License File Creation.....	19
2.1.2	License File Installation and Verification.....	19
2.1.3	SmartTAP Upgrades.....	20
3	Before Installing SmartTAP.....	23
3.1	SmartTAP Software Package Contents.....	23
3.2	Installation Prerequisites.....	23
3.2.1	Configure Microsoft SNMP Service.....	24
3.2.1.1	Automatic SNMP Setup.....	25
3.2.1.2	Manual SNMP Setup.....	25
3.3	Installation Wizard Methods.....	29
3.3.1	All-In-One.....	29
3.3.2	Distributed.....	29
3.4	Post Installation Actions.....	30
4	Installation Wizard - All-In-One Method.....	31
4.1	Database Service.....	33
4.2	Installing the Application Service.....	35
4.3	Installing the Communication Service.....	38
4.4	Installing the Call Delivery Service.....	40
4.5	Installing the Media Server.....	42
4.6	Completing Wizard Installation.....	44
4.7	Post-Installation Integration.....	44
5	Installation Wizard - Distributed Method.....	45
5.1	Installing SmartTAP Database Server.....	47
5.1.1	Database Service Configuration.....	47

5.2	Installing SmartTAP Application Server	48
5.3	Installing SmartTAP Communication Server	49
5.3.1	Configure Windows SNMP Service	49
5.4	Installing SmartTAP Media Server	49
5.4.1	Media Server Configuration	50
5.4.1.1	Network File Server	50
5.4.1.2	Media Server	54
5.4.2	Configure Windows SNMP Service	55
5.5	Installing SmartTAP Call Delivery Server	56
5.5.1	Configure Windows SNMP Service	56
5.5.2	SmartTAP File Server Installation	57
5.5.2.1	Firewall Configuration	57
5.5.2.2	Domain Controller Configuration	57
6	Uninstalling SmartTAP	61
7	Firewall Configuration	63
7.1	Skype for Business Recording Firewall	63
7.1.1	Front End Server(s)	64
7.1.2	Edge, Mediation or Conference Server(s)	64
7.1.3	SmartTAP Server	65
7.1.4	SmartTAP Media Proxy Server	65
7.1.5	SmartTAP Announcement Server	66
7.1.6	Automated Firewall Exception Scripts for Windows Firewall	66
7.2	Distributed SmartTAP Firewall	67
7.2.1	Application Server (AS)	69
7.2.2	Communications Server (CS)	69
7.2.3	Database Server (DB)	69
7.2.4	File Server (FS)	69
7.2.5	Media Server (MS)	70
7.2.5.1	Remote Transfer Service (RTS)	70
7.2.6	Call Delivery(CD)	70
7.2.7	Media Delivery (MD)	71
7.2.8	Media Proxy (MP)	71
7.2.9	Announcement Server (AN)	71
7.2.9.1	Example	71
8	Integration Configuration	73
8.1	Microsoft Skype for Business	73
8.1.1	Installing Skype for Business Plugin	74
8.1.1.1	Pre-install Preparation	75
8.1.1.2	Install Procedure	85
8.1.1.3	Plugin Configuration	90
8.1.2	Installing Call Delivery for Skype for Business (IP-based Recording)	94
8.1.2.1	Monitoring	96
8.1.2.2	Edge	100
8.1.2.3	Configuring Media Proxy for Call Delivery-IP	101
8.1.2.4	Configuring Call Delivery for Skype for Business	104
8.1.3	Installing Media Proxy Server for Skype for Business	105
8.1.3.1	Editing Media Proxy Server Parameters	109
8.1.4	Installing Media Delivery Server for Skype for Business	109
8.1.5	Installing Announcement Server	110
8.1.5.1	Call Recording Notifications	110
8.1.5.2	Announcement Server Software Installation	117
8.1.5.3	Consent to Record Calls	120
8.1.6	Skype for Business Remote Branch Site	127
8.2	SIP Recording (SIPRec)	128

8.2.1	What is SIPRec?	128
8.2.2	Session Recording Server (SRS)	128
8.2.3	Session Recording Client (SRC)	128
8.2.4	Configuring Gateway & SBC for SIP Recording	129
8.2.5	Configuring Call Delivery for SIP Recording	130
8.3	VoIP Port Mirroring	131
8.3.1	Inbound / Outbound	131
8.3.2	Station to Station	132
8.3.3	Call Delivery Install for VoIP (Port Mirror)	133
8.3.4	Additional Configuration	135
8.3.5	Setting Up Monitoring Interfaces	136
8.4	Avaya AES Integration	137
8.5	Analog Trunk / Radio	137
8.5.1	Call Delivery Install for Analog Recording (Passive Tap)	138
8.5.2	Additional Configuration	140
8.5.2.1	Activity Detection	142
8.5.2.2	SmartCONTROL	143
9	Additional Configuration Options	145
9.1	Configuring Digital Signatures	145
9.1.1	Configuring the SmartTAP Web interface	145
9.1.1.1	Steps to Configure the PC Client	145
9.2	Configuring LDAP	146
9.2.1	Pre-Requisites	146
9.3	Configuring SSO	146
9.4	Configuring HTTP/S	146
9.4.1	Disabling HTTP Communications on Application Server (Optional)	146
9.4.1.1	Automatic	147
9.4.2	Configuring SmartTAP Components for HTTPS	148
9.4.2.1	Communication Server	148
9.4.2.2	Call Delivery	148
9.4.2.3	Media-Proxy	149
9.4.2.4	Announcement Server	149
9.4.2.5	Media Server and Remote Transfer Service	149
9.4.2.6	Health Monitor	150
9.5	Configuring Syslog Server Connection	150
9.6	Skype for Business Plug-in	150
9.7	Location-Based Targeting in SmartTAP	151
9.7.1	Assign a Location Attribute to each Call Delivery Component	151
9.7.2	Create a Location Attribute in the SmartTAP GUI	154
9.7.3	Assign a Location to Each User/Device in the SmartTAP GUI	155
9.7.4	Verify the Target List in Each Call Delivery	156
10	Backup and Restore	159
10.1	Prerequisites	159
10.2	Backup	160
10.2.1	Call Delivery Service	160
10.2.2	Media Service	160
10.2.3	Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server	161
10.2.4	Communication Service	161
10.2.5	Application Service	161
10.2.6	Database	161
10.2.7	SmartTAP Skype for Business Plug-in (FE, SBS, SBA)	162
10.2.8	SmartTAP Announcement Server	162

10.2.9	SmartTAP Media Proxy	162
10.2.9.1	Media	162
10.2.9.2	System Profile Tool	163
10.3	Restore.....	163
10.3.1	Call Delivery Service.....	164
10.3.2	Media Service	164
10.3.3	Media Delivery Service	164
10.3.4	Database	165
10.3.5	SmartTAP Skype for Business Plug-in (FE, SBS, SBA)	165
10.3.6	Announcement Server	165
10.3.7	Media Proxy.....	166
10.3.8	Media	166
11	Troubleshooting.....	167
11.1	How To Validate Port Mirror for Recording Skype for Business Calls	167
11.1.1	Prerequisites	167
11.1.1.1	Introduction: SmartTAP Recording Concepts	167
11.1.1.2	SmartTAP Processing of Skype for Business Signaling	167
11.1.1.3	SmartTAP Media Processing	168
11.1.2	Procedure	169
11.1.2.1	Setup Skype for Business Logging	169
11.1.2.2	Setup Sniffer.....	169
11.1.2.3	Capture a Test Call	170
11.1.3	Analysis.....	170
11.1.3.1	Locate Test Call in Skype for Business Log.....	170
11.1.3.2	Compare Call Information with Sniffer Trace	172
11.1.3.3	Determine Whether SmartTAP will Record this Call	172
11.2	Troubleshooting Skype for Business Plugin Installation	173
11.2.1	Enable the Browser Service	173
11.2.2	Use “net view” to verify	173
11.3	Troubleshoot Skype for Business Recording	174
11.3.1	No Records for the Calls.....	174
11.3.2	Calls with No Audio.....	174
11.3.3	Enabling Promiscuous Mode on VMWare ESXi.....	174
12	Known Issues	175
12.1	Internet Explorer Security Messages and SmartTAP not Running on Server.....	175

List of Figures

Figure 2-1: License Generator	19
Figure 2-2: SmartTAP Upgrades	21
Table 3-1: Package Contents (Root Folder).....	23
Figure 3-2: PowerShell Script Execution Policy	24
Figure 3-3: Add Features Wizard	25
Figure 3-4: SNMP Service.....	26
Figure 3-5: SNMP Service Properties	26
Figure 3-6: SNMP Service Properties - Security	27
Figure 3-7: SNMP Service Properties - Traps.....	28
Figure 3-8: SNMP Service Properties – Traps – Add Trap Destinations	28
Figure 4-1: Installation Wizard.....	31
Figure 4-2: Setup Type.....	32
Figure 4-3: Custom Setup	33
Figure 4-4: Database Server Installation Wizard.....	34
Figure 4-5: Application Server Installation Wizard	35
Figure 4-6: License Agreement	36
Figure 4-7: Application Information	36
Figure 4-8: Setup Type.....	37
Figure 4-9: Ready to Install	37
Figure 4-10: Complete Installation	38
Figure 4-11: Communication Server	39
Figure 4-12: Call Delivery Service.....	40
Figure 4-13: Select Network Type.....	41
Figure 4-14: Media Server.....	43
Figure 4-15: Media Server Configuration	43
Figure 4-16: InstallShield Wizard Completed	44
Figure 5-1: InstallShield Wizard SmartTAP	45
Figure 5-2: Setup Type.....	46
Figure 5-3: Custom Setup	46
Figure 5-4: Active Directory Users and Computers.....	50
Figure 5-5: New SmartTAP User.....	51
Figure 5-6: Password Never Expires.....	51
Figure 5-7: User Add Confirmation.....	52
Figure 5-8: Assign Read and Write Permissions	53
Figure 5-9: Add SmartTAP user to Administrators Group.....	54
Figure 5-10: Add Smart TAP User to Administrator	55
Figure 5-11: Assign User to SmartTAP MS-TR Service Account	55
Figure 5-12: Active Directory Users and Computers.....	57
Figure 5-13: New SmartTAP User.....	58
Figure 5-14: User Settings.....	58
Figure 5-15: User Add Confirmation.....	59
Figure 5-16: System Properties.....	59
Figure 5-17: System Properties.....	60
Figure 6-1: Program Maintenance - Remove.....	61
Figure 6-2: InstallShield Wizard Completed - Uninstall.....	62
Figure 7-1: Skype for Business Recording Firewall	63
Figure 7-2: Distributed SmartTAP Firewall.....	68
Figure 8-1: Capture Call Signaling - 1	73
Figure 8-2: Capture Call Signaling - 2	73
Figure 8-3: Active Directory Users and Computers.....	75
Figure 8-4: New SmartTAP User.....	76
Figure 8-5: Password Never Expires.....	76
Figure 8-6: User Add Confirmation.....	77
Figure 8-7: Add SmartTAP user to CSAdministrators group.....	77
Figure 8-8: Add Smart TAP User to CSAdministrator	78
Figure 8-9: Add Smart TAP User to RTCUniversalReadOnlyAdmins.....	78
Figure 8-10: Add SmartTAP user to the Administrators group.....	79

Figure 8-11: Administrators Properties.....	79
Figure 8-12: SmartTAP User Added to Administrators	80
Figure 8-13: RTCServerApplications.....	80
Figure 8-14: RTC Server Applications Properties	81
Figure 8-15: Add RTC Server Applications User	81
Figure 8-16: Local Security Policy.....	82
Figure 8-17: Log on as a service Properties	82
Figure 8-18: SmartTAP User.....	83
Figure 8-19: Start Menu.....	84
Figure 8-20: Windows Security.....	84
Figure 8-21: Windows PowerShell	85
Figure 8-22: Documents Library.....	86
Figure 8-23: Lync Plug-in Server.....	86
Figure 8-24: Software License Agreement.....	87
Figure 8-25: Browse for a User Account	87
Figure 8-26: Logon Information	88
Figure 8-27: Lync Plug-in Registrar Select.....	88
Figure 8-28: Media Proxy Server Configuration	89
Figure 8-29: Announcement Server Configuration.....	89
Figure 8-30: Setup Type.....	90
Figure 8-31: Call Delivery-IP	94
Figure 8-32: Network Type	95
Figure 8-33: Lync Configuration	95
Figure 8-34: Choose Recording Mode	96
Figure 8-35: Choose Media Tap Location	97
Figure 8-36: Interface Setup.....	97
Figure 8-37: Server IP Setup.....	98
Figure 8-38: Choose Media Tap Location	98
Figure 8-39: Media Delivery Configuration.....	99
Figure 8-40: Server IP Setup.....	99
Figure 8-41: Choose Recording Mode	100
Figure 8-42: Lync Edge Servers Configuration	100
Figure 8-43: Server IP Setup.....	101
Figure 8-44: Choose Recording Mode – Media Proxy	102
Figure 8-45: Media Proxy Configuration.....	102
Figure 8-46: Lync Edge Servers Configuration	103
Figure 8-47: Server IP Setup.....	103
Figure 8-48: Media Proxy Welcome	105
Figure 8-49: License Agreement.....	106
Figure 8-50: Choose Media Proxy IP Address	106
Figure 8-51: Choose Application Server IP Address.....	107
Figure 8-52: Choose Application Server IP Address.....	107
Figure 8-53: Media Proxy Setup Type.....	108
Figure 8-54: Media Proxy Install.....	108
Figure 8-55: Announcement Server Installation Wizard.....	111
Figure 8-56: License Agreement.....	111
Figure 8-57: Announcement Server	112
Figure 8-58: Choose Application Server IP Address.....	112
Figure 8-59: Application Server IP Address	113
Figure 8-60: Setup Type.....	113
Figure 8-61: Install.....	114
Figure 8-62: Skype for Business Server 2015 – Deploy	114
Figure 8-63: Install Administrative Tools	115
Figure 8-64: Install Status.....	115
Figure 8-65: Skype for Business Server – Deployment Wizard	116
Figure 8-66: Install Local Configuration Store	116
Figure 8-67: Executing Commands.....	117
Figure 8-68: Sound Recorder	118
Figure 8-69: AN Server.....	119
Figure 8-70: Skype for Business Remote Branch Site	127

Figure 8-71: Session Recording Client.....	128
Figure 8-72: Configure Gateway & SBC for SIP Recording.....	129
Figure 8-73: Server IP Setup.....	130
Figure 8-74: Inbound/Outbound	131
Figure 8-75: Station to Station.....	132
Figure 8-76: Call Delivery IP	133
Figure 8-77: Select Network Type.....	133
Figure 8-78: Server IP Setup.....	134
Figure 8-79: Interface Setup.....	134
Figure 8-80: Passive Tap Implementation.....	137
Figure 8-81: Figure 1 and Figure 2.....	138
Figure 8-82: Call Delivery LD	138
Figure 8-83: Server IP Setup.....	139
Figure 8-84: LD.xml Basic Structure Diagram.....	140
Figure 8-85: Activity Detection	142
Figure 8-86: Board Tab	143
Figure 9-1: Digital Signatures	145
Figure 9-2: Location Attribute for each Call Delivery Component.....	151
Figure 9-3: Skype and SIPREC Targets	152
Figure 9-4: Add User Attribute.....	154
Figure 9-5: Add User	155
Figure 9-6: SmartTAP LDAP Configuration page	156
Figure 10-1: Board Tab Configuration.....	159
Figure 10-2: Add Recording Location.....	163
Figure 10-3: Add Recording Location.....	166
Figure 11-1: AudioCodes Software Plugin	168
Figure 11-2: SmartTAP Media Processing.....	168
Figure 11-3: Skype for Business Logging	169
Figure 11-4: Sniffer Trace.....	172
Figure 12-1: Enhanced Security Configuration	175

List of Tables

Table 1-1: SmartTAP Server	13
Table 1-2: License Factors	14
Table 1-3: Add-On Blades	16
Table 1-4: Power Requirements.....	16
Table 1-5: HTML5 Media Player Browser Support	18
Table 7-1: Front End Server(s) - Inbound Firewall.....	64
Table 7-2: Front End Server(s) - Outbound Firewall	64
Table 7-3: Edge, Mediation or Conference Server(s) - Inbound Firewall.....	64
Table 7-4: Edge, Mediation or Conference Server(s) - Outbound Firewall.....	64
Table 7-5: SmartTAP Server - INBOUND Firewall.....	65
Table 7-6: SmartTAP Server - Outbound Firewall.....	65
Table 7-7: SmartTAP Media Proxy Server - Inbound Firewall	65
Table 7-8: SmartTAP Media Proxy Server - Outbound Firewall	65
Table 7-9: SmartTAP Announcement Server- Inbound Firewall	66
Table 7-10: SmartTAP Announcement Server - Outbound Firewall	66
Table 7-11: Firewall - Application Server (AS)	69
Table 7-12: Firewall - Communications Server (CS).....	69
Table 7-13: Firewall - Database Server (DB)	69
Table 7-14: Firewall - File Server (FS)	69
Table 7-15: Firewall - Media Server (MS)	70
Table 7-16: Remote Transfer Service (RTS).....	70
Table 7-17: Firewall - Call Delivery(CD).....	70
Table 7-18: Firewall - Media Delivery (MD).....	71
Table 7-19: Firewall - Media Proxy (MP).....	71
Table 7-20: Firewall - Announcement Server (AN)	71
Table 8-1: Plugin Configuration Options	90
Table 8-2: Description of the Skype for Business Specific Changes	104
Table 8-3: System.config File	121
Table 8-4: SIP Recording – Additional Configuration Files	131
Table 8-5: Description of the Avaya H.323 Specific Changes	135
Table 8-6: Description of the SIP Recording Specific Changes	135
Table 8-7: Most Common Values to be Adjusted per Board or Channel	141
Table 10-1: Backup - Call Delivery Service.....	160
Table 10-2: Backup - Media Service	160
Table 10-3: Backup - Media Delivery Service	161
Table 10-4: Backup - Communication Service	161
Table 10-5: Backup - Application Service	161
Table 10-6: Backup - Database.....	161
Table 10-7: SmartTAP Skype for Business Plug-in (FE, SBS, SBA).....	162
Table 10-8: Backup - SmartTAP Announcement Server	162
Table 10-9: Backup - SmartTAP Media Proxy	162
Table 10-10: System Profile Tool	163
Table 10-11: Restore – Call Delivery Service	164
Table 10-12: Restore – Media Service.....	164
Table 10-13: Restore – Media Delivery Service.....	164
Table 10-14: Restore – Database	165
Table 10-15: Restore – SmartTAP Skype for Business Plug-in (FE, SBS, SBA)	165
Table 10-16: Restore – Announcement Server.....	165
Table 10-17: Restore – Media Proxy.....	166

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-26-2018

WEEE EU Directive

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

Customer Support

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

Email: support@audiocodes.com

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

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

International Number: +800 444 22 444

APAC: +65-6493-6690



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

Abbreviations and Terminology

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

Related Documentation

Document Name
SmartTAP Release Notes
SmartTAP Administrator Guide

Document Revision Record

LTRT	Description
27180	Initial document release for Version 3.2.0.
27181	Note update in Call Delivery Service section.
27182	Sections Updated: Disabling HTTP Communication, Call Recording Notifications (Prerequisites), Activating Announcement Services (Note).
27183	Sections Updated: Minimum System Requirements; Installation Wizard procedures and general enhancements to related chapters; Call Recording Notifications (Prerequisites), Activating Announcement Services (Note), Call Recording Notifications, Skype for Business Recording; Firewall Configuration; Microsoft Skype for Business integration; Configuring SSO, Disabling HTTP Communication. Removal of support for Avaya AES Integration and Digital Station Side.
27185	Sections updated: HTML5 Media Player support table; Minimum Server Requirements. Several screens updated with new AudioCodes logo. Sections added: Network Adapter Configuration Sections removed: Configuring SSO (except for Introduction: this subject is documented in the Administrators Guide).
27187	Sections updated: Supported Operating Systems; Microsoft Hyper-V; Installation Prerequisites for PowerShell permissions; Plugin configuration for Microsoft Skype for Business; Editing Media Proxy Server Parameters; Enabling Consent to Record Calls Demo.
27188	Updates to hardware and software requirements; SmartTAP License Management; Configure Microsoft SNMP Service; Firewall configuration; Configuring HTTP/S; Location-based targeting.

Documentation Feedback

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

1 Hardware and Software Requirements

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



Note: Microsoft rebranded *Lync* as *Skype for Business* so when the term *Skype for Business* appears in this document, it also applies to Microsoft Lync.

1.1 Minimum System Requirements

1.1.1 Server Configurations

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

Table 1-1: SmartTAP Server

Server	Specification	Available Resources
SmartTAP server (Low Profile)	Win 2012 R2 64bit 2 Core 2.5 GHz 6 GB Memory 2 SATA 7200 RPM HDD* Dual Gb NIC PCIe slots FL / FH2**	50 resources (audio only)
		25 resources when Media Proxy Service is installed on the same server (audio only)
SmartTAP server (Medium Profile)	Win 2012 R2 64bit 6 Cores 2 GHz**** 8 GB Memory 2 SATA 7200 RPM HDD* Dual Gb NIC PCIe slots FL / FH2**	150 resources
		50 resources when Media Proxy Service is installed on the same server (audio only)
SmartTAP server*** (High Profile)	Win 2012 R2 64bit 12 Core 2 GHz**** 14 GB Memory 2 SATA 7200 RPM HDD* Dual Gb NIC PCIe slots FL / FH2** For network adapter configuration, see Section 1.2	300 resources
Media Proxy server***	Win 2012 R2 64bit Quad Core 2 GHz 8 GB Memory SATA 7200 RPM HDD Dual Gb NIC For network adapter configuration, see Section 1.2	300 resources

Server	Specification	Available Resources
Announcement server***	Win 2012 R2 64bit Quad Core 2 GHz 8 GB Memory SATA 7200 RPM HDD Dual Gb NIC	300 resources (assuming the announcement length does not exceed 20% of an average call length)

* SmartTAP server requires two dedicated HDDs - one for the Windows OS, SmartTAP 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 Server in a virtual environment, the HDDs has to be dedicated and mapped to SmartTAP 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 3 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.



Note: When running in a virtual environment, all specification resources in Table 1-1 must be reserved for all servers of SmartTAP.

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.

Table 1-2: License Factors

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

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

$$\text{Required Number of Resources} = (\text{Number of Audio Recorder Licenses}) * (\text{Audio Recorder License Factor}) + (\text{Number of Video Recorder Licenses}) * (\text{Video Recorder License Factor}) + (\text{Number of Desktop Sharing Recorder Licenses}) * (\text{Desktop Sharing Factor})$$

Choose the SmartTAP 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:

$$\text{Required Number of Resources} = (\text{Number of Announcement Licenses}) * (\text{Announcement License Factor})$$

Example 1: 100 Audio Recorder Licenses

- Required Number of Resources = (100 Audio Recorder Licenses)*(1 Audio Recorder License Factor) = 100
- Choose Medium Profile SmartTAP 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 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 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 server with Media Proxy service installed on the SmartTAP server
 - Low Profile SmartTAP server and separate Media Proxy server

Example 5: 200 Audio Recorder Licenses with Announcement

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

1.2 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** and **MediaProxy** servers must be implemented.

1.2.1 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>

1.2.2 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>

1.3 Telephony Integration Hardware

1.3.1 Add-On Blades

Table 1-3: Add-On Blades

Interface	Description	Connector	Gender
Analog	24 channel PCIe Full Length Full Height Card <ul style="list-style-type: none"> ▪ 6' 180 degree Male to 90 degree female cable included 	RJ21x	Female

- 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.

1.3.2 Power Requirements

Table 1-4: Power Requirements

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.

1.4 Antivirus Software

- No virus software is included with SmartTAP
- 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\\

1.5 Windows Defender

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

1.6 Supported Operating Systems

- Windows Server 2016
- Windows 2012 Server 64bit
- Windows 2008 Server 64bit SP2

1.7 Windows Updates

- Recommend to disable to prevent unknown side effects.
- AudioCodes only certifies major Service Pack updates

1.7.1 Installing Windows Updates

- Schedule a maintenance window. ST will not be recording 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.
- Once the Windows updates are complete, reboot the server again.

1.8 Supported Virtual Machine (VM) Environments

1.8.1 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 system that is monitoring (tapping) the network.

1.8.2 Microsoft Hyper-V

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012 64bit
- Windows Server 2008 R2 SP1 or latest service pack
- Windows Server 2008 R2
- Windows Server 2008 64bit SP2



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

1.9 Active / Standby Resiliency Configuration (Optional)

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

- Two identical Windows 2008 R2 or 2012 servers, which meet the minimum specifications mentioned above
- A SAN (Storage Area Network) with iSCSI support. The SmartTAP 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 should not be configured to write the media directly to the 3rd media target; instead, it should be set as Media Transfer Service destination.

1.10 HTML5 Media Player Browser Support

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

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

Table 1-5: HTML5 Media Player Browser Support

SmartTAP 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 MP3 or WebM with VP8 and Opus support, Web Audio API, Readable streams



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

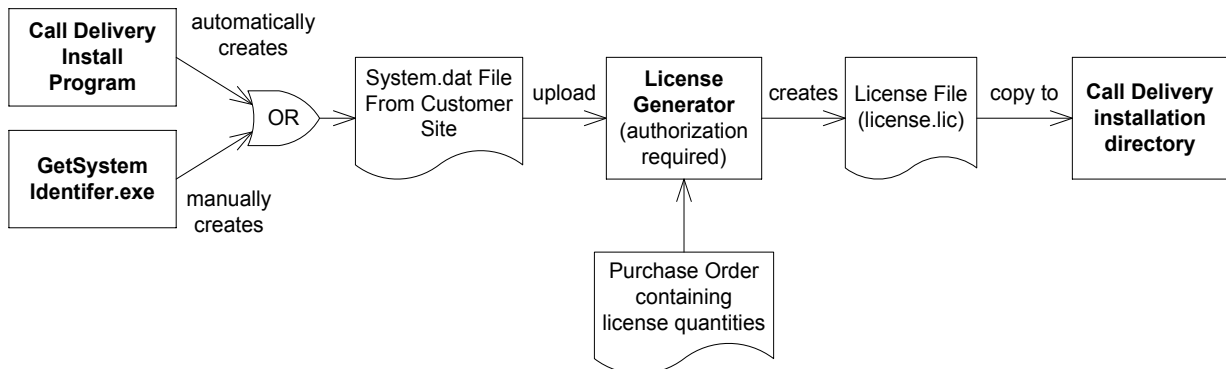
2 SmartTAP License Management

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

2.1 License File Creation and Installation

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

Figure 2-1: License Generator



2.1.1 License File Creation

Two SmartTAP 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\CD-xx
```

where xx represents which type of Call Delivery is installed.



Note: 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 “GetSystemIdentifier.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 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.

2.1.2 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\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.



Note: 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 Administrator Guide. The “Licenses” page under the “System” tab in the SmartTAP 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.

2.1.3 SmartTAP Upgrades

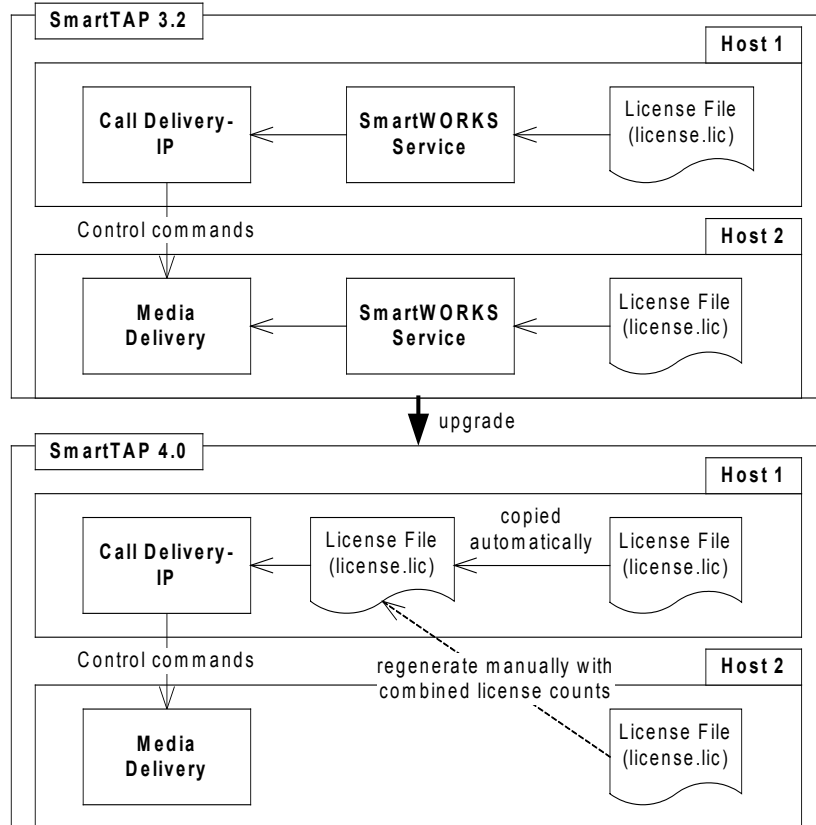
In general, SmartTAP components are designed to be backward compatible regarding license files. Therefore, when performing an upgrade from one SmartTAP version to another, it is generally not necessary to make any licensing changes with the following exceptions:

- 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 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 4.0 and higher are ignored.

A special case occurs if the upgrade involves a SmartTAP solution that includes Media Delivery from a version prior to version 4.0. Before SmartTAP 4.0, Media Delivery relied on SmartWORKS Service, which required a license file. Beginning with SmartTAP 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 Upgrades



For upgrades of CD-SIPREC prior to SmartTAP 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.

This page is intentionally left blank.

3 Before Installing SmartTAP

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

3.1 SmartTAP Software Package Contents

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

Table 3-1: Package Contents (Root Folder)

Contents	Description
Microsoft Lync and Skype for Business	Includes Microsoft Lync 2010, 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 installation package folder
Tools	Contains various utilities for installing and troubleshooting SmartTAP
SmartTAP Developer's Guide.pdf	Describes the REST API development interface for SmartTAP.
SmartTAP Release Notes.pdf	Describes the new features, issues resolved and any known issues for the SmartTAP software release.
SmartTAP InstallationGuide.pdf	Defines the Installation setup for the SmartTAP software.

3.2 Installation Prerequisites

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

- Base Windows 64 bit operating system installation complete without any additional software or features enabled
- Specific SmartTAP hardware must be plugged into the server
- “Optional” PCI cards for Analog Station recording
- Specific SmartTAP 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 (for more information, see Section 3.2.1 below).
- Ensure that the Windows PowerShell script execution policy is set as follows on all of the servers where SmartTAP 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:

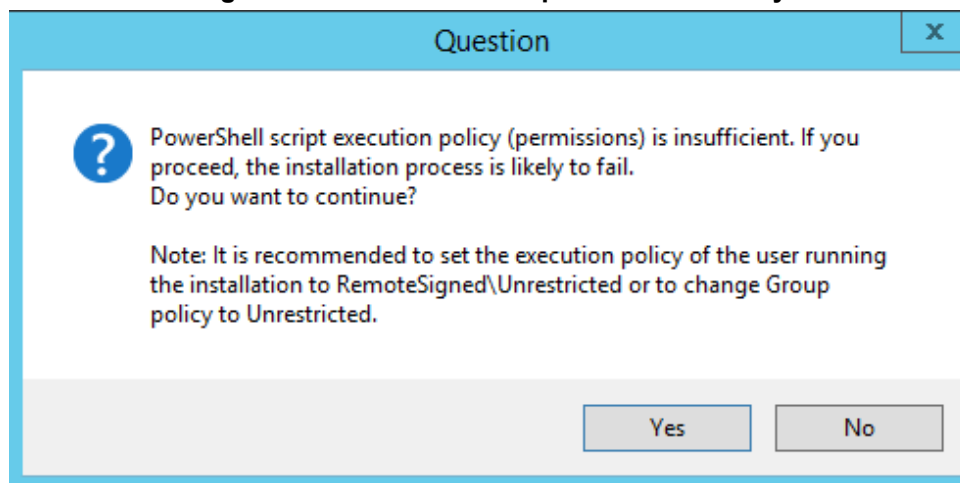
```
PS> Set-ExecutionPolicy -scope CurrentUser Unrestricted
```

```
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.

3.2.1 Configure Microsoft SNMP Service

The SmartTAP system requires the installation of the Microsoft SNMP agent for configuration and alarms. All Windows servers that are part of a SmartTAP installation must have the SNMP feature enabled and configured. This service must be configured on the following servers:

- SmartTAP Communication Server Installation
- SmartTAP Media Server Installation
- SmartTAP Call Delivery Server Installation



Note:

- SNMP Trap Service must be disabled on SmartTAP servers running the Application Server component.
- For each SmartTAP 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 4.4).

You can install Microsoft SNMP Agent using one of the following methods:

- Automatic
- Manual

3.2.1.1 Automatic SNMP Setup

Starting from SmartTAP 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 3.2.1.

By default, the installer is located within the install package as is not installed to the local drive with the SmartTAP installer.

➤ **Do the following:**

1. In your SmartTAP distribution directory, locate the following file in either of the following locations:
 - .\Program Files\AUDIOCODES\SmartTap\Install\EnableSNMPOnServer.bat
 - ..\installation suite\tools\EnableSNMPOnServer.bat
2. Right-click and choose "Run as administrator".

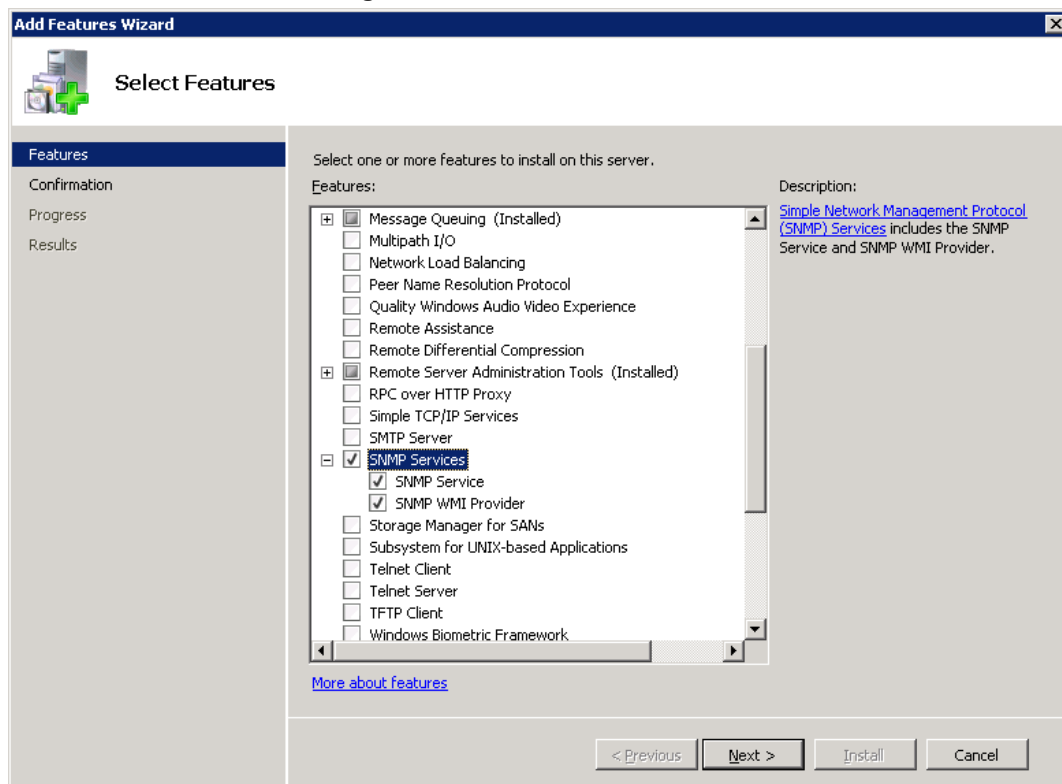
3.2.1.2 Manual SNMP Setup

The procedure below describes how to install the SNMP Server feature.

➤ **Do the following:**

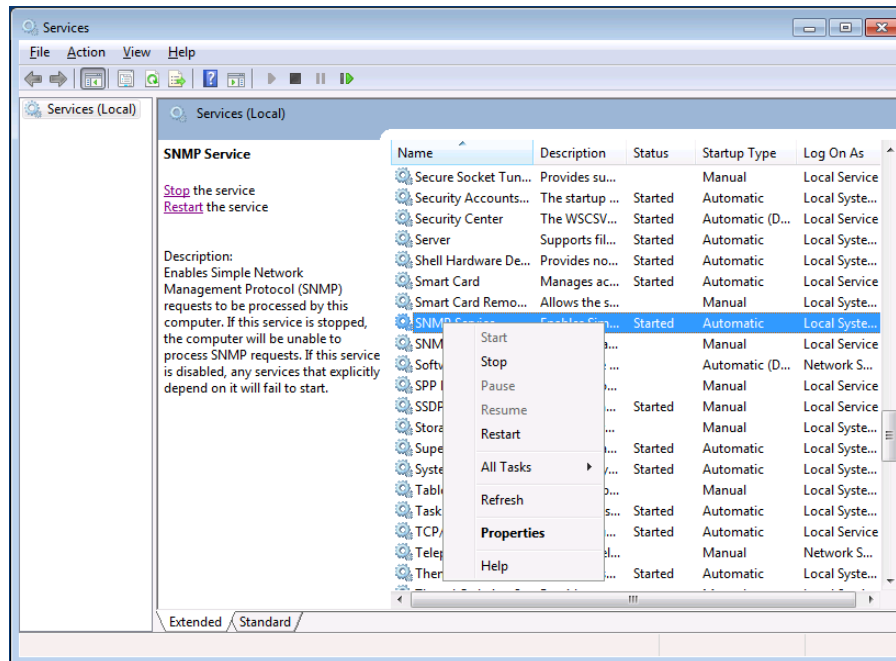
1. Open **Turn on Windows features on or off (Control Panel > Programs and Features > Turn on Windows features on or off)**.
2. Click **Features**, and click **Add Features**.
3. Select **SNMP Services**.

Figure 3-3: Add Features Wizard



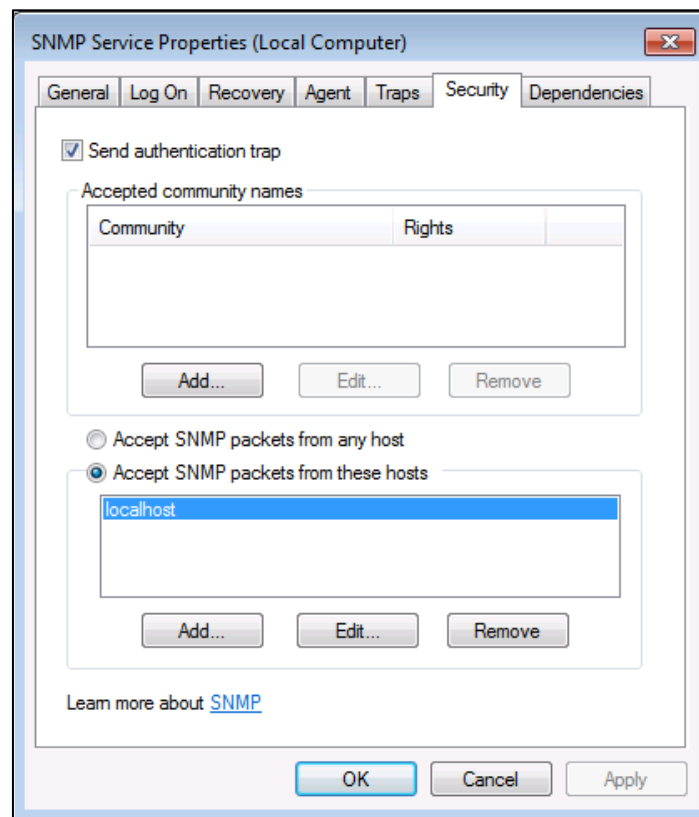
4. Open **Services** (**Start** > **Run...** > **services.msc**).
5. Right click over the **SNMP Service** listing.

Figure 3-4: SNMP Service



6. Select **Properties** > **Security**; the following screen appears:

Figure 3-5: SNMP Service Properties

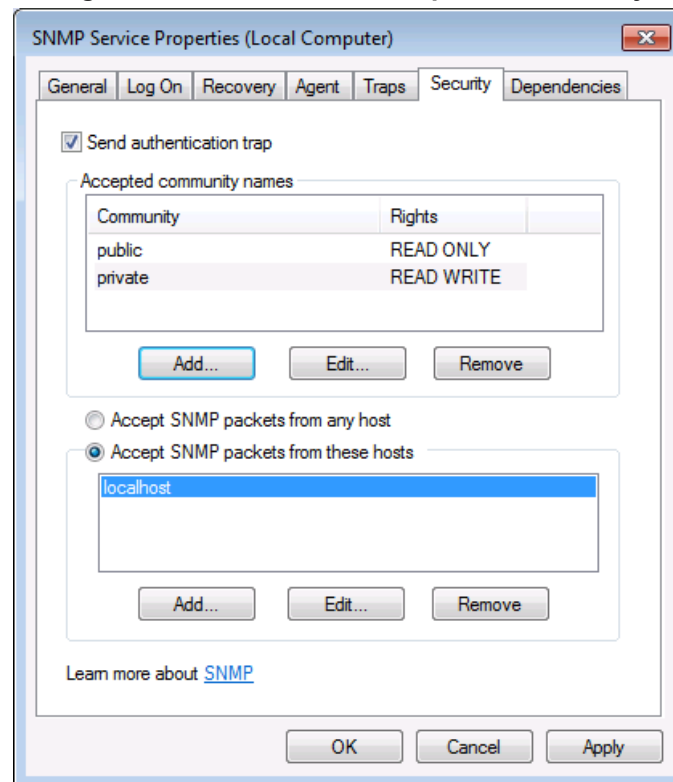


7. In the **Accepted community names** window, add the following:
 - public Community with READ ONLY rights
 - private Community with READ WRITE rights



Note: The community names must be in lower case.

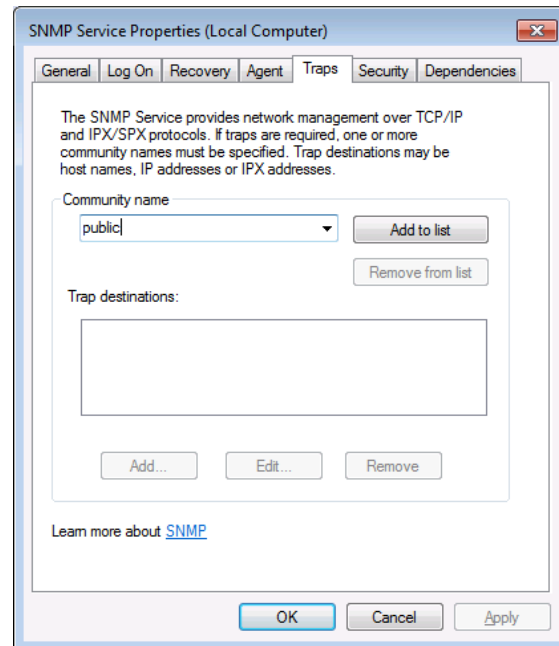
Figure 3-6: SNMP Service Properties - Security



8. In the **Accept SNMP packets from these hosts** window, click **Add...** to add the following:
 - If this is a standalone SmartTAP server, leave **localhost** as the only entry
 - If this is for a SmartTAP 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**.

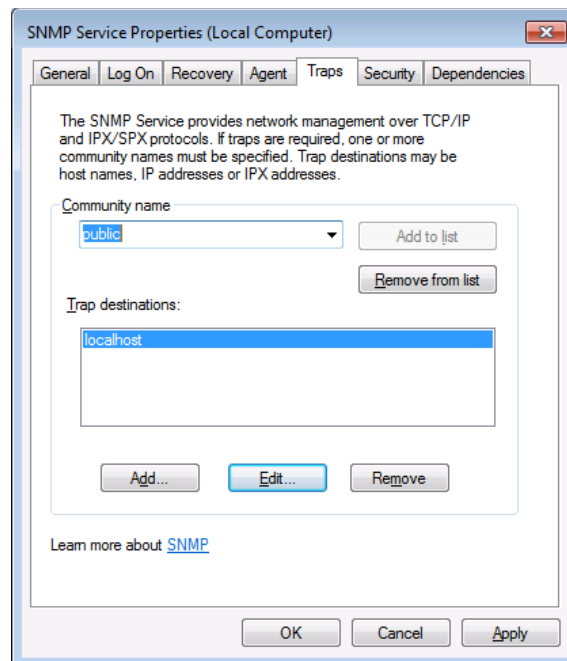
12. Click **Add to list**.

Figure 3-7: 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 installation that involves more than one server add the IP address of the Application Server (AS) instead

Figure 3-8: SNMP Service Properties – Traps – Add Trap Destinations



14. Click **OK**.

3.3 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 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

3.3.1 All-In-One

This method installs the following default SmartTAP components in a single Wizard process, including recording and integration components. For more information, proceed to Chapter 4 (recording components and Chapter 8 (integration components).

3.3.2 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 RDD)
- If you need to install SmartTAP Media Proxy or Announcement Server for Skype for Business.
- If some SmartTAP elements will reside on different servers.
- If you are installing Analog Station Integration.
- If you are installing SIPRec.



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

Proceed to Chapter 5.

3.4 Post Installation Actions

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

- **Configure Firewall rules:** The deployment of the SmartTAP 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 7.
- **Integrate SmartTAP with other network components:**
 - Skype for Business (see Section 8.1)
 - SIPRec (see Section 8.2)
 - Analog trunk/radio (see Section 8.5)
- **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 Section 8.3)
- **Additional Configuration options:**
 - Configuration Digital Signatures (see Section 9.1)
 - Configuring LDAP (see Section 9.2)
 - Configuring SSO (see Section 9.3)
 - Configuring HTTP/S (see Section 9.4)
- 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 ps1 and runs each one of them in alphabetical order.

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 installation on a single server.

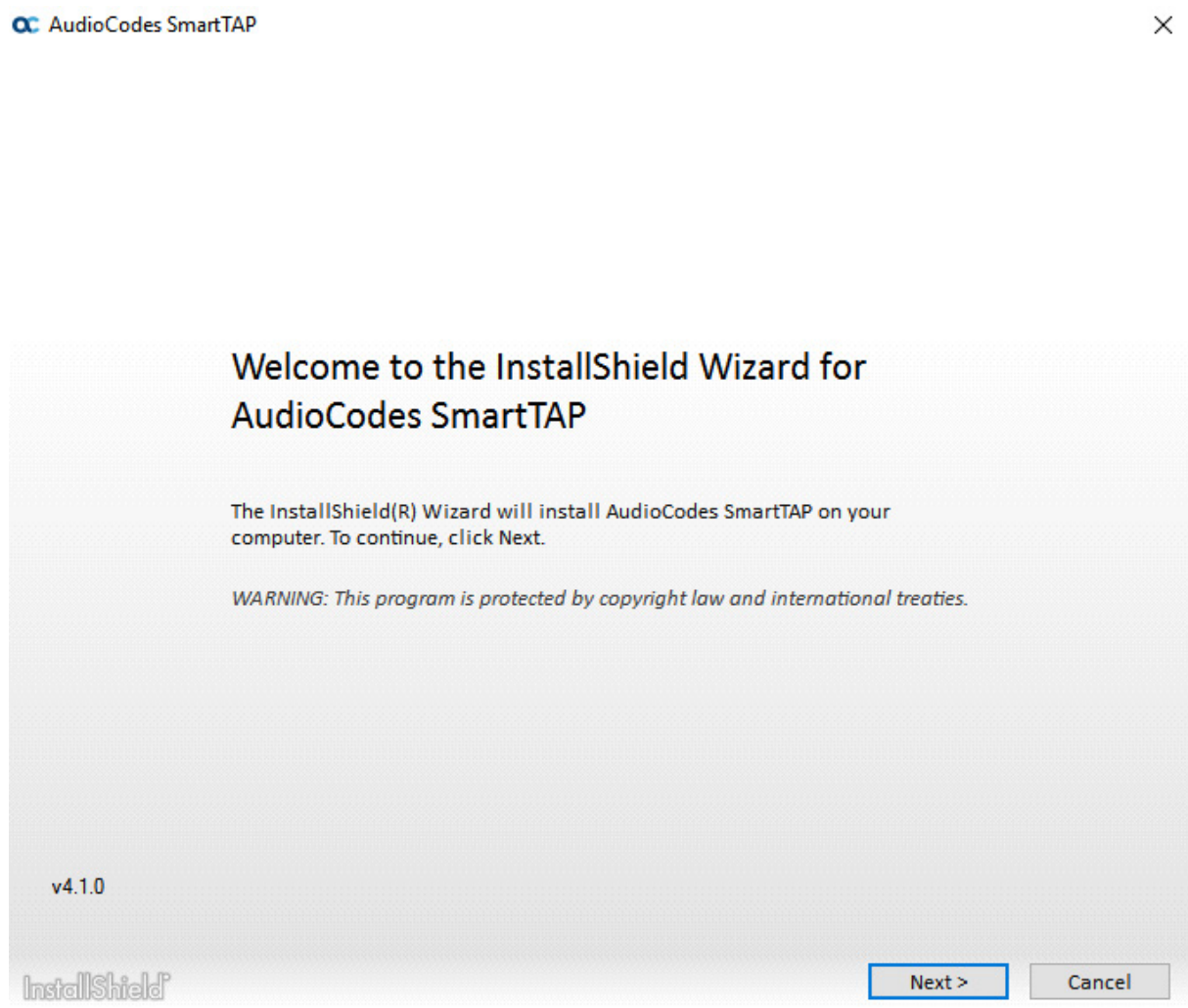


Note: Refer to the Chapter 5 for installations that involve more than one SmartTAP server.

➤ **To install SmartTAP:**

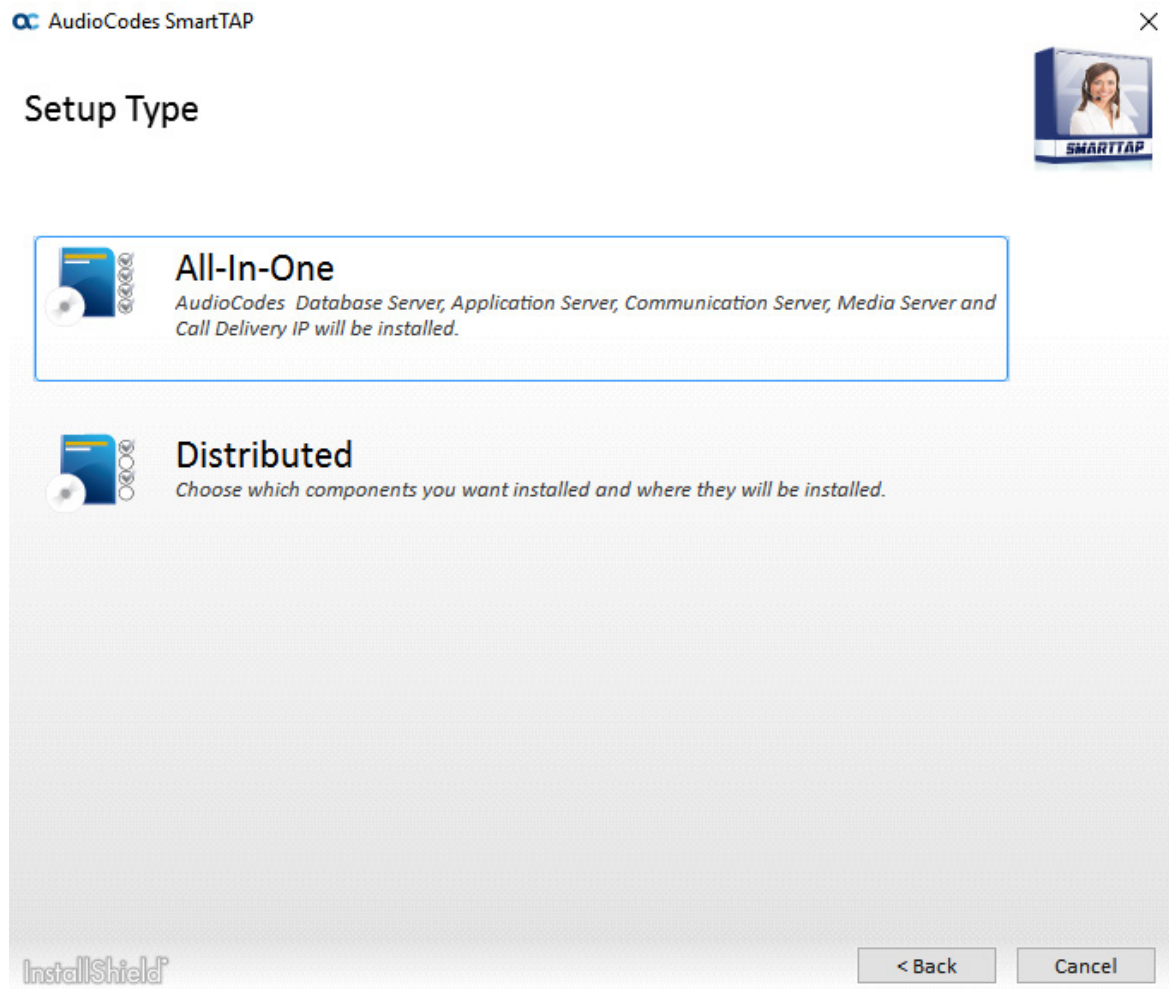
1. Verify all prerequisites for the installation are met before moving forward with the installation.
2. Launch **install.bat** from the “Suite” folder.
3. Click **Next** to continue.

Figure 4-1: Installation Wizard



4. Click **Next** after accepting SmartWORKS license.
5. Click **Next** after accepting SmartTAP license.

Figure 4-2: Setup Type



6. Select **All-In-One**:

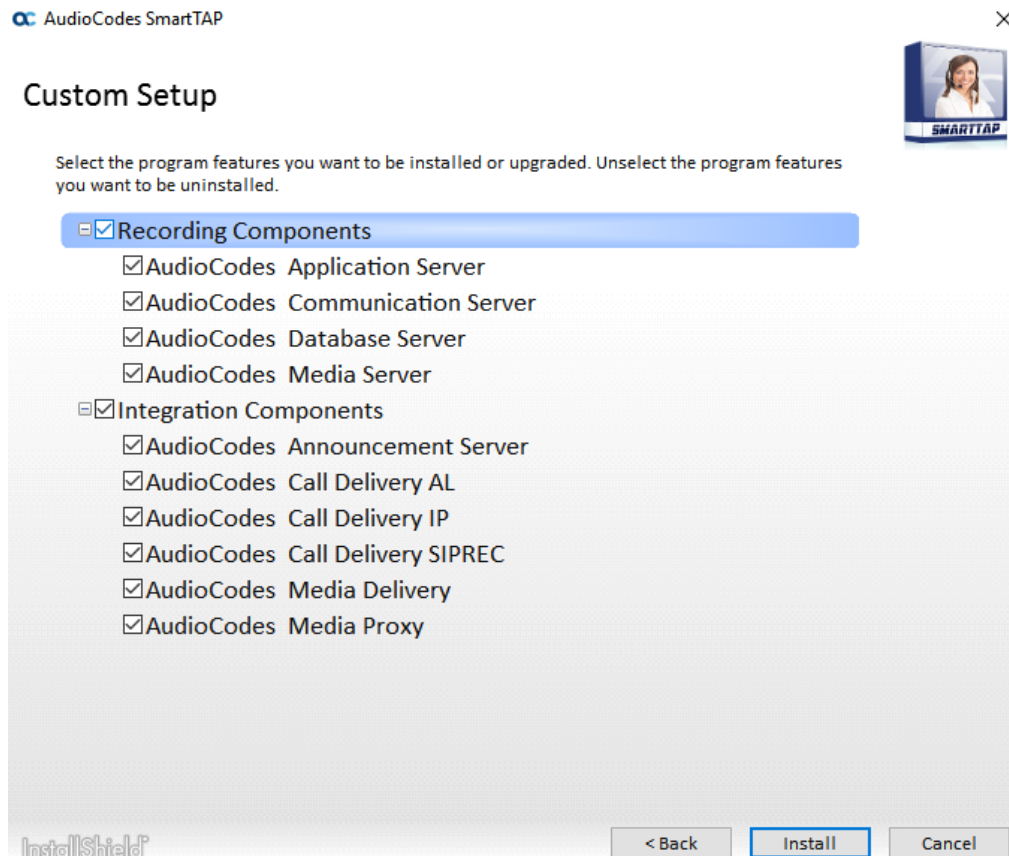
Refer to the following sections:

- Installing Database Service (see Section 4.1)
- Installing Application Server (AS) (see Section 4.2)
- Installing Communication Server (CS) (see Section 4.3)
- Installing Media Server (MS) (see Section 4.3)
- Installing Call Delivery-IP (CD-IP) (see Section 4.4)



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

Figure 4-3: Custom Setup



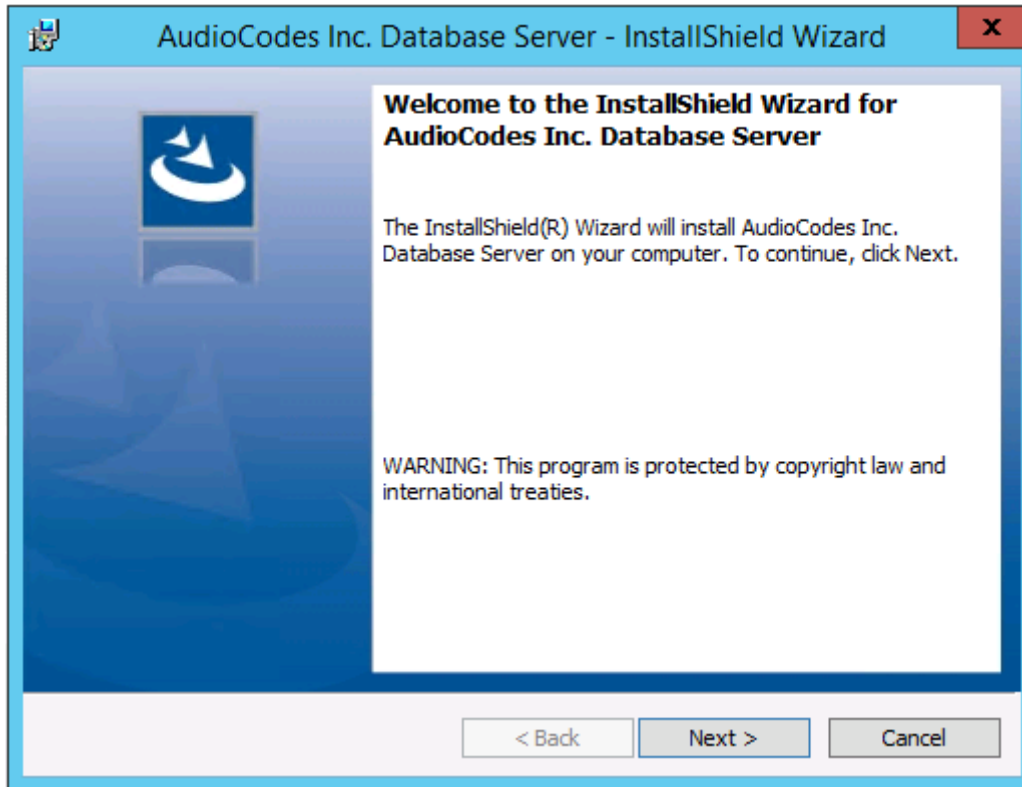
4.1 Database Service

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.

Figure 4-4: Database Server Installation Wizard



2. Accept ALL defaults.
3. Click **Install**.
4. Click **Finish**.



Notes:

- For setting up clustered configurations of the database, please contact AudioCodes Technical Support for further information.
- When upgrading from SmartTAP 1.8.x through SmartTAP 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\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.

4.2 Installing the Application Service

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



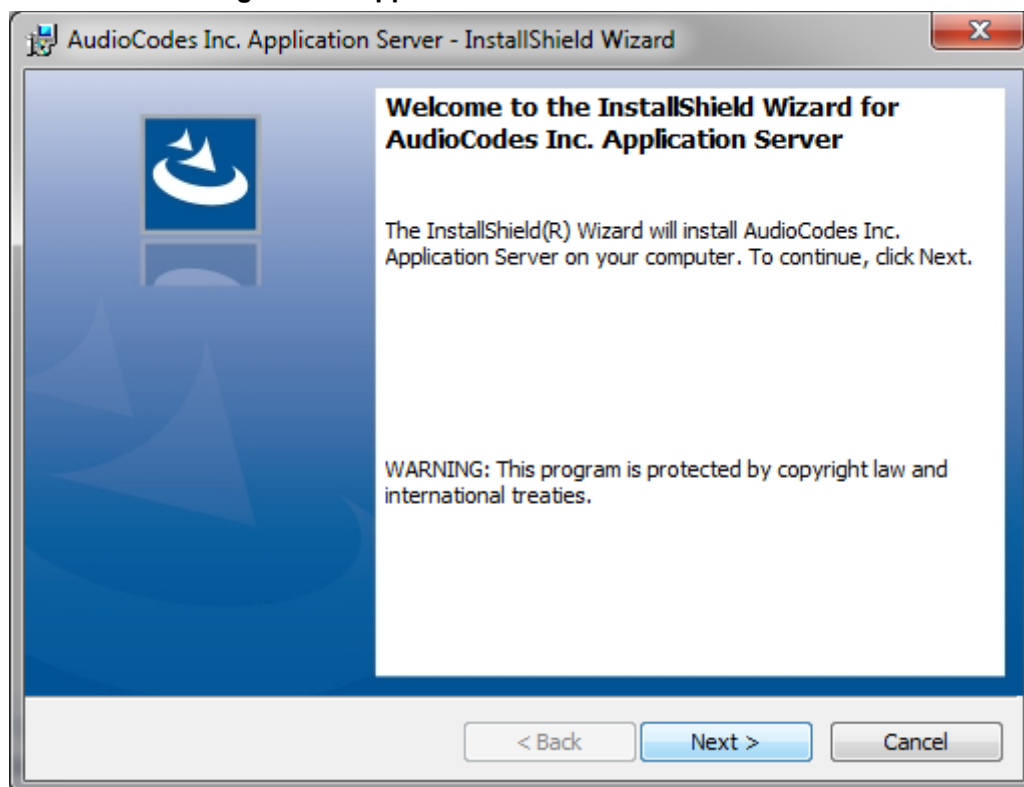
Note:

- The database must be installed first before continuing.
- This procedure also runs a silent installation of the Health Monitor utility. For more information, refer to the *Administrator Guide*.

➤ **To install the Application service:**

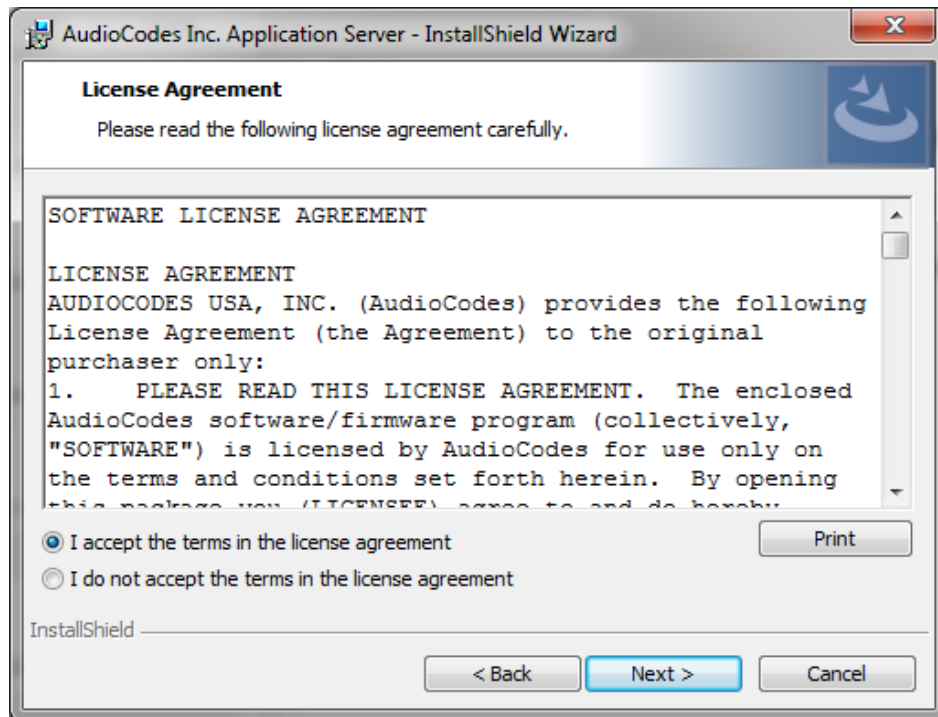
1. The Application Service installation starts in the proper sequence when all or multiple services are selected on the installer menu.
2. When the Application Server installation wizard starts, click **Next** to install.

Figure 4-5: Application Server Installation Wizard



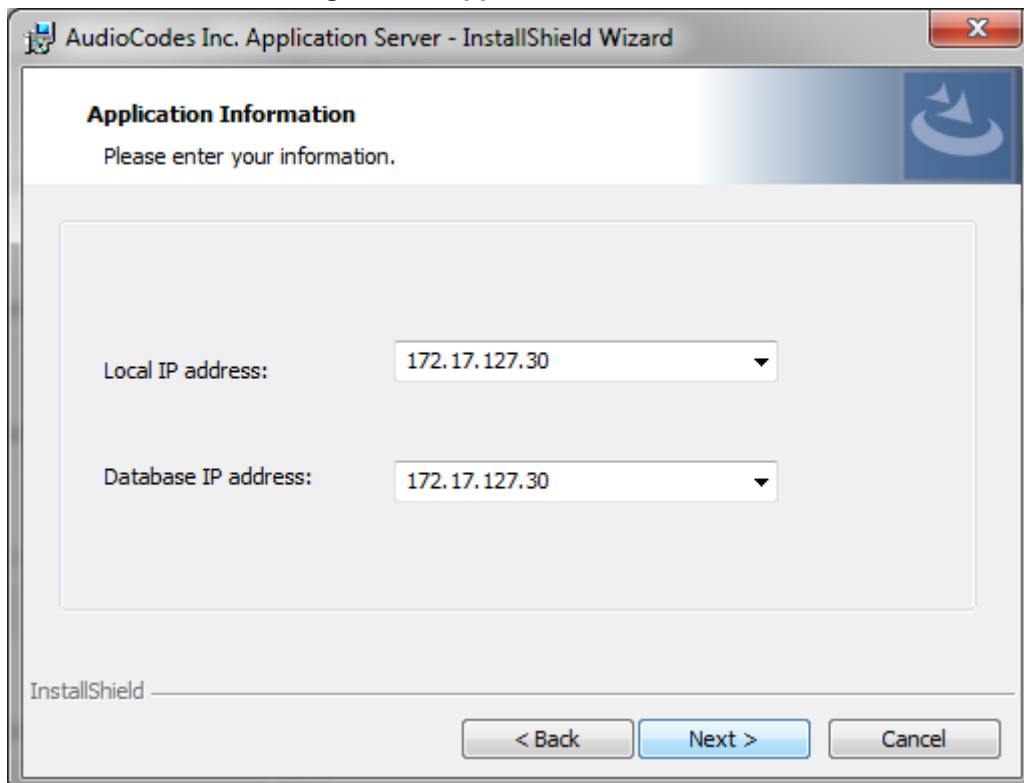
If you are installing from a Suite, then the following screen may not be displayed.

Figure 4-6: License Agreement



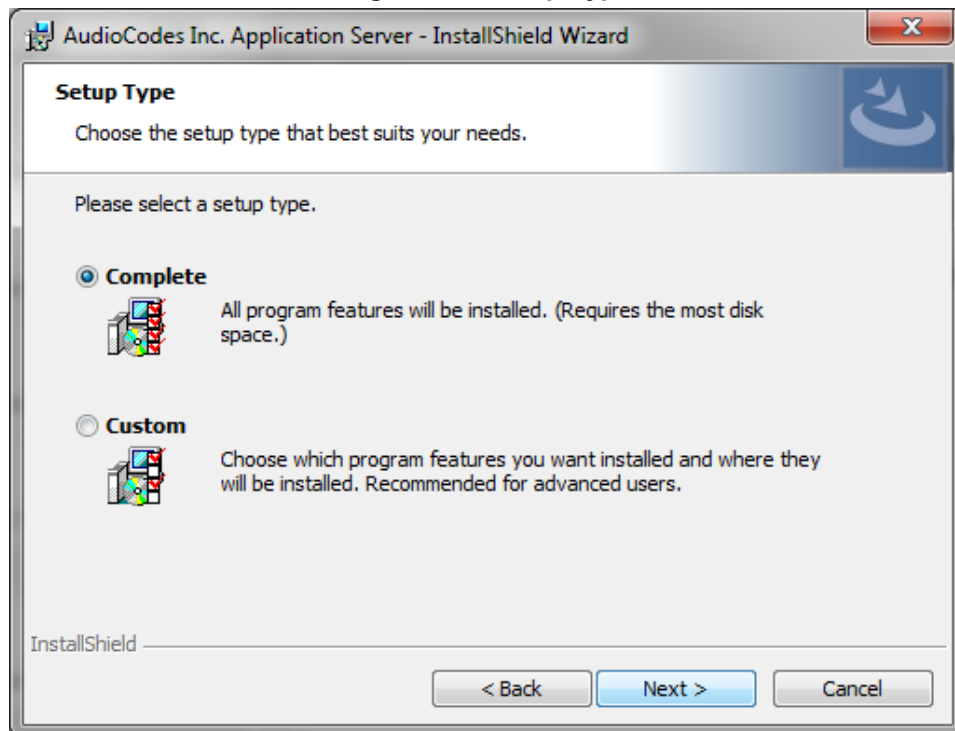
3. Select the “I accept the terms in the license agreement” check box and click **Next**.
If you are performing an upgrade, the screen below is not displayed.

Figure 4-7: Application Information



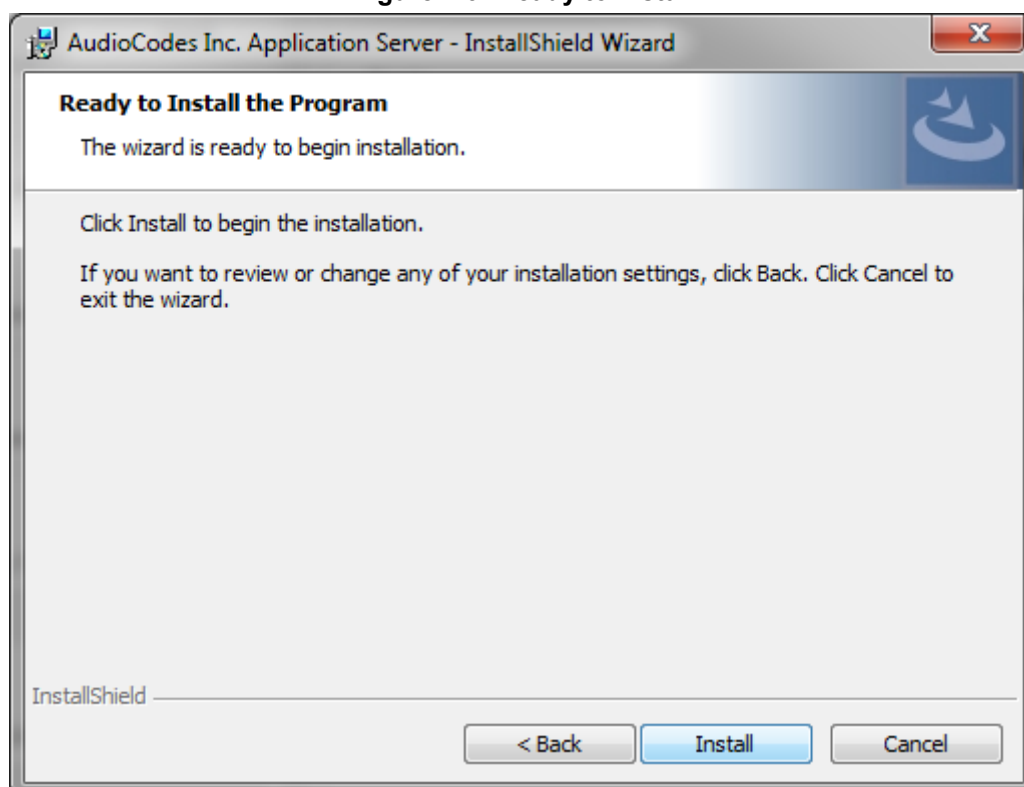
4. Enter the IP address of the Application Server location and the IP address of the Database location. The IP addresses should be external i.e. not the IP address of the local host. Click **Next** to proceed.

Figure 4-8: Setup Type



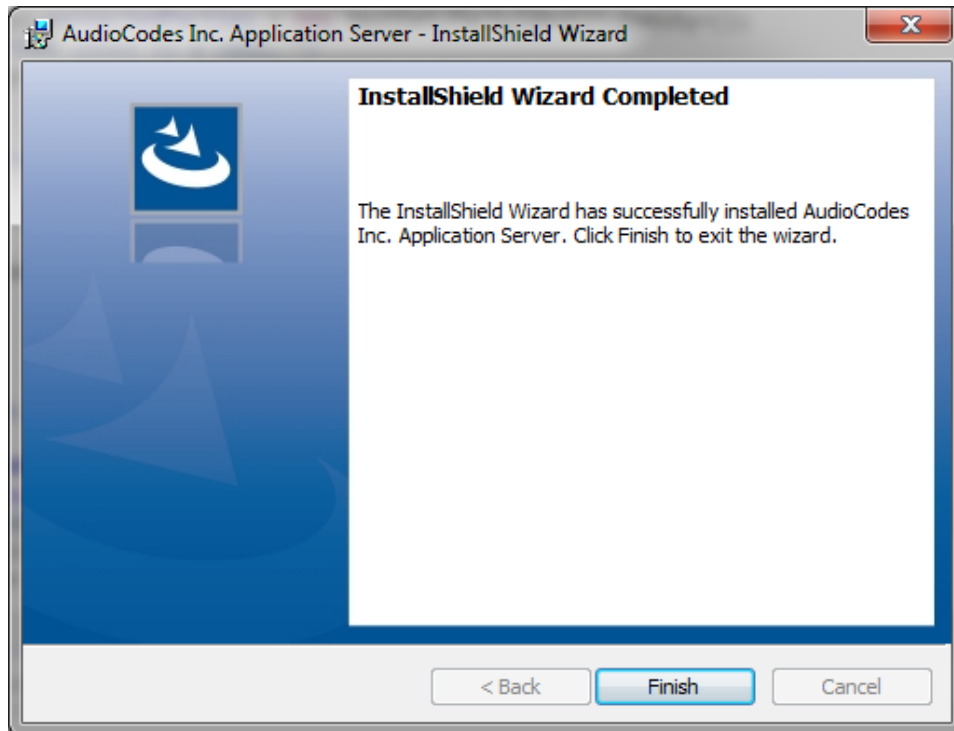
5. Select one of the following setup types and click **Next**:
 - **Complete:** Install to the default location: C:\Program Files\AudioCodes\SmartTAP\AS
 - **Custom:** Change the destination location

Figure 4-9: Ready to Install



6. Click **Install**.

Figure 4-10: Complete Installation



7. Click **Finish**.

4.3 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.

➤ 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 4-11: Communication Server



4. Accept ALL defaults.
5. If you are upgrading, you are prompted to enter the IP address of the Application server.
6. Click **Install**.
7. Click **Finish**.

4.4 Installing the Call Delivery Service

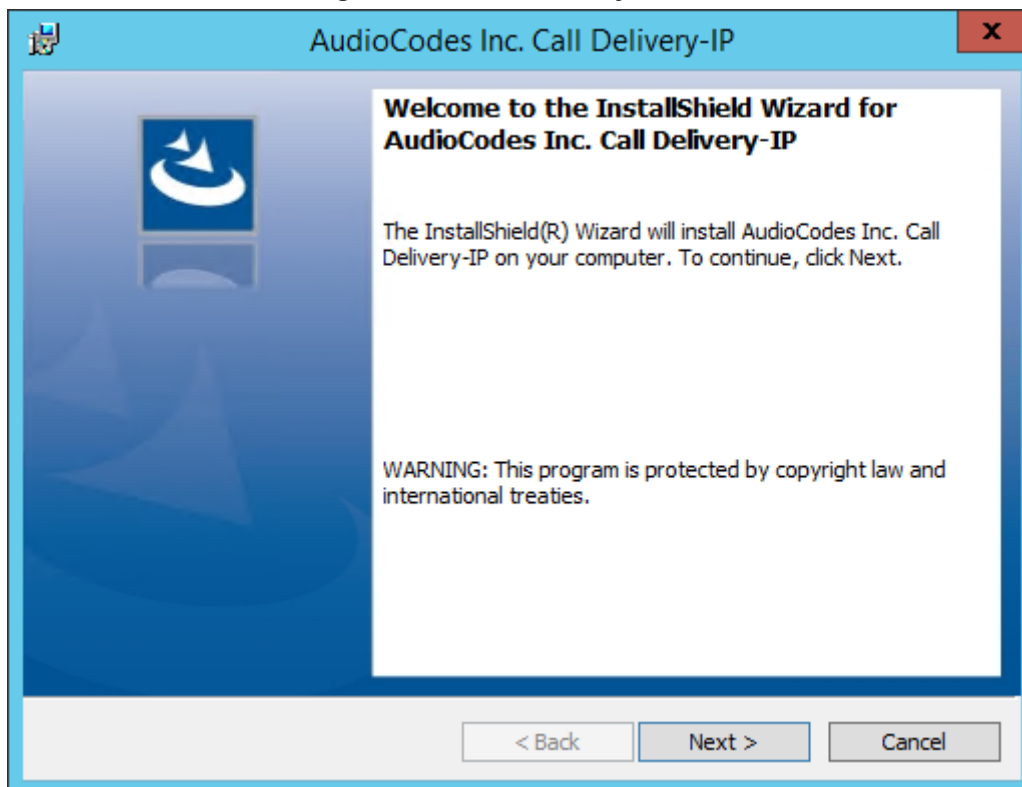
The Call Delivery is responsible for passively tapping or actively connecting to the telephony environment and then determining which calls to record using the dynamic state machine and target list. A separate Call Delivery Service will be installed for each telephony environment.

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

➤ **To install the Call Delivery Service:**

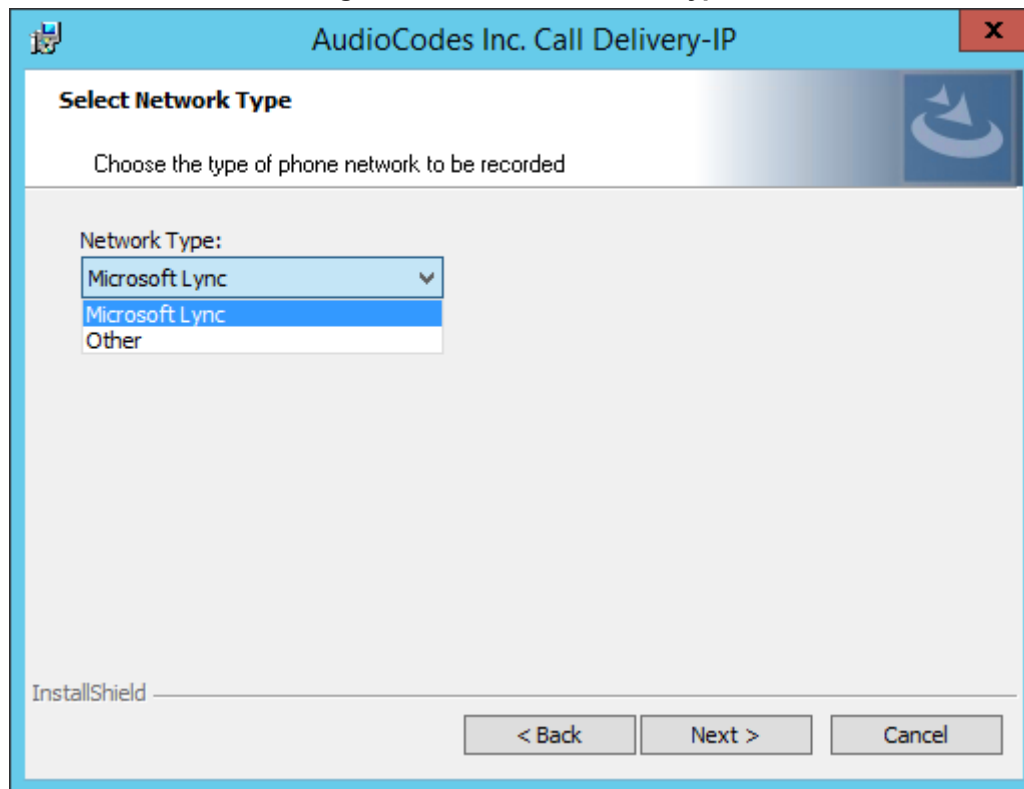
1. When the Call Delivery Service installation wizard starts click **Next** to install.

Figure 4-12: Call Delivery Service



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

Figure 4-13: Select Network Type



3. Click **Next**
4. To finish the CD-IP installation, choose one of the following:
 - **Skype for Business**— See Section 8.1.2 on page 90
 - **Other (VoIP Port Mirror)** – See Section 8.3.3 on page 133



Note: After upgrading SmartTAP, 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.

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 localIp="CDRealIP" port="11161"
    name="SWCallDelivery"
    oid="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.

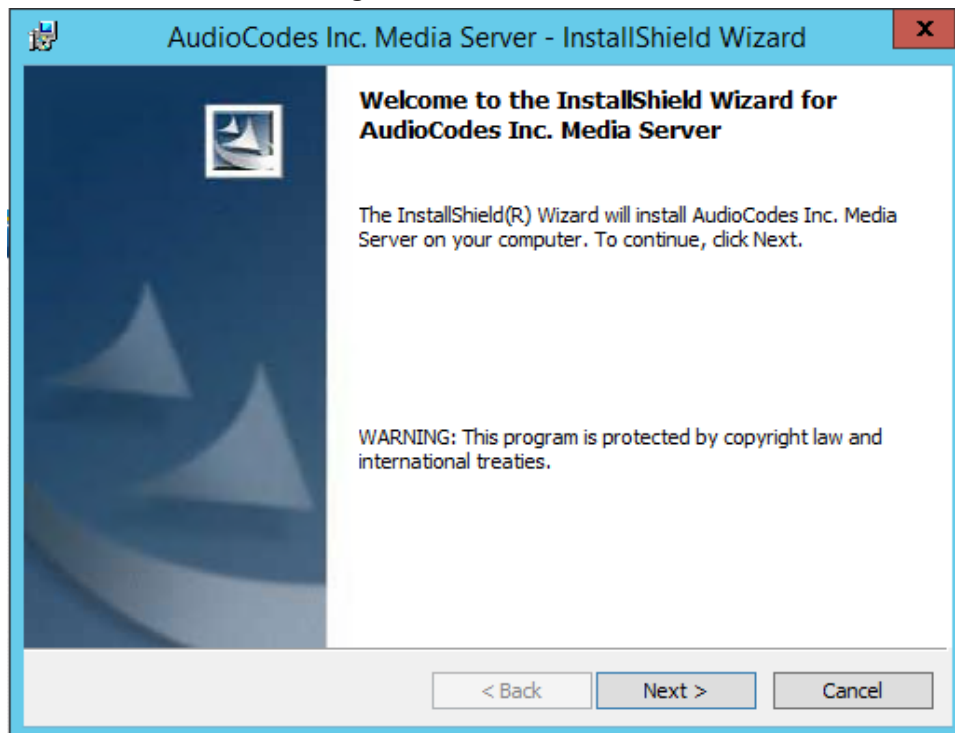
4.5 Installing the Media Server

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

➤ To install the Media Server:

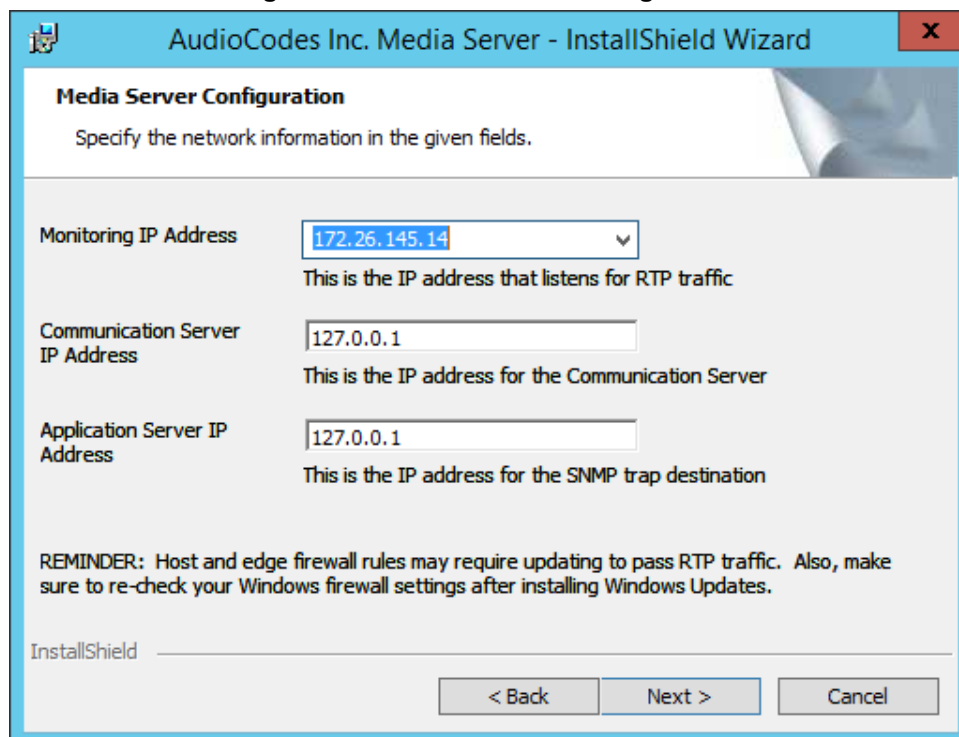
1. The Media Server installation starts in the proper sequence when all or multiple services are selected on the installer menu.
2. When the Media Server installation wizard starts, click **Next** to install.

Figure 4-14: Media Server



3. Select the IP Address of the SmartTAP Server from the "Monitoring IP Address" drop-down 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.

Figure 4-15: Media Server Configuration



6. Click **Next**.

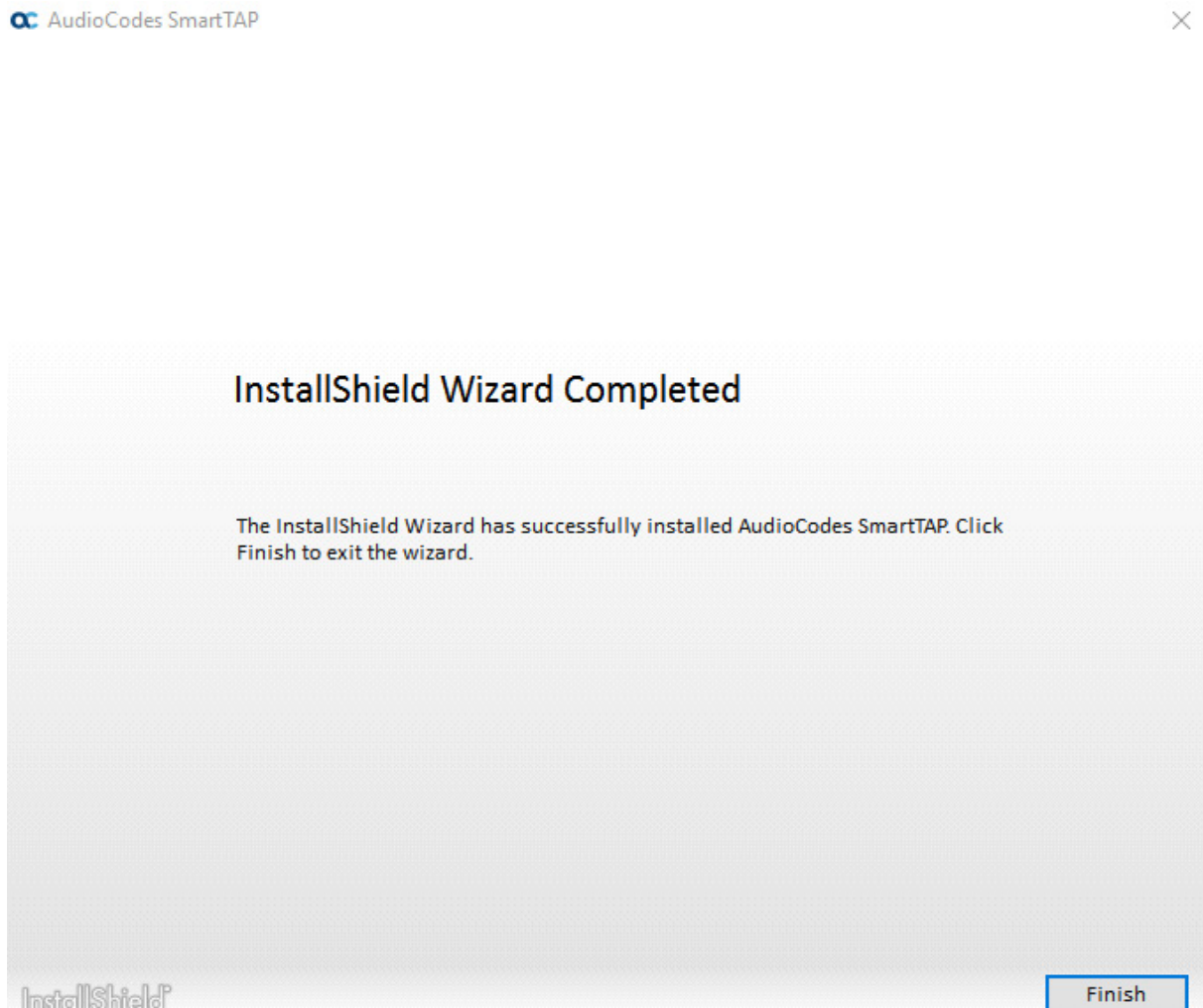
7. Click **Install**.
8. Click **Finish**.

4.6 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:

Figure 4-16: InstallShield Wizard Completed



2. Click **Finish** to exit the installer.
3. Go to the configuration information on Chapter 5 – Integration Configuration to complete the integration configuration steps required before the server is ready to record calls.

4.7 Post-Installation Integration

At this point in the installation, the software is running on the server. However, the SmartTAP recorder needs additional integration specific configuration before it is capable of recording calls. This integration is described in Chapter 8.

5 Installation Wizard - Distributed Method

This Chapter describes the Distributed method for installing SmartTAP.

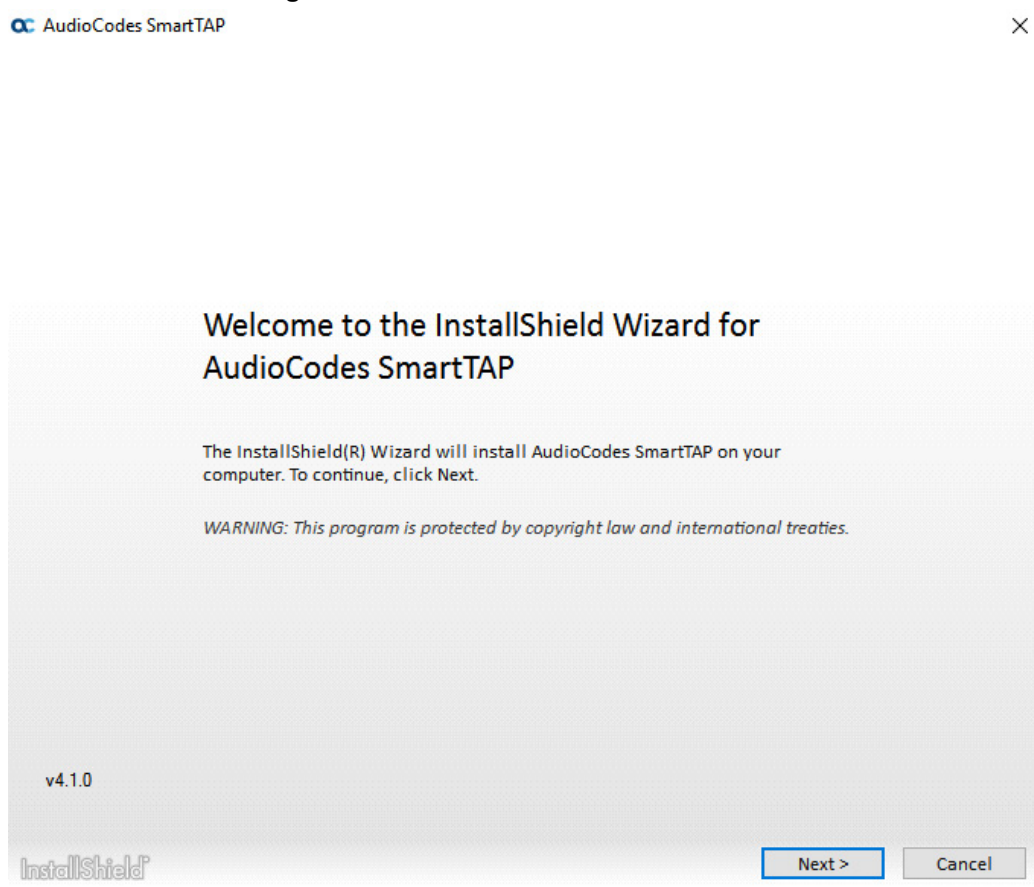


Note: This installation method assumes that each SmartTAP component will be installed on a separate physical or virtual server.

➤ **To install the distributed method:**

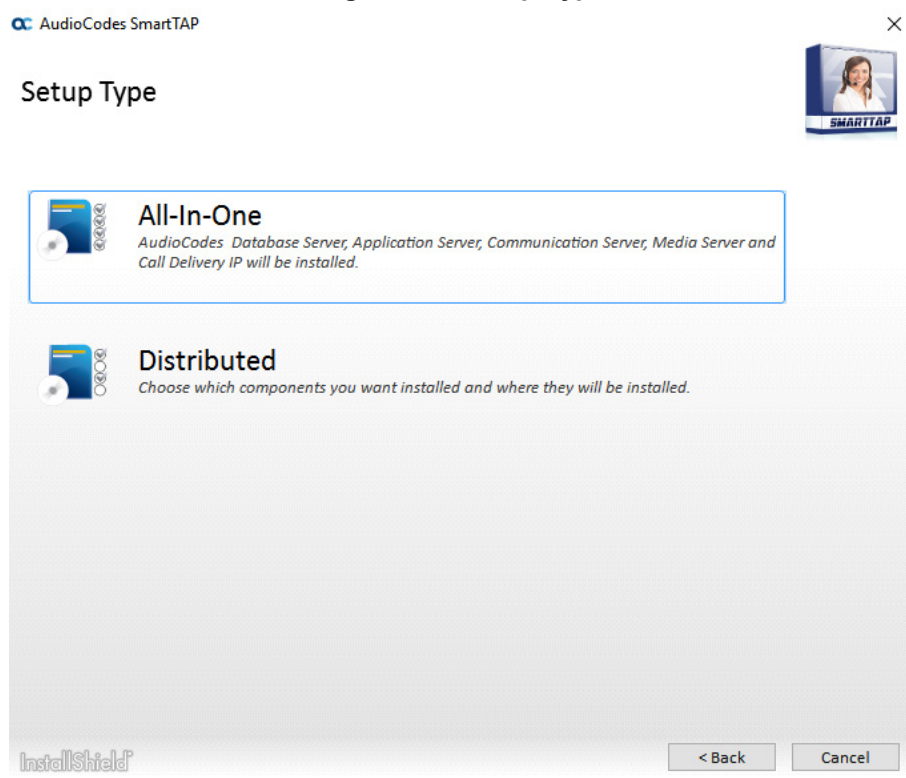
1. Launch **install.bat** from the “Suite” folder.
2. Click **Next** to continue.

Figure 5-1: InstallShield Wizard SmartTAP



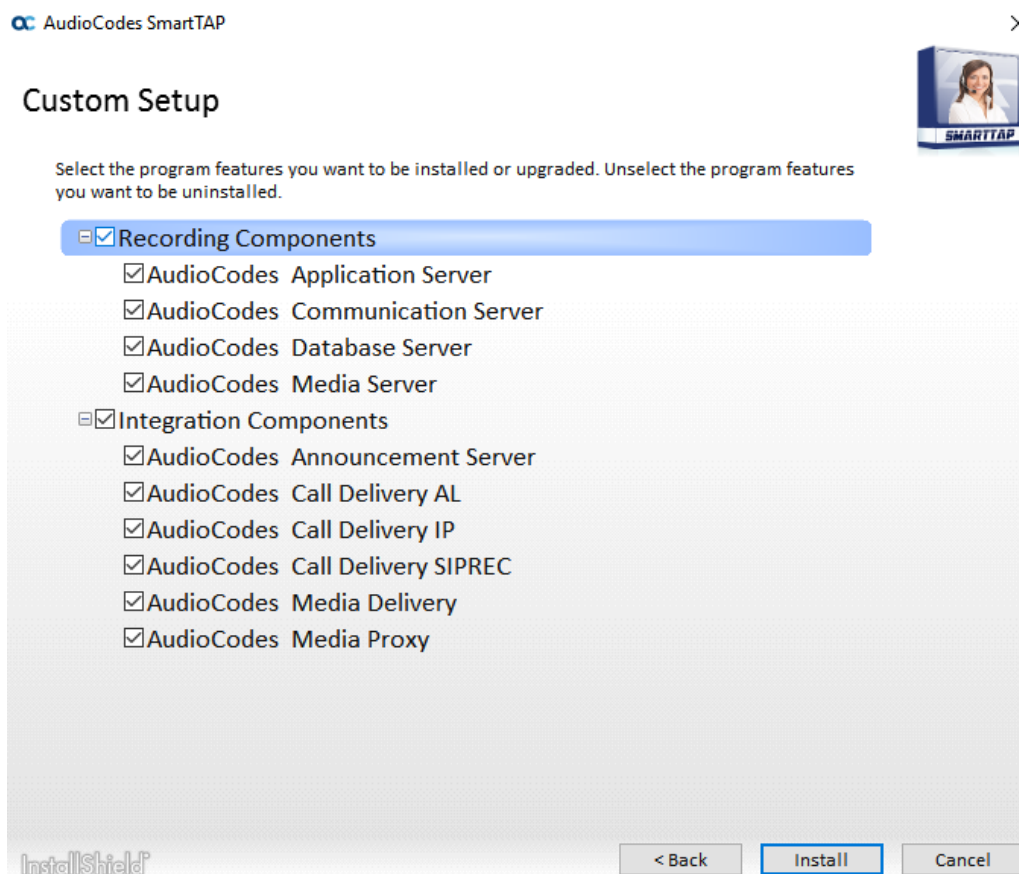
3. Click **Next** after accepting SmartWORKS license.
4. Click **Next** after accepting SmartTAP license.

Figure 5-2: Setup Type



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 Database Server (see Section 5.1)
- Installing SmartTAP Application Server Installation (see Section 5.2)
- Installing SmartTAP Communication Server (see Section 5.3)
- Installing SmartTAP Media Server (see Section 5.4)
- Installing SmartTAP Call Delivery Server (see Section 5.5)

5.1 Installing SmartTAP Database Server

This section describes the database service software installation.



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 7 on page 63.

➤ **To install the database service software:**

1. Run the **Install.bat** from the SmartTAP “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.

5.1.1 Database Service Configuration

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

5.2 Installing SmartTAP Application Server



Note:

- During an upgrade of the Application 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 7 on page 63.
- This procedure also runs a silent installation of the Health Monitor utility. 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 “..\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.

5.3 Installing SmartTAP Communication Server

**Note:**

- 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 7 on page 63.

➤ **To install the Communication Server:**

1. Run the **Install.bat** from the SmartTAP “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.

5.3.1 Configure Windows SNMP Service

See Section 3.2.1.

5.4 Installing SmartTAP Media Server

**Note:**

- 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 7 on page 63.

➤ **To install the Media Server:**

1. Run the **Install.bat** from the SmartTAP “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.

5.4.1 Media Server Configuration



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

5.4.1.1 Network File Server

This section describes how to create a user account for SmartTAP 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 right-click **New > User**.

Figure 5-4: Active Directory Users and Computers

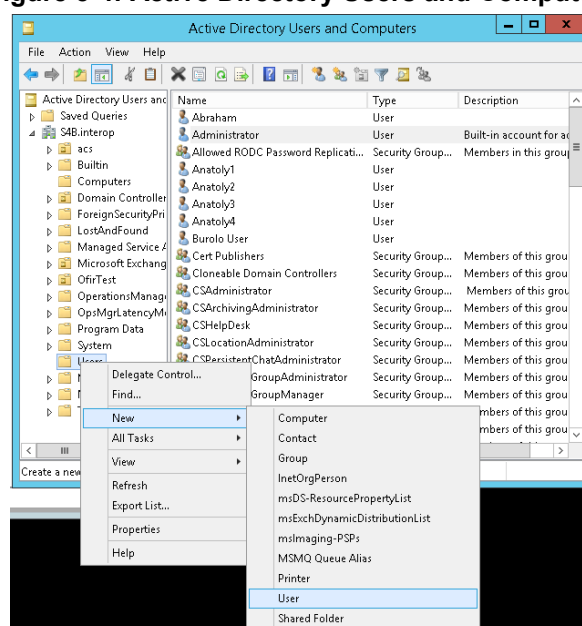


Figure 5-5: New SmartTAP User

New Object - User

Create in: S4B.interop/Users

First name: SmartTAPUser Initials:

Last name:

Full name: SmartTAPUser

User logon name: SmartTAPUser @S4B.interop

User logon name (pre-Windows 2000): S4B\ SmartTAPUser

< Back Next > Cancel

2. Enter the name of the SmartTAP 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:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

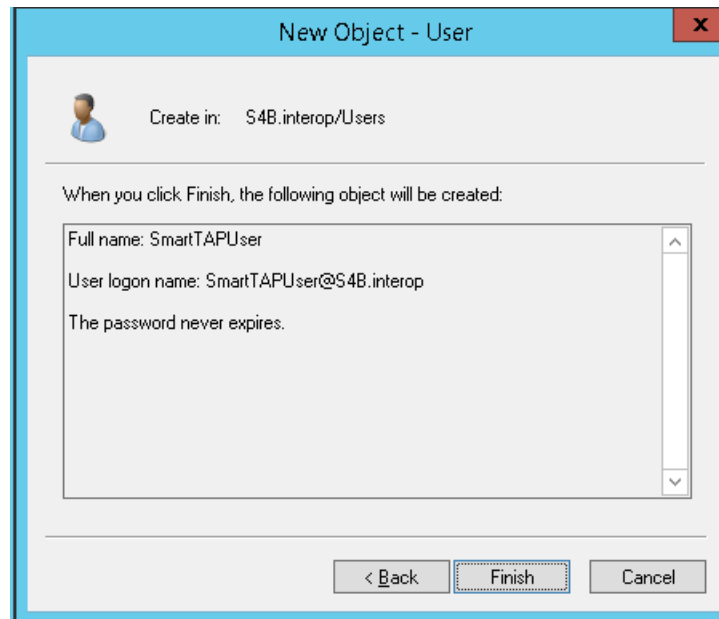
☐ Account is disabled

< Back Next > Cancel

3. Enter a password, select the “Password never expires” check box and click **Next**.

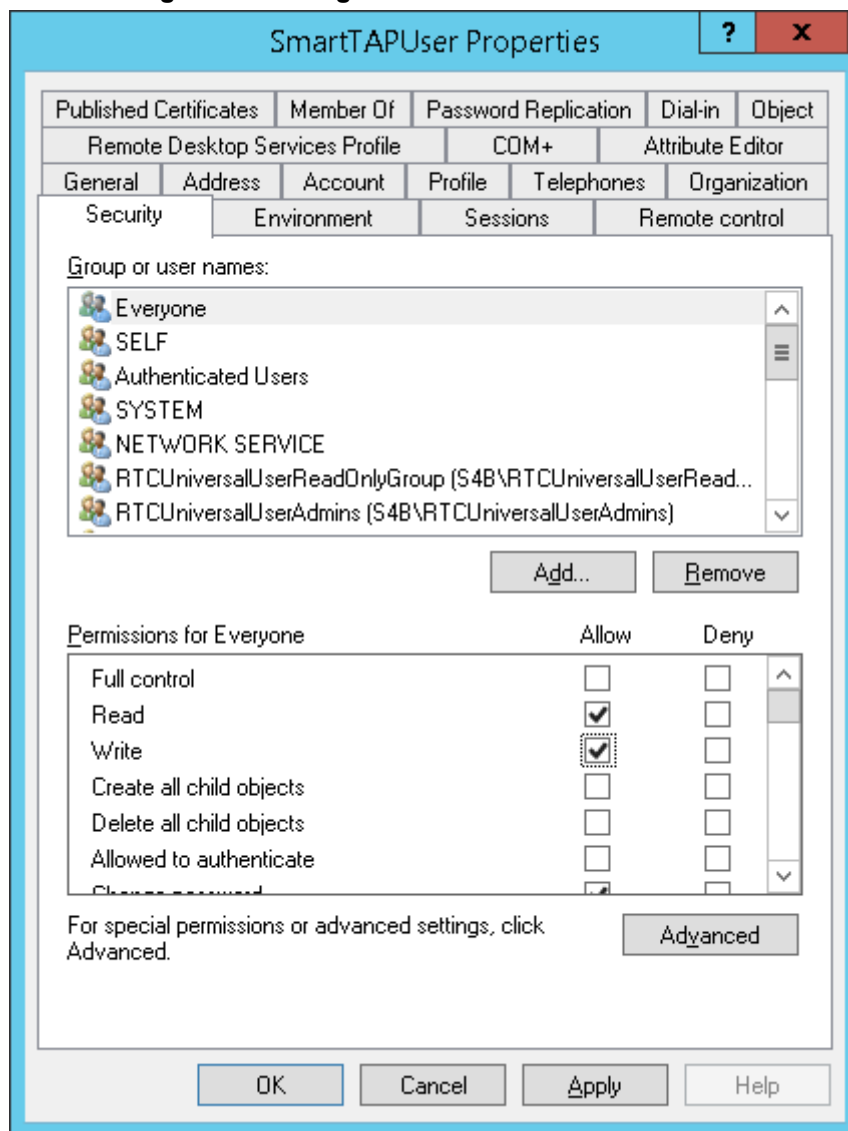
The following confirmation dialog is displayed:

Figure 5-7: User Add Confirmation



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

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".
8. Access the SmartTAP shared media storage in the File server.
9. Create, edit, and delete a test file in the storage directory.
10. Log off.

5.4.1.2 Media Server

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

➤ **Do the following:**

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

Figure 5-9: Add SmartTAP user to Administrators Group

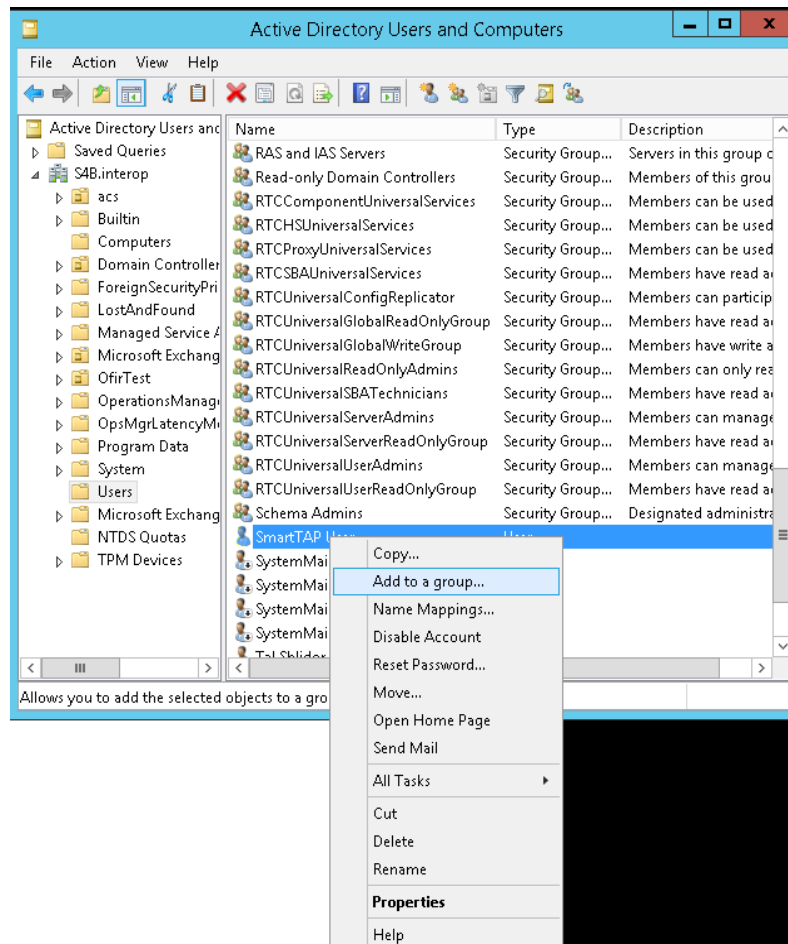
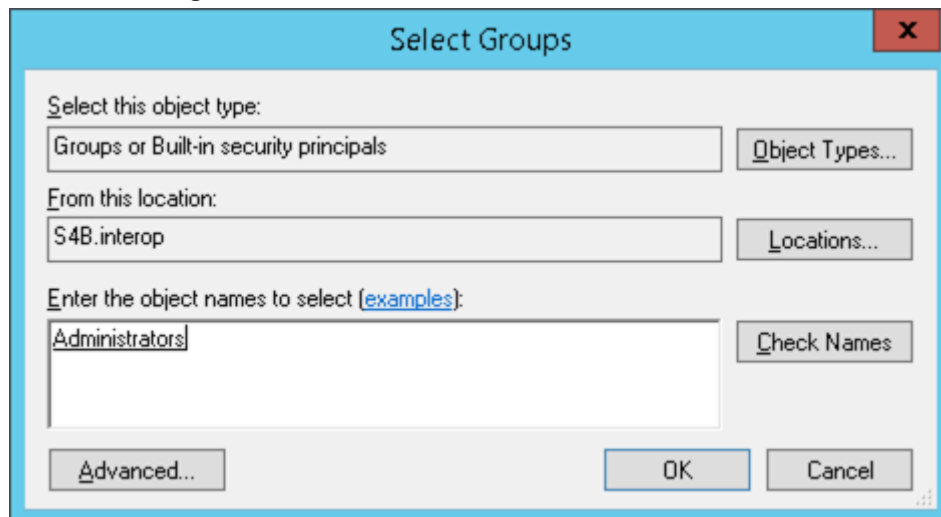
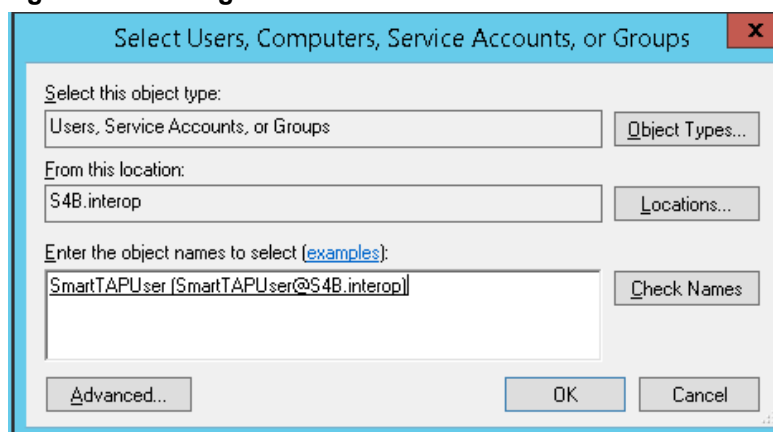


Figure 5-10: Add Smart TAP User to Administrator

- a. Enter **Administrator** and then click **Check Names**. The successfully recognized entry is underlined.
- b. Click **OK**. A confirmation screen is displayed.
2. Assign the SmartTAP user to the SmartTAP MS-TR service:
 - a. Open the **Services (Local)** application (services.msc).
 - b. Select the service "SmartTAP 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 user or any other user defined for this purpose.

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

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

5.4.2 Configure Windows SNMP Service

See Section 3.2.1

5.5 Installing SmartTAP 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 7 on page 63.

➤ To Install the Call Delivery server:

1. Run the “Install.bat” from the SmartTAP “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 8.1.1.3 on page 90.
 - Return here once the configuration has completed.
 - No additional CD-IP configuration should be necessary.
8. Click link to install the Other (IP). Refer to VoIP Port Mirroring.
 - Return here once the configuration has completed.
 - Once the installation of the CD-IP has completed, an additional configuration is required. See Section 8.3.4 on page 135.
9. Click link to install Analog Trunk/Radio. See Section 8.5 on page 137:
 - Return here once the configuration has completed.
 - Once the installation of the CD-AL has completed, an additional configuration is required. See Section 8.5.2 on page 140.
10. Click **Next** to continue.
11. Click **Install** to complete the installation.

5.5.1 Configure Windows SNMP Service

See Section 3.2.1

5.5.2 SmartTAP File Server Installation



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

5.5.2.1 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 7 on page 63.

5.5.2.2 Domain Controller Configuration

This configuration is an example of what must be performed in a windows environment to allow the SmartTAP 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 user on the Windows server Domain Controller:**

1. Create a user account for SmartTAP on the Domain Controller. For example “SmartTAP User”:
 - a. In the Active Directory Users and Computers folder, select the Users folder and then right-click **New > User**.

Figure 5-12: Active Directory Users and Computers

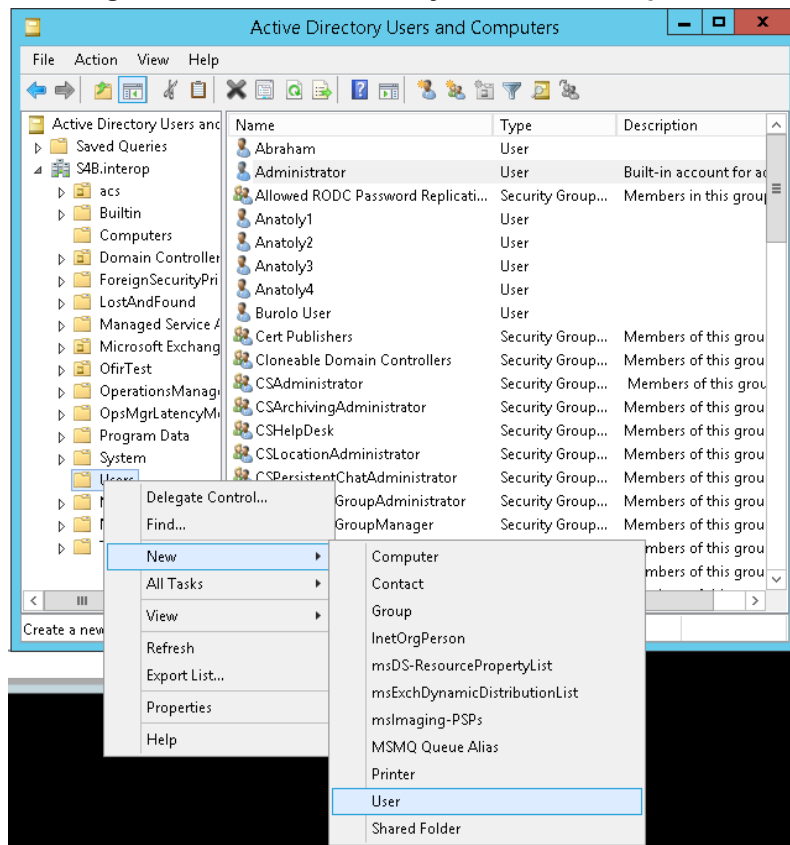


Figure 5-13: New SmartTAP User

The dialog box is titled "New Object - User" and shows the "Create in:" path as "S4B.interop/Users". It contains the following fields:

- First name:** SmartTAP User
- Initials:** (empty)
- Last name:** (empty)
- Full name:** SmartTAP User
- User logon name:** SmartTAP User
- Domain:** @S4B.interop (dropdown menu)
- User logon name (pre-Windows 2000):** S4B\SmartTAP User

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

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

Figure 5-14: User Settings

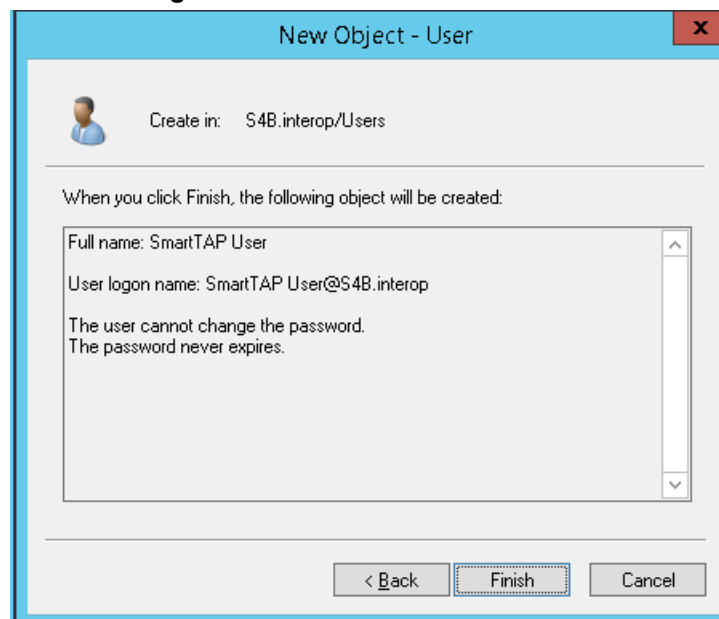
This dialog box shows the password configuration section. It includes:

- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- ☐ User must change password at next logon
- ☒ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

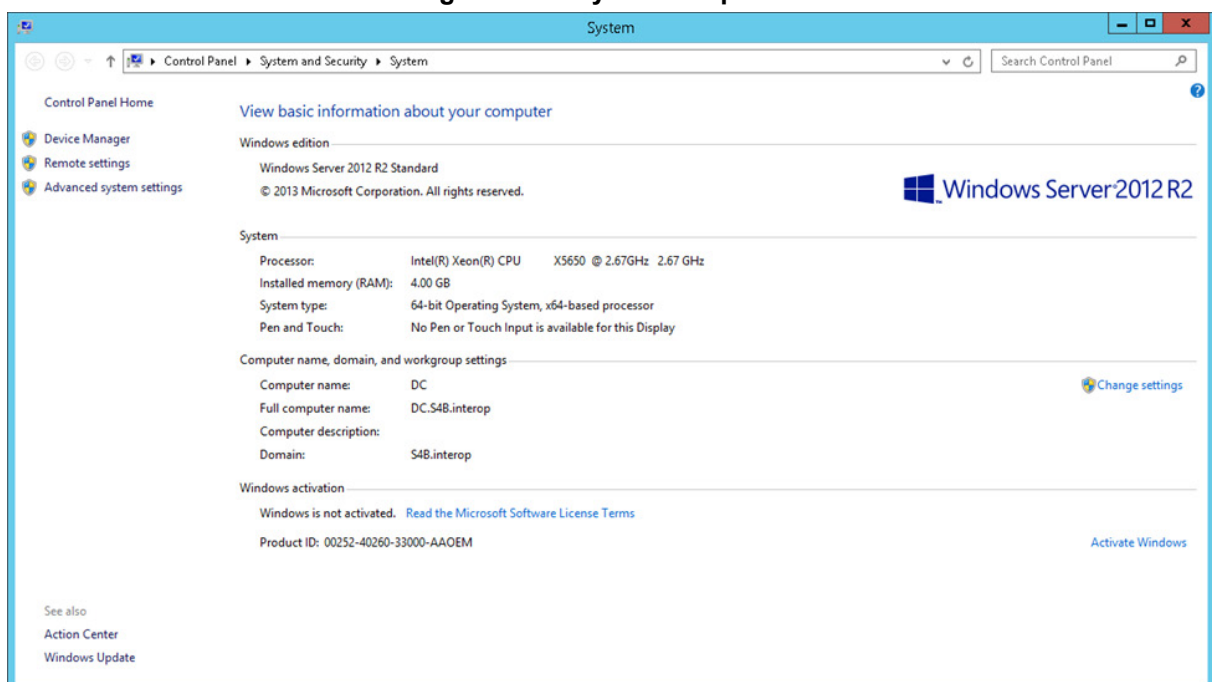
The following confirmation dialog is displayed:

Figure 5-15: User Add Confirmation



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

Figure 5-16: System Properties

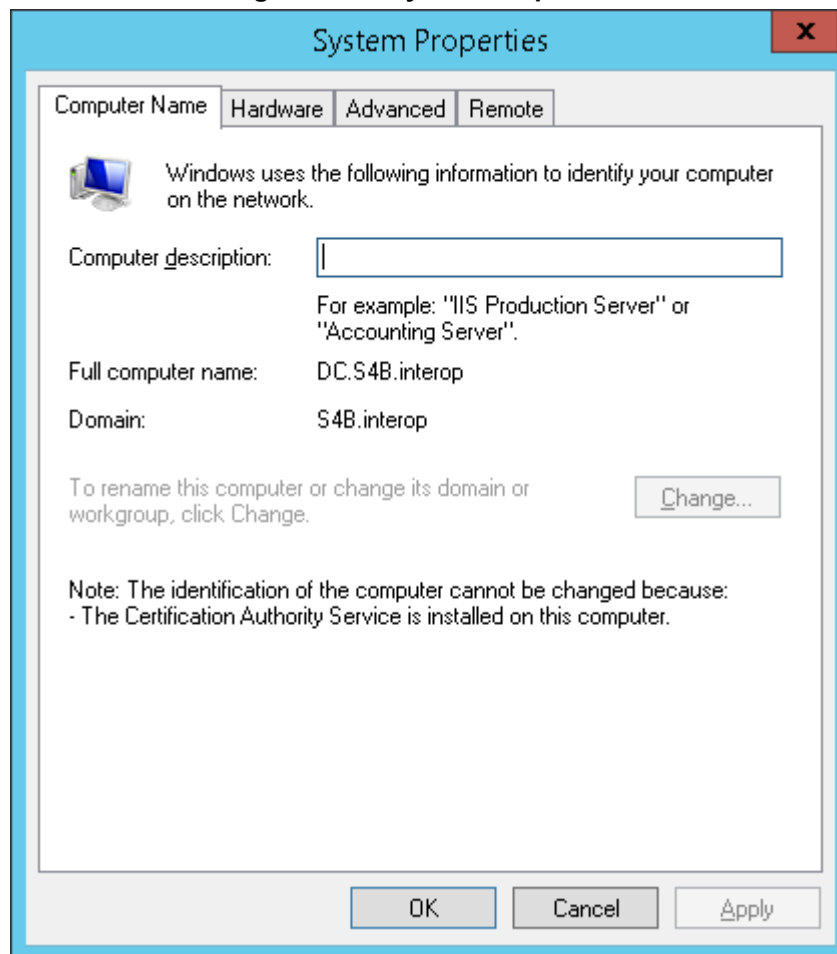


- b. Select **Change settings** in the Computer name, domain, and workgroup settings.
- c. Click **Change..** in the Computer Name tab.
- d. Select the **Domain** radio button and enter the name of the domain.
- e. When prompted, enter the domain administrator user and password.

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

- f. Restart the File Server.

Figure 5-17: System Properties



5. Log in into the file server as user “SmartTAP” 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.

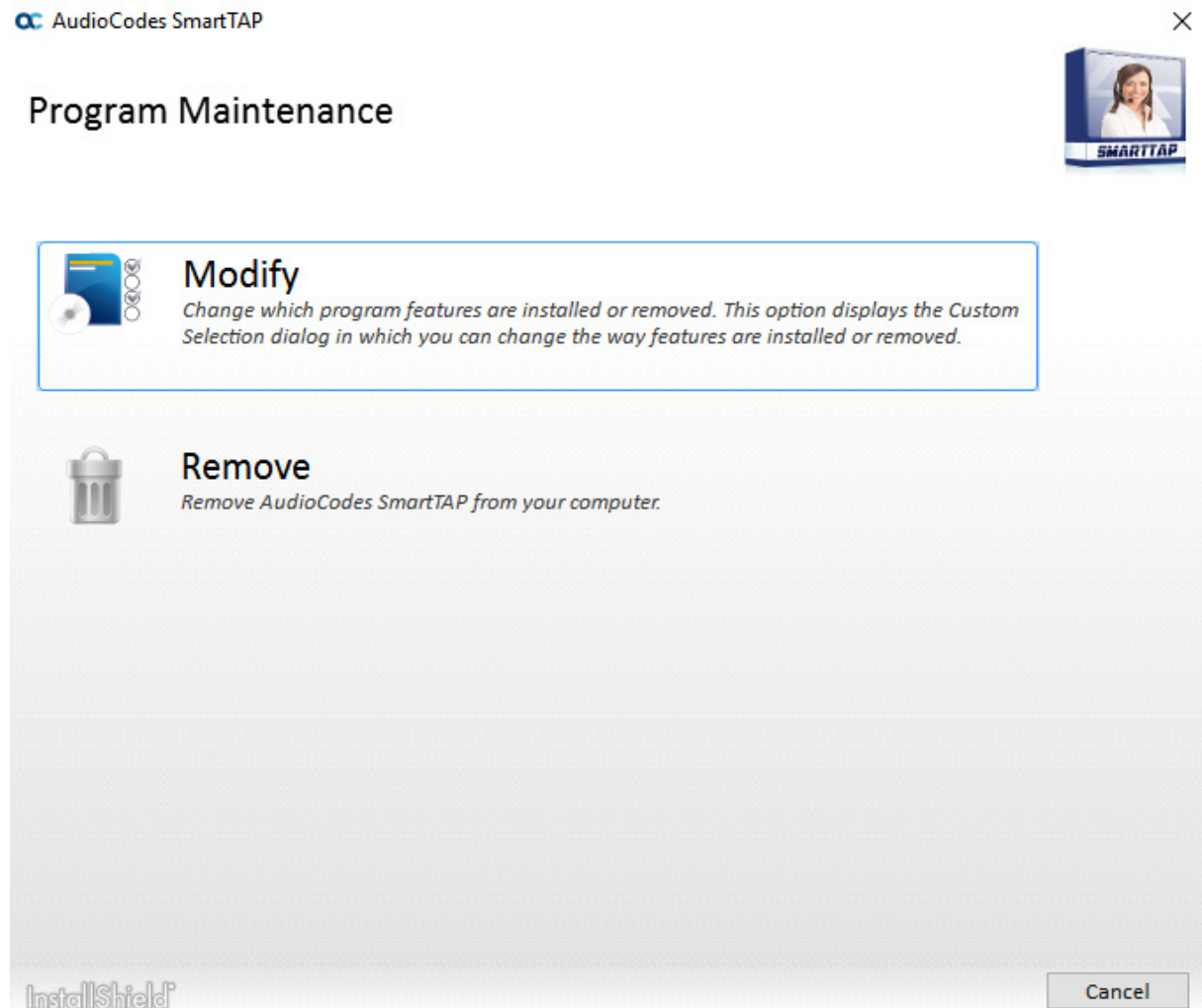
6 Uninstalling SmartTAP

The following describes how to uninstall SmartTAP.

➤ **To uninstall SmartTAP:**

1. Launch **install.bat** from the “Suite” folder.
2. From the Program Maintenance screen, click **Remove** to remove the SmartTAP component from the PC.

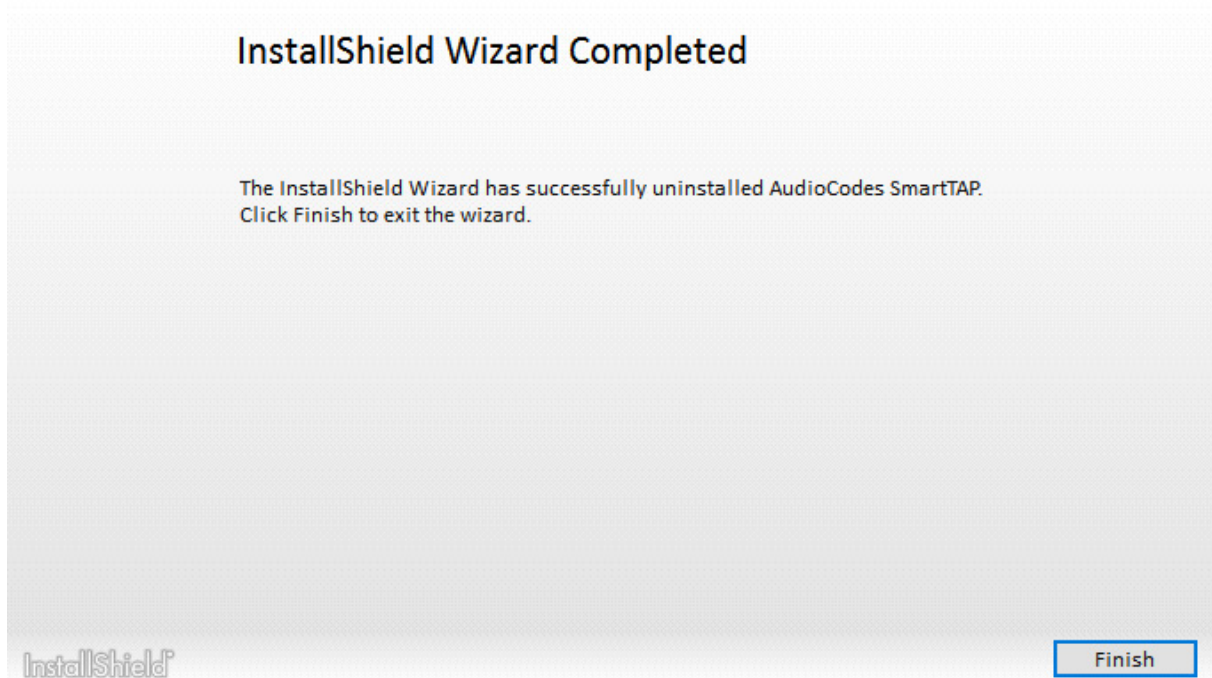
Figure 6-1: Program Maintenance - Remove



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

Figure 6-2: InstallShield Wizard Completed - Uninstall

AudioCodes SmartTAP



7 Firewall Configuration

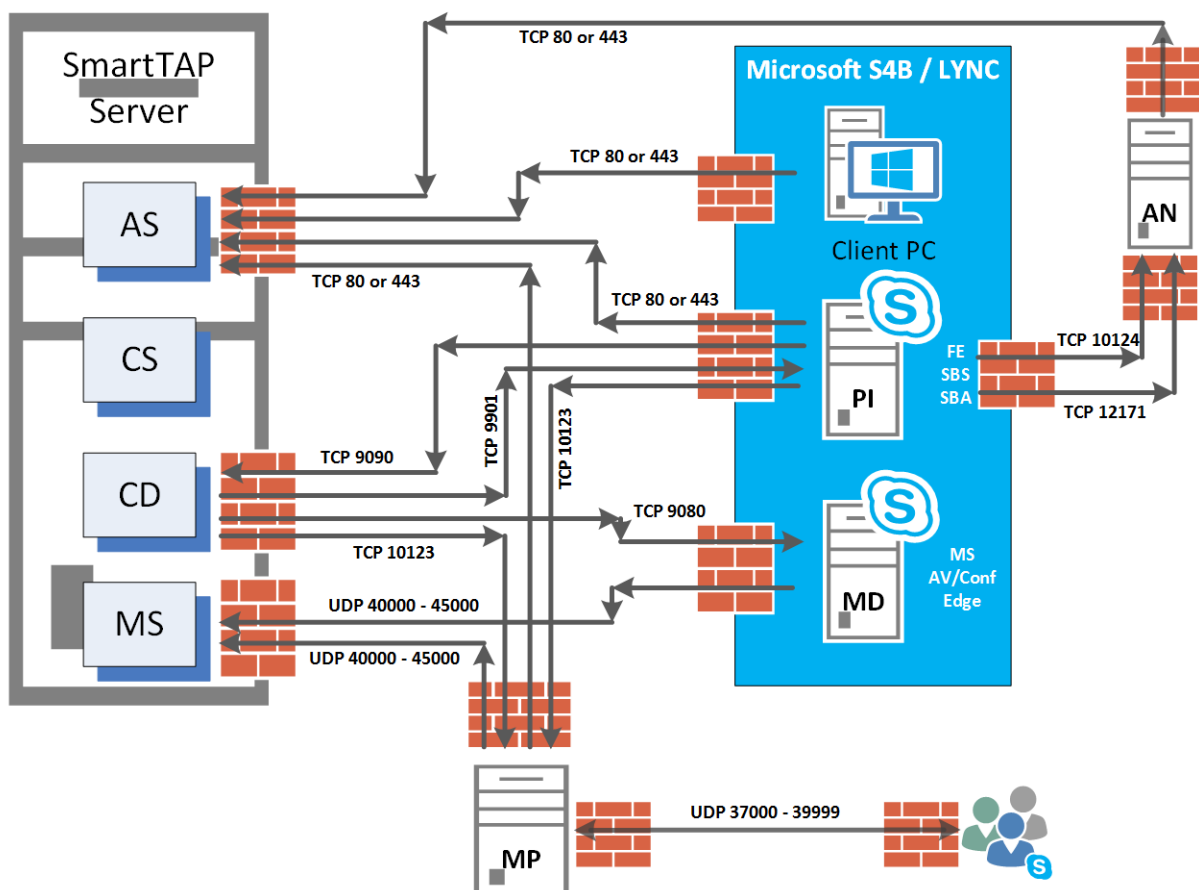
The deployment of the SmartTAP servers may have to comply with customer security policies, which require the implementation of firewall rules. This section provides the basic information required by the Windows administrator to configure the Windows firewall, to ensure the required connectivity between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



Note: All Firewall Ports listed are default.

7.1 Skype for Business Recording Firewall

Figure 7-1: Skype for Business Recording Firewall



7.1.1 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
TCP	9901	DOMAIN/INTERNAL (from SmartTAP to FE)
TCP	12171	DOMAIN/INTERNAL (from SmartTAP Announcement Server to FE)

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

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

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

7.1.2 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
TCP	9080	DOMAIN/INTERNAL (from SmartTAP 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)



Note: 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.

7.1.3 SmartTAP Server

The following Inbound firewall exceptions are required.

Table 7-5: SmartTAP Server - INBOUND Firewall

Protocol	Allow Port	Allowed Network
TCP	80	DOMAIN/INTERNAL (from FE servers) EXTERNAL (Web Browser Access for end-users)
TCP	443	DOMAIN/INTERNAL (from FE to AS when AS is configured with HTTPS)
TCP	9090	DOMAIN/INTERNAL (from FE servers)
UDP	40000-45000 ¹	DOMAIN/INTERNAL (from MD) DOMAIN/INTERNAL (from MP servers)
TCP	10125	DOMAIN/INTERNAL (from AS) Note: The port is only required for CD when AS is installed on another server.

The following Outbound firewall exceptions are required.

Table 7-6: SmartTAP Server - Outbound Firewall

Protocol	Allow Port(s)	Allowed Network
TCP	9080 ¹	DOMAIN/INTERNAL (to MD)
TCP	9901	DOMAIN/INTERNAL (to FE servers)
TCP	10123	DOMAIN/INTERNAL (to MP servers)

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

7.1.4 SmartTAP Media Proxy Server

The following Inbound firewall exceptions are required.

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

Protocol	Allow Port	Allowed Network
TCP	10123	DOMAIN/INTERNAL (from FE and SmartTAP servers)
UDP	37000-39999	DOMAIN/INTERNAL (from Skype for Business clients to MP)

The following Outbound firewall exceptions are required.

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

Protocol	Allow Port	Allowed Network
UDP	37000-39999	DOMAIN/INTERNAL (from MP to Skype for Business or Lync clients)
TCP	80	DOMAIN/INTERNAL (from MP to AS)

Protocol	Allow Port	Allowed Network
TCP	443	DOMAIN/INTERNAL (from MP to AS when AS is configured with HTTPS)

7.1.5 SmartTAP Announcement Server

The following Inbound firewall exceptions are required.

Table 7-9: SmartTAP Announcement Server- Inbound Firewall

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

The following Outbound firewall exceptions are required.

Table 7-10: SmartTAP Announcement Server - Outbound Firewall

Protocol	Allow Port	Allowed Network
TCP	80	DOMAIN/INTERNAL (from ANN to SmartTAP AS)
TCP	443	DOMAIN/INTERNAL (from ANN to SmartTAP 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>

7.1.6 Automated Firewall Exception Scripts for Windows Firewall

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

... \AUDIOCODES\SmartTap\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.
2. Copy the entire directory to each component that needs to have firewall exceptions added (SmartTAP, Skype for Business Edge, Mediation or Conference Server and the Skype for Business Front Ends).
3. On each server, modify the *\$machine_type* line to match the machines functionality (smarttap, 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 firewall exceptions start with the word "SmartTAP".

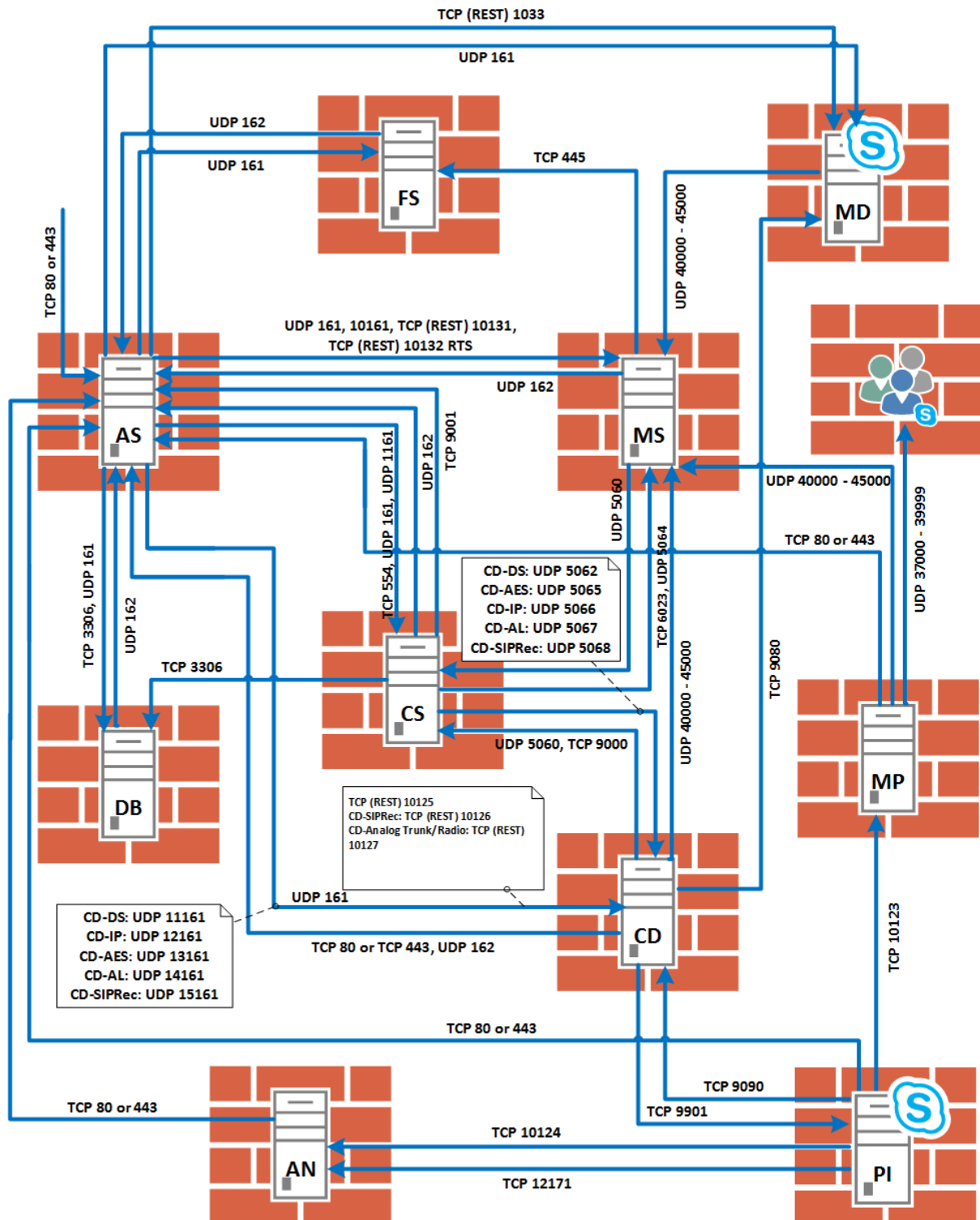
7.2 Distributed SmartTAP Firewall

The following firewall rules are required in the event that you install each component of the SmartTAP installation on a physically separate machine (as described in Chapter 5). 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 7.2.1).



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

Figure 7-2: Distributed SmartTAP Firewall



7.2.1 Application Server (AS)

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

Protocol	Allow Port	Allowed Network
TCP	80	EXTERNAL (Web Browser Access for end-users) DOMAIN/INTERNAL (from other SmartTAP servers)
TCP	9001	DOMAIN/INTERNAL (from other SmartTAP servers)
UDP	162	DOMAIN/INTERNAL (from other SmartTAP servers)

7.2.2 Communications Server (CS)

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

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

7.2.3 Database Server (DB)

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

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

7.2.4 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 servers)

7.2.5 Media Server (MS)

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

Protocol	Allow Port	Allowed Network
UDP	161, 5064, 10161, 40000-45000	DOMAIN/INTERNAL (from other SmartTAP servers)
TCP	6023	DOMAIN/INTERNAL (from other SmartTAP servers)
TCP REST	10131	DOMAIN/INTERNAL (from other SmartTAP servers)

7.2.5.1 Remote Transfer Service (RTS)

Table 7-16: Remote Transfer Service (RTS)

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

7.2.6 Call Delivery(CD)

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

Protocol	Allow Port	Allowed Network
UDP	161, 40000-45000	DOMAIN/INTERNAL (from other SmartTAP servers)
UDP (Add any required)	12161 – All VoIP	DOMAIN/INTERNAL (from other SmartTAP servers)
	14161 – Analog	DOMAIN/INTERNAL (from other SmartTAP servers)
	15161 – SIPRec	DOMAIN/INTERNAL (from other SmartTAP servers)
	5066 – All VoIP	DOMAIN/INTERNAL (from other SmartTAP servers)
	5067 – Analog	DOMAIN/INTERNAL (from other SmartTAP servers)
	5068 – SIPRec	DOMAIN/INTERNAL (from other SmartTAP servers)
TCP	9090	DOMAIN/INTERNAL (from other SmartTAP servers)
	10125 – All VoIP	DOMAIN/INTERNAL (from other SmartTAP servers)
TCP (REST)	10125	DOMAIN/INTERNAL (from other SmartTAP servers)
TCP (REST)	10126	DOMAIN/INTERNAL (from SIP Recording server)

TCP (REST)	10127	DOMAIN/INTERNAL (from Analog Trunk / Radio)
------------	-------	---

7.2.7 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
TCP	9080	DOMAIN/INTERNAL (from other SmartTAP servers)
TCP REST	10133	DOMAIN/INTERNAL (from other SmartTAP servers)

7.2.8 Media Proxy (MP)

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

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

Protocol	Allow Port	Allowed Network
TCP	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)

7.2.9 Announcement Server (AN)

This applies to SmartTAP Announcement servers exclusively in a Microsoft Skype for Business environment.

Table 7-20: Firewall - Announcement Server (AN)

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

7.2.9.1 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 Integration Configuration

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

- Microsoft Skype for Business - See Section 8.1 on page 73
- SIPRec – See Section 8.2 on page 128
- Voip Mirror Port (SIP, H.323, Avaya, Cisco, etc.) – See Section 8.3 on page 131
- Analog Trunk, Station & Radio – See Section 8.5 on page 137

8.1 Microsoft Skype for Business

In a Skype for Business environment, SmartTAP 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 server(s) so that SmartTAP is aware of call states only for recorded calls. Using the call signaling, SmartTAP 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.

Figure 8-1: Capture Call Signaling - 1

Criteria	Capture Call Signaling		Capture Call Audio				
	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
Client to Client	✓	✓	✓	✓	n/a	n/a	✓
PSTN – Media Bypass Disabled	✓	✓	✓	✓	✓	n/a	✓
PSTN - Media Bypass Enabled	✓	✓	✓	✓	n/a	n/a	✓
Conferencing	✓	n/a	✓	✓	n/a	✓	✓
Remote / Federated	✓	n/a	n/a	✓	n/a	n/a	n/a
Mobile	✓	n/a	n/a	✓	n/a	n/a	n/a
Home User	✓	n/a	n/a	✓	n/a	n/a	n/a

✓ = Call Type Supported | n/a = Not Applicable

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

Figure 8-2: Capture Call Signaling - 2

Software	Capture Call Signaling		Capture Call Audio					
	SmartTAP Server	Front End Server	SBA Appliance	Proxy Server	Edge Server	Mediation Server	Conference Server	Mirror Port
S4B / Lync plug-in	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
Communication Server	✓	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
Media Server	✓	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
Media Delivery	n/a	✓ ¹	✓ ¹	n/a	✓	✓	✓	n/a
Media Proxy	n/a	n/a	n/a	✓ ²	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	✓ ³

- 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 to Record Skype for Business:

- Installing SmartTAP Skype for Business plugin (see Section 8.1.1)
- Installing SmartTAP Call Delivery, choose Microsoft Lync as network type (see Section 8.1.2)
- Installing Media Proxy in case of utilizing the Media Proxy solution (see Section 8.1.3)
- Installing SmartTAP Media Delivery (see Section 8.1.4)

8.1.1 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 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.

Pre-Requisites:

- .NET Framework 4.5



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 7 on page 63.
- Install the Skype for Business plugin described in this section on every Front End Server processing calls to record.

8.1.1.1 Pre-install Preparation

This section describes the pre-install preparation for the Skype for Business Plugin.

8.1.1.1.1 On the Active Directory Domain Controller

This section describes the setup on the Active Directory Domain Controller.

➤ **Do the following:**

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

Figure 8-3: Active Directory Users and Computers

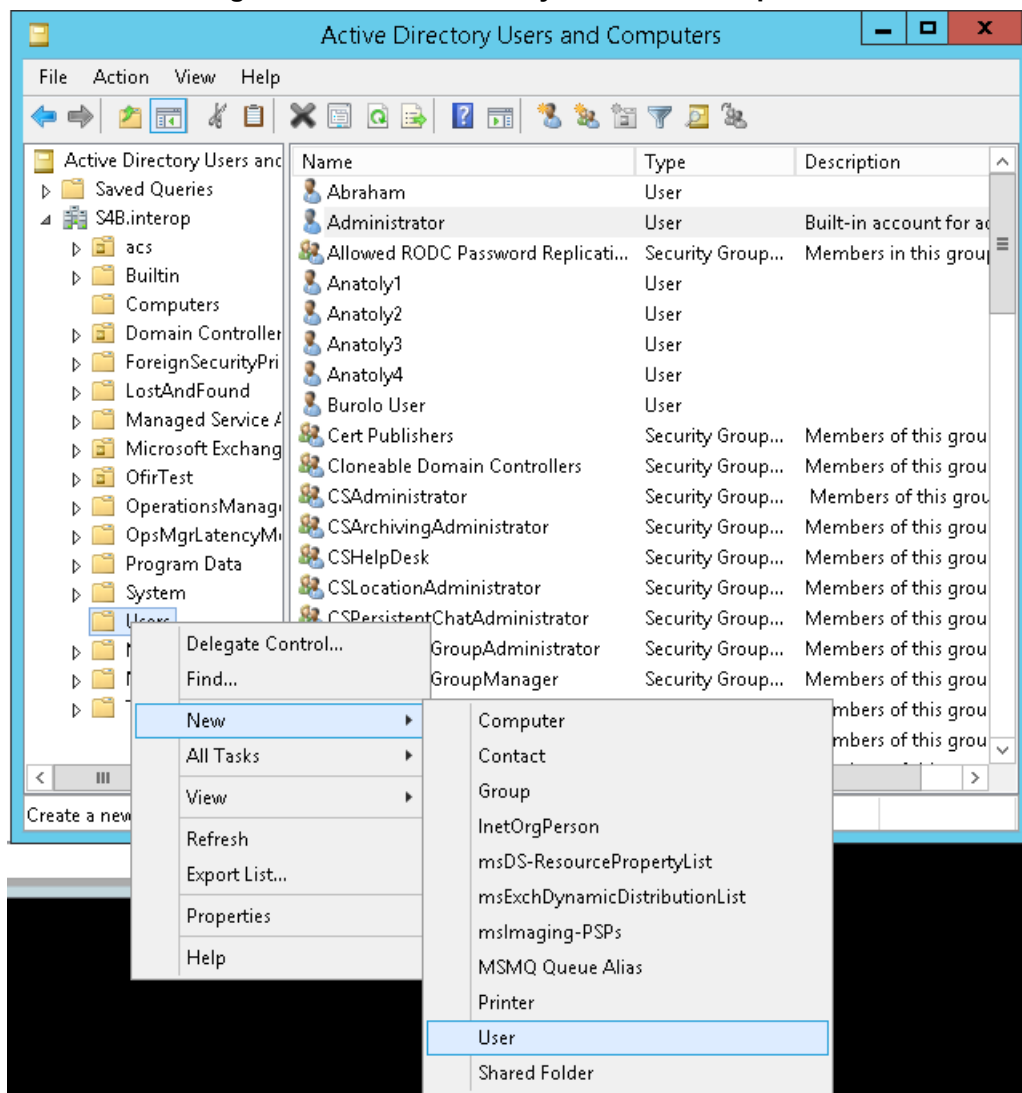
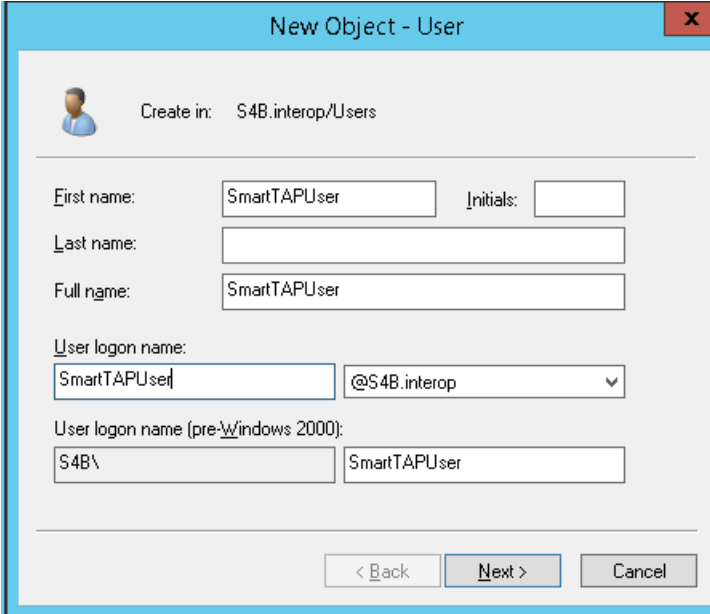


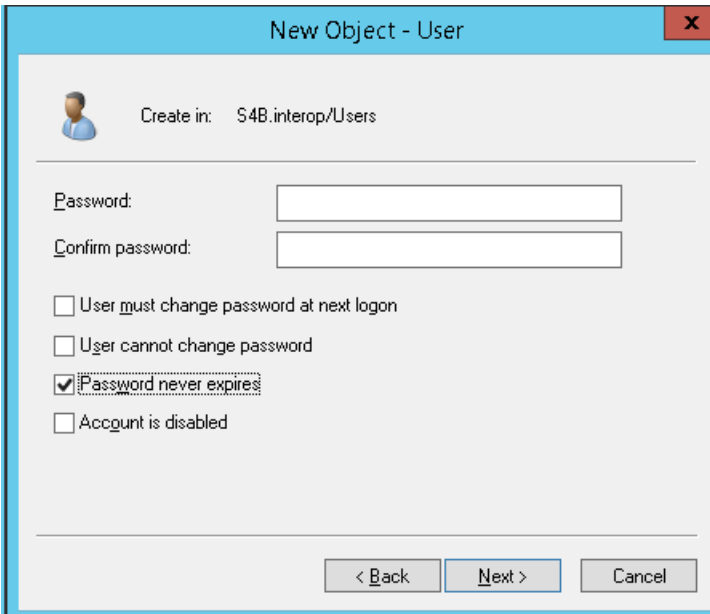
Figure 8-4: New SmartTAP User



The screenshot shows a 'New Object - User' dialog box with a blue header and a red close button. Below the header, there is a user icon and the text 'Create in: S4B.interop/Users'. The form contains several input fields: 'First name' (containing 'SmartTAPUser'), 'Initials' (empty), 'Last name' (empty), 'Full name' (containing 'SmartTAPUser'), 'User logon name' (containing 'SmartTAPUser'), a dropdown menu for the domain (showing '@S4B.interop'), 'User logon name (pre-Windows 2000):' (containing 'S4B\'), and another input field for the pre-Windows 2000 logon name (containing 'SmartTAPUser'). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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

Figure 8-5: Password Never Expires

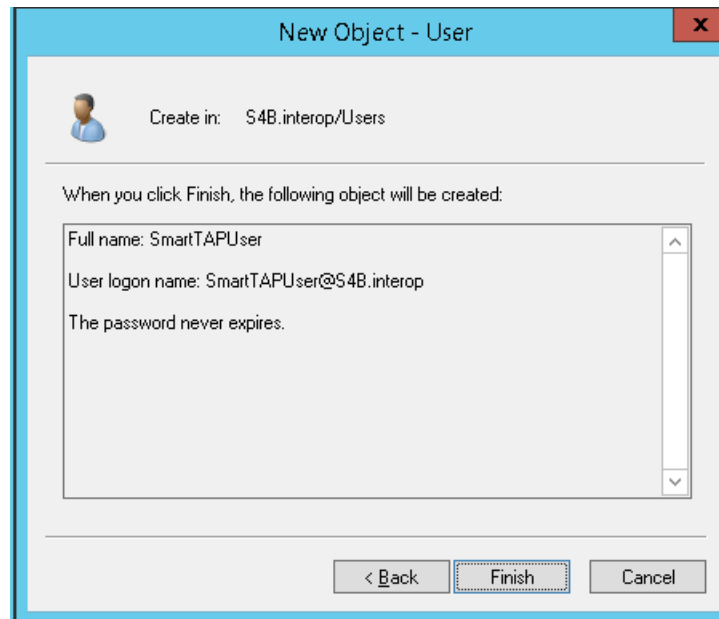


The screenshot shows the same 'New Object - User' dialog box, but with different fields visible. It includes 'Password:' and 'Confirm password:' input fields. Below these are four checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires' (which is checked), and 'Account is disabled'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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

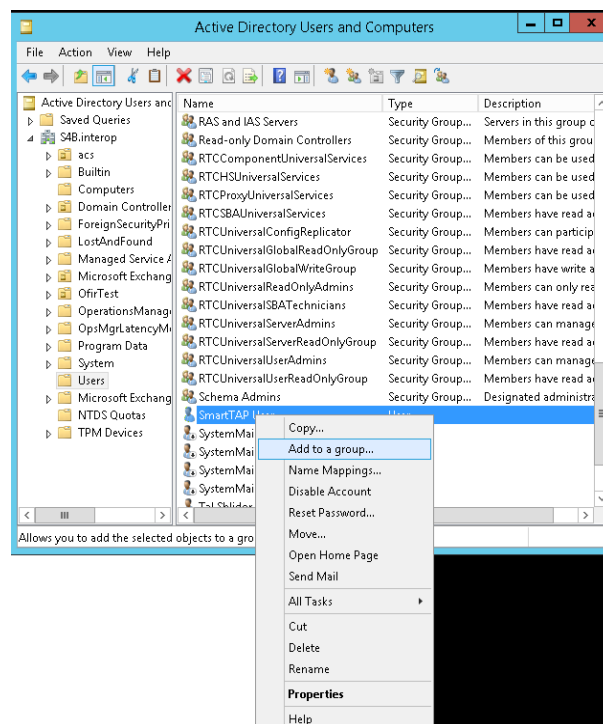
The following confirmation dialog is displayed:

Figure 8-6: User Add Confirmation



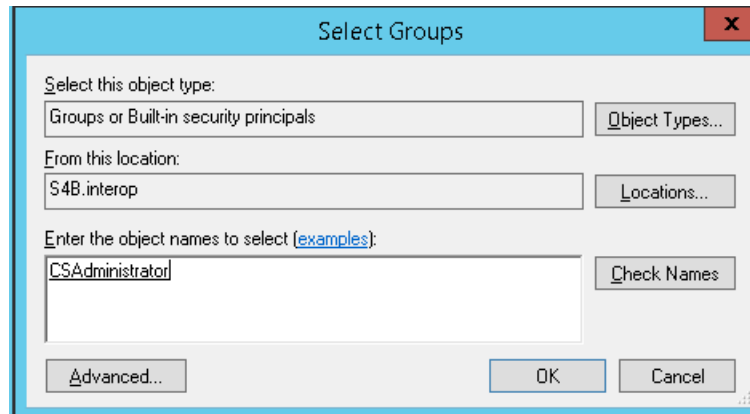
- d. Click **Finish**.
2. (Optional) Add the account to the "CSAdministrator" group. This membership is not mandatory; however, may be required for running the Plugin installation. The account can be removed from the group after the installation:
 - a. Right-click the newly created SmartTAP user and choose **Add to a group**.

Figure 8-7: Add SmartTAP user to CSAdministrators group



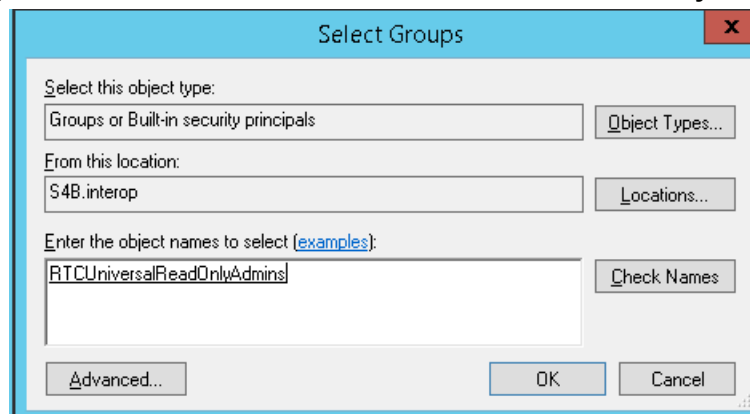
- b. Enter **CSAdministrator** and then click **Check Names**. The successfully recognized entry is underlined.

Figure 8-8: Add Smart TAP User to CSAdministrator



- c. Click **OK**. A confirmation screen is displayed.
3. Add the SmartTAP 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 user and choose **Add to a group**.
 - b. Enter **RTCUniversalReadOnlyAdmins** and then click **Check Names**. The successfully recognized entry is underlined.

Figure 8-9: Add Smart TAP User to RTCUniversalReadOnlyAdmins



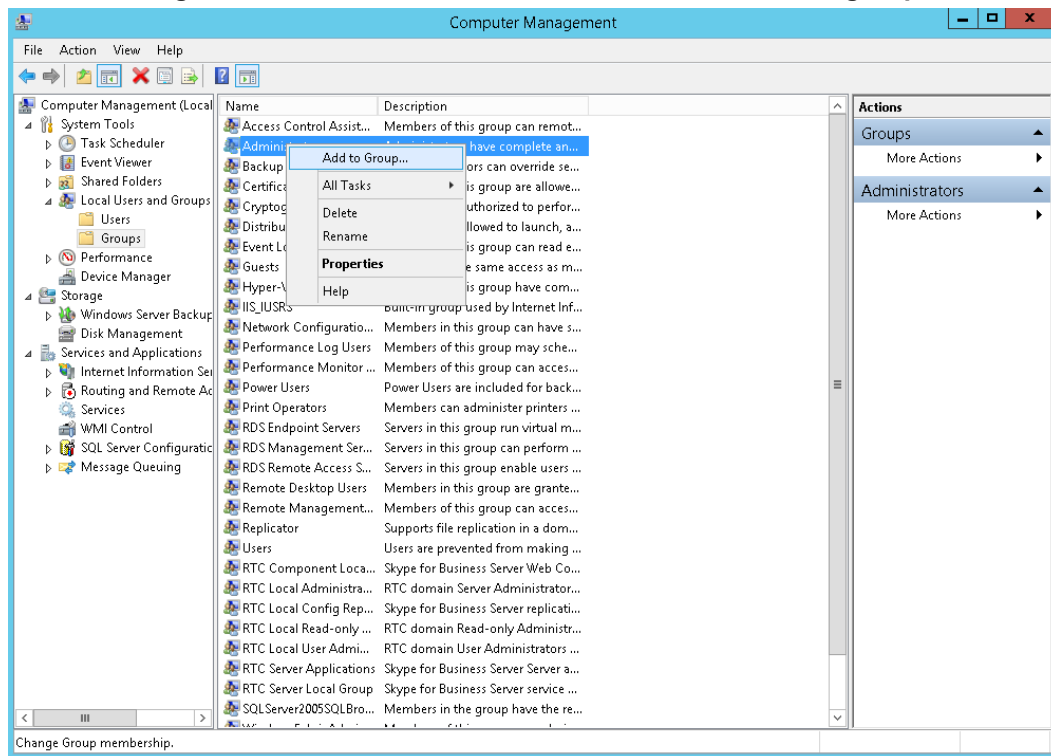
- c. Click **OK**. A confirmation screen is displayed.

8.1.1.1.2 On each Front End, SBS or SBA

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

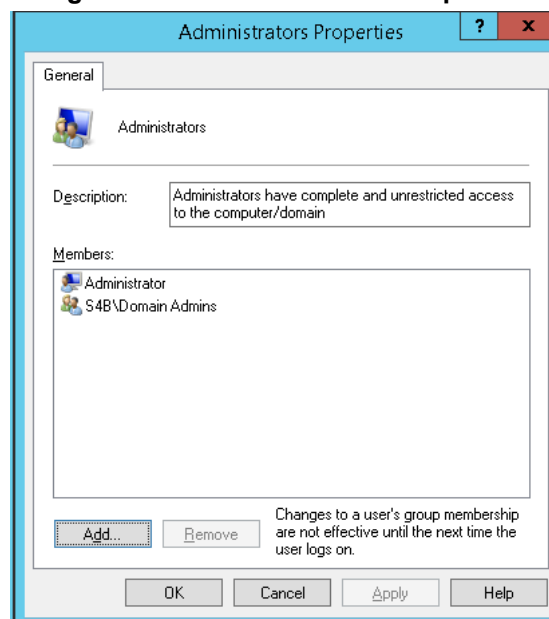
- **Do the following:**
1. Add new "SmartTAP User" to the local "Administrators" group:
 - a. Log in to the machine using a local administrator or a domain administrator account.
 - b. Open the Computer Management window.
 - c. Open the Local Users and Groups folder.
 - d. Select the Groups folder and then select the Administrators entity.
 - e. Right-click and choose **Add to Group**.

Figure 8-10: Add SmartTAP user to the Administrators group



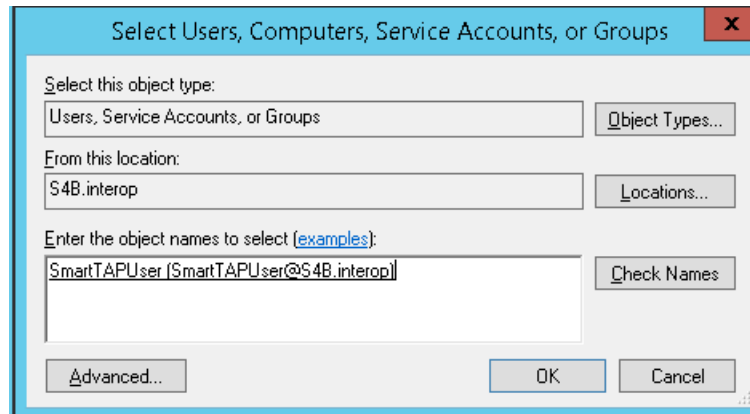
- f. In the Administrator Properties window, click **Add**.

Figure 8-11: Administrators Properties



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

Figure 8-12: SmartTAP User Added to Administrators



- h. Click **OK**. A confirmation screen is displayed.
2. Add the SmartTAP 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**.

Figure 8-13: RTCServerApplications

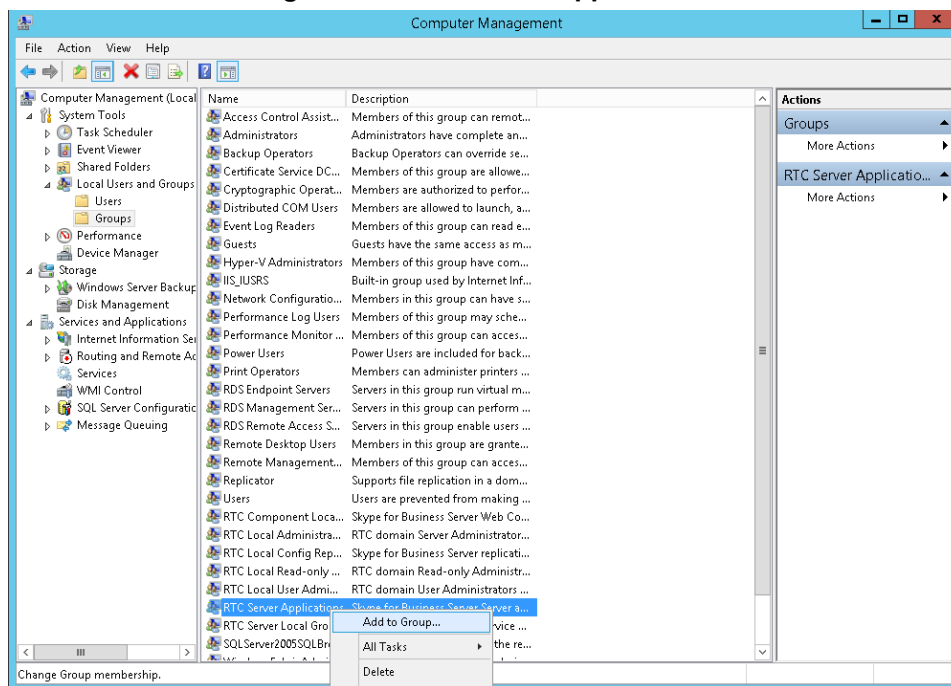
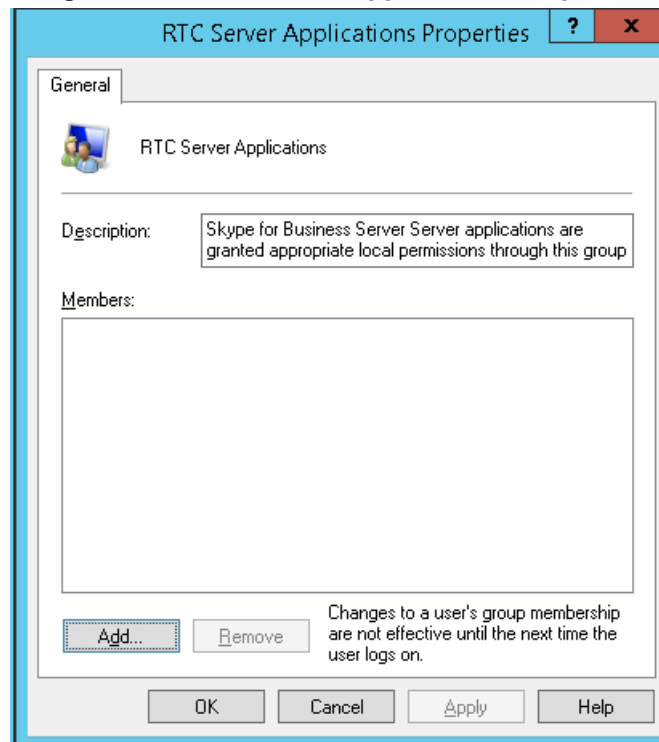
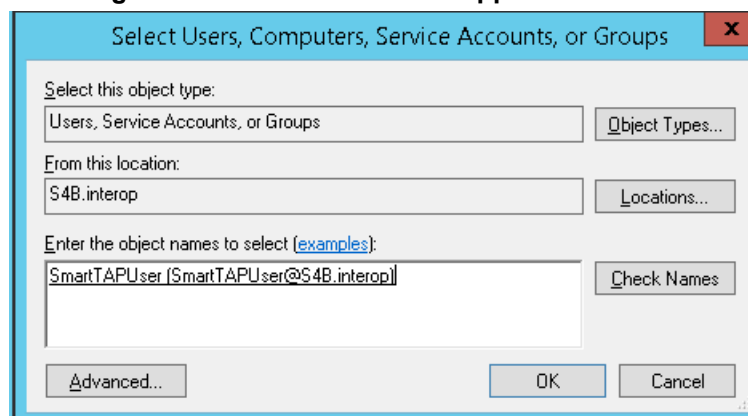


Figure 8-14: RTC Server Applications Properties

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

Figure 8-15: 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 8-16: Local Security Policy

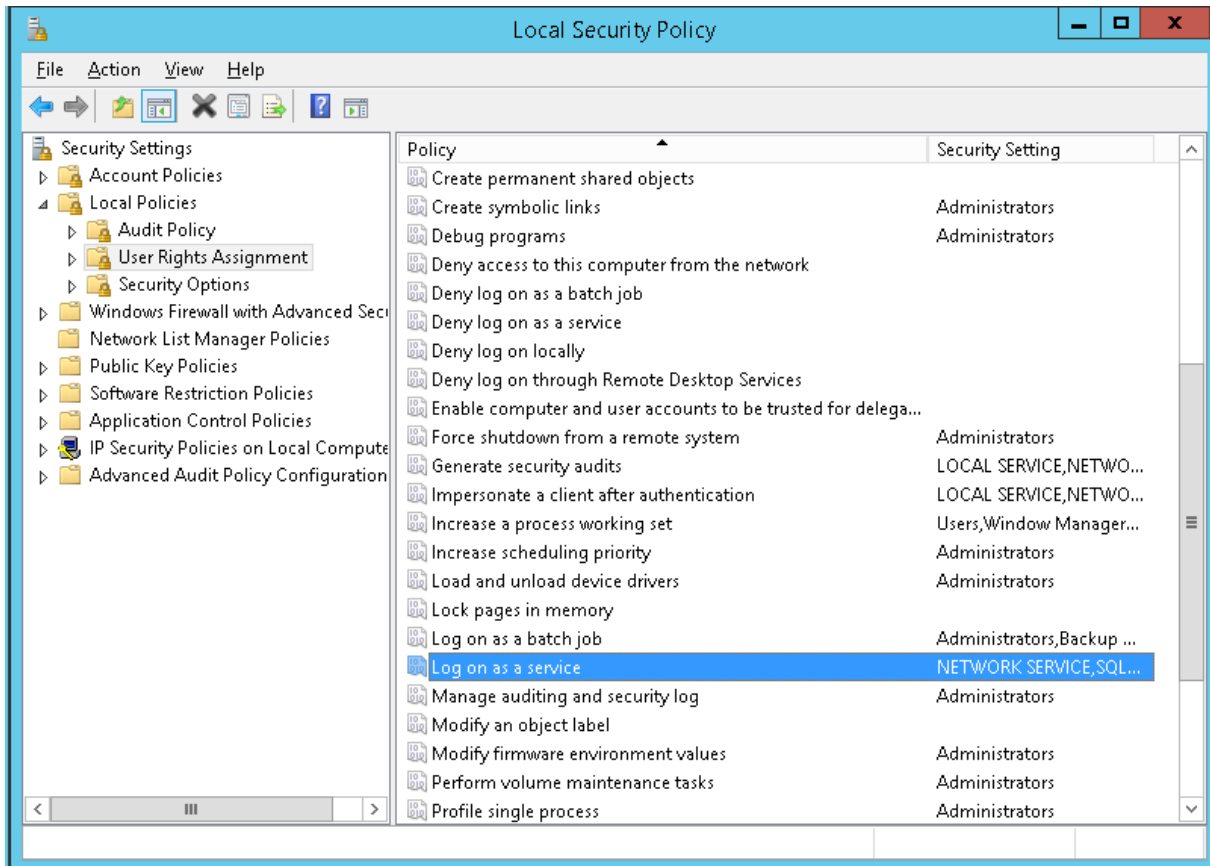
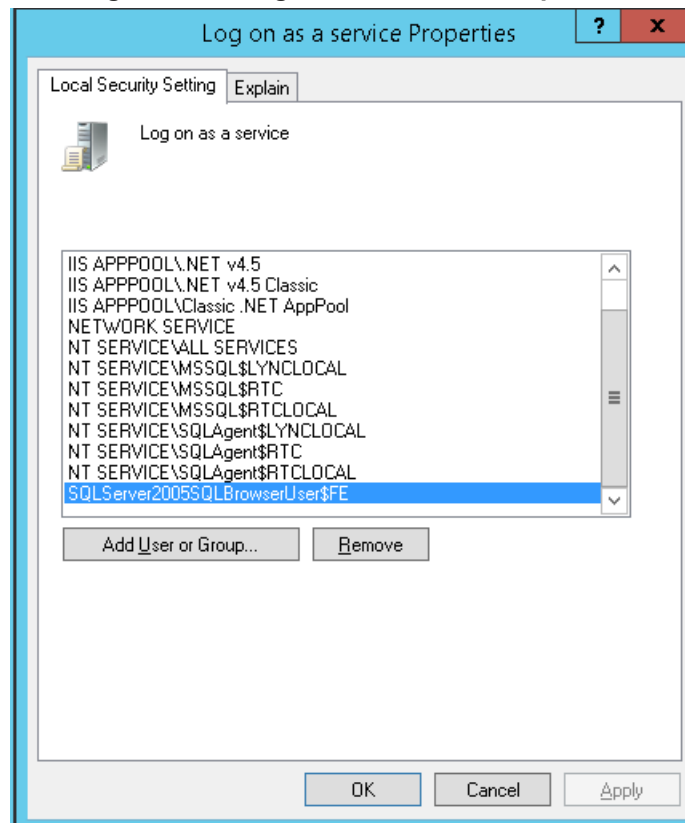


Figure 8-17: Log on as a service Properties



4. Assign the SmartTAP 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.

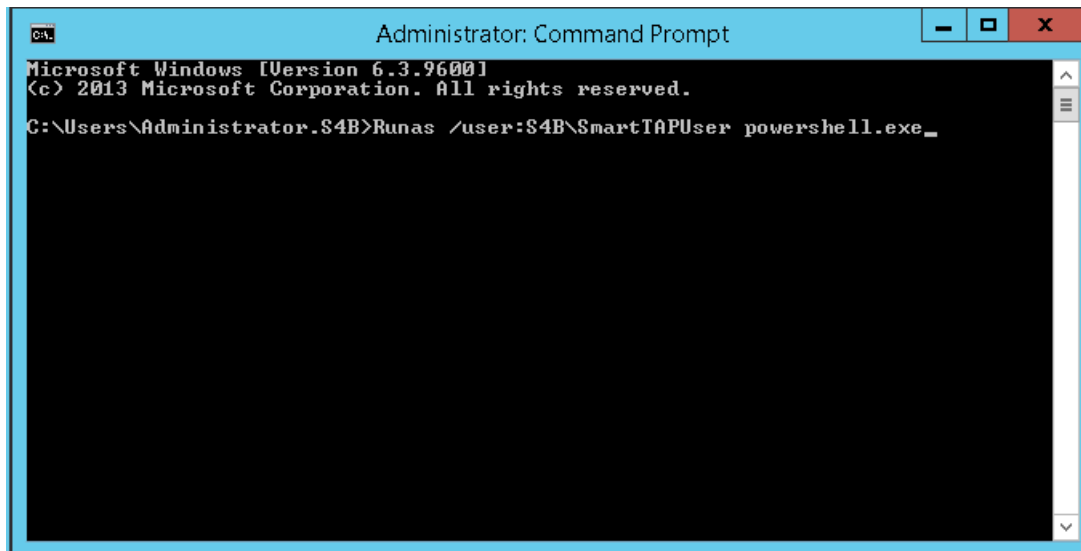
- a. Run PowerShell as the "SmartTapUser" that you defined on the Domain Controller using one of the following methods:

- ◆ **Command line:**

1. Enter the following command and press enter:

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

Figure 8-18: SmartTAP User



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

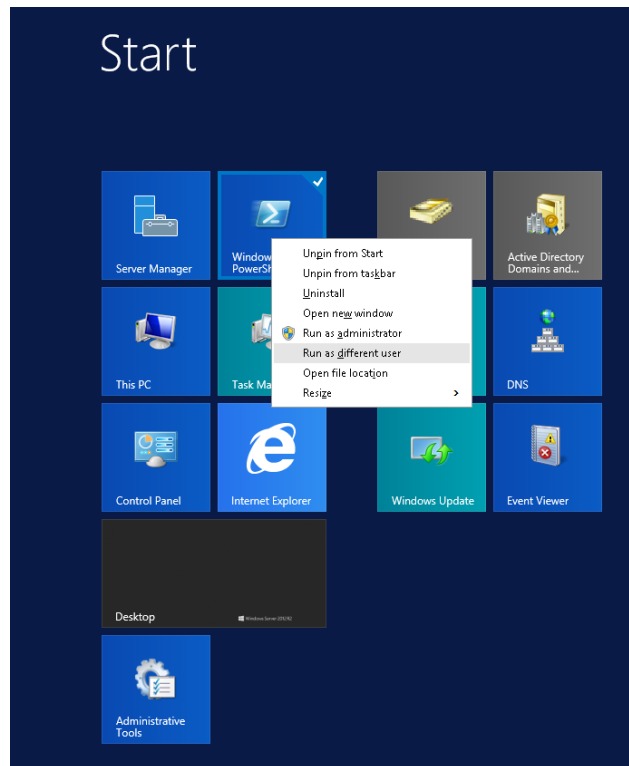


Note: If the SmartTAP username contains spaces, ensure that you insert quotation marks at the beginning and end of the user name string in the command line e.g. "SmartTAP User".

◆ **Using PowerShell:**

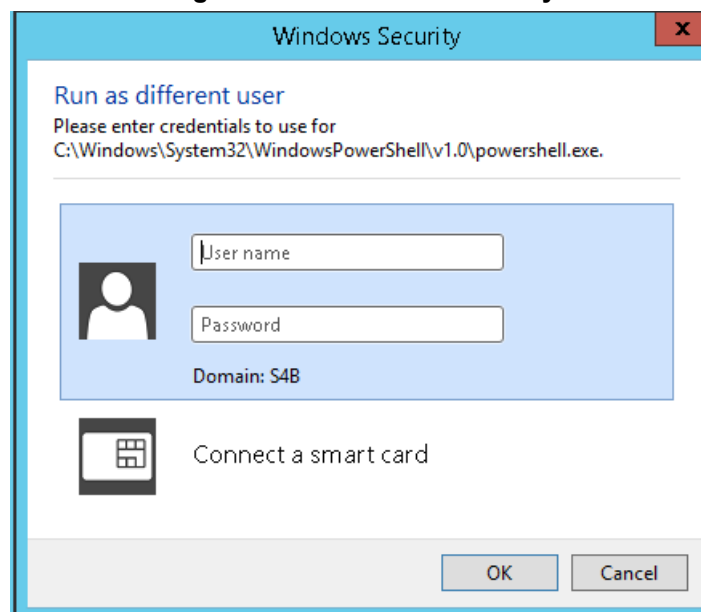
1. On the Domain Controller in the Start menu, right-click the Windows PowerShell icon and choose **Run as different user**:

Figure 8-19: Start Menu



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

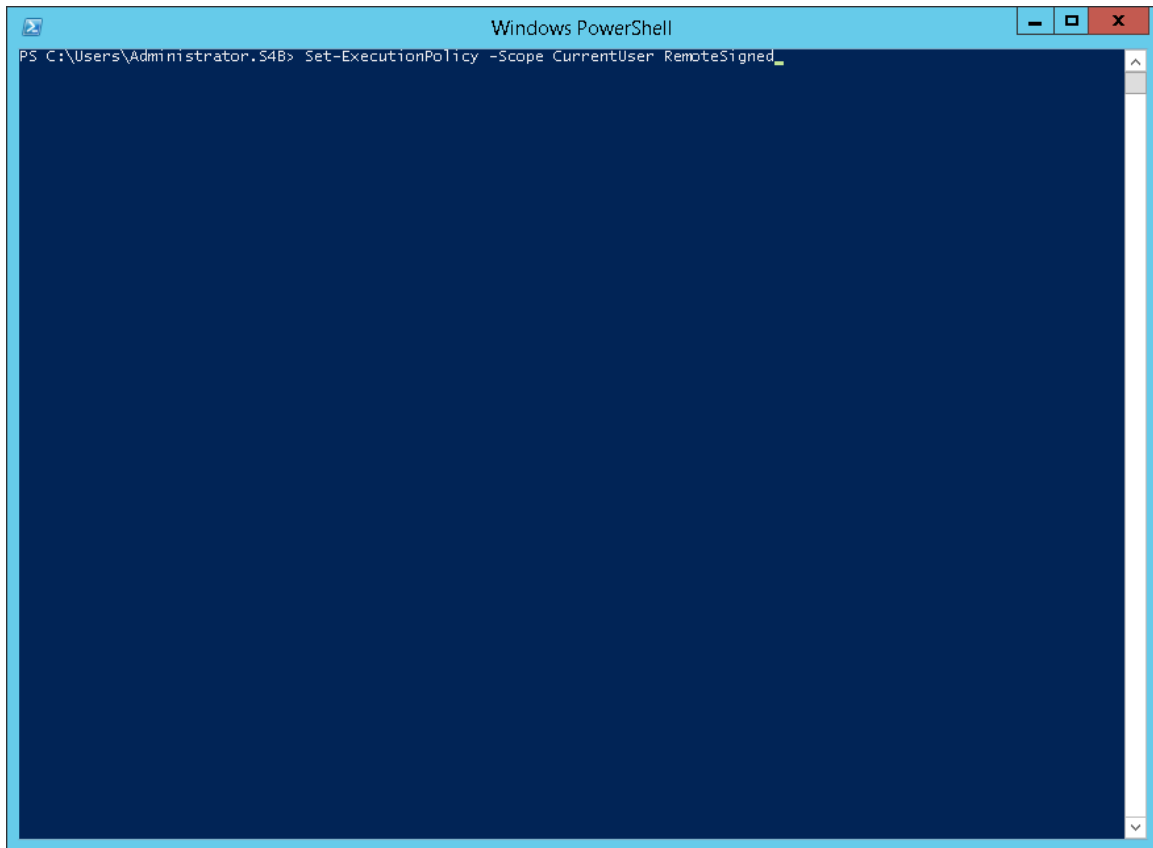
Figure 8-20: Windows Security



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

```
Set-ExecutionPolicy -Scope CurrentUser RemoteSigned
```

Figure 8-21: Windows PowerShell



Note: 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.

8.1.1.2 Install Procedure

This section describes the procedure for installing the plugin.

➤ **To install the plugin:**

1. Copy the Skype for Business installation application **SmartTAP <Plugin_type> Plugin Setup** to the FE, SBS or SBA desktop.

Where <Plugin_type> is one of the following:

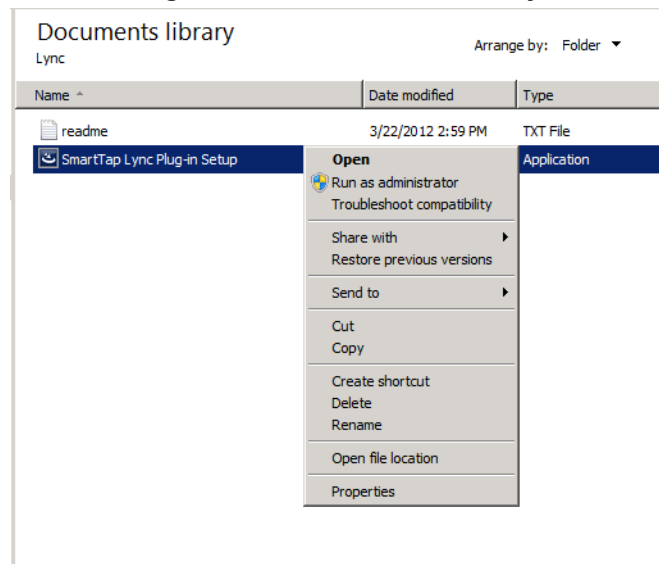
- Lync2010
- Lync2013
- Skype for Business



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

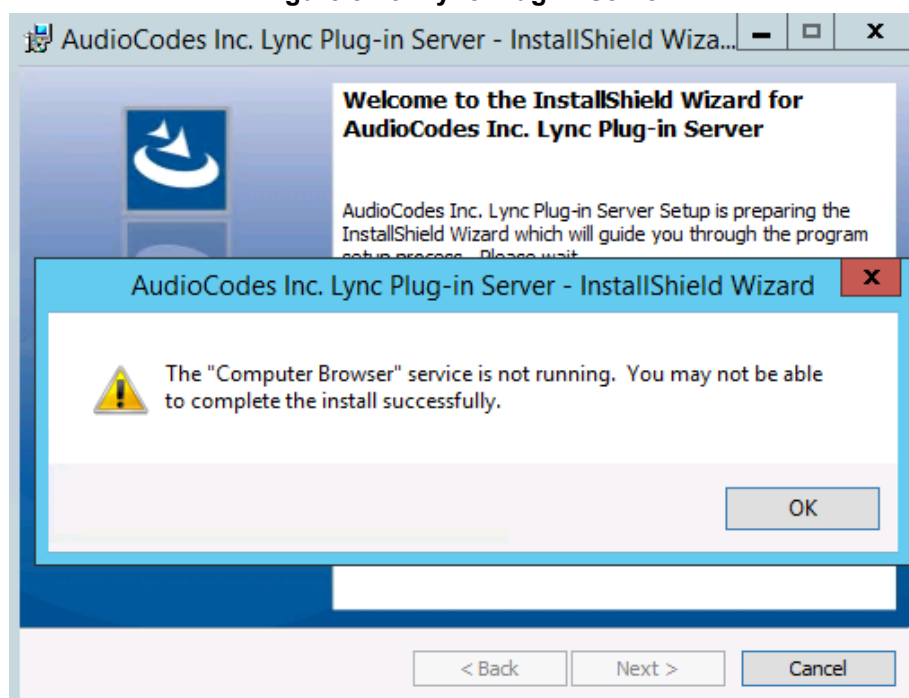
2. Right-click on the file and select **Run as Administrator**.

Figure 8-22: Documents Library



3. 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.

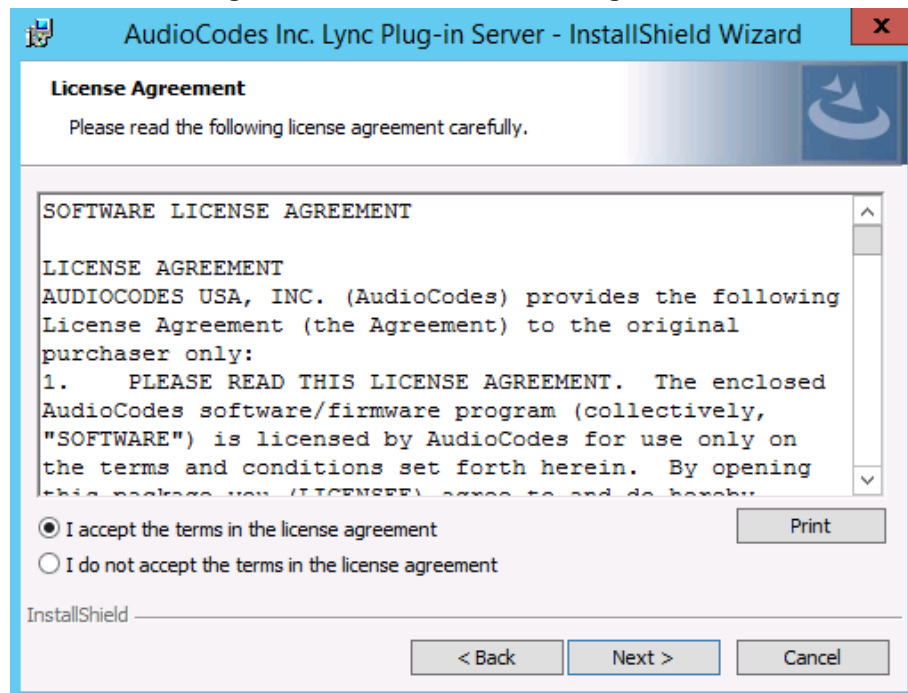
Figure 8-23: Lync Plug-in Server



4. Click **Next** to continue.

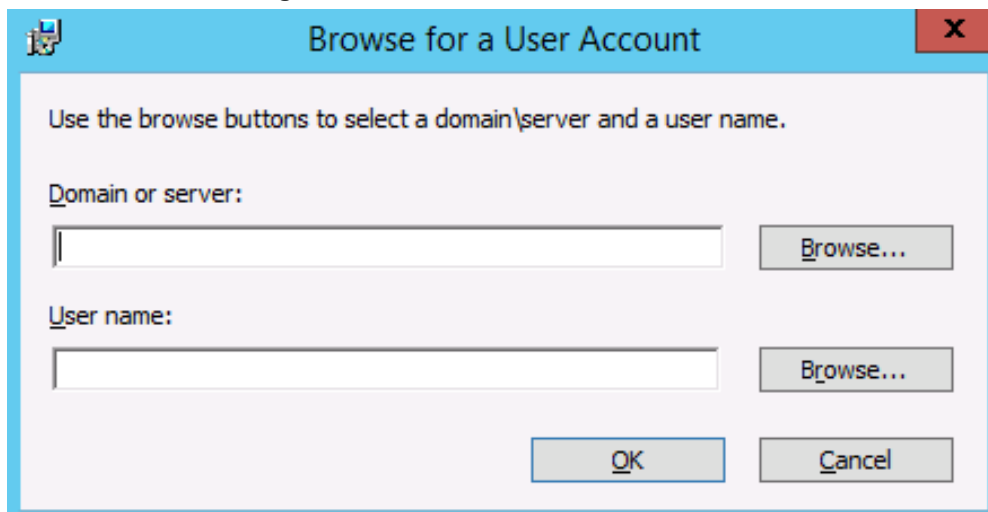
5. Click the **I accept the terms in the license agreement** radio button, and then click **Next**.

Figure 8-24: Software License Agreement



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 8-25: Browse for a User Account



7. Click **Next** to continue.

Figure 8-26: Logon Information

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:

Password:

InstallShield

< Back Next > Cancel

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

Figure 8-27: Lync Plug-in Registrar Select

AudioCodes Inc. Lync Plug-in Server

Lync Plug-in Registrar Select

Your account information has been validated, please select the host or pool that the service will register with.

▼

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 installation, otherwise leave the fields empty.

Figure 8-28: Media Proxy Server Configuration

The screenshot shows the 'Media Proxy Server Configuration' window. The title bar reads 'AudioCodes Inc. Lync Plug-in Server'. The window has a blue header with the title and a close button. Below the header, there is a sub-header 'Media Proxy Server Configuration' and a note: 'If you plan or have Media Proxy servers, enter their details here. Otherwise click Next.' The main area contains the instruction 'Add all Media Proxy Server IP addresses to list'. On the left, there is a text box labeled 'Media Proxy Server IP address' with a vertical cursor. To its right are two buttons: '>>' and '<<'. To the right of these is a large empty rectangular box labeled 'IP Addresses:'. At the bottom left, there is a label 'InstallShield'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

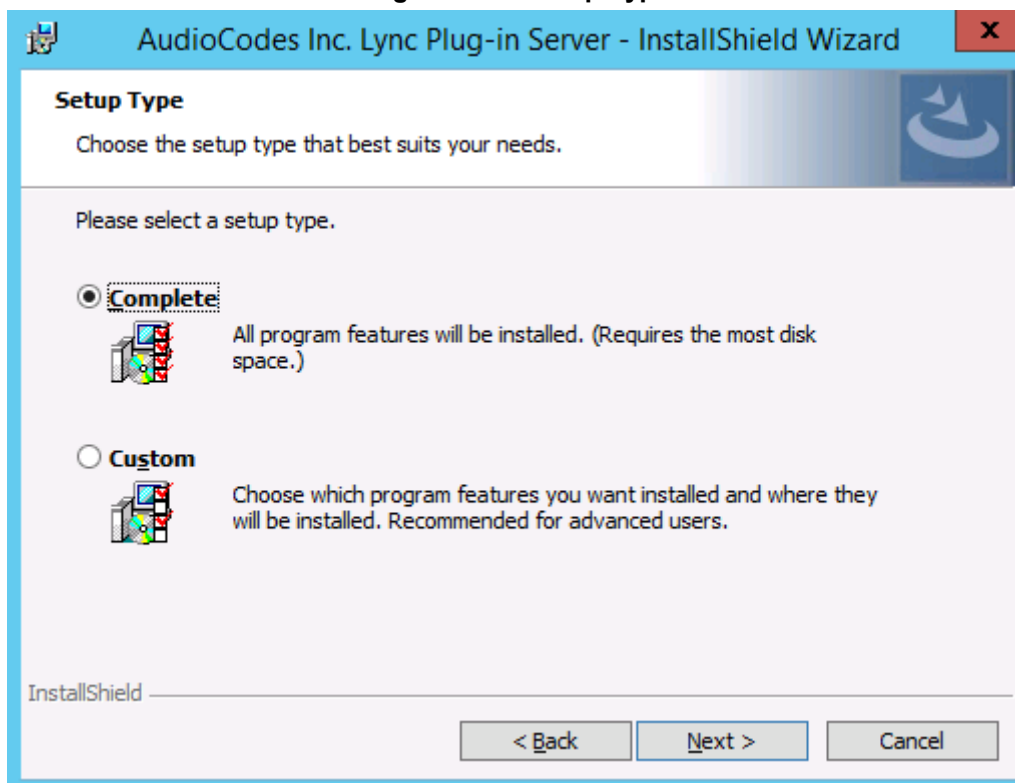
11. Click **Next**.
12. Enter IP addresses of Announcement servers in case SmartTAP Announcement servers are installed, otherwise leave the fields empty.

Figure 8-29: Announcement Server Configuration

The screenshot shows the 'Announcement Server Configuration' window. The title bar reads 'AudioCodes Inc. Lync Plug-in Server'. The window has a blue header with the title and a close button. Below the header, there is a sub-header 'Announcement Server Configuration' and a note: 'If you plan or have Announcement servers, enter their details here. Otherwise click Next.' The main area contains the instruction 'Add all Announcement Server IP addresses to list'. On the left, there is a text box labeled 'Announcement Server IP address' with a vertical cursor. To its right are two buttons: '>>' and '<<'. To the right of these is a large empty rectangular box labeled 'IP Addresses:'. At the bottom left, there is a label 'InstallShield'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

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.

Figure 8-30: Setup Type



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



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

8.1.1.3 Plugin Configuration

In some cases, it may be necessary to modify the “LyncPlugIn.exe.config” file after the install is complete. Restart the plugin after any changes are made to the configuration file.

The following table outlines the configuration options:

Table 8-1: Plugin Configuration Options

Variable	Value	Description
CONFIG_PORT	Default = “9901”	Default TCP listening port on the Skype for Business plugin for configuration from CD
BLACKLIST_CODECS	Default = “117,116”	Used for removing unsupported codecs from the list of codecs for Skype for Business clients

Variable	Value	Description
MASTER_DOMAIN	Default = ""	A comma separated list of domains that if present WILL be used for matching targets.
NON_LYNC_IP	Default = ""	This should be a non-routable IP address in the customer's environment. By default, if no value is specified 192.0.2.0 will be used.
AnnouncementApplicationEndpointUri	Default = ""	Deprecated from version 3.1. Application Service GRUU value. In Power shell type Get-CsTrustedApplication to get the value
ReferredByAddedParamByAnnouncementApp	Default = "X-Announcements=AnnouncementsApp"	Param name and value added to referred-by header value when EnableAnnouncements is True.
EnableAnnouncements	Default = "False"	True/False to enable Announcement Server for Skype for Business
RecordAnnouncements	Default = "False"	Set true to record incoming call to announcement server
RecordAnnouncementOutCall	Default = "False"	Set true to record the call that AN server initiates to target user
RecordPstnCallsOnly	Default = "False"	Set true to record meta-data of targeted users' calls with PSTN participants only. Note that a conference conversation for a PSTN call elevated to the conference will not be recorded in this configuration.
RecordExternalCallsOnly	Default = "False"	Set true to record calls of targeted users with external parties (PSTN, federation)
AnnouncementCallType	Default = "InboundExternal"	Set the call type to play announcement to InboundExternal/OutboundExternal/AllExternal
CdLbCheckConnectivityMilisec	Default = "5000"	Plug-in checks connectivity to Call Delivery components registered to receive copy of signaling.
MpLbCheckConnectivityMilisec	Default = "5000"	Plugin checks connectivity to Media Proxy servers in the set time intervals (milliseconds). The parameter is applicable when "MediaProxyServersList" value set with one or more IP addresses.
AnnLbCheckConnectivityMilisec	Default = "5000"	Plugin checks connectivity to Announcement servers in the set time intervals (milliseconds). The parameter is applicable when "AnnouncementServersList" value set with one or more IP addresses.

Variable	Value	Description
MediaProxyServersList	Default = ""	Comma separated list of Media Proxy server IP addresses. When more than one IP address is set, Plugin applies round robin algorithm to distribute the targeted to be recorded calls' media between the servers. Plugin's installer populates the parameter's value when entered during its installation. Example: "10.21.80.121:10123,10.21.80.123:10123"
AnnouncementServersList	Default = ""	Comma separated list of Announcement server IP addresses. When more than one IP address is set, Plugin applies round robin algorithm to distribute the targeted to be recorded calls' between the Announcement servers. Plugin's installer populates the parameter value when entered during its installation. Example: "10.21.80.121:10124,10.21.80.124:10124"
RecordIM	Default = "True"	Set to false to disable instant messaging recording
UserAgentBlackList	Default = ""	Comma separated list of the user agents which should not be recorded
AnnouncementBlackList	Default = "911"	Comma separated list of destination numbers or user names which should not be routed to ANN server.
BlockCallAnnNotAvail	Default = "False"	Set true to disconnect calls when there is no announcement server available to play an announcement to the call parties
normalizeNumbers	Default = "False"	The parameter should be set to true when normalization of called numbers in the Announcement server is required.
asList		Contains comma separated Application Server list. The list should contain one Application Server (AS) address with exception to deployment of the Media Proxy in SmartTAP Active/Active Configuration. This deployment should include addresses of both AS servers.

Variable	Value	Description
StripAppSharingRdp	default ="DontRemove"	<p>During desktop application sharing session, determines whether to remove the RDP part from the SDP. Possible values:</p> <ul style="list-style-type: none"> • Don't Remove: don't remove the RDP part from the SDP message. All messages contain RDP and for Skype for Business 2016 clients and later, VBSS as well. When recording a desktop application and this value is configured, for specific scenarios such as when the recorded user has given control to another party, the Desktop Sharing recording will stop and the following alarm is triggered "Failed to allocate system resource Desktop Sharing call won't be recorded" • Remove Video Exist: For Skype for Business 2016 clients and later, removes the RDP part (leaving only the VBSS part in the SDP message). When recording a desktop application and this value is configured, some features like giving control won't be available, Desktop Sharing will not be recorded in cases the call uses RDP (clients older than 2016) and the following alarm is triggered "Failed to allocate system resource Desktop Sharing call won't be recorded" • AlwaysRemove: always remove the RDP part from the SDP message. When this value is configured, you will not be able to grant control to someone else during a Desktop application recording session.

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

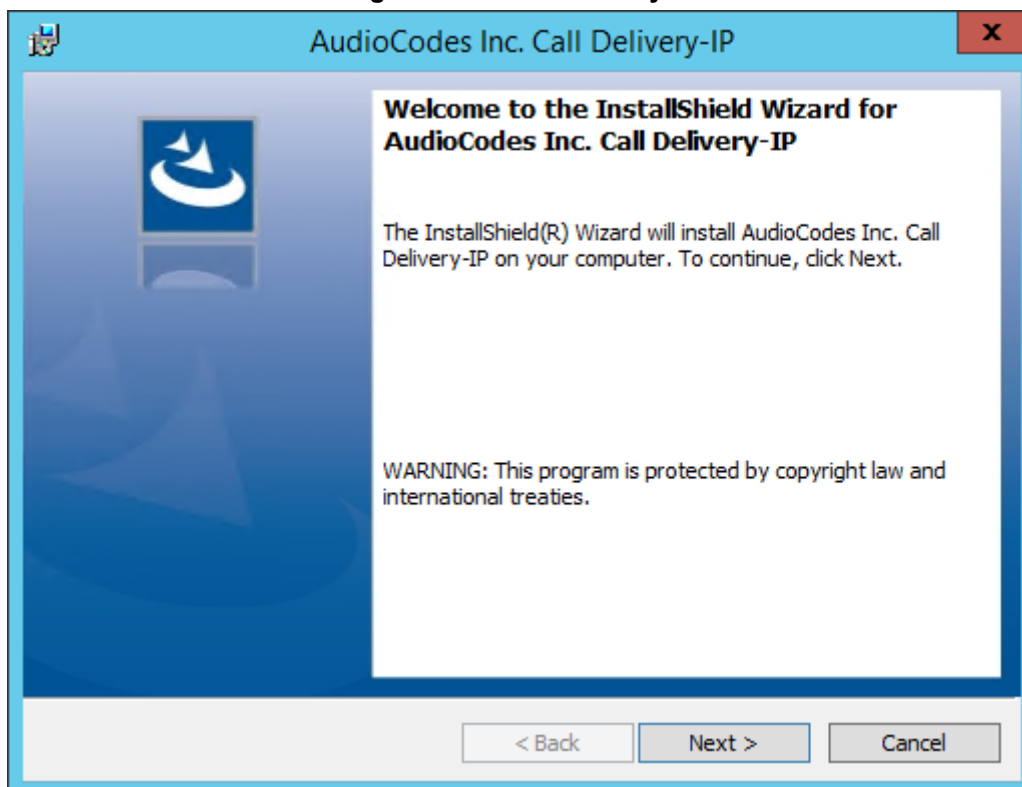


Note: It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter 7 on page 63.

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

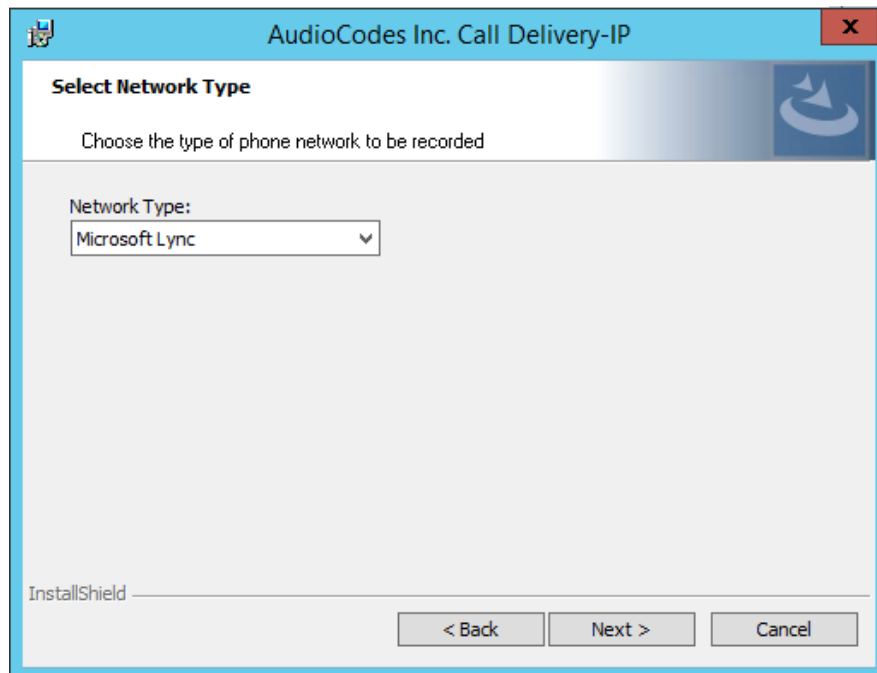
1. Click **Next** to continue.

Figure 8-31: Call Delivery-IP

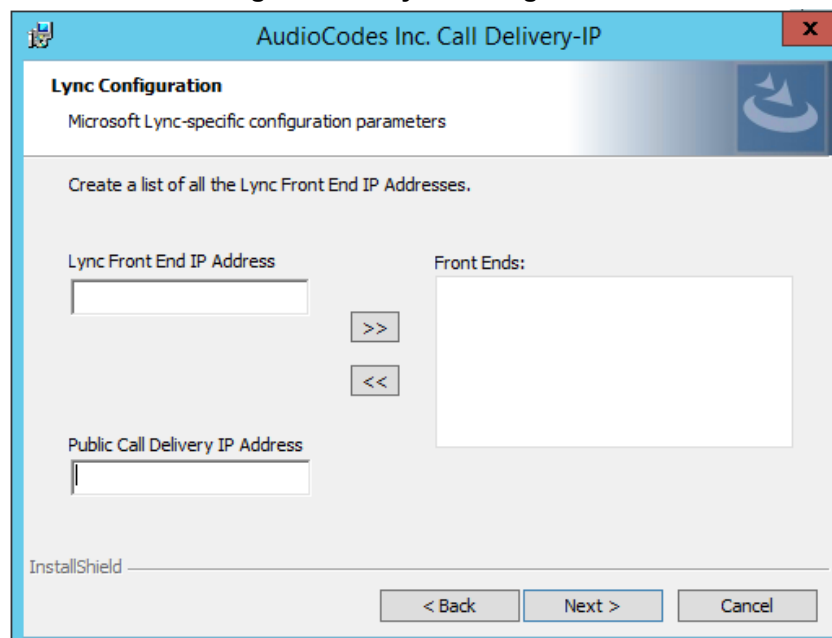


Assuming you are setting up for a Skype for Business installation, select “Microsoft Lync” when prompted for the network type.

2. Click **Next** on the Server IP Setup.

Figure 8-32: Network Type

3. 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 “SmartTAP 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.

Figure 8-33: Lync Configuration

6. To capture the audio:
 - Monitoring (Capture SRTP from Mediation, Conference servers or Port Mirroring) - See Section 8.1.2.1 on page 96:
 - ◆ Local – Port Mirroring
 - ◆ Remote – Conference or Mediation Server
 - Edge (Capture SRTP from Edge server) See Section 8.1.2.2 on page 100
 - Media Proxy (Capture SRTP from the SmartTAP Media Proxy server) See Section 8.1.2.3 on page 101.
7. Click **Next** to select the Recording Type.

8.1.2.1 Monitoring

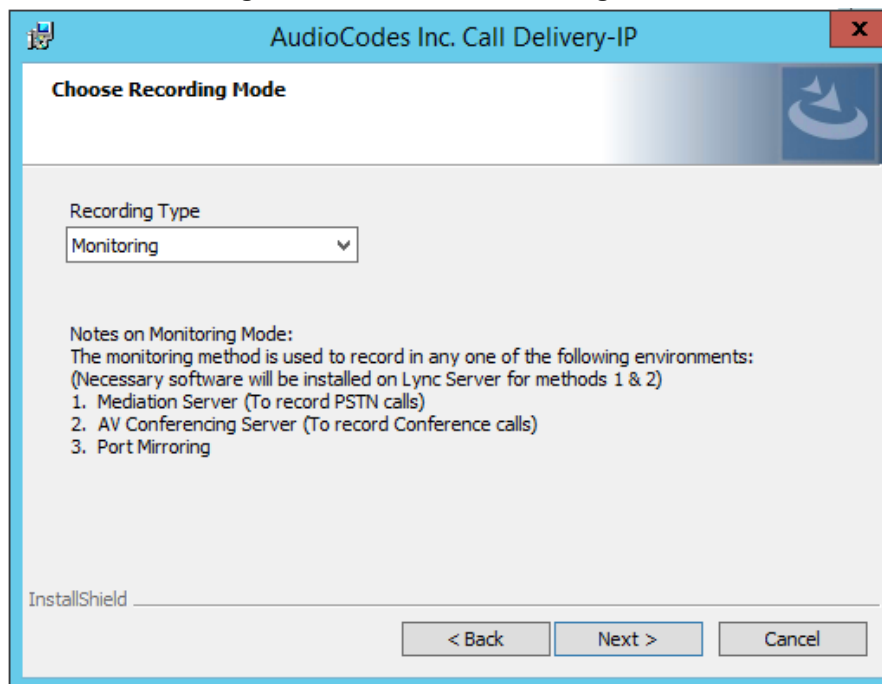
This section describes how to configure the location for capturing monitored recording:

- **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.

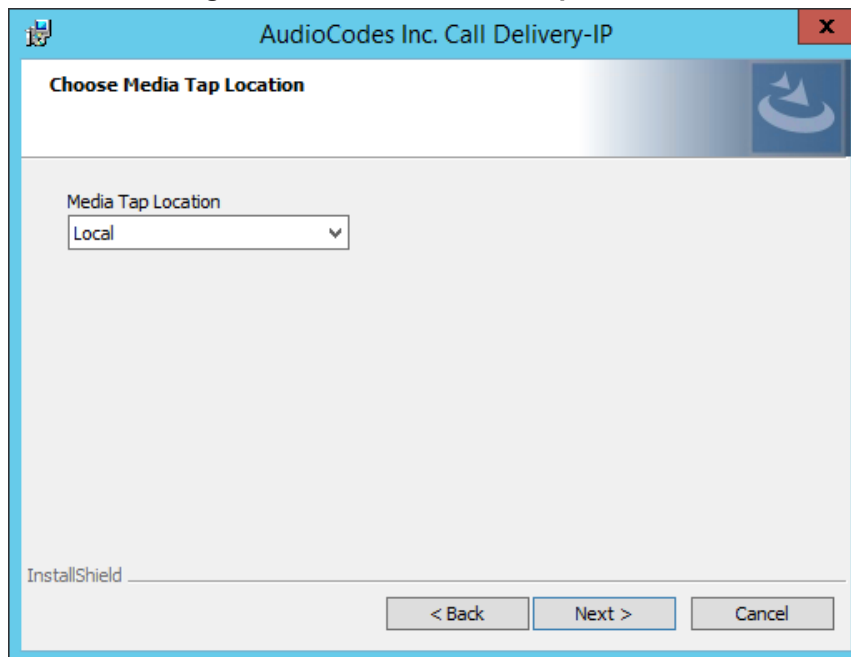
➤ **To capture monitored recordings locally:**

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

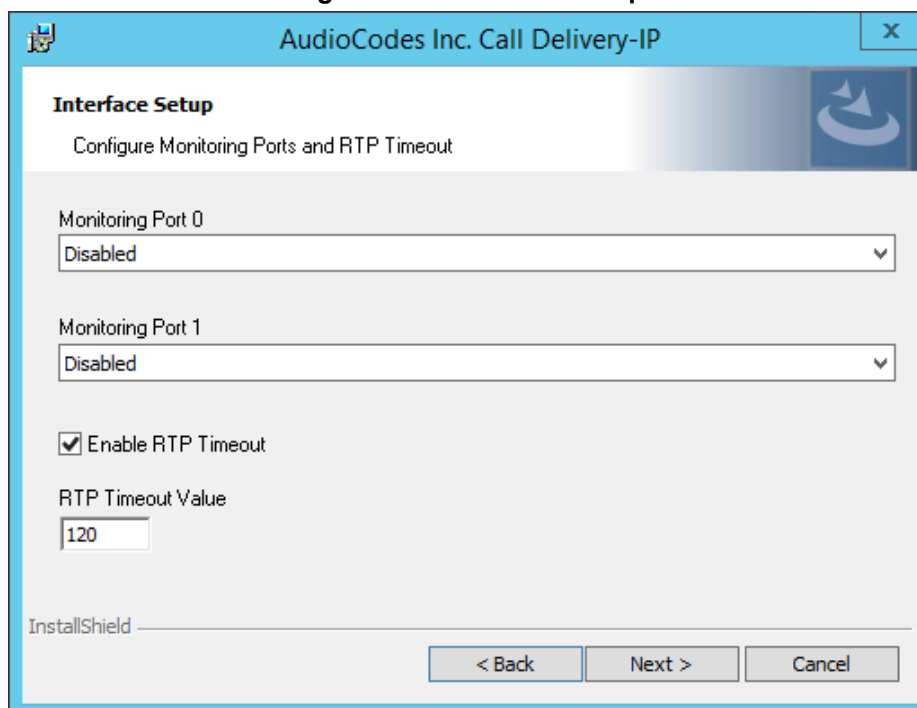
Figure 8-34: Choose Recording Mode



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

Figure 8-35: Choose Media Tap Location

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

Figure 8-36: Interface Setup

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 IP address.

Figure 8-37: Server IP Setup

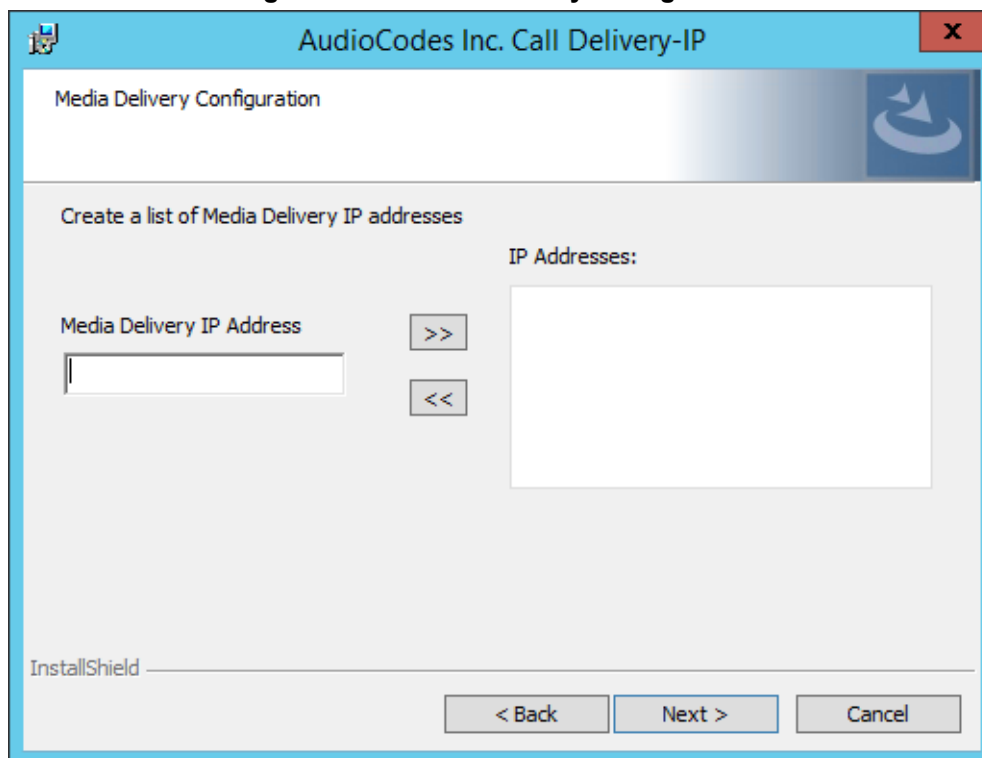
4. Click **Next** on the Server IP Setup.
 5. Click **Next** on the Setup Type screen.
 6. Click **Install** on the install screen.
 7. Click **Finish** to finish.
- **To capture monitored recordings remotely:**
1. From the Media Tap Location drop-down list, select **Remote**.

Figure 8-38: Choose Media Tap Location

2. Specify the IP Address of the Media Delivery Host machine and click >> to add it to the IP Address list.

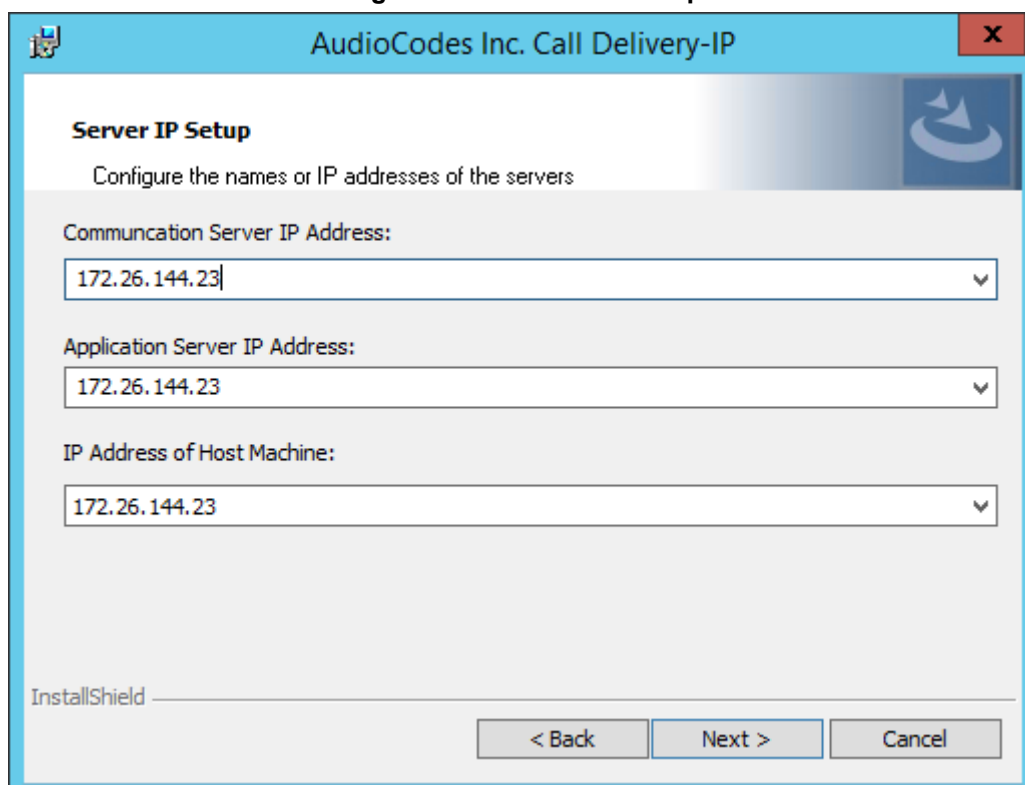
3. Repeat for each Host machine where Media Delivery is installed.

Figure 8-39: Media Delivery Configuration



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 IP address.

Figure 8-40: Server IP Setup



4. Click **Next** on the Server IP Setup.

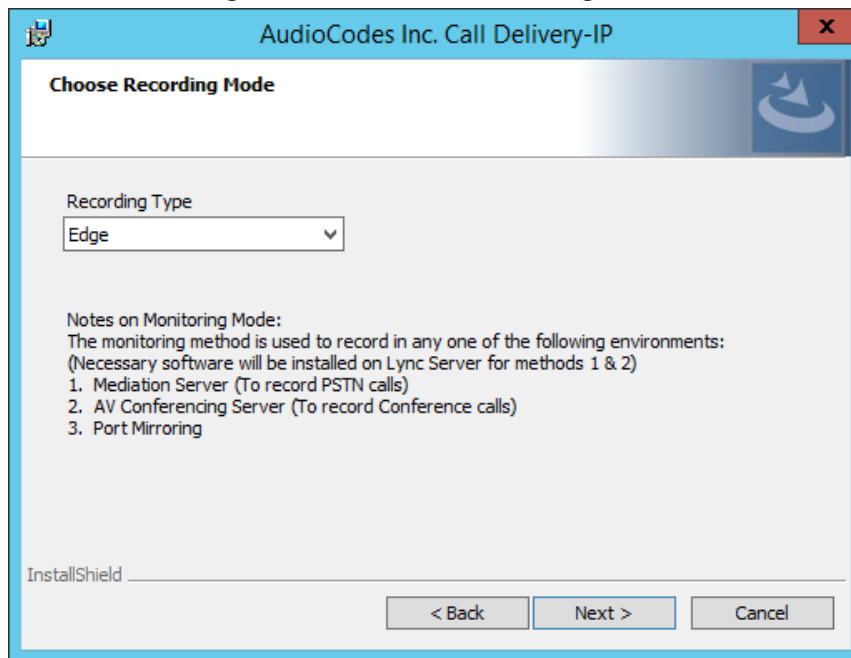
5. Click **Next** on the Setup Type screen.
6. Click **Install** on the install screen.
7. Click **Finish**.

8.1.2.2 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 LYNC environment.

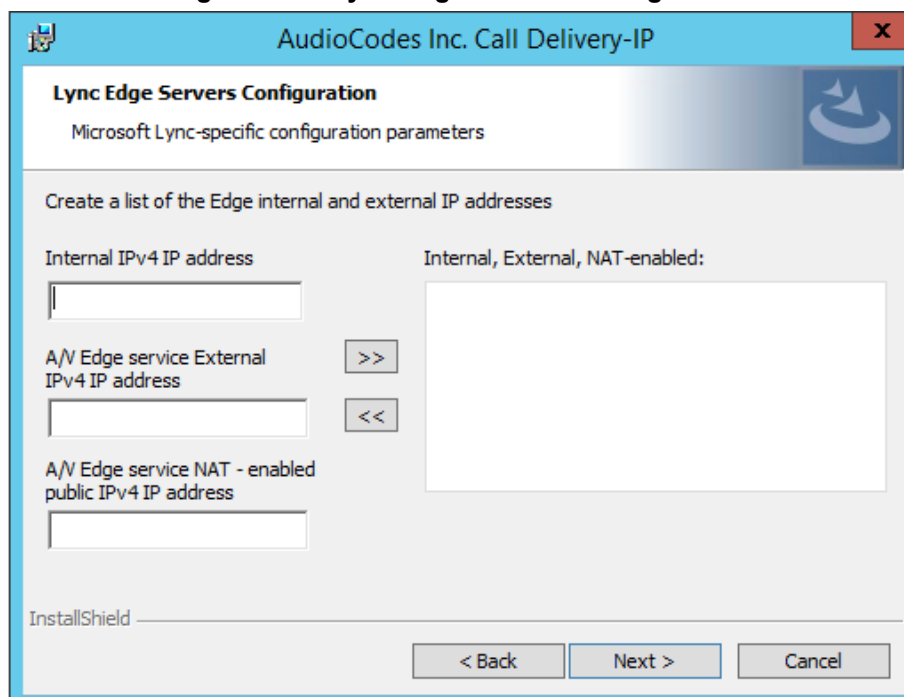
- **To install the Edge server:**

Figure 8-41: Choose Recording Mode



1. Click **Next** to select Record Type “**Edge**”.

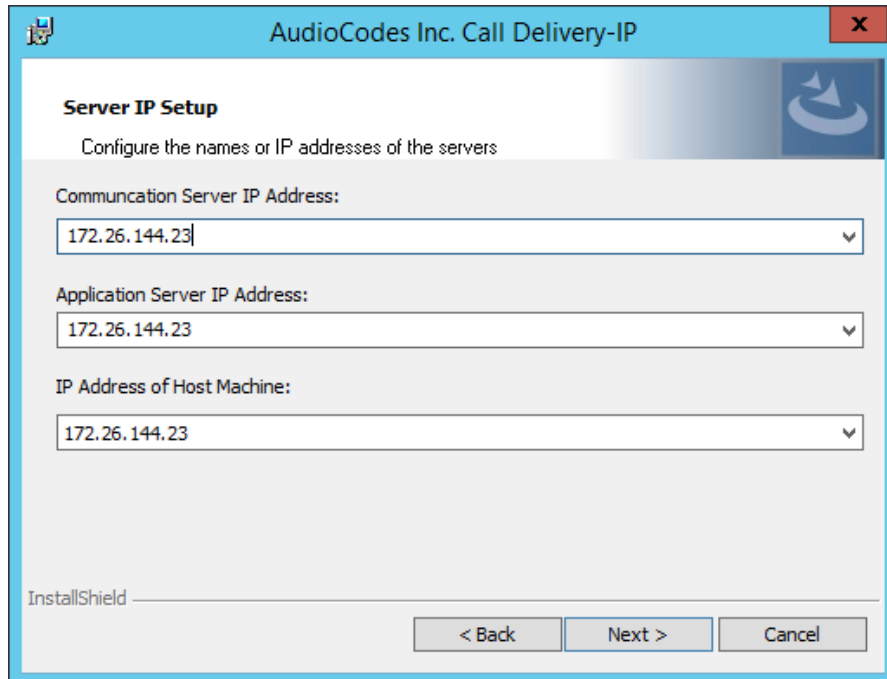
Figure 8-42: Lync Edge Servers Configuration



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 IP address.

Figure 8-43: 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**.

8.1.2.2.1 Firewall Exceptions

Firewall exceptions are **REQUIRED** for this solution to work. Please refer to Chapter 7 on page 63 for the required exceptions.

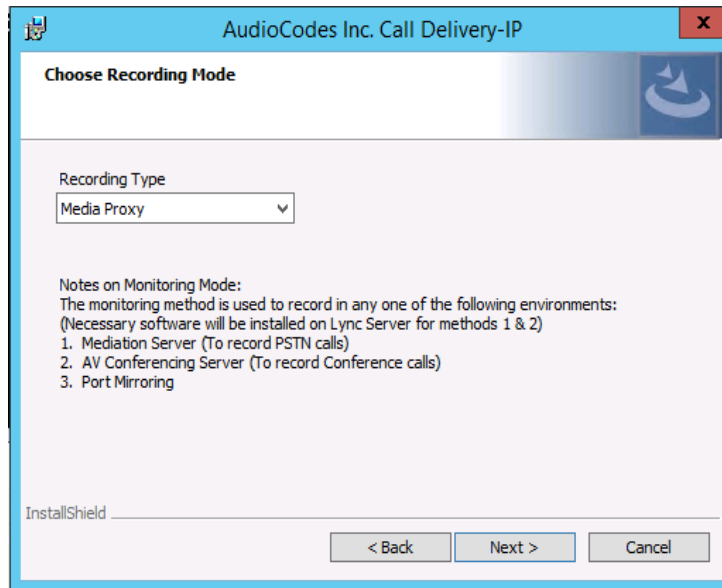
8.1.2.3 Configuring Media Proxy for Call Delivery-IP

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

➤ **To configure Media Proxy for Call Delivery-IP:**

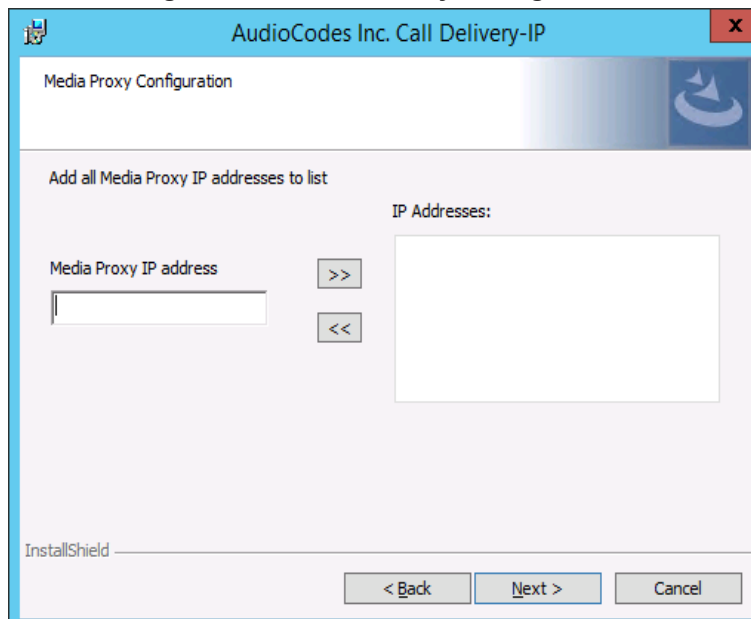
1. Select the Media Proxy recording type.

Figure 8-44: 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 8-45: Media Proxy Configuration



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.

4. Provide the Internal & External Edge IP.
5. Add the NAT IP if configured.

Figure 8-46: Lync Edge Servers Configuration

AudioCodes Inc. Call Delivery-IP

Lync Edge Servers Configuration
Microsoft Lync-specific configuration parameters

Create a list of the Edge internal and external IP addresses

Internal IPv4 IP address

A/V Edge service External IPv4 IP address

A/V Edge service NAT - enabled public IPv4 IP address

Internal, External, NAT-enabled:

InstallShield

< Back Next > Cancel

6. Specify the real IP addresses of the SmartTAP Communication Server and Application Server.
7. Select the NIC interface of the local server.

Figure 8-47: Server IP Setup

AudioCodes Inc. Call Delivery-IP

Server IP Setup
Configure the names or IP addresses of the servers

Communication Server IP Address:

Application Server IP Address:

IP Address of Host Machine:

InstallShield

< Back Next > Cancel

8. Select **Complete** setup type, and then click **Next** to continue.
9. Click **Install** to complete installation.

8.1.2.4 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 software installation. Remember to restart the service if any changes are made manually to the voip.cfg file.

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



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

Table 8-2: Description of the Skype for Business Specific Changes

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	
CC	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 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 Server IP
  RECORDINGTYPE=#          # 0 - monitoring(default), 3 - EdgeProxy
  (used on the Edge server), 4 - MediaProxy
  MEDIAPROXYURL=http://IP:10123 # required if RECORDINGTYPE=4
  (MediaProxy)

```


8.1.3 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 Skype for Business plugin on the FE will redirect the targeted SRTP “voice” only to the MP and the MP will send the voice on to the original destination. A copy of the SRTP “voice” call that is traversing the MP is sent to the SmartTAP server for long-term storage.

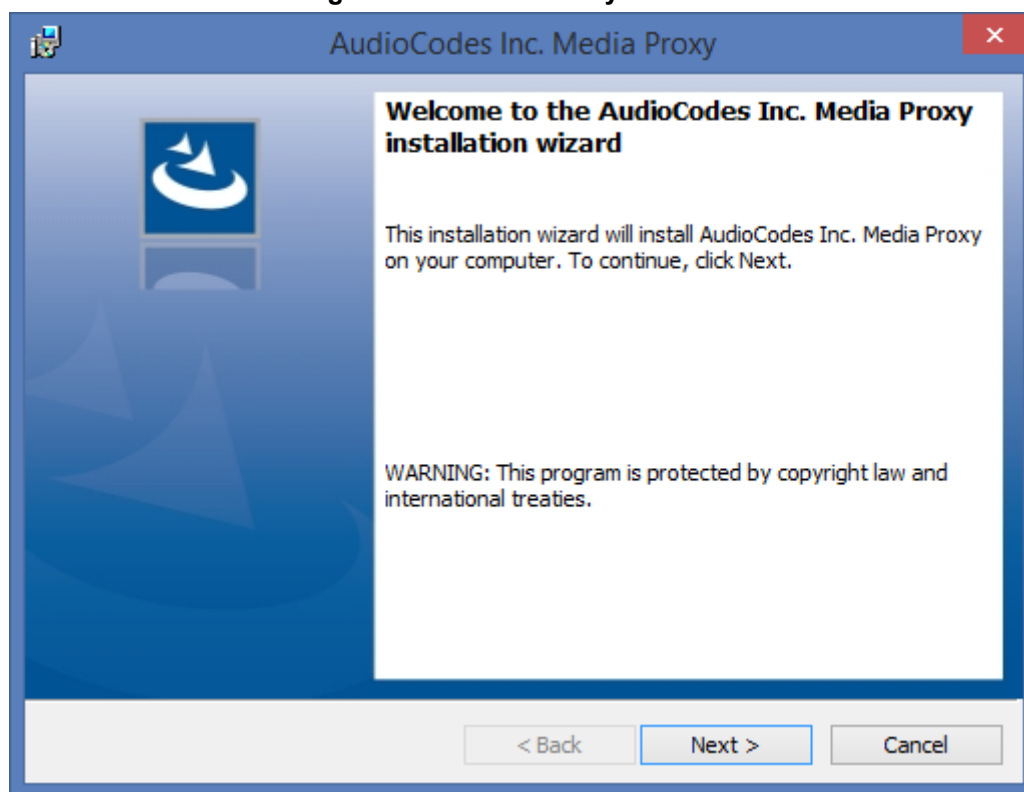


Note: It is highly recommended to configure the Firewall with the required ports to ensure proper communication prior to the software installation. Refer to Chapter 7 on page 63.

➤ **To install the Media Proxy:**

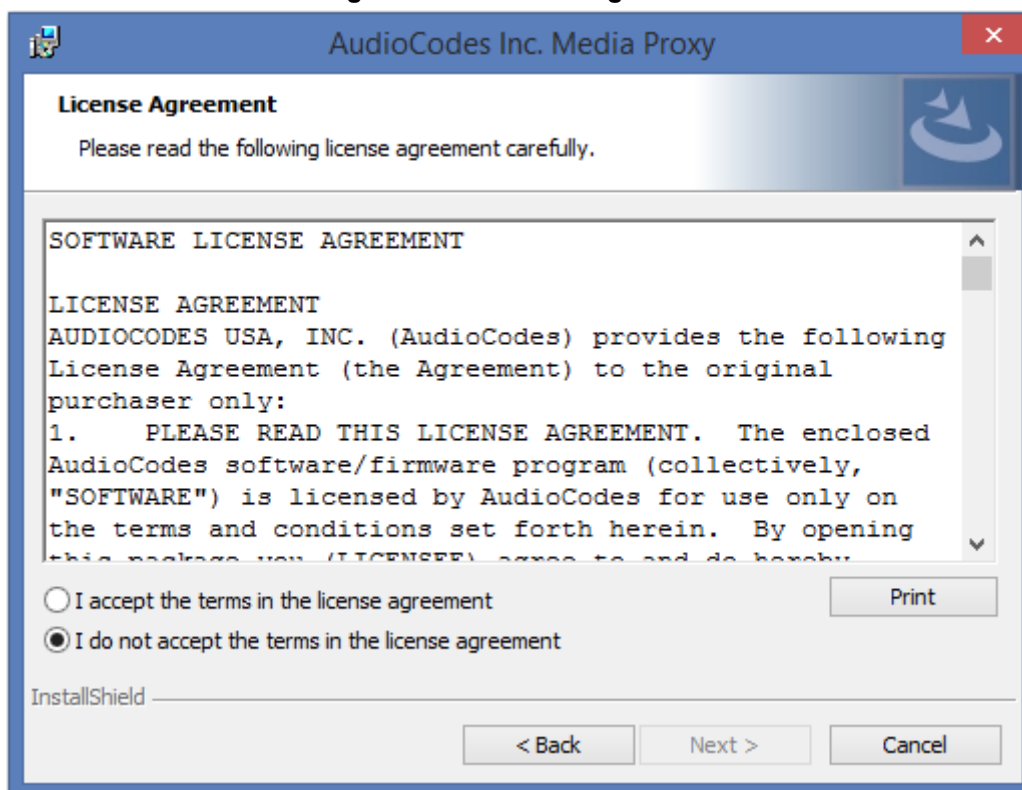
1. When the Media Proxy installation wizard starts, click **Next** to install.

Figure 8-48: Media Proxy Welcome



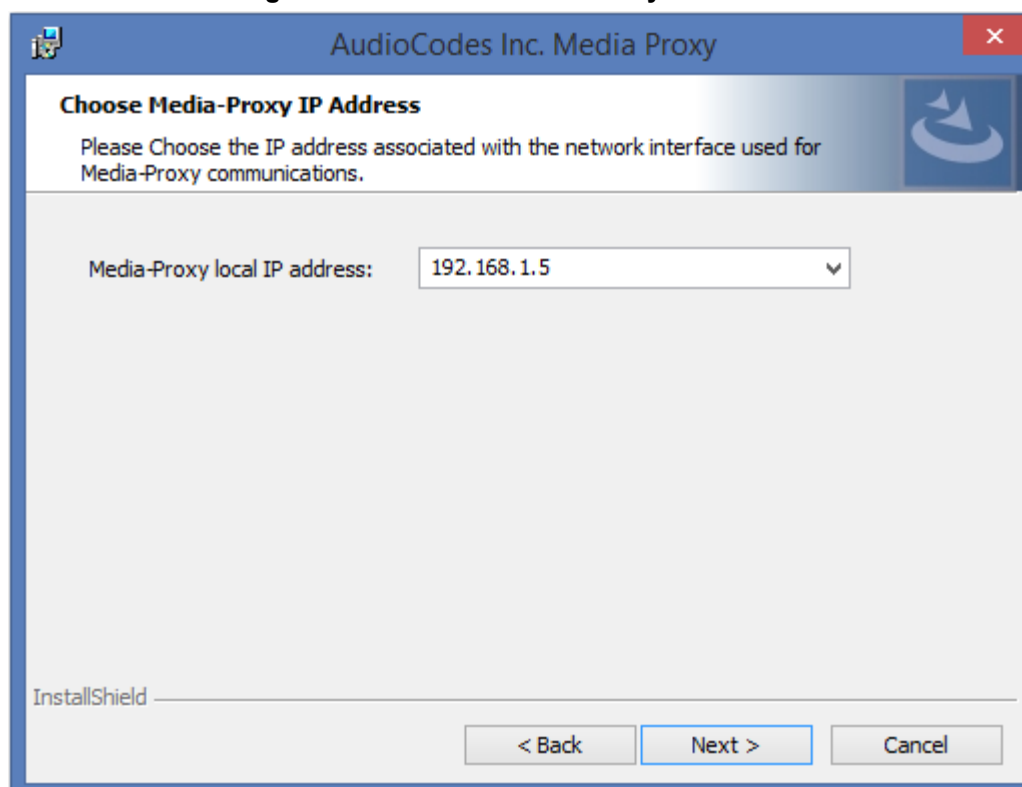
If you are installing from a Suite, the following screen may not be displayed.

Figure 8-49: License Agreement



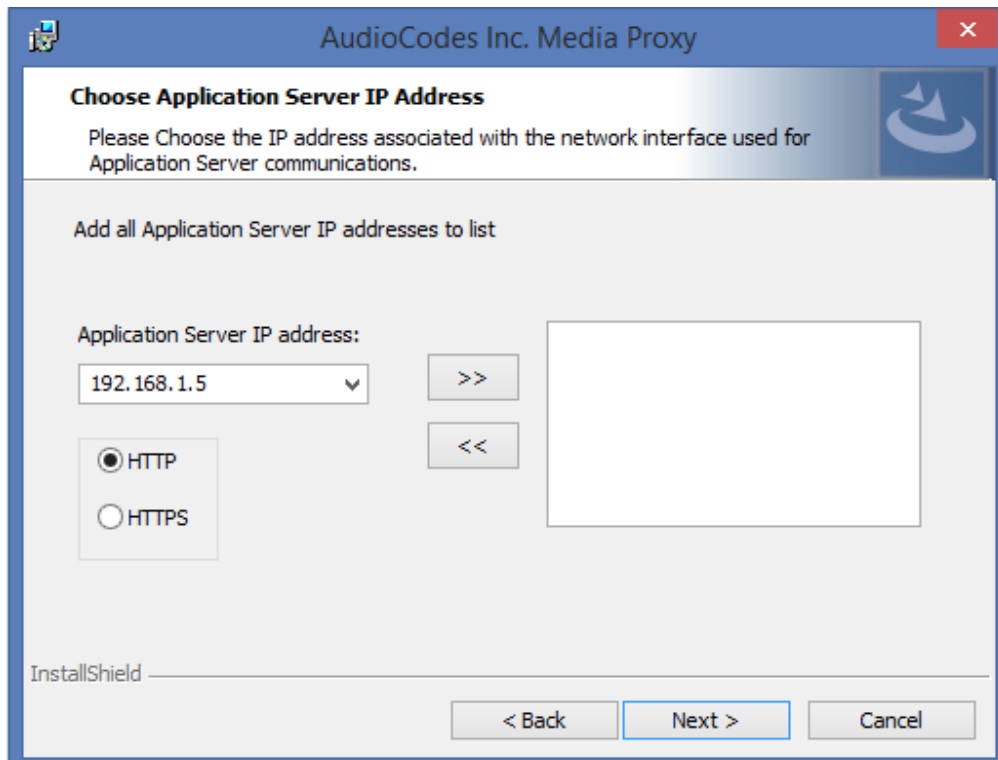
2. Select the "I accept the terms in the license agreement" radio button and click **Next**.

Figure 8-50: 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**.

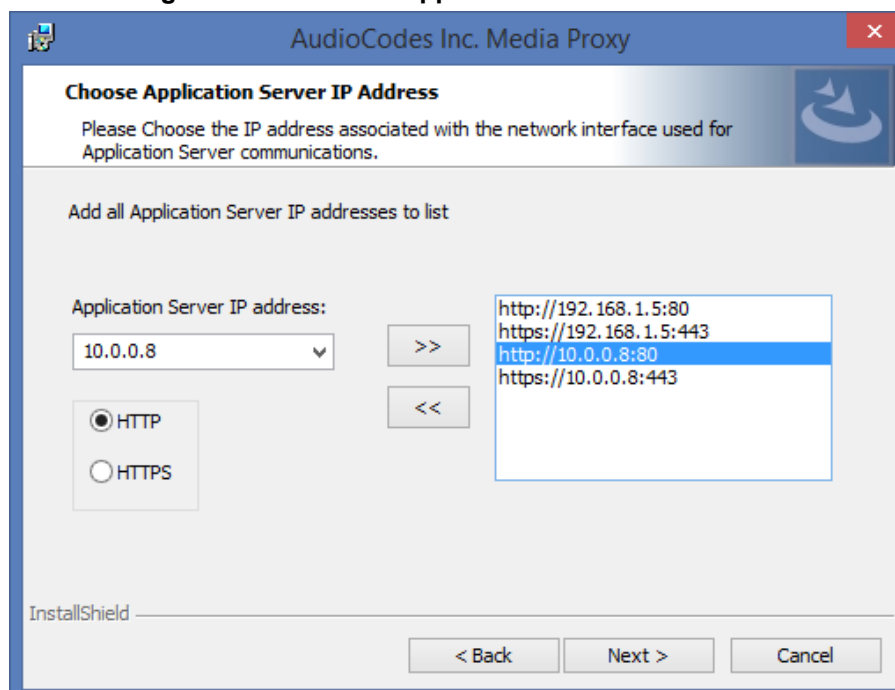
Figure 8-51: Choose Application Server IP Address



4. Configure the 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 remove. At least one entry should be configured. Click **Next** to proceed.

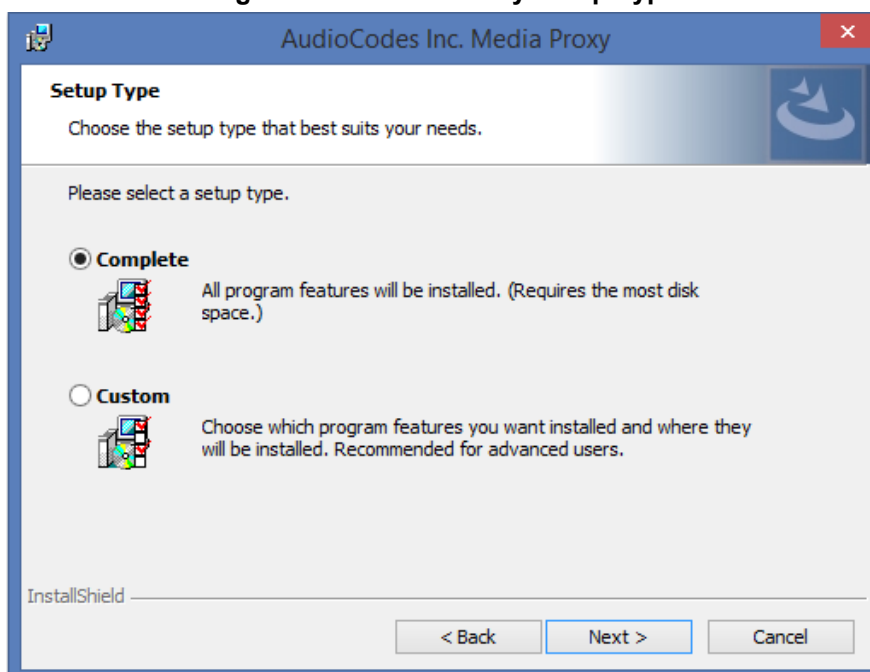
An example configuration is shown in the figure below:

Figure 8-52: Choose Application Server IP Address



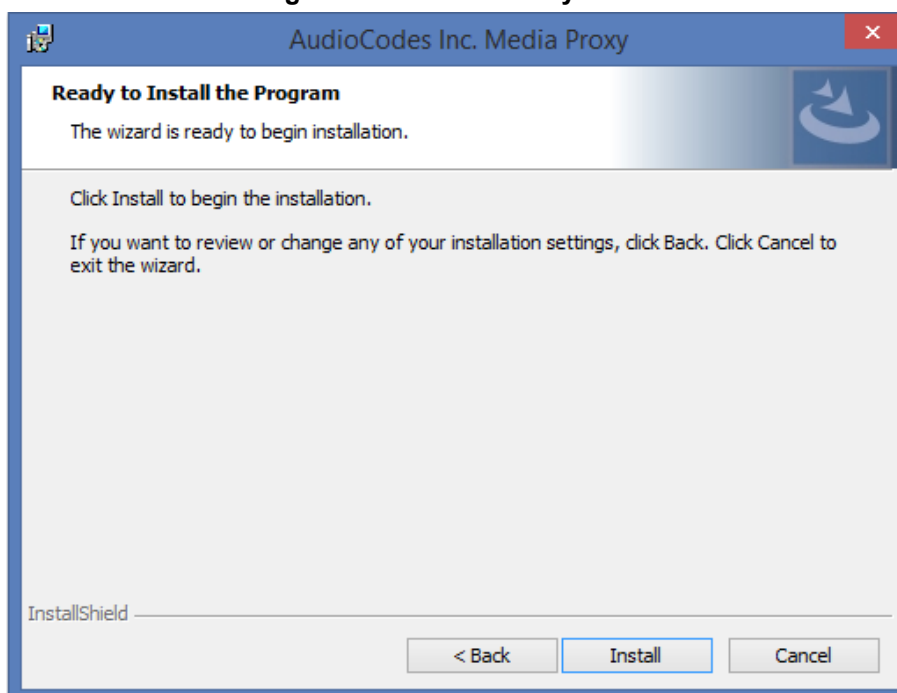
5. When you have completed the configuration, click **Next** to proceed.
If you are performing an upgrade, the following screen may not be displayed.

Figure 8-53: 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\MP
 - **Custom:** Change the destination location.

Figure 8-54: Media Proxy Install



7. Click **Install**.

8.1.3.1 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\MP\Config\.
2. If there is more than one interface in this machine, the Media Proxy server will use this interface.

```
<System
key: localIpInterfaceAddress ="<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 Active/Active Configuration.

4. Restart Media Proxy Service.

8.1.4 Installing Media Delivery Server for Skype for Business

The Media Delivery is used specifically in Microsoft Skype for Business environment. The SmartTAP 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 server for long-term storage.



Note:

- 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 7 on page 63.

➤ **To Install Media Delivery (Skype for Business only):**

1. Run the **Install.bat** from the SmartTAP “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** to continue.
10. Click **Finish** to continue.
11. Installer will automatically install **AcProcDump**.
12. Click **Finish** to complete installation.

8.1.5 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 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.

8.1.5.1 Call Recording Notifications

8.1.5.1.1 Pre-requisites

- Stand-alone Physical or Virtual server.
- 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)
 - Make sure UCMA 5.0 is installed.
- From the Lync 2013 Installation Media:
 - 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.

8.1.5.1.2 Installing Skype for Business Software Required for Announcement Server

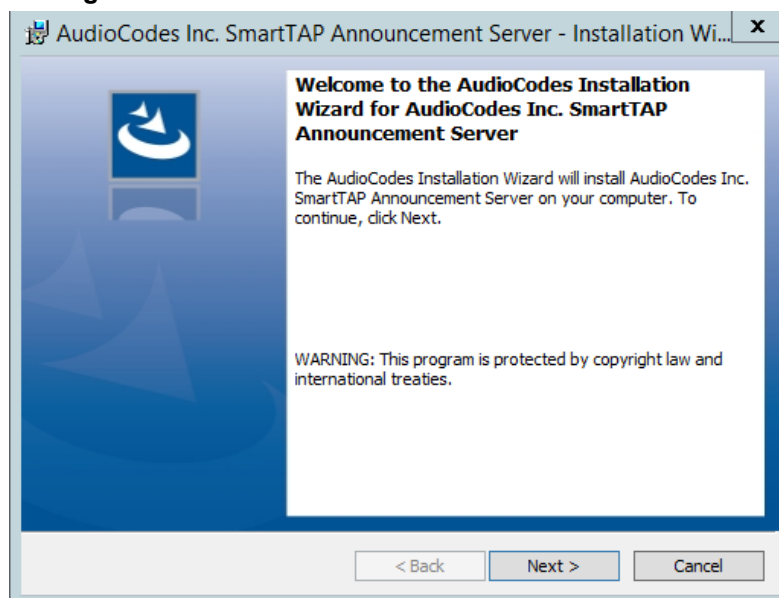


Note: Ensure that the server is joined to the domain before proceeding.

➤ **To install the Announcement server:**

1. Launch the Installation wizard.

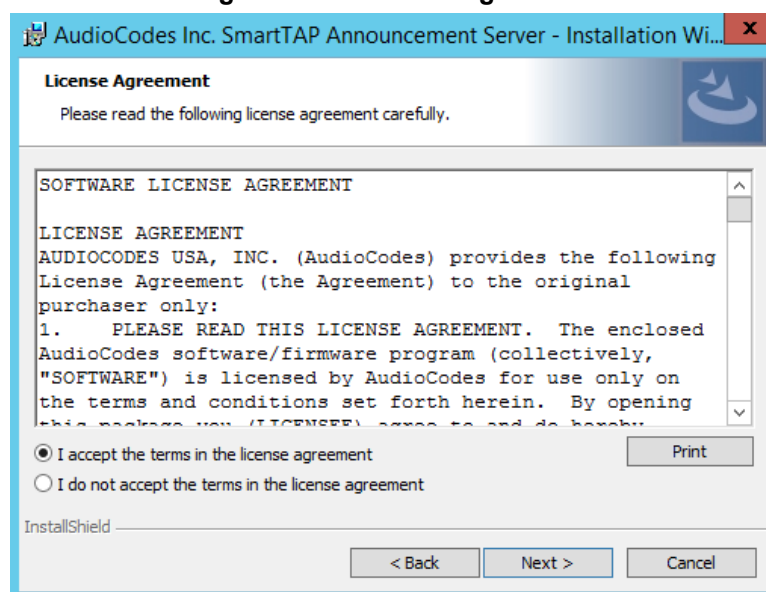
Figure 8-55: Announcement Server Installation Wizard



2. Click **Next**.

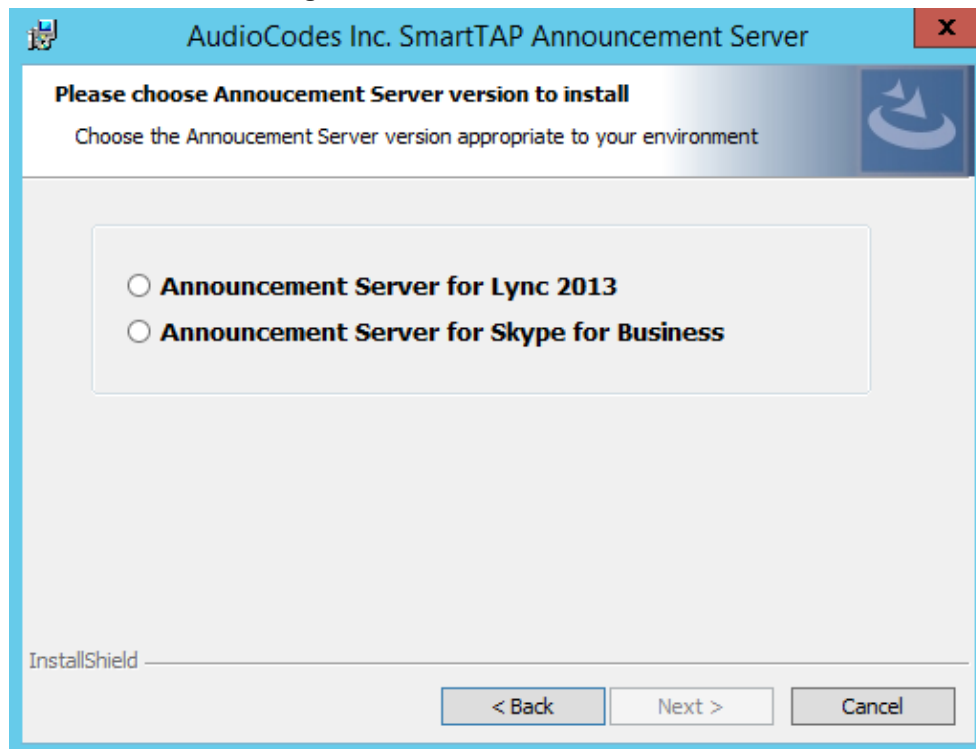
If you are installing from a Suite, then the following screen may not be displayed.

Figure 8-56: License Agreement



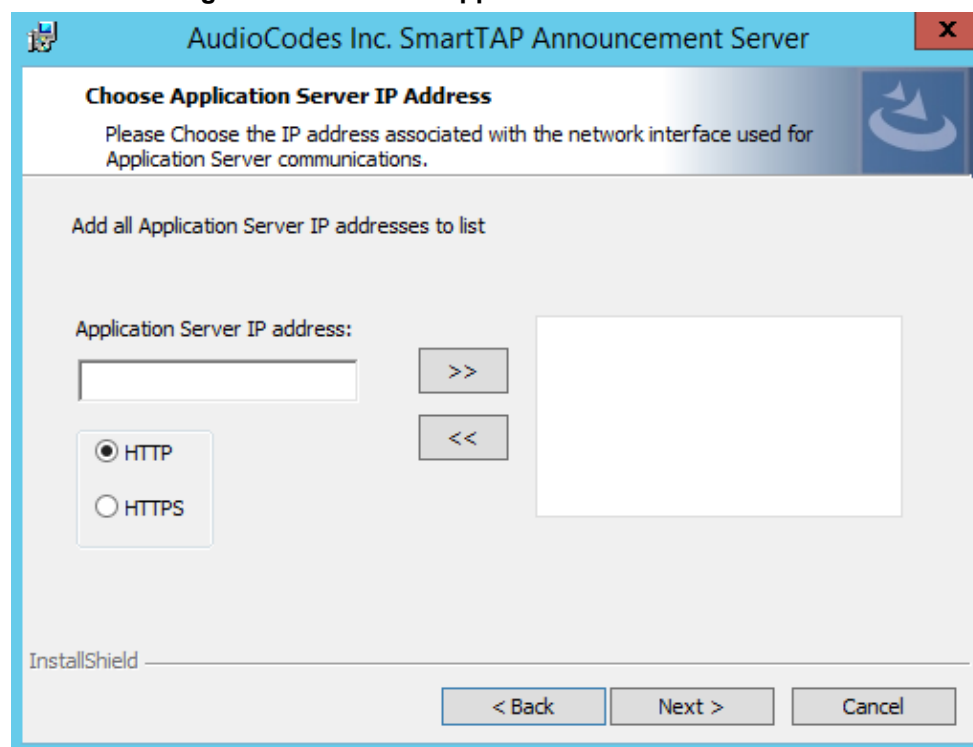
3. Click **Next** to agree to the license.

Figure 8-57: Announcement Server



4. Select the type of Announcement server and click **Next**:
 - Lync 2013
 - Skype for Business

Figure 8-58: Choose Application Server IP Address



5. 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 on the entry that you wish to move. At least one entry should be configured.

An example configuration is shown in the figure below.

Figure 8-59: Application Server IP Address

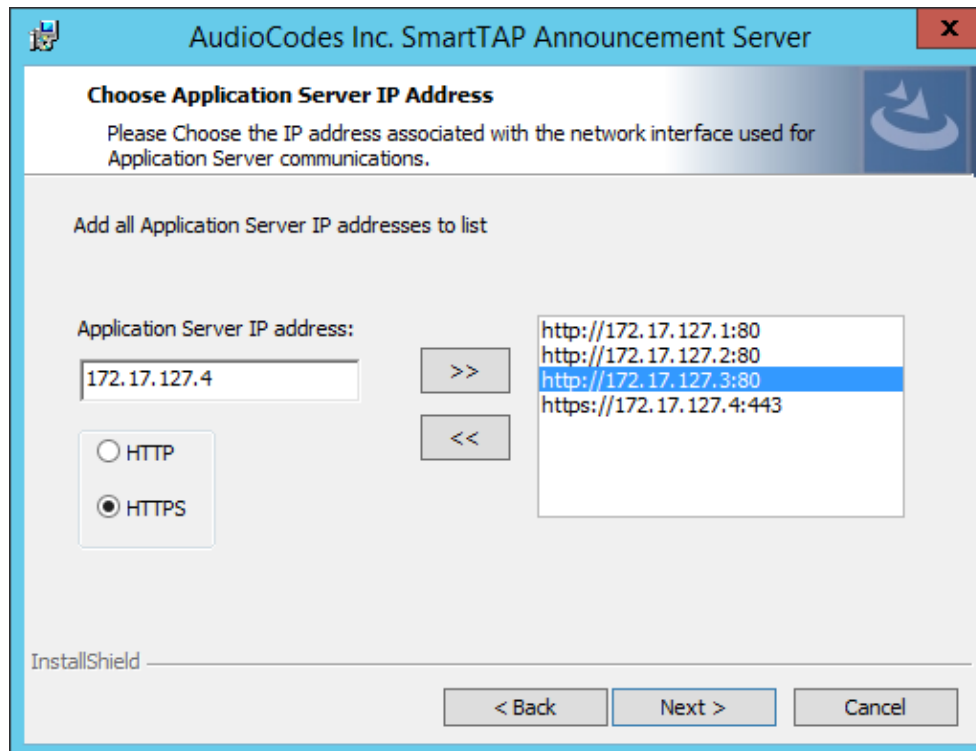
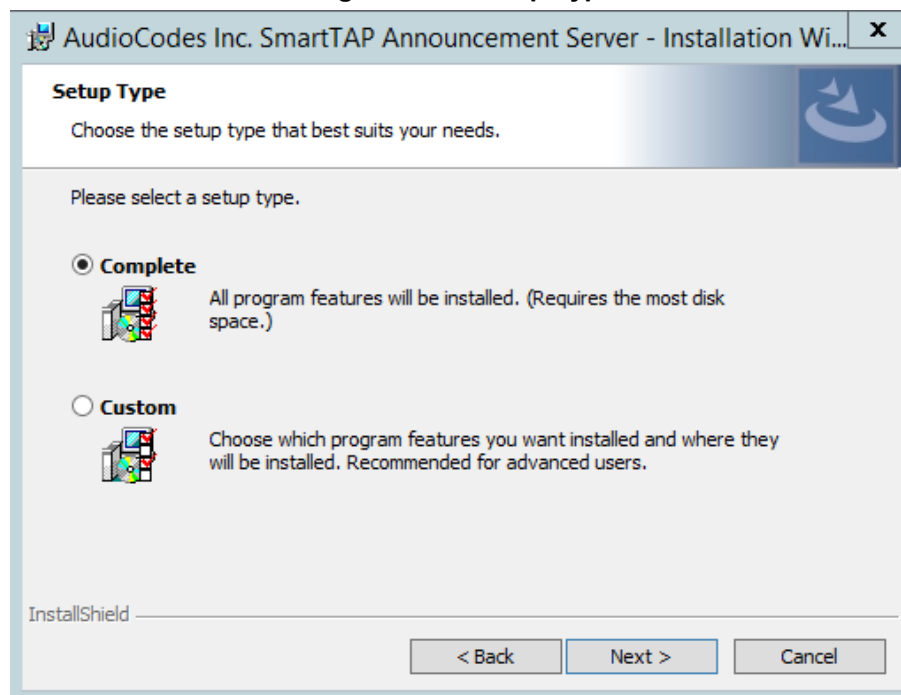


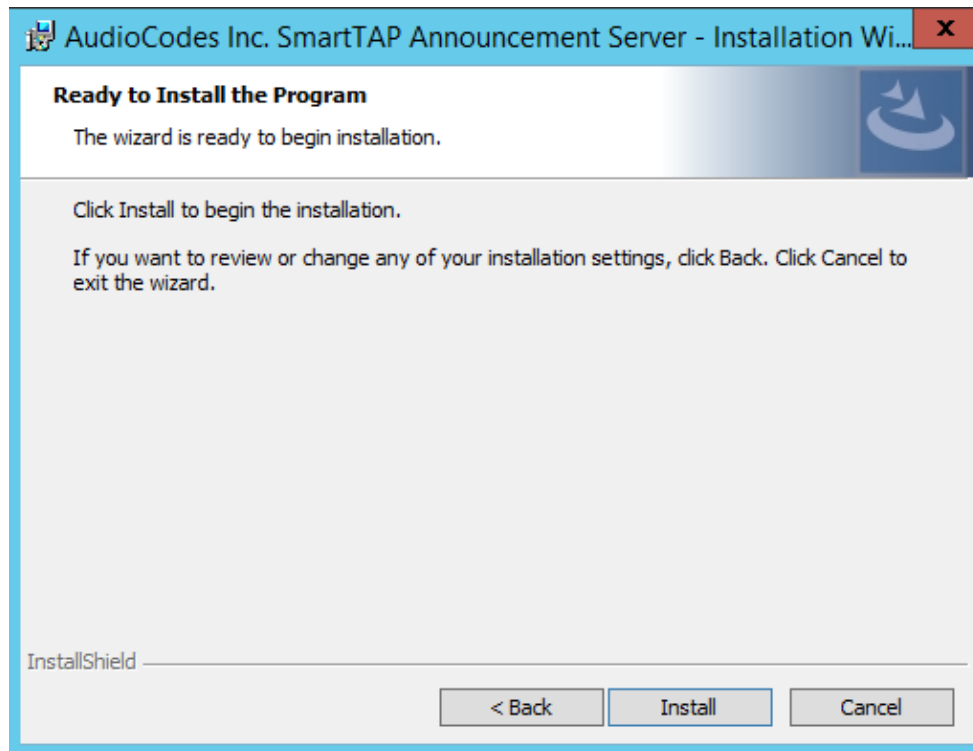
Figure 8-60: Setup Type



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

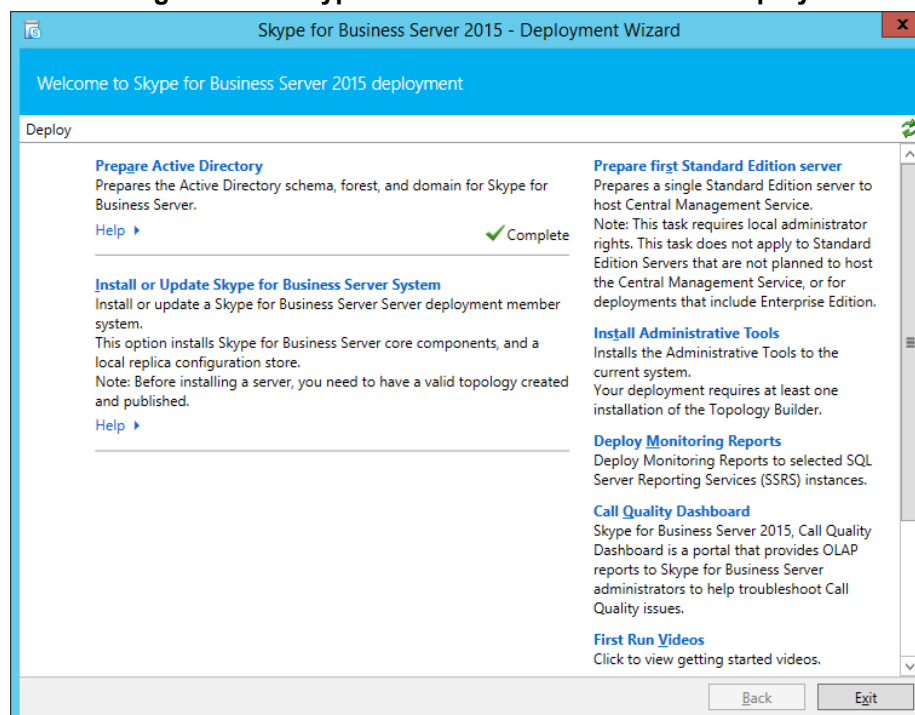
Note that if you are performing an upgrade, this screen may not be displayed.

Figure 8-61: Install



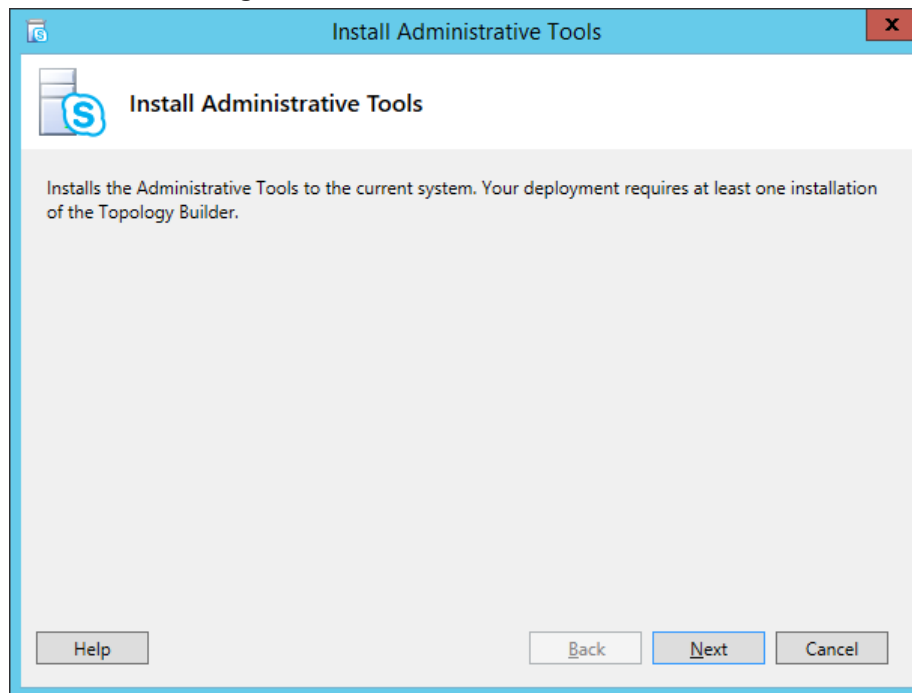
7. Click **Install** to commence the installation process.

Figure 8-62: Skype for Business Server 2015 – Deploy



8. Select **Install Administrative Tools**.

Figure 8-63: Install Administrative Tools



9. When done, you will see this.

Figure 8-64: Install Status

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

10. Install or Update Skype for Business Server System.
11. Installs core components & local replica configuration store.
12. Install only **Step 1**, then click **Run**.

Figure 8-65: Skype for Business Server – Deployment Wizard

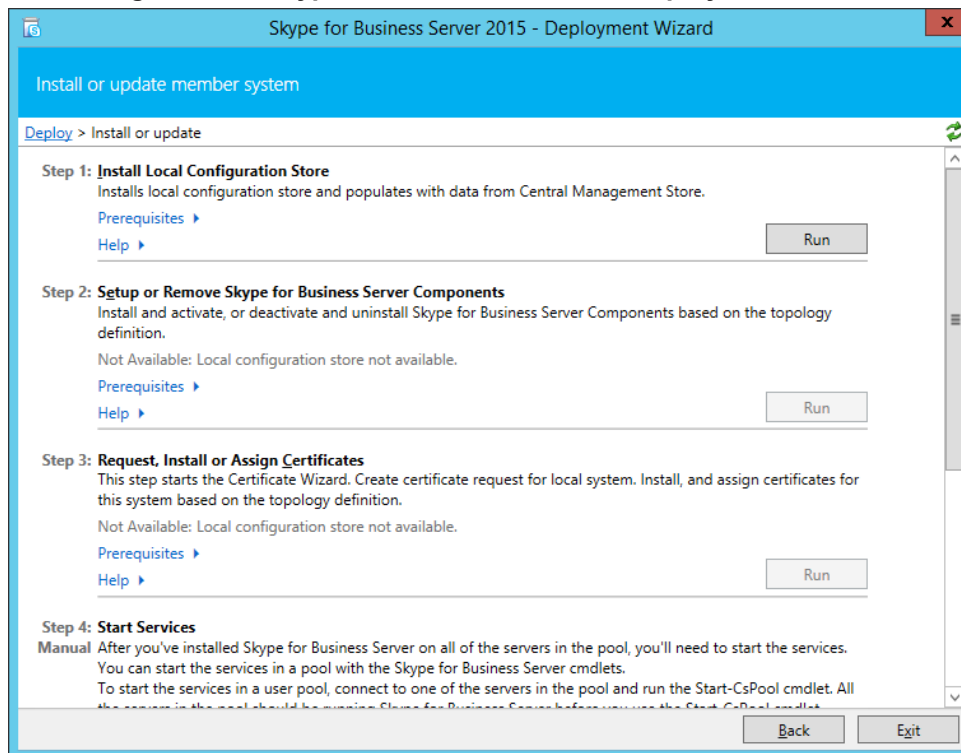
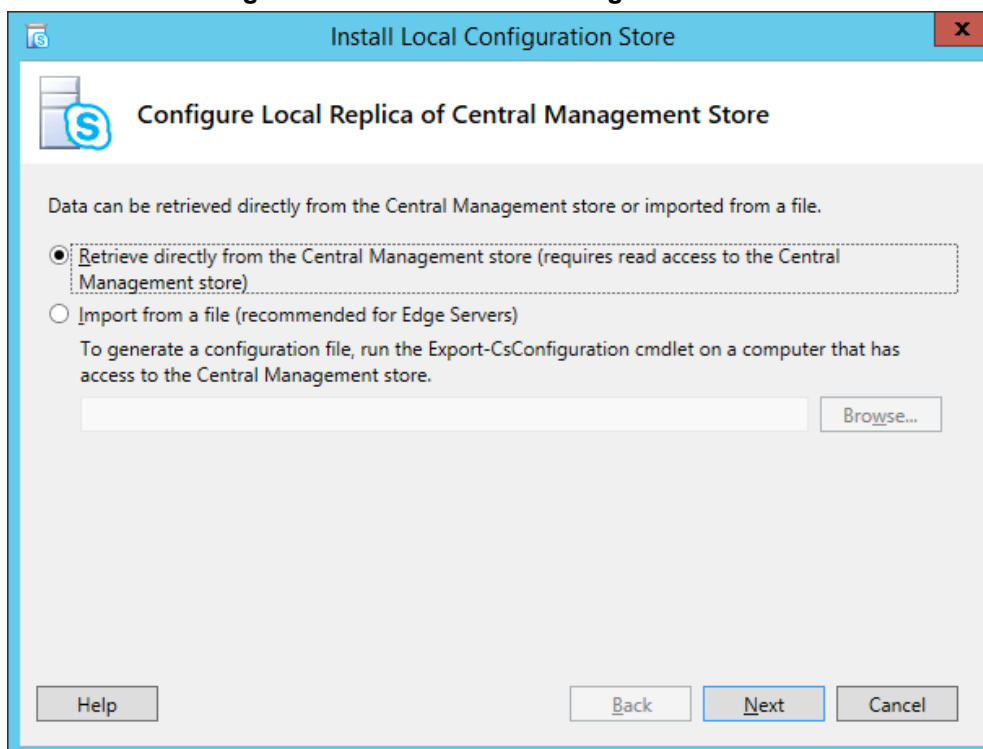
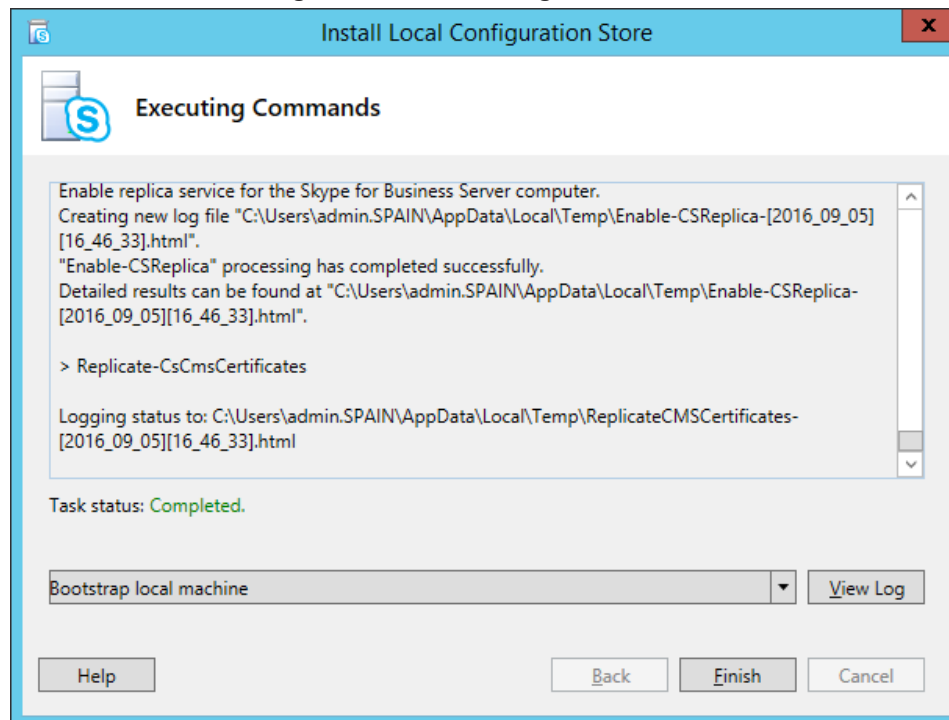


Figure 8-66: Install Local Configuration Store



13. Once complete, you should see the following:

Figure 8-67: Executing Commands



14. Click **Finish**.

8.1.5.1.3 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 7 on page 63.

8.1.5.2 Announcement Server Software Installation

This section describes how to install the Announcement server.

8.1.5.2.1 Step 1: Installing Announcement Server (Skype for Business) from Batch File

This section describes how to install the Announcement Server from the Install.bat file.

➤ **To install the Announcement server:**

1. Run the **Install.bat** from the SmartTAP "Suite\ " folder.
2. Select the Distributed software Custom Setup type.
3. Click **AudioCodes Inc. Announcement Server for Skype for Business**.
4. Click **Install** to continue.
5. Click **Next** to continue. Note that this process may take time while the PowerShell script runs.
6. When prompted, select Skype for Business according to the deployed Unified Communication platform.
7. Click **Finish** to complete the installation.



Note:

- Do not install on the SmartTAP server.
- The Announcement Service will not start automatically. It needs to be started manually after configuring the Announcement Services (see Section 8.1.5.2.2) .

8.1.5.2.2 Step 2: Configure Announcement 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 trusted-application.
 - 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.



Note: 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\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:
 "...**AnnouncementsApp** application endpoint name sip:**NAME@domain.com**..."
6. Save the **NAME** string and use it in the "Steps to add Announcement Servers to DNS" section.
7. Start AudioCodes Announcement Service.

8.1.5.2.3 Step 3: Adding Announcement Servers to DNS

➤ **To Add Announcement Servers to DNS**

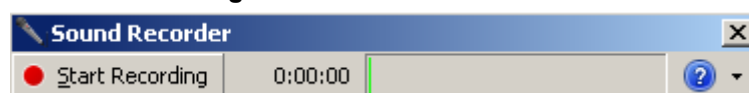
- Add DNS 'A' record to the appropriate zone on the configured DNS server per Announcement server against the AnnouncementApp name that was saved in "Steps to activate Announcement Services" section (**NAME**, example: AnnouncementsApp-pool-2013-1, AnnouncementsApp-pool-2015-1).

8.1.5.2.4 Step 4: Configuring Announcement Server (Skype for Business)

➤ **To configure the Announcement Server:**

1. Configure a simple announcement.
2. Create a WMA audio file. You can use the Windows Sound Recorder.

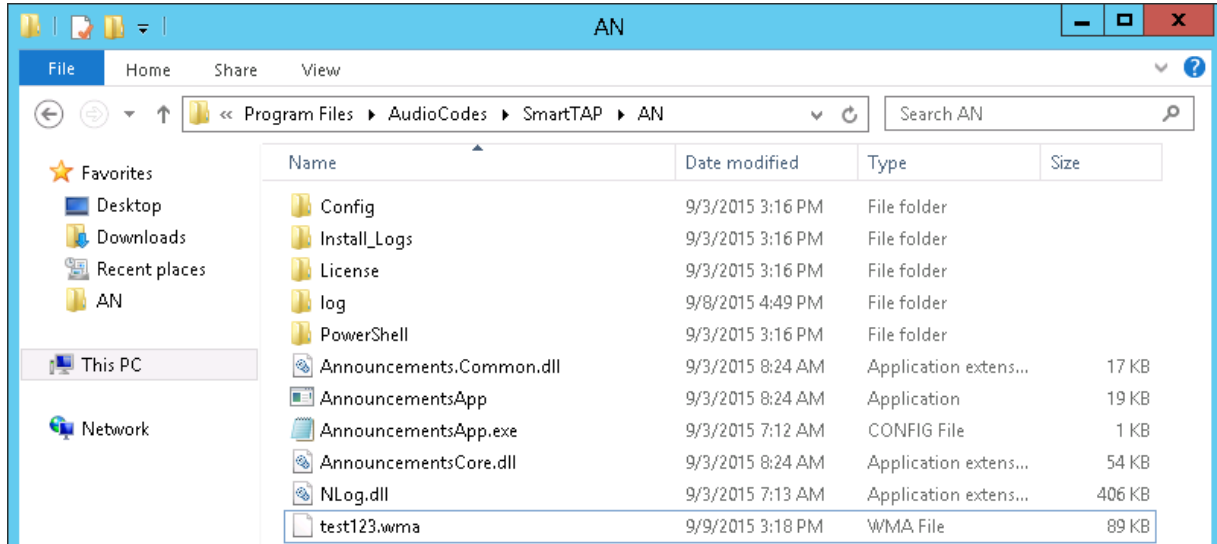
Figure 8-68: Sound Recorder



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

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

Figure 8-69: AN Server



5. Edit the System.config file at Program Files\AudioCodes\SmartTAP\AN\Config\.
6. Add option `inCallPlayPrompt="true"` and `inCallPlayPromptFilePath="filename.wma"`.

```
<System
  InCallPlayPrompt="true"
  inCallPlayPromptFilePath="filename.wma"
/>
```

7. Add option `'normalizeNumbers="true"'` when normalization of called numbers for the Announcement Server is required.

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

8. 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>"
/>
```

9. Restart AN Service.

8.1.5.2.5 Adding Support for Skype for Business Plugin Components for SmartTAP Announcement Server

This procedure describes how to add support for Skype for Business Plugin Components for SmartTAP Announcement server. This procedure should be applied for each each Skype for Business plugin component.

➤ To add support for plugins:

1. Edit the file "LyncPlugIn.exe.config".
2. Change <add key="EnableAnnouncements" value="false"></add> to "true".
3. If you want to record the Announcement leg of the call, enable the following:
 - <add key="RecordAnnouncements" value="false"></add> change to "true"
4. Save and close the configuration file.
5. Restart the plugin service.

8.1.5.3 Consent to Record Calls

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

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

By default, call consent is disabled. You can enable call consent by following the procedure below:

➤ To enable Call Consent:

1. Open the System.config file located under Program Files\AudioCodes\SmartTAP\AN\Config\.
2. Add option enableIvr="true" and playIVRToExternalCallingParty="true"


```
<System enableIvr="true"
playIVRToExternalCallingParty="true"
/>
```
3. Restart the AN Service.

8.1.5.3.1 Enabling Consent to Record Calls Demo

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

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

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

2. Restart AN Service.

➤ To enable playing the demo IVR to External Answering Party:

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

```
<System
enableIvr="true"
```



```
playIVRToExternalAnsweringParty="true"
AnnouncementRecipients="BothParties"
/>
```

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

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

4. Restart Plug-in Service

➤ **To enable playing the demo IVR to External Calling and Answering Parties:**

1. To enable playing the demo IVR to External Calling and Answering Parties add the following:

On each Announcement Server uncomment and edit the System.config file at Program Files\AudioCodes\SmartTAP\AN\Config\ with the following:

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

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

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

4. Restart Plug-in Service

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

Table 8-3: System.config File

Parameter	Description
appEndpointDiscoveryName	Defines the value of Skype for Business trusted application endpoint that will be used by this application. The default value is "AnnouncementsApp".
userAgent	Defines the Application User agent. The default value is " AnnouncementsApp".
inviteDest	If the value is not empty the application will call to this destination and will ignore from the destination the is in To header of incoming invite. The default value is "".
bufferSize	Defines buffer size of transferring data between calls. The default value is "60".
supervisedTransferHeaderName	Defines the header name of supervised transfer invite that should be returned by FE to the App. The default value is "X-Announcements-Supervised-Transfer".
supervisedTransferHeaderValue	Defines the header value of supervised transfer invite that should be returned by FE to the App. The default value is "\$1MsplApp".

Parameter	Description
outCallPassThroughHeaderNames	Defines the headers to pass from in call to out call. The default value is "Ms-Exchange-Command;HISTORY-INFO" e.g., "headerNameA;headerNameB;headerNameC".
inCallPlayPrompt	Defines playing announcements to in call before call is accepted. Possible values: <ul style="list-style-type: none"> True False (default)
inCallPlayPromptFilePath	Defines the file path of in call announcements. The default value is "".
outCallPlayPrompt	Defines playing announcements to out call after call accepted. Possible values: <ul style="list-style-type: none"> True False (default)
outCallPlayPromptFilePath	Defines the file path of out call announcements. The default value is "".
diagnosticsHeaderName	Defines the diagnostics header name. The default value is X-Announcements-DIAGNOSTICS.
maxEndpointDiscoveryMiliSeconds	Defines the maximum time in milliseconds to wait for first application endpoint discovery. The application exits if no endpoints are discovered by this time. The default value is 30000.
maxPlayPromptsMiliSeconds	Defines the maximum time in milliseconds to play prompts. The default value is 1800000.
nlogNetworkLayout	Defines the Nlog network layout. The default value is: \${longdate} \${level} \${message} \${exception:format=Message}\${newline}
referredByAddedParamName	This parameter name is added to the SIP 'Referred-By' header. The default value is " X-Announcements".
referredByAddedParamValue	This parameter value is added to the SIP 'Referred-By' header. The default value is " AnnouncementsApp".
transferType	Defines the Transfer Type. Valid Values: <ul style="list-style-type: none"> Attended - Perform attended transfers. Unattended - Performs unattended transfers.
AnnouncementRecipients	This parameter determines how the Announcement server plays the prompt. Valid Values: <ul style="list-style-type: none"> CallingParty - announcement played only to calling party. BothParties - announcement played to calling party and called party as well.
webServiceBaseUrl	Describes the listening URL of the Announcement server's Web service Rest API.

Parameter	Description
enableMoh	Sets true to enable Music on Hold. Possible values: <ul style="list-style-type: none"> • True (default) • False
mohFileName	Defines the Music on Hold file name. The file must be located at the project directory tree inside the MusicOnHold directory. The default value is "music-default.wma".
enableIvr	If this parameter is set to "true", the IVR will be played instead of an Announcement for an incoming call. Possible values: <ul style="list-style-type: none"> • True • False (default)
playIVRToExternalCallingParty	If this parameter is set to "true", the IVR will be played to a calling external user. Possible values: <ul style="list-style-type: none"> • True (default) • False
playIVRToExternalAnsweringParty	If this parameter is set to "true", the IVR will be played to an answering external user. Possible values: <ul style="list-style-type: none"> ▪ True ▪ False (default) <p>Note: In order to play the announcement to an answering party, the AnnouncementRecipients parameter has to be set to "BothParties".</p>
ivrResultParamName	Defines the parameter name that will be added in the referred-By header. The default value is "X-AnnIvrResult".
ivrCleanerSec	Clean stale calls IVR container every period of time in seconds. The default value is 1800.
impersonateInCall	If true, in call will be impersonated, the meaning is that the P-Asserted header of 200OK the value will be not of Announcement but of original destination user. Possible values: <ul style="list-style-type: none"> • True • False (default)
uaReceiveReferRegex	A regular expression (case insensitive). If UserAgent matches then REFER is sent to this device. This parameter provides a solution for an issue with Polycom VVX500 phone where ANN should send the SIP REFER to the phone when rerouting the call to the original destination. Default Value: "PolycomVVX-VVX_500"

Parameter	Description
asList	<p>Application Server comma-separated list. ANN sends alarms to the AS in the list.</p> <p>For example http://10.21.8.120:80,https://10.21.80.170:443</p> <p>Default Value: ""</p>
restClientTimeoutMilliseconds	<p>Alarms timeout in milliseconds.</p> <p>Default Value: 5000</p>
normalizeNumbers	<p>This parameter should be set to true when normalization of called numbers in the Announcement server is required. ANN will normalize the called number before rerouting the call to the original destination.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • True • False (default)
managedDeviceHeartbeatIntervalMs	<p>Interval in ms between each heartbeat request to AS. valid range [1000 minimum value]</p> <p>Default Value: 30000</p>
disableAlarms	<p>Determines whether to enable the alarms mechanism.</p> <p>Default Value: false</p>
uaDontReceiveReferRegex	<p>A regular expression (case insensitive). If the value of the UserAgent header matches the expression, then the SIP REFER is not sent to this device when rerouting the call to the original destination. This solves the problem for Skype for Business clients answering with "488 Not Acceptable Here" on reception of SIP INVITE with replaces from the mobile clients.</p> <p>Default Value: "ucwa"</p>
noAttendedTransferSupportRegex	<p>A regular expression (case insensitive). When one of the devices in the call to ANN doesn't support the Attended transfer, ANN will execute the UnAttended transfer. Mobile clients (Skype for Business) and voicemail don't support Attended transfers.</p> <p>Default Value: "ucwa"</p>
redirectIfReferNotSupported	<p>When the caller doesn't support REFER, ANN may redirect the caller without playing ANN (true) or disconnect the call (false),</p>

Parameter	Description
	<p>When in “BothParties” mode, redirect the caller if both sides don't support the REFER (true), or disconnect the calls (false).</p> <p>Possible values:</p> <ul style="list-style-type: none">• True (default) – AN redirects the caller• False – ANN disconnects the call
voicemailRegex	<p>A regular expression (case insensitive). This parameter is used to identify voicemail as a participant of the call routed through the ANN according to 'user-agent' and 'server' headers.</p> <p>Default Value: "Exchange"</p>
dontPlayAnnRegex	<p>A regular expression (case insensitive). This parameter is used to identify conference as a participant of the call routed through the ANN according to 'user-agent' and 'server' headers.</p> <p>Default Value: "AV-MCU"</p>
isPlayAnnIfAnsweredByVoicemail	<p>The announcement is not played to the caller when the call is routed through ANN and answered by the voicemail.</p> <p>Possible values:</p> <ul style="list-style-type: none">• True• False (default)

Example:

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

/>

<System

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

/>
```

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

➤ **To prepare the TTS platform:**

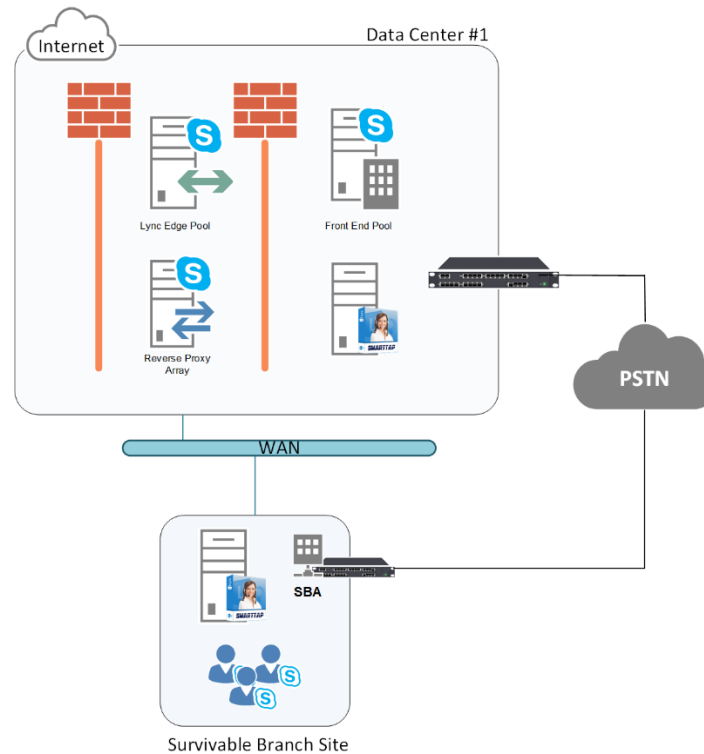
1. Download and install Microsoft Speech Platform - Runtime (Version 11) from here:
<https://www.microsoft.com/en-us/download/details.aspx?id=27225>
2. After you have the platform installed, now you need to download and install TTS languages which you want to support in yours ANN application.
Microsoft Speech Platform - Runtime Languages (Version 11)
<https://www.microsoft.com/en-us/download/details.aspx?id=27224>
The link above is for download the whole TTS (text to speech) and SR (speech recognition) files.
3. After you download it, you need to install each relevant file you want according to language. For example if you want support text to speech for Russian then install the file **MSSpeech_TTS_ru-RU_Elena.msi**.
For English, install **MSSpeech_TTS_en-US_Helen.msi** or **MSSpeech_TTS_en-US_ZiraPro.msi**.
Don't install SR files because currently ANN doesn't support speech recognition. It may support it in the future. If you install SR, it won't damage ANN behavior. It just won't be used.

It is important to install platform and language from same Version 11. A combination of Versions 10 and 11 won't work.

8.1.6 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 deployed in the branch location can record user/device calls regardless of WAN up/down.

Figure 8-70: Skype for Business Remote 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 8.1.
- (Optional) Install Media Delivery to record PSTN calls. See Section 8.1.3 on page 105.

SmartTAP Server:

- Install Communication Server. See Section 5.3 on page 49.
- Install Media Server. See Section 5.4 on page 49.
- Install Call Delivery Server. See Section 5.5 on page 56.

Media Proxy: (Optional)

- Install Media Proxy (Optional method to record Internal IP-to-IP and PSTN calls). See Section 8.1.3 on page 105.

8.2 SIP Recording (SIPRec)

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

8.2.1 What is SIPRec?

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

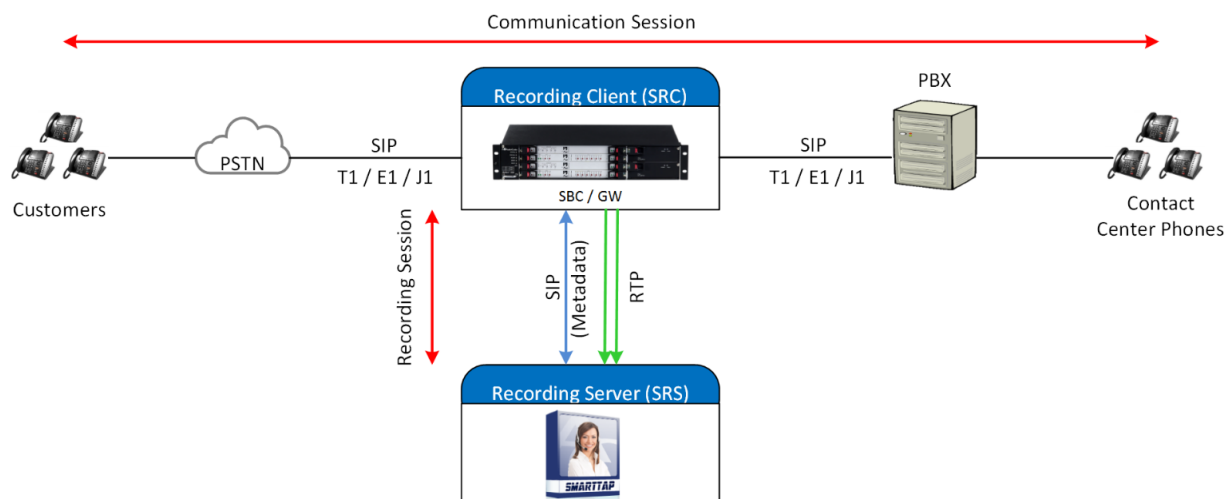
8.2.2 Session Recording Server (SRS)

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.

8.2.3 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.

Figure 8-71: Session Recording Client



➤ To configure SIPRec:

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

8.2.4 Configuring Gateway & SBC for SIP Recording

Refer to the appropriate Gateway & SBCs User's Manual for configuration instructions.

Figure 8-72: Configure Gateway & SBC for SIP Recording

The figure shows two screenshots of a configuration interface for SIP Recording.

Top Screenshot: SIP Recording Settings

The interface has a top navigation bar with tabs: IP NETWORK, SIGNALING & MEDIA, and ADMINISTRATION. A search bar on the right contains "sip recording". Below the navigation bar is a sidebar with a "TOPOLOGY VIEW" icon and a list of categories: CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, INTRUSION DETECTION, and SIP RECORDING. The SIP RECORDING category is expanded, showing "SIP Recording Settings" (selected) and "SIP Recording Rules (0)".

The main content area is titled "SIP Recording Settings" and contains a "GENERAL" tab with the following fields:

- SIP Recording Application: Disable (dropdown menu)
- Recording Server (SRS) Destination Username: (text input)
- SIP Recording Time Stamp Format: Local Time (dropdown menu)

At the bottom right of the main area are "Cancel" and "APPLY" buttons.

Bottom Screenshot: SIP Recording Rules

The interface is titled "SIP Recording Rules" and has a "GENERAL" tab with the following fields:

- Index: 0 (text input)
- Recorded IP Group: Any (dropdown menu)
- Recorded Source Prefix: * (text input)
- Recorded Destination Prefix: * (text input)
- Condition: .. (dropdown menu)
- Peer IP Group: Any (dropdown menu)
- Peer Trunk Group ID: -1 (text input)
- Caller: Both (dropdown menu)

Each dropdown menu has a "View" link next to it. At the bottom right of the main area are "Cancel" and "APPLY" buttons.

8.2.5 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 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 IP address.

Figure 8-73: Server IP Setup

AudioCodes Inc. Call Delivery-SIPREC

Server IP Setup

Configure the names or IP addresses of the servers

Communication Server Name or IP Address:
172.26.144.23

Application Server Name or IP Address:
172.26.144.23

Local IP Address:
172.26.144.23

Local UDP Port:
5069

Local SIPREC listener IP Address:
172.26.144.23

Local SIPREC listener UDP Port:
5068

InstallShield

< Back Next > Cancel

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

Table 8-4: SIP Recording – Additional Configuration Files

Configuration File	Purpose
CdSipRecConfig.xml	Set the IP & Port to receive the SIPRec data. Typically the SmartTAP server
Calldeliveryconfig.xml	<ul style="list-style-type: none"> Set the IP of the SmartTAP Application server. The default value is 127.0.0.1 assuming the AS and CD are on the same server. Configure the Regular Expressions to match the specific needs of each customer network. Refer to Target Attributes for more information.

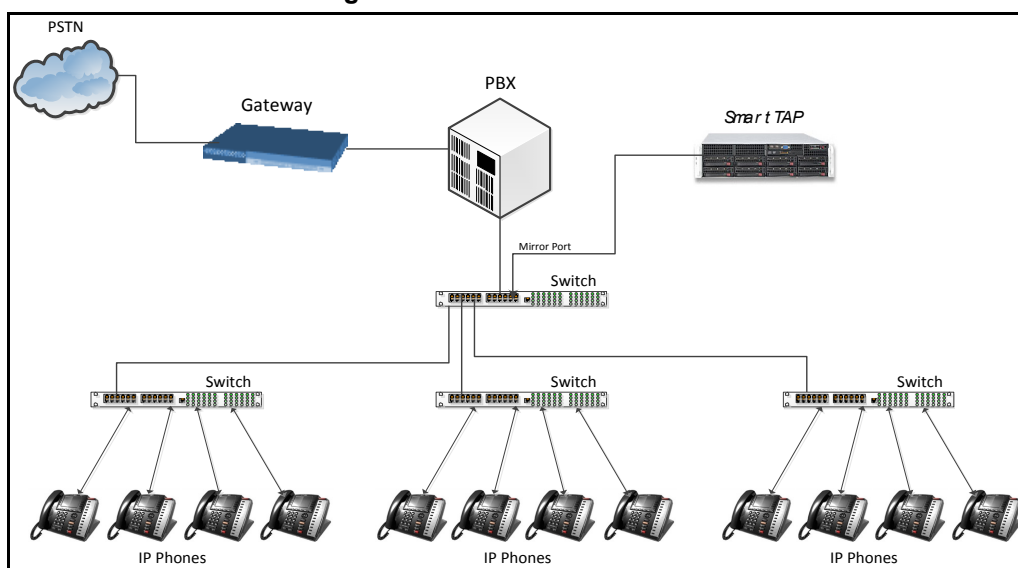
8.3 VoIP Port Mirroring

The SmartTAP 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.

8.3.1 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.

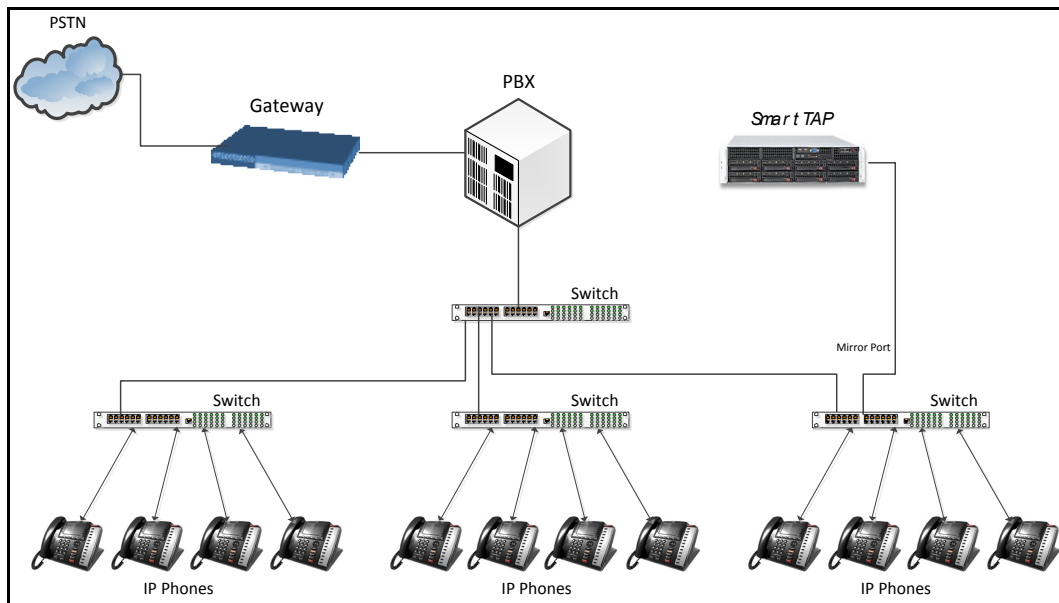
Figure 8-74: Inbound/Outbound



8.3.2 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 8-75: Station to Station



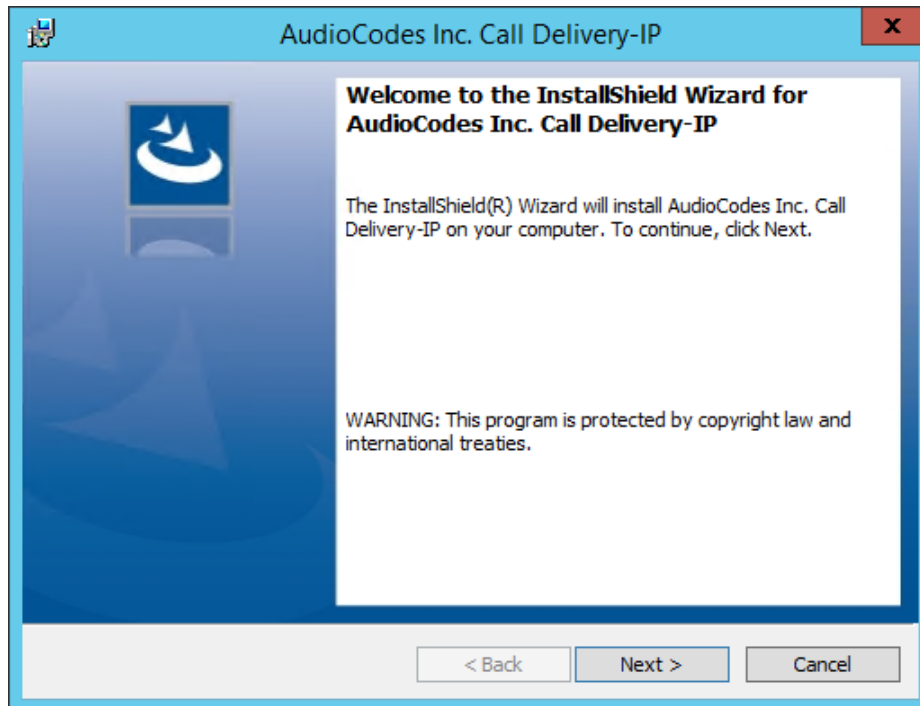
8.3.3 Call Delivery Install for VoIP (Port Mirror)

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.

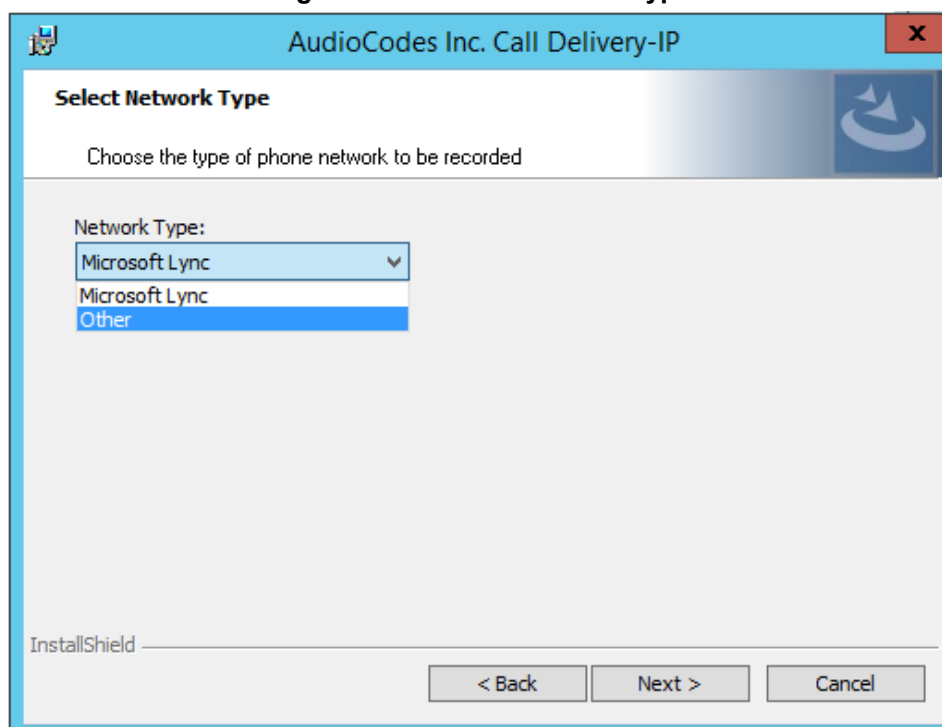
Figure 8-76: Call Delivery IP



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 8-77: Select Network Type



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.

Figure 8-78: Server IP Setup

SmartTAP 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 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

Figure 8-79: Interface Setup

5. Click **Next** on the Setup Type screen.

6. Click **Install** on the install screen.
7. Click **Finish** to finish.

8.3.4 Additional Configuration

This section describes additional 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 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\\CD-IP\\Config\\Voip.cfg

Table 8-5: Description of the 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
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
#   DCHFILTER=OFF
#   CC=ON
#   SUBTYPE=CM]
```

Table 8-6: 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 ]
]
```

8.3.5 Setting Up Monitoring Interfaces

This section describes how to manually setup the monitoring interfaces.



Note: SmartControl is no longer available for CD-IP.

➤ To setup the monitoring interfaces:

1. Run the System Profile Tool, C:\Program Files\AudioCodes\SmartTAP\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\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: 0x0000000e:
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"
```

3. Edit the C:\Program Files (x86)\AudioCodes\SmartTAP\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.

8.4 Avaya AES Integration

SmartTAP records standard non-encrypted Avaya IP calls with the standard VoIP configuration.



Note: Support is no longer provided for Avaya AES Integration.

8.5 Analog Trunk / Radio

The SmartTAP 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.

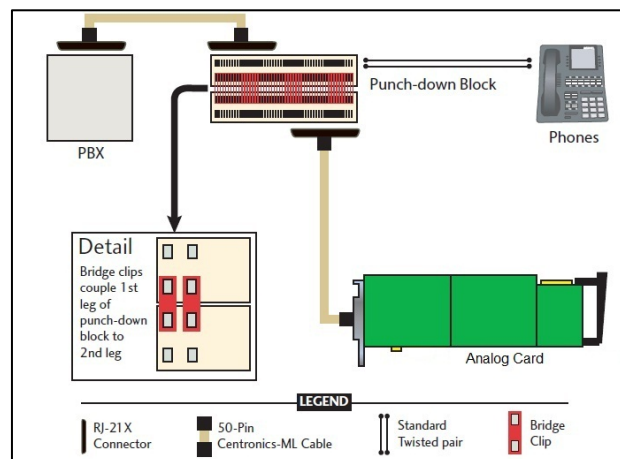
Loop Start Trunk / Station

The battery voltage of the analog line may be different between Trunk and Station side. Adjusting SmartTAP 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.

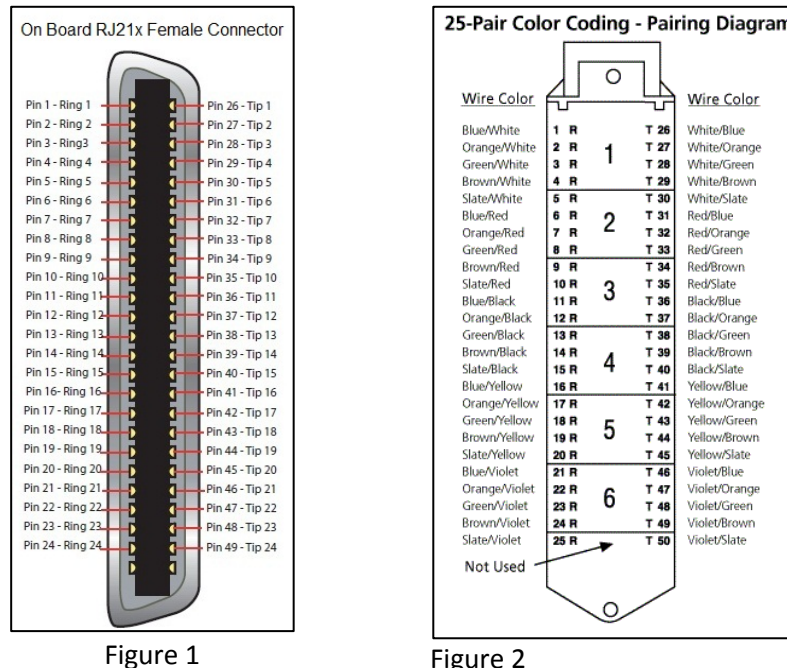
The figure below represents a typical passive tap implementation using a 66 block. The maximum distance tested from PBX to Analog phone while tapping is 2200'.

Figure 8-80: Passive Tap Implementation



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 8-81: Figure 1 and Figure 2



8.5.1 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.

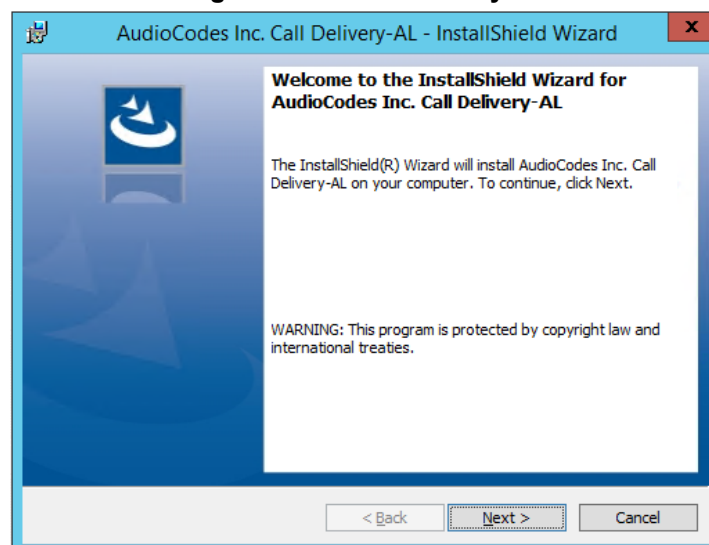


Note: The screens shown in the procedure below are specific to the installation when a LD card is detected on the server

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

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

Figure 8-82: 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 IP address.

2. Click **Next** on the Server IP Setup.

Figure 8-83: Server IP Setup

AudioCodes Inc. Call Delivery-AL

Server IP Setup

Configure the names or IP addresses of the servers

Communication Server Name or IP Address:

172.26.144.23

Application Server Name or IP Address:

172.26.144.23

Local (non-monitoring) IP Address:

172.26.144.23

InstallShield

< Back Next > Cancel

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

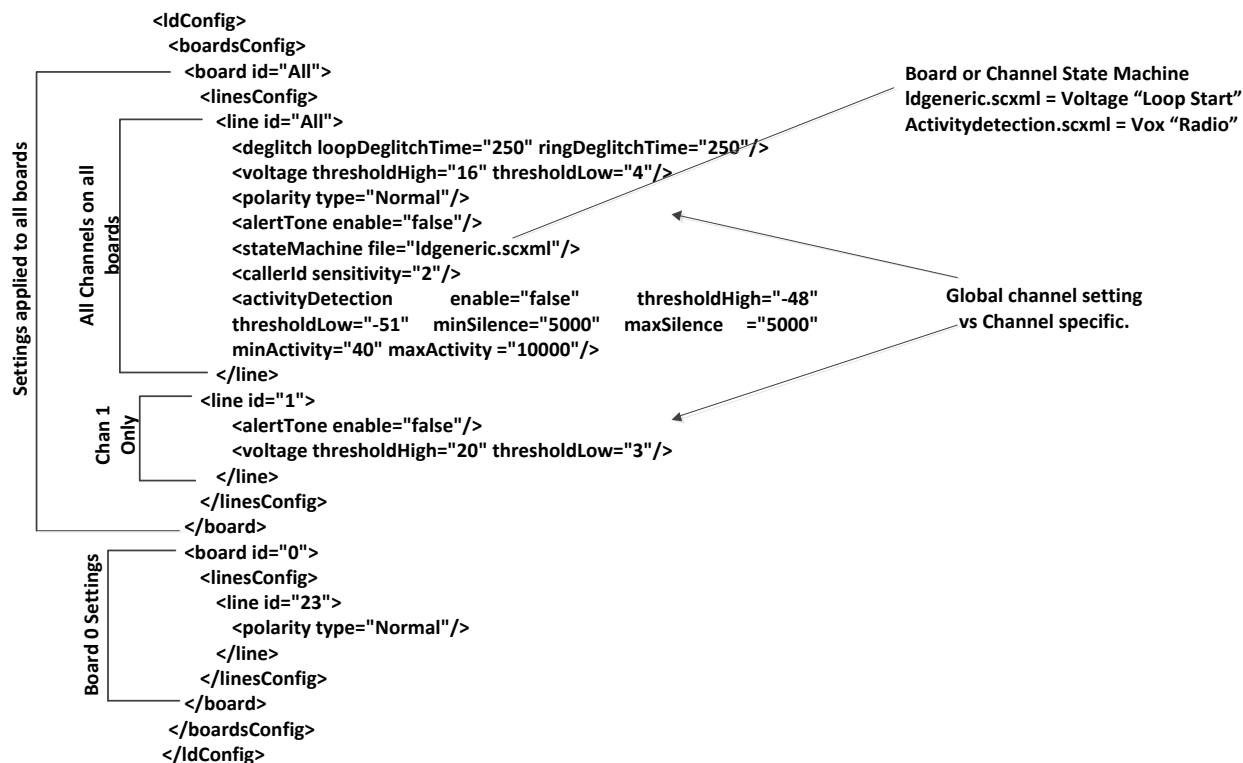
8.5.2 Additional Configuration

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\\CD-AL\\Config\\

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

Figure 8-84: LD.xml Basic Structure Diagram



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

Table 8-7: Most Common Values 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 thresholdLow and below thresholdHigh.	4vdc
Polarity	type	Normal, will cosmetically change line polarity to positive. Reversed, will cosmetically change line polarity to negative.	normal
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

Element Name	Attribute Name	Description	Default
	minSilence	Min = 500, Max = 20000	5000ms
	maxSilence	Min = 500, Max = 20000	5000ms
boardID		0 – 31	All
lineID		0 – 23, 24 channels per board	All

8.5.2.1 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 thresholdLow
- The activity threshold thresholdHigh

Whenever the detector is in the silence state and the measured input signal energy remains above thresholdHigh 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 8-85: Activity Detection

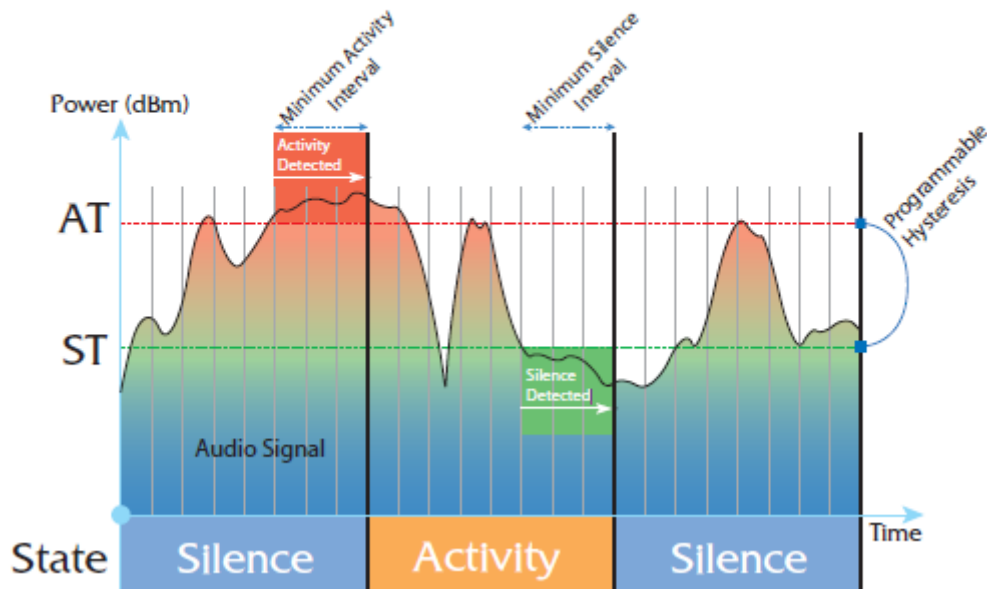
Activity Detection

Legend:

AT - Activity Threshold (dBm)

ST - Silence Threshold (dBm)

Hysteresis - Difference between AT and ST (dB)

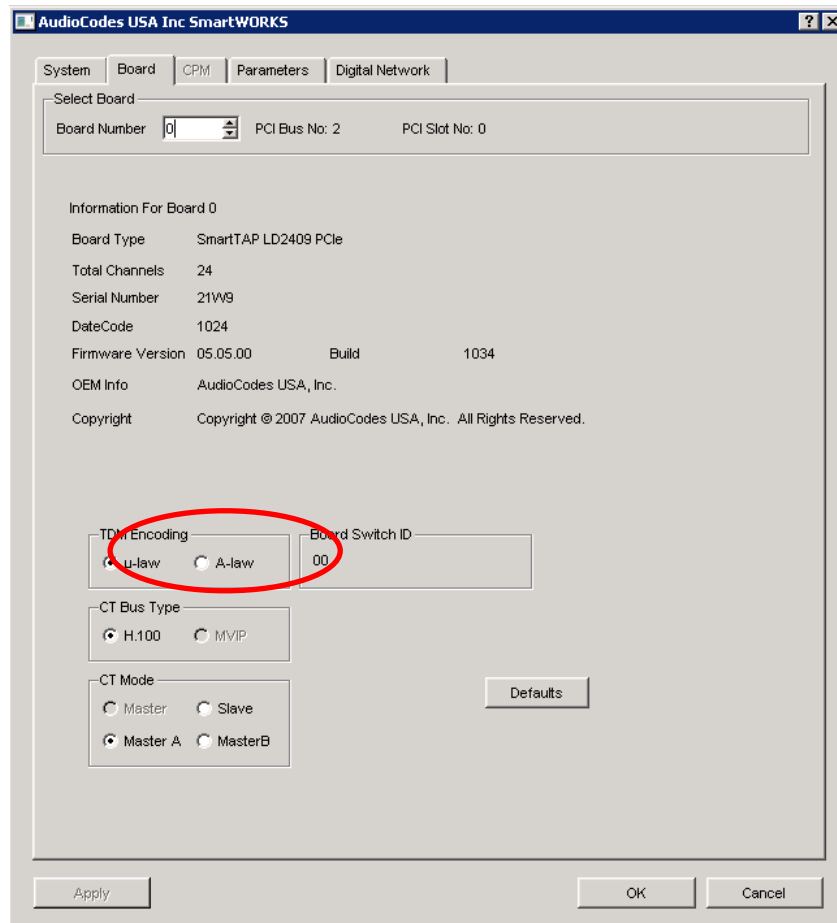


8.5.2.2 SmartCONTROL

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...

Figure 8-86: Board Tab



This page is intentionally left blank.

9 Additional Configuration Options

This chapter describes the following additional configuration options:

- Configuring Digital Signature
- Configuring LDAP
- Configuring SSO
- Configuring HTTP/S

9.1 Configuring Digital Signatures

Configuring Digital Signature is a two-stage process:

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

9.1.1 Configuring the SmartTAP Web interface

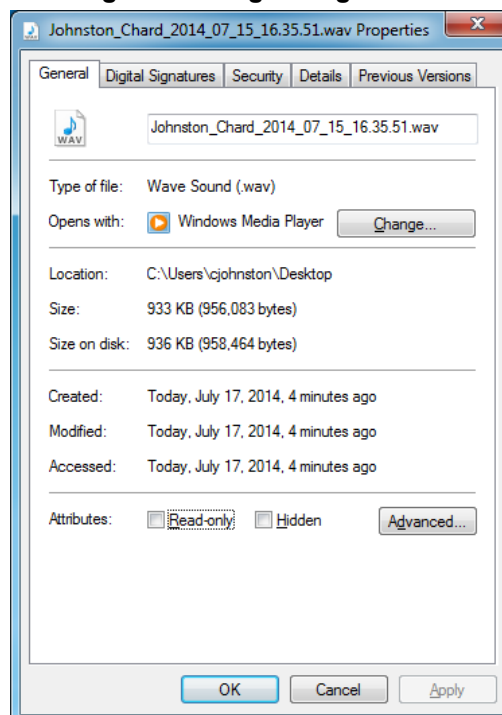
Please refer to the Certificate and Digital Signature sections within Chapter 3 in the SmartTAP User Guide.

9.1.1.1 Steps to Configure the PC Client

➤ To configure the PC client:

1. Open SmartTAP 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.

Figure 9-1: Digital Signatures





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

9.2 Configuring LDAP

The SmartTAP LDAP feature allows you to use your Windows Active Directory users and groups in SmartTAP, and map them into users, groups and security groups in SmartTAP. The users and groups are not imported. SmartTAP 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.

Please refer to the SmartTAP User's Guide for LDAP configuration details.

9.2.1 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"

9.3 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 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.



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

9.4 Configuring HTTP/S

This section describes how to configure HTTP/S.

9.4.1 Disabling HTTP Communications on Application Server (Optional)

This section describes how to disable non-encrypted HTTP communication on SmartTAP 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.



Note: Configuring SmartTAP Application Server for HTTPS does not automatically disable the HTTP (non-encrypted) interface. While the SmartTAP management Web page would be available over HTTPS, SmartTAP components would continue to communicate with SmartTAP Application Server over HTTP. To convert the entire application to encrypted communications (over SSL), after disabling HTTP in Application Server as described below, SmartTAP components must be configured as described in Section 9.4.2 (Configuring SmartTAP Components for HTTPS).

9.4.1.1 Automatic

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.
2. Locate the PowerShell directory. For example C:\Program Files\AUDIOCODES\SmartTap\AS\PowerShell.
3. Run the DisableHttp.ps1 script (located in the “Tools” folder of SmartTAP installation) with the following parameters:
 - [Mandatory] managementIP – IP address of HTTP Management interface (Application Server IP)
 - Management user credentials:
 - ◆ [Mandatory] username
 - ◆ [Mandatory] password
 - [Optional] jbossCliPath – Full path to jboss-cli.bat (Command Line Interface)

For example:

```
DisableHttp.ps1 -managementIP 192.168.1.100 -username
username -password pass -jbossCliPath C:\Program
Files\AUDIOCODES\SmartTap\AS\Bin\jboss-cli.bat
```
4. Restart the requested service.

9.4.1.1.1 Manual

You can perform the manual procedure using one of the following interfaces:

- Edit domain.xml (restart the server after editing and saving file).
- Wildfly Web console.
- jboss-cli.bat

➤ **Do the following:**

1. In urn:jboss:domain:undertow:1.2, comment out the listener element:


```
Remove http-listener
```
2. Under urn:jboss:domain:messaging: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 “default-ssl”
 - Change http-acceptor-throughput http-listener from “default” to “default-ssl”
3. Under subsystem urn:jboss:domain:remoting:2.0 change http-remoting-connector connector-ref from “default” to “default-ssl”.
4. Restart the requested service.

9.4.2 Configuring SmartTAP Components for HTTPS

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



Note: For generating and loading certificates, refer to Section 'Generating and Loading Certificates' in the SmartTAP Administrators Guide.

9.4.2.1 Communication Server

This section describes how to configure the Communication server

➤ **Do the following:**

1. 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.

9.4.2.2 Call Delivery

This section describes how to configure the Call Delivery server.

➤ **Do the following:**

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

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

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

3. 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.
```

9.4.2.3 Media-Proxy

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 present in the certificate SAN field and is resolvable by DNS.
4. Restart the service to apply changes.

9.4.2.4 Announcement Server

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 present in the certificate SAN field and is resolvable by DNS.
4. Restart the service to apply changes.

9.4.2.5 Media Server and Remote Transfer Service

This section describes how to configure the Media Server and Remote Transfer Service

➤ **Do the following:**

A single configuration file applies to both the Media Server Service and the Remote Transfer Service.

1. Edit the config file: MS\server\bin\mediaserverconfig.xml
2. Find the following section in the configuration file:

```
<applicationServer>
  <recorder ip="127.0.0.1" port="80">
    <protocols>
      <protocol>http</protocol>
    </protocols>
  </recorder>
</applicationServer>
```

3. Make the highlighted changes:

```
<applicationServer>
  <recorder ip="AS_FQDN" port="443">
    <protocols>
      <protocol>https</protocol>
    </protocols>
  </recorder>
</applicationServer>
```

4. Make sure AS_FQDN is present in the certificate SAN field and is resolvable by DNS.
5. Save the configuration file and restart the Media Server Service and the Remote Transfer Service.

9.4.2.6 Health Monitor

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

9.5 Configuring Syslog Server Connection

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

9.6 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\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="Local17" />
  <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>
```

3. On the front-end machine, edit the C:\Program Files\AudioCodes\SmartTAP\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.

9.7 Location-Based Targeting in SmartTAP

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.

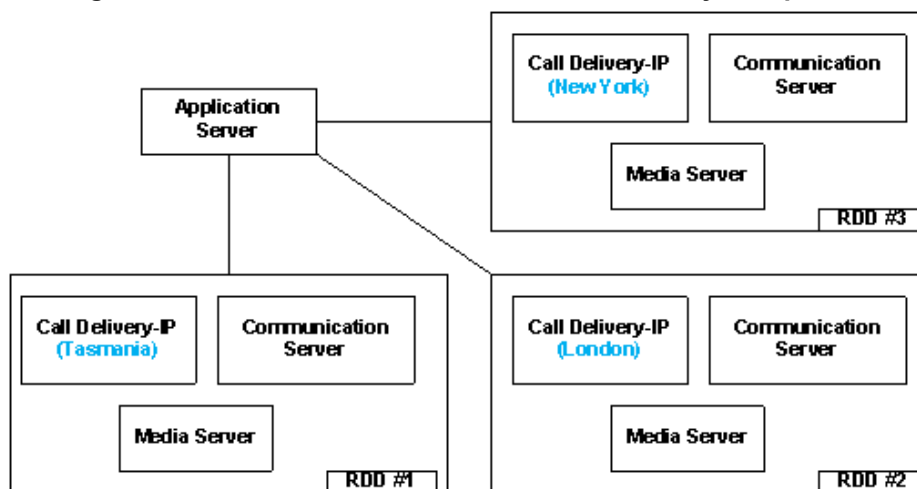
By assigning targets to specific Call Delivery components, the physical location of the recording can be controlled. In addition, the loads on each Call Delivery can be minimized. By default, when no location attributes are set, Call Delivery tracks all targets. In systems with large numbers of targets,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

9.7.1 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".

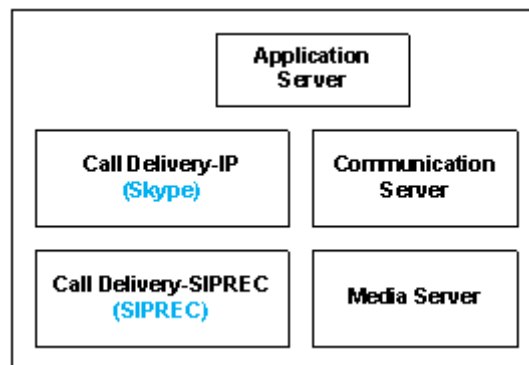
Figure 9-2: Location Attribute for each Call Delivery Component



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 9-3: Skype and SIPREC Targets



In the case of SmartTAP 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 GUI.

➤ **Do the following:**

1. Stop the Call Delivery service(s) in the service manager.
2. Open the calldeliveryconfig.xml file for editing. By default, the configuration file is located in “C:\Program Files (x86)\AudioCodes\SmartTAP\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>
  <attributes>
  </attributes>
  <targetConversions>
    <converter format="\2"
regex="(sips?:)?([^\@]*) (@.*)?"
type="SIP_URI"></converter>
    <converter format="\1" regex="(\d+)"
type="TRUNK_ID"></converter>
    <converter format="\5"
regex="(tel:)?(\+?) (\d+) (;ext=) (\d+)"
type="EXTENSION"></converter>
    <converter format="\2" regex="^(\+?) (\d+)"
type="EXTENSION"></converter>
    <converter regex="(tel:)?(\+?) (\d+) (;ext=) (\d+)"
type="TEL_URI">
      <target format="\3" />
      <target format="\5" />
      <target format="\3\4\5" />
    </converter>
    <converter format="\3" regex="^(tel:)?(\+?) (\d+)$"
type="TEL_URI"></converter>
  </targetConversions>
</targeting>
  
```


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>
  </attributes>
```

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 system.



Note: 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.

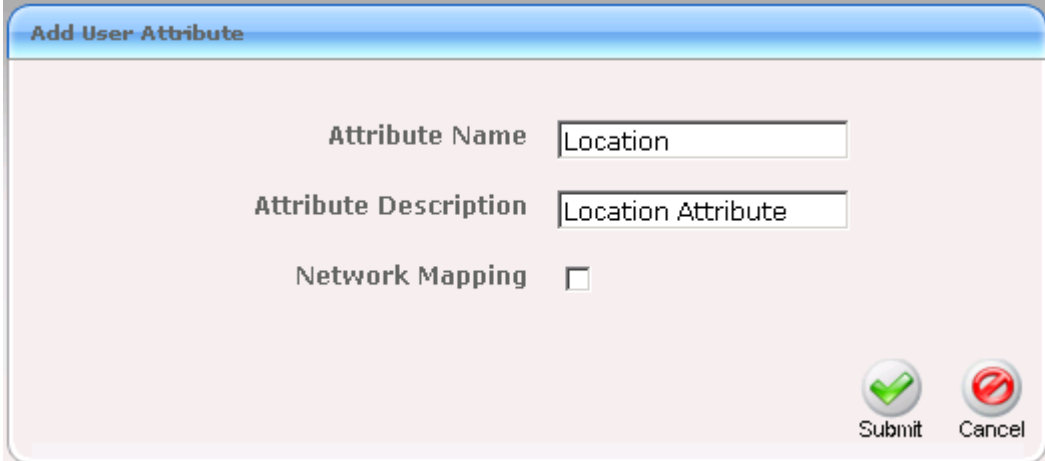
9.7.2 Create a Location Attribute in the SmartTAP GUI

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 9-4: Add User Attribute



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.



Note: 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".

9.7.3 Assign a Location to Each User/Device in the SmartTAP 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.

Figure 9-5: Add User

The screenshot shows the 'Add User' window. The 'Location' field is highlighted with a red box. The 'Security Profiles' list has 'agent' selected. The 'Groups' list has 'Default' selected. The 'Submit' and 'Cancel' buttons are at the bottom right.

➤ **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.



Note: The procedures for setting up Devices and for setting up Users are identical.

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

Figure 9-6: SmartTAP 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.

9.7.4 Verify the Target List in Each Call Delivery

Optionally, it is possible to 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\CD-xx\TargetList.xml”, where xx represents which type of installed Call Delivery instance. Be sure not to edit or save this file.

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>
  </targets>
</targeting>
```

In this example, John Smith is targeted by his user name, which was configured to be “JohnS”. This value is found in the TargetList.xml file, as shown in red, if the user’s location attribute matches the equivalent entry in the Call Delivery configuration file. 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 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 GUI. 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.

This page is intentionally left blank.

10 Backup and Restore

This chapter describes the backup and restore procedures

10.1 Prerequisites

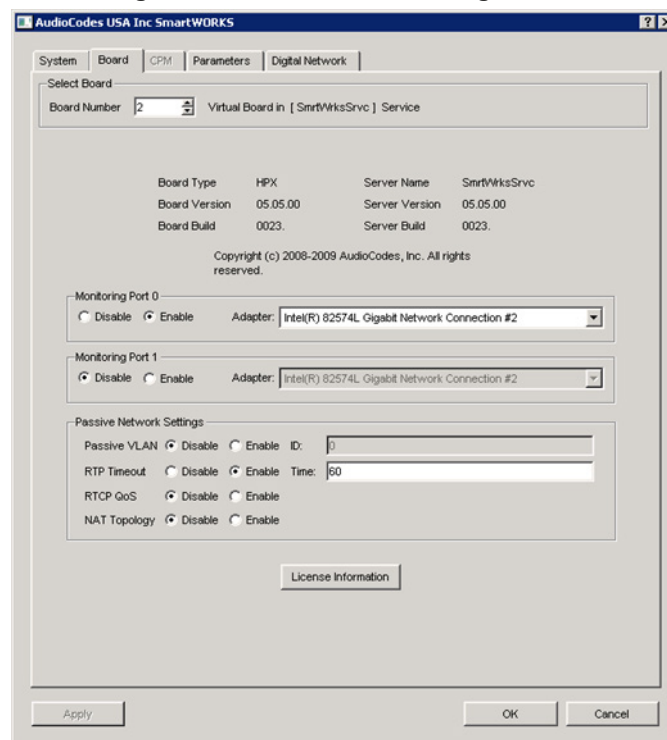
This section describes actions that you need to perform before running backup and restore procedures.

➤ **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 10-1: Board Tab Configuration



3. Run services.msc (Start->Run->type "services.msc" enter), and stop all SmartTAP services.
 - AudioCodes AS (SmartTAP Server)
 - AudioCodes CS (SmartTAP Server)
 - AudioCodes MS (SmartTAP Server)
 - AudioCodes MS-TR (SmartTAP Server)
 - AudioCodes CD-XX (SmartTAP Server)
 - AudioCodes MD (Skype for Business Edge, Mediation or Conference Server)
 - AudioCodes AN (SmartTAP AN Server)
 - AudioCodes MP (SmartTAP MP Server)
 - AudioCodes Skype for Business plug-In (Skype for Business FE or SBA)
 - MySQL (SmartTAP Server)
 - SmartWORKS Service (SmartTAP, Edge, Mediation or Conference Server)

10.2 Backup

This section describes how backup the following components from the command prompt:

- Call Delivery Service (see Section 10.2.1)
- Media Service (see Section 10.2.2)
- Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server (see Section 10.2.3)
- Communication Service (see Section 10.2.4)
- Application Service (see Section 10.2.5)
- Database (see Section 10.2.6)
- SmartTAP Skype for Business Plug-in (FE, SBS, SBA) (see Section 10.2.7)
- SmartTAP Announcement Server (see Section 10.2.8)
- SmartTAP Media Proxy (see Section 10.2.9)

10.2.1 Call Delivery Service

Table 10-1: Backup - Call Delivery Service

Configuration	Path	...\AudioCodes\SmartTAP\CD-XX\
	Instructions	Copy ...\\AudioCodes\SmartTAP\CD-XX\Config to \$backup_dir\CD-XX\
Logs	Path	...\AudioCodes\SmartTAP\CD-XX\
	Instructions	Copy ...\\AudioCodes\SmartTAP\CD-XX\Logs to \$backup_dir\CD-XX\



Note: Replace XX with IP, DS or AL depending upon the type of CallDelivery service installed. The SmartTAP server must be added to the Domain.

10.2.2 Media Service

Table 10-2: Backup - Media Service

Configuration	Path	...\AudioCodes\SmartTAP\MS\Server\
	Instructions	Copy ...\\AudioCodes\SmartTAP\MS\Server\bin\ac-hmp20.ini to \$backup_dir\MS\Server\bin\
Logs	Path	...\AudioCodes\SmartTAP\MS \
	Instructions	Copy ...\\AudioCodes\SmartTAP\MS\Log to \$backup_dir\MS\

10.2.3 Media Delivery Service: Installed on Skype for Business Edge, Mediation or Conference Server

Table 10-3: Backup - Media Delivery Service

Configuration	Path	...\AudioCodes\SmartTAP\MD\Config\
	Instructions	Copy ...\\AudioCodes\SmartTAP\MD\Config\ to \$backup_dir\MD\
Logs	Path	...\AudioCodes\SmartTAP\MD \
	Instructions	Copy ...\\AudioCodes\SmartTAP\MD\Logs to \$backup_dir\MD\

10.2.4 Communication Service

Table 10-4: Backup - Communication Service

Configuration	Path	...\AudioCodes\SmartTAP\CS\bin\
	Instructions	Copy ...\\AudioCodes\SmartTAP\CS\bin\service.bat to \$backup_dir\CS\bin\
Logs	Path	...\AudioCodes\SmartTAP\CS \Server\NGP\
	Instructions	Copy ...\\AudioCodes\SmartTAP\CS\Server\NGP\Log to \$backup_dir\CS\Server\NGP\

10.2.5 Application Service

Table 10-5: Backup - Application Service

Configuration	Path	...\AudioCodes\SmartTAP\AS\bin\
	Instructions	Copy ...\\AudioCodes\SmartTAP\AS\bin\service.bat to \$backup_dir\AS\bin\
Logs	Path	...\AudioCodes\SmartTAP\AS\standalone\
	Instructions	Copy ...\\AudioCodes\SmartTAP\AS\standalone\log to \$backup_dir\AS\standalone\

10.2.6 Database

Table 10-6: Backup - Database

Configuration	Path	...\MySQL\MySQL Server 5.6\
	Instructions	Stop SmartTAP 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_dir\MySQL_PD\
		Start MySQL & SmartTAP AS service

10.2.7 SmartTAP Skype for Business Plug-in (FE, SBS, SBA)

Table 10-7: SmartTAP Skype for Business Plug-in (FE, SBS, SBA)

Configuration	Path	...\\AudioCodes\\SmartTAP\\SmartTAP Lync Client\\
	Instructions	Copy ...\\AudioCodes\\SmartTAP\\SmartTAP Lync Client\\SmartTapLyncSvc.exe.config to \$backup_dir\\SmartTap Lync Client\\FE#\\
Logs	Path	...\\AudioCodes\\SmartTAP\\SmartTAP Lync Client\\
	Instructions	Copy ...\\AudioCodes\\SmartTAP\\SmartTAP Lync Client\\Logs to \$backup_dir\\SmartTap Lync Client\\



Note: Replace # in instructions above to the actual ID # of the FE server. Repeat above instructions for each FE in Pool.

10.2.8 SmartTAP Announcement Server

Table 10-8: Backup - SmartTAP Announcement Server

Configuration	Path	...\\AudioCodes\\SmartTAP\\AN\\Config
	Instructions	Copy Config folder to \$backup_dir\\AN\\
Logs	Path	...\\AudioCodes\\SmartTAP\\AN\\Logs
	Instructions	Copy Log folder to \$backup_dir\\AN\\

10.2.9 SmartTAP Media Proxy

Table 10-9: Backup - SmartTAP Media Proxy

Configuration	Path	...\\AudioCodes\\SmartTAP\\MP\\Config
	Instructions	Copy Config folder to \$backup_dir\\AN\\
Logs	Path	...\\AudioCodes\\SmartTAP\\MP\\Logs
	Instructions	Copy Log folder to \$backup_dir\\AN\\

10.2.9.1 Media

Copy the directory structure and media files from the path defined in the SmartTAP 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.

Figure 10-2: Add Recording Location

The screenshot shows a dialog box titled "Add Recording Location". It has the following fields and values:

- Location Name:** Prime Media Storage
- Description:** Storage location for media recordings
- Scheme:** file (dropdown menu)
- Host:** (empty text box)
- Path:** /C:/media/yyyy/MMMMM/dd/HHmmss

At the bottom right, there are two buttons: "Submit" (with a green checkmark icon) and "Cancel" (with a red X icon).

10.2.9.2 System Profile Tool

The System Profile Tool provides a convenient method to capture all the log files for the SmartTAP services on a specific server.

Table 10-10: System Profile Tool

Configuration	Path	...\\AUDIOCODES\\Tools\\
	Instructions	<ul style="list-style-type: none"> 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 <p>Note: Before you run a test, you must go to the folder of the SmartTAP service and set the appropriate log level</p>

10.3 Restore

This section describes how to restore the SmartTAP components.

➤ To restore the SmartTAP components:

1. Install SmartTAP on the new server.
2. Run services.msc (**Start > Run >** type "services.msc" enter), and stop all SmartTAP services.



Note: You MUST restore to the same version of SmartTAP that was backed up (with the same major and minor versions).

This section describes how to restore the following components:

- Call Delivery Service (see Section 10.3.1)
- Media Service (see Section 10.3.2)
- Media Delivery Service (see Section 10.3.3)

- Database (see Section 10.3.4)
- SmartTAP Skype for Business Plug-in (FE, SBS, SBA) (see Section 10.3.5)
- Announcement Server (see Section 10.3.6)
- Media Proxy (see Section 10.3.7)
- Media (see Section 10.3.8)

10.3.1 Call Delivery Service

Table 10-11: Restore – Call Delivery Service

Configuration	Path	...\AudioCodes\SmartTAP\CD-XX\
	Instructions	Rename ...\\AUDIOCODES\SmartTAP\CD-XX\Config to Config.orig Copy \$backup_dir\CD_XX\Config to ...\\AUDIOCODES\SmartTAP\CD-XX\



Note: Replace XX with IP, DS or AL depending upon the type of CallDelivery service installed.

10.3.2 Media Service

Table 10-12: Restore – Media Service

Configuration	Path	...\AudioCodes\SmartTAP\MS\Server\bin\
	Instructions	Rename ...\\AUDIOCODES\SmartTAP\MS\Server\bin\ac-hmp20.ini to ac-hmp20_orig.ini Copy \$backup_dir\MS\Server\bin\ac-hmp20.ini to ...\\AUDIOCODES\SmartTAP\MS\Server\bin\

10.3.3 Media Delivery Service

Table 10-13: Restore – Media Delivery Service

Configuration	Path	...\AudioCodes\SmartTAP\MD\
	Instructions	Rename ...\\AudioCodes\SmartTAP\MD\Config\ folder to \Config.orig Copy \$backup_dir\MD\Config to ...\\AudioCodes\SmartTAP\MD\

10.3.4 Database

Table 10-14: Restore – Database

Configuration	Path	...\MySQL\MySQL Server 5.6\
	Instructions	Stop SmartTAP 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 AS service

10.3.5 SmartTAP Skype for Business Plug-in (FE, SBS, SBA)

This step is only required if the FE, SBS or SBA was rebuilt

Table 10-15: Restore – SmartTAP Skype for Business Plug-in (FE, SBS, SBA)

Configuration	Path	...\AudioCodes\SmartTAP\Lync Plug-in\
	Instructions	Copy \$backup_dir\ Lync Plug-in\FE#\LyncPlugIn.exe.config to ...\\AudioCodes\SmartTAP\Lync Plug-in\



Note: Replace # in instructions above to the actual ID # of the FE server. Repeat above instructions for each FE in Pool.

10.3.6 Announcement Server

Table 10-16: Restore – Announcement Server

Configuration	Path	...\AudioCodes\SmartTAP\AN\
	Instructions	Rename ...\\AudioCodes\SmartTAP\AN\Config\ folder to \Config.orig Copy \$backup_dir\AN\Config to ...\\AudioCodes\SmartTAP\AN\

10.3.7 Media Proxy

Table 10-17: Restore – Media Proxy

Configuration	Path	...\AudioCodes\SmartTAP\MP\
	Instructions	Rename ...\\AudioCodes\\SmartTAP\\MP\\Config\\ folder to \\Config.orig Copy \$backup_dir\\MP\\Config to ...\\AudioCodes\\SmartTAP\\MP\\

10.3.8 Media

This section describes how to restore media.

➤ **To restore media:**

1. Copy the directory structure and media files from the path defined in the SmartTAP 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.

Figure 10-3: Add Recording Location

2. Reboot the SmartTAP machine
3. Check SmartTAP 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.

11 Troubleshooting

This chapter is for technical personnel who are responsible for the installation and maintenance of the SmartTAP 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 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.

11.1 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 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.

11.1.1 Prerequisites

The following tools and Administrative privileges are required to perform the procedure in this document:

- Wireshark or IP sniffer tool on SmartTAP 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

11.1.1.1 Introduction: SmartTAP Recording Concepts

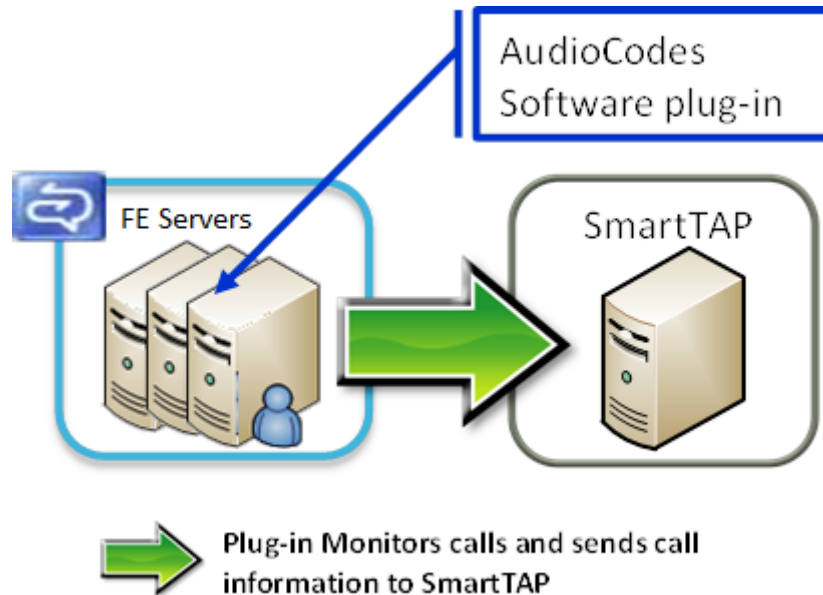
The SmartTAP recorder relies on a Microsoft Certified Skype for Business plugin to process the call signaling and on the availability of the MEDIA for the call at the recording NIC interface(s).

The Skype for Business plugin resides on the Front End Server(s) and provides the call details to the SmartTAP recorder which records the MEDIA for the call through the recording NIC interface.

11.1.1.2 SmartTAP Processing of Skype for Business Signaling

The SmartTAP 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 plugin is responsible for collecting the call information (signaling) and sending it to the SmartTAP recorder as shown below in Figure 11-1.

Figure 11-1: AudioCodes Software Plugin

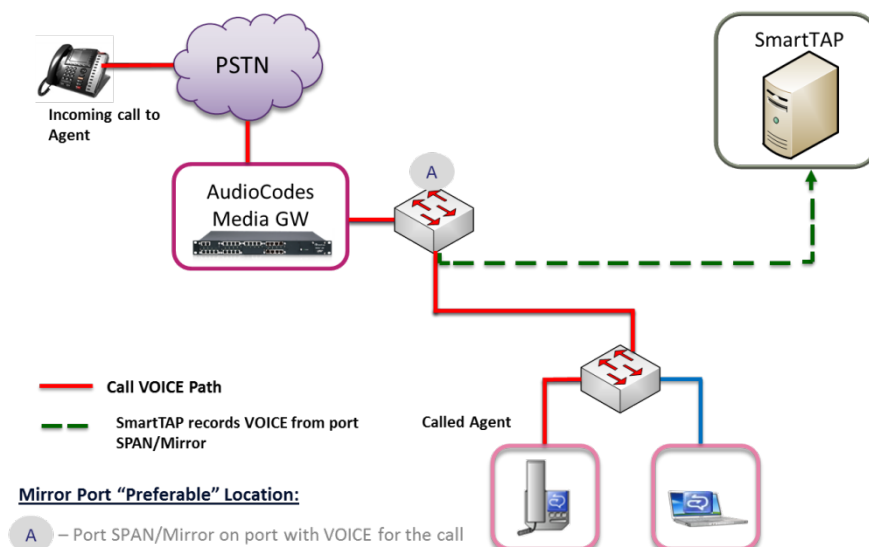


Whether the SmartTAP Skype for Business plugin is installed, the Skype for Business Administrator has access to logging facilities that enables the logging of SIP signaling and saving these logs to a text file. This log file contains the Skype for Business call information and the MEDIA information that correlates with the call information that the plugin sends to the SmartTAP recorder.

11.1.1.3 SmartTAP Media Processing

The SmartTAP 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 at the recording NIC interface (or interfaces if 2 recording NICs). The recording NIC interface is connected to the switch/router interface that forwards the mirrored data.

Figure 11-2: SmartTAP Media Processing



11.1.2 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.

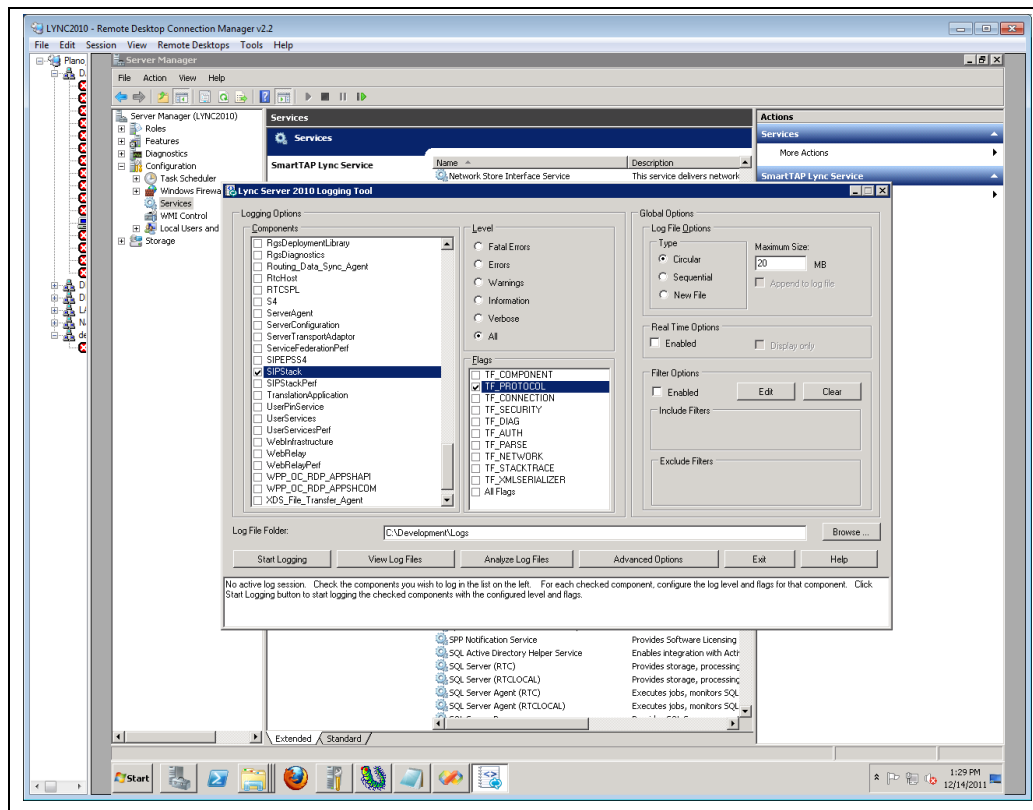
11.1.2.1 Setup Skype for Business Logging

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**.

Figure 11-3: Skype for Business Logging



11.1.2.2 Setup Sniffer

This section describes how to setup the sniffer.

➤ **To setup the sniffer:**

1. Log into the test PC (or SmartTAP Server).
2. Start the sniffer software (Wireshark).
3. Select the recording NIC interface to monitor.

11.1.2.3 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...).

11.1.3 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.

11.1.3.1 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;ms-
opaque=f265f30ed4;ms-received-cid=FB00;grid SIP/2.0
From:
<sip:ocs_client3@planolab.audiocodes.com>;tag=79882da9cf;e
pid=518fe1de1d
To:
<sip:ocs_client2@planolab.audiocodes.com>;epid=ad43a533af;
tag=e63e42b63f
CSeq: 3 INVITE
Call-ID: 3c5eed8dfdc748729bd72ad2c64bf510
... (removed text here)
o=- 0 0 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:1 1 UDP 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)
```



Note: 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.

11.1.3.2 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.

Figure 11-4: Sniffer Trace

lync call for paul.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

Filter: `ip.addr == 10.133.11.71 and ip.addr == 10.133.11.73`

No.	Time	Source	Destination	Protocol	Length	Info
485	9.200563	10.133.11.71	10.133.11.73	STUN	146	Binding Request user: E385:I//2
537	9.229705	10.133.11.71	10.133.11.73	CLASSIC-S	86	Message: Binding Request
540	9.280358	10.133.11.71	10.133.11.73	STUN	146	Binding Request user: E385:I//2
541	9.280429	10.133.11.71	10.133.11.73	STUN	146	Binding Request user: E385:I//2
542	9.306160	10.133.11.73	10.133.11.71	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: 10.133.11.71:26064 user:
554	9.331301	10.133.11.71	10.133.11.73	STUN	146	Binding Request user: E385:I//2
558	9.355431	10.133.11.73	10.133.11.71	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: 10.133.11.71:26065 user:
559	9.355528	10.133.11.73	10.133.11.71	STUN	146	Binding Request user: I//2:E385
560	9.355572	10.133.11.73	10.133.11.71	STUN	146	Binding Request user: I//2:E385
561	9.381954	10.133.11.71	10.133.11.73	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: 10.133.11.73:1462 user: I
562	9.382162	10.133.11.71	10.133.11.73	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: 10.133.11.73:1463 user: I
859	13.852980	10.133.11.73	10.133.11.71	CLASSIC-S	86	Message: Binding Request
861	13.911661	10.133.11.73	10.133.11.71	STUN	150	Binding Request user: I//2:E385
862	13.911751	10.133.11.73	10.133.11.71	STUN	150	Binding Request user: I//2:E385
863	13.932921	10.133.11.71	10.133.11.73	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: 10.133.11.73:1462 user: I
864	13.933108	10.133.11.71	10.133.11.73	STUN	130	Binding Success Response XOR-MAPPED-ADDRESS: 10.133.11.73:1463 user: I
870	14.093031	10.133.11.71	10.133.11.73	UDP	85	Source port: 26065 Destination port: nucleus
871	14.093103	10.133.11.71	10.133.11.73	UDP	197	Source port: 26065 Destination port: nucleus
902	15.522599	10.133.11.71	10.133.11.73	UDP	85	Source port: 26065 Destination port: nucleus
903	15.522701	10.133.11.71	10.133.11.73	UDP	217	Source port: 26065 Destination port: nucleus
925	17.521083	10.133.11.73	10.133.11.71	UDP	85	Source port: nucleus Destination port: 26065
926	17.521114	10.133.11.73	10.133.11.71	UDP	233	Source port: nucleus Destination port: 26065
928	17.878241	10.133.11.71	10.133.11.73	UDP	85	Source port: 26065 Destination port: nucleus
929	17.878440	10.133.11.71	10.133.11.73	UDP	217	Source port: 26065 Destination port: nucleus
932	18.081266	10.133.11.71	10.133.11.73	UDP	85	Source port: 26065 Destination port: nucleus
933	18.081358	10.133.11.71	10.133.11.73	UDP	217	Source port: 26065 Destination port: nucleus
936	18.284338	10.133.11.71	10.133.11.73	UDP	85	Source port: 26065 Destination port: nucleus
937	18.284442	10.133.11.71	10.133.11.73	UDP	217	Source port: 26065 Destination port: nucleus
939	18.593043	10.133.11.71	10.133.11.73	UDP	217	Source port: 26065 Destination port: nucleus
940	18.593148	10.133.11.71	10.133.11.73	UDP	217	Source port: 26065 Destination port: nucleus

Frame 939: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)

Ethernet II, Src: Dell 4a:b8:78 (00:14:28:4a:b8:78), Dst: Dell 4b:4f:ef (00:14:22:4b:4f:ef)

Internet Protocol Version 4, Src: 10.133.11.71 (10.133.11.71), Dst: 10.133.11.73 (10.133.11.73)

User Datagram Protocol, Src Port: 26065 (26065), Dst Port: nucleus (1463)

Data (43 bytes)

11.1.3.3 Determine Whether SmartTAP 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 recording requirements for Skype for Business.

11.2 Troubleshooting Skype for Business Plugin Installation

This section describes the troubleshooting options when the Skype for Business installation plugin fails.

11.2.1 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.

11.2.2 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
```

```
-----
-----
```

```
\\BE
\\EDGE
\\FE1
\\OCS-CLIENT3
\\OCSCIENT1
\\QA-USER2
\\SMARTTAP
```

```
The command completed successfully.
```

11.3 Troubleshoot Skype for Business Recording

This section describes troubleshooting for Skype for Business Recording.

11.3.1 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 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.

11.3.2 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.

11.3.3 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**

12 Known Issues

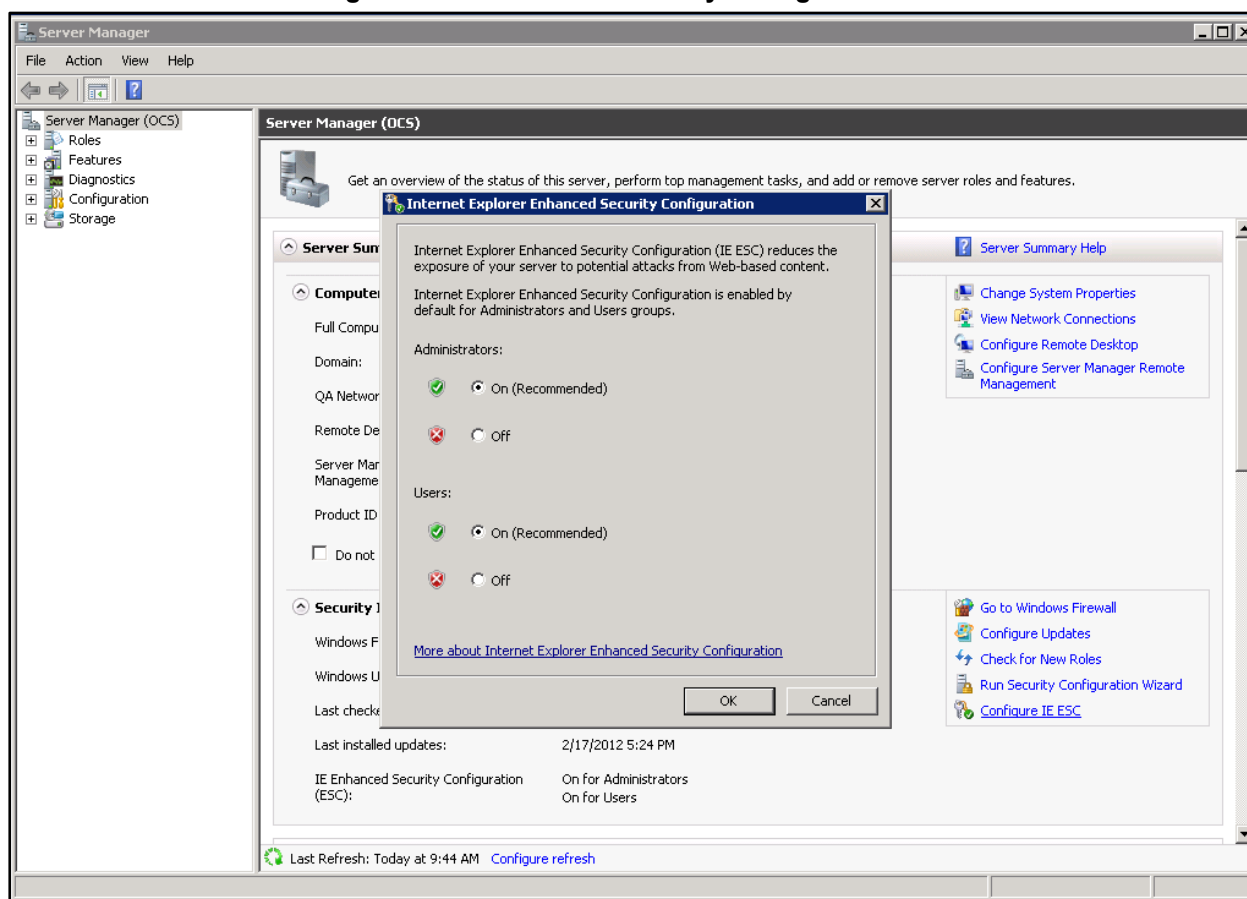
This chapter describes known issues.

12.1 Internet Explorer Security Messages and SmartTAP not Running on Server

Sometimes when configuring SmartTAP on its machine, IE pops-up security messages and/or avoids SmartTAP 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:

Figure 12-1: Enhanced Security Configuration



International Headquarters

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

AudioCodes Inc.

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

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

website: www.audiocodes.com

©2018 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 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-27188

