

400HD IP Phones Series - Teams Compatible

Version 3.4.6



Microsoft Partner

Gold Communications

 Skype for Business

 **audiocodes**

Table of Contents

WEEE EU Directive.....	14
Customer Support	14
Stay in the Loop with AudioCodes	14
Abbreviations and Terminology.....	14
Documentation Feedback.....	14
Related Documentation.....	15
1 Introduction	16
2 Automatic Mass Provisioning of IP Phones using DHCP	17
2.1 Preparing the Microsoft Skype for Business Environment for IP Phones.....	19
2.1.1 Making Sure DHCP Server Options are Correctly Configured.....	19
2.1.1.1 DHCP Option 43.....	20
2.1.1.2 VLAN Discovery via DHCP Option 43	20
2.1.1.3 DHCP Option 120.....	20
2.1.1.4 DHCP Option 42.....	21
2.1.1.5 DHCP Scope Option	21
2.1.2 Making Sure the DHCP Server is Correctly Configured for Auto Provisioning.....	34
2.2 Creating a Configuration File for Auto Provisioning	35
2.2.1 Saving a Single Phone's Default Configuration as a .cfg File	35
2.2.2 Configuring the Phone According to Requirements	36
2.2.3 Save the Phone's Newly Configured Settings as a .cfg File	36
2.2.4 Creating a Delta Configuration .cfg File	36
2.2.5 Loading the Delta .cfg File to Another Phone, Signing In, Testing	36
2.2.5.1 Loading the Delta .cfg File to Another Phone	37
2.2.5.2 Signing In to the Phone.....	37
2.2.5.3 Testing the Phone.....	37
2.2.5.4 Changing the Order of the Sign-In Method.....	37
2.2.5.5 Allowing Users to Display Phone # or Ext # in Phone Screen	38
2.2.5.6 Forcing Sign-in with PIN Code	38
2.2.5.7 Online Sign-in through Microsoft's Cloud PBX	39
2.2.5.8 Disabling AutoDiscover Web Service Protocol	40
2.3 Copying the Configuration File to the Provisioning Server	40
2.4 Triggering Automatic Provisioning	40
2.5 Troubleshooting Automatic Provisioning	41
2.5.1 Using the Phone Screen	41
2.6 Device Manager.....	43
2.7 Audiocodes Device Manager Validation.....	44
2.7.1 Introduction	44
2.7.2 Prerequisites	44

2.7.3	Overview	44
2.7.4	Existing Root CA Files in IP Phone.....	45
2.7.5	Certification Details Dialog.....	46
3	Manual Configuration of a Single IP Phone.....	47
3.1	Configuring Network Connections	47
3.1.1	Configuring LAN Connection Type.....	47
3.1.2	Configuring LAN Port / PC Port.....	50
3.1.3	Configuring VLAN Settings	51
3.2	Configuring Personal Settings	52
3.2.1	Configuring Language	52
3.3	Configuring Function and Programmable Keys.....	53
3.3.1	Configuring a Function Key	55
3.3.1.1	Configuring a Function Key for Speed Dialing	55
3.3.1.2	445HD, 450HD, C450HD and RX50	56
3.3.1.3	Configuring a Function Key for Making a Discreet Call	57
3.3.2	Configuring Programmable Keys	58
3.3.3	Configuring Programmable Softkeys for a Customized UI Experience	60
3.3.4	Configuring a Programmable Softkey to Allow Paging during an Ongoing Call Call Hold Call Park61.....	
3.3.5	Configuring Tones.....	62
3.3.5.1	Configuring CPT Regional Settings.....	62
3.3.5.2	Uploading Ring Tones	64
3.3.6	Configuring Phone Screen Settings.....	65
3.3.7	Configuring a Distinctive Ring Tone	68
3.4	Configuring VoIP Settings.....	69
3.4.1	Configuring TLS/SSL over SIP	69
3.4.2	Configuring TLS/SSL over SIPE	70
3.4.3	Configuring an Outbound Proxy	71
3.4.4	Configuring IP Phone Office 365 Services via HTTP Proxy Support.....	72
3.4.5	Configuring Dialing	73
3.4.5.1	Adjusting the DTMF Level	73
3.4.5.2	Configuring Automatic Dialing	73
3.4.5.3	Configuring Pause Dialing for a Speed Dial to an Ext. behind an IVR.....	74
3.4.5.4	Configuring Default Audio Device	74
3.4.6	Enabling Direct Voice Dialing.....	75
3.4.7	Disabling the Phone Microphone	76
3.4.8	Configuring the TRANSFER Key to Perform Consultative Transfer	76
3.4.9	Enabling Semi-Consultative Transfer	77
3.4.10	Disabling the BXfer (Blind Transfer) Softkey	77
3.4.11	Enabling Electronic Hook Switch	78
3.4.12	Disabling Audial Call Waiting Indication.....	79

3.4.13	Disabling Call Forward	79
3.4.14	Configuring Busy on Busy.....	80
3.4.15	Configuring Disconnect if Handset On-Hooked after Putting Call on Hold	80
3.4.16	Configuring Media Streaming.....	81
3.4.16.1	Configuring Quality of Service.....	81
3.4.16.2	Configuring Codecs.....	82
3.4.16.3	Configuring Real Time Protocol (RTP) Port Range	83
3.4.16.4	Configuring RTCP Extended Report	84
3.4.16.5	Configuring Media Bypass.....	85
3.4.17	Enabling Paging	86
3.4.18	Enabling Barge-in.....	87
3.4.19	Configuring the VocaNOM Service	88
3.4.20	Configuring a Dedicated Voicemail Server	89
3.4.21	Securing Voicemail Access by PIN Code Authentication	90
3.4.22	Setting up a Cloud User's Voicemail / MWI.....	90
3.4.22.1	Enabling Unified Messaging	94
3.4.22.2	Troubleshooting	96
3.5	Configuring Security	97
3.5.1	Using the Encryption Tool.....	97
3.5.1.1	Encrypting Configuration Files	97
3.5.2	Encrypting Passwords in Configuration File	97
3.5.3	Managing Security Certificates.....	98
3.5.3.1	Loading the Root CA Certificate to the Phone	98
3.5.3.2	Loading the Client Certificate to the Phone	99
3.5.3.3	Enabling Server-side Authentication (Mutual Authentication)	100
3.5.3.4	Generating a Certificate Signing Request	101
3.5.4	Server Certificate Validation for Secured HTTPS Communications over SSL.....	101
3.5.5	Configuring 802.1X Authentication	102
3.5.5.1	Using the Phone Screen.....	102
3.5.5.2	EAP MD5 Mode	102
3.5.5.3	EAP TLS Mode	102
3.5.6	Using the Configuration File.....	103
3.5.6.1	EAP MD5 Mode	103
3.5.6.2	EAP TLS Mode	103
3.5.7	Configuring HTTPS	104
3.5.8	Supported Encryption Ciphers and TLS Version	104
3.5.9	Support for Enterprise HTTP/S Proxy Servers	105
3.6	Configuring Advanced Applications.....	106
3.6.1	Wi-Fi Capability	106
3.6.2	Bluetooth	106
3.6.3	Dynamic URL Provisioning.....	106

3.6.4	Configuring Date and Time	109
3.6.4.1	Configuring NTP Server	112
3.6.4.2	Configuring NTP Server via DHCP	113
3.6.5	Configuring Contacts (LDAP)	115
3.6.6	Configuring T9	117
3.6.7	Configuring the Caller Name to be Displayed	117
4	Configuring Microsoft Skype for Business Features	118
4.1	Microsoft Screen Theme	118
4.2	Configuring Phone Status and User Status Timeouts	118
4.3	Park Call	118
4.4	Music on Hold (MoH)	118
4.5	Configuring Timeouts for Presence Status Changes	120
4.6	Group Call Pickup (GCP)	120
4.7	Location	120
4.8	Configuring Skype for Business Server for SRTP / TLS	121
4.9	Updating Device Firmware from the Skype for Business Server	122
4.9.1	Enabling Automatic Firmware Updates from the Server	122
4.9.2	Enabling Automatic Firmware Updates from the Server using Configuration File	123
4.9.3	Manually Downloading Firmware to the Phone from the Server	123
4.10	Enabling Phone Lock	124
4.10.1	Allowing Users Other Capabilities besides Emergency Calls if Phones Lock	125
4.10.1.1	Allowing Users to use the Phone's Handset	125
4.10.1.2	Allowing Users to Make/Receive Incoming/Outgoing Calls	125
4.10.1.3	Allowing Users to Answer Second-Hand (SLA Delegation) Incoming Calls	126
4.11	Exchange Server Features	126
4.11.1	Configuring Calendar Displayed in the Phone's Screen	127
4.11.2	Configuring Meeting Reminders Popping up in the Phone's Screen	128
4.11.3	Visual Voicemail	128
4.11.4	Skype for Business 'Favorites' Contacts & Outlook Contacts	129
4.12	Better Together over Ethernet	129
4.12.1	BToE Firewall Ports	130
4.12.2	Installing the BToE PC Application	130
4.12.3	Distributing the BToE PC Application msi Package	138
4.12.4	Making Sure BToE is Correctly Installed	139
4.12.5	Enabling BToE for Online Users in the Skype for Business Server	139
4.12.6	Configuring the BToE TCP Port	140
4.12.7	Automatically Pairing the BToE PC/Laptop Application with the IP Phone	141
4.12.8	Manually Pairing the BToE PC/Laptop Application with the Phone	141
4.12.8.1	Support for Citrix XenDesktop VDI	141
4.12.8.2	Manually Generating a Pair Code	142

4.12.8.3	Connecting the IP Phone with the BToE PC/Laptop Application	142
4.12.9	Connecting the Skype for Business Client with the IP Phone	145
4.12.10	Making Sure IP Phone/ Skype for Business Client are Paired	146
4.12.10.1	Making Sure the Skype for Business Client is Paired	146
4.12.10.2	Making Sure the Phone is Paired with the PC/Laptop	146
4.12.11	Configuring Mode of Operation for Phone-PC Pairing	146
4.12.12	Pairing Across Different Subnets	147
4.12.13	Troubleshooting	148
4.13	Device Duo	148
4.13.1	Benefits	148
4.13.2	Installing the Device Duo on the PC	148
4.13.3	Making Sure Device Duo is Correctly Installed	152
4.13.4	Pairing the Device Duo Application with the IP Phone	152
4.13.4.1	Pairing Code	153
4.13.4.2	Automatically Pairing the RXV100Hub with the RX50	155
4.13.4.3	Automatic Pairing using PC Port	157
4.13.5	Configuring Mode of Operation for Phone-PC Pairing	158
4.13.6	Pairing Across Different Subnets	159
4.13.7	Troubleshooting	159
4.14	Boss Admin	160
4.14.1	Viewing Admin Lines on Boss's Phone	163
4.14.2	Viewing Boss's Line on Admin's Phone	163
4.14.3	Configuring Boss Privacy Mode	163
4.15	Enabling the Delegated Line Feature	164
4.15.1	Configuring Boss Admin Delegated Line	165
4.15.1.1	Configuring Multiple Points of Presence (MPOPs)	165
4.15.1.2	Configuring Boss-Admin Sidecar Functionality	165
4.16	Configuring a Distinctive Ring on the Phone of Each Boss	166
4.17	Configuring Phones to Operate in an OVR Deployment	166
4.18	Disabling Local 3-Way Conferencing Capability	167
4.19	Blocking All Phone Users from Signing Out	167
4.20	Enabling HotDesking	167
4.21	Uploading Logs to Microsoft Server for Support Purposes	168
4.22	Enabling an IP Phone Voice Quality Check	169
4.23	Signing in / out with the Web Interface	170
4.24	Signing in and Authenticating with Microsoft's Cloud PBX	172
4.25	Initiating a Skype for Business Server Based Phone Conference	172
4.26	Provisioning the Server for Downloading Contacts Pictures	173
4.26.1	Disabling Contacts Pictures	174
4.27	Enabling QoE Reports to be Sent to Microsoft's SQL Server	175

4.28	Enabling Malicious Call Tracing	176
4.29	Disabling the C450HD IP Phone Screen Saver	177
4.30	Registering the Phone on Azure Cloud	177
5	Maintenance	178
5.1	Upgrading Phone Firmware	178
5.2	Enabling/Disabling Device Update	179
5.3	Administration.....	180
5.3.1	Managing Users.....	180
5.3.2	Managing the Web Login Sign-in Option	180
5.3.3	Allowing / Disallowing Management via the Web Interface.....	181
5.3.4	Restoring Defaults	181
5.3.5	Restarting the Phone	181
5.4	Enabling Remote Management.....	181
5.4.1	Enabling Telnet Access.....	181
5.4.2	Enabling SSH Access.....	182
6	Status and Performance.....	183
6.1	Viewing Network Status.....	183
6.1.1	Viewing LAN Status.....	183
6.1.2	Viewing Port Mode Status.....	183
6.1.3	Viewing 802.1X Status	183
6.2	Viewing VoIP Status	184
6.2.1	Viewing Phone Status	184
6.2.2	Viewing Line Status.....	184
6.2.3	Viewing Call Information.....	184
6.3	Viewing Call History	185
6.4	Viewing Phone Model / Firmware Version	186
6.4.1	Viewing from the Phone's Screen.....	186
6.4.2	Viewing Release Information	186
7	Diagnostics.....	187
7.1	Logging.....	187
7.1.1	Analyzing and Debugging Traffic using Syslog	187
7.1.2	Analyzing and Debugging Traffic using Syslog.....	189
7.2	Enabling Recording to Debug Voice	189
7.3	Downloading a Tombstone Dump.....	190
7.4	Activating Core Dump.....	191
7.5	Monitoring: Traceroute	192
7.6	Enabling Port Mirroring	192
8	Troubleshooting.....	193
8.1	Unable to Sign in to Skype for Business using Username/Password	193

8.2	Unable to Authenticate User using PIN	193
8.3	IP Phone Fails Registration Process	193
8.4	How to Verify CA Certificate is Trusted / Authorized by IP Phone	194
8.5	Invalid Time Server	194
8.6	Invalid Time Offset	194
8.7	General Corrective Actions	195
8.7.1	Restoring Phone Defaults.....	195
8.7.1.1	Restoring Factory Defaults from the Phone Screen	195
8.7.1.2	Restoring Factory Defaults from the Web Interface.....	195
8.7.2	Loading the Configuration File Manually	196
8.7.3	Recovering Firmware	197
8.7.4	Restarting the Phone	197
8.7.4.1	Restarting the Phone from the Screen	197
8.7.4.2	Restarting the Phone from the Web Interface.....	198
A	Installing the Expansion Module.....	199
A.1	Installation Procedure	199
A.1.1	Step 1: Place Phone and Module on a Table	199
A.1.2	Step 2: Invert and Unscrew Three Screws.....	200
A.1.3	Step 3: Remove Rubber Cover and Connect	200
A.1.4	Step 4: Attach the Panel.....	201
A.1.5	Step 5: Secure the Side Panel.....	201
A.1.6	Step 6: Secure the Connection of the Two Units.....	202
A.1.7	Step 7: Mount Phone on Base Stand, Expansion Module on Base Stand	202
B	Alternative Automatic Provisioning Methods.....	203
B.1	Static DNS Record Method.....	203
B.2	AudioCodes' HTTPS Redirect Server	205
B.2.1.1	Redirection Process	206
C	Recovering AudioCodes' IP Phone	207
C.1	Identifying that the Phone is in Recovery Mode	207
C.2	Making Sure the Phone is in Recovery Mode	208
C.3	Recovering the Phone.....	209
C.4	Make Sure the Phone is Downloading the Image File	211
C.4.1	Making Sure Using Wireshark	211
C.4.2	Making Sure Using tftpd64.....	213
C.4.3	Making Sure Using the Phone Screen	213
D	Huddle Room Solution (HRS)	214
E	Migrating from Skype for Business to Teams Environment.....	216
E.1	Signing in with Web Sign-in (Cloud)	216
E.2	Signing Out and then Signing In Again.....	218

- F Switching Devices from Teams Compatible to Teams Native Mode219**
- F.1 Prerequisites 219
- F.2 Upload Software Files to the Device Manager..... 219
 - F.2.1 Enable MD5 File Uploading to the Device Manager 219
 - F.2.2 Upload Teams Compatible Firmware File 220
 - F.2.3 Upload Teams Native Firmware 222
 - F.2.4 Upload MD5 File..... 222
 - F.2.5 Verify Files Successful Upload 222
- F.3 Add Parameters to Provision in the Teams Phone Template 223
- F.4 Upgrade the Phone to Teams Compatible Transition Firmware..... 224
- F.5 Generate Configuration on the Phone 224
- F.6 Verify Successful Upgrade to Teams Native 225
- G Specifications226**
- G.1 SIP Support (RFC, Headers) 226
 - G.1.1 SIP Compliance Tables 228
 - G.1.1.1 SIP Methods..... 228
 - G.1.1.2 SIP Headers 228

List of Figures

Figure 2-1: Setting up Automatic Provisioning	18
Figure 2-2: DHCP Server Options	19
Figure 2-3: DHCP Options Assigned to IPv4 Addresses	21
Figure 2-4: Defining User Classes	22
Figure 2-5: DHCP User Classes	22
Figure 2-6: New Class	22
Figure 2-7: Packet Bytes Window	23
Figure 2-8: DHCP User Classes	23
Figure 2-9: Set Predefined Options	24
Figure 2-10: Predefined Options and Values	24
Figure 2-11: Option Type – Add AudioCodes 160 Option	25
Figure 2-12: Predefined Options and Values – Add IP Phone Management Server Location	25
Figure 2-13: 'Scope Leased' Folder - Configure Options	26
Figure 2-14: Configure Options 1	26
Figure 2-15: Configure Options 2	27
Figure 2-16: Server Options	27
Figure 2-17: Scope Options Created [Illustrative Purposes Only]	28
Figure 2-18: New Policy	28
Figure 2-19: DHCP Policy Configuration Wizard – Policy Name	29
Figure 2-20: DHCP Policy Configuration Wizard - Add	29
Figure 2-21: Add/Edit Condition	30
Figure 2-22: Policy Conditions	31
Figure 2-23: Policy Settings – IP Address Range for the Policy	31
Figure 2-24: Policy Settings – Available Options	32
Figure 2-25: Policy Settings – Summary	33
Figure 2-26: DHCP GUI - Policy Name: AudioCodes IPP User Class	33
Figure 2-27: Web Interface - Configuration File	35
Figure 2-28: Web Interface – Loading a New Configuration File	37
Figure 3-1: HTTP Proxy Functioning	72
Figure 3-2: Exchange Admin Center - Unified Messaging	91
Figure 3-3: Setting up a Dial Plan	92
Figure 3-4: New Dial Plan: URI Type = SIP URI	92
Figure 3-5: Dial Plan: Rules and Settings	93
Figure 3-6: Edit	93
Figure 3-7: Enabling UM for Users	94
Figure 3-8: Enabling UM	94
Figure 3-9: Browse to the UM Dial Plan	95
Figure 3-10: User's SIP Address and/or Extension Number, and PIN	95
Figure 3-11: Troubleshooting – Protected Voice Mail	96
Figure 3-12: Web Interface – Certificate Signing Request	101
Figure 4-1: Skype for Business Server - Edit Trunk Configuration - Global	121
Figure 4-2: Microsoft Server Page from which the Firmware Version is Updated	122
Figure 4-3: Web Interface – Automatic Provisioning	123
Figure 4-4: InstallShield Wizard – Preparing to Install	131
Figure 4-5: Welcome to the InstallShield Wizard	131
Figure 4-6: License Agreement	132
Figure 4-7: License Agreement	132
Figure 4-8: Destination Folder	133
Figure 4-9: Change Current Destination Folder	134
Figure 4-10: Ready to Install	134
Figure 4-11: Installing AudioCodes Better2Gether	135
Figure 4-12: InstallShield Wizard Completed	135
Figure 4-13: AudioCodes Icon in Taskbar	136

Figure 4-14: Control Panel>Programs>AudioCodes Better2Gether.....	136
Figure 4-15: Computer Management > Services and Applications.....	137
Figure 4-16: Device Manager > AudioCodes B2GoE USB Driver.....	137
Figure 4-17: Popup Menu.....	139
Figure 4-18: About AC BToE.....	139
Figure 4-19: TCP Port.....	140
Figure 4-20: AC BToE TCP Port.....	140
Figure 4-21: Popup Menu.....	142
Figure 4-22: Phone Pairing.....	142
Figure 4-23: AC BToE Failed Indication.....	143
Figure 4-24: AC BToE is Connected Indication.....	143
Figure 4-25: Popup Menu: 'Disconnect' Enabled, 'Phone Pairing' Disabled.....	143
Figure 4-26: BToE Disconnected.....	143
Figure 4-27: Popup Menu: BToE Disconnected.....	143
Figure 4-28: Start > Programs > AudioCodes > BToE Controller.....	144
Figure 4-29: Sign-in Request Prompt.....	145
Figure 4-30: Web Interface - Configuration File.....	147
Figure 4-31: Popup Menu.....	152
Figure 4-32: About AudioCodes Device Duo.....	152
Figure 4-33: Web Interface - Configuration File.....	159
Figure 4-34: Skype for Business Client – Call Forwarding Settings.....	160
Figure 4-35: Skype for Business Client - Edit my delegate members.....	161
Figure 4-36: Skype for Business Client – Call Forwarding – Add Delegates.....	161
Figure 4-37: Skype for Business Client – Call Forwarding – Added Delegate - Receive Calls.....	162
Figure 4-38: Skype for Business Client – Call Forwarding – Simultaneously ring - My Delegates.....	162
Figure 4-39: Sign-in – Content Blocked Page.....	170
Figure 4-40: Sign-in – Windows Security Prompt.....	170
Figure 4-41: Windows Security Prompt.....	171
Figure 4-42: Sign-in with PIN Code.....	171
Figure 4-43: Sign-in with Username & Password.....	171
Figure 5-1: Manual Firmware Upgrade.....	178
Figure 6-1: Web Interface - LAN Information.....	183
Figure 6-2: Web Interface - Port Mode Status.....	183
Figure 6-3: Web Interface - 802.1X Status.....	183
Figure 6-4: Web Interface - Phone Status.....	184
Figure 6-5: Web Interface - Line Status.....	184
Figure 6-6: Web Interface - Call Information.....	185
Figure 6-7: Web Interface - Call History.....	185
Figure 6-8: Web Interface - System Information - Release Information.....	186
Figure 7-1: Web Interface - Crash Dump.....	190
Figure 7-2: Web Interface - Monitoring - Traceroute.....	192
Figure 8-1: Web Interface - Restore Defaults.....	195
Figure 8-2: Confirm Restore to Factory Defaults.....	195
Figure 8-3: Web Interface - Configuration File.....	196
Figure 8-4: Web Interface - Load New Configuration File.....	196
Figure 8-5: Web Interface - Restart System.....	198
Figure 8-6: Confirmation Prompt.....	198
Figure A-7: HTTPS Redirect Server Directing Phones to Provisioning Server.....	205
Figure B-1: Identifying Recovery Mode.....	207
Figure B-2: Verifying Recovery Mode in Wireshark.....	208
Figure B-3: Source Ethernet MAC Address in Wireshark Identical to Phone Base's.....	208
Figure B-4: Recovering the Phone - Configure the PC NIC to which the Phone is Connected.....	209
Figure B-5: Make Sure with Wireshark that the Phone is Downloading Phone .img File.....	211
Figure B-6: Verifying .img File Download with Wireshark – Filtering by TFTP.....	212
Figure B-7: Verifying .img File Download using tftpd64.....	213

- Figure B-8: Verifying .img File Download using tftpd64 213
- Figure B-9: Verifying .img File Download from the Phone Screen 213
- Figure C-10: System Information page..... 214
- Figure C-11: Release Information page..... 214
- Figure C-12: Personal Settings (Left HRS | Right 450HD and C450HD) 214
- Figure C-13: UI Theme..... 215

List of Tables

Table 2-1: DHCP Option 43 Configuration Reference	20
Table 2-2: DHCP Option 43, Sub-Option 010, Configuration Reference	20
Table 2-3: DHCP Option 120 Configuration Reference	20
Table 2-4: DHCP Option 120 Configuration Reference	21
Table 2-5: DHCP User Class Entry for Each AudioCodes Phone Model Deployed.....	23
Table 2-6: Forcing Sign-In with PIN Code	38
Table 2-7: Online Sign-In	39
Table 2-8: AutoDiscover Web Service Protocol	40
Table 2-9: Troubleshooting Deployment Problems	41
Table 2-10: OVOC Server Parameters	43
Table 3-1: Network Settings – Static IP	48
Table 3-2: Network Settings - Automatic IP (DHCP).....	49
Table 3-3: Port Settings.....	50
Table 3-4: VLAN Parameters Description	51
Table 3-5: Language Display Parameters	52
Table 3-6: Function / Programmable Keys Parameters.....	54
Table 3-7: Speed Dial Parameter	55
Table 3-8: Discreet Call Parameters.....	57
Table 3-9: Programmable Key Parameters in the Configuration File	58
Table 3-10: Configuring a PSK for Paging during an Ongoing Call Call Hold Call Park.....	61
Table 3-11: Regional Parameters.....	62
Table 3-12: Ring Tone File URI in the Configuration File	64
Table 3-13: Ring Tones Parameter in the Configuration File.....	64
Table 3-14: Screen Contrast Parameters [445HD, 450HD, C450HD and RX50]	66
Table 3-15: Distinctive Ring Tone Parameters.....	68
Table 3-16: TLS/SSL over SIP Parameters	69
Table 3-17: TLS/SSL over SIPE Parameters	70
Table 3-18: Proxy and Registrar Parameters	71
Table 3-19: HTTP Proxy - Parameter	72
Table 3-20: Automatic Dialing Parameters.....	73
Table 3-21: Automatic Dialing Parameters.....	73
Table 3-22: Pause Dialing	74
Table 3-23: Default Audio Device Parameter	74
Table 3-24: Enabling Voice Dialing.....	75
Table 3-25: Disable Microphone Parameter.....	76
Table 3-26: Changing TRANSFER Key Functionality	76
Table 3-27: Semi-Consultative Transfer Parameter	77
Table 3-28: Blind Transfer Softkey Parameter.....	77
Table 3-29: EHS Parameter.....	78
Table 3-30: Call Waiting Audial Indication Parameter	79
Table 3-31: Call Forward Parameter	79
Table 3-32: Call Forward Parameter	80
Table 3-33: Disconnect if Handset On-Hooked after Call Put on Hold.....	80
Table 3-34: QoS Parameters.....	81
Table 3-35: Codec Parameters.....	82
Table 3-36: Media Streaming - RTP Port Range.....	83
Table 3-37: RTCP_XR Parameter.....	84
Table 3-38: Paging Parameters.....	86
Table 3-39: Paging – Allow Barge In.....	87
Table 3-40: Voice-Dialing Parameter Descriptions	88
Table 3-41: Dedicated Voicemail Server - Parameters.....	89
Table 3-42: Securing Voicemail Access by PIN Code Authentication Parameter	90
Table 3-43: Root CA Certificate Parameters.....	98

Table 3-44: Client Certificate Parameters	99
Table 3-45: Server-side Authentication.....	100
Table 3-46: Server Certificate Validation for Secured HTTPS Communications over SSL.....	101
Table 3-47: EAP MD5 Parameters.....	103
Table 3-48: EAP TLS Parameters	103
Table 3-49: HTTPS Parameter	104
Table 3-50: Configuring HTTP/S Server	105
Table 3-51: Configuring Automatic Provisioning Performed by DHCP	106
Table 3-52: Daylight Saving Time Parameters	109
Table 3-53: NTP Server Parameters	112
Table 3-54: NTP Server and GMT Parameters	113
Table 3-55: Time Zones	114
Table 3-56: LDAP Parameters	115
Table 3-57: T9 Parameter.....	117
Table 3-58: Caller Name to be Displayed	117
Table 4-1: Presence Status Timeout Parameters.....	120
Table 4-2: Automatic Firmware Update from Skype for Business Server - Configuration File	123
Table 4-3: PIN Lock Parameter	124
Table 4-4: Inband Provisioning Parameter 'DisableHandsetOnLockedMachine'	125
Table 4-5: Local Phone Parameter 'AllowCallsInLockState'.....	125
Table 4-6: Local Phone Parameter 'AnswerDelegateIncomingCalls'.....	126
Table 4-7: Microsoft's Exchange Calendar	127
Table 4-8: Calendar Meeting Reminders.....	128
Table 4-9: Maximum Number of Outlook Contacts to Display in the Phone's Screen	129
Table 4-10: Pairing Mode Parameter	147
Table 4-11: Pairing Mode Parameter	158
Table 4-12: Boss Privacy Mode Parameter.....	163
Table 4-13: Distinctive Ring Tone Parameter	166
Table 4-14: Removing Local 3-Way Conferencing Capability from Users - Parameter	167
Table 4-15: Blocking All Users from Signing out - Parameter	167
Table 4-16: Inband Provisioning Parameters for Downloading Contacts Pictures to Phones	173
Table 4-17: Local Phone Parameters for Downloading Contact Pictures.....	174
Table 4-18: Enabling QoE Reports using the Configuration File	175
Table 4-19: Disabling the C450HD IP Phone Screen Saver	177
Table 4-20: Enabling the Client ID using the Configuration File	177
Table 5-1: Automatically Checking for Updates Using the Configuration File	179
Table 5-2: Administrator account - Username and Password	180
Table 5-3: User account - Username and Password	180
Table 5-4: Telnet Parameters	181
Table 7-1: Syslog Parameters	187
Table 7-2: Packet Recording Parameters	189
Table 7-3: Crash Dump Parameters	190
Table 7-4: Core Dump Parameter	191
Table 7-5: Port Mirroring Parameters.....	192
Table B-1: Static DNS Record Parameters	204
Table C-1: Configuring tftpd64 Settings	209
Table G-1: Supported IETF RFCs.....	226
Table G-2: Supported SIP Methods.....	228
Table G-3: Supported SIP Headers.....	228

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-22-2021

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

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 at <https://online.audiocodes.com/documentation-feedback>.

Related Documentation

Document Name
445HD IP Phone Quick Guide – Teams Compatible
445HD IP Phone User’s Manual - Teams Compatible
450HD IP Phone Quick Guide - Teams Compatible
450HD IP Phone User’s Manual - Teams Compatible
C450HD IP Phone Quick Guide - Teams Compatible
C450HD IP Phone User’s Manual - Teams Compatible
HRS Conference Device Quick Guide - User’s Manual - Teams Compatible
HRS Conference Device User’s Manual - Teams Compatible
RX50 Conference Phone Quick Guide - Teams Compatible
RX50 Conference Phone User’s Manual - Teams Compatible
Device Manager Administrator’s Manual
One Voice Operations Center (OVOC) IOM Manual
OVOC User’s Manual

1 Introduction

This *Administrator's Manual* is intended for administrators responsible for provisioning AudioCodes' 400HD Series of IP Phones deployed with Microsoft Skype for Business in an enterprise network.



AudioCodes Skype for Business devices support Microsoft 'Teams Compatible'.

The document describes the new features and known and resolved restraints for AudioCodes' 400HD Series of IP Phones, including:

- 445HD, 450HD, C450HD IP Phones
- RX50 Conference Phone
- Huddle Room Solution (HRS)

AudioCodes' 445HD-R IP Phone without the Expansion Module (sidecar) and BLFs + 12 SDs (phone models UC445HDG-R and UC445HDEPSG-R) are identical to the 445HD IP phone but do not feature the Expansion Module (sidecar) nor the BLFs + 12 Speed Dials.

AudioCodes IP phones are based on AudioCodes' proprietary High Definition (HD) voice technology, providing clarity and a rich audio experience in Voice-over-IP (VoIP) calls.

The phones are fully-featured telephones that provide voice communication over an IP network, allowing you to place and receive phone calls, put calls on hold, transfer calls, etc.

The phones offer different automatic provisioning options.

This manual shows how to automatically provision a mass deployment of AudioCodes IP phones using DHCP.

2 Automatic Mass Provisioning of IP Phones using DHCP

This section shows how to automatically provision a mass deployment of AudioCodes IP phones in a Microsoft Skype for Business environment.



Instead of using DHCP as the automatic provisioning method, you can alternatively use Static DNS Record or SIP SUBSCRIBE and NOTIFY messages.

As DHCP clients, AudioCodes IP phones can be automatically provisioned with the following files:

- Configuration file (.cfg)
- Firmware file (.img)

These files can be placed on any of these three provisioning server types:

- HTTP/S server
- TFTP server
- FTP server

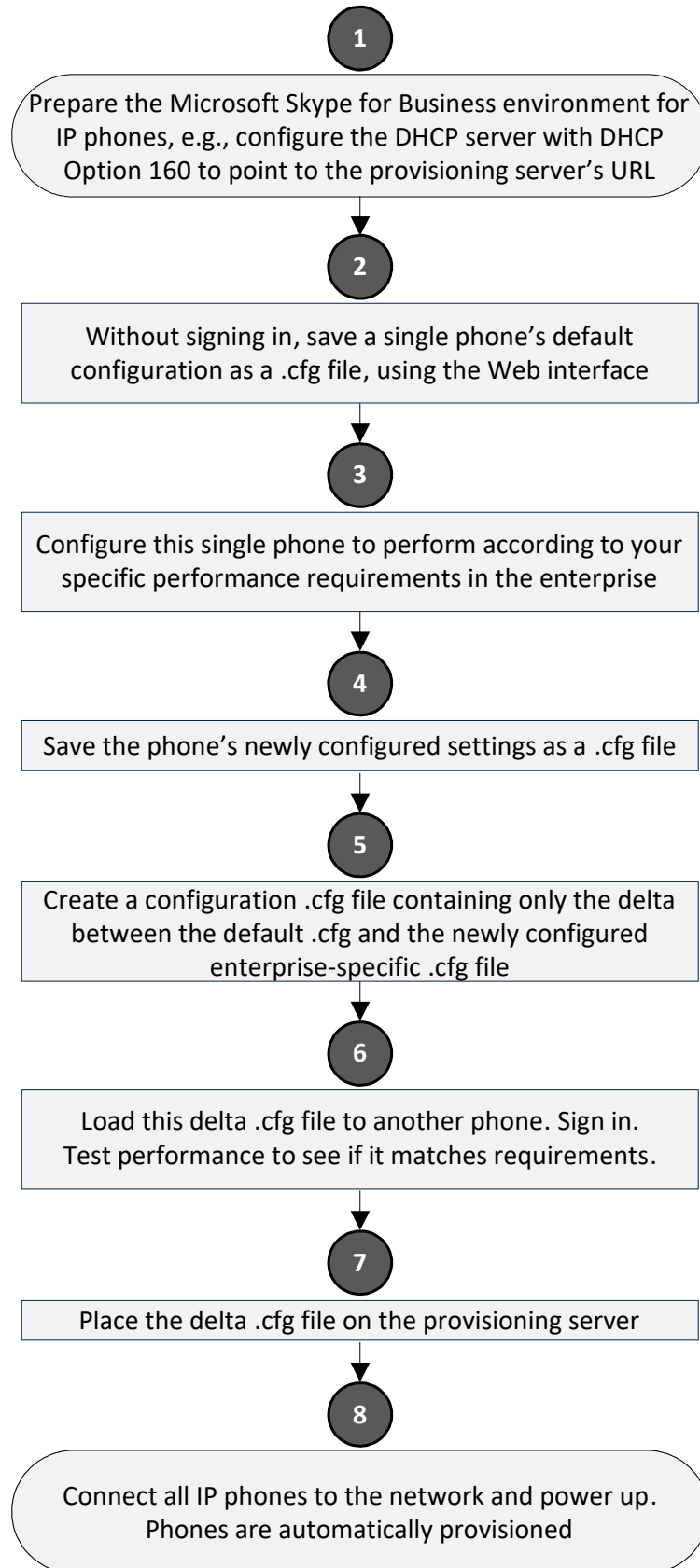
[Figure 2-1](#) summarizes the steps required for setting up mass provisioning of IP phones in a Microsoft environment.

These steps are described in detail in the following sections.



Automatic mass provisioning of IP phones using the DHCP provisioning method can alternatively be performed from the phones' management server. For detailed information, see the *Device Manager Administrator's Manual*.

Figure 2-1: Setting up Automatic Provisioning



2.1 Preparing the Microsoft Skype for Business Environment for IP Phones

Before plugging in and playing the phones in an enterprise's Microsoft Skype for Business environment, make sure the environment is ready for them.

To prepare it for phones, you must set up:

1. Front End Skype for Business Server
2. Domain Controller, including:
 - a. Active Directory, LDAP service
 - b. DNS service
 - c. DHCP service
 - d. NTP service (optional)
3. Unified Messaging Server (optional)
4. Mediant™ Gateway
5. SBA Server (optional)

For details, refer to Microsoft's website at:

<http://technet.microsoft.com/en-us/library/gg425854%28v=ocs.14%29.aspx>

2.1.1 Making Sure DHCP Server Options are Correctly Configured

This section shows how to ensure that your enterprise's DHCP server options are correctly configured and that the network environment is ready for deployment of IP phones.

For detailed Microsoft instructions on setting up DHCP for the IP phone, see:

[http://technet.microsoft.com/en-us/library/gg398369\(v=ocs.14\).aspx](http://technet.microsoft.com/en-us/library/gg398369(v=ocs.14).aspx)

Figure 2-2: DHCP Server Options

Option Name	Vendor	Value
001 UCIIdentifier	MSUCCient	4d 53 2d 55 43 2d 43 6c 69 65 6e 74
002 URLScheme	MSUCCient	68 74 74 70 73
003 WebServerFqdn	MSUCCient	41 43 6c 79 6e 63 70 6f 6f 6c 2e 41 ...
004 WebServerPort	MSUCCient	34 34 33
005 CertProvRelPath	MSUCCient	2f 43 65 72 74 50 72 6f 76 2f 43 65 ...
003 Router	Standard	10.59.0.1
002 Time Offset	Standard	0x1c20
004 Time Server	Standard	10.59.0.20, 10.59.0.21
006 DNS Servers	Standard	10.59.0.21, 192.168.81.21
015 DNS Domain Name	Standard	ACentralDom.AC3pip.com
042 NTP Servers	Standard	10.59.0.21, 10.59.0.20
120 UCSipServer	Standard	00 0a 41 43 4c 79 6e 63 70 6f 6f 6c ...

Make sure:

- DHCP Option 43 (comprising 001-005 in the figure above) is correctly configured (see Section 2.1.1.1 on page 20 below)
- DHCP Option 120 is correctly configured (see Section 2.1.1.3 on page 20 below)
- DHCP Option 42 is correctly configured (see Section 2.1.1.4 on page 21 below)

Correct configuration of these three is critically important. The other DHCP options shown in the figure above are also important but are less susceptible to inaccuracies than these.

2.1.1.1 DHCP Option 43

Option 43 comprises the five sub-options 001-005 shown in the figure above and in the table below. These point the phone to the location of the Certificate Provisioning service on the Skype for Business server. Use the table as a reference to make sure each sub-option is correctly configured. Sub-option 010 is shown in the next section (VLAN Discovery via DHCP).

Refer also to [http://technet.microsoft.com/en-us/library/gg398088\(v=ocs.14\).aspx](http://technet.microsoft.com/en-us/library/gg398088(v=ocs.14).aspx)

Table 2-1: DHCP Option 43 Configuration Reference

Sub-Option Number	Sub-Option Name	ASCII Value (example)
001	UCIdentifier	MS-UC-Client
002	URLScheme	https
003	WebServerFQDN	skypeforbusinessserver.domain.com
004	WebServerPort	443
005	CertProvRelPath	/CertProv/CertProvisioningService.svc

2.1.1.2 VLAN Discovery via DHCP Option 43

Option 43 comprises the five sub-options 001-005 shown in the previous section, as well as sub-option 010, shown in the table below. Sub-option 010 is used to specify a voice VLAN. It is *not mandatory*.

Refer also to [http://technet.microsoft.com/en-us/library/gg398088\(v=ocs.14\).aspx](http://technet.microsoft.com/en-us/library/gg398088(v=ocs.14).aspx)

Table 2-2: DHCP Option 43, Sub-Option 010, Configuration Reference

Sub-Option Number	Sub-Option Name	ASCII Value (example)
010	VoiceVLAN	Valid values: 1-4094

2.1.1.3 DHCP Option 120

Option 120, which includes the Skype for Business Server's fully qualified domain name (FQDN) as shown in the table below, is required for the certification authority (CA) pool Registrar. Use the table as reference to make sure Option 120 is correctly configured.

Table 2-3: DHCP Option 120 Configuration Reference

Option Number	Option Name	ASCII Value (example)
120	UCSipServer	skypeforbusinessserver.domain.com

2.1.1.4 DHCP Option 42

Option 42 specifies the servers that provide NTP / SNTP for the network. Make sure NTP server IP addresses are correct, as shown in the table below.

Table 2-4: DHCP Option 120 Configuration Reference

Option Number	Option Name	String (example)
42	NTP Servers	10.59.0.20, 10.59.0.21

2.1.1.5 DHCP Scope Option

Use a DHCP Scope Option if vendor phones other than those of AudioCodes are deployed in the same enterprise as AudioCodes' phones and a DHCP Option cohabitation issue consequently occurs.

This section shows how to configure provisioning of AudioCodes phones using a DHCP Scope Option when other vendor phones in the enterprise point to the same DHCP server and use one of the standard DHCP Options described in the previous sections.

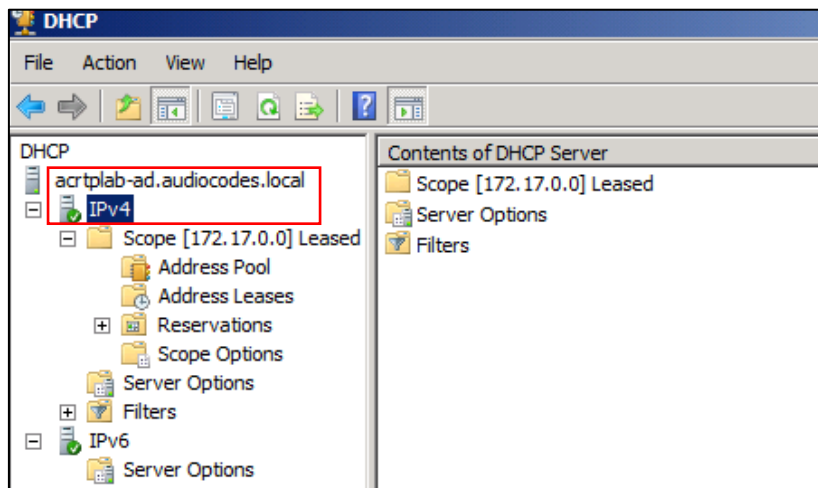
To configure provisioning of AudioCodes phones using a DHCP Scope Option:

1. Determine the DHCP server hosting the phones.
2. Determine if DHCP Options are assigned to IPv4 or IPv6 addresses.



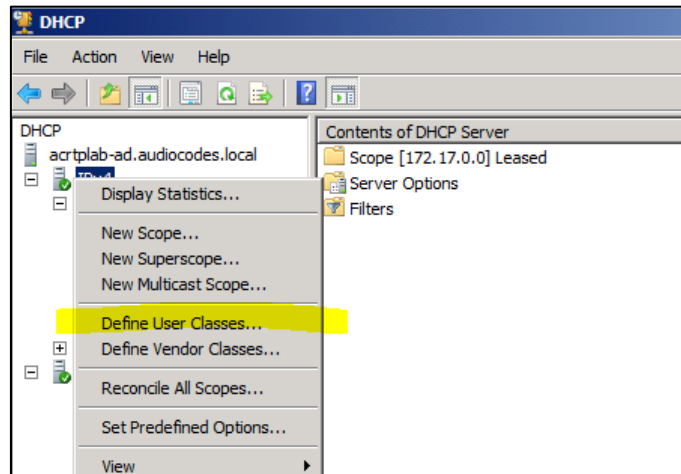
- The examples below show DHCP server **acrtpiab-ad.audiocodes.local**
- The examples below show IPv4 addresses

Figure 2-3: DHCP Options Assigned to IPv4 Addresses



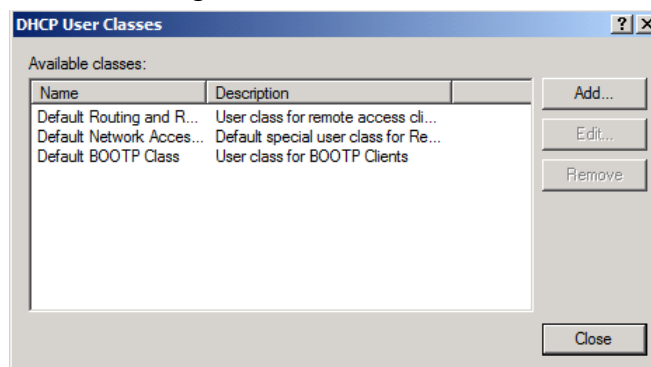
3. Define a separate **User Class** for each AudioCodes phone model deployed: Right-click the **IPv4** server icon and from the popup menu, select **Define User Classes...**

Figure 2-4: Defining User Classes



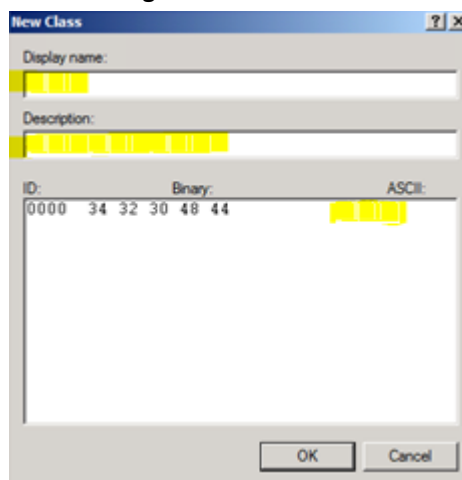
The DHCP User Classes dialog opens.

Figure 2-5: DHCP User Classes



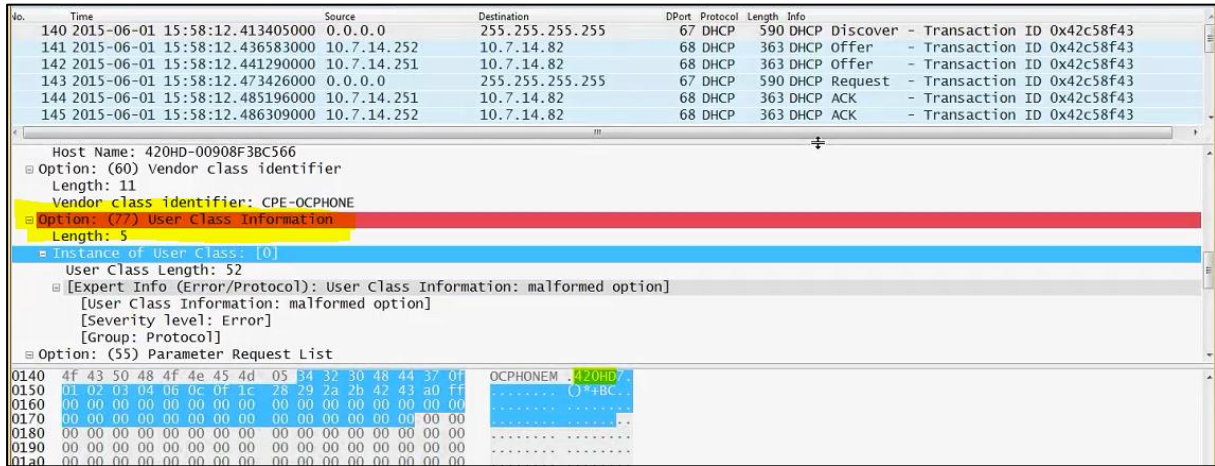
4. Click **Add...**

Figure 2-6: New Class



5. In the New Class dialog, enter **Display name** and **Description** as indicated in the figure above, and then in the **ASCII** field, enter the **User Class Phone Type** (see the Packet Bytes window in Wireshark below for an *illustrative example*, and see the table below for the other AudioCodes phone models) to be sent from the phone during DHCP Discover via Option 77 (supported by DHCP Server 2008). Do this for each AudioCodes phone model so that a User Class entry for each model deployed will exist when completed.

Figure 2-7: Packet Bytes Window



6. Make sure one DHCP User Class entry exists for each AudioCodes phone model deployed in the enterprise.

Figure 2-8: DHCP User Classes

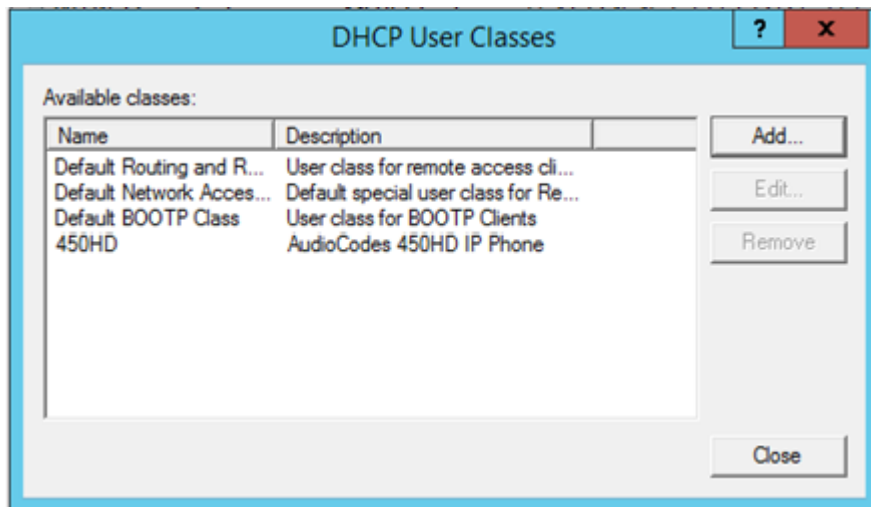


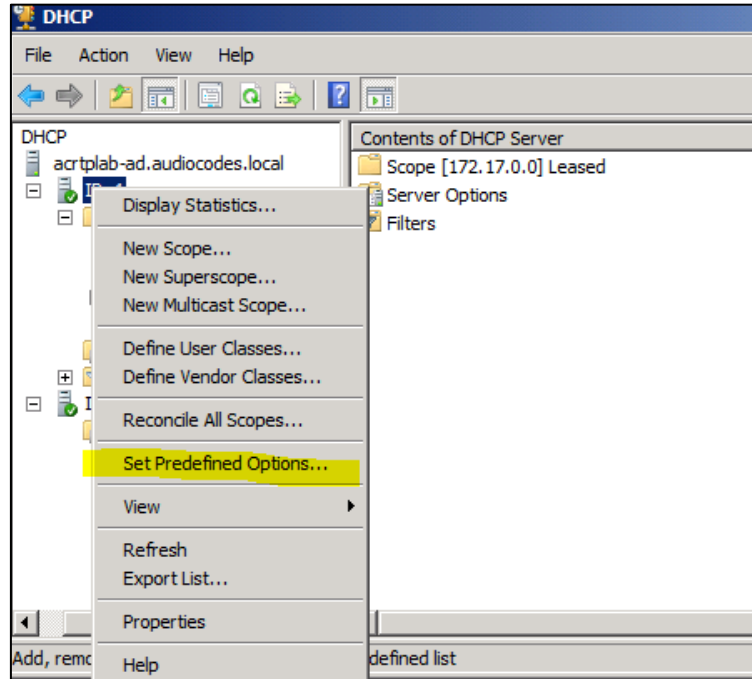
Table 2-5: DHCP User Class Entry for Each AudioCodes Phone Model Deployed

Display Name	Description	ASCII
445HD	AudioCodes 445HD IP Phone	445HD
450HD	AudioCodes 450HD IP Phone	450HD
C450HD	AudioCodes C450HD IP Phone	C450HD
RX50	AudioCodes Conference Phone	RX50

Defining a User Class on Windows 2008, using 'Set Predefined Options'

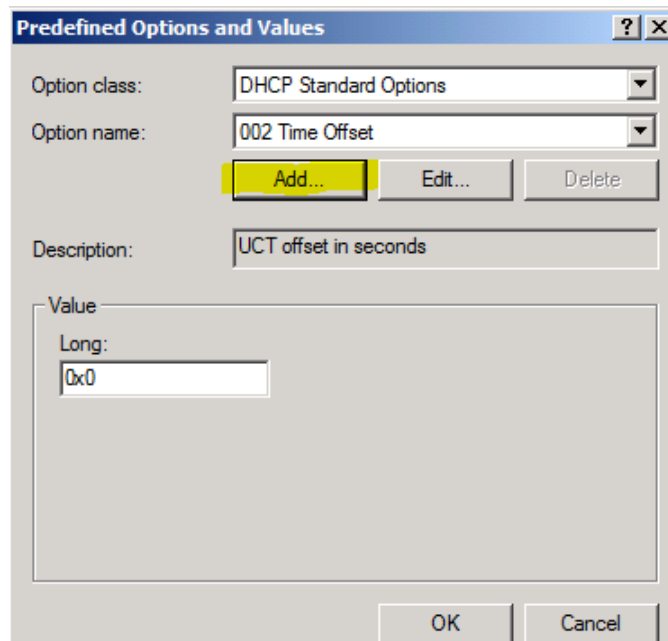
7. Configure Scope Option 160. This is not a *standard* Scope Option, so it needs to be created. To create it on the server, select the IP version (IPv4) and select **Set Predefined Options...**

Figure 2-9: Set Predefined Options



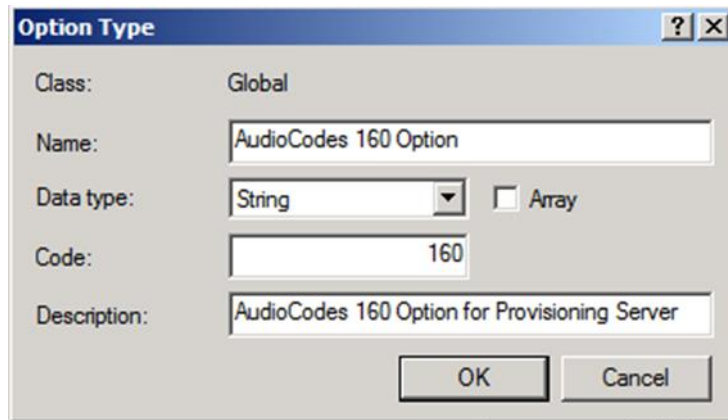
8. From the 'Option class' dropdown, select **DHCP Standard Options**, and then click **Add...**

Figure 2-10: Predefined Options and Values



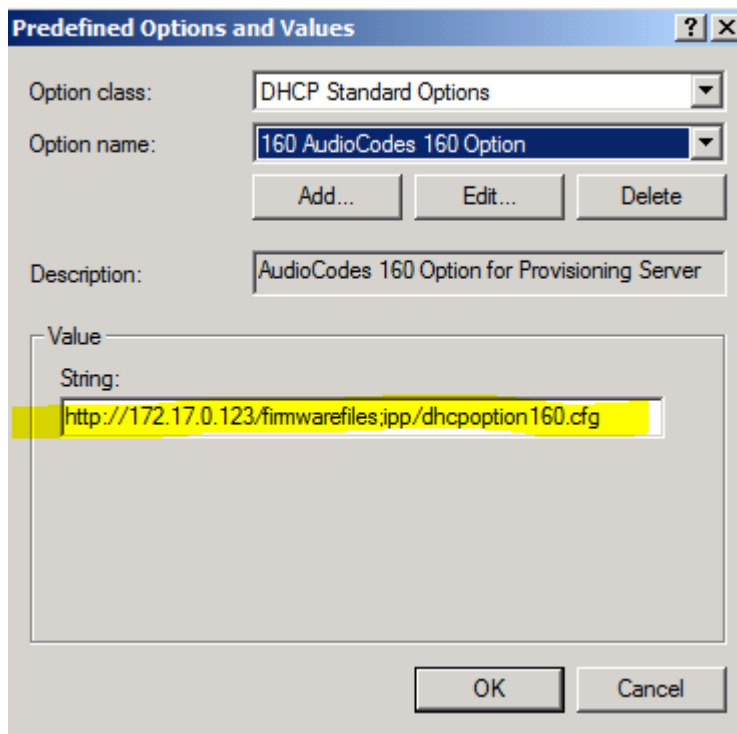
9. Add the **AudioCodes 160 Option** as shown below, and then click **OK**.

Figure 2-11: Option Type – Add AudioCodes 160 Option



10. Add the IP Phone Management Server location using HTTP. In the figure below, it's `http://<EMS IP address>/firmwarefiles;ipp/dhcption160.cfg`. See the *Device Manager Administrator's Manual* for detailed information.

Figure 2-12: Predefined Options and Values – Add IP Phone Management Server Location



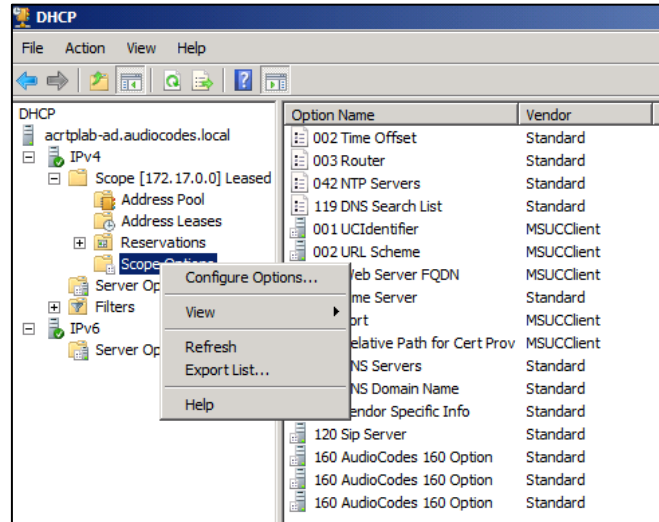
Ensure you defined `http://<EMS IP address>/firmwarefiles;ipp/dhcption160.cfg` for DHCP Option 160 in the enterprise's DHCP server.

11. Decide if the DHCP Scope Option needs to be assigned to phones in a *specific VLAN (Scope)*, or to the *entire server* (`acrtplab-ad.audiocodes.local`) for IPv4 addresses.

VLAN Scope

12. Assign to a specific VLAN (Scope of IP addresses such as the Scope below 172.17.0.0, or to multiple Scopes, to be performed separately on each Scope).
 - a. If selecting a VLAN, expand the 'Scope Leased' folder, select 'Scope Options', and then select **Configure Options** from the popup menu.

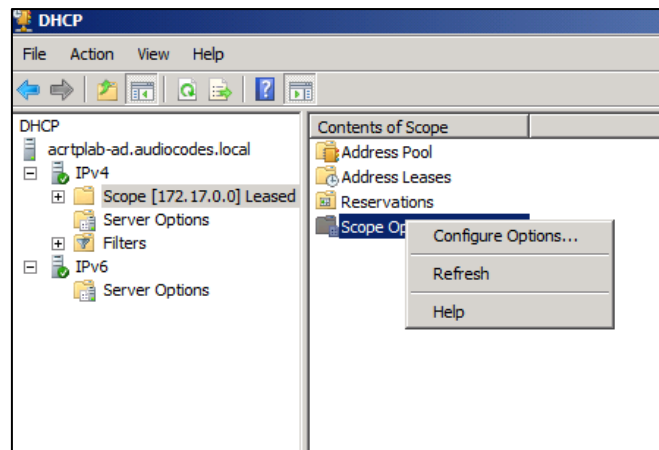
Figure 2-13: 'Scope Leased' Folder - Configure Options



-OR-

- b. Select the collapsed folder 'Scope Leased' and in the main window, right-click 'Scope Options' and select **Configure Options...**

Figure 2-14: Configure Options 1

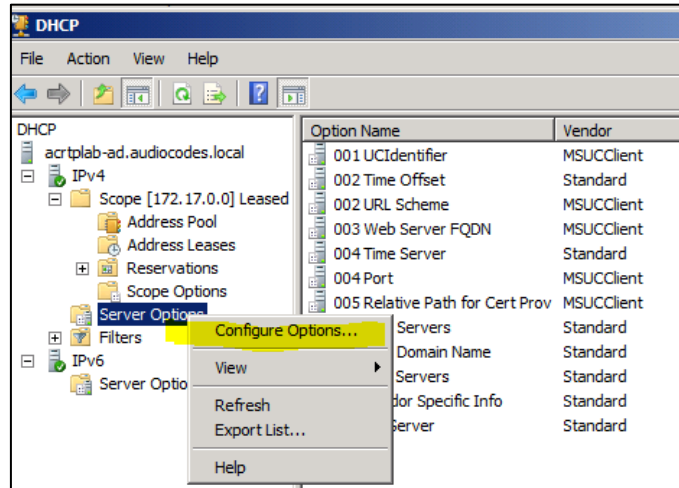


-OR-

Server Option

- 13. If assigning to the entire server (acrtp lab-ad.audiocodes.local), select the 'Server Options' folder under server **IPv4**, right-click 'Server Options' and select **Configure Options...**

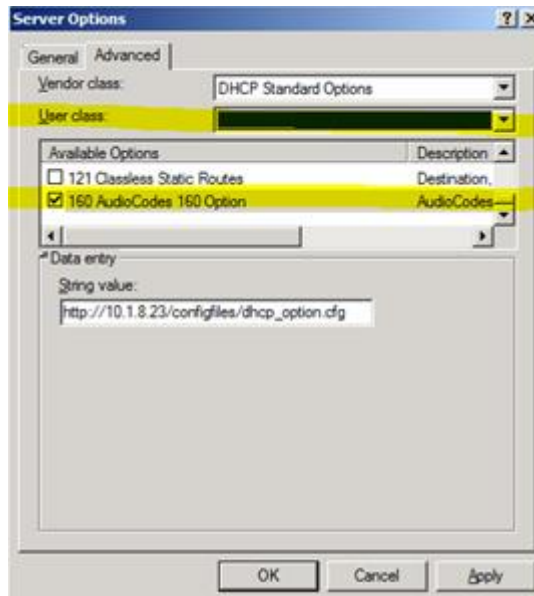
Figure 2-15: Configure Options 2



- In the Server Options page (or Scope Options page) that opens, select the **Advanced** tab, ensure that **DHCP Standard Options** remains selected, and select the phone model for the first **User Class** to be defined. Scroll through the Available Options (all are cleared) and select only **160 AudioCodes 160 Option**.

The figure below shows the Server Options page. The Scope Options page is identical. Note that the String value you defined for Scope Option 160 is automatically populated, so it's unnecessary to change it. Note also that if additional DHCP Options are required (such as DNS or time server) that are different from the Servers Options for the rest of the Scopes on the server, they can also be selected, but this is typically not needed.

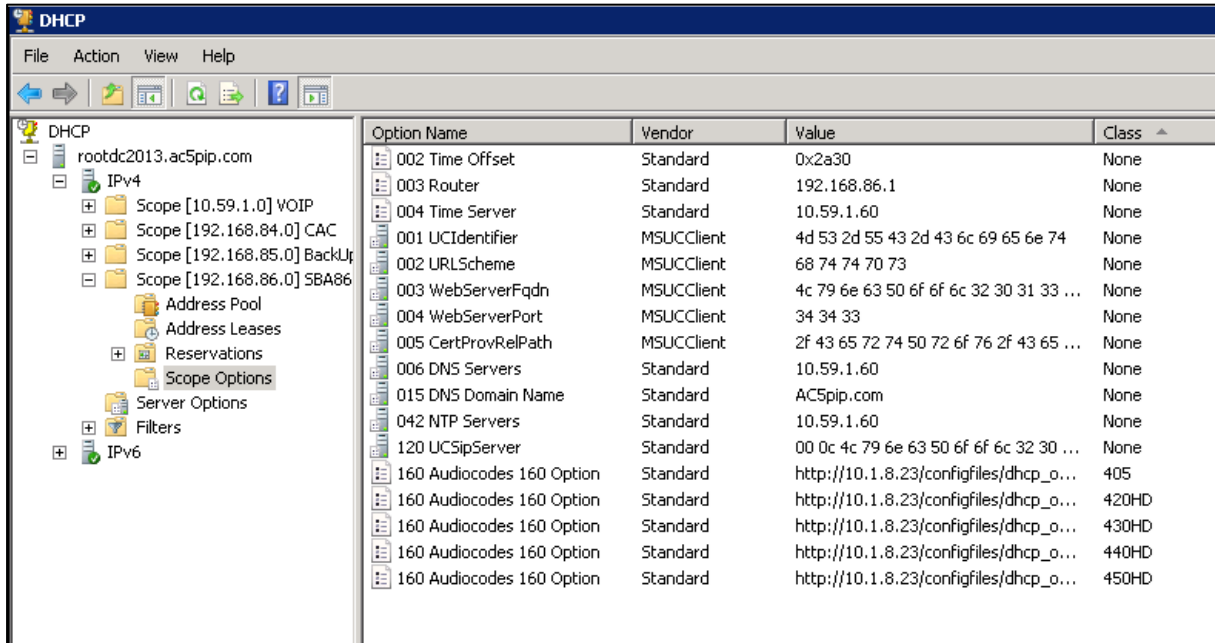
Figure 2-16: Server Options



- Add each phone's User Class.

You have successfully created separate Scope Options that will only allow AudioCodes phones to connect to the Device Manager when they boot up and will not allow other vendor phones from receiving Device Manager server as their configuration server.

Figure 2-17: Scope Options Created [Illustrative Purposes Only]



Defining a User Class on Windows 2012, using 'Policies'

- Right-click **Policies** and from the menu that pops up, select **New Policy**:

Figure 2-18: New Policy

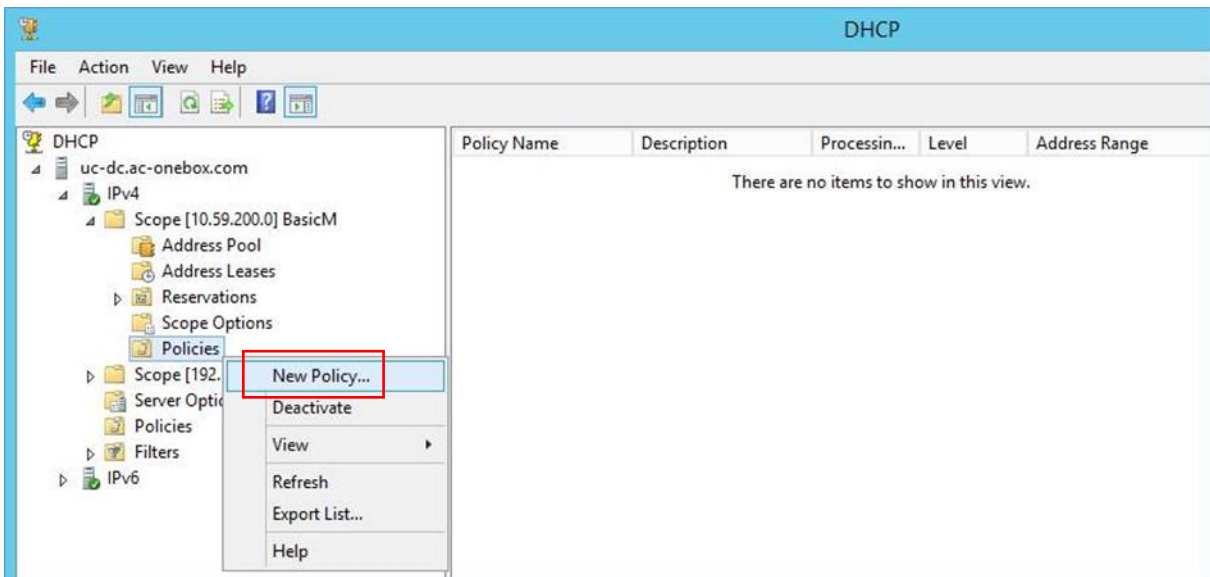


Figure 2-19: DHCP Policy Configuration Wizard – Policy Name

DHCP Policy Configuration Wizard

Policy based IP Address and Option Assignment

This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name: Audiocodes IPP User Class

Description:

< Back Next > Cancel

17. In the 'Policy Name' field, enter the name of the policy and click **Next**.

Figure 2-20: DHCP Policy Configuration Wizard - Add

DHCP Policy Configuration Wizard

Configure Conditions for the policy

A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

! A policy with conditions based on fully qualified domain name can have configuration settings for DNS but not for options or IP address ranges.

Conditions	Operator	Value
------------	----------	-------

AND OR Add... Edit... Remove

< Back Next > Cancel

18. Click **Add** as shown in the figure above; the Add/Edit Condition screen opens:

Figure 2-21: Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: User Class

Operator: Equals

Value(s)

Value: [dropdown menu]

Prefix wildcard(*)

Append wildcard(*)

450HD

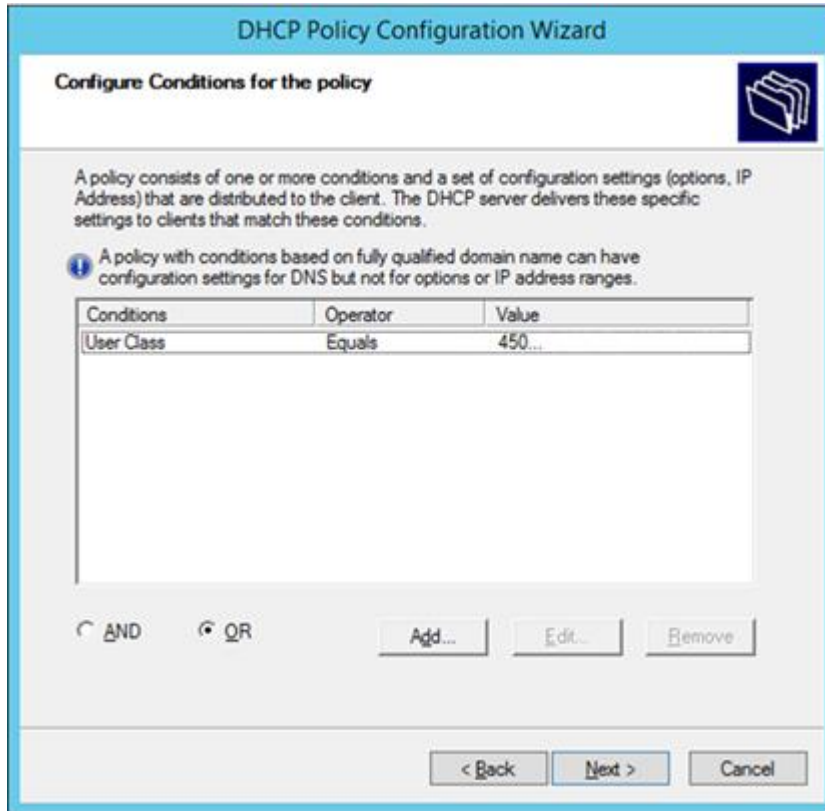
Add

Remove

Ok Cancel

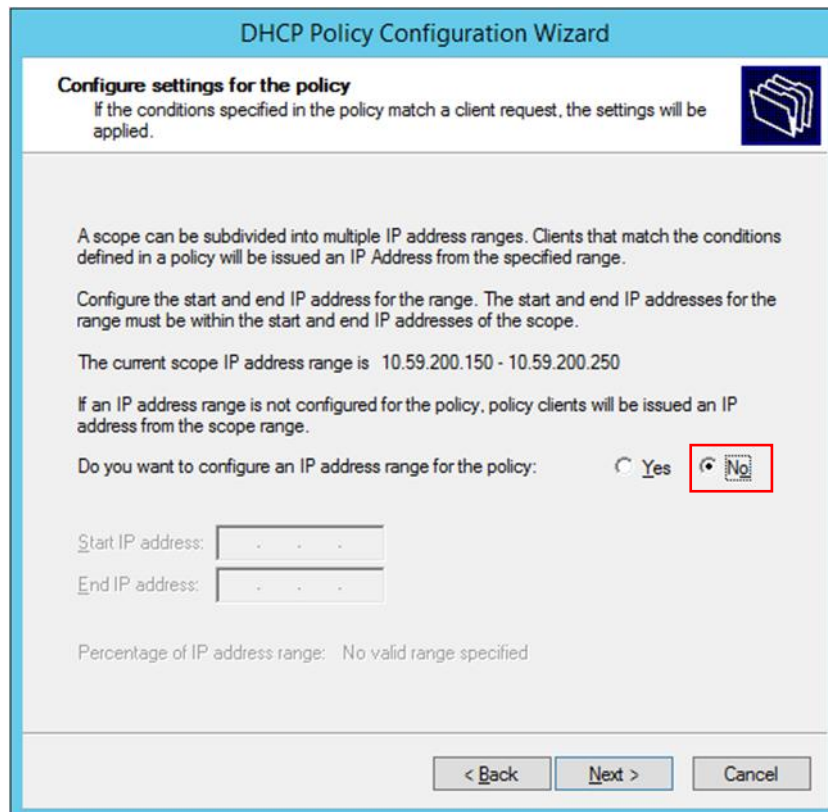
19. From the 'Criteria' dropdown, select **User Class**.
20. From the 'Operator' dropdown, select **Equals**.
21. From the 'Value' dropdown, select the relevant user class created in the previous step (**445HD / 450HD / C450HD / RX50**) and then click **Add**.
22. After each relevant User Class has been added, click **Ok**; the policy conditions screen opens, as shown in the figure on the next page:

Figure 2-22: Policy Conditions



23. Click **Next**; the policy settings screen opens:

Figure 2-23: Policy Settings – IP Address Range for the Policy



24. Select the **No** option, and click **Next**; the policy settings screen opens:

Figure 2-24: Policy Settings – Available Options

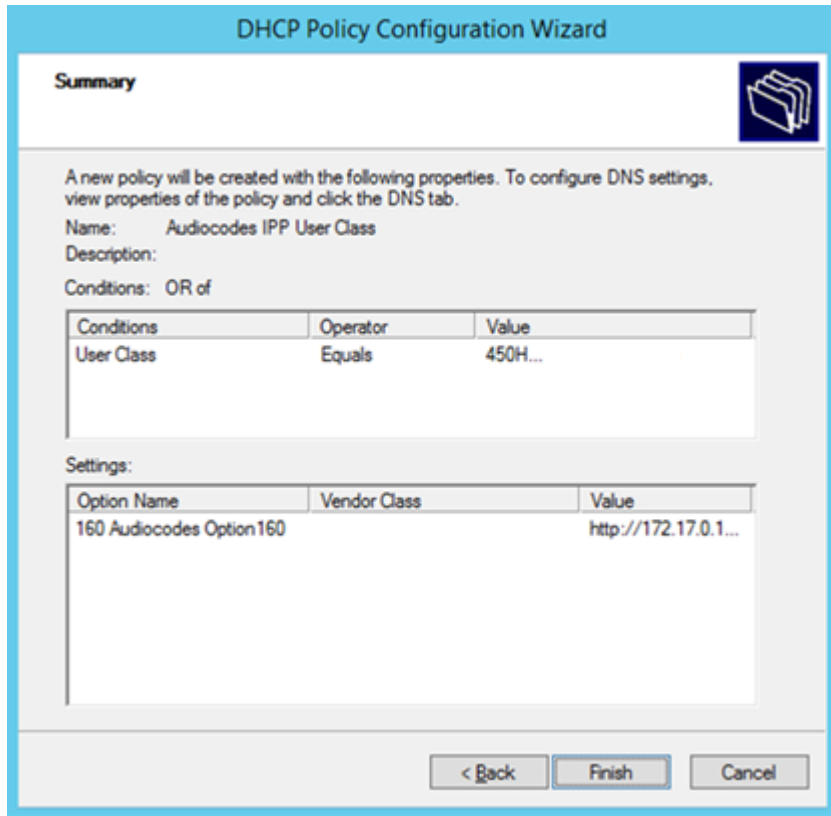
The screenshot shows the 'DHCP Policy Configuration Wizard' window. The title bar reads 'DHCP Policy Configuration Wizard'. Below the title bar, the text says 'Configure settings for the policy' and 'If the conditions specified in the policy match a client request, the settings will be applied.' There is a folder icon on the right. The 'Vendor class' dropdown is set to 'DHCP Standard Options'. Below this is a table of 'Available Options':

Available Options	Description
<input checked="" type="checkbox"/> 160 160 Audiocodes Option160	160 Audiocodes Option160
<input type="checkbox"/> 240 Private	private

Below the table is a 'Data entry' section with a 'String value:' label and a text box containing the URL: 'http://172.17.0.123/firmwarefiles.jsp/dhcptior'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

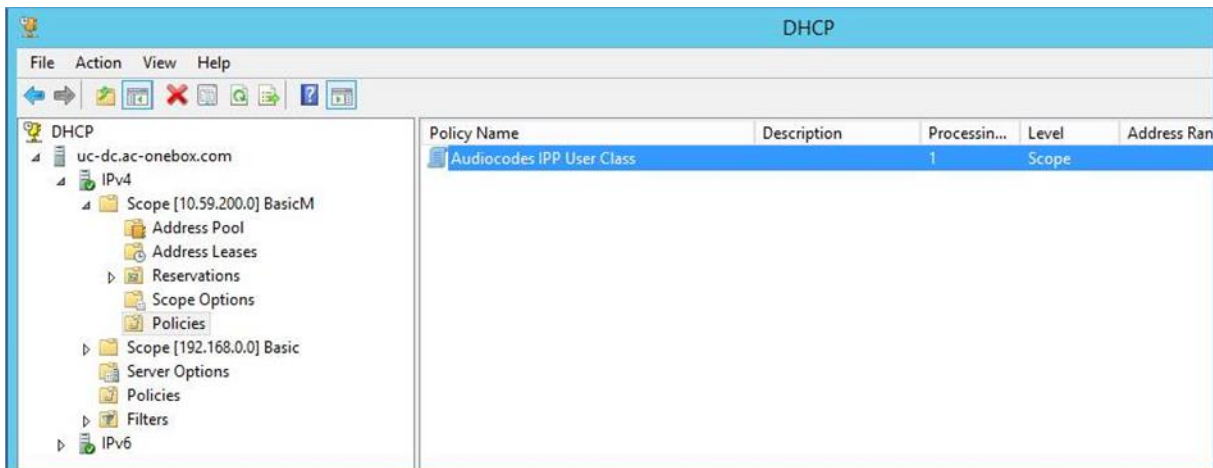
25. From the 'Vendor class' dropdown, select **DHCP Standard Options**, as shown above.
26. Scroll down in the 'Available Options' pane until you locate the predefined **Audiocodes Option160** option, and then select it.
27. In the 'String value' field, enter the correct provisioning URL, and click **Next**; the Summary screen opens, shown in the figure on the next page.

Figure 2-25: Policy Settings – Summary



28. Click **Finish** to complete the settings. Make sure the new policy name is displayed in the DHCP GUI, as shown in the figure below:

Figure 2-26: DHCP GUI - Policy Name: AudioCodes IPP User Class



2.1.2 Making Sure the DHCP Server is Correctly Configured for Auto Provisioning

After creating a .cfg configuration file (see Section 2.2), place it - and the software file (img) and other files such as tone files - on a provisioning server from where the IP phones can download and install it.

To get the URLs to this provisioning server, the IP phones use DHCP. The provisioning server can be HTTP/S, TFTP or FTP server.

The phone features *automatic update capability* to update the configuration and the software. Checks for newer configuration files and software versions are routinely automatically performed. Manual checks can also be performed.

To make sure the feature functions correctly:

1. Verify that the provisioning server is running and that the configuration and firmware files are located in the correct location on it.
2. Connect the phone to the IP network and then to power.
3. On the DHCP server, configure DHCP Option 160 with the URL to the provisioning server where the configuration and firmware files are located.
By default, the IP phone uses Option 160 which has highest priority.
If absent, the IP phone uses Options 66/67 for TFTP.

The following syntax is available for DHCP option 160:

- <protocol>://<server IP address or host name>/<firmware file name>;<configuration file name>
- <protocol>://<server IP address or host name>
- <protocol>://<server IP address or host name>/<firmware file name>
- <protocol>://<server IP address or host name>;<configuration file name>

Where <protocol> can be "ftp", "tftp", "http" or "https"

4. During DHCP negotiation, the phone requests DHCP options 66/67/160 to receive provisioning information. The DHCP server responds with Option 160 providing the provisioning URL, or Options 66 and 67 providing the TFTP IP address and firmware file name respectively.
5. The phone then checks whether new firmware is available by checking the firmware file header. If the version is different from the one currently running on it, the phone downloads the complete image and burns it to its flash memory.
6. If new firmware is unavailable, the phone checks whether a new configuration file is available on the server. If available, the phone downloads it and updates the phone's configuration after verifying that the configuration file is related to the phone model. When a configuration update is needed, the phone might reboot.



- Only *img* (firmware) and *cfg* (configuration) files can be used.
- In the DHCP Discover message, the phone publishes its model name in Option fields 60 and 77 (e.g., 450HD). To provide different provisioning information to different models, set up a policy in the DHCP server according to phone model name.
- If the phone is powered off during provisioning, it becomes unusable; perform a recovery process (see Section 5 on page 178).

2.2 Creating a Configuration File for Auto Provisioning

Most phones deployed in an enterprise typically require identical configuration settings. Best practice for creating a configuration file for auto provisioning is to:

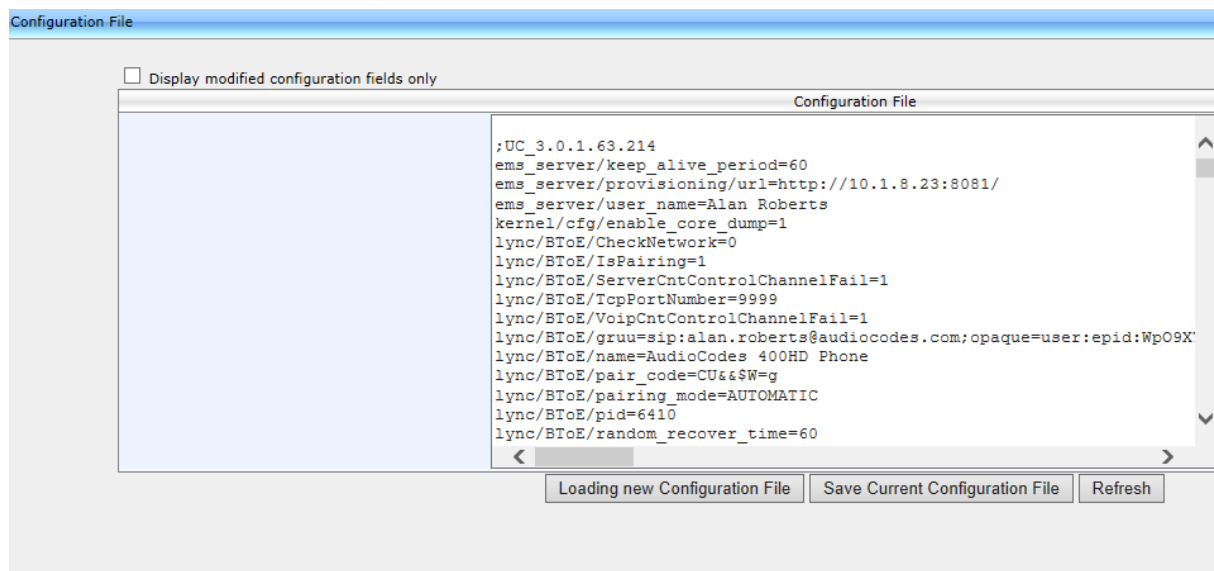
1. Without signing in, use the Web interface to save a single phone's default configuration (factory settings) as a .cfg file.
2. Configure that single phone to perform according to your specific performance requirements in the enterprise.
3. Save the phone's newly configured settings as a .cfg file.
4. Create a configuration .cfg file containing only the delta between the default .cfg and the newly configured enterprise-specific .cfg file.
5. Load this delta .cfg file to another phone, sign in, and test that phone's performance to see if it matches requirements.
6. Use this delta configuration .cfg file to automatically provision all IP phones through DHCP.

2.2.1 Saving a Single Phone's Default Configuration as a .cfg File

To save a single phone's default configuration as a .cfg file:

1. Get the phone's IP address (MENU key > **Status** > **Network Status** > **IP Address**) and point your Web browser to it; the phone's Web interface login page opens.
2. Enter the login credentials (default user name is **admin**; get Windows credentials from IT); the Home page of the Web interface is displayed.
3. Open the Configuration File page (**Management** tab > **Manual Update** menu > **Configuration File**).

Figure 2-27: Web Interface - Configuration File



4. Click **Save Current Configuration File** and save the .cfg file in a folder on your PC.

2.2.2 Configuring the Phone According to Requirements

You must configure a phone according to your specific requirements in the enterprise.

To configure a phone according to your specific requirements in the enterprise:

- Use Section 3 as reference.

2.2.3 Save the Phone's Newly Configured Settings as a .cfg File

After configuring a single phone according to your specific requirements, save the newly configured settings as a .cfg file.

To save the newly configured settings as a .cfg file:

1. In the Web interface, open the Configuration File page (**Management** tab > **Manual Update** menu > **Configuration File**) (see [Figure 2-27](#)).
2. Click **Save Current Configuration File** and save the .cfg file in a folder on your PC.

2.2.4 Creating a Delta Configuration .cfg File

Create a configuration .cfg file containing only the delta between the default .cfg and the newly configured enterprise-specific .cfg file.

To create a configuration .cfg file of the delta:

1. In the Web interface, open the Configuration File page (**Management** tab > **Manual Update** menu > **Configuration File**) (see [Figure 2-27](#)).
2. Select the **Display modified configuration fields only** option; only those default parameters you modified are displayed.
3. Click **Save Current Configuration File** and save the .cfg file in a folder on your PC.

2.2.5 Loading the Delta .cfg File to Another Phone, Signing In, Testing

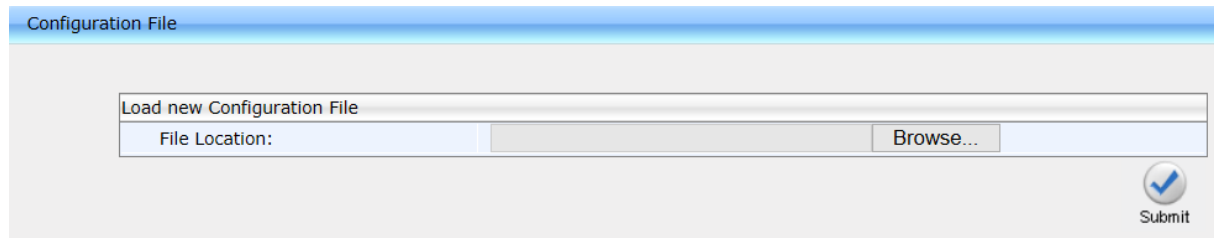
You must load the delta .cfg file you created in the previous section to another phone, sign in, and test that phone's performance to see if it matches requirements.

2.2.5.1 Loading the Delta .cfg File to Another Phone

To load the delta .cfg file to another phone:

1. Get the phone's IP address (MENU key > **Status** > **Network Status** > **IP Address**) and point your Web browser to it; the phone's Web interface login page opens.
2. Enter the login credentials (default user name is **admin**; get Windows credentials from IT); the Home page of the Web interface is displayed.
3. Open the Configuration File page (**Management** tab > **Manual Update** menu > **Configuration File**) and then click **Loading new Configuration File**:

Figure 2-28: Web Interface – Loading a New Configuration File



The screenshot shows a web interface titled 'Configuration File'. Below the title is a section labeled 'Load new Configuration File'. This section contains a text input field for 'File Location:' followed by a 'Browse...' button. In the bottom right corner of this section, there is a blue circular 'Submit' button with a checkmark icon.

4. Navigate to the folder in which you stored the delta configuration .cfg file, select it, and then click **Submit**; the configuration file is loaded to the phone.

2.2.5.2 Signing In to the Phone

- For instructions on how to sign in through the phone's screen, see the phone's *User's Manual*.
- For instructions on how to sign in through the Web interface, see Section 4.23.



The RX50 by default does not include a sign-in key for users. Sign-in can be performed by users with Administrator privilege (via MENU > **Admin** key). The administrator can however change the privileges of the user for a sign-in to be available to them, by changing the value of configuration file parameter 'account/sip/permission' from **ADMIN** (default) to **USER**.

2.2.5.3 Testing the Phone

You must test the phone to see if the newly configured settings match your requirements. See the *User's Manual* for information on how to operate the phone's functions and features.

2.2.5.4 Changing the Order of the Sign-In Method

Most enterprises prefer the 'PIN code' option to precede the 'Phone number' option as the default method for signing in. In the default order, 'Phone number' precedes 'PIN code', but administrators can change it.

To change the default method for signing in:

- In the Configuration File (**Management** tab > **Configuration File**), change the 'lync/sign_in/method' parameter value to **NUMBER_AND_PIN**.

2.2.5.5 Allowing Users to Display Phone # or Ext # in Phone Screen

Using parameter 'lync/sign_in/line_type_display/ext', you can allow users to define whether to display their telephone number or their extension number in the phone's screen. This is only possible if the enterprise's Active Directory includes both. Default: **1** (extension number).

2.2.5.6 Forcing Sign-in with PIN Code

Network administrators can force users to sign in with PIN code using Configuration File parameter *sign_in/pin_code_only*. In this mode, the only sign-in option is with user extension number and PIN code. Allowing only the basic PIN code option on the user's phone helps avoid user mistakes and helps avoid storing the user password on the phone.

To force sign-in with PIN code:

1. Open the Configuration File page in the Web interface (**Management** tab > **Manual Update** > **Configuration File**).
2. Configure the parameter using the table below as reference.

Table 2-6: Forcing Sign-In with PIN Code

Parameter	Description
sign_in/pin_code_only	Determines which online sign-in method option must be used. <ul style="list-style-type: none">■ [0] (Default) Allows sign-in with user credentials and with user extension number and PIN code.■ [1] Sign-in can only be with user extension number and PIN code.

2.2.5.7 Online Sign-in through Microsoft's Cloud PBX

Users can sign in, connect and authenticate with Microsoft's Cloud PBX (online sign-in), Microsoft's cloud-hosted version of enterprise voice. The phone features two sign-in method options allowing users to connect to Microsoft's Cloud PBX:

- ADAL (Azure AD Authentication Library) that is based on OAuth 2.0 ([RFC 6749](#)). The phone always starts with ADAL and if it's unavailable on the server side, the phone moves to OrgID.
- OrgID (Organizational ID) or LiveID is Microsoft's proprietary connectivity to Cloud services.



Online sign-in must be in the following format:

- Sign-in address
- Username in UPN (User Principal Name) format. UPN format is the way the user's name appears in their e-mail address listed in the Active Directory, i.e., **username@domain.com**
- User's network IT password

Signing in with a username that is a NetBIOS Domain Name, i.e., **domain\username**, as well as signing in with the phone Extension and PIN Code, are disallowed for Skype for Business *online sign-in*. They are only allowed for *on-premises* sign-in.

Users can sign in using the **Web sign-in** option, a.k.a. Device Pairing, which allows them to connect to Microsoft's Cloud PBX, i.e., to get connectivity to Microsoft's Cloud PBX, Microsoft's cloud-hosted version of enterprise voice.



This sign-in option applies only to Microsoft Cloud PBX users.

The option exempts users from having to laboriously key in their user name and password using the phone keypad in order to sign in. If the option is selected, a URL and a Pairing Code are displayed, as shown in the figure above. Users must then point their browser to the URL and enter the Pairing Code in the Microsoft web page. Sign-in to Microsoft's Cloud PBX is then performed.

To sign-in:

1. Open the Configuration File page in the Web interface (**Management** tab > **Manual Update** > **Configuration File**).
2. Configure the parameter using the table below as reference.

Table 2-7: Online Sign-In

Parameter	Description
lync/sign_in/support_adal	<p>Determines which online sign-in method option is used.</p> <ul style="list-style-type: none"> ■ [0] The phone uses the OrgID method option to sign in. ■ [1] (Default) The phone first attempts to use the ADAL (Azure Active Directory Authentication Libraries) method option and only if ADAL fails, the phone uses the OrgID option.

2.2.5.8 Disabling AutoDiscover Web Service Protocol

You can disable AutoDiscover Web Service Protocol [MS-OCDISCWS] which is by default enabled. AutoDiscover improves discovery of the phone's SIP home server during the sign-in process. The phone finds its home server URL for a specific Skype for Business account, based on user credentials. The protocol is especially efficient for Skype for Business online and hybrid environments, when phones must sign in to a different Skype for Business server according to the user's account.

The home server was previously found using DNS SRV records based only on a SIP account domain [MS-CONMGMT]. If AutoDiscover is unsuccessful, the phone falls back to SRV DNS.

Table 2-8: AutoDiscover Web Service Protocol

Parameter	Description
lync/sign_in/auto_discovery_enabled	<ul style="list-style-type: none">■ [0] Disabled.■ [1] Enabled (Default)

2.3 Copying the Configuration File to the Provisioning Server

After creating the delta configuration .cfg file as shown in the previous section, copy the file to the provisioning server (e.g., TFTP server) from which the phones download it when they're connected and powered up. Make sure DHCP Option (e.g., Option 160) on your DHCP server is configured with the correct URL pointing to the provisioning server's directory.

2.4 Triggering Automatic Provisioning

When you connect the IP phones to the network and power them up, the phones' automatic provisioning is triggered. The phones automatically send out a DHCP Discovery request and then receive IP address information (e.g., TFTP server's address) in the DHCP Options sent by the DHCP server. The phones then contact the provisioning server for downloading the required files (e.g., .cfg file and firmware .img file).

2.5 Troubleshooting Automatic Provisioning

2.5.1 Using the Phone Screen

Use the table below to help troubleshoot deployment problems that can occur after preparing the enterprise network environment for IP phone deployment.



Tip: Use the *first phone* that you deploy as an *indicator* for the entire deployment. If the first phone plugs in and plays without irregularities, all phones deployed after it should also. If it doesn't, troubleshoot as shown in this section before proceeding to deploy the other phones.



After preparing the network and verifying readiness, make sure the Skype for Business PC client is operating, i.e., that the Skype for Business server-client (Front End) setup is correct. Only after this, deploy the first phone.

Table 2-9: Troubleshooting Deployment Problems

Problem / Phone Screen Notification	Corrective Action
Certificate problem Phone Screen Notification: "Failed to validate certificate" -or- "Failed to obtain user certificate"	Three possible actions: <ul style="list-style-type: none"> ■ Make sure DHCP Option 43, sub-option 5, was enabled in the DHCP server. If it wasn't, enable it. ■ Make sure you can access the Skype for Business Web service URL: ■ https://lyncsvrWebPoolFQDN:443/CertProv/CertProvisioningService.svc ■ Query the LDAP server: _ldap._tcp.<DOMAIN name> Make sure it was enabled. If it wasn't, enable it in order to get the root certificate.
Synchronization problem. Phone Screen Notification: "Failed to connect to time server" -or- "PIN internal error"	<ul style="list-style-type: none"> ■ Make sure <i>at least one</i> of the following was configured to enable synchronization: <ul style="list-style-type: none"> • NTP server, via DNS SRV record (_ntp._udp.<SIP domain>pointing to NTP server) • NTP server, returned via DHCP Option 42 • Time.windows.com • Time.nist.gov • Configuration Parameter (manually)
Phone not initializing	Make sure DHCP is enabled.
Cannot find SIP server for 'Domain name'. Phone can't perform registration. Phone Screen Notification: "Failed to connect <domain> server" -or- "Cannot find Lync server at <>"	<ul style="list-style-type: none"> ■ Make sure <i>at least one</i> of the following is enabled in the DNS server: ■ _sipinternaltls._tcp.<domain> (for TLS) ■ DHCP results (Option 120) (for TLS) ■ _sipinternal._tcp.<Domain> (for TCP) ■ DHCP results (Option 120) (for TCP) ■ _sip._tls.<Domain> (for TLS) ■ _sip._tcp.<Domain> (for TCP)
Phone Screen Notification: "Location look-up failed. Please enter your address."	<ul style="list-style-type: none"> ■ Make sure 'Location look up' is configured by the management shell in the Skype for Business server.

Problem / Phone Screen Notification	Corrective Action
Phone Screen Notification: "LAN Link failure"	The LAN link is disconnected. This is a general networking problem that's beyond the scope of this document. Either there's a physical cabling issue or there's a local or VLAN communications problem.
Phone Screen Notification: "Duplicate IP"	This is a general networking problem. The IP address configured for this endpoint was already configured for another. <ul style="list-style-type: none"> ■ In the DHCP server, delete the duplicate IP address and request another.
Phone Screen Notification: "Failed to connect to Lync server"	This is a general networking problem beyond the scope of this document. If a communications problem occurs in the enterprise network, for example, if the server goes down, this notification is displayed on the phone screen.
Phone Screen Notification: "PIN invalid phone info"	The phone number or extension that was entered is invalid. <ul style="list-style-type: none"> ■ Make sure the correct information was entered in the phone screen and in the Skype for Business server interface, and that they tally. ■ Verify in the Skype for Business server interface that the PIN is enabled and if it isn't, enable it.
Phone Screen Notification: "PIN not set"	<ul style="list-style-type: none"> ■ Make sure in the Skype for Business server interface that a PIN was configured for this user account. ■ If it wasn't, create a PIN for the account.
Phone Screen Notification: "PIN expired"	<ul style="list-style-type: none"> ■ In the Skype for Business server interface, renew the PIN expiration policy.
Phone Screen Notification: "PIN account disabled"	<ul style="list-style-type: none"> ■ Make sure in the Skype for Business server interface that the account was enabled. If it wasn't, enable it.
Phone Screen Notification: "PIN internal error"	<ul style="list-style-type: none"> ■ Test the PIN Authentication process on the Skype for Business server: Run in the server shell the emulate cmdlet: Test-CsPhoneBootstrap -PhoneOrExt nnnn -PIN nnnn ■ If the test result is 'fail', there's a configuration error on the Skype for Business server side, hence the PIN sign-in failure on the phone side. To troubleshoot, see: http://technet.microsoft.com/en-us/library/gg412852.aspx



- The *ringer* LED remains red until the problem is corrected.
- Users cannot dial or initiate calls if a phone screen notification is displayed.

2.6 Device Manager

Network administrators can provision an enterprise's phones from the server of the One Voice Operations Center (OVOC) module, Device Manager.



- Device Manager and OVOC share the same server location.
- For more information on using Device Manager to provision phones, see the *Device Manager Administrator's Manual*.

To configure provisioning phones from the OVOC server:

- Use the table as reference.

Table 2-10: OVOC Server Parameters

Parameter	Description
ems_server/keep_alive_period	The OVOC server sends a keep alive message at a configured interval to verify that its link with the network is operating. If no reply is received, the link is determined to be down or not working. Default: 60 minutes
ems_server/provisioning/url	Defines the URL of the OVOC server, for example, http://10.1.8.23:8081
ems_server/user_name	Defines the username of the administrator who'll use the OVOC server for provisioning, for example, John Smith.
ems_server/user_password	Defines the password (encrypted) of the network administrator who'll provision the phones from the OVOC server, for example: {"Y6QYmP53BDkoTvulFjEBuQ=="}

2.7 Audiocodes Device Manager Validation

2.7.1 Introduction

This section describes the configuration requirements of working with Audiocodes IP-Phone device series **Teams Compatible** out of the box in secured environment.

The security process (SSL connection) starts with a phone request to the server, followed phone verification if the server can be trusted. During this process the server send his certificate to the phone and the phone verifies this certificate based on its pre burned trusted certificates list. TLS handshake is strict security.

A valid server cert defined if (1) the server's certificate chain is valid against a list of Trusted CAs (see appendix A) pre-installed on the phone, (2) the server's hostname is valid for each certificate in the chain (issuer field of the certificate should match subject field of the upper issuer in the chain certificate) and (3) the expiration date is valid.

2.7.2 Prerequisites

Audiocodes IP-Phone device with pre-installed trusted CAs

2.7.3 Overview

The device validates the AudioCodes Device Manager identity using known root CA:

The device is shipped with known Root CAs installed. (See Appendix B – AudioCodes Root CA Certificate)

For the initial connection phase, the AudioCodes Device Manager should access the device using a known CA.

Once a successful secured connection has been established between the device and the Device Manager, the user can replace the root CA on the Device Manager and on the device and re-establish the connection leveraging any private root CA.

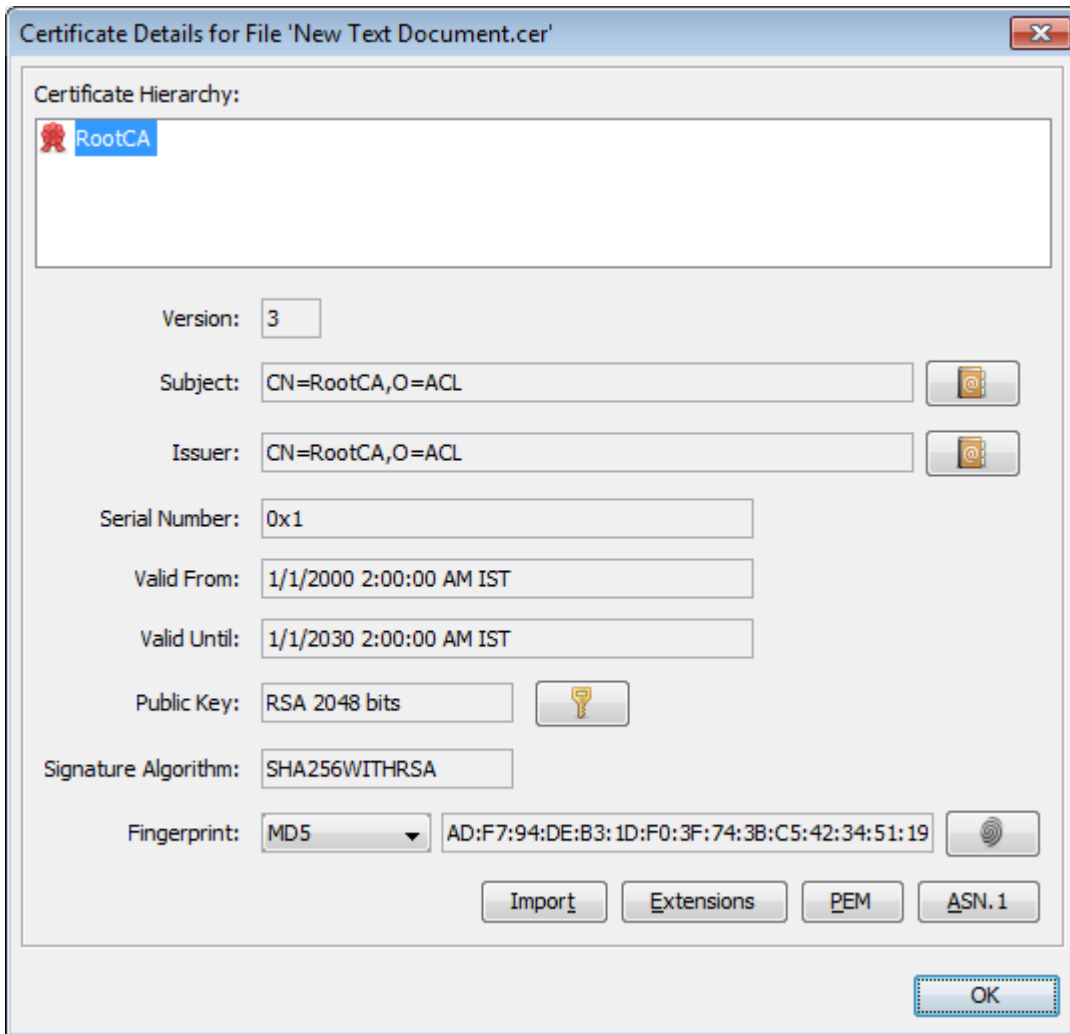
- **Backward compatibility is supported:**
- To implement backward compatibility, the configuration file parameter 'security/SSLCertificateErrorsMode' must be changed from the default to Ignore:
 - SSLCertificateErrorsMode = **Disallow** (default)
 - SSLCertificateErrorsMode = **Ignore** (allows backward compatibility though vulnerability will increase); the phone will proceed without checking the received certificates and without any notifications
 - In case the server isn't signed by one of the root-CAs IP-Phone supports, it is recommended to:
 - Download the needed root-CA via HTTP by IPP configuration using **security/ca_certificate/<0-4>/uri**
 - This way the user doesn't need to change security/SSLCertificateErrorsMode to IGNORE.
 - Before upgrade to 3.4.6.x version download the root-CA using the secured connection https.

2.7.4 Existing Root CA Files in IP Phone

The following list are existing Root CA Files in IP Phone:

- CNNIC_ROOT.cer
- Comodo_AAA_Certificate_Services.cer
- COMODO_Root_CA.cer
- Cybetrust_Baltimore_CyberTrust_Root.cer
- Cybetrust_GlobalSign_Root_CA.cer
- Cybetrust_GTE_CyberTrust_Global_Root.cer
- DigiCert_Cloud_Services_CA-1.cer
- DigiCertGlobalG2TLSRSASHA2562020CA1.cer
- DigiCertGlobalRootCA.cer
- DigiCertGlobalRootG2.cer
- DigiCertGlobalRootG3.cer
- DigiCert_High_Assurance_EV_Root_CA.cer
- DigiCertSHA2SecureServerCA.cer
- DST_Root_CA_X3.cer
- D-Trust_Root_Class_3_CA_2_2009.cer
- D-TRUST_Root_Class_3_CA_2_EV_2009.cer
- Entrust_Entrust.net_Certification_Authority_2048.cer
- Entrust_Root_Certification_Authority_G2.cer
- GeoTrustEVRSA2018.cer
- GeoTrust_GeoTrust_Global_CA.cer
- GlobalSign.cer
- Go_Daddy_Go_Daddy_Class_2_Certification_Authority.cer
- Go_Daddy_Starfield_Class_2_Certification_Authority.cer
- isrgrootx1.pem.cer
- letsencryptauthorityx3.cer
- StartCom_Certification_Authority.cer
- thawte_Primary_Root_CA_G3.cer
- VeriSign_Class_2_Public_Primary_Certification_Authority.cer
- VeriSign_Class_3_Public_Primary_Certification_Authority.cer
- VeriSign_Class_3_Public_Primary_Certification_Authority_G1.cer
- VeriSign_Class_3_Public_Primary_Certification_Authority_G2.cer
- VeriSign_Class_3_Public_Primary_Certification_Authority_G3.cer
- VeriSign_Class_3_Public_Primary_Certification_Authority_G5.cer

2.7.5 Certification Details Dialog



```

-----BEGIN CERTIFICATE-----
MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTB1Jvb3RDQTAEFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa
MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYIEYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGwmsRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhDaoqNM6Kp5b7sJ1ew4I9kfd/ma9Cz15koESLlw/inLj/r+rD96
mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKks
EhGAJsnHaRqsR2Su3X/WtSlgEF+cvP34pxhlhFL29nMfnaFATSS3rgGafLsv11ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBQBQDXySn9hz151DraZ+iXddZGREB+zBHBgNVHSME
QDA+gBQDXySn9hz151DraZ+iXddZGREB+6EjpcEwHzEMMAoGA1UEChMDQUNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywommWWJnH3
JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFKkxMp
0KKWZ4F39caOLRjqhzya+xUeeJ9HQZCXyAJ6XgvTfn2BtyZk9Ma8WG+H1hNvvTZY
QLbWsjQdu4eFniEufeYDke1jQ6800LwM1Flc59hMQCeJTEnRx4HdJbJV86k1gBUE
A7fJTlePrRnXNDRz6QtADWoX3OmN7Meqen/roTwwLpEP22nYwvB28dq3JetlQKwu
XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en513RDz1YpYwWqWHA8jJIu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE-----

```


3 Manual Configuration of a Single IP Phone

Most phones in an enterprise typically require identical configuration settings. Best practice is therefore to manually configure a single IP phone with the settings you require, and then to use the delta configuration (the difference between the default and your configured settings) to automatically provision all phones in the enterprise via DHCP.

This section shows how to manually configure a single IP phone. After manually configuring a single IP phone, create the delta configuration file as shown in Section 2.2, and place it on the provisioning server.

3.1 Configuring Network Connections

You can configure IP network connections. For information on configuring Port Mirroring, see Section 7.5 on page 192 under 'Performing Diagnostics'.

3.1.1 Configuring LAN Connection Type

The phone's LAN Connection Type can be:

- Automatic IP (DHCP) (automatically provisioned by DHCP server from where the LAN IP address is obtained) (default)
- Static IP Address

This section shows how to change LAN Connection Type in the phone's screen and through the Web interface.

To change LAN Connection Type in the phone's screen:

1. When the phone's screen is in idle display, press the MENU key and then navigate to and select the **Administration** option in the Menu screen that is displayed.



- The default password is **1234**. It's advisable for the network administrator to change it to prevent unauthorized access.
- To change the default password, use the phone's Web interface or Configuration File.

2. Enter the password and then **OK**.
3. In the Administration screen that opens, select Network Settings.
4. In the Network Settings screen, select LAN Connection Type.
5. In the LAN Connection Type screen, navigate to and select Static IP.
6. Define a static IP addressing scheme:
 - a. Press the **Edit** softkey and enter the new address in dotted-decimal notation, using the following keys:
 - ◆ **Navigation control**: moves the cursor left or right in the IP address
 - ◆ **Clear** softkey: deletes the digit to the left of the cursor.
 - b. Press the **Save** and then **Apply** softkey.
7. Navigate to and configure **Netmask**, **Gateway**, **Primary DNS** and **Secondary DNS Address**.

To change the LAN Connection Type:

1. Open the Configuration File page in the Web interface (**Management** tab > **Manual Update** > **Configuration File**).
2. Configure the parameters using the table below as reference.

Table 3-1: Network Settings – Static IP

Parameter	Description
Note: To add a value to these parameters, enter network/ followed by the parameter name, equal sign and then the value (e.g. <code>network/lan_type=DHCP</code>).	
<code>network/lan_type</code>	Defines the IP addressing method: <ul style="list-style-type: none"> ■ [STATIC] Static IP - IP address defined manually ■ [DHCP] Automatic IP DHCP (default) - IP address is acquired automatically from a DHCP server
<code>network/lan/fixed_ip/ip_address</code>	The LAN IP address
<code>network/lan/fixed_ip/netmask</code>	The subnet mask address
<code>network/lan/fixed_ip/gateway</code>	The IP address of the default gateway.
<code>network/lan/fixed_ip/domain_name</code>	The domain name.
Domain Name Server (DNS)	
<code>network/lan/fixed_ip/primary_dns</code>	The primary DNS server address.
<code>network/lan/fixed_ip/secondary_dns</code>	The secondary DNS server address. The phone connects to this server if the primary DNS server is unavailable.

The following parameters can be configured:

Table 3-2: Network Settings - Automatic IP (DHCP)

Parameter	Description
network/lan_type	<p>Defines the IP addressing method:</p> <ul style="list-style-type: none"> ■ [STATIC] Static IP - Phone's IP address is defined manually ■ [DHCP] Automatic IP DHCP (default) - Phone's IP address is acquired automatically from a DHCP server
network/lan/dhcp/domain_name/enabled	<p>Enables setting the domain name manually.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>Note: If enabled, network/lan/fixed_ip/domain_name must also be set.</p>
network/lan/dhcp/ip_address/enabled	<p>Enables setting the IP address manually.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>Note: If enabled, network/lan/fixed_ip/ip_address must be set.</p>
network/lan/dhcp/netmask/enabled	<p>Enables setting the network mask manually.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>Note: If enabled, network/lan/fixed_ip/netmask must be set.</p>
network/lan/dhcp/gateway/enabled	<p>Enables setting the default gateway manually.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>Note: If enabled, network/lan/fixed_ip/gateway must be set.</p>
network/lan/dhcp/primary_dns/enabled	<p>Enables setting the primary DNS manually.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>Note: If enabled, network/lan/fixed_ip/primary_dns must be set.</p>
network/lan/dhcp/secondary_dns/enabled	<p>Enables setting the secondary DNS manually.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>Note: If enabled, network/lan/fixed_ip/secondary_dns must be set.</p>

3.1.2 Configuring LAN Port / PC Port

Port settings can be configured using the Configuration File.



This section does not apply to the RX50 conference phone.

To define phone port settings:

1. Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**)
2. Configure using the table below as reference.

Table 3-3: Port Settings

Parameter	Description
network/lan/port_mode	Sets the LAN port mode. Valid values are: AUTOMATIC] = Auto negotiation. FULL_10] = 10Mbps + full duplex FULL_100] = 100Mbps + half duplex HALF_10] = 10Mbps + full duplex HALF_100] = 100Mbps + half duplex
network/pc/port_mode	Sets the computer port mode. Valid values are: AUTOMATIC] = Auto negotiation FULL_10] = 10Mbps + full duplex FULL_100] = 100Mbps + half duplex HALF_10] = 10Mbps + full duplex HALF_100] = 100Mbps + half duplex DISABLE] = Disables the PC port mode

3.1.3 Configuring VLAN Settings

VLAN settings can be configured using the Web interface, Configuration File, or the phone's screen.

To configure the phone's VLAN settings:

1. Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**).
2. Configure using the table below as reference.

Table 3-4: VLAN Parameters Description

Parameter	Description
network/lan/vlan/mode	<p>Determines the VLAN mode of operation.</p> <ul style="list-style-type: none"> ■ [Disable] Disable ■ [Manual] Manual Configuration of LAN - Static configuration of VLAN ID and priority ■ [CDP] Automatic Configuration of VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol (CDP) ■ [LLDP] Automatic Configuration of VLAN - VLAN discovery mechanism based on LLDP. ■ [CDP_LLDP] Automatic Configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol (CDP). LLDP protocol is with higher priority.
network/lan/vlan/period	<p>The time period in seconds between discovery messages when configured to CDP, LLDP or CDP and LLDP.</p> <p>The default value is 30.</p>
network/lan/vlan/id	<p>Only displayed when the 'VLAN Discovery Mode' parameter (above) is configured to Manual.</p> <p>The valid range is 0 to 4094. The default VLAN ID is 0.</p>
network/lan/vlan/priority	<p>Only displayed when the 'VLAN Discovery Mode' parameter (above) is configured to Manual.</p> <p>Defines the priority of traffic pertaining to this VLAN.</p> <p>The valid range is 0 to 7 (where 7 is the highest priority). The default VLAN priority is 0.</p>

To configure the phone's VLAN settings from the phone's screen:

1. Press the phone's MENU hard key when the screen is in idle display and then in the Menu screen that opens, navigate to and select the **Administration** option.
2. Enter the same password you use to access your PC, and then **OK**; the Administration menu opens.
3. Select **Network Settings** and in the Network Settings screen that opens, navigate to and select **VLAN Settings**.
4. For 'VLAN mode', press the navigation control's left or right rim to choose either **DISABLE**, **MANUAL**, **CDP**, **LLDP**, or **CDP_LLDP**.
5. If you choose **MANUAL**, enter 'VLAN ID' and 'VLAN Priority'.
6. If you choose **CDP**, **LLDP**, or **CDP_LLDP**, you can configure an **Interval**.

3.2 Configuring Personal Settings

3.2.1 Configuring Language

This section describes how to configure the language displayed in the phone screen. Language displayed can be configured using the Configuration File.

To choose a language:

- Use the table below as reference.

Table 3-5: Language Display Parameters

Parameter	Description
personal_settings/language	<p>Determines the phone screen language.</p> <ul style="list-style-type: none">■ [English] English (default)■ [Spanish] Spanish■ [Russian] Russian■ [Portuguese] Portuguese■ [German] German■ [Ukraine] Ukrainian■ [French] French■ [Italian] Italian■ [Hebrew] Hebrew■ [Polish] Polish■ [Korean] Korean■ [Finnish] Suomalainen■ [Chinese] Chinese Simplified■ [Chinese] Chinese Traditional■ [Magyar] Hungarian■ [Japanese] Japanese■ Slovak■ Czech

3.3 Configuring Function and Programmable Keys

Function Keys can be configured for Speed Dials and for Multicast Paging. Function Keys are located on the sidecar.

On the 445HD phones:

- Up to 33 Function Keys can be configured for Speed Dialing or for Multicast Paging. The 33 Speed Dials are configured on pages 1, 2 and 3 of the phone's sidecar. Users define 12 Speed Dials and then when defining the 13th, the 12th Speed Dial shows the page number and the name in the 12th moves to the 13th.
- Six programmable keys are located adjacent to the screen. There are three on each side.
 - To configure 1-6 Programmable Keys, configure **n = 12-17** correspondingly.
 - To configure 1-12 Functional Keys, configure **n = 0-11** correspondingly.
 - To configure 13-33 Functional Keys, configure **n = 18-38** correspondingly.

On the 450HD / C450HD / HRS:

To configure 1-8 Programmable Keys, configure **n = 0-7** correspondingly.

On the 450HD / C450HD phone with Expansion Module (which supports two pages and a total of 40 Functional Keys, each page displaying 20 Functional Keys):

To configure 1-40 Functional Keys, configure **n = 8-27** for the first page and **n = 28-47** for the second page.

On the RX50 conference device configure:

functional_key/0-5

Speed_dial/0-5

Table 3-6: Function / Programmable Keys Parameters

Parameter Name	Description
personal_settings/functional_key/n/key_label	Used to define a free string label allowing users to identify the key.
personal_settings/functional_key/n/type	Choose either: <ul style="list-style-type: none"> ■ EMPTY = (default) If left as is, the key will be disabled. ■ SPEED_DIAL = key to help users quickly dial numbers that are often used or hard to remember. ■ PAGING = When the Paging feature is enabled, you can define Paging Groups. ■ Event = Key used to access events like DnD, Missed Call, etc. (See the next parameter for more information). ■ VocaNOM = Enable the key if the feature is enabled. ■ Discreet_Call = See Section 3.3.1.3 for detailed information.
personal_settings/functional_key/n/key_event	<ul style="list-style-type: none"> ■ Missed_Calls ■ Received_Calls ■ Dialed_Calls ■ Directory ■ Dnd_All ■ Forward_All ■ Calendar ■ Hot_Desking
personal_settings/functional_key/n/speed_dial_number	Allows the user to quickly call someone whose number is often used or is hard to remember. Default: 4403.
personal_settings/functional_key/n/line	Corresponding to the line ID. n = the value you configured as the line index.

3.3.1 Configuring a Function Key

3.3.1.1 Configuring a Function Key for Speed Dialing



The phone's speed dials can be defined in a simple text-based editor, placed on a server (e.g., HTTP or FTP/TFTP), and then uploaded to the phone using the Configuration File.

The Configuration File can include a link to a user-defined Speed Dial file, using the **provisioning/speed_dial_uri** parameter. This allows you to upload speed dial settings to the phone.

The Speed Dial file must include a list of speed dial configurations. The file must be a simple text file that can be created using an Excel document and saved as a CSV file.

The syntax of the speed dial file is as follows:

```
<memory key>,<speed dial phone number>,<type>
```

where:

- *memory key* denotes the speed dial memory key on the phone.
- *speed dial phone number* denotes the phone number that is automatically dialed, when the user presses the speed dial key.
- *type* denotes the Speed Dial feature and must be set to "0".

Below is an example of a Speed Dial file:

```
1,4418,0
2,4403,0
3,039764432,0
4,4391,0
12,1234,0
```

To configure a Function Key for speed dialing:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-7: Speed Dial Parameter

Parameter Name	Description
provisioning/speed_dial_uri	<p>The URI for retrieving the speed dial list which must be included in a separate file to be downloaded to the phone during provisioning.</p> <p>For example: provisioning/speed_dial_uri=speed_dial_list.txt</p> <p>Note:</p> <ul style="list-style-type: none"> ■ The speed dial file is downloaded after boot up and periodically ■ If the speed dial file is new, the phone reboots.

3.3.1.2 445HD, 450HD, C450HD and RX50

On the 450HD and C450HD phones, 1-8 Function Keys are available in the idle screen, four keys on the left side of the screen and four on the right.

On the 450HD phone + Expansion Module and C450HD phone + Expansion Module, Function Keys 9-48 are available in the phone's sidecar to the right of the phone's physical interface. In the Configuration File, the keys are labeled 8-47.

On the RX50, 1-6 Programmable Keys are available from the **Menu** softkey > **Keys**.

On the 445HD phone, all keys **1-33** can be configured as Speed Dial, Paging, Key Event or VocaNOM.

3.3.1.2.1 Saving Configured Features in a cfg File

In the Web interface, after configuring features you can save the configuration in a cfg file on your computer and load it to other phones.

To save features in a cfg file:

- In the Function Keys page (**Configuration** tab > **Personal Settings** menu > **Function Keys**), click **Save Function Keys**; the configuration is saved in a .cfg file.

3.3.1.2.2 Loading the cfg File to Other Phones

After saving the configuration in a cfg file on your computer, you can load it to other phones.

To load the cfg file to another phone:

1. In the Function Keys page of another phone's Web interface (**Configuration** tab > **Personal Settings** menu > **Function Keys**), click **Browse....**
2. In the Choose File to Upload page that opens, navigate to and select the cfg file saved on your computer.
3. Click **Load Function Keys**; the file is uploaded to the phone.

3.3.1.2.3 Deleting a Configured Dial

To delete configured dials either:

- Select the 'Delete' check boxes corresponding to the dials that you want to delete and click **Submit**.
- Click **Delete All** and at the prompt click **OK**.
- Click **Reset** to clear (unselect) all selected 'Delete' check boxes.

3.3.1.3 Configuring a Function Key for Making a Discreet Call

This feature answers a requirement for more security measures such as a silent mode call for public institutions. If a call is made in discreet mode, it's a one-way call to a remote phone. The caller's phone does not indicate audially that a call is in progress. The phone's screen remains in idle mode and the backlight is not activated. The only indication that a call is in progress is the presence status of the caller changes to red (busy). The caller cannot end the call. It's recommended that the called party's phone be a dedicated phone to avoid the scenario of being on another call when needed for the discreet call; the phone automatically answers the discreet call; there is no need to pick up the handset. The called party then 'listens' to what's happening at the caller's end. When the called party ends the call, the call ends on both sides.

To configure a Function Key for making a discreet call:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-8: Discreet Call Parameters

Parameter Name	Description
personal_settings/functional_key/[X]/key_label	Configure a label for the key. The label is displayed in the phone's screen next to the Functional Key. Make it intuitive to facilitate easy and quick action in an emergency. The label should differentiate it from other Speed Dials.
personal_settings/functional_key/[X]/speed_dial_extension	Configure the extension of the authority in the organization to whom to make the discreet call.
personal_settings/functional_key/[X]/speed_dial_number	Configure the telephone number of the authority in the organization to whom to make the discreet call.
personal_settings/functional_key/[X]/type	Configure this parameter to DISCREETCALL .
personal_settings/discreet_call/enabled	Enables or disables the discreet call feature. <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable



- Both caller and called party phones must be AudioCodes phones.
- Device Lock must be disabled on the called party's phone
- The call runs via the Skype for Business server as a regular call when the phone tunes the behavior to match the required functionality.

3.3.2 Configuring Programmable Keys

This section shows how to configure a programmable key on the device using the Configuration File.

To configure a Programmable Key:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the tables below as reference.

Table 3-9: Programmable Key Parameters in the Configuration File

Parameter Name	Description
personal_settings/functional_key/n/shared_line_index	<p>n = 0-7 on the 450HD and C450HD; eight line keys can be configured.</p> <p>n = 0-5 on the RX50; six line keys can be configured.</p> <p>n = 12-17 on the 445HD; six line keys can be configured.</p> <p>Each can be configured as Key Type VocaNOM, Speed Dial, Discreet Call, Paging, Key Event or Empty. VocaNOM is a service that lets users vocalize a destination number to call, instead of manually dialing it.</p> <p>Speed Dial lets users quickly access and dial numbers they use often. Speed Dial indicates the presence status of people for whom speed dials are configured.</p> <p>Key Event lets users quickly access Calendar (default), Dialed Numbers, Missed Calls, Received Calls, Dialed Calls, Directory, DnD All or Forward All.</p>
personal_settings/functional_key/n/type	<p>Each Line Key can be configured as type:</p> <ul style="list-style-type: none"> ■ VOCANOM ■ SPEED_DIAL ■ PAGING ■ Discreet Call ■ KEY_EVENT ■ Empty
personal_settings/functional_key/ n/key_label	<p>Displayed in the Web interface only if 'Key Type' is configured. Allows you to configure a label for the Programmable Key, e.g., the name of a person to whose phone number a speed dial will dial. The label is displayed in the phone's screen.</p>
personal_settings/functional_key/n/speed_dial_number	<p>Displayed in the Web interface only if 'Key Type' is configured as Speed Dial. Configure the telephone number of the contact to whom the speed dial will dial.</p>
personal_settings/functional_key/n/key_event	<p>Lets users quickly access CALENDAR (default), Missed Calls, Received Calls, Dialed Calls, Contacts, Hot Desking, DnD All or Forward All.</p>

3.3.2.1.1 Saving Configured Programmable Keys in a cfg File

After configuring Speed Dials, you can save the configuration in a cfg file on your computer and load it to other phones.

To save Speed Dials in a cfg file:

1. Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).
2. Click **Save Programmable Keys**; the configuration is saved in a cfg file.

3.3.2.1.2 Loading the cfg File to Other Phones

To load the cfg file to another phone:

1. In the Programmable Keys page in another phone's Web interface, click **Browse....**
2. In the Choose File to Upload dialog that opens, navigate to and select the cfg file saved previously on your computer.
3. Click **Load Programmable Keys**; the file is uploaded to the phone.

3.3.3 Configuring Programmable Softkeys for a Customized UI Experience

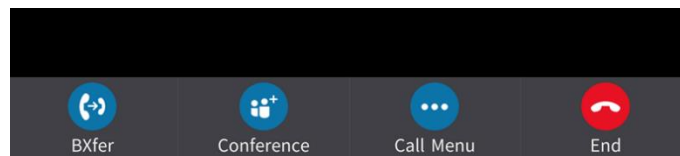
Users can configure Programmable Softkeys for **New Call** state, **Ongoing call** state and **Idle** screen state as part of the phone's capability of allowing a customized user interface experience.

- Configurable idle screen

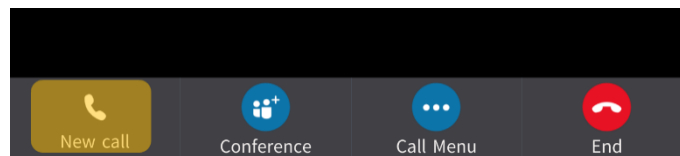
Administrators can customize the home screen in line with the preferences / requirements of enterprise management and / or the employees. A typical use for this feature can be the option to disable the **Meet Now** softkey and replace it with another softkey such as the **Received Calls** softkey or the **Calendar** softkey.

- Configurable ongoing call screen.

- Administrators can customize the ongoing call screen (shown in the figure below) in line with the preferences / requirements of enterprise management and / or the employees.

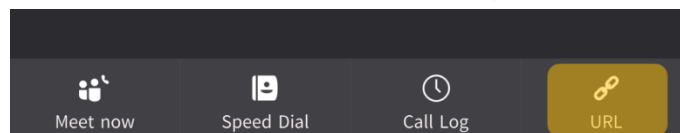


For example, the **Bxfer** softkey in the ongoing call screen shown in the preceding figure can be replaced with the **New Call** softkey shown in the figure below on the phones of enterprise users who infrequently transfer calls.

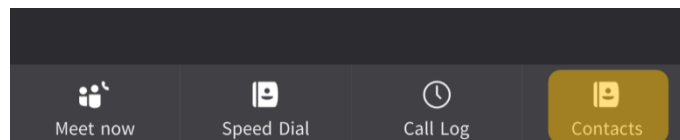


- Configurable initiate call screen

Administrators can customize the initiate call screen (shown in the figure below) in line with the preferences / requirements of enterprise management and / or the employees.



For example, the **URL** dialing softkey in the initiate call screen shown in the preceding figure can be replaced with the **Contacts** softkey shown in the figure below.



3.3.4 Configuring a Programmable Softkey to Allow Paging during an Ongoing Call | Call Hold | Call Park

Network administrators can allow users to perform paging during an ongoing call, call hold and call park. To enable the feature, administrators must program a softkey for users to use the functionality. The softkey is displayed in the ongoing call screen.



Paging must be configured as described in Section 3.4.17 as a prerequisite for the feature to function.

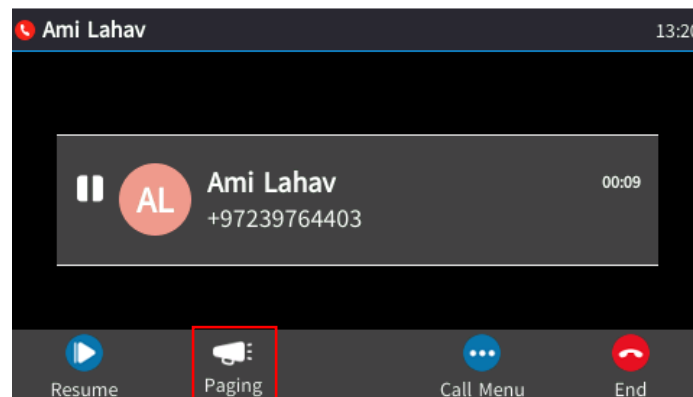
To configure a PSK for paging during an ongoing call | call hold | call park:

- Use the table as reference:

Table 3-10: Configuring a PSK for Paging during an Ongoing Call | Call Hold | Call Park

Parameter	Description
personal_settings/soft_keys/ongoing_call/n/key_function	Set to PAGING . Note that n=0-19.

Users will view a 'Paging' softkey in the phone's Hold screen (i.e., in the screen displayed when the user holds a call).



3.3.5 Configuring Tones

This section shows how to configure ring tones using the Configuration File and how to upload them to the phone.

3.3.5.1 Configuring CPT Regional Settings

It's important to match your phone's Call Progress Tones (CPT) to the country in which your phone is located. This section shows how to configure it.

To configure regional location:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-11: Regional Parameters

Parameter	Description
voip/regional_settings/selected_country	<p>Defines the country in which your phone is located. The behavior and parameters of analog telephones lines vary between countries. CPTs are country-specific. The phone automatically selects the correct regional settings according to this parameter. Supported countries are:</p> <ul style="list-style-type: none"> ■ [Israel] Israel ■ [China] China ■ [France] France ■ [Germany] Germany ■ [Netherlands] Netherlands ■ [UK] UK ■ [Brazil] Brazil ■ [Italy] Italy ■ [Argentina] Argentina ■ [Portugal] Portugal ■ [Russia] Russia ■ [Australia] Australia ■ [USA] USA ■ [India] India
voip/regional_settings/use_config_file_values	<p>Enables the user-defined CPT. When this parameter is enabled, the 'selected_country' parameter is not relevant and the CPT values below can be determined by the user.</p> <ul style="list-style-type: none"> ■ [0] - Disable (default) ■ [1] - Enable
Call Progress Tones (CPT)	
Note: Up to 10 CPTs can be configured (voip/regional_settings/call_progress_tones/0...9).	
voip/regional_settings/call_progress_tones/%d/enabled	<p>Enables the specific CPT.</p> <ul style="list-style-type: none"> ■ [0] - Disable ■ [1] - Enable
voip/regional_settings/call_progress_tones/%d/name	<p>Defines the name of the CPT.</p>
voip/regional_settings/call_progress_tones/%d/cadence	<ul style="list-style-type: none"> ■ Defines the cadence type of the tone. ■ [0] - Continuous signal ■ [1] - Cadence signal ■ [2] - Burst signal

Parameter	Description
<code>voip/regional_settings/call_progress_tones/%d/frequency_a</code>	Defines the low frequency (in Hz) of the tone. Range: 300 - 1980 Hz, in steps of 1 Hz. Unused frequencies must be set to zero.
<code>voip/regional_settings/call_progress_tones/%d/frequency_b</code>	Defines the high frequency (in Hz) of the tone. Range: 300 - 3000 Hz, in steps of 1 Hz. Unused frequencies must be set to zero.
<code>voip/regional_settings/call_progress_tones/%d/frequency_a_level</code>	Output level of the low frequency tone (in -dBm) in Call Progress generation. Range: 0 - 63, where 63 is mute.
<code>voip/regional_settings/call_progress_tones/%d/frequency_b_level</code>	Output level of the low frequency tone (in -dBm) in Call Progress generation. Range: 0 - 63, where 63 is mute.
<code>voip/regional_settings/call_progress_tones/%d/tone_on_0</code>	tone_on_0 to tone_on_3. If the signal is Cadence or Burst, then this value represents the on duration. If a Continuous tone, then this value represents the minimum detection time. In units of 10 msec. Range: 0 - 10000.
<code>voip/regional_settings/call_progress_tones/%d/tone_off_0</code>	tone_off_0 to tone_on_3. If the signal is Cadence, then this value represents the off duration, in units of 10 msec. If not used, then set it to zero. If the signal is Burst, only tone_off 0 is relevant. It represents the off time that is required from the end of the signal to the detection time. Range: 0 - 10000.

3.3.5.2 Uploading Ring Tones

This section shows how to upload ring tones using the Configuration File.



- The ring tone file must be in WAV file format (A/Mu-Law, 8-kHz audio sample rate and 8-bit audio sample size or PCM 16-kHz audio sample rate and 16-bit audio sample size, Intel PCM encoding).
- For the phone to use an uploaded ring tone, select it in the phone's screen (refer to the phone's *User's Manual*).

To define the Ring Tone File URI:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-12: Ring Tone File URI in the Configuration File

Parameter	Description
provisioning/ring_tone_uri	<p>The URI for retrieving the ring tones file. The ring tones can be compressed to zip or tgz files and provided to the phone during provisioning.</p> <p>For example: provisioning/ring_tone_uri=tones.tgz</p> <p>Note:</p> <ul style="list-style-type: none"> ■ The ringtone file is downloaded only after boot up, and not periodically. ■ If the tones file is new, the phone updates the information, but does not reboot.

To select Ring Tones:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-13: Ring Tones Parameter in the Configuration File

Parameter	Description
personal_settings/lines/0/ring_tone	<p>Define the ring tone name.</p> <p>Default Range: Ring01 - Ring11.</p> <p>Default Selection: Ring01.</p> <p>Alternatively, you can select the name of a previously uploaded file, as in the example above (tones.tgz).</p>

3.3.6 Configuring Phone Screen Settings

This section shows how to configure phone screen settings using the Configuration File.



The 445HD, 450HD, C450HD and RX50 screen contrast parameters apply only if Microsoft Skype for Business' online Power Save Mode feature is enabled, i.e., the parameters apply only to *online* users. They do not apply to Skype for Business *on premises* users. Three inband Microsoft parameters control Skype for Business's online Power Save mode:

- EnablePowerSaveMode [True] = the phone will use these Skype for Business timeout values instead of 'lcd_active_mode_timeout'.
- PowerSaveDuringOfficeHoursTimeoutMS [15 minutes]
- PowerSavePostOfficeHoursTimeoutMS [5 minutes]
- If inband provisioning is performed and all three Microsoft parameters are provisioned and the first is enabled:
 - The second determines 'active mode' timeout if in working hours.
 - The third determines 'active mode' timeout if in non-working hours.

The screen will change to 'night mode' only if the user is in non-working hours, i.e., the screen will never go lower than 'dimmer mode' when the user is in working hours. In the morning, when working hours start, the screen automatically changes from 'night mode' to 'dimmer mode'. The phone gets the user's work hours from Microsoft Exchange server. Users can configure a brightness level of High, Medium or Low for Active mode, Dimmer mode and Night mode. By default, the phone enters Dimmer mode after 15 minutes of inactivity; by default, the phone enters Night mode after another 60 minutes of inactivity. If the capability to determine working hours is configured, the phone only enters Night mode during non-working hours.

Dimmer mode is less bright than Active mode. Night mode is lowest. When a phone enters Dimmer mode, *LCD_Dimmer_mode_timeout* starts. When it expires, the phone switches to Night mode (which is allowed only during non-working hours if working hours are available). Any phone operation such as an incoming call or touching the screen causes the phone to exit Power Saving mode and revert to the regular screen brightness level.

To configure phone screen settings:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the tables below as reference.

Table 3-14: Screen Contrast Parameters [445HD, 450HD, C450HD and RX50]

Parameter	Description
personal_settings/lcd_active_mode_brightness	Configures the brightness of the screen when its in 'active mode', which is - for example - after a calendar reminder pops up, or when a call comes in, or after you press a key on the dial pad, etc. <ul style="list-style-type: none"> ■ LOW ■ MEDIUM ■ HIGH (default)
personal_settings/lcd_active_mode_brightness_high	Configures the HIGH level of brightness when the screen is in 'active mode'. Minimum: 0. Maximum: 31 (default).
personal_settings/lcd_active_mode_brightness_low	Configures the LOW level of brightness when the screen is in 'active mode'. Minimum: 0. Maximum: 31. Default: 20.
personal_settings/lcd_active_mode_brightness_medium	Configures the MEDIUM level of brightness when the screen is in 'active mode'. Minimum: 0. Maximum: 31. Default: 26.
personal_settings/lcd_active_mode_timeout	Defines the timeout of 'active mode', in minutes. If the timeout expires, the screen changes to 'dimmer mode' (see the next parameter). Either: 15 (default), 30, 45 or 60 minutes.
personal_settings/lcd_dimmer_mode_brightness	Configures the brightness of the screen when its in 'dimmer mode'. The screen changes to 'dimmer mode' after the timout configured for 'active mode' times out (see the parameter above). Either: <ul style="list-style-type: none"> ■ LOW ■ MEDIUM (default) ■ HIGH
personal_settings/lcd_dimmer_mode_brightness_high	Configures the HIGH level of brightness when the screen is in 'dimmer mode'. Minimum: 0. Maximum: 31 (default).
personal_settings/lcd_dimmer_mode_brightness_low	Configures the LOW level of brightness when the screen is in 'dimmer mode'. Minimum: 0. Maximum: 31. Default: 20.

Parameter	Description
personal_settings/lcd_dimmer_mode_brightness_medium	Configures the MEDIUM level of brightness when the screen is in 'dimmer mode'. Minimum: 0. Maximum: 31. Default: 26.
personal_settings/lcd_dimmer_mode_timeout	Defines the timeout of 'dimmer mode', in minutes. If it expires, the screen changes to 'night mode' (see the next parameter). Either: 30, 60 (default), 90 or 120 minutes.
personal_settings/lcd_night_mode_brightness	Configures the brightness of the screen when its in 'night mode'. The screen changes to 'night mode' after the timout configured for 'dimmer mode' times out (see the parameter above). Either: <ul style="list-style-type: none"> ■ LOW (default) ■ MEDIUM ■ HIGH There is no timeout for 'night mode'.
personal_settings/lcd_night_mode_brightness_high	Configures the HIGH level of brightness when the screen is in 'night mode'. Minimum: 0. Maximum: 31. Default: 26. There is no timeout for 'night mode'.
personal_settings/lcd_night_mode_brightness_low	Configures the LOW level of brightness when the screen is in 'night mode'. Minimum: 0. Maximum: 31. Default: 5. There is no timeout for 'night mode'.
personal_settings/lcd_night_mode_brightness_medium	Configures the MEDIUM level of brightness when the screen is in 'night mode'. Minimum: 0. Maximum: 31. Default: 20. There is no timeout for 'night mode'.

3.3.7 Configuring a Distinctive Ring Tone

The network administrator can configure a distinctive ring tone on the phone of a user. Distinctive ring tones help users audially distinguish between phones when calls come in, optimizing work efficiency.

To configure a distinctive ring tone:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-15: Distinctive Ring Tone Parameters

Parameter	Description
voip/distinctive_ringing/0-4/ringtone	Select either: <ul style="list-style-type: none">■ Ring01 (Default)■ Ring02■ Ring03■ Ring04
voip/distinctive_ringing/0-4/type	Not applicable to Skype for Business phones

3.4 Configuring VoIP Settings

This section shows how to configure VoIP settings. Only the settings documented in this *Administrator's Manual* are applicable.

3.4.1 Configuring TLS/SSL over SIP

This section shows how to configure TLS/SSL over SIP using the Configuration File. TLS/SSL authenticates and secures communications over SIP using certificate-based authentication and symmetric encryption keys.

To configure TLS/SSL over SIP:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-16: TLS/SSL over SIP Parameters

Parameter	Description
voip/signalling/sip/tls_method	<p>Possible values:</p> <ul style="list-style-type: none"> ■ ssl_2 ■ ssl_3 ■ ssl_2_3 (default) ■ tls_1 ■ tls_1_1 ■ tls_1_2 <p>Generally, set to the default because only the default allows for flexibility when selecting a mutually acceptable method. With all other values, the method is set specifically.</p>
voip/signalling/sip/tls_disable	<p>Possible values: space separated list of values from above list. For example:</p> <ul style="list-style-type: none"> ■ " ssl_2 ssl_3 " (default) <p>Used only when 'tls_method' is set to ssl_2_3 because only the default allows for flexibility when selecting a mutually acceptable method. With all other values, the method is set specifically.</p>

3.4.2 Configuring TLS/SSL over SIPE

This section shows how to configure TLS/SSL over SIPE using the Configuration File. TLS/SSL authenticates and secures communications using certificate-based authentication and symmetric encryption keys.

To configure TLS/SSL over SIP:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-17: TLS/SSL over SIPE Parameters

Parameter	Description
voip/signalling/sipe/tls_method	<p>Possible values:</p> <ul style="list-style-type: none"> ■ ssl_2 ■ ssl_3 ■ ssl_2_3 (default) ■ tls_1 ■ tls_1_1 ■ tls_1_2 <p>Generally set to the default because only the default allows for flexibility when selecting a mutually acceptable method. With all other values, the method is set specifically.</p>
voip/signalling/sipe/tls_disable	<p>Possible values: space separated list of values from above list. For example:</p> <ul style="list-style-type: none"> ■ "ssl_2 ssl_3" (default) <p>Used only when 'tls_method' is set to ssl_2_3 because only the default allows for flexibility when selecting a mutually acceptable method. With all other values, the method is set specifically.</p>

3.4.3 Configuring an Outbound Proxy

Microsoft Skype for Business Server Multitenant Hosting Pack is a Microsoft® Unified Communications (UC) hosting solution for telecommunications and hosting providers. The solution enables Microsoft hosting partners to deploy a single instance of the Skype for Business Server software to securely and economically host multiple tenants with a rich, fully integrated UC solution. To connect the AudioCodes Skype for Business-compatible phone to a hosted Skype for Business environment, a dedicated 'Outbound Proxy' parameter is available which is used to configure the hosted service provider's domain name (FQDN).



In hosted environments, it's common practice that this hosted domain name is different to the enterprise's domain name.

To configure a phone for an LHP environment, configure the address of the Outbound Proxy as the hosted service provider's domain name (FQDN).

To configure:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and use the table below as reference.

Table 3-18: Proxy and Registrar Parameters

Parameter	Description
voip/signalling/sip/sip_outbound_proxy/enabled	Determines whether an outbound proxy server is used (all SIP messages are sent to this server as the first hop). <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable
voip/signalling/sip/sip_outbound_proxy/addr	Displayed when the 'Use Hosting Outbound Proxy' parameter is enabled. Defines the IP address of the outbound proxy. If set, all outgoing messages (including Registration messages) are sent to this Proxy according to the Stack behavior.
voip/signalling/sip/sip_outbound_proxy/port	Displayed when the 'Use Hosting Outbound Proxy' parameter is enabled. Defines the port on which the outbound proxy listens. Range: 1024 to 65535. Default: 5060.

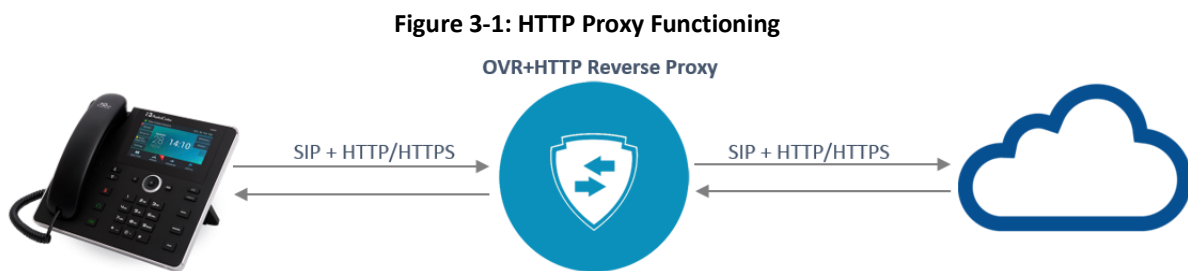
3.4.4 Configuring IP Phone Office 365 Services via HTTP Proxy Support

Network administrators can configure One Voice Resiliency (OVR) IP phones to forward Office 365 services via an OVR embedded reverse proxy, to comply with enterprise security policy. The phone then forwards Office 365 HTTP services designated to port 80/443 (TLS), to AudioCodes' HTTP reverse proxy embedded within the OVR, instead of to the original destination (origin server), similarly to the way in which the phone directs SIP traffic to the OVR instead of directly to Office 365 SIP servers.

Two main components comprise the solution:

- IP phone: Responsible for directing Office 365 HTTP/S client traffic towards the trusted AudioCodes HTTP reverse proxy embedded within the OVR
- OVR + HTTP Reverse Proxy (server) responsible for forwarding the requests to the original address, i.e., the 'real' destination.

The figure below illustrates how the feature functions.



To configure the HTTP Proxy:

- Use the table below as reference.

Table 3-19: HTTP Proxy - Parameter

Parameter	Description
system/ac_http_proxy_ip	Defines the HTTP proxy's IP address. If left unconfigured, the feature will be disabled. Ports 80/HTTP and 443/TLS are used by default. This parameter requires the phone to be rebooted.



HTTP Proxy limitations are:

- The feature is only applicable to users who have the AudioCodes OVR VoIP application running on AudioCodes' Mediant 800B or 1000B devices in their enterprise.
- Only IP phones behind the OVR can access the HTTP proxy
- The HTTP proxy feature is only applicable to users whose Microsoft Exchange server is online
- Some algorithms are functioning incorrectly

3.4.5 Configuring Dialing

This section shows how to configure Dialing parameters. Only the parameters documented in this section are applicable.

3.4.5.1 Adjusting the DTMF Level

Network administrators can adjust the DTMF level of the phone to suit personal requirements.

To adjust the DTMF level:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-20: Automatic Dialing Parameters

Parameter	Description
voip/audio/gain/dtmf_tone_signal_level	Range: 1-32. Default: 16

3.4.5.2 Configuring Automatic Dialing

This section shows how to configure Automatic Dialing using the Configuration File.

To activate automatic dialing:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-21: Automatic Dialing Parameters

Parameter	Description
voip/dialing/auto_dialing/enabled	Determines whether automatic dialing is enabled (i.e., phone number is automatically dialed when you off-hook the phone). <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable
voip/dialing/auto_dialing/timeout	Only displayed if the 'Activate' parameter is configured to Enable . Defines the timeout (in seconds) before automatic dialing occurs after the phone is off-hooked. When set to 0, automatic dialing is performed immediately. <ul style="list-style-type: none"> ■ The valid range is 0 to 120. The default value is 15.
voip/dialing/auto_dialing/destination	Only displayed if the 'Activate' parameter is configured to Enable . Defines a number that will be automatically dialed when the phone is off-hooked. The valid value can be up to 32 characters.

3.4.5.3 Configuring Pause Dialing for a Speed Dial to an Ext. behind an IVR

Pause dialing can be configured for a Speed Dial to create a time break, typically required for a Speed Dial which dials a destination extension number that is behind an Interactive Voice Response (IVR) system. You can configure a dial string that includes ",", "p" or "P" which indicates a pause in the dial sequence.

This section shows how to configure pause dialing using the Configuration File.

To configure pause dialing:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-22: Pause Dialing

Parameter	Description
voip/services/pause_dialing/digit_duration	Defines the duration time for each pressed digit. Default: 100 [milliseconds].
voip/services/pause_dialing/digit_gap	Defines the duration time between two digits. Default: 300 [milliseconds].
voip/services/pause_dialing/pause_duration	Defines the time duration for each pause symbol. Default: 2 [seconds].

3.4.5.4 Configuring Default Audio Device

This section shows how to configure the Default Audio Device using Configuration File.

To select the default Audio Device:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-23: Default Audio Device Parameter

Parameter	Description
voip/answer_device	<p>Sets the default audio device to answer or initiate a new call when no explicit audio device is set.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ When pressing the Answer softkey. ■ When initiating a call by speed dial key, call history or phone directory. ■ Answering talk event or auto-answer. ■ When starting to dial in "on hook" mode. <p>Valid values are:</p> <ul style="list-style-type: none"> ■ [SPEAKER] (default) ■ [HEADSET]
voip/headset_only/enabled	<p>Lets you control audio device usage. Lets you enable headset only, and disable the phone hook and the SPEAKER button.</p> <ul style="list-style-type: none"> ■ [0] Headset only (default) ■ [1] Disables the phone hook and the SPEAKER button. Leaves the headset as the only possible audio device that can be used.

3.4.6 Enabling Direct Voice Dialing

Users can use the AudioCodes VocaNOM voice dialing service to *directly* voice dial other parties by vocalizing their name. Additionally, the phone numbers of parties who are voice-dialed are displayed in the the Call Log from where users can redial. The feature powers up efficiency in organizations, increases productivity and improves users' telephony experience. Users can configure a key which they can press and then vocalize the name of the party to whose number the VocaNOM service will directly dial.

To enable voice dialing:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-24: Enabling Voice Dialing

Parameter	Description
voip/services/vocanom_server/enabled	Enables or disables the method on user phones. [1] Enables the method 'Use VocaNOM server directly' [0] Disables the method 'Use VocaNOM server directly' (default)
voip/services/vocanom_server/ip_address	Defines the IP address of the VocaNOM server. Default: 0.0.0.0
voip/services/vocanom_server/port	Defines the port number on the VocaNOM server. Its value must match Transport Mode. <ul style="list-style-type: none"> ■ 5060 for UDP, TCP ■ 5061 for TLS
voip/services/vocanom/transport_mode	Defines the Transport Mode for sending SIP messages. <ul style="list-style-type: none"> ■ TLS ■ UDP ■ TCP
voip/services/vocanom/label	Defines the name of the key configured as VocaNOM displayed in the idle screen, and the name displayed in the screen that opens after pressing the key. Default: VocaNOM
voip/services/vocanom/number	Defines the number to dial to the VocaNOM server. Default: None



All parameters must be configured for the user's VocaNOM key to be activated.

3.4.7 Disabling the Phone Microphone

This section shows how to disable the phone's microphone, which by default is enabled. Enterprise's may require this restriction to enhance confidentiality in the organization. The feature can be disabled using the Configuration File.

To disable the microphone:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-25: Disable Microphone Parameter

Parameter	Description
voip/audio/microphone/enable	Enables/disables the phone's microphone functionality. <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)

3.4.8 Configuring the TRANSFER Key to Perform Consultative Transfer

The phone's hard TRANSFER key *by default* performs *blind transfer* but you can change the default for the key to perform *consultative transfer*.

You need to reconfigure the parameter 'voip/signalling/sip/hk_blind_transfer/enable' as shown in this section.

To change the TRANSFER key functionality:

- Use the table below as reference, and then click **Submit**.

Table 3-26: Changing TRANSFER Key Functionality

Parameter	Description
voip/signalling/sip/hk_blind_transfer/enable	Changes the hard TRANSFER key's functionality from performing blind transfer (default) to performing consultative transfer. <ul style="list-style-type: none"> ■ [0] TRANSFER hard key performs Consultative Transfer ■ [1] TRANSFER hard key performs Blind Transfer (default)

3.4.9 Enabling Semi-Consultative Transfer

You can enable semi-consultative transfer. The user will then be able to transfer the call after the party whom the caller requested to be transferred to, picks up the phone.

To enable semi-consultative transfer:

- Use the table below as reference, and then click **Submit**.

Table 3-27: Semi-Consultative Transfer Parameter

Parameter	Description
system/semi_attended/enable	<p>Enables semi-consultative transfer.</p> <ul style="list-style-type: none"> ■ [0] [Default] A asks B to transfer A to C. B puts A on hold, calls C, and waits until C answers. After C answers, B transfers the call from A. ■ [1] A calls C and presses the Trans softkey when A hears the ringback from C.

3.4.10 Disabling the BXfer (Blind Transfer) Softkey

This section shows how to disable the **BXfer** softkey displayed by default in the phone's screen during a call. If the network administrator disables the **BXfer** softkey, **Hold** will be displayed instead. The **BXfer** softkey gives users an alternative way to perform Blind Transfer (see the *User's Manual* for more information on call transfer).

To disable the **BXfer** softkey:

- Use the table below as reference, and then click **Submit**.

Table 3-28: Blind Transfer Softkey Parameter

Parameter	Description
voip/signalling/sip/sk_blind_transfer/enable	<p>Enables display / removes display of the BXfer softkey in the phone screen when in a call.</p> <ul style="list-style-type: none"> ■ [0] Removes display of the BXfer softkey when in a call; the Hold softkey is displayed instead. ■ [1] Enables display of the BXfer softkey when in a call (default).

3.4.11 Enabling Electronic Hook Switch

The phone supports the Electronic Hook Switch (EHS) DHSG feature. Calls can be answered and volume level can be changed with EHS-capable headsets. The feature is supported on the following headsets:

- Jabra® PRO 920
- Jabra® PRO 9450

The headset's base unit connects to the phone's headphone port. The Audio connector connects to the headphone's port. The management connector connects to the Auxiliary port using a DHSG cable which can be ordered from AudioCodes.

The feature can be enabled using the Configuration File. The feature allows users to handle calls, i.e., answer calls and change volume level, with EHS-capable wireless headsets at a distance from the phone.

To enable EHS:

- Configure the EHS parameter using the table below as reference.

Table 3-29: EHS Parameter

Parameter	Description
voip/services/electronic_hook_switch/enabled	<p>Enables the EHS DHSG-standard feature.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>DHSG (Drahtlose Hör-Sprechgarnitur) is the protocol used to convert a wireless headset's internal control signals to a commonly supported standard, and which uses the special AUX port.</p> <p>Supported wireless headsets can be connected to the AUX port (in addition to the regular headset port). This allows the user to connect and disconnect calls by pressing the button on the headset. See under Appendix B for information about supported wireless headsets.</p>

The base unit of the headset connects to the phone's headset port, i.e., to the same port that all headsets' base units connect to. The Audio connector must be connected to the headphones port. The management connector must be connected to the Auxiliary port using a DHSG-standard cable which can be ordered from AudioCodes.

3.4.12 Disabling Audial Call Waiting Indication

This section shows how to disable the audial call waiting indication (beep progress tone) so that only visual indication for call waiting occurs. Audial call waiting indication can interfere with a conversation. This feature addresses the issue. If a user is in a call and a third party calls that user, the called user's screen visually indicates that a calling party is waiting: the incoming call icon flashes, the adjacent Programmable Key LED flashes, and the blue Ring LED in the uppermost right corner of the device flashes (see the *User's Manual* for more information).

To disable Call Waiting audial indication:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-30: Call Waiting Audial Indication Parameter

Parameter	Description
voip/services/call_waiting/generate_tone/enabled	<p>Enables a call waiting audial indication (beep progress tone), which can interrupt a phone conversation.</p> <ul style="list-style-type: none"> ■ [0] Disabled. If disabled, only visual indication for call waiting occurs. Call waiting is visually indicated in the called party's phone screen. If a user is in a call and a third party calls that user, the called user's screen visually indicates that a calling party is waiting. ■ [1] Enabled (default)

3.4.13 Disabling Call Forward

By default, the call forward feature is enabled on all users' phones unless the phone is configured as a CAP, but the network administrator can disable the feature on phones if enterprise policy, for example, requires this.

To disable the call forward feature:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-31: Call Forward Parameter

Parameter	Description
voip/line/0/call_forward/enabled	<p>Configure either.</p> <ul style="list-style-type: none"> ■ [0] The call forward feature will be disabled and the Forward softkey won't be displayed in the phone screen. ■ [1] (Default) The call forward feature will be enabled and the Forward softkey will be displayed in the phone screen.

3.4.14 Configuring Busy on Busy

The phone signals a 'Busy Here' message when the end user who is being called has an active Skype for Business call (an active call using the phone or any other client the user is logged in with).

To configure Busy on Busy:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-32: Call Forward Parameter

Parameter	Description
voip/services/call_waiting/mode	Configure either. <ul style="list-style-type: none"> ■ [DISABLE] The call waiting feature will be disabled ■ [ENABLE] (Default) The call waiting feature will be enabled ■ [BUSY_ON_BUSY] If you're already in an active call on either the conference phone or Skype for Business client and a call comes in, the Busy on Busy feature rejects the coming call and plays a busy signal to the caller.

3.4.15 Configuring Disconnect if Handset On-Hooked after Putting Call on Hold

This section describes how to configure the phone so that when using the handset in a call, if the call is put on hold and the handset is then on-hooked, audio switches to the speaker and the call is *not* disconnected.

To maintain backward compatibility, users can set the ini file parameter 'voip/onhook_disconnect_when_held/enabled' to **1**. This causes the call to be *disconnected* in the above scenario, as it was in earlier versions.

To configure this:

- Use the table below as reference.

Table 3-33: Disconnect if Handset On-Hooked after Call Put on Hold

Parameter	Description
voip/onhook_disconnect_when_held/enabled	When using the handset in a call, if the handset is on-hooked after putting the call on hold, the call is not disconnected and the audio is switched to the speaker. To maintain backward compatibility, users can set 'voip/onhook_disconnect_when_held/enabled' to 1 . This causes the call to be disconnected in the above scenario, as it was in earlier versions. <ul style="list-style-type: none"> ■ [0] Disable (default). When using the handset in a call, if the handset is on-hooked after putting the call on hold, the call is not disconnected and the audio is switched to the speaker. ■ [1] Enable. When using the handset in a call, if the handset is on-hooked after putting the call on hold, the call is disconnected.

3.4.16 Configuring Media Streaming

This section describes configuring the Media Streaming parameters. Only the parameters documented in this section are applicable.

3.4.16.1 Configuring Quality of Service

This section shows how to configure Quality of Service (QoS) using the Configuration File.

To configure QoS:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-34: QoS Parameters

Parameter	Description
voip/media/media_tos	<p>Defines DS (Differentiated Services) containing a DSCP (Differentiated Services Code Point) value and an ECN (Explicit Congestion Notification) value.</p> <p>DSCP is backwards compatible with ToS. ECN is not.</p> <p>QoS in hexadecimal format, TOS is part of the IP header that defines the type of routing service to tag outgoing voice packets originated from the phone. It informs routers that this packet must receive a specific QoS. Values can be set in decimal (e.g., 184) or hexadecimal (e.g., 0xb8). The default value is 0xb8 (184).</p> <pre> 0 1 2 3 4 5 6 7 +---+---+---+---+---+---+---+---+ DS FIELD, DSCP ECN FIELD +---+---+---+---+---+---+---+---+ DSCP: differentiated services codepoint ECN: Explicit Congestion Notification </pre> <p>The network administrator must therefore take into account the two LSBs that are reserved for ECN, when setting the desired value for DSCP, e.g., for a DSCP value of 46 (EF), the proper value for this parameter should be 184 in decimal, or 0xb8 in HEX, which corresponds to '10111000'. For a DSCP value of 22 (AF23), this parameter should be set to 88 decimal or 0x85 in HEX ('01011000'). See RFC 3168 for detailed information.</p>

3.4.16.2 Configuring Codecs

This section shows how to configure codecs using the Configuration File.

To define the codecs:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-35: Codec Parameters

Parameter	Description
voip/codec/codec_info/%d/enabled	<p>Determines the codecs that you want to implement and their priority. Up to five codecs can be configured, where the first codec (i.e., voip/codec/0/...) has the highest priority. To make a call, at least one codec must be configured. In addition, for best performance it is recommended to select as many codecs as possible.</p> <p>When you start a call to a remote party, your available codecs are compared with the remote party's to determine the codec to use. If there is no codec that both parties have made available, the call attempt fails. Note that if more than one codec is common to both parties, you cannot force which of the common codecs are used by the remote party's client. To force the use of a specific codec, configure the list with only that specific codec.</p> <p>The <i>%d</i> variable stands for the priority:</p> <ul style="list-style-type: none"> ■ [0] - Disabled ■ [1] (default) - Enabled
voip/codec/codec_info /%d/name	<p>Name of the codec. The variable <i>%d</i> depicts the index number of the codec entry and its priority, where the first codec (i.e. voip/codec/codec_info/0/name=...) has the highest priority. The valid codec parameters are:</p> <ul style="list-style-type: none"> ■ [SILK_8000 / SILK_16000] Skype's audio compression format and audio codec that can use a sampling frequency of 8, 12, 16 or 24 kHz and a bit rate from 6 to 40 Kbit/s. <ul style="list-style-type: none"> • Compatible with Skype for Business • Flexible bit rate • High quality • Variety of sampling frequencies • Inband FEC and good resilience to packet loss <p>Note: G.722 was the first priority vocoder in version releases prior to 3.0. When upgrading from releases prior to 3.0, the list of vocoders remains unchanged. To set the SILK to be the priority vocoder (inapplicable to the 445HD), restore the phone to its defaults or set the vocoder list differently so that SILK is added. This can be done manually or by provisioning.</p> <ul style="list-style-type: none"> ■ [G722] G.722 (default) ■ [PCMA] G.711 A-Law ■ [PCMU] G.711 Mu-Law ■ [G729] G.729 <p>For example, voip/codec/codec_info/0/name=G722.</p> <p>Note: Specific codecs require specific firmware files. For more information, refer to the <i>Release Notes</i>.</p>

Parameter	Description
voip/codec/codec_info /%d/ptime	Length of the digital voice segment that each packet holds. The default is 20 millisecond packets, excluding G.723 which is 30 millisecond packets.
voip/codec/g723_bitrate	Low or high bit rate for G.723. <ul style="list-style-type: none"> ■ [LOW] Low ■ [HIGH] High (default)
voip/codec/g722_bitrate	G.722 bit rate. <ul style="list-style-type: none"> ■ [G722_64K] (default) ■ [G722_56K] ■ [G722_48K] <p>Note: Currently, only 64bps is supported.</p>
<ul style="list-style-type: none"> ■ [system/activation_keys/amr_coder 	Activation key (string) required to unlock AMR coder (relevant for supporting firmware only).

3.4.16.3 Configuring Real Time Protocol (RTP) Port Range

This section shows how to configure the RTP port range.

To configure the RTP port range:

- Configure using the table below as reference, and then click **Submit**.

Table 3-36: Media Streaming - RTP Port Range

Parameter	Description
voip/media/media_port	Defines the base port for the range of RTP ports which the enterprise network administrator must open on the network's firewall. Default: 4000 Valid possible ports: If, for example, 6000 is selected as base port, the valid possible ports will be 6000-60120.

3.4.16.4 Configuring RTCP Extended Report

This section shows how to configure Extended Report for RTP Control Protocol (RTCP-XR) working mode.

To configure RTCP_XR:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-37: RTCP_XR Parameter

Parameter	Description
voip/rtcp_xr/vq_statistics/mode	<p>Sets RTCP_XR working mode. Select either:</p> <ul style="list-style-type: none"> ■ [DISABLE] (default). In this state, no RTCP-XR events are retrieved from the phone and the SIP PUBLISH is not sent, regardless of the state of parameter 'qoe_publish_enabled' (see below). ■ [EVENTS_ONLY]. In this state, RTCP-XR events with voice quality parameter calculations are sent internally on the phone every five seconds. Each calculation is made on the basis of these RFC 3611 parameters: BT=7, block length = 8SSRC of source, loss rate, discard rate, burst density, gap density, burst duration, gap duration, round trip delay, end system delay, signal level, noise level, Gmin, R factor, ext. R factor, MOS-LQ, MOS-CQ, RX config, JB nominal, JB maximum and JB abs max. The phone sends the summarized RTCP-XR events to the Skype for Business server / EMS via SIP SERVICE messages (in Genesis-SIP, SIP PUBLISH messages are used). ■ [REMOTE_AND_EVENTS]. In this state, the phone sends RTCP-XR events to the remote calling party (i.e. party A sends these events to party B) every five seconds during the VoIP session. The phone sends the summarized RTCP-XR events to the Skype for Business server / EMS via SIP SERVICE messages (in Genesis-SIP, SIP PUBLISH messages are used).

3.4.16.5 Configuring Media Bypass

Media bypass allows a phone to send media directly to the SBC or PSTN gateway, eliminating the Cloud Connector Edition (CCE) from the media path when possible, thereby reducing latency, the possibility of packet loss and the number of points of potential failure, and thereby improving voice quality.

The feature is only applicable:

- to Skype for Business online phones with one or more CCEs interconnected to SBCs or to gateways
- if enabled by inband provisioning parameter
- if the phone receives a valid bypassID from a CCE Web service
- to phones connected to CCE over an internal IP network [External phones do not have access to the CCE Web service – they're unable to connect to the media bypass service URL - so they cannot use media bypass and instead send media to the SBC / PSTN gateway through CCE Edge and Mediation servers]

Identical to media bypass for *on-premises phones* (already supported), except that bypassID is acquired by sending an HTTP request to the CCE URL instead of getting it from inband provisioning for on-premises accounts.

The feature is enabled by two inband provisioning parameters:

- VoiceDeploymentMode
 - <property name="VoiceDeploymentMode">OnPremOnlineHybrid
- HybridConfigServiceInternalURL
 - <hybridConfigServiceInternalURL>http://ccetestlab.info.cce.local/hybridconfig/hybridconfigservice.svc

The phone uses the feature only if 'VoiceDeploymentMode' is set to **OnPremOnlineHybrid**. The phone sends an HTTP GET request to the provided 'hybridConfigServiceInternalURL' and receives a 200OK HTTP response with the bypass' settings xml body containing the following parameters:

- bypassEnabled="true" or "false"
- internalBypassMode="Any" or "off"
- externalBypassMode="Any" or "off"
- bypassID="2cd1a522-b9c5-4410-8aed-f3eca85eb367"

The phone proceeds with media bypass only if

- bypassEnabled="true"
- one of the bypass modes equals "any"
- the bypassID is provided

The phone sends an HTTP GET request to get the media bypass properties once every eight hours, each time it receives the inband provisioning parameters.

3.4.17 Enabling Paging

This feature allows a live announcement to be made (paged) from a phone to a group of phones, to notify a team (for example) that a meeting is about to commence at a certain venue.

All Function Keys can be configured for paging, allowing the user to page multiple paging groups.



Applies to all phones. Does not apply to the HRS.

The paged announcement is multicast via a designated group IP address, in real time, on all idle phones in the group, without requiring listeners to pick up their receivers. The name of the group is displayed on phone screens when the paging call comes in. If the Barge-in feature (see the next section) is disabled (default), recipients of the paging call who are in calls can choose to reject it.

To enable Paging:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-38: Paging Parameters

Parameter	Description
voip/services/group_paging/codec	Sets the required codec. All the codecs used for regular calls can be used for paging. See Section 3.4.16.2 for supported codecs. Default: G722_8000.
voip/services/group_paging/enabled	Enables or disables the paging feature. <ul style="list-style-type: none"> ■ [0] = Disabled [Default] ■ [1] = Enabled
voip/services/group_paging/end_income_paging_timeout	Sets the timeout, i.e., how many milliseconds must pass after receipt of RTP ends, before paging times out. Default: 800 milliseconds (8 seconds).
voip/services/group_paging/group/n-n/activated	Activates or deactivates for the pager and the paged parties a Speed Dial configured as a paging key. <ul style="list-style-type: none"> ■ [0] = Deactivated [Default]. Paging was deactivated for the key configured as paging dial, so the key will be a regular speed dial. ■ [1] = Activated. Paging was activated for the key configured as paging dial. Note: n-n are the Functional Keys indexed in the Configuration File.
voip/services/group_paging/group/n-n/multicast_addr	Applies only if 'Key Type' is configured as PAGING . Enter the paging group's multicast IP address. Default = 224.0.1.0. For phones to be in a group, all must be configured with the same multicast address. Note: n-n are the Functional Keys indexed in the Configuration File.

Parameter	Description
voip/services/group_paging/group/n-n /name	Defines the name of the group displayed in the phone's screen when there's an incoming paging call; the label defined in the Speed Dial or Programmable Key is also displayed. For phones to be in a group, all must be configured with the same name. Note: n-n are the Functional Keys indexed in the Configuration File.
voip/services/group_paging/group/n-n /port	Enter the group's port. Default: 8888. For phones to be in a group, all must be configured with the same port.

After enabling Paging, you can add each phone you want to include in the paging group (see the *User's Manual* for detailed configuration information).

3.4.18 Enabling Barge-in

This feature when enabled allows paging calls to interrupt (barge in on) phone conversations that are in progress, without prompting recipients with an option to accept or reject the paging call.

When disabled (default), those who are in regular calls when the paging call comes in are prompted in their phones' screens to choose whether or not to accept or reject the paging call. If it's accepted, the regular call will be put on hold and the paging call will be heard.

To enable Barge-in:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-39: Paging – Allow Barge In

Parameter	Description
voip/services/group_paging/allow_barge_in/enabled	Lets incoming paging calls interrupt (barge in on) regular calls that are in progress. <ul style="list-style-type: none"> ■ [0] = [Default] Those in regular calls are prompted whether or not to accept an incoming paging call. ■ [1] = Incoming paging calls interrupt (barge in on) regular calls that are in progress.

3.4.19 Configuring the VocaNOM Service

VocaNOM allows users to voice-dial colleagues by articulating the full name of a colleague adding "Office" or "Mobile" when prompted. The solution then dials the requested party. The feature increases day-to-day work productivity.

For information on how to enable or disable the feature, see Section 3.4.6.



Applies to the 445HD, 450HD, 450HD and Expansion Module, C450HD, C450HD and Expansion Module, as well as to the RX50 conference phone.

To configure the VocaNOM service:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-40: Voice-Dialing Parameter Descriptions

Parameter	Description
voip/services/vocanom/number	Defines the number that the phone dials to access the VocaNOM server, either directly, or indirectly, via the Skype for Business server. Example: 7777
voip/services/vocanom/label	Defines the name that will be displayed in phone screens after users press their configured VocaNOM key to voice-dial another party using the VocaNOM service. Default: VocaNOM
voip/services/vocanom_server/enabled	Can be enabled or disabled. The user's experience remains the same whether enabled (direct voice dialing) or disabled (indirect voice dialing). Direct or indirect voice dialing occurs in the background, so user experience is unaffected. When enabled (direct voice dialing), the call is forwarded directly to the server. When disabled (indirect voice dialing), the call is forwarded via the Skype for Business server. The VocaNOM server can be on premises or in the cloud. <ul style="list-style-type: none"> ■ [0] Access to the VocaNOM server is indirect via the Skype for Business server [default] ■ [1] Access to the VocaNOM server is direct
voip/services/vocanom_server/ip_address	Only displayed in the Web interface if the previous parameter (above) is enabled. Defines the VocaNOM server's IP address. The server can be either in the AWS cloud (Amazon Web Services) or on premises. Default: 0.0.0.0
voip/services/vocanom_server/port	Defines the port number on the VocaNOM server. Its value must match Transport Mode. <ul style="list-style-type: none"> ■ 5060 [for UDP, TCP] ■ 5061 [default] [for TLS]
voip/services/vocanom/transport_mode	Defines the Transport Mode for sending SIP messages. <ul style="list-style-type: none"> ■ TLS [Default] ■ UDP ■ TCP

3.4.20 Configuring a Dedicated Voicemail Server

This section shows how to configure a dedicated voicemail server for the enterprise, as an alternative option to Microsoft Exchange Server.

To configure a dedicated voicemail server:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-41: Dedicated Voicemail Server - Parameters

Parameter	Description
voip/services/msg_waiting_ind/voice_mail_number	Enter the number of the service to dial in order to retrieve voicemail.
voip/services/msg_waiting_ind/enabled	Configure either: <ul style="list-style-type: none"> ■ [0] Disabled if a voicemail service isn't required. ■ [1] Enabled (default) in order to use Microsoft Exchange Server for voicemail. ■ AUDC_VM in order to use a dedicated voicemail server other than Microsoft Exchange Server for voicemail.
voip/services/msg_waiting_ind/subscribe	<ul style="list-style-type: none"> ■ [0] Disabled (default) configure this option if you chose in the previous parameter to use Microsoft Exchange Server for voicemail. ■ [1] Enabled configure this option if you chose in the previous parameter to use a dedicated voicemail server, other than Microsoft Exchange Server, for voicemail.
voip/services/msg_waiting_ind/subscribe_address	Enter the IP address of the AudioCodes gateway or PBX on which the voicemail application is located.
voip/services/msg_waiting_ind/subscribe_port	Enter the port number of the AudioCodes gateway or PBX on which the voicemail application is located. Default: 5060.
voip/services/msg_waiting_ind/expiration_timeout	Defines how often the voicemail application is updated (refreshed) for new mail. Default: Every 3600 seconds (i.e., every hour).

3.4.21 Securing Voicemail Access by PIN Code Authentication

Network administrators can secure user access to voicemail with PIN code authentication so that when users press the voicemail button, they're prompted to enter their PIN code.

By default, the phone skips PIN code authentication and allows users direct access to voicemail.

To secure voicemail access:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-42: Securing Voicemail Access by PIN Code Authentication Parameter

Parameter	Description
voip/services/vm_skip_pin_code/enabled	Configure: <ul style="list-style-type: none"> ■ [0] Disable to secure user access to voicemail with PIN code authentication so that when users press the voicemail button, they're prompted to enter their PIN code. ■ [1] Enable (default) for the phone to skip PIN code authentication and allow the user direct access to voicemail.

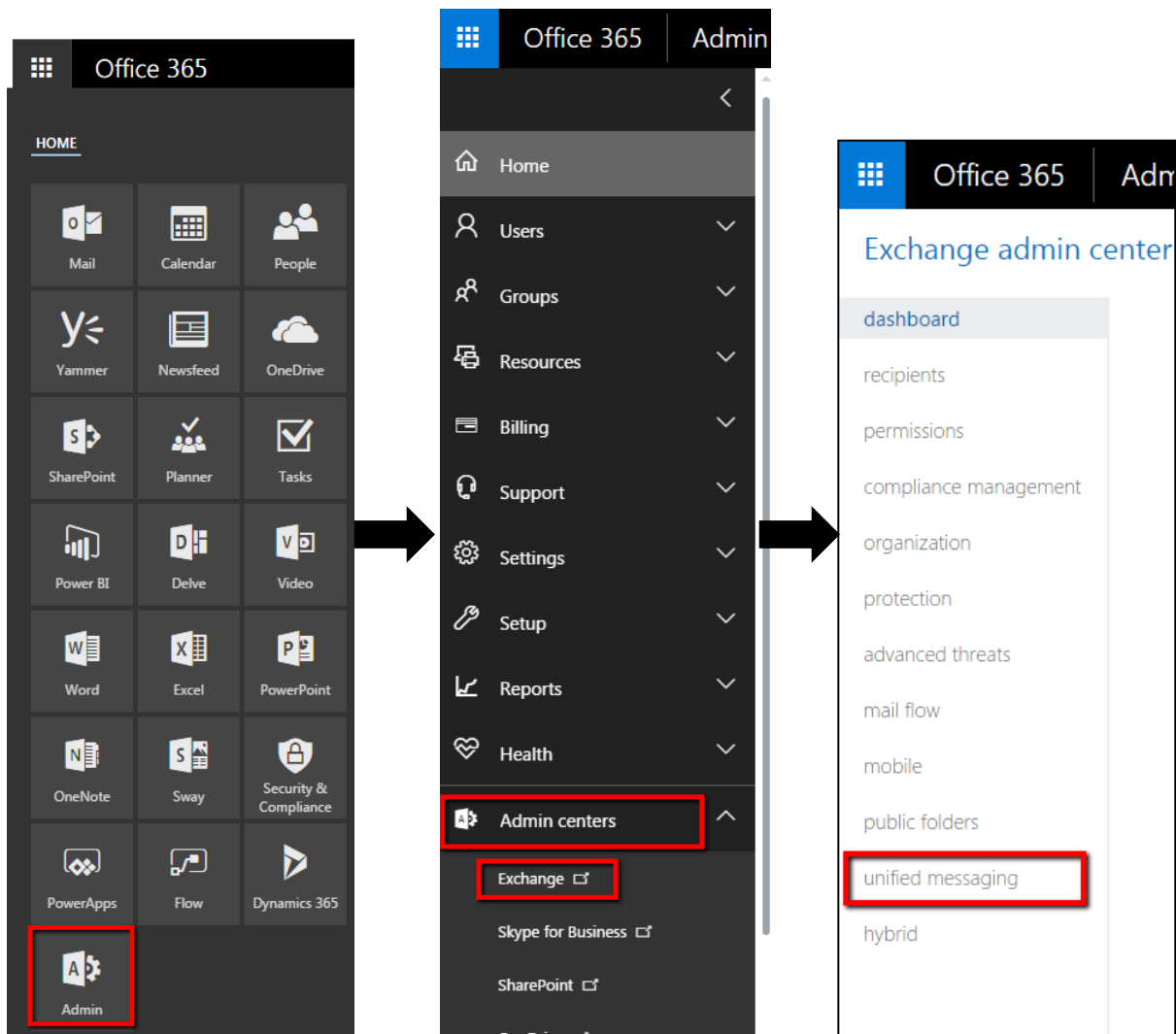
3.4.22 Setting up a Cloud User's Voicemail / MWI

This section shows how to set up a cloud (online) user's Voicemail / MWI (Message Waiting Indication). To set up a cloud user's Voicemail / MWI you need to configure their related cloud server settings. MWI configuration information is part of the SELF SUBSCRIBE/NOTIFY when the content type is **vnd-microsoft-roaming-self+xml**. The tokens in the XML message are **unreadVoiceMailCount** and **readVoiceMailCount**.

To set up a cloud user's Voicemail / MWI:

1. In the Microsoft Office 365 server GUI, navigate to the 'Exchange Admin Center - Unified Messaging' screen as shown in the figure below (**Home** > **Admin** > **Admin Centers** > **Exchange** > **Unified Messaging**).

Figure 3-2: Exchange Admin Center - Unified Messaging

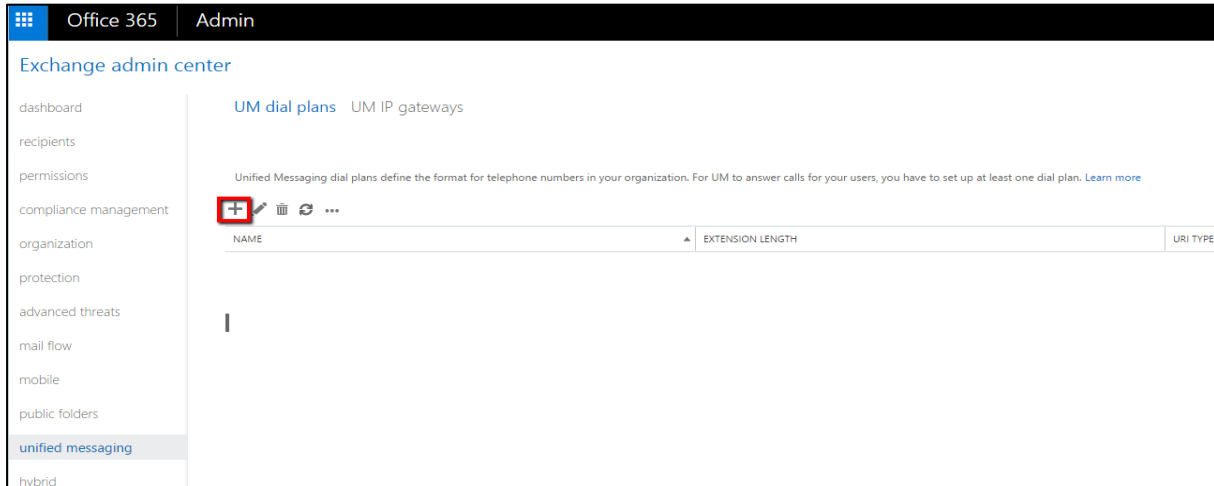


2. In the Exchange Admin Center – Unified Messaging screen (see the figure below), click the + icon to set up a dial plan.



You need to define a new dial plan for voicemail before performing the procedure below. The default dial plan must not be used.

Figure 3-3: Setting up a Dial Plan

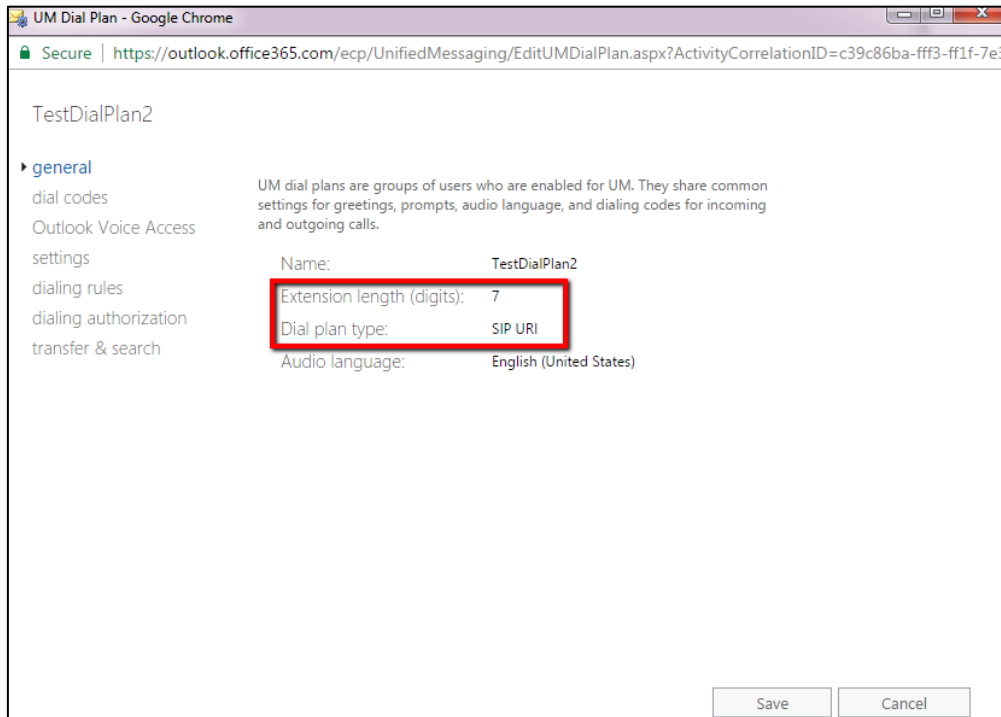


3. Set up the new Dial Plan with URI TYPE = SIP URI, as shown in the figure below.

Figure 3-4: New Dial Plan: URI Type = SIP URI

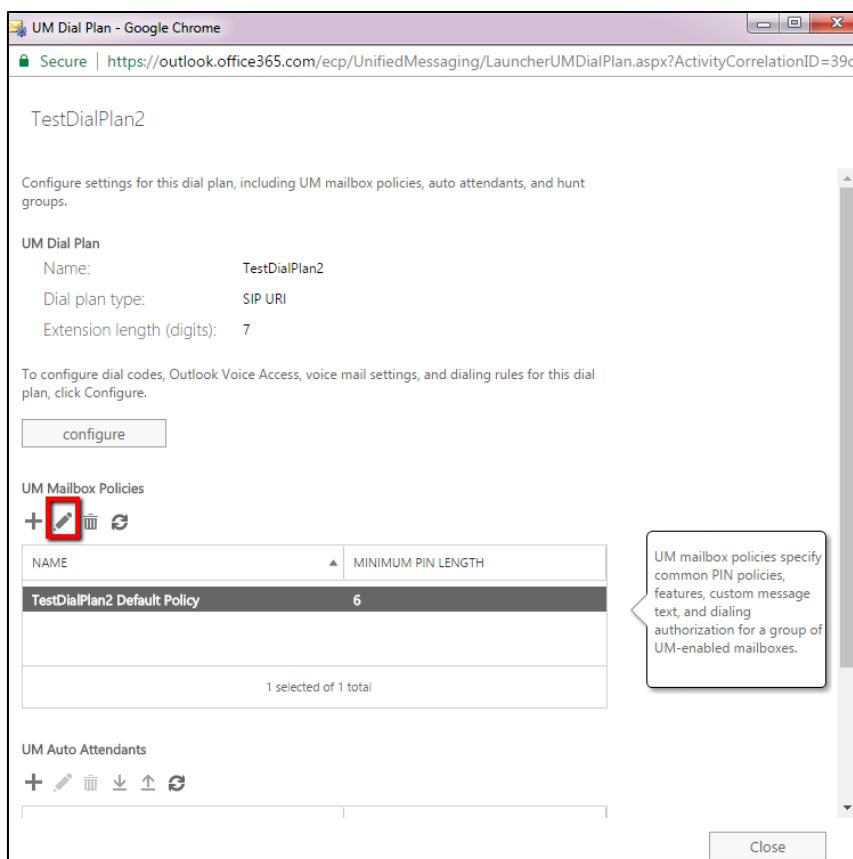
4. Click **Save**.

Figure 3-5: Dial Plan: Rules and Settings



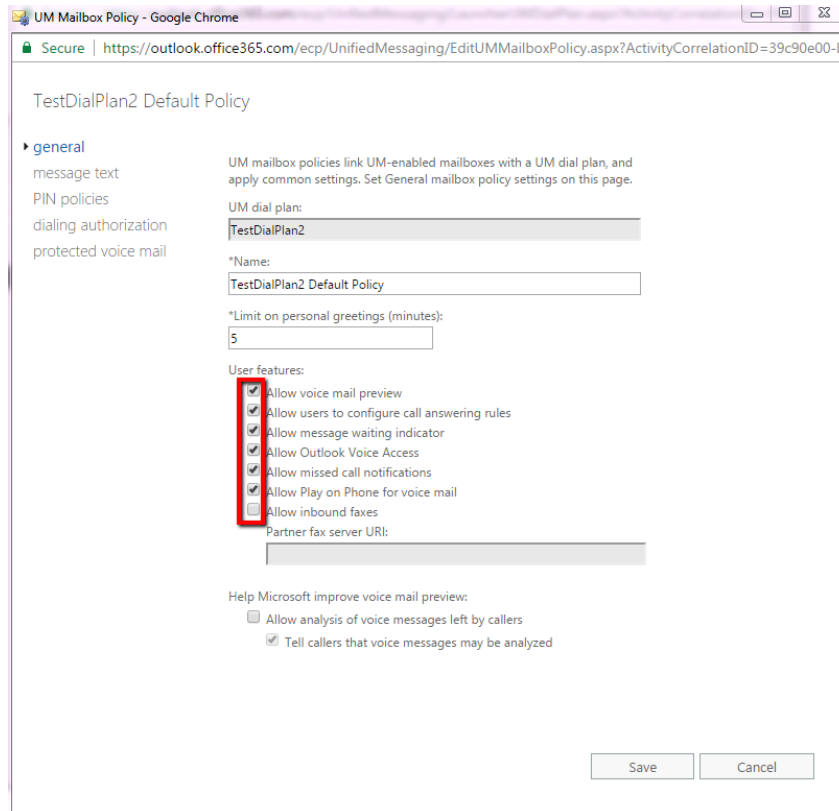
5. After setting up the UM Mailbox Policy, click the **Edit** icon shown in the figure below.

Figure 3-6: Edit



6. Make sure the MWI option is selected.

Figure 3-7: Enabling UM for Users



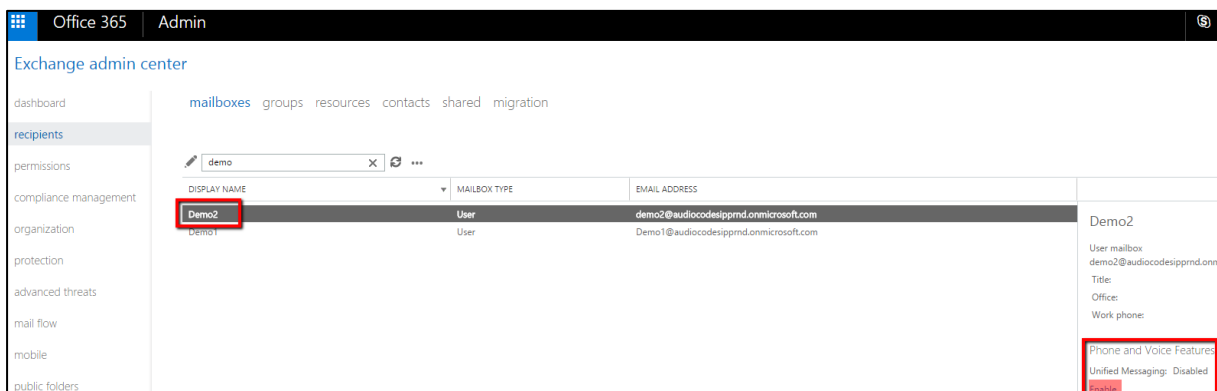
3.4.22.1 Enabling Unified Messaging

This section shows how to enable UM for the user.

To enable UM:

1. Connect with Admin user to the online server.
2. Access the **Admin** screen.
3. Navigate to **Admin centers** and select **Exchange**.
4. In the navigation pane on the left, select **Recipients** and under the **mailboxes** tab, search for the user.
5. Under 'Phone and Voice Features' in the pane on the right, click **Enable**.

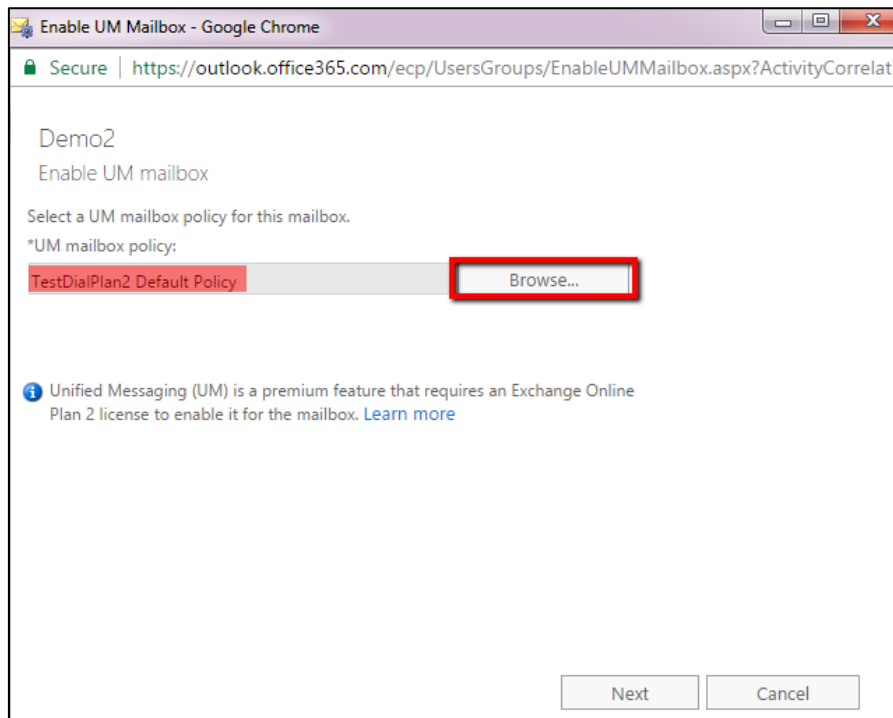
Figure 3-8: Enabling UM



6. Click **Browse** as shown in the figure below, to browse to and select the UM Dial Plan you set

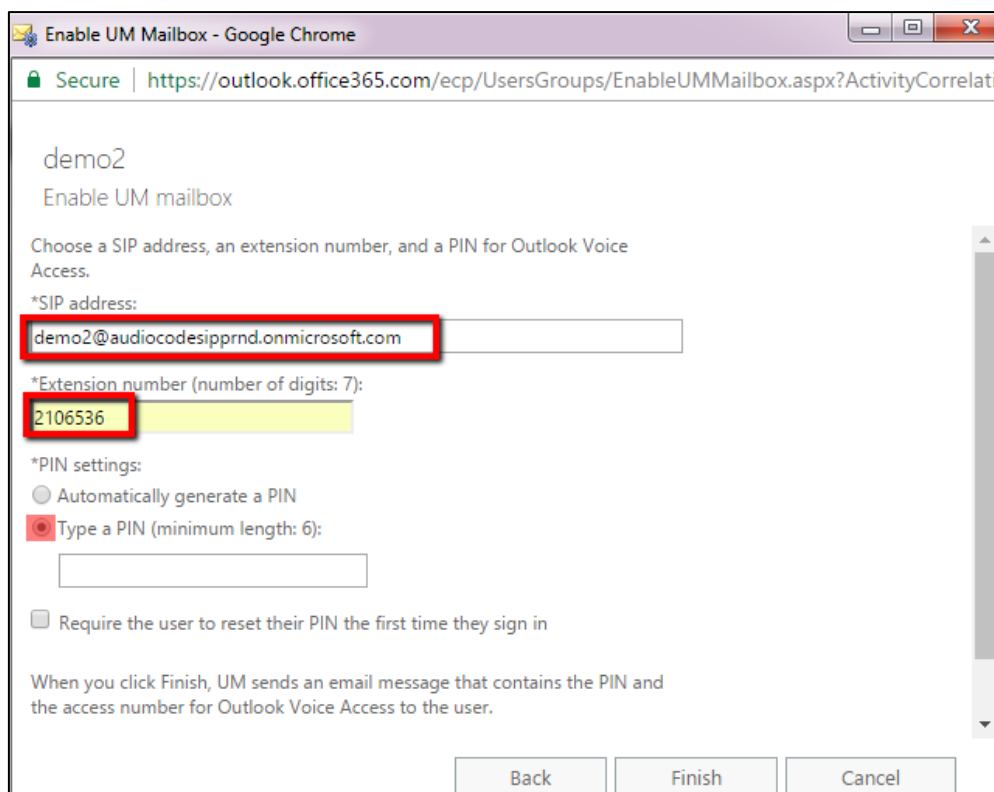
up previously.

Figure 3-9: Browse to the UM Dial Plan



7. Click **Next** and enter the user's SIP address and/or Extension Number, and enter the PIN if the checkbox is selected.

Figure 3-10: User's SIP Address and/or Extension Number, and PIN

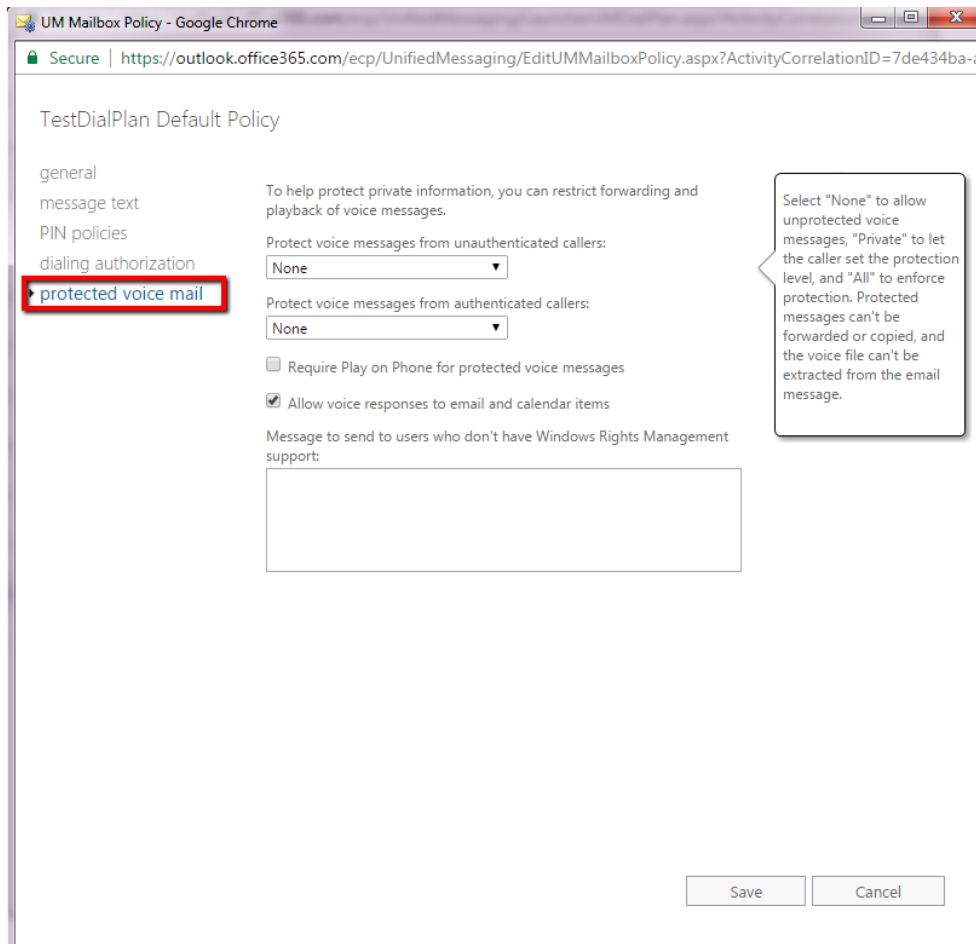


8. After the user is enabled and configured with a UM Dial Plan for VoiceMail indicator, the phone must be rebooted - or signed out and then signed back in again.

3.4.22.2 Troubleshooting

Use the figure below as a reference when troubleshooting issues related to setting up a cloud user's voice mail / MWI.

Figure 3-11: Troubleshooting – Protected Voice Mail



3.5 Configuring Security

3.5.1 Using the Encryption Tool

AudioCodes' IP phones use the Triple Data Encryption Standard (3DES) algorithm for encryption. This section shows how to use the encryption tool.

3.5.1.1 Encrypting Configuration Files

This section shows how to encrypt the configuration file when, for example, it is sent over an unsecure network.

To encrypt the configuration file:

- At the command line prompt, specify the following:

```
encryption_tool.exe -f <filename>.cfg
```

where *<file name>.cfg* specifies the name of the Configuration file that you wish to encrypt.

Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

3.5.2 Encrypting Passwords in Configuration File

This section shows how to encrypt IP phone passwords used in the configuration process, for example, the 'System' password and the 'SIP Authentication' password.

To encrypt passwords:

1. At the command line prompt, specify the following:

```
encryption_tool.exe -s <password_string>
```

where *<password_string>* specifies the string of the password that you wish to encrypt.

Once the password is encrypted, a string is generated with the following syntax:

```
{"<encrypted_string>"}
```

For example:

```
{"0qrNRpSJ6aE="}
```

2. Copy the generated string (including the {" "}) with the syntax specified above to the relevant parameter in the Configuration File.

For example, if you encrypted the SIP authentication password, the following is displayed in the relevant line in the configuration file:

```
voip/line/0/auth_password={"0qrNRpSJ6aE="}
```



It is recommended to encrypt the System password using this procedure. If you choose not to do so, then the System password is by default encrypted using MD5.

3.5.3 Managing Security Certificates

AudioCodes IP phones are loaded with factory-set preinstalled certificate files: private key file, certificate file and a Trusted Root CA file that is signed by AudioCodes.

Whenever the IP phone authenticates with a remote server, it can be authenticated using these certificate files. Each IP phone receives a uniquely generated private key certificate file based on its MAC address. If the remote server is configured to authenticate the client and AudioCodes factory-set certificates are used for authentication, then the AudioCodes Certificate and AudioCodes Trusted Root CA must be downloaded to the remote server. These files can be downloaded from the AudioCodes Web site. For more information, contact your local AudioCodes sales representative. If you use the AudioCodes Redirect server to obtain firmware and configuration files, then the factory-set certificates are used to authenticate the connection with this server. If default certificate files are missing or deleted, the phone will regenerate these files automatically the next time it is powered up.

3.5.3.1 Loading the Root CA Certificate to the Phone

The section shows how to load the root CA certificate to the phone. The certificate enables signing in with 802.1x Authentication. With Microsoft Skype for Business, more than one certificate file is loaded automatically using DHCP Option 43.

To load the root CA certificate to the phone:

- Use the table below as reference.

Table 3-43: Root CA Certificate Parameters

Parameter	Description
security/ca_certificate/0/uri=	The first root CA certificate loaded to the phone.
security/ca_certificate/1/uri=	The second root CA certificate loaded to the phone.
security/ca_certificate/2/uri=	The third root CA certificate loaded to the phone.
security/ca_certificate/3/uri=	The fourth root CA certificate loaded to the phone.
security/ca_certificate/4/uri=	The fifth root CA certificate loaded to the phone.

3.5.3.2 Loading the Client Certificate to the Phone

The section shows how to load the Client Certificate to the phone.

To load the root CA certificate to the phone:

- Refer to the table below. You can also load the file/s to the phone using the Configuration File.

Table 3-44: Client Certificate Parameters

Parameter	Description
security/sip_certificate_uri	Downloads to the phone from this URI a Client Certificate for SIP TLS (SIP calls with Transport Layer Security).
security/sip_private_key_uri	Downloads to the phone from this URI a Client Private Key for SIP TLS (SIP calls with Transport Layer Security).
security/ieee802_1x_certificate_uri	Downloads to the phone from this URI a Client Certificate for 802.1X Authentication.
security/ieee802_1x_private_key_uri	Downloads to the phone from this URI a Client Private Key for 802.1X authentication. The certificate must be in .pem format.
security/autoupdate_certificate_uri	Downloads to the phone from this URI an external certificate that is used to secure the connection with the automatic provisioning server.
security/autoupdate_private_key_uri	Downloads to the phone from this URI a private key that is used to secure the connection with the automatic provisioning server.

3.5.3.3 Enabling Server-side Authentication (Mutual Authentication)

You can enable server-side authentication of a connection with the RADIUS / LDAP and Provisioning server.



OpenSSL 1.0.1m is supported. This open source version supports SHA2 algorithms.

Table 3-45: Server-side Authentication

Parameter	Description
security/ieee802_1x/verify_server_certificate	Configures the phone to verify received server certificates over a secure EAP-TLS connection.
security/provisioning/verify_server_certificate	Configures the phone to verify received server certificates over a secure HTTPS connection with a provisioning server.
security/ldap/RootCAoverLDAP	Controls whether or not use LDAP to search for a certificate. Valid values (bool): <ul style="list-style-type: none"> ■ 0 [LDAP will not be used to search for a certificate] ■ 1 (default) [LDAP will be used to search for a certificate]
system/ldap/TLMode	Defines the connection with the LDAP server. Valid values are: <ul style="list-style-type: none"> ■ NONE - Defines an unencrypted connection with the LDAP server (port 389 is used by default) ■ StartTLS (Default) - Defines a TLS/SSL connection with the LDAP server (port 389 is used by default) ■ OverTLS - Defines a TLS/SSL connection with the LDAP server (port 636 is used by default)

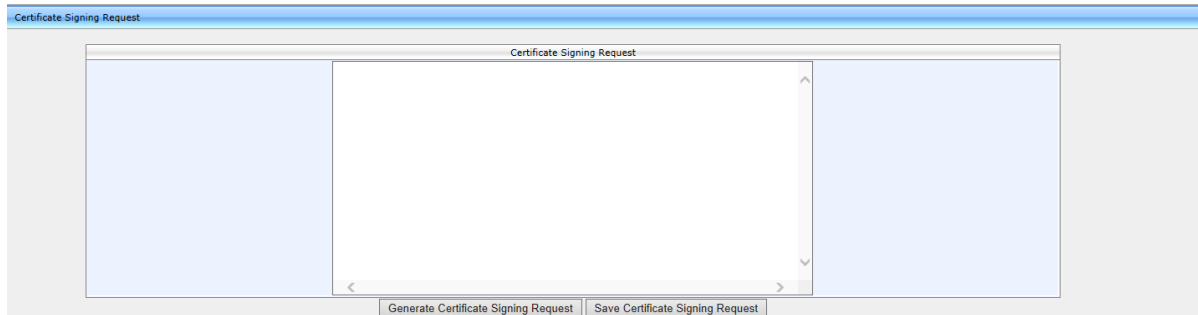
3.5.3.4 Generating a Certificate Signing Request

The section shows how to generate a certificate signing request (CSR) to send to the Certificate Authority (CA) for the CA to sign the Client Certificate.

To generate a CSR:

1. Open the Certificate Signing Request page (**Configuration** tab > **Security** menu > **Certificate Signing Request**).

Figure 3-12: Web Interface – Certificate Signing Request



2. Click **Generate Certificate Signing Request**; the phone creates a CSR file.
3. Click **Save Certificate Signing Request** and download the CSR file to your PC.
4. Send the CSR file to the Certificate Authority to sign the Client Certificate.
5. You can load the Client Certificate to the phone for 802.1X Authentication or SIP TLS.

3.5.4 Server Certificate Validation for Secured HTTPS Communications over SSL

This feature decreases vulnerability to breaches of security. If validation fails after installing phone firmware, HTTPS communication with Skype for Business and EWS servers are impacted, including but not restricted to Skype for Business auto-discover, contacts search, EWS auto-discover, Outlook Calendar, Authorization, etc.

The certificate is verified in two steps:

- The Root CA is installed using DHCP option 43, LDAP or the Web interface.
- The server's hostname is validated; for each certificate in the chain, the 'issuer' field in the certificate must match the 'subject' field of the issuer (uppermost in the chain) certificate.

To configure the feature:

- Use the table as reference.

Table 3-46: Server Certificate Validation for Secured HTTPS Communications over SSL

Parameter Name	Description
security/SSLCertificateErrorsMode	<ul style="list-style-type: none"> • Disallow (default) = TLS connection will be rejected and the phone will not communicate with the server. • Ignore = Allows backward compatibility though vulnerability will increase; the phone will proceed without checking the received certificates and without any notifications.

3.5.5 Configuring 802.1X Authentication

802.1X Authentication is an IEEE Standard for port-based Network Access Control (PNAC). It's part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices joining a LAN or WLAN.

The employee's PC negotiates 802.1X. Messages are sent transparent to the enterprise switch. The IP phone is uninvolved in the negotiation, but if an employee's PC is disconnected, their IP phone notifies the switch. If an employee's PC is disconnected from the IP phone, a PROXY-EAP-LOGOFF mechanism lets the IP phone immediately log off the port from the authentication server in order to not let anyone else connect to it.

The phone performs like this:

- IP phone and PC connected to IP phone's PC port successfully perform 802.1X authentication. The authentication server records the IP phone and PC as authorized.
- If the PC is disconnected from IP phone's PC port, the phone sends an EAPoL-Logoff message for the PC. The authentication server then records the PC as unauthorized.
- If the PC reconnects to the IP phone's PC port, the authentication server requests the PC to perform 802.1X authentication again.

3.5.5.1 Using the Phone Screen

This section shows how to configure 802.1X from the phone screen.

To configure 802.1X:

1. Open the 802.1X Settings screen (MENU key > **Administration** > **Network Settings** > **802.1X Settings**).
2. Navigate to and select either:
 - **Disabled** – disables the 802.1X feature
 - **EAP-MD5** – see Section 3.5.5.2
 - **EAP-TLS** - see Section 3.5.5.3

3.5.5.2 EAP MD5 Mode

This section shows how to configure EAP (Extensible Authentication Protocol) MD5 mode for 802.1X Authentication.

To configure EAP MD5 mode for 802.1X:

1. Navigate to the **EAP-MD5** option and press the **Edit** softkey:
2. Enter this information:
 - **Identity:** User ID
 - **Password:** MD5 password (optional)
3. Press the **Save** softkey; a message appears notifying you that the phone will restart.
4. Press **Apply**.

3.5.5.3 EAP TLS Mode

This section shows how to configure EAP TLS mode for 802.1X.

To configure EAP TLS mode for 802.1X:

- Navigate to the **EAP-TLS** option and press the **Save** softkey.

3.5.6 Using the Configuration File

This section shows how to configure 802.1X using the Configuration File.

3.5.6.1 EAP MD5 Mode

This section shows how to configure 802.1X settings for EAP MD5.

To configure EAP MD5:

- Open the Configuration File page (**Management tab > Manual Update > Configuration File**) and configure the parameters using the table below as reference.

Table 3-47: EAP MD5 Parameters

Parameter	Description
network/lan/_802_1x/eap_type	Sets 802.1X Extensible Authentication Protocol mode [Disable] = Disables the use of 802.1X [EAP_MD5]=Authentication is implemented by user name and password (Password is optional).
network/lan/_802_1x/md5_identity	User ID for MD5 mode.
network/lan/_802_1x/md5_password	Password for MD5 mode (leave blank if no password).

3.5.6.2 EAP TLS Mode

This section shows how to configure phone's 802.1X settings for EAP TLS using the Configuration File.

To configure EAP TLS:

- Open the Configuration File page (**Management tab > Manual Update > Configuration File**) and configure the parameters using the table below as reference.

Table 3-48: EAP TLS Parameters

Parameter	Description
network/lan/_802_1x/eap_type	Sets 802.1X EAP mode. [Disable] = Disables the use of 802.1X [EAP_TLS]= Authentication is implemented by Certificate, Client Certificate, and Client Private Key.



Make sure the Root CA certificate and the Private Key certificate are installed on the RADIUS server as well.

3.5.7 Configuring HTTPS

This section shows how to configure the connection between AudioCodes' Device Manager and the phone using HTTPS, to secure communications.

To configure HTTPS:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-49: HTTPS Parameter

Parameter	Description
security/web/https_only	Enables the HTTPS protocol. <ul style="list-style-type: none">■ [0] Disable (default)■ [1] Enable

3.5.8 Supported Encryption Ciphers and TLS Version



The 400HD Series of IP Phones is aligned with TLS version 1.2.

3.5.9 Support for Enterprise HTTP/S Proxy Servers

This feature enables phones in an enterprise to send packets via the enterprise's proxy server instead of sending packets directly to the server. The new support enables customers to leverage their proxy as security when accessing cloud services. The network administrator can configure the feature via the configuration file.

To configure HTTP/S proxy server capability:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-50: Configuring HTTP/S Server

Parameter	Description
http_client/fwd_proxy/ip	Default: 0.0.0.0. Defines the proxy's IP address.
http_client/fwd_proxy/port	Default: 8080. Defines the port.
http_client/fwd_proxy/username	Default: 0. Defines the proxy username, for example, johnd .
http_client/fwd_proxy/password	Default: 0. Defines the proxy user's password. If 'username' is configured, then 'password' must also be configured, otherwise the same 'password' as it will not be taken from the domain's data.
http_client/fwd_proxy/direct/ip	Default: Local . When set to the default, phone HTTP requests destined for private IP addresses will not be sent to the forward proxy. If not set to the default, the phone will send all HTTP requests to the forward proxy (if its address is different to 0.0.0.0). Note: The IP Local/Private addresses are defined in RFC 1918.



Important:

- If the proxy server's username and password are not configured, the phone will use the NTLM domain's username and password.
- If 'username' is configured, then 'password' must also be configured as it will not be taken from the domain's data.
- To disable network communications going through the proxy server, the proxy IP address can be configured to "0.0.0.0".

3.6 Configuring Advanced Applications

3.6.1 Wi-Fi Capability



- Beta level
- Only applies to the 445HD and C450HD phones
- Only applies to 445HD-BW and C450HD-BW models
- Supported in specific regions such as the USA, Canada, the European Union, Switzerland, South Africa and Israel, and requires a specific CPN with a 'BW' suffix when ordering. For an updated list of supported regions, contact AudioCodes.

The phone can connect to an Access Point via Wi-Fi. The Wi-Fi interface can be used when the phone is installed in an environment free of LAN/cables, to perform VoIP calls over Wi-Fi. The phone can be connected by pressing the **Networks** icon in the phone's main menu -or- navigating in the 'Settings' menu and then selecting the **Wi-Fi** option.

3.6.2 Bluetooth

The phones support integrated Bluetooth for (wireless) USB headset connectivity.



- Beta level
- Only applies to the 445HD and C450HD phones (to the 445HD-BW and C450HD-BW models).
- Supported in specific regions such as the USA, Canada, the European Union, Switzerland, South Africa and Israel, and requires a specific CPN with a 'BW' suffix when ordering. For an updated list of supported regions, contact AudioCodes.

The feature is configured in the Settings screen (**Menu > Settings**).



- All Bluetooth headsets are defined by the phone as headsets and the phone's headset hard key onhooks / offhooks the headset.
- Connecting both the USB headset and the Bluetooth headset is currently not recommended.
- Known speakers such as the HRS 457, Jabra 710 and Jabra 510 are not defined as Bluetooth headsets. Users can define a known Bluetooth speaker as the phone's default Audio Device from **Settings > Audio Device**.

3.6.3 Dynamic URL Provisioning

Dynamic Host Configuration Protocol (DHCP) can be used to automatically provision all phones in the enterprise. The DHCP feature can be configured using the Configuration File.

To configure DHCP:

- Open the Configuration File page (**Management tab > Manual Update > Configuration File**) and configure the parameters using the table below as reference.

Table 3-51: Configuring Automatic Provisioning Performed by DHCP

Parameter	Description
Note: To add a value to these parameters, enter provisioning/ followed by the parameter name equals the value (e.g. <code>provisioning/method=dynamic</code>).	
provisioning/method	Defines the provisioning method:

Parameter	Description
	<ul style="list-style-type: none"> ■ [Disable] Disable - Automatic update is disabled. The phone attempts to upgrade its firmware and configuration ■ [Dynamic] DHCP Options (Dynamic URL) (default) - Using DHCP options 160 or 66/67 for provisioning ■ [Static] Static URL - Using Static URL for provisioning
provisioning/url_option_value	<p>Determines the DHCP option number to be used for receiving the URL for provisioning.</p> <p>The default value is 160.</p> <p>The phone supports DHCP Option 160 for complete URL and Options 66/67 for TFTP usage. Option 160 has the highest priority and if absent, Options 66/67 are used.</p> <p>The following syntax is available for DHCP option 160:</p> <ul style="list-style-type: none"> ■ <protocol>://<server IP address or host name> ■ <protocol>://<server IP address or host name>/<firmware file name> ■ <protocol>://<server IP address or host name>/<firmware file name>;<configuration file name> ■ <protocol>://<server IP address or host name>;<configuration file name> <p>Where <protocol> can be either "ftp", "tftp", "http" or "https" and where <configuration file name> can be either:</p> <ul style="list-style-type: none"> ■ A unique configuration file, per phone, for example: <MAC>.cfg -or- ■ A global configuration file, per deployment, for example, 450HD.cfg <p><u>Unique Configuration Example</u></p> <p>http://192.168.2.1/different.img;<MAC>.cfg</p> <p>The retrieved firmware file is <i>different.img</i> and the configuration file name is <MAC>.cfg such as <i>001122334455.cfg</i></p> <p><u>Global Configuration Example</u></p> <p>http://192.168.2.1/<450HD>.cfg</p> <p>The configuration file name is <i>450HD.cfg</i></p> <p>The following syntax is available for DHCP Options 66/67:</p> <ul style="list-style-type: none"> ■ Option 66 must be a valid IP address or host name of a TFTP server only. ■ Option 67 must be the firmware name. <p>If Option 67 is absent, the phone requests for the 450HD.img image file. For example:</p> <ul style="list-style-type: none"> ■ Option 66: 192.168.2.1 or myTFTPServer ■ Option 67: 450HD_2.0.9.img <p>Note:</p> <ul style="list-style-type: none"> ■ This parameter is applicable only when method is configured to "Dynamic". ■ It is recommended to leave the parameter at its default value to avoid conflict with other DHCP options settings.

Parameter	Description
provisioning/random_provisioning_time	<p>Defines the maximum random number to start the provisioning process.</p> <p>This is used for periodic checking of firmware and configuration files to avoid multiple devices from starting the upgrade process at the same time. When the device is meant to start the upgrade, the device randomly selects a number between 1 and the value set for random_provisioning_time and performs the check only after the random time.</p> <p>The valid range is 0-65535. The default value is 120.</p>
provisioning/period/type	<p>Defines the period type for automatic provisioning:</p> <ul style="list-style-type: none"> ■ [hourly] Hourly - Sets an interval in hours. ■ [daily] Daily (default) - Sets an hour in the day. ■ [weekly] Weekly - Sets a day in the week and an hour in the day. ■ [powerup] On Power-up Only - The phone tries to upgrade only after power-up.
provisioning/period/hourly/hours_interval	<p>The interval in hours for automatically checking for new firmware and configuration files.</p> <p>The valid range is 1 to 168. The default is 24.</p> <p>Note: This parameter is applicable only when type is configured to "hourly".</p>
provisioning/period/daily/time	<p>The hour in the day for automatically checking for new firmware and configuration files.</p> <p>The format of this value is hh:mm, where hh is hour and mm is minutes. For example, 00 : 30.</p> <p>The default time is 00:00.</p> <p>Note: This parameter is applicable only when type is configured to "daily".</p>
provisioning/period/weekly/day	<p>The day in the week for automatically checking for new firmware and configuration files.</p> <ul style="list-style-type: none"> ■ [Sunday] Sunday (default) ■ [Monday] Monday ■ [Tuesday] Tuesday ■ [Wednesday] Wednesday ■ [Thursday] Thursday ■ [Friday] Friday ■ [Saturday] Saturday <p>Note: This parameter is applicable only when type is configured to "weekly".</p>
provisioning/period/weekly/time	<p>The hour in the day for automatically checking for new firmware and configuration files.</p> <p>The format of this value is: hh:mm, where hh is hour and mm is minutes. For example: 00 : 30</p> <p>The default time is 00:00.</p> <p>Note: This parameter is applicable only when type is configured to "weekly".</p>

3.6.4 Configuring Date and Time



By default, date and time settings are *automatically provisioned* via the enterprise DHCP server when the phone is connected to the Internet and to the power supply, but you can *manually* change them if required. This section describes how.

The phone automatically retrieves date and time from a Network Time Protocol (NTP) server when it is connected to the Internet. NTP is a protocol for distributing Coordinated Universal Time (UTC) by synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

You can configure Daylight Saving Time using the Configuration File.

To configure Daylight Saving Time:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-52: Daylight Saving Time Parameters

Parameter	Description
system/daylight_saving/activate	Determines whether the phone automatically detects the Daylight Saving Time for the selected Time Zone. <ul style="list-style-type: none"> ■ [DISABLE] Disable (default) ■ [ENABLE] Enable
system/daylight_saving/mode	Configures the date format. Valid values are: FIXED = Date is specified as: Month, Day of month. DayOfWeek = Date is specified as Month, Week of month, Day of week.
system/daylight_saving/start_date	This subsection defines the starting day for the daylight saving offset. <ul style="list-style-type: none"> ■ [month] - defines specific month in year ■ [day] - defines specific day in month ■ [hour] - defines specific hour in day ■ [minute] - defines specific minute in hour <p>Example: To configure the phone to start daylight savings with a specific offset on February 22nd at 14:30, set the following:</p> <pre>system/daylight_saving/start_date/month=2 system/daylight_saving/start_date/day=22 system/daylight_saving/start_date/hour=14 system/daylight_saving/start_date/minute=30</pre>
system/daylight_saving/start_date/month	The month in a year. The valid range is 1 to 12.
system/daylight_saving/start_date/day	The day in a month. The valid range is 1 to 31.
system/daylight_saving/start_date/hour	The hour in the day. The valid range is 0 to 23.
system/daylight_saving/start_date/minute	The minute in an hour. The valid range is 0 to 59.

Parameter	Description
system/daylight_saving/end_date	<p>This subsection defines the ending day for the daylight saving offset.</p> <ul style="list-style-type: none"> ■ [month] - defines the specific month in a year ■ [day] - defines the specific day in a month ■ [hour] - defines the specific hour in a day ■ [minute] - defines the specific minute in an hour <p>For example: To configure the phone to end the daylight savings on July 16th at 22:15, set the following:</p> <pre>system/ntp/daylight_saving/end_date/month=7 system/ntp/daylight_saving/end_date/day=16 system/ntp/daylight_saving/end_date/hour=22 system/ntp/daylight_saving/end_date/minute=15</pre>
system/daylight_saving/end_date/month	<p>The month in a year. The valid range is 1 to 12.</p>
system/daylight_saving/end_date/day	<p>The day in a month. The valid range is 1 to 31.</p>
system/daylight_saving/end_date/hour	<p>The hour in the day The valid range is 0 to 23.</p>
system/daylight_saving/end_date/minute	<p>The minute in an hour. The valid range is 0 to 59.</p>
system/daylight_saving/offset	<p>The offset value for the daylight saving. The valid range is 0 to 180. The default offset is 60.</p>
system/daylight_saving/start_date/week	<p>Relevant to 'Day of week' mode: The week of month (values 1-5) for start of daylight saving time.</p>
system/daylight_saving/start_date/day_of_week	<p>Relevant to 'Day of week' mode: The day of week for daylight saving time start Valid values :</p> <ul style="list-style-type: none"> [SUNDAY] [MONDAY] [TUESDAY] [WEDNESDAY] [THURSDAY] [FRIDAY] [SATURDAY]
system/daylight_saving/end_date/week	<p>Relevant to 'Day of week' mode: The week of month (values 1-5) for end of daylight saving time.</p>

Parameter	Description
system/daylight_saving/end_date/day_of_week	Relevant to 'Day of week' mode: The day of week for daylight saving time start Valid values : [SUNDAY] (Default) [MONDAY] [TUESDAY] [WEDNESDAY] [THURSDAY] [FRIDAY] [SATURDAY]

3.6.4.1 Configuring NTP Server

The Network Time Protocol (NTP) server can be configured using the Configuration File.

To configure the NTP server:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-53: NTP Server Parameters

Parameter	Description
system/ntp/enabled	Enables the NTP server from which the phone retrieves the date and time. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable – obtains the time information from a configured NTP server
system/ntp/primary_server_address	Defines the address of the main NTP server. This can be a domain name, e.g., tick.nap.com.ar . You can select from the dropdown or leave the dropdown as User defined and manually define your domain in the adjacent field.
system/ntp/secondary_server_address	Defines the address of the secondary NTP server.
system/ntp/sync_time	This sub-section defines how often the phone must perform an update with the NTP server. <ul style="list-style-type: none"> ■ [days] - defines the number of days ■ [hours] - defines the number of hours For example: To configure the phone to perform an update with an NTP server every 1 day and 6 hours, set the following: system/ntp/sync_time/days=1 system/ntp/sync_time/hours=6
system/ntp/sync_time/days	The number of days. The valid range is 0 to 7. The default of days is 0.
system/ntp/sync_time/hours	The number of hours. The valid range is 0 to 24. The default is 12.
system/ntp/time_display_format	The format of the time displayed on the phone screen. <ul style="list-style-type: none"> ■ [24Hour] (default) ■ [12Hour]

To enable the NTP server in the phone's screen:

1. Open the Date and Time screen (MENU key > **Settings** > **Date and Time**).
2. If not already **Enabled**, select the **NTP Server** option.
3. Enter the password and then choose the **OK** softkey; the NTP server is enabled.

3.6.4.2 Configuring NTP Server via DHCP

If the phone is set to obtain GMT offsets and NTP servers via DHCP (default), it receives the following fields in the DHCP options:

- Primary Server and Secondary Server – (Option 4 or 42).



If both options (4 and 42) are received, the higher priority is given to Option 42.

- Time Zone – (Option 2) (see the table [below](#) for more information)

The phone sends an NTP request to the Primary NTP server. If there is no response, the NTP request is sent to the Secondary NTP server.

After obtaining the time from the server, it adds the GMT offset in Option 2. This is the updated system time.

To manually configure NTP / GMT offset:

- Configure the NTP and Time Settings using the table below as reference.



If the 'Obtain Time Zone from DHCP' parameter is set to **Disabled**, only the Primary Server NTP server parameter will be modifiable.

Table 3-54: NTP Server and GMT Parameters

Parameter	Description
system/ntp/gmt_offset	<p>Default is 00:00</p> <p>Enables the NTP server from which the phone retrieves the date and time.</p> <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable – obtains the time information from a configured NTP server
network/lan/dhcp/ntp/server_list/enabled	<p>Enables prioritization of the NTP server's information received from the DHCP server (Option fields 42 or 4), over the static configuration (system/ntp/primary_server_address and system/ntp/secondary_server_address).</p> <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)
network/lan/dhcp/ntp/gmt_offset/enabled	<p>Enables prioritization of the NTP GMT offset information received from the DHCP server (Option field 2), over the static configuration (system/ntp/gmt_offset).</p> <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)

Table 3-55: Time Zones

Time Zone	Place
(GMT-12:00)	Eniwetok, Kwajalein
(GMT-11:00)	Midway Is, Samoa
(GMT-10:00)	Hawaii
(GMT-09:00)	Alaska
(GMT-08:00)	Pacific Time (US & Canada)
(GMT-07:00)	Chihuahua, Mazatlan, Mountain Time (US & Canada)
(GMT-06:00)	Central Time (US & Canada)
(GMT-05:00)	Eastern Time (US & Canada)
(GMT-04:00)	Atlantic Time (Canada)
(GMT-03:30)	Newfoundland, Buenos Aires, Georgetown, Brasilia, Greenland
(GMT-03:00)	Buenos Aires, Georgetown, Brasilia, Greenland
(GMT-02:00)	Mid-Atlantic
(GMT-01:00)	Azores, Cape Verde Is
(GMT 00:00)	Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London, Casablanca, Monrovia
(GMT+01:00)	Amsterdam, West Central Africa, Madrid, Paris, Vilnius, Berlin, Bern, Rome, Vienna, Prague
(GMT+02:00)	Cairo, Jerusalem, Bucharest, Helsinki, Riga, Tallinn, Athens, Istanbul, Minsk, Harare, Pretoria
(GMT+03:00)	Kuwait, Riyadh, Nairobi, Baghdad, Moscow, St. Petersburg, Volgograd
(GMT+03:30)	Tehran
(GMT+04:00)	Abu Dhabi, Muscat, Baku, Tbilisi, Kabul
(GMT+05:00)	Islamabad, Karachi, Tashkent, Yekaterinburg
(GMT+05:30)	Bombay, Calcutta, Madras, New Delhi
(GMT+05:45)	Kathmandu
(GMT+06:00)	Almaty, Dhaka, Colombo, Almaty, Novosibirsk
(GMT+06:30)	Rangoon
(GMT+07:00)	Bangkok, Hanoi, Jakarta, Krasnoyarsk
(GMT+08:00)	Beijing, Chongqing, Hong Kong, Urumqi, Perth, Singapore, Taipei, Irkutsk, Ulaan Bataar
(GMT+09:00)	Osaka, Sapporo, Tokyo, Seoul, Yakutsk
(GMT+09:30)	Darwin, Adelaide
(GMT+10:00)	Canberra, Melbourne, Sydney, Brisbane, Guam, Port Moresby, Hobart, Vladivostok
(GMT+11:00)	Magadan, Solomon Is, New Caledonia
(GMT+12:00)	Fiji, Kamchatka, Marshall Is, Auckland, Wellington
(GMT+13:00)	Nuku'alofa

3.6.5 Configuring Contacts (LDAP)

This section shows how to configure Lightweight Directory Access Protocol (LDAP) using the Configuration File.



It's recommended not to change the default setup.

LDAP is an application protocol for accessing and maintaining distributed directory information services over an IP network.

See RFC 4510 for a full description.

To configure LDAP:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 3-56: LDAP Parameters

Parameter Name	Description
system/ldap/enabled	Enables or disable LDAP.
system/ldap/server_address	Defines the IP address or URL of the LDAP server.
system/ldap/port	Defines the LDAP service port.
system/ldap/user_name	Defines the user name used for the LDAP search request.
system/ldap/password	Defines the password of the search requester.
system/ldap/base	Defines the access point on the LDAP tree.
system/ldap/name_filter	Specifies your search pattern for name look ups. For example: When you type in the following field: (&(telephoneNumber=*)(sn=%)), the search result includes all LDAP records, which have the 'telephoneNumber' field set and the ("sn"-->surname) field starting with the entered prefix. When you type in the following field: (!(cn=%)(sn=%)), the search result includes all LDAP records which have the ("cn"-->CommonName) OR ("sn"-->Surname) field starting with the entered prefix. When you type in the field (!(cn=%)), the search result includes all LDAP records which "do not" have the "cn" field starting with the entered prefix.
system/ldap/name_attrs	Specifies the LDAP name attributes setting, which can be used to specify the "name" attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, cn sn displayName", this requires you to specify 'cn-->commonName'. This is the Full name of the user, sn-->Surname, last name or family name and "displayName" fields for each LDAP record.

Parameter Name	Description
system/ldap/number_filter	Specifies your search pattern for number look ups. When you type in the following field, for example, <i>((telephoneNumber=%)(Mobile=%)(ipPhone=%))</i> , the search result is all LDAP records which have the “telephoneNumber” OR “Mobile” OR “ipPhone” field match the number being searched. When you type in the following field: <i>(&(telephoneNumber=%)(sn=*))</i> , the search result is all LDAP records which have the “sn” field set and the “telephoneNumber” match the number being searched.
system/ldap/number_attrs	Specifies the LDAP number attributes setting, which can be used to specify the “number” attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, <i>Mobile telephoneNumber ipPhone</i> , you must specify ‘Mobile’, ‘telephoneNumber’ and ‘ipPhone’ fields for each LDAP record.
system/ldap/display_name	Specifies the format in which the “name, e.g. “Mike Black” of each returned search result is displayed on the IPPHONE. When you type in the following field, for example: <i>%sn, %givenName</i> , the displayed result returned should be “Black, Mike”.
system/ldap/max_hits	Specifies the maximum number of entries expected to be sent by the LDAP server (this parameter is sent to the LDAP server).
system/ldap/sorting_result	Sorts the search result by display name on the client side.
system/ldap/predict_text	This parameter appears in the configuration file; however, it is currently not supported.
system/ldap/search_timeout	The time out value for LDAP search (this parameter is sent to the LDAP server).
system/ldap/ui/use_right_arrow_active_search	This parameter appears in the configuration file; however, it is currently not supported.
system/ldap/lookup_incoming_call	This parameter appears in the configuration file; however, it is currently not supported.
system/ldap/call_lookup	Performs an LDAP search during call (search the display name for a number).
system/ldap/country_code	Defines the country code prefix added for number search.
system/ldap/area_code	Defines the area code prefix added for number search.
system/ldap/minimal_name_search_length	Starts to perform an LDAP search after x characters are input.
system/ldap/send_queries_while_typing	Sends an LDAP search each time the user presses a key (all keys with both number and letters).

3.6.6 Configuring T9

When searching for a contact in the Corporate Directory, users can press dial pad keys *to input letters*. Only a single press on any key, regardless of the letter's position on the key, is necessary

See the phone's *User's Manual* for more information.

To configure T9:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-57: T9 Parameter

Parameter Name	Description
lync/contact_search_t9_enabled	Enables or disable T9 mode. Default= Enable .

3.6.7 Configuring the Caller Name to be Displayed

Network administrators can configure the caller's name to be displayed from the incoming SIP message's "From" header or from information in the Active Directory (default).

To configure the feature:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 3-58: Caller Name to be Displayed

Parameter Name	Description
lync/contact_name_priority	<ul style="list-style-type: none"> ■ CONTACT_SEARCH (Default) = phone displays the caller name from the Active Directory's information ■ CALL_DESCRIPTION = phone displays caller name from the incoming SIP message's "From" header

4 Configuring Microsoft Skype for Business Features

This section shows how to configure Microsoft Skype for Business features.

4.1 Microsoft Screen Theme



Applies only to the 450HD and C450HD phone.

The screen theme by default reflects Microsoft Skype for Business 2016 client look & feel but network administrators can opt to switch from the default to the legacy by changing the *personal_settings/ui_theme* parameter from MSFT_THEME to AUDIOCODES_THEME.

4.2 Configuring Phone Status and User Status Timeouts

Network administrators can configure how long it takes for the phone status to change from 'Inactive' to 'Away', using parameter *lync/presence/state_change_timeout*.

Network administrators can also configure how long it takes for the user's status to change from 'Available' to 'Inactive', using parameter *lync/presence/state_inactive_timeout*.

Default for both parameters: 300 seconds (five minutes).

Range for both parameters: 300 seconds – 2073600 seconds (24 days).

4.3 Park Call

The IP phone lets users park a call, i.e., transfer a call to a "parking lot" for it to be picked up on any other phone in the enterprise by a party who must dial a retrieval number in order to retrieve it on that phone. The retrieval number is configured in the Skype for Business server's parking lot parameter. The retrieval number can be changed if required.

To pre-configure Microsoft's Skype for Business server for park call capability, see:

<http://technet.microsoft.com/en-us/library/gg399014.aspx>

Refer to all subsections.

4.4 Music on Hold (MoH)

If a user puts a call on hold to answer an incoming call or to make another call, the party put on hold can hear music played. The Play Music on Hold feature allows this. By default, the Play MoH feature is not enabled in Skype for Business.

To enable the MoH feature on the Skype for Business server:

1. In the Skype for Business Server Management Shell, run the following command in order to view the current settings of the client policy:

```
Get-CSClientPolicy Global
```



```
Administrator: Lync Server Management Shell
PS C:\Users\administrator.DOITFIXIT> Get-CSClientPolicy Global

Identity                : Global
PolicyEntry              : ()
Description              :
AddressBookAvailability : WebSearchAndFileDownload
AttendantSafeTransfer   :
AutoDiscoveryRetryInterval :
BlockConversationFromFederatedContacts :
CalendarStatePublicationInterval :
ConferenceIMIdleTimeout :
CustomizedHelpUrl       :
CustomLinkInErrorMessage :
CustomStateUrl           :
DGRefreshInterval       :
DisableICE               :
DisableCalendarPresence :
DisableContactCardOrganizationTab :
DisableEmailComparisonCheck : True
DisableEmoticons        : False
DisableFeedsTab         :
DisableFederatedPromptDisplayName :
DisableFreeBusyInfo     :
DisableHandsetOnLockedMachine :
```

- Note that the **EnableClientMusicOnHold** parameter is set to **FALSE**. Run the following command to set it to **TRUE**:

```
Set-CSClientPolicy Global -EnableClientMusicOnHold:$TRUE
```

But note that in case the phone and PC client are connected with same user, the Skype for Business PC client setting is “stronger” than the phone setting (in case of collision).

```
Administrator: Lync Server Management Shell

SearchPrefixFlags       :
ShowRecentContacts      : True
ShowManagePrivacyRelationships : False
ShowSharepointPhotoEditLink : False
SPSearchInternalURL     :
SPSearchExternalURL     :
SPSearchCenterInternalURL :
SPSearchCenterExternalURL :
TabURL                  :
WebServicePollInterval  :

PS C:\Users\administrator.DOITFIXIT> Set-CSClientPolicy Global -EnableClientMusicOnHold:$TRUE
PS C:\Users\administrator.DOITFIXIT> _
```

- To prevent users from selecting or changing the music played on hold, run the following command defining the audio file:

```
Set-CSClientPolicy -EnableClientMusicOnHold:$TRUE -
MusicOnHoldAudioFile <Audio file Path>
```

To choose the music to be played on the IP phone:

- Open the ini configuration file in an editor like Notepad.
- Configure the 'lync/moh/url' parameter with the required file transport (TFTP). The format supported by the IP phone is:
 - WAV linear 16k 16 bit -OR-
 - WAV a/u law
- Save and close the file and load it to the phone.



The maximum file size allowed is 300Kb. If it exceeds 300Kb, loading it will fail.

4.5 Configuring Timeouts for Presence Status Changes

Network administrators can configure how it will take for user presence status to change from

- 'Available' to 'Inactive' (use the table below as reference)
- 'Inactive' to 'Away' (use the table below as reference)

Table 4-1: Presence Status Timeout Parameters

Parameter Name	Description
lync/presence/state_change_timeout	Configures how long it will take for presence status to change from 'Available' to 'Inactive' Min: 0 seconds; Default: 300 seconds (5 minutes); Max: 2073600 seconds (24 days)
lync/presence/state_inactive_timeout	Configures how long it will take for presence status to change from 'Inactive' to 'Away' Min: 0 seconds; Default: 300 seconds (5 minutes); Max: 2678400 seconds (31 days)

4.6 Group Call Pickup (GCP)

GCP lets an employee take a call coming in on a colleague's phone, on their phone. If an employee in an open space hears a colleague's phone ringing and knows that colleague is unavailable, instead of having the call go unanswered and routed to Voice Mail, the call can be redirected and answered by the available employee. Only employees configured in the Skype for Business server's GCP parameter can pick up the call.

To pre-configure Microsoft's Skype for Business server for GCP capability, see:

<http://technet.microsoft.com/en-us/library/jj945645.aspx>

Refer to all subsections.

4.7 Location

This feature enables the called party to identify the geographical location of the calling party. For example, if a caller in the U.S. makes an emergency call to E911, the feature extracts the caller's information for the police department to immediately identify the caller's location.

To enable users for E9-1-1:

<http://technet.microsoft.com/en-us/library/gg425892.aspx>

To define Location Policy in Microsoft's Skype for Business server, see:

<http://technet.microsoft.com/en-us/library/gg398962.aspx>

4.8 Configuring Skype for Business Server for SRTP / TLS

This section shows how to configure Microsoft Skype for Business Server for Secure Real-Time Transport Protocol (SRTP) / TLS, if it isn't configured already.

To configure Microsoft Skype for Business Server for SRTP/TLS:

1. Open the Microsoft Skype for Business Server management interface.
2. Configure a 'Route' on the Skype for Business Server.
3. Open the server's Edit Trunk Configuration – Global screen.

Figure 4-1: Skype for Business Server - Edit Trunk Configuration - Global

4. Select the **Enable media bypass** option.
5. Select one of the following options from the the 'Encryption Support Level' dropdown:
 - **Required** - SRTP encryption will be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
 - **Optional** - SRTP encryption will be used if the service provider or equipment manufacturer supports it.
 - **Not Supported** - SRTP encryption is not supported by the service provider or equipment manufacturer and will therefore not be used.
6. The option selected depends on customer configuration / requirements.
 - If you set 'Encryption Support Level' to **Optional**, make sure the encryption is enabled in PowerShell (<https://support.microsoft.com/en-us/kb/2761579>):

```
Get-CsMediaConfiguration |Set-CsMediaConfiguration -
EncryptionLevel SupportEncryption
Identity                : Global
EnableQoS                : False
EncryptionLevel       : SupportEncryption
EnableSiren              : False
MaxVideoRateAllowed     : VGA600K
```

4.9 Updating Device Firmware from the Skype for Business Server

The phone's firmware version can be updated from the Skype for Business server.



For more information on the firmware update process, refer to <https://technet.microsoft.com/en-us/library/gg398861.aspx/>.

Figure 4-2 shows Microsoft's Lync Server 2013 page from which the phone's firmware version is updated. The same concept applies to the Skype for Business server page.

Figure 4-2: Microsoft Server Page from which the Firmware Version is Updated

The screenshot shows the Lync Server 2013 Administration Console. The left navigation pane has 'Clients' selected. The main area shows the 'Device Update' page with a table of devices. The table has the following columns: Device type, Model, Locale, and Pool. The data rows are as follows:

Device type	Model	Locale	Pool
3PIP	420HD	ENU	WebServer.LyncPool2013.ac5pi
3PIP	405	ENU	WebServer.LyncPool2013.ac5pi
3PIP	440HD	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	4120	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	4110	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	4120	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	4110	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	4120	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	4110	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX600	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX600	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX600	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX600	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX500	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX500	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX500	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX500	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX3000	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX5000	ENU	WebServer.LyncPool2013.ac5pi
UCPhone	CX3000	ENU	WebServer.LyncPool2013.ac5pi

4.9.1 Enabling Automatic Firmware Updates from the Server

The network administrator must locate the phone's firmware file on the Skype for Business server's embedded automatic upgrading facility, and configure the server to provision the phone. The facility allows for centralized automated phone upgrade to the latest firmware version. The firmware of any phone connected to the facility can be automatically upgraded from the facility. The phone then periodically - usually once a day - checks the Skype for Business server's automatic upgrading facility to determine if the firmware file on the phone is different to the firmware located on the Skype for Business server. The firmware file on the phone will be updated if it's different to the firmware located on the Skype for Business server.

4.9.2 Enabling Automatic Firmware Updates from the Server using Configuration File

You can use the Configuration File to enable automatic firmware updates from the Skype for Business Server.

To enable automatic firmware updates from the Skype for Business server:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-2: Automatic Firmware Update from Skype for Business Server - Configuration File

Parameter Name	Description
lync/SfBDeviceUpdate=0	Enables / disables automatic firmware update from the Skype for Business server. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable

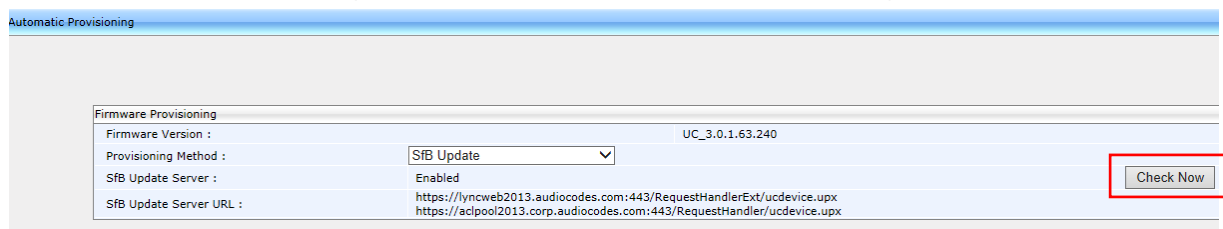
4.9.3 Manually Downloading Firmware to the Phone from the Server

When the 'SfB Update' provisioning method is used to provision the phone, you can *manually* check and download the firmware file on the Skype for Business server's automatic upgrading facility.

To manually check and download the firmware file located on the server to the phone:

1. In the Web interface, open the Automatic Provisioning page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

Figure 4-3: Web Interface – Automatic Provisioning



2. Click the **Check Now** button; the firmware file on the Skype for Business server's automatic upgrading facility is checked and downloaded to the phone if different.

4.10 Enabling Phone Lock

The phone supports the capability to automatically lock after a preconfigured period of time. The feature secures the phone against unwanted (mis)use.



- The network administrator must enable *both* the Skype for Business server *and* the Web interface for the feature to function. If enabled in the server but disabled in the the Web interface, the feature will not function.
- The timeout is set in the Skype for Business server only.

When the phone is locked:

- Incoming calls are allowed
- Outgoing calls are not allowed except for calls to emergency numbers (police, ambulance service, firefighting service, etc.) which will be available via the **Emergency** softkey displayed after the phone locks.
- Voice Mail, Call Log, Calendar and Contacts cannot be accessed

To enable the feature:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-3: PIN Lock Parameter

Parameter Name	Description
system/pin_lock/enabled	Enables/disables automatic lock. If enabled, the user will be prompted for a PIN code when signing in for the first time. E.g.: 40004696 . The minimum length is configured on the server side. <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)



If a user's phone was automatically paired (see Section 4.12.7) and if the PC/laptop is active (not locked), the phone cannot be manually locked. The user can manually lock it only after locking the PC/laptop. If the user doesn't manually lock the phone, it will nevertheless automatically lock after the timeout preconfigured in the Skype for Business server lapses. The phone will unlock only after the user unlocks their PC/laptop or if the user manually unlocks the phone.

4.10.1 Allowing Users Other Capabilities besides Emergency Calls if Phones Lock

Network administrators can allow other capabilities besides dialing emergency numbers to users whose phones lock, in compliance with Microsoft Skype for Business.

Network administrators can configure parameters to:

- *Allow users to make outgoing calls even though the phone is locked*
- *Allow users to receive incoming calls even though the phone is locked*
- *Allow users to answer Delegate calls even though the phone is locked*
- *Allow users to use the phone's handset even though the phone is locked*

4.10.1.1 Allowing Users to use the Phone's Handset

Network administrators can configure the inband provisioning parameter 'DisableHandsetOnLockedMachine' on the server to allow users to use the phone's handset even if the phone is locked. Use the table below as reference.

Table 4-4: Inband Provisioning Parameter 'DisableHandsetOnLockedMachine'

Parameter Name	Description
DisableHandsetOnLockedMachine	<p>Determines handset functionality when the phone is locked.</p> <p>[0] Allows incoming and outgoing calls when the phone is locked</p> <p>[1] Allows only incoming calls when the phone is locked</p> <p>[2] Disallows incoming and outgoing calls when the phone is locked</p> <p>If the parameter is not provisioned, the phone functions as if the parameter is set to [1] - only incoming calls are allowed when the phone is locked.</p>

4.10.1.2 Allowing Users to Make/Receive Incoming/Outgoing Calls

Network administrators can configure a local phone parameter 'AllowCallsInLockState' to determine if users can make/receive incoming/outgoing calls even if the phone is locked. Use the table below as reference.

Table 4-5: Local Phone Parameter 'AllowCallsInLockState'

Parameter Name	Description
AllowCallsInLockState	<p>Determines if users can make/receive incoming/outgoing calls if the phone locks.</p> <p>[GET_FROM_INBAND] The phone's capabilities when locked are set by inband provisioning parameter (default)</p> <p>[ALLOW_BOTH] Allows users to make/receive incoming/outgoing calls when the phone is locked</p> <p>[ALLOW_INCOMING_ONLY] Allows users to make/receive incoming/outgoing calls when the phone is locked</p> <p>[DENY_BOTH] Disallows users from making/receiving incoming/outgoing calls when the phone is locked</p> <p>If set to ALLOW_BOTH or ALLOW_INCOMING_ONLY or DENY_BOTH, this parameter overrides the 'DisableHandsetOnLockedMachine' inband provisioning parameter.</p>

4.10.1.3 Allowing Users to Answer Second-Hand (SLA | Delegation) Incoming Calls

Network administrators can configure a local parameter 'AnswerDelegatelncomingCalls' to determine if users can answer second-hand (Share Line Appearance and Delegation) incoming calls when the phone is locked.

The parameter is applicable only if parameter 'AllowCallsInLockState' is configured to allow the phone to answer incoming calls in lock state. See the previous section for details.

Use the table below as reference.

Table 4-6: Local Phone Parameter 'AnswerDelegatelncomingCalls'

Parameter Name	Description
AnswerDelegatelncomingCalls	<p>Determines if users can answer second-hand (Share Line Appearance and Delegation) incoming calls when the phone is locked.</p> <p>[0] Users cannot answer incoming Delegate calls when the phone is locked (default)</p> <p>[1] Users can answer incoming Delegate calls when the phone is locked.</p> <p>Note that the parameter is only applicable if parameter 'AllowCallsInLockState' is configured to allow the phone to answer incoming calls in lock state. See the previous section for details.</p>

4.11 Exchange Server Features

Microsoft Exchange server features such as the Calendar feature are available on the phone.



To connect to Microsoft Exchange and receive these features, (online) sign-in *must be with username in UPN format*.

- Sign-in address
- Username in UPN (User Principal Name) format. UPN format is the way the user's name appears in their e-mail address listed in the Active Directory, i.e., **username@domain.com**
- User's network IT password

Signing in with a username that is a NetBIOS Domain Name, i.e., **domain\username**, as well as signing in with the phone Extension and PIN Code, are disallowed for Skype for Business *online sign-in*. They are only allowed for *on-premises* sign-in.

4.11.1 Configuring Calendar Displayed in the Phone's Screen

Microsoft Exchange Calendar is by default displayed in the phone's screen. To connect to Microsoft Exchange and receive the Calendar feature, sign-in *must be with username in UPN format* as described in the Note above.

To configure the feature with the Configuration File:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 4-7: Microsoft's Exchange Calendar

Parameter Name	Description
lync/calendar/enabled	Enables or disables displaying Microsoft Exchange Calendar items in the phone's screen. <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)
lync/calendar/mode	Determines which Microsoft Exchange Calendar meetings will be displayed in the phone's screen. <ul style="list-style-type: none"> ■ [24H] (Default) Displays meetings scheduled to commence <ul style="list-style-type: none"> • between now and 24 hours from now • before now but scheduled to end after now • before 24 hours from now but scheduled to end after 24 hours from now ■ [TODAY] Displays meetings scheduled to commence between the midnight of the night before now and the midnight of the night ahead.
lync/calendar/sync_time/minutes	Determines how frequently the phone synchronizes with Microsoft Exchange Server. Default: Every 15 minutes.

4.11.2 Configuring Meeting Reminders Popping up in the Phone's Screen

By default, reminders for *all* types of meetings; Skype for Business meetings as well as other types of meetings, will automatically pop up in the phone's screen. The feature can be modified using the Configuration File. The network administrator can configure for *which types of* meetings reminders will pop up.

To configure the feature:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-8: Calendar Meeting Reminders

Parameter Name	Description
lync/calendar/ReminderMode	<p>Determines for which types of meetings reminders will automatically pop up in the phone's screen.</p> <ul style="list-style-type: none"> ■ [ALL] (Default) Enables reminders for <i>all</i> types of meetings; Skype for Business meetings as well as other types of meetings will pop up in the phone's screen. ■ [NONE] Disables reminders for <i>all</i> types of meetings; no meeting reminders will pop up in the phone's screen. ■ [ONLINE] Enables reminders for online meetings, i.e., Skype for Business meetings.

4.11.3 Visual Voicemail



- For the feature to function:
 - Your network administrator must enable your voicemail.
 - You need to sign in to the phone with username and password. If you signed in with PIN code, the feature will not be available and your phone will display the following message:
 - Your account is not configured for Exchange Unified Messaging.
 - Features activated from Microsoft's Exchange Server - such as this one - are only available after signing in to the phone with *username in UPN format* described in the Note [above](#).

If voicemail is enabled and the phone was signed in by online sign-in, the user will be able to view a list of voicemail messages and select which message to listen to or to delete after pressing the voicemail hard key on the phone.

4.11.4 Skype for Business 'Favorites' Contacts & Outlook Contacts

Contact groups defined in Skype for Business and Outlook contacts are integrated with the phone. Pressing the CONTACTS hard key on the phone displays by default the 'Favorites' defined in the Skype for Business client. In the 'Favorites' screen, the **Groups** softkey provides the option to access 'Outlook contacts'. See the *User's Manual* for more information. The network administrator can limit the number of Outlook contacts to display in the phone's screen, to optimize phone resources.

To configure the maximum number of Outlook contacts to display in the phone's screen:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-9: Maximum Number of Outlook Contacts to Display in the Phone's Screen

Parameter Name	Description
lync/ews/OutlookContactReply	<p>Determines the maximum number of Outlook contacts to retrieve for display in the phone's screen.</p> <p>[50] (Default) = the phone will be able to retrieve for display up to 50 Outlook contacts in the screen.</p> <p>[0] = an unlimited number of Outlook contacts can be retrieved for display in the phone's screen, i.e., as many contacts as there are defined in Outlook can be retrieved for display.</p> <p>[500] = The maximum number of Outlook contacts that the phone can retrieve for display.</p>

4.12 Better Together over Ethernet

This section shows how to set up the Microsoft Skype for Business feature 'Better Together over Ethernet' on AudioCodes' 400HD Series of IP Phones.



BToE is not supported on the RX50 Conference Phone but the device by default includes a new **Pair** key that will appear after restoring to the phone's default settings. The key is for the future **Duo** feature.

BToE enables operations to be mirrored on both AudioCodes' IP phone and the Skype for Business client on the PC/laptop, so that these operations can be controlled from either the IP phone or the PC/laptop, whichever is convenient to the user at the time, for enhanced unified communications and optimized enterprise efficiency.

After your IP phone is paired with your Skype for Business client, you can control (from phone or PC/laptop) operations such as answering incoming calls, making outgoing calls (click-to-dial), putting calls on hold and resuming them, and making conference calls (see the *User's Manual*).

4.12.1 BToE Firewall Ports

Before installing the BToE, make sure the following firewall ports are configured:

- TCP port 9999 for communication between the BToE PC application and the phone.
- UDP port 9999 for the first steps of automatic pairing.
- UDP port 9998 for audio streaming.



- Port 9999 can be configured with parameter *lync/BToE/TcpPortNumber=9999*
- The audio streaming is equal to *TcpPortNumber - 1*

4.12.2 Installing the BToE PC Application

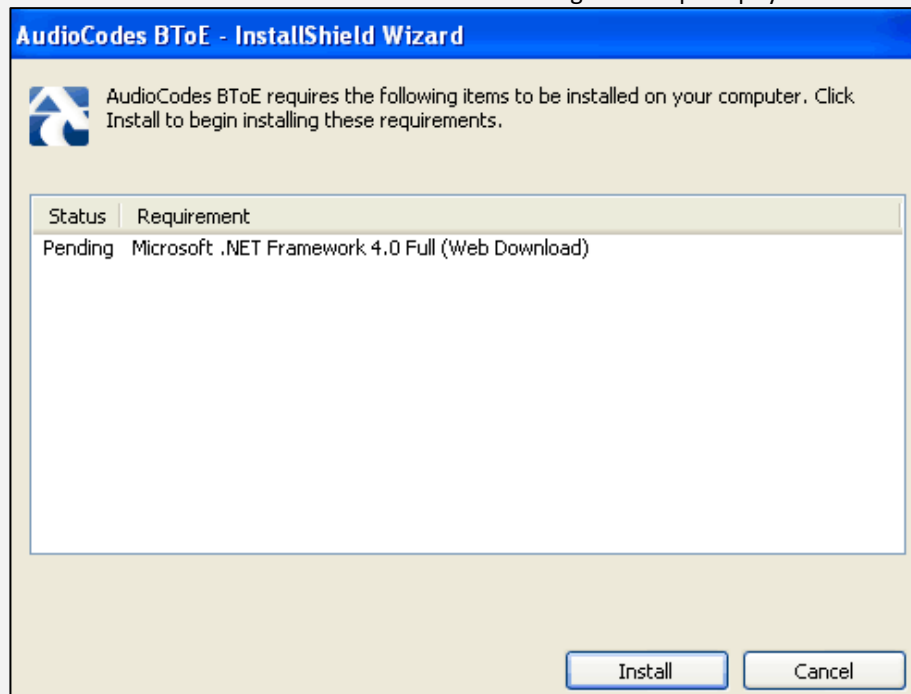
This section shows how to install AudioCodes' BToE PC/laptop application.

To install the BToE PC/laptop application:

1. After obtaining the installation file whose name will be either *AudioCodes BToE.exe* or *AudioCodes BToE.msi*, save it to your PC and then double-click it.



- If you install with the *exe*, then when upgrading you must use the *exe*. You cannot upgrade with the *msi* if you first installed with the *exe*, and vice versa.
- See Section 4.12.3 for information on how to distribute the BToE PC application *msi* package.
- Some PCs require the installation of .Net 4.0 prior to the installation of the BToE PC/laptop application. If you use the installation file *AudioCodes BToE.exe*, the Installation Wizard will detect that .Net 4.0 is missing and will prompt you to install it:



When installing the BToE PC/laptop application using the installation file *AudioCodes BToE.msi*, you won't be prompted to install .Net 4.0 and the network administrator should make the necessary preparations prior to installation of the BToE PC application.

The Prepare to Install screen opens showing preparation progress until the Welcome to the InstallShield Wizard screen opens as shown in [Figure 4-7](#).

Figure 4-4: InstallShield Wizard – Preparing to Install

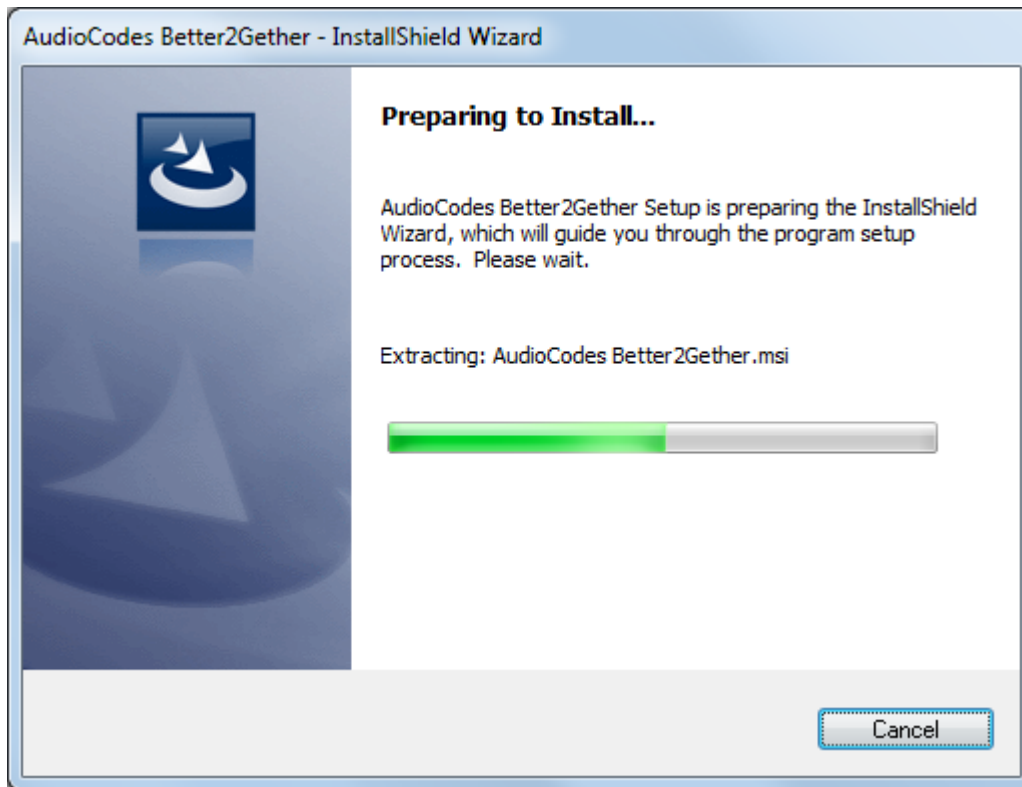
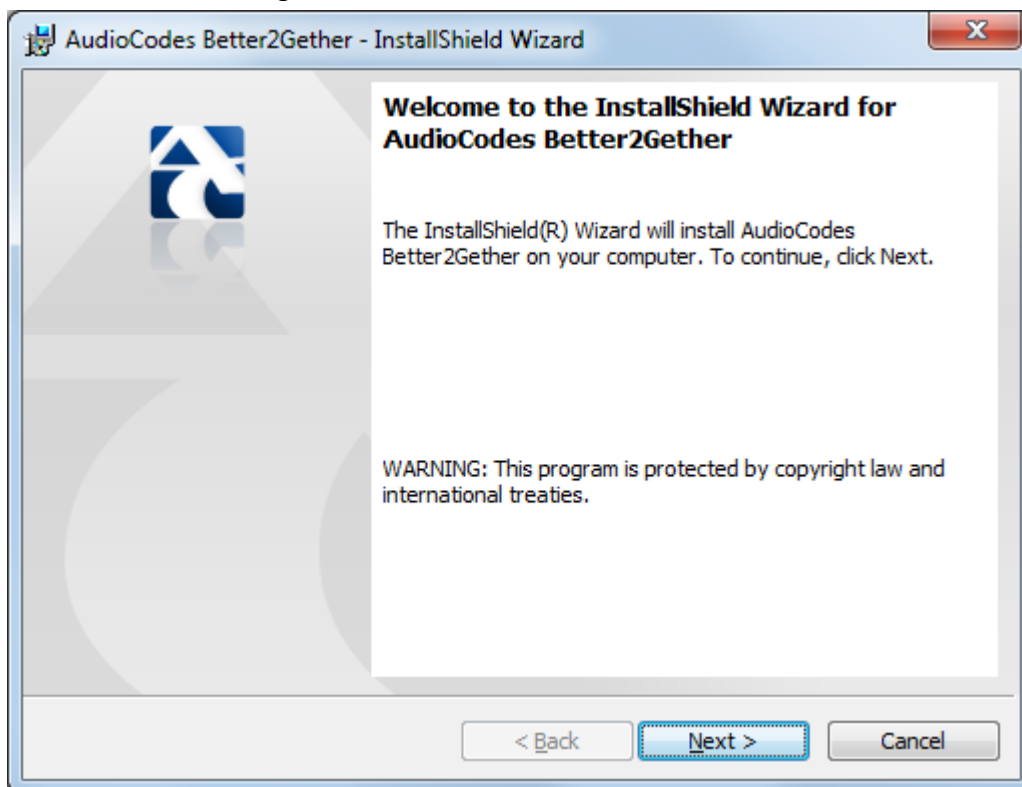
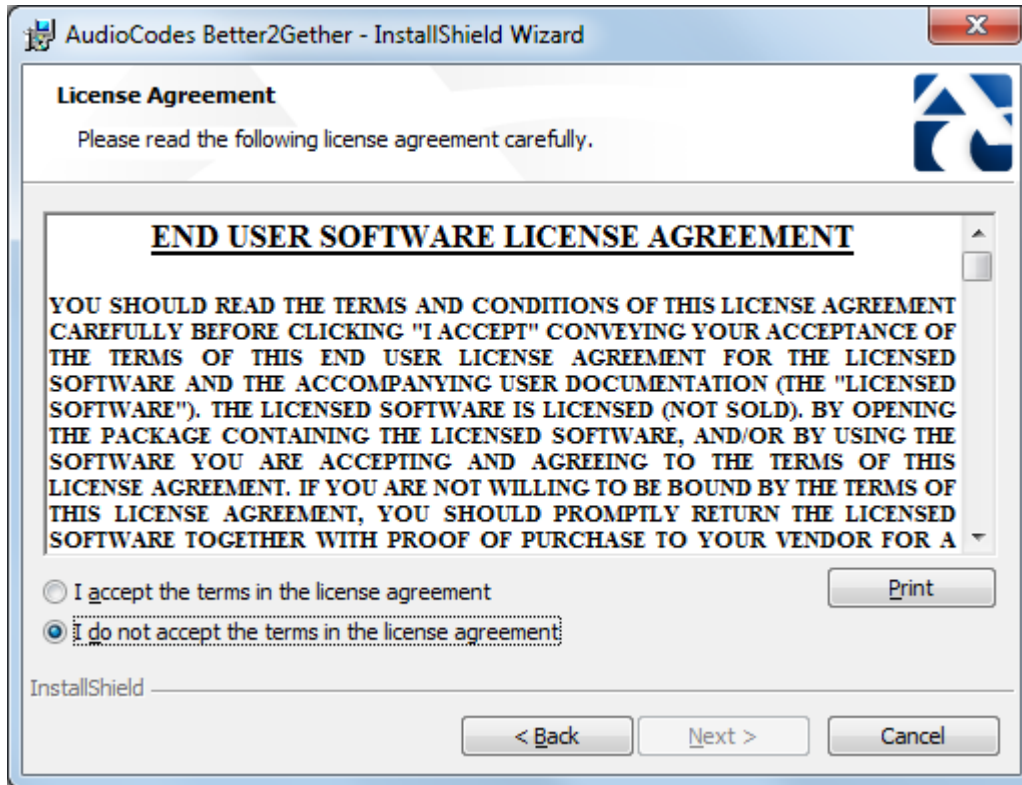


Figure 4-5: Welcome to the InstallShield Wizard



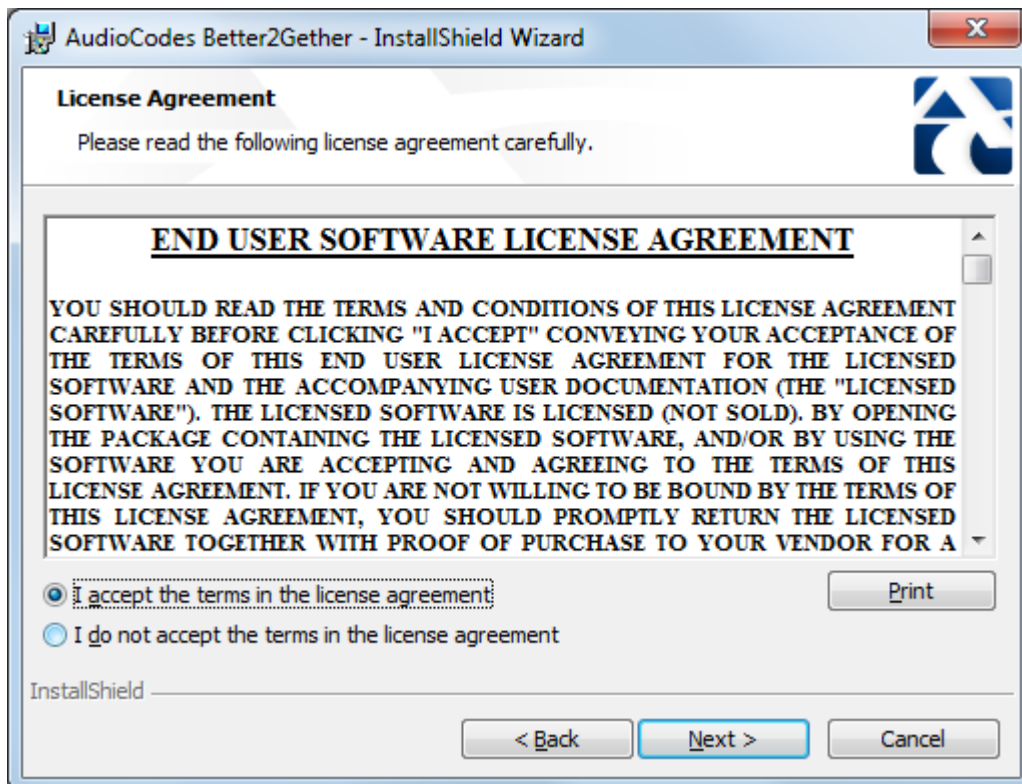
2. Click **Next**; the License Agreement dialog opens.

Figure 4-6: License Agreement



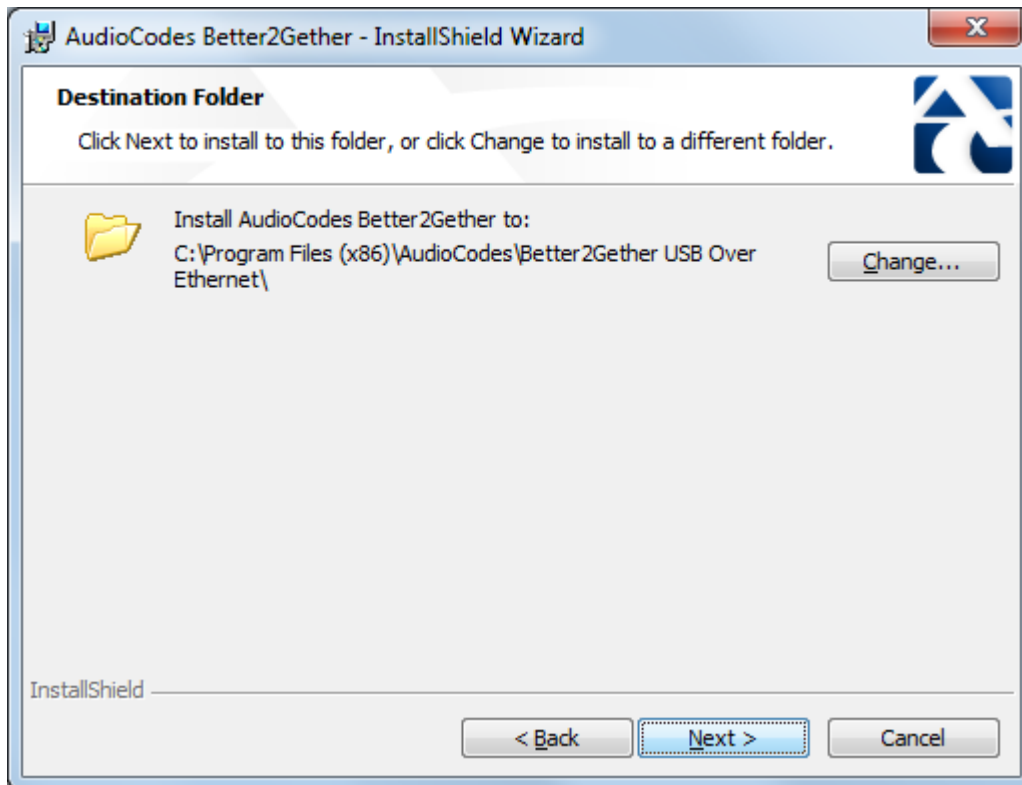
3. Select the **I accept...** option and click **Next**.

Figure 4-7: License Agreement



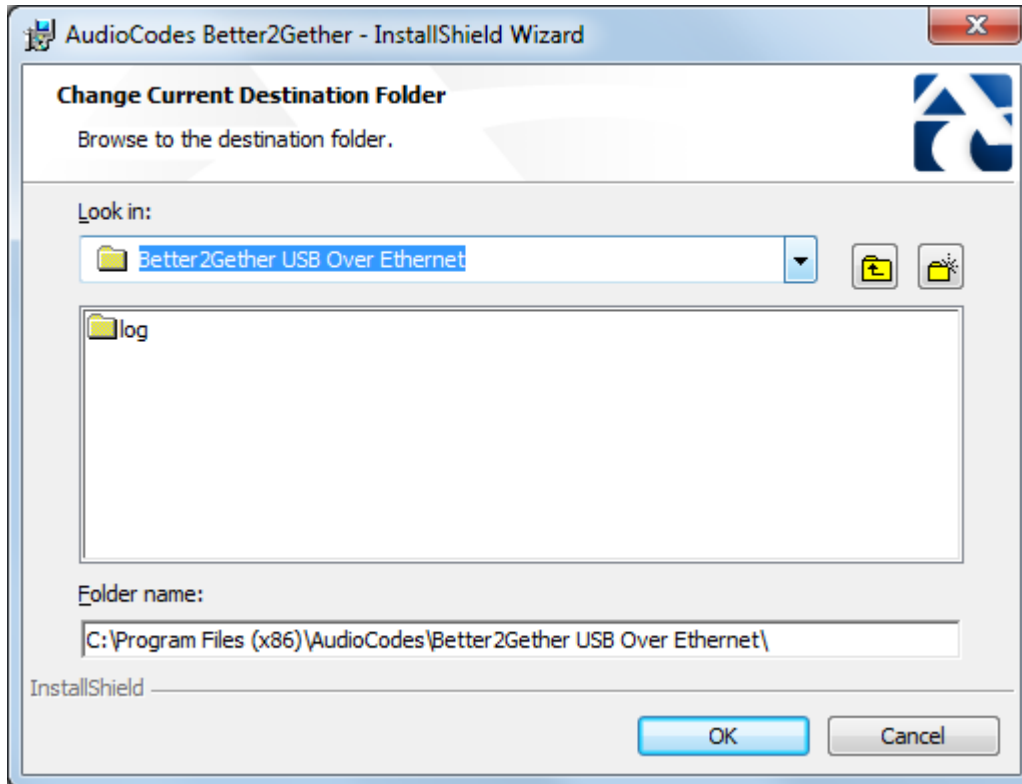
4. Click **Next**; the Destination Folder dialog opens.

Figure 4-8: Destination Folder



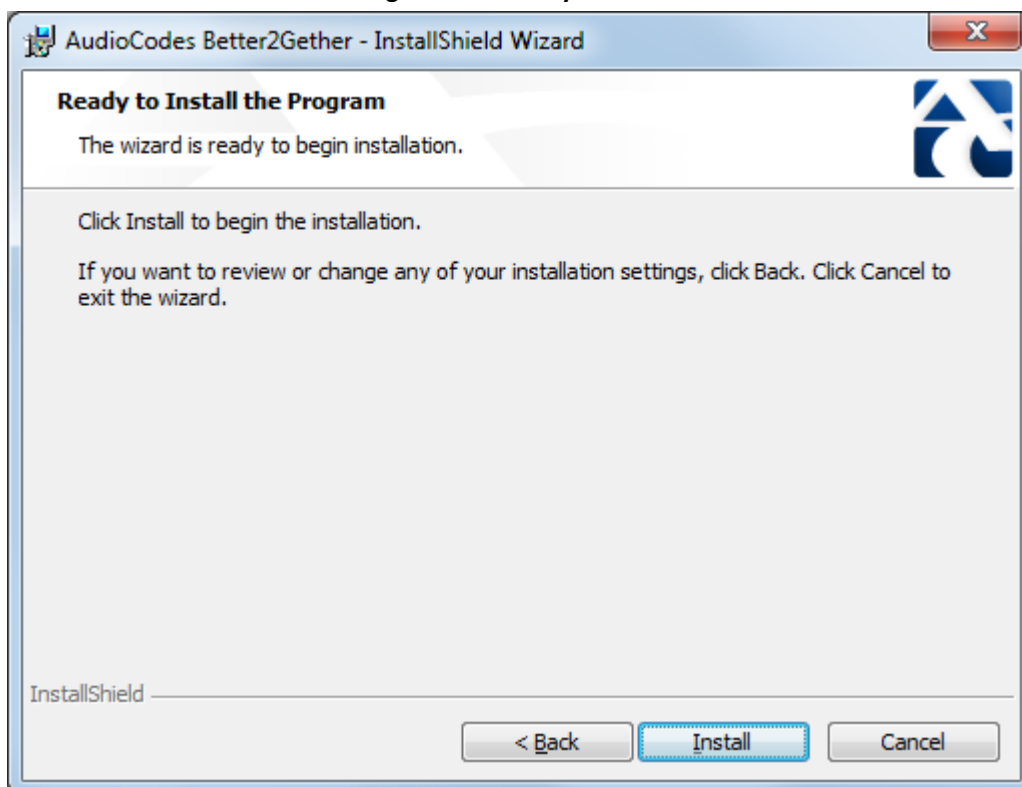
5. To change the default Destination Folder, click **Change** and proceed to step 6. To leave the Destination Folder at its default, click **Next** and proceed to step 7.

Figure 4-9: Change Current Destination Folder



6. Click **OK**; you're returned to the Destination Folder dialog.
7. Click **Next**; the Ready to Install dialog opens.

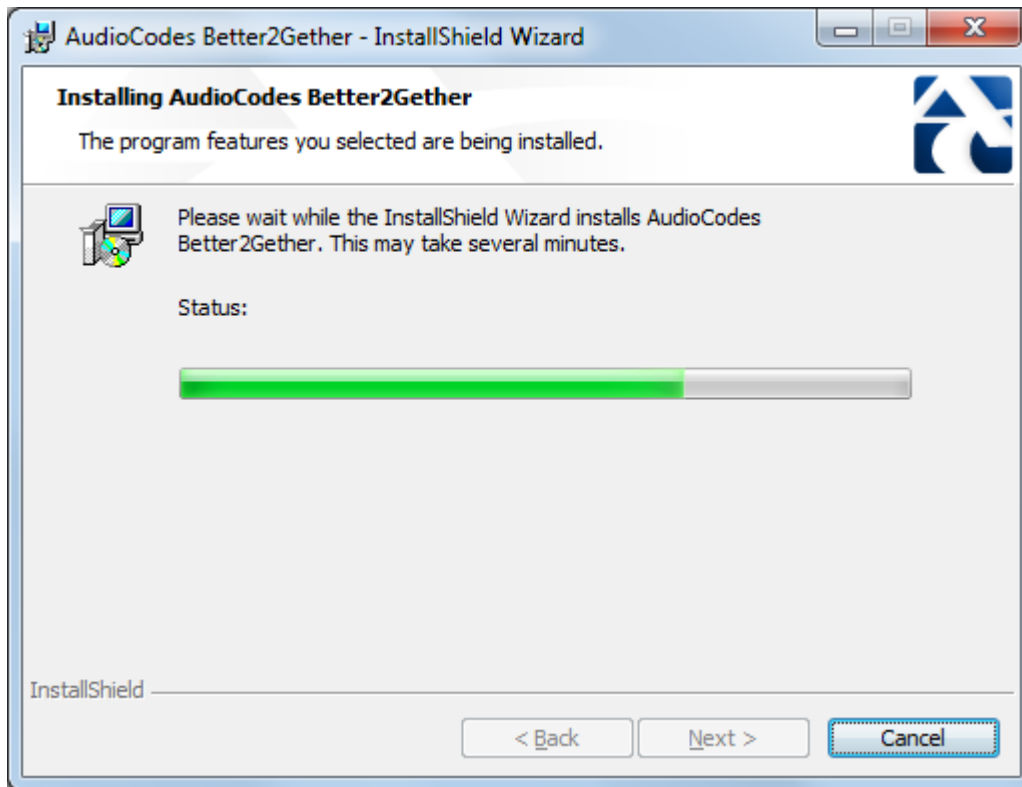
Figure 4-10: Ready to Install



8. Click **Install**; the Installing AudioCodes Better2Gether dialog opens indicating installation

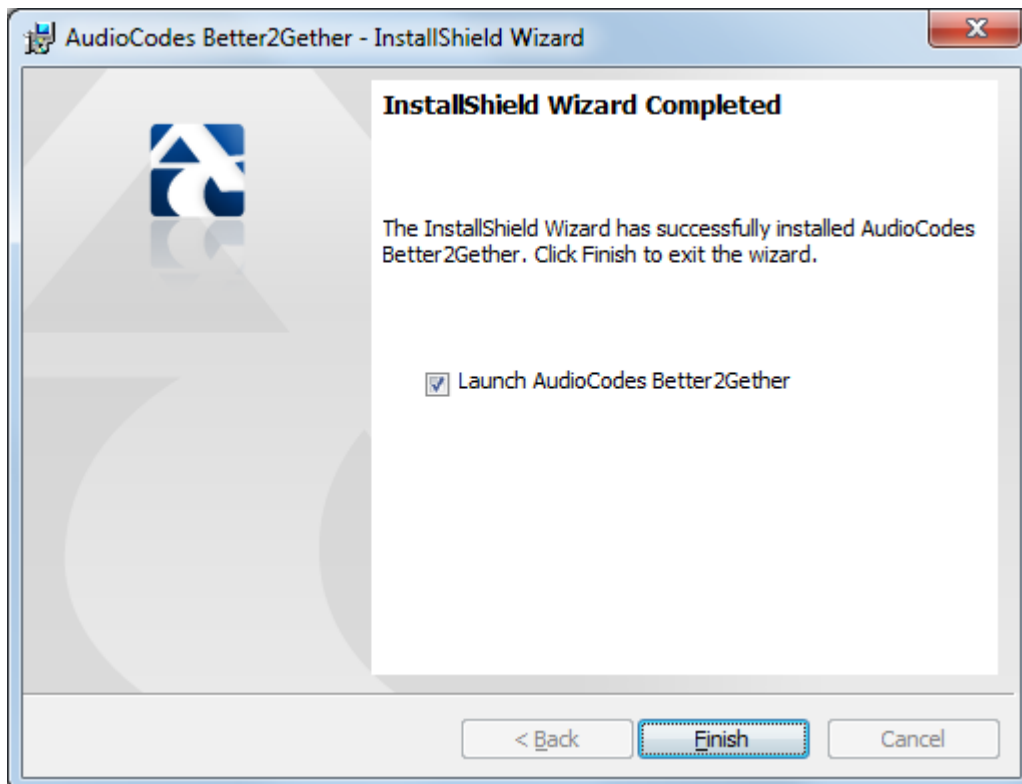
progress status.

Figure 4-11: Installing AudioCodes Better2Gether



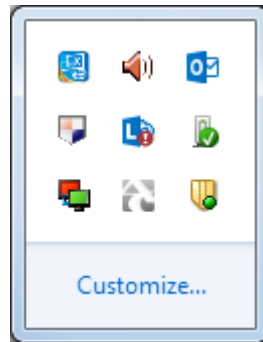
9. Wait until the following dialog is displayed:

Figure 4-12: InstallShield Wizard Completed



- Click **Finish** and then check your Windows taskbar and locate the newly displayed AudioCodes icon (AC) as shown below:

Figure 4-13: AudioCodes Icon in Taskbar

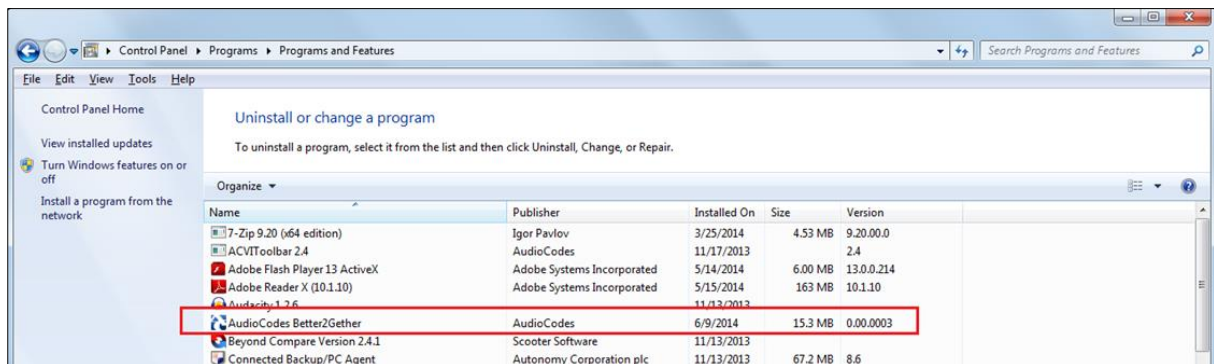


- Wait until the “Installing device driver software” process completes:



- Check your programs in the Control Panel > Programs. You should see:

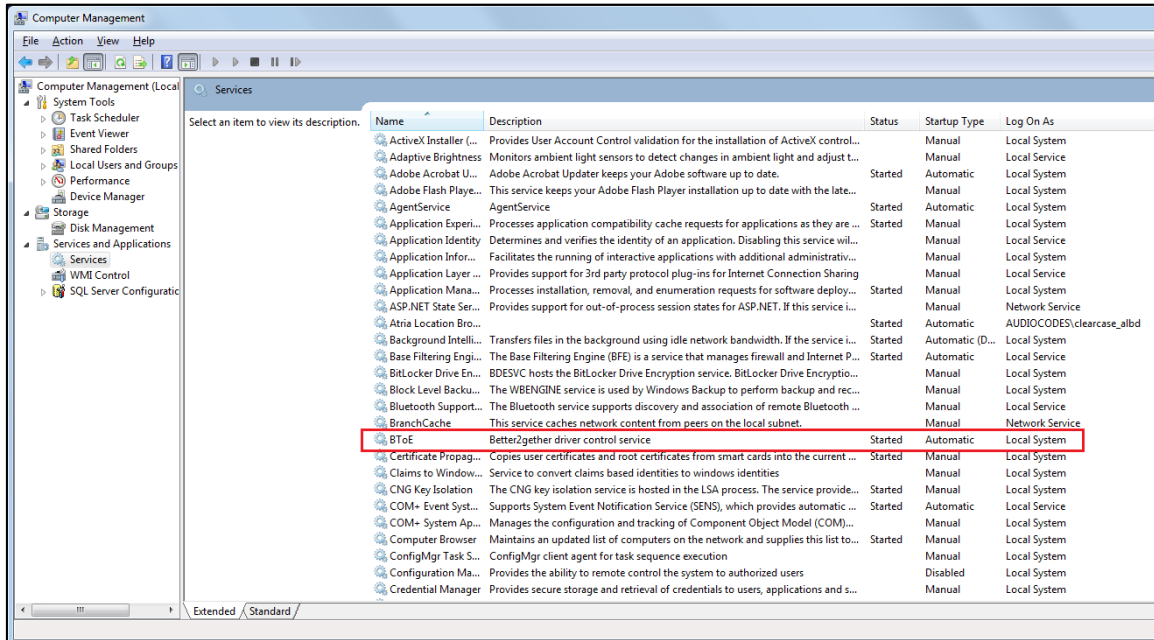
Figure 4-14: Control Panel>Programs>AudioCodes Better2Gether



You can use this entry in the Control Panel > Programs to uninstall.

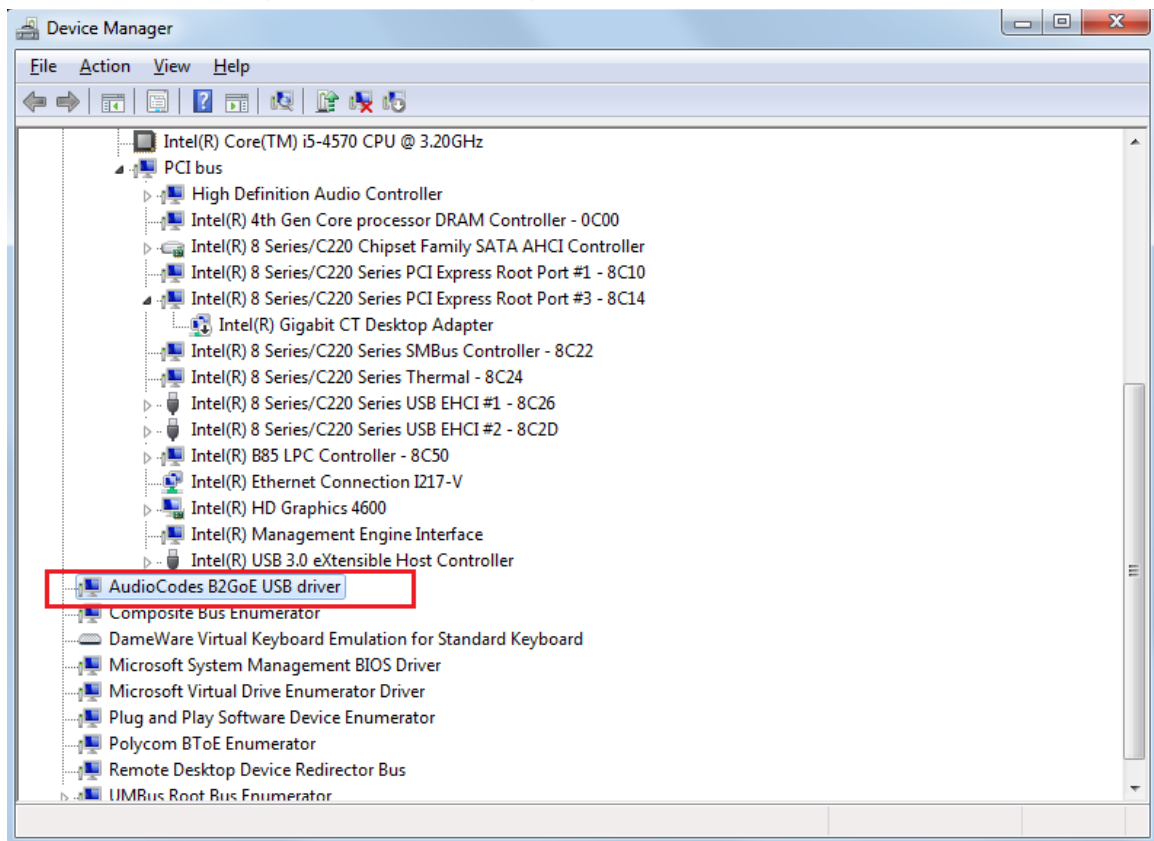
- Access Computer Management > Services and Applications and locate BToE:

Figure 4-15: Computer Management > Services and Applications



14. Access the Device Manager and locate 'AudioCodes B2GoE USB driver'.

Figure 4-16: Device Manager > AudioCodes B2GoE USB Driver



You've successfully installed the program.

4.12.3 Distributing the BToE PC Application msi Package

This section shows how to distribute the BToE PC application *msi* package. The name of the BToE PC application *msi* package is *AudioCodes BToE.msi*.



Do not change the file name. Changing it is disallowed.

To distribute the BToE PC application *msi* package:

15. Use the following command to install the *msi* package:

```
msiexec /I "AudioCodes BToE.msi" /qn
```

16. Use the following command to reinstall/upgrade the BToE PC application:

```
msiexec.exe /i "AudioCodes BToE.msi" REINSTALLMODE=voums  
REINSTALL=ALL /qn
```

If the *msi* filename was modified before installation, you may encounter issues with the reinstall/upgrade.

To troubleshoot:

17. Uninstall the previous BToE PC application installation: Use the following command to uninstall the full BToE PC application:

```
msiexec /X {1ED60F87-9DD1-4A3A-9A7F-BAA708F6FFA5} /L*v  
"c:\windows\temp\btoe.log" /qn /norestart
```

18. Refer to the instructions above. Reinstall without renaming the *msi* file.

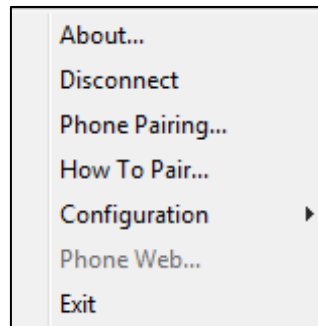
4.12.4 Making Sure BToE is Correctly Installed

This section shows how to make sure Better Together over Ethernet is correctly installed.

To make sure BToE is correctly installed:

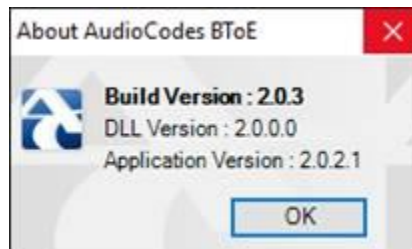
1. Click the **AC** (AudioCodes) taskbar icon; the following menu pops up:

Figure 4-17: Popup Menu



2. Select the **About...** menu option to verify the DLL and BToE version:

Figure 4-18: About AC BToE



4.12.5 Enabling BToE for Online Users in the Skype for Business Server

To enable BToE for an online user, the Skype for Business server must be configured to enable BToE.

To enable BToE for online users in the Skype for Business server:

3. Copy the file *LyncOnlineConnector.psd1* to the following path:
PS C:\Users\Administrator> Import-Module 'C:\Program Files\Common Files\Skype for Business Online\Modules\LyncOnlineConnector'
4. Configure the following parameters in the Skype for Business server:
 - \$credential = Get-Credential
 - \$credential
 - \$session = New-CsOnlineSession -Credential \$credential
 - Import-PSSession \$session
 - Get-CsTenant
 - Get-CsIPPhonePolicy

4.12.6 Configuring the BToE TCP Port

You can opt to configure a different BToE TCP port to the default 9999, depending on the requirements of your enterprise. For example, you may decide to change the BToE TCP port to 5000 because your enterprise is using the default port of 9999, and 5000 is available. This feature therefore provides enterprise administrators with more freedom in network administration.

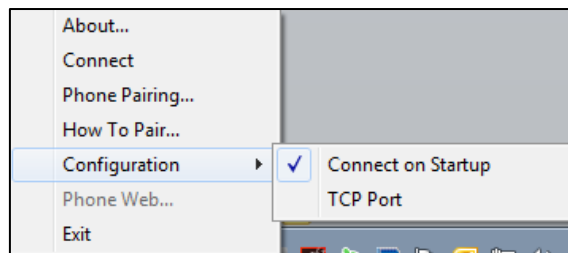


If you decide to change the default BToE TCP port, you must update *both* the PC/laptop *and* the IP phone with the new BToE TCP port number.

To change the BToE TCP port on the PC/laptop side:

5. Click the **AC** (AudioCodes) taskbar icon; the menu shown in [Figure 4-20](#) pops up.
6. Select **Disconnect** in the popup menu and then select **Configuration > TCP Port**.

Figure 4-19: TCP Port



7. From the AC BTOE TCP Port dialog that opens, configure the TCP Port:

Figure 4-20: AC BToE TCP Port



The valid range is 1 to 65535.

To change the BToE TCP port on the IP phone side:

- In the Configuration File, change the 'lync/BToE/TcpPortNumber' parameter. For example, lync/BToE/TcpPortNumber=5000.

4.12.7 Automatically Pairing the BToE PC/Laptop Application with the IP Phone

Pairing is *by default automatically* performed when the phone's PC port is connected to the PC/laptop 'behind' the phone, using a standard straight-through RJ-45 cable.

Manual pairing is *by default disabled*.

To enable manual pairing, see the next section.



Automatic pairing requires BToE PC/laptop application Version 2.x.

If the laptop after automatic pairing is disconnected and moved to another location, its speaker/headset becomes the audio device associated with the Skype for Business client.

If the laptop is *manually* paired and then relocated, Skype for Business audio will remain through the phone. It's therefore advisable to pair *automatically*.

4.12.8 Manually Pairing the BToE PC/Laptop Application with the Phone

This section shows how to manually pair the phone with the BToE PC/laptop application, using a pair code.

Before manually pairing, *enable* the manual pairing functionality by configuring the Configuration File parameter 'lync/BToE/pairing_mode' to **BOTH**.

Then follow this procedure:

1. Generate a pair code (see Section 4.12.8.1)
2. Connect the phone and BToE PC/laptop application using the pair code (see Section 4.12.8.3)



- If the IP address changes, you'll need to generate a pair code again.
- If you know the last pair code, you don't need to generate a new one. If you don't know it, see the next section.

4.12.8.1 Support for Citrix XenDesktop VDI

BToE supports Citrix XenDesktop virtual desktop infrastructure (VDI); BToE can connect a phone in a XenDesktop environment. To connect the phone to XenDesktop, set the configuration file parameter '/lync/BToE/pairing_mode' to **VDI**. BToE version 2.1.8 must be installed. BToE runs in the following XenDesktop modes:

- **Persistent Sessions.** In this mode, a dedicated VM is used per user; it's always active.
- **Non-Persistent Session.** In this mode, the user is connected to an available VM in the pool. After the user logs off, the machine can be used by another user. When the user is connected, their settings and data are restored.

After the user is connected to the XenDesktop environment and signs-in to Skype for Business, all BToE functions are available. BToE runs on Xen Desktop, paired manually to the phone. The user's pc running the XenDesktop client can be connected directly to the phone. The BToE application runs on XenDesktop and is paired via manual IP pairing. During a video call, audio is routed from the XenDesktop client to the phone.



- HDI optimization must be disabled for BToE to function correctly with Citrix XenDesktop.
- XenDesktop (for remote users) runs on Windows 10.
- Thin client is not supported.

4.12.8.2 Manually Generating a Pair Code

This section shows how to manually generate a pair code.

To manually generate a pair code:

- On the phone, press the MENU hard key and in the Menu screen that is displayed, choose **BToE**; the BToE pair code is displayed:



- This is the pair code that will be used by the BToE PC/laptop application to pair the PC/laptop with the phone for unified communications.
- Make a note of this pair code for reference when connecting the phone with the BToE PC/laptop application.

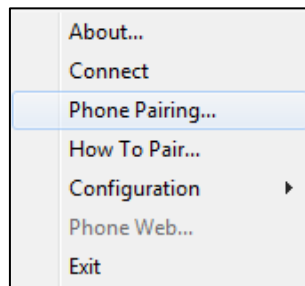
4.12.8.3 Connecting the IP Phone with the BToE PC/Laptop Application

This section shows how to connect the IP phone with the BToE PC/laptop application.

To connect the two:

1. Open the AudioCodes BToE Connect dialog: Click the BToE client icon placed on your taskbar after installation; the following popup menu opens.

Figure 4-21: Popup Menu



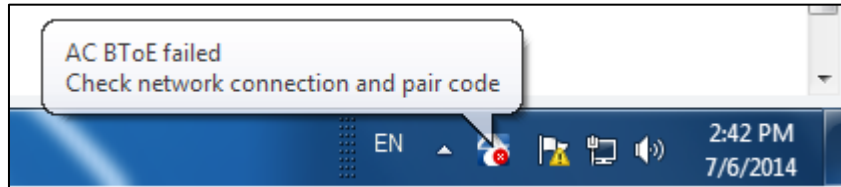
2. Select the **Phone Pairing** option

Figure 4-22: Phone Pairing



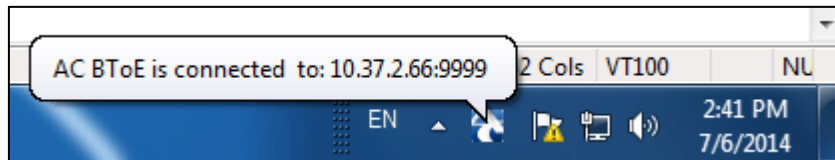
3. In the 'Enter your phone pairing code' dialog, enter the pair code that you generated as shown in Section 4.12.8.1; the **OK** button is activated after 8 characters are entered.
4. Click **OK**; BToE is activated. If a communication error occurs or the wrong pair code was entered, the following icon indication appears:

Figure 4-23: AC BToE Failed Indication



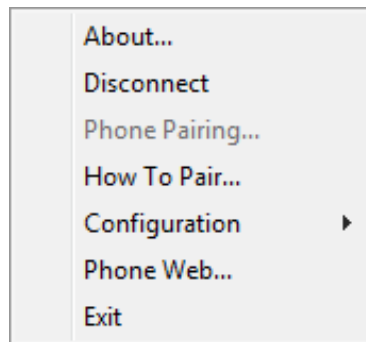
- When BToE is successfully connected, view the following icon indication:

Figure 4-24: AC BToE is Connected Indication



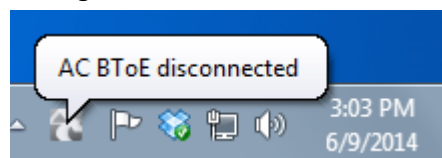
- When BToE is in 'Connected' state, the popup menu shows the **Disconnect** menu item and the **Phone Pairing** menu item is deactivated:

Figure 4-25: Popup Menu: 'Disconnect' Enabled, 'Phone Pairing' Disabled



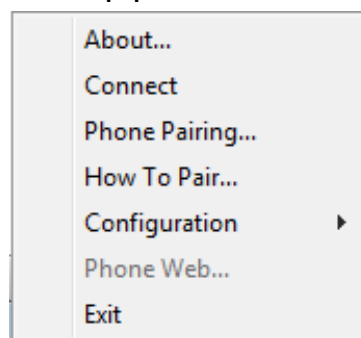
- After selecting the **Disconnect** menu option, the 'AC BToE Disconnected' indication is displayed:

Figure 4-26: BToE Disconnected



- From the popup menu as well you can see if BToE is disconnected:

Figure 4-27: Popup Menu: BToE Disconnected





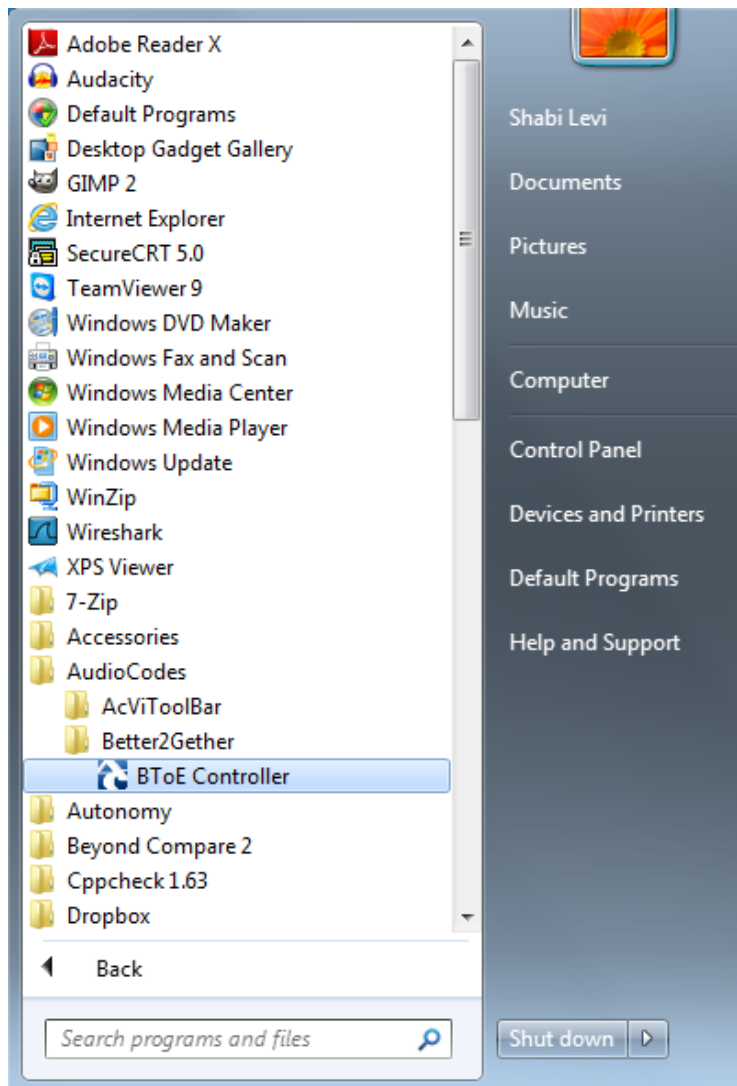
When BToE is connected, you can select the **Phone Web** menu option to open the phone's Web interface.

- Use the table below as reference when determining BToE's connection state from the taskbar icon.

Taskbar Icon	BToE's connection state
	BToE is connected
	BToE is disconnected
	BToE is connected but a failure is preventing a correct connection. The failure can be a network problem or the wrong pair code was defined.

- From the click popup menu, you can select the **Exit** option; the BToE PC application stops. You can activate the application again from the Start menu as shown in [Figure 4-31](#).

Figure 4-28: Start > Programs > AudioCodes > BToE Controller



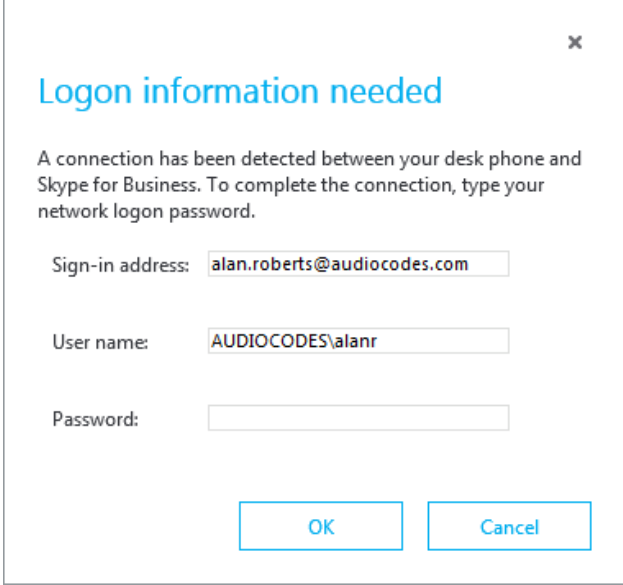
4.12.9 Connecting the Skype for Business Client with the IP Phone

This section shows how to connect the Microsoft Skype for Business client with the IP phone using the Skype for Business login screen.

To connect the two:

- Enter your credentials in the Sign-in request prompt, and click **OK**.

Figure 4-29: Sign-in Request Prompt



Logon information needed

A connection has been detected between your desk phone and Skype for Business. To complete the connection, type your network logon password.

Sign-in address:

User name:

Password:



- Signing in via the Skype for Business client is flexible with respect to user name format: It can be entered in NetBIOS format (domain\user, for example, companyname\johnb) as well as User Principal Name (UPN) format (user@domain, for example, johnb@companyname.com).
 - BToE version 2.1.8 must be installed.
 - The configuration file parameter 'lync/BToE/use_UPN_str' must be configured to 1 (Default: 0).
- Primary Device cannot be changed in the Skype for Business PC client during a call. When the phone is in idle mode (not in a call), the PC application must be disconnected in order to change Primary Device.


4.12.10 Making Sure IP Phone/ Skype for Business Client are Paired

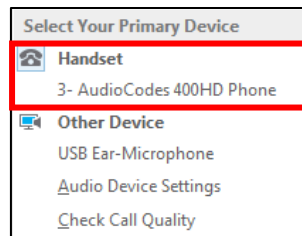
This section shows how to make sure you successfully paired your IP phone with the Skype for Business client.

4.12.10.1 Making Sure the Skype for Business Client is Paired

You can make sure the Skype for Business client is paired with the IP phone.

To make sure the Skype for Business client is paired with the IP phone:

1. In the Skype for Business application, in the lowermost left corner of the screen, click the Select Primary Device icon ; the following popup menu opens:



2. Make sure **Handset AudioCodes 400HD Phone** is selected.



- When answering an incoming *video* call with a paired phone, the call is established. The default device is the PC speaker/microphone rather than the phone. Subsequent audio calls will be unaffected; the paired phone will still be the default device.
- In pairing mode, the user (Skype for Business PC client /phone) can perform up to two concurrent calls (incoming/outgoing). See the *Release Notes*.

4.12.10.2 Making Sure the Phone is Paired with the PC/Laptop

You can determine from the phone's idle screen if the phone is paired with the Skype for Business client.

- After connecting the phone's PC port to the PC/laptop 'behind' the phone using a standard straight-through RJ-45 cable, the notification **Better Together Activated** pops up and then disappears. Two interlocked rings displayed in the idle screen indicates that the phone is paired.



The icon shown above is that displayed in the 450HD and C450HD phone's idle screen. The concept is identical for all phones, though size and color differ from one to another.

- If the idle screen does not display two interlocked rings, this indicates that the phone is not paired with the PC/laptop.



4.12.11 Configuring Mode of Operation for Phone-PC Pairing

A Configuration File parameter 'pairing_mode' can be used to configure the mode of operation for pairing the phone with the PC.

To configure the pairing mode:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-10: Pairing Mode Parameter

Parameter Name	Description
lync/BToE/pairing_mode	<ul style="list-style-type: none"> ■ AUTOMATIC mode When the PC port of the phone is connected directly to the PC, the phone is <i>automatically</i> paired with the PC -OR- ■ BOTH mode <ul style="list-style-type: none"> • When the user manually enters the pairing code into the PC application and the PC is connected to the network or directly connected to the phone's PC port, the phone is <i>manually</i> paired -or- • When the PC port of the phone is connected directly to the PC, the phone is <i>automatically</i> paired with the PC

The PC application does not have a Configuration File parameter, so if the user manually enters a pairing code into the PC:

- the PC application toggles every second between MANUAL and AUTOMATIC mode
- the PC waits for automatic pairing (listens to UDP port 9999 to determine if a phone is connected directly to the PC).



If a phone is detected and automatic pairing is established, the old pairing code is removed from the Windows registry.

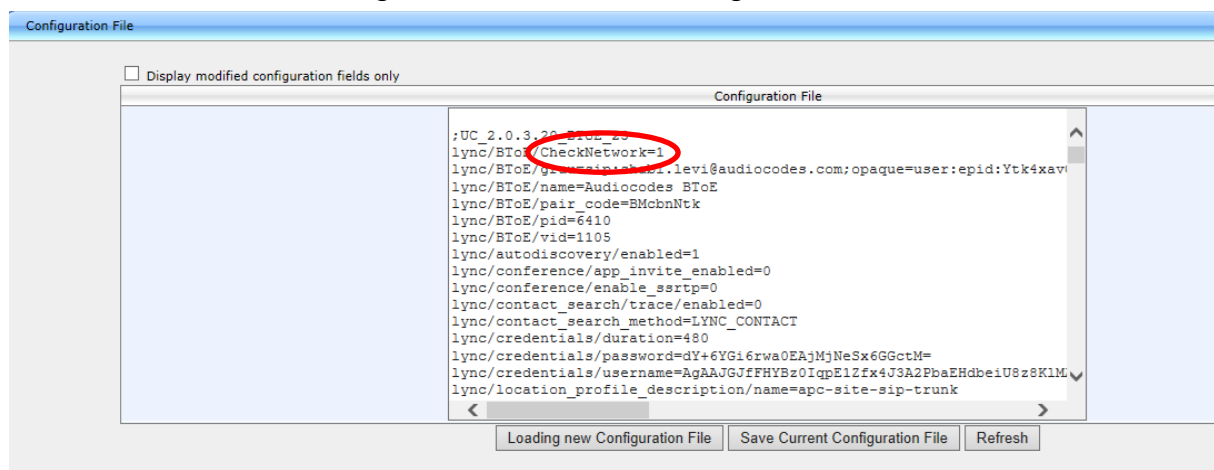
4.12.12 Pairing Across Different Subnets

Pairing across different subnets is enabled by default. The 'lync/BToE/CheckNetwork=0' field in the configuration file enables it.

To make sure pairing across different subnets is enabled:

1. In the Web interface, access the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**).

Figure 4-30: Web Interface - Configuration File



2. Locate the 'CheckNetwork' field. Make sure it is set to its default of **0**.
 - 0** = pairing across different subnets enabled
 - 1** = pairing across different subnets disabled

4.12.13 Troubleshooting

If a BToE issue occurs such as a pairing issue, or if a BToE error notification is received, access the logged issue on the pc on which BToE is installed, in the location equivalent to the following location:

C:\Program Files (x86)\AudioCodes\Better2Gether USB Over Ethernet\log

Use the details of the logged issue to inform you how to troubleshoot.

Also refer to AudioCodes' video tutorial about BToE, at <http://youtu.be/fZZ0nPWJ7uM>.

4.13 Device Duo

The Device Duo mode feature enables AudioCodes' IP phones to be configured as a *paired audio device*. The feature allows users to use their phone not only as a desk phone but also as a loudspeaker over a network that supports telephony operations such as accept / end calls, in addition to supporting basic audio operations.



- The Device Duo feature is currently supported for pairing AudioCodes' IP phone *with Microsoft's Teams application*.
- The Device Duo feature is currently also supported for pairing AudioCodes' phones with Zoom client application for basic functionalities.
- The feature is currently supported for Windows 10.
- The screens shown in these RNs are of the C450HD. The screens of the RX50, 450HD and 445HD are similar with insignificant differences. They're not shown here unless differences are significant.
- The screen of the C450HD is a touch screen, so 'touch' in this document is interchangeable with 'press'.

4.13.1 Benefits

The Device Duo allows users to use their IP phone not only as a phone but rather as a 'smart' audio device that *combines handset with loud speaker*.

The 'smart' audio device allows telephony controls such as call start and call end in addition to audio device controls such as volume up and down and mute but it is *not limited to these controls*.

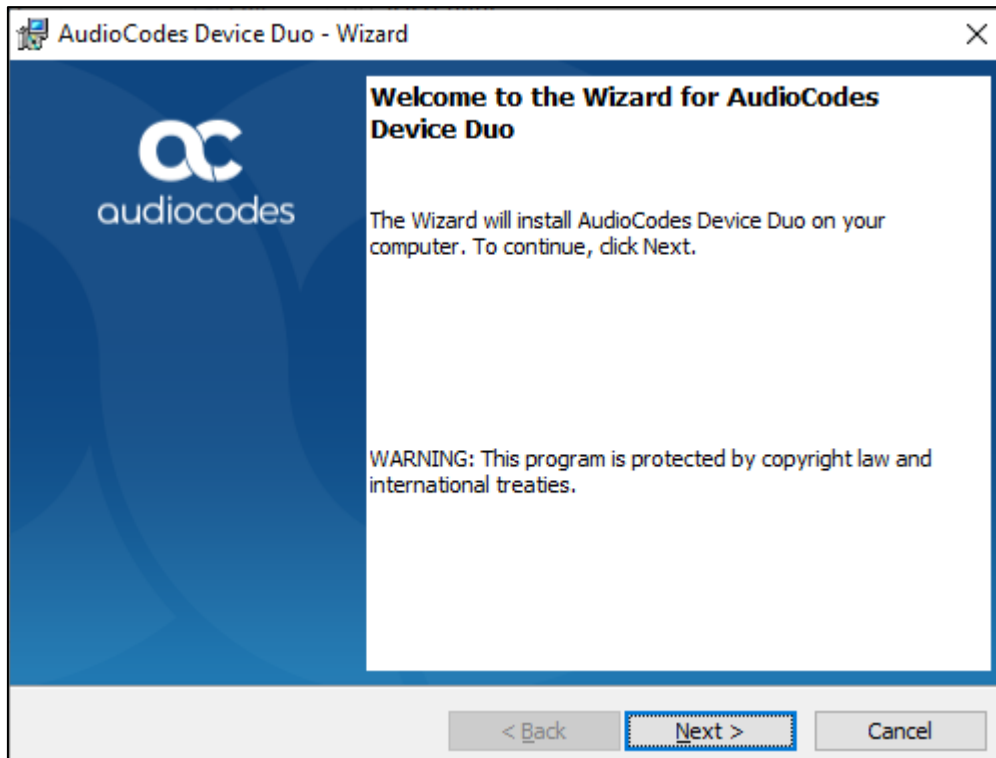
The feature is based by standard implementation on the generalized portion of BToE capabilities to allow other third party desktop applications to use the device as a loud speaker.

4.13.2 Installing the Device Duo on the PC

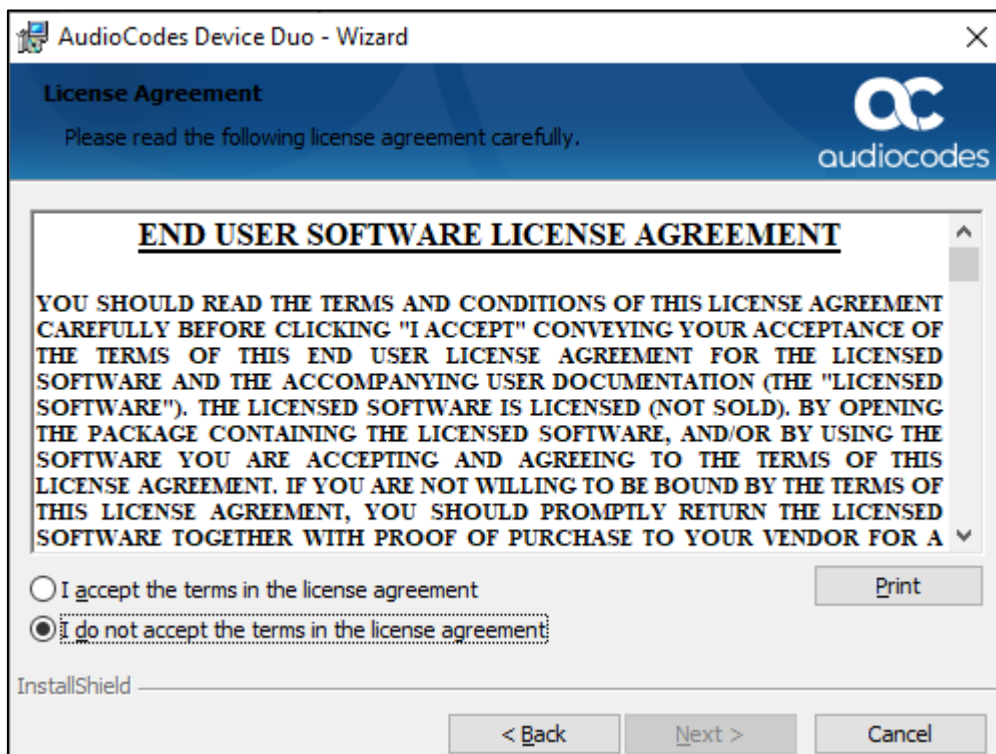
AudioCodes' Device Duo Wizard facilitates installation of the controller on your PC. Before installing the Device Duo, uninstall BToE if it's installed.

To install the Device Duo:

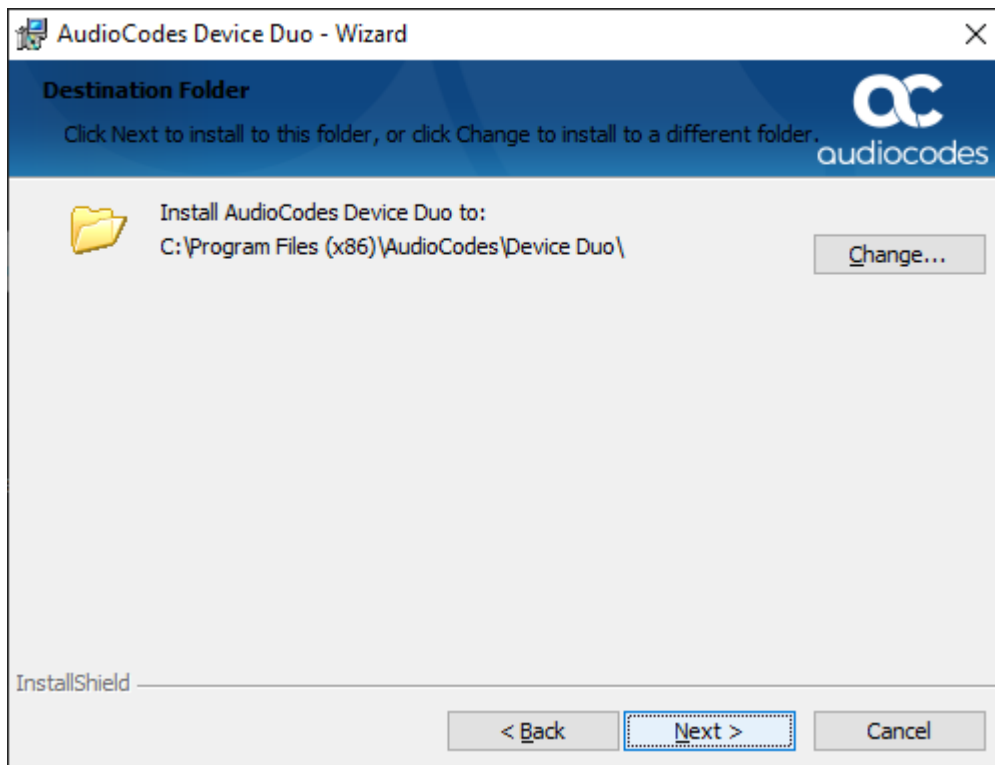
1. Run the executable file *AudioCodes Device Duo.exe* locally (from the user's PC).



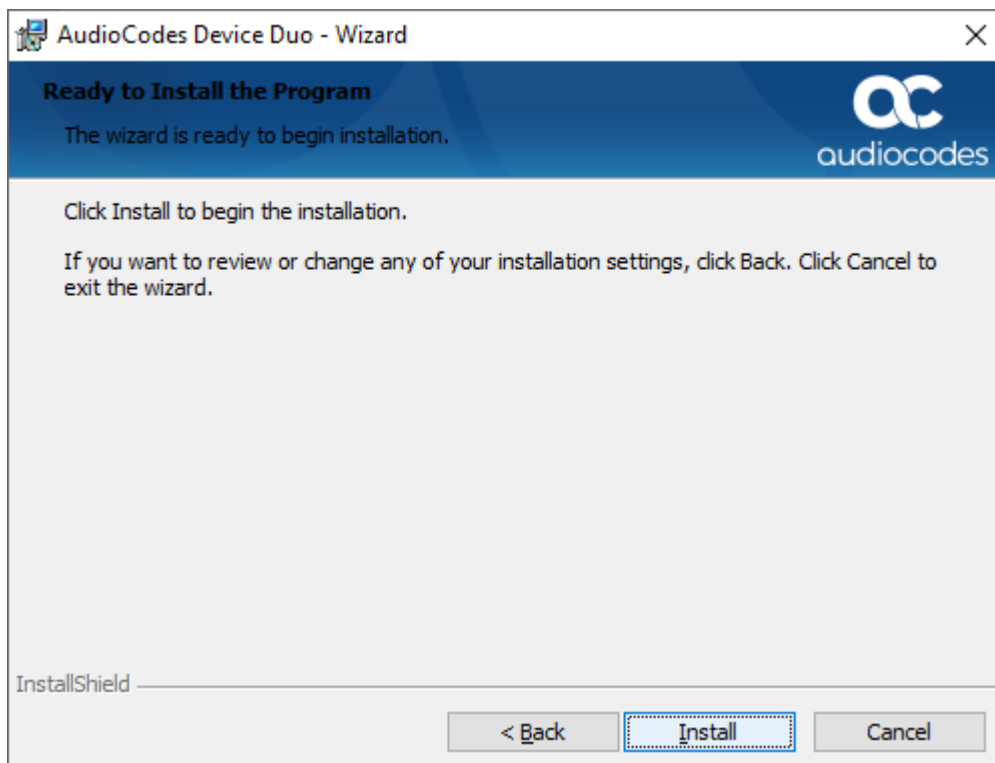
2. In the wizard that opens, click **Next**.



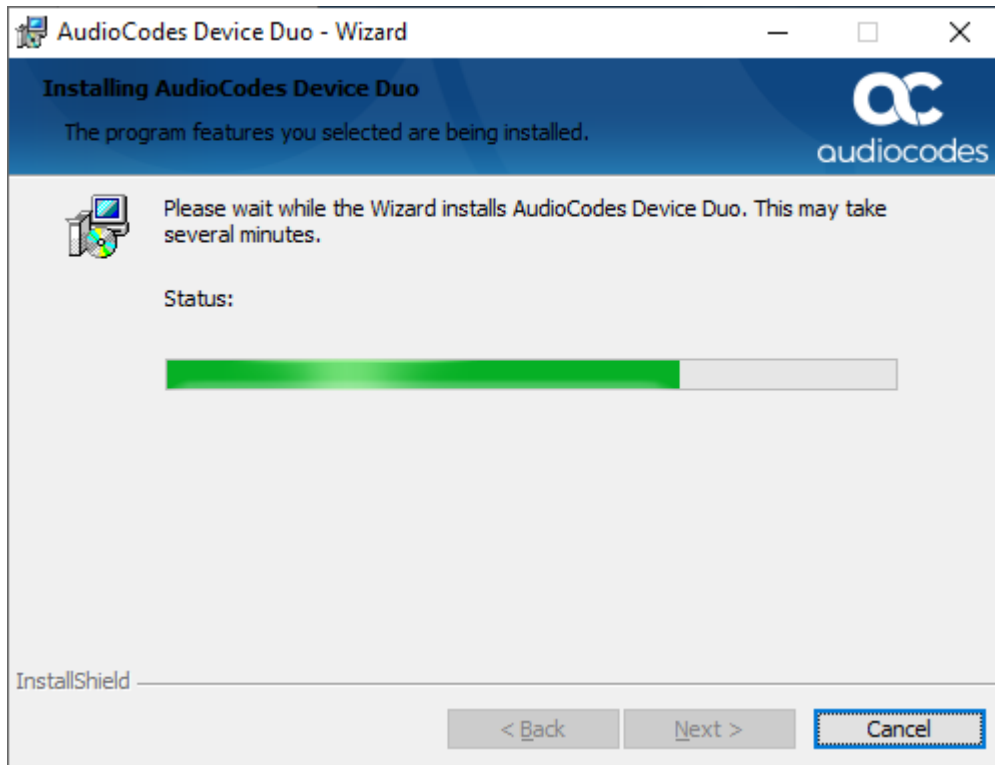
3. Accept the terms and click **Next**.



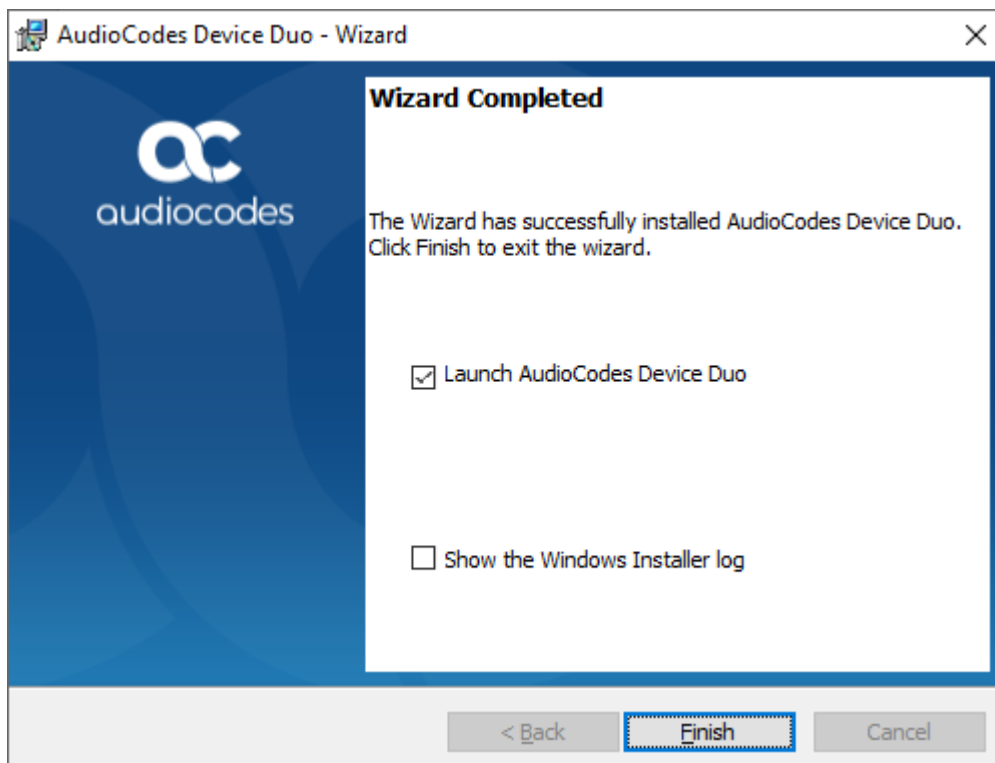
4. Note the installation path and click **Next**.



5. Click **Install** or click **Back** to review or change settings – or **Cancel** to exist the wizard..



6. Wait for the installation process to complete.



7. Click **Finish**; the installation is complete.

4.13.3 Making Sure Device Duo is Correctly Installed

This section shows how to make sure Device Duo is correctly installed.

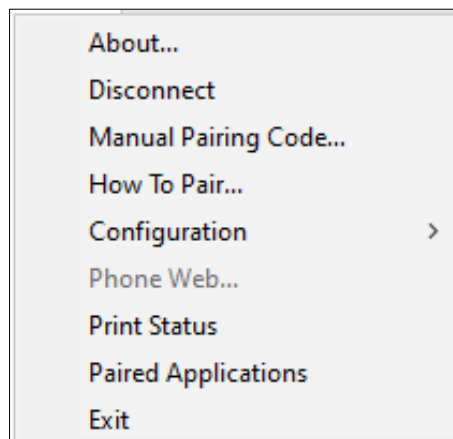
To make sure Device Duo is correctly installed:

1. After running the application, click the **AC** Device Duo taskbar icon.



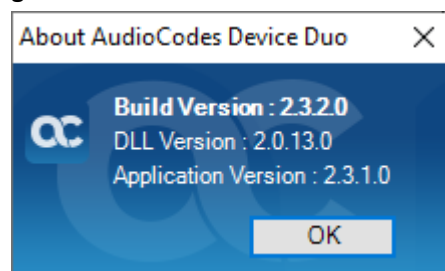
2. View the following menu that pops up:

Figure 4-31: Popup Menu



3. Select the **About...** menu option to verify the DLL and Device Duo version:

Figure 4-32: About AudioCodes Device Duo



4.13.4 Pairing the Device Duo Application with the IP Phone

This section shows how to pair the Device Duo application with the IP phone.

Pairing can be done by:

- **Pairing code**
 - Set configuration file parameter 'lync/BToE/pairing_mode' to **BOTH**
By default, it's configured to **AUTOMATIC** for all devices except RX50; for RX50, it's by default configured to **BOTH**.
- **Automatic pairing mode**
 - (RX50 and RXV100Hub) Set configuration file parameter 'lync/BToE/pairing_mode' by default configured to **BOTH** and set 'system/duo/advertise_over_network' to **1** (see Section 4.13.4.2 for more information)

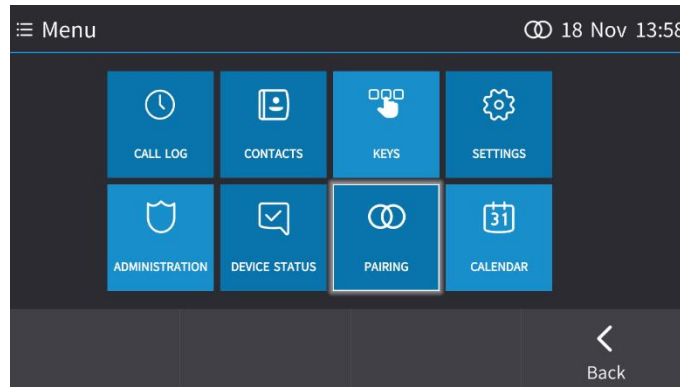
- By connecting the phones by cable to PC port. (see Section 4.13.4.3 for more information)

4.13.4.1 Pairing Code

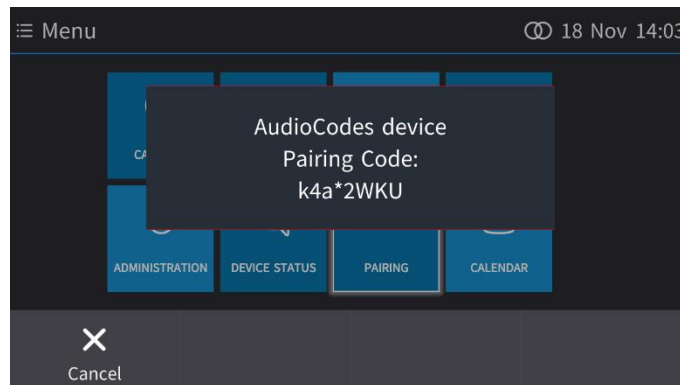
This section shows how to pair the Device Duo app with the phone using a pairing code generated by the phone as a unique ID of the device.

To pair:

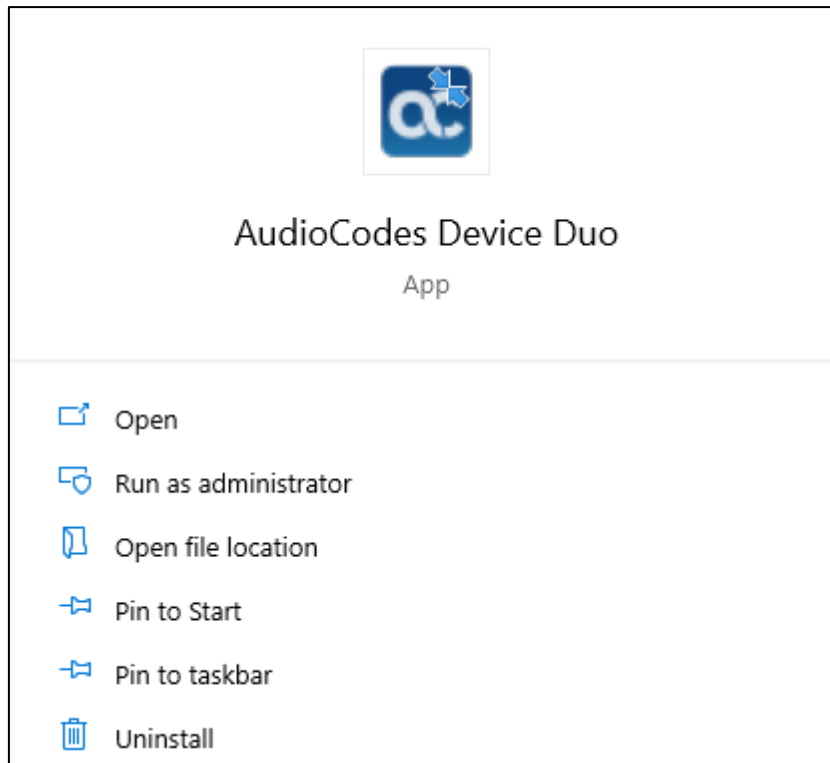
1. Press the MENU key on the phone:



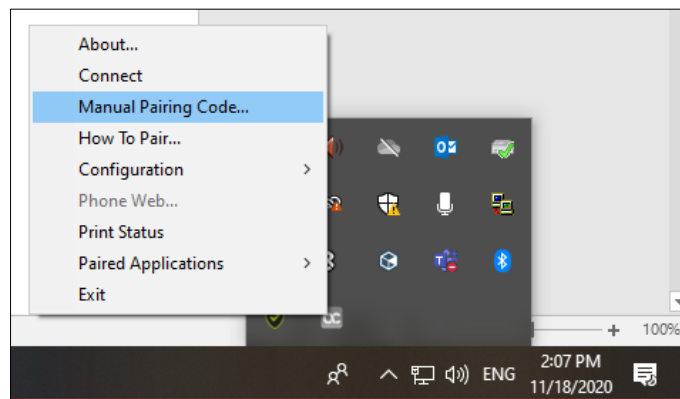
2. In the Menu screen, touch **Pairing**.



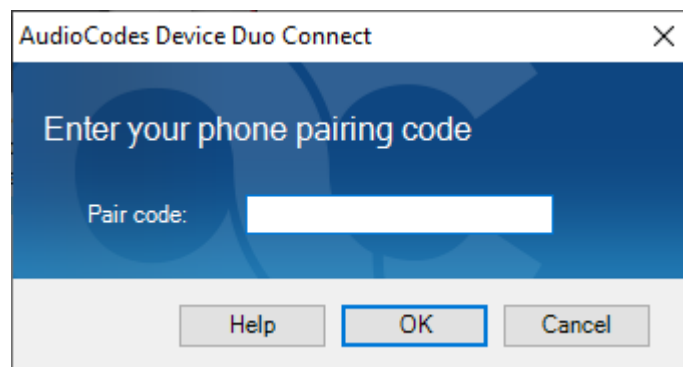
3. Make a note of the pairing code, in this example, **k4a*2WKU**
4. On the PC, open the Device Duo:



5. In the systray, click the **AC Device Duo** icon.



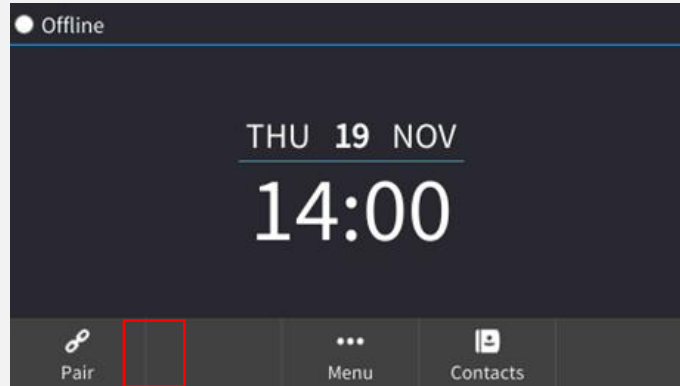
6. Select **Manual Pairing Code...**



7. In the 'Pair code' field, enter the pairing code **k4a*2WKU** you noted earlier and click **OK**; view on the phone the briefly displayed message **Pairing activated**; the **AC Device Duo** icon is now highlighted and indicates **AC Device Duo is now connected to <Phone IP Address>**.



If the RX50 is signed in with a Skype for Business user, the **Menu** softkey will be displayed and pairing will be available as explained above. If the RX50 Skype for Business user is signed out and 'voip/account/primary_type' OR 'voip/account/secondary_type' is **TEAMS_DESKTOP**, then a **Pair** softkey will be displayed for pairing. Since the RX50 default value is **TEAMS_DESKTOP**, the **Pair** softkey is displayed when signed out.



4.13.4.2 Automatically Pairing the RXV100Hub with the RX50

This section shows how to automatically pair the Device Duo app on the RXV100Hub with the RX50 conference phone.

RXV100Hub must already be set up in the same subnet (see the *RXV100Hub Installation & Getting Started Guide* for more information).

Make sure configuration file parameters

- 'lync/BToE/pairing_mode' is set to **BOTH** (default)
- 'system/duo/advertise_over_network' is configured to **1** (default)



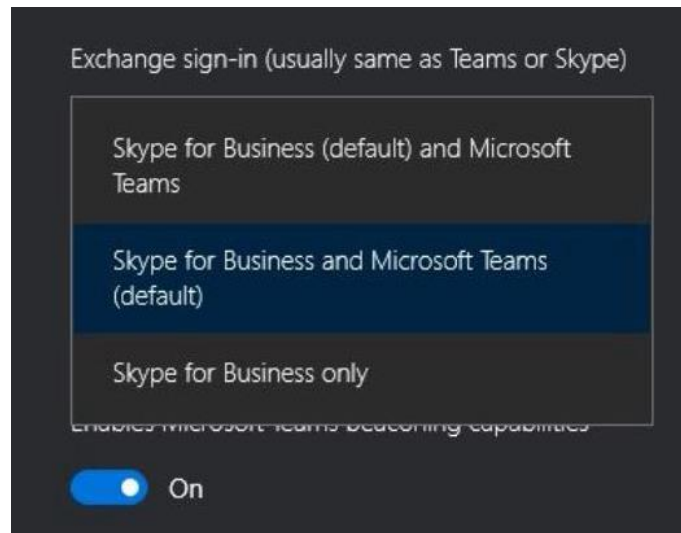
- Before pairing your RX50, upgrade it with firmware version 3.4.6.231 (see Section 5.1 for detailed information).
- After the upgrade, restore the RX50 to defaults (MENU>**ADMIN**>**Restore Defaults**). [Applies only to customers who want to connect to the RX50 after purchasing the RX50 *not as part of the MTR*].

4.13.4.2.1 Providing MTR Credentials

When the RXV100Hub is switched on for the first time, Microsoft Teams Rooms (MTR) credentials must be provided to sign in.

To provide MTR credentials:

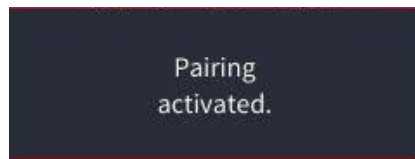
1. In the RXV100Hub Setup Wizard, select Keyboard (English - US) and Region.
2. Accept the license agreement and select **Next**.
3. Under 'Supported meeting mode', select **Skype for Business and Microsoft Teams** (default).




4. Enter the Teams Rooms credentials and select **Next > Next > Next > Finish**.


4.13.4.2.2 Pairing the RXV100Hub with the RX50

After completing the previous steps, RXV100Hub and the RX50 are *automatically paired*.



On the RX50 screen, view **Pairing activated**. View also the pairing icon  in the top right corner and **MTR Audio** (instead of **Offline**) in the top left corner. After they're paired, log in to the RXV100Hub as Administrator and set RX50 to be its default audio device.


To log in to the RXV100Hub as Administrator

1. From the **Main Menu**, touch **More**, and then touch  **Settings**.
2. Enter the Administrator password, and then touch **Yes**.
3. Select **Windows Settings**, and then select the Administrator account displayed in the lower left corner; a prompt appears requesting Administrator credentials.
4. Enter the credentials; after successful validation, you're logged in as Administrator to manage the RXV100Hub. Note that the default Administrator password is **sfb**.



If prompted to change the Administrator password, enter **12345678**, confirm and then execute the `change_admin_password.exe` script from the **<admin> Windows** account; the password is re-set to **sfb**.

To set the RX50 as the default audio device:

5. After logging in to the RXV100Hub as Administrator (see next section for details), select **More** and then select  **Settings**; enter the Administrator password (default is **sfb**) and press **Yes**.
6. Under **Peripherals**, select **AudioCodes RX50** as 'Microphone for Conferencing', **Speaker** for 'Conferencing' and 'Default Speaker', and then press **Save** and **Exit**.

4.13.4.3 Automatic Pairing using PC Port



This section is not relevant to RX50 as there is no PC port on the device.

Before performing pairing:

- Make sure configuration file parameter 'lync/BToE/pairing_mode' is configured to **AUTOMATIC** (default).
- Make sure the phone's PC port is connected to the PC as follows:



4.13.5 Configuring Mode of Operation for Phone-PC Pairing

The configuration file parameter 'pairing_mode' can be used to configure the mode of operation for pairing the phone with the PC with Device Duo.

To configure the pairing mode:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-11: Pairing Mode Parameter

Parameter Name	Description
lync/BToE/pairing_mode	<ul style="list-style-type: none"> ■ AUTOMATIC mode When the PC port of the phone is connected directly to the PC, the phone is <i>automatically</i> paired with the PC Device Duo application -OR- ■ BOTH mode <ul style="list-style-type: none"> ● When the user manually enters the pairing code into the Device Duo application on the PC, and the PC is connected to the network or directly connected to the phone's PC port, the phone is <i>manually</i> paired -or- ● When the PC port of the phone is connected directly to the PC, the phone is <i>automatically</i> paired with the PC application.

- The PC application does not have a Configuration File parameter, so if the user manually enters a pairing code into the PC:
 - the PC application toggles every second between MANUAL and AUTOMATIC mode
 - the PC waits for automatic pairing (listens to UDP port 9999 to determine if a phone is connected directly to the PC).

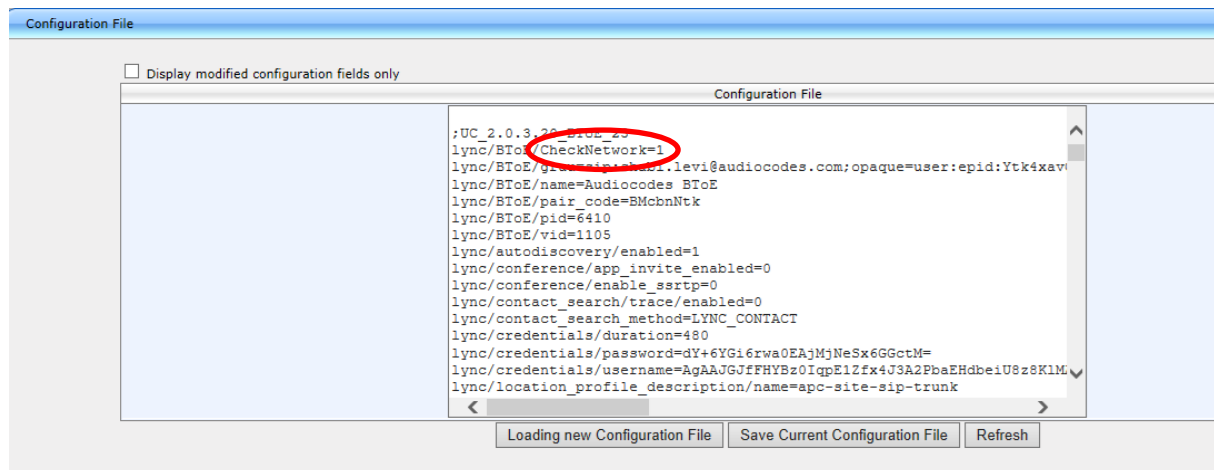
4.13.6 Pairing Across Different Subnets

Pairing across different subnets is enabled by default. The 'lync/BToE/CheckNetwork=0' field in the configuration file enables it.

To make sure pairing across different subnets is enabled:

1. In the Web interface, access the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**).

Figure 4-33: Web Interface - Configuration File



2. Locate the 'CheckNetwork' field. Make sure it is set to its default of **0**.

0 = pairing across different subnets enabled

1 = pairing across different subnets disabled

4.13.7 Troubleshooting

If an issue occurs such as a pairing issue, or if an error notification is received, access the logged issue on the PC on which the Device Duo is installed, in the location equivalent to the following location:

C:\Program Files (x86)\AudioCodes\Device Duo\log

The Application Controller logs are located here:

\AppData\Local\DeviceDuo\log

Use the details of a logged issue to inform you how to troubleshoot.

4.14 Boss Admin

This section shows how to configure an Admin (delegate). Each phone can support up to five Bosses or Admins. One Boss can have up to five Admins. One Admin can have up to five Bosses. A many-to-many configuration is also supported. Admins are configured on the Boss's phone. For information on using the feature, see the *User's Manual*.

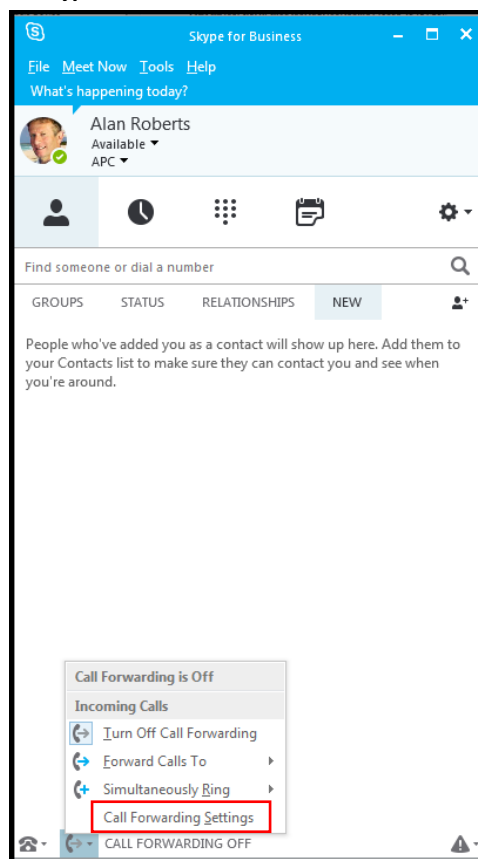


- The Boss Admin feature does not apply to the HRS.
- Make sure your environment allows delegation for the user. If it doesn't, configuration will not work. All users must be allowed to configure all users as delegates.
- To remove an Admin, the Boss must remove the Admin in the 'Call Forwarding – Delegates' screen (open the Skype for Business client > click **Call Forward Settings** > click **Edit my delegate members** > select the Admin > click **Remove**). It's not enough to turn off call forwarding.
- The 'Forward unanswered calls' parameter on the phone allows users to configure the phone to send unanswered calls to voicemail or to a phone number and to define the unanswered timeout. Timeout can be set from 5-60 seconds in 5 sec resolution.

To configure an Admin:

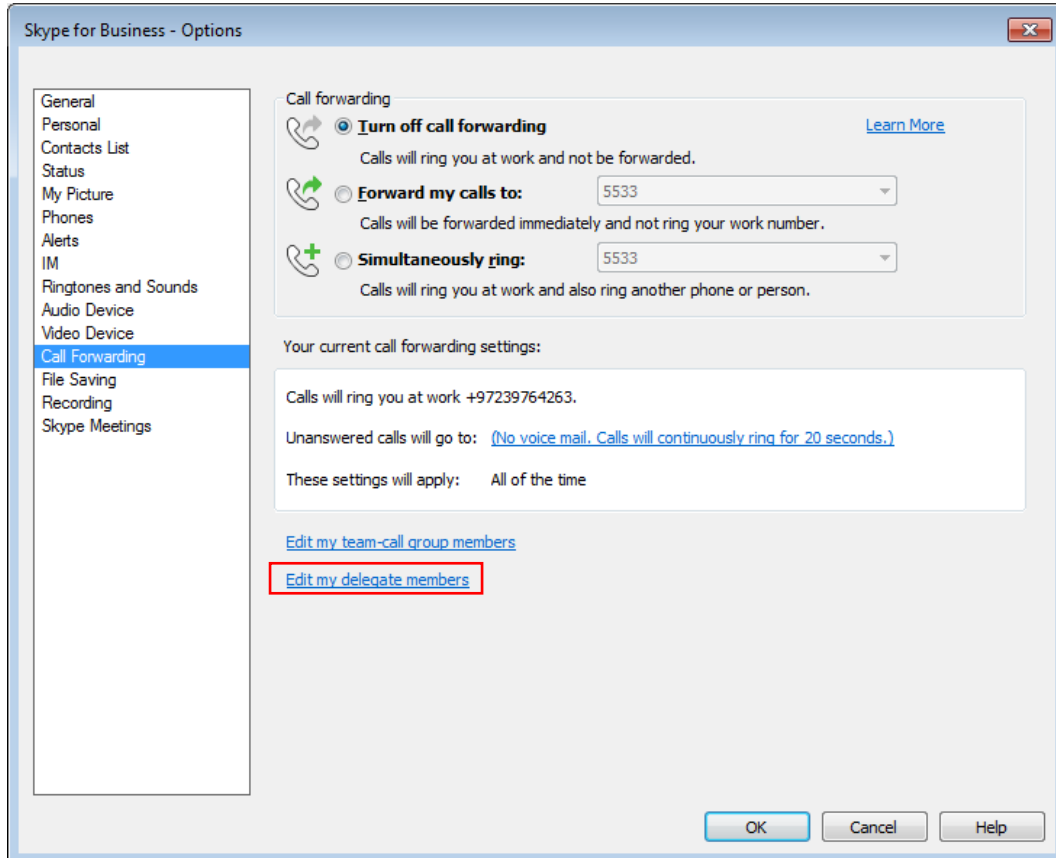
1. In Boss's Skype for Business client, click the handset icon and from the menu that opens, choose the **Call Forwarding Settings** option, as shown in [Figure 4-34](#).

Figure 4-34: Skype for Business Client – Call Forwarding Settings



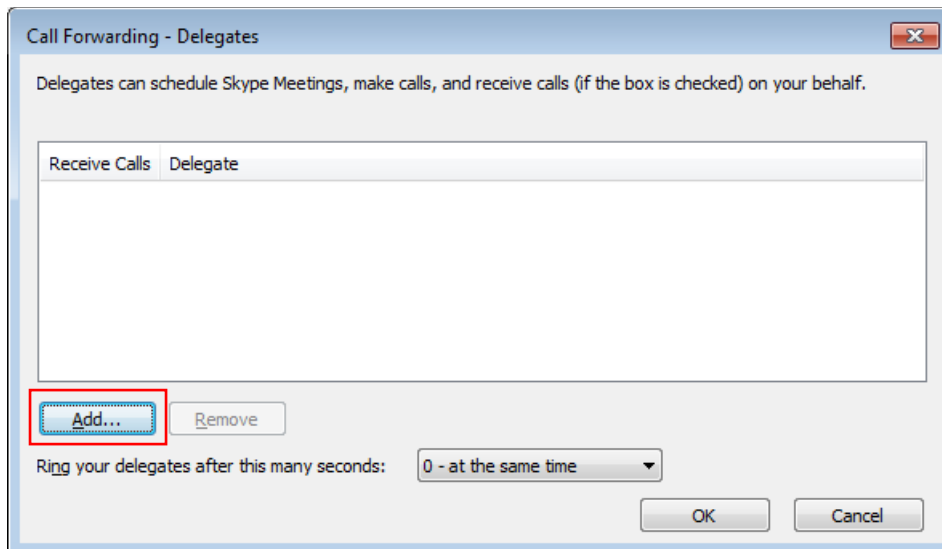
2. In the screen that opens, shown below, click the **Edit my delegate members** link.

Figure 4-35: Skype for Business Client - Edit my delegate members



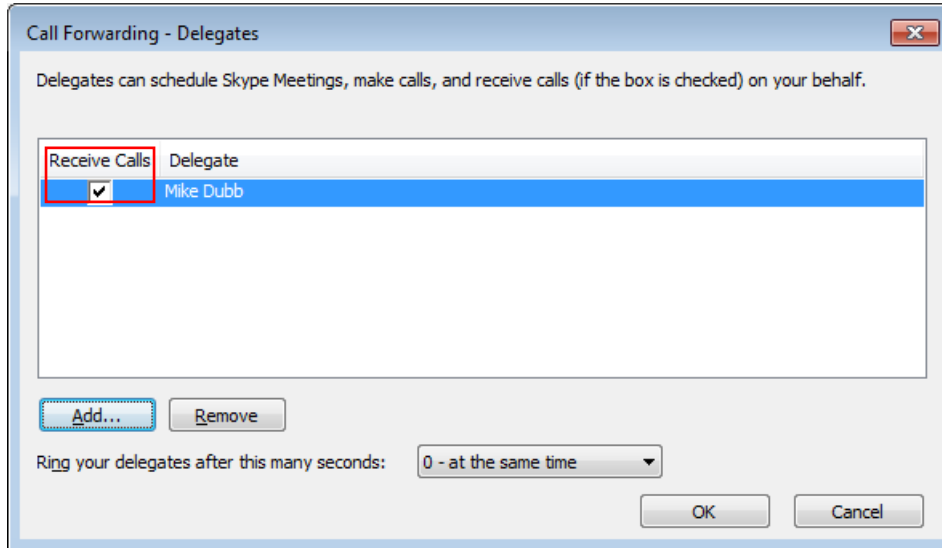
3. In the screen that opens, shown below, click **Add** and add a contact from the list.

Figure 4-36: Skype for Business Client – Call Forwarding – Add Delegates



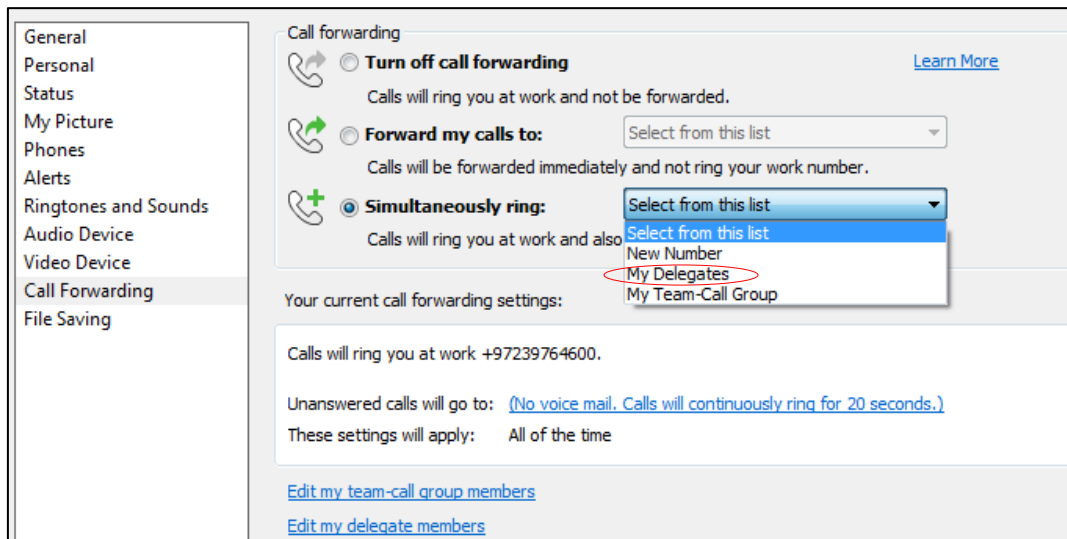
4. Adjacent to the added delegate in the screen that opens (Mike Dubb, shown below), make sure the **Receive Calls** option is selected:

Figure 4-37: Skype for Business Client – Call Forwarding – Added Delegate - Receive Calls



5. Click **OK**.
6. Select the **Simultaneously ring** option and configure it to **My Delegates**.

Figure 4-38: Skype for Business Client – Call Forwarding – Simultaneously ring - My Delegates



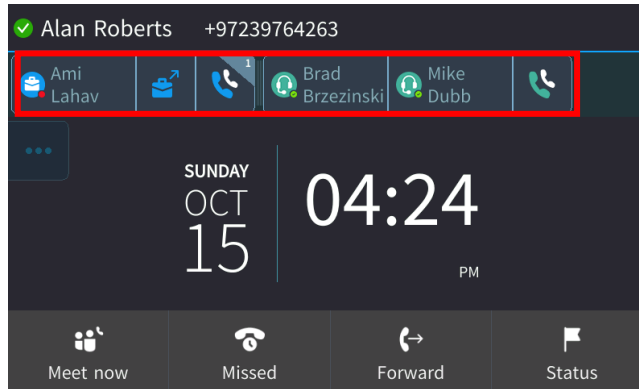
7. Click **OK**; you're returned to the Skype for Business client main screen.





To remove a delegate, it's insufficient for the Boss to *turn off* Call Forwarding under the Lync client's Call Forward Settings. The Boss must also *remove* the delegate from the Call Forwarding – Delegates list.

4.14.1 Viewing Admin Lines on Boss's Phone

After setting up the feature, you'll view, for example, a screen like this:




- View Brad  and Mike  configured as Admins under Boss Alan Roberts' phone



The phone screen shown here is of the C450HD but the concept is identical for the 445HD and the 450HD models.

4.14.2 Viewing Boss's Line on Admin's Phone

- [Refer to the preceding figure] View Ami Lahav configured as Boss  over Admin Alan Roberts' phone

4.14.3 Configuring Boss Privacy Mode

The Boss Privacy mode feature conceals a remote caller's ID from Admin's phone in order to protect their Boss's privacy.

To configure Boss Privacy mode:

- Open the Configuration File page (**Management tab > Manual Update > Configuration File**) and configure the parameter using the table below as reference.

Table 4-12: Boss Privacy Mode Parameter

Parameter Name	Description
lync/bossPrivacyEnable	<p>[0] = Admin sees a remote caller's ID when they call (Default).</p> <p>[1] = A call from a remote caller indicates 'Private Call' on the Admin's phone instead of caller ID.</p> <p>The Boss's phone indicates the remote side's caller ID for all calls.</p>



- If Admin has more than one Boss, the same privacy rule applies to all Bosses.
- The parameter is configured per phone rather than per user.
- The Boss's phone indicates the remote side's caller ID for all calls.

4.15 Enabling the Delegated Line Feature

[Applies only to the 445HD phone] When this feature is enabled, the phones' sidecars display active calls. Each phone can present up to 12 calls (the number of sidecar keys). Up to eight calls can be handled simultaneously. The color of the BLF key adjacent to each call displayed in the sidecars indicates the call's status:

- Red = ongoing call on another phone that is configured with the same user
- Flashing red = call on hold on another phone that is configured with the same user
- Green = ongoing call on the phone
- Flashing green = call on hold which can be resumed or picked up by another phone that is configured with the same user

To enable the feature:

1. Configure the following on the phone:
 - New configuration parameter *lync/sidecardSL=1*
 - Make sure parameter *provisioning/speed_dial_uri=NULL*
2. Associate a 'Delegate' with the user. The delegator can only delegate this user, none other. See the *User's Manual* for information on defining delegates.



- The feature promotes fairness in response to incoming calls. Multiple incoming calls (ringing but not answered yet, i.e., displayed in the phone's screen but not in the phone's sidecar), are presented from the oldest waiting calls to the newest incoming calls. The focus is on the oldest waiting calls.
- When the phone has a call on hold, picking up the handset initiates a new call. It does not resume the last active call.
- Making an outbound call while an incoming call is presented functions as follows: If the user is already handling one or more calls (ongoing or held), a newly incoming call will be displayed on top and in focus. To make a new call and not accept the incoming call, the user navigates to one of the ongoing/held calls, presses the **Menu** softkey, and selects the NEW CALL option.
- If one of the held calls are disconnected by the far end, other calls will remain on hold; the user will not be prompted to resume one of the held calls.
- After a call is answered by one of the phones, all the other phones will display this call in their sidecars.

Calls are picked up by pressing the BLF LED when it flashes red or green.

4.15.1 Configuring Boss Admin Delegated Line

4.15.1.1 Configuring Multiple Points of Presence (MPOPs)

Use a fake Admin **dummy@domain.com** who can define a Boss even though phoneless. Fake Admin does not occupy any screen Programmable Key. The phone does not indicate a fake Admin.

4.15.1.2 Configuring Boss-Admin Sidecar Functionality



Applies to the 445HD phone.

To configure Boss-Admin sidecar functionality:

1. Set the configuration file parameter 'lync/SideCarUse' to **MULTIPLE_BOSS_ADMIN**. Boss and Admin will be able to utilize the phone's sidecar to manage active and held calls in the queue.



The legacy configuration parameter 'lync/sidecardSL' became obsolete as of version 3.0.1. If 'lync/sidecardSL' was previously configured to **1**, after updating to 3.0.1 it will automatically be set to **0** and the parameter 'lync/SideCarUse' (see below) will be configured to **SHARED_LINE** to maintain backward compatibility.

2. When the 'lync/SideCarUse' configuration file parameter is configured to **MULTIPLE_BOSS_ADMIN**:
 - Admin can see in the sidecar each Boss queue
 - Boss can see in the sidecar all Boss calls in the queue
 - A mix of Admin and Boss can be also used in this mode
 - Users can still use the sidecar for Speed Dial/BLF. The upper sidecar key allows users to switch between BLF and Boss/Admin queues.
 - See the phone's *User's Manual* for detailed information on how to use this feature.
3. When the 'lync/SideCarUse' configuration file parameter is configured to **SPEED_DIAL_ONLY** (default), Boss and Admin will be able to use the sidecar for Speed Dials only.
4. When the 'lync/SideCarUse' configuration file parameter is configured to **SHARED_LINE** - the delegate feature that existed up to version 3.0.1 - set the configuration file parameter 'provisioning/speed_dial_uri' to NULL. Configure the configuration file parameter 'voip/number_of_calls_per_line'. This determines the number of calls that can be handled simultaneously per phone. Multiple calls can be handled. Switching between them can be performed. This is very advantageous for receptionists. The setting is customer-specific. It can be 8x [number of Boss phones]. However, the 13th call and up are unmanageable in the sidecar (no appearance, no pick up). Even if an index becomes free, the 13th call and up will not occupy the free index. A newly free index will be occupied by the next incoming call.

4.16 Configuring a Distinctive Ring on the Phone of Each Boss

The network administrator can configure a distinctive ring on the phone of each configured Boss using the configuration file. Distinctive ring tones help Admins audially distinguish between their Bosses phones when calls come in, optimizing Admins' work efficiency.

The feature allows control over the volume of Admin's ringtone in the Boss's phone as well as control over the volume of the Boss's ringtone in Admin's phone.

The configuration can also be performed from the Admin's phone menu option Settings > Distinctive Ringing (see the phone's *User's Manual* for details).

To configure a distinctive ring tone on the phone of a Boss:

- Use the table below as reference.

Table 4-13: Distinctive Ring Tone Parameter

Parameter Name	Description
lync/delegate/boss/[0-6]/distinRingtone	<p>Allows Admins to audially distinguish between their Bosses phones when calls come in. An Admin can configure a specific ringtone for each Boss. This can be configured from Menu > Settings > Boss Ring Tone. The network administrator can also configure the ring on the phone of each configured Boss through the configuration file parameter <code>/lync/delegate/boss/[0-6]/distinRingtone</code>.</p> <ul style="list-style-type: none"> ■ Ring01 (Default) ■ Ring02 ■ Ring03 ■ Ring04 ■ Ring05 ■ Ring06 ■ Ring07 ■ Ring08 ■ Ring09 ■ Ring10 ■ Ring11
lync/delegate/boss/0/distinRingSignalLevel	<p>Allows configuration of the volume level for the type of ring configured with the previous parameter. Range: -32 (silence) to 6 (top volume)</p>

4.17 Configuring Phones to Operate in an OVR Deployment

Network administrators can configure phones to operate in an OVR (One Voice Resiliency) deployment, supporting `dhcption160.cfg`. New configuration file parameters are:

- `lync/sign_in/fixed_outbound_proxy_address=<SBC IP address>`
- `lync/sign_in/fixed_outbound_proxy_port=<SBC listening port>` (Default: 0)
- `lync/sign_in/use_hosting_outbound_proxy=1`

For detailed information on configuring this feature, see the *One-Voice Resiliency (OVR) Configuration Note* available from AudioCodes.

4.18 Disabling Local 3-Way Conferencing Capability

This section shows how to remove the capability of local 3-way conferencing from users.

To disable local 3-way conferencing:

- Use the table below as reference.

Table 4-14: Removing Local 3-Way Conferencing Capability from Users - Parameter

Parameter	Description
lync/local3wayConf/enabled	<p>[0] = the Conf softkey is not displayed in the screen when a call is in progress, as shown in the figure below</p> <p>[1] = the Conf softkey is displayed in the screen when a call is in progress (default)</p>

4.19 Blocking All Phone Users from Signing Out

This section shows how to block *all phone users* from signing out (overrides the Common Area parameter 'voip/common_area/enhanced_mode').

To block all phone users from signing out:

- Use the table below as reference.

Table 4-15: Blocking All Users from Signing out - Parameter

Parameter	Description
lync/userSetting/prevent_user_sign_out	<p>[0] = Sign out softkey is displayed in screens (default)</p> <p>[1] = Sign out softkey is not displayed in screens</p>

4.20 Enabling HotDesking

The HotDesk feature applies to enterprises that operate according to a 'touch-down desk' concept. Employees in these enterprises typically travel frequently to remote branches, or work in shifts. They can sign in to a phone that is already signed in by another user (CAP or regular) without signing out the original user to whom the phone was assigned for primary use.

When the HotDesk user signs out or if the phone stays in idle state longer than the HotDesk timeout defined on the server, the phone automatically returns to its original user and state; its configuration and data are preserved as they were before the phone was leased for HostDesk use. HotDesk users cannot perform all operations that the original user (CAP or regular) could perform, for example, change Language.

Network administrators must enable the feature on the server by setting parameter *EnableHotDesking* to 'True'.

```

Administrator: Windows PowerShell
PS C:\Users\administrator.AC5PIP> get-CsClientPolicy

Identity           : Global
PolicyEntry        : <>
Description        :
AddressBookAvailability : WebSearchAndFileDownload
AttendantSafeTransfer :
AutoDiscoveryRetryInterval :
BlockConversationFromFederatedContacts :
CalendarStatePublicationInterval :
ConferenceIMIdleTimeout :
CustomizedHelpUrl :
CustomLinkInErrorMessage :
CustomStateUrl :
DGRefreshInterval :
DisableCalendarPresence :
DisableContactCardOrganizationTab :
DisableEmailComparisonCheck :
DisableEmoticons :
DisableFeedsTab :
DisableFederatedPromptDisplayName :
DisableFreeBusyInfo :
DisableHandsetOnLockedMachine :
DisableMeetingSubjectAndLocation :
DisableHtmlIM :
DisableInkIM :
DisableOneNote12Integration :
DisableOnlineContextualSearch :
DisablePhonePresence :
DisablePICPromptDisplayName :
DisablePoorDeviceWarnings :
DisablePoorNetworkWarnings :
DisablePresenceNote :
DisableRTFIM :
DisableSavingIM :
DisplayPhoto       : AllPhotos
EnableAppearOffline :
EnableCallLogAutoArchiving :
EnableClientMusicOnHold : True
EnableConversationWindowTabs :
EnableEnterpriseCustomizedHelp :
EnableEventLogging :
EnableExchangeContactSync : True
EnableExchangeDelegateSync : True
EnableFullscreenVideo :
EnableHighPerformanceConferencingAppSharing : False
EnableHotdesking   : True

```

4.21 Uploading Logs to Microsoft Server for Support Purposes

An integrated log upload feature allows network administrators to upload logs from the phone to the Microsoft server for troubleshooting/support purposes, in compliance with Microsoft's certification requirements for 3rd party Skype for Business clients.

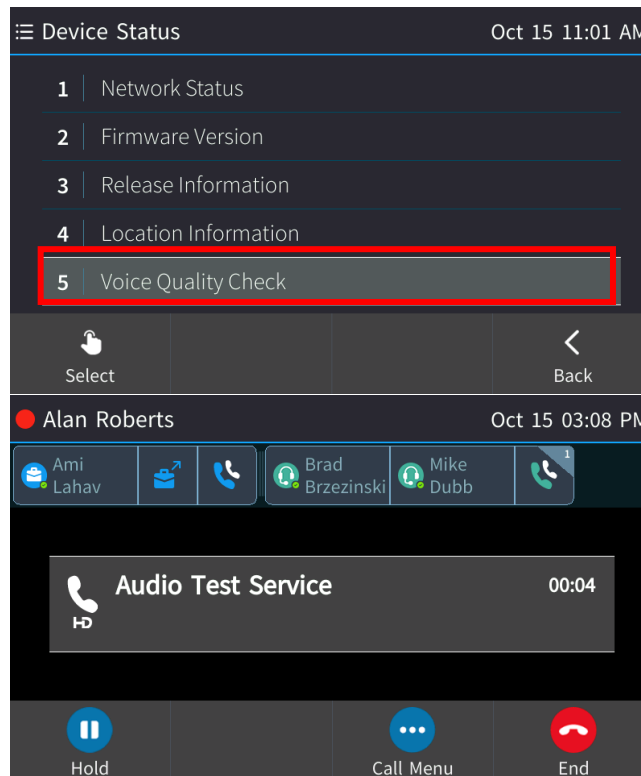
If a user experiences an irregularity such as poor voice quality, they'll contact an AudioCodes Field Application Engineer (FAE) who will instruct them to upload and send the logs for analysis. The FAE then downloads the logs to their PC, performs the analysis, and provides a fix.

To perform log upload:

1. Press the phone's MENU hard key and then open the Settings menu.
2. In the Settings menu, navigate to and select the **Log upload** option; the notification **Uploading log file** is displayed and then replaced by the notification **Log upload finished**.

4.22 Enabling an IP Phone Voice Quality Check

IP phone voice quality can be tested through the phone's Device Status menu.



- If selected, an invitation is played to "Record a short message after the tone then wait to hear how you sound". To enable the feature, the network administrator must enter the following command on the Skype for Business server:

```
set-CsAudioTestServiceApplication -Enabled $True
```

- Additionally, the 'Identity' parameter must be configured with the the SIP address of the audio test service contact to be modified. For example:
- **<sip:RtcApplication-bc516080-3233-42f2-a732-826dd6f99702@audio-codes.info>**

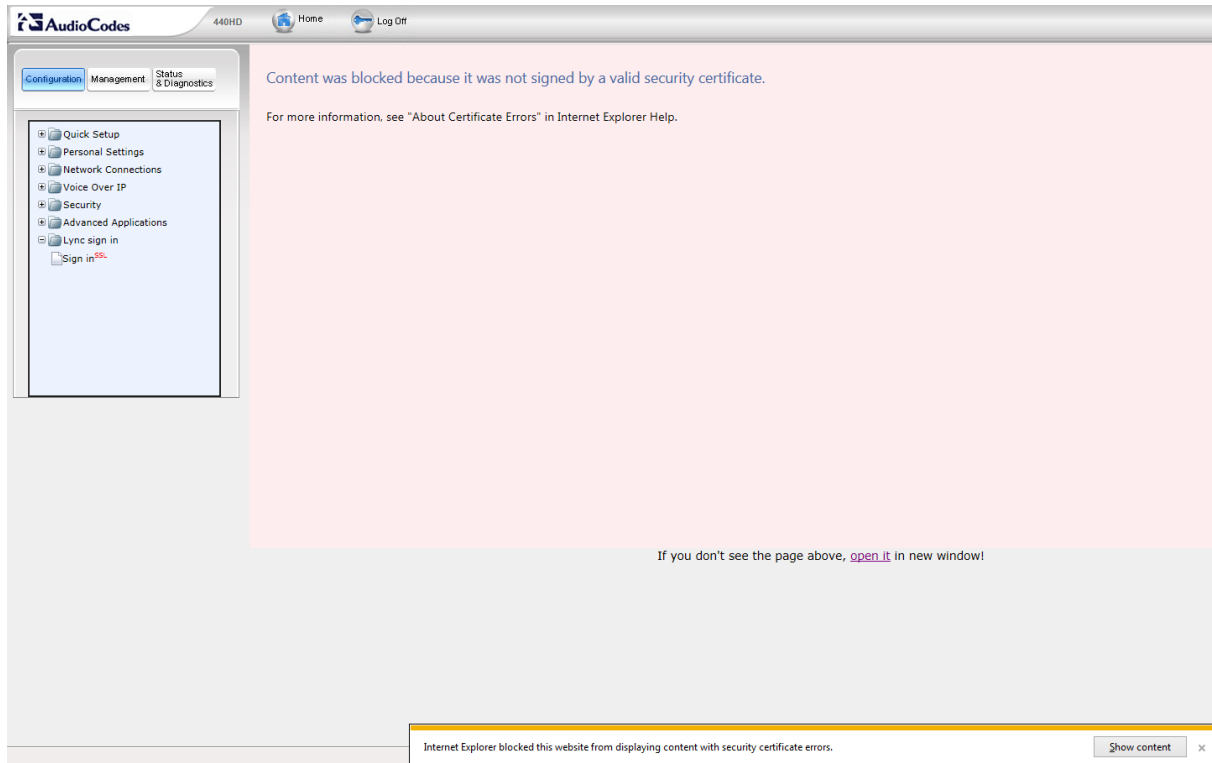
4.23 Signing in / out with the Web Interface

The Web interface can be used to sign in to and out of the phone.

To sign in to and out of the phone using the Web interface:

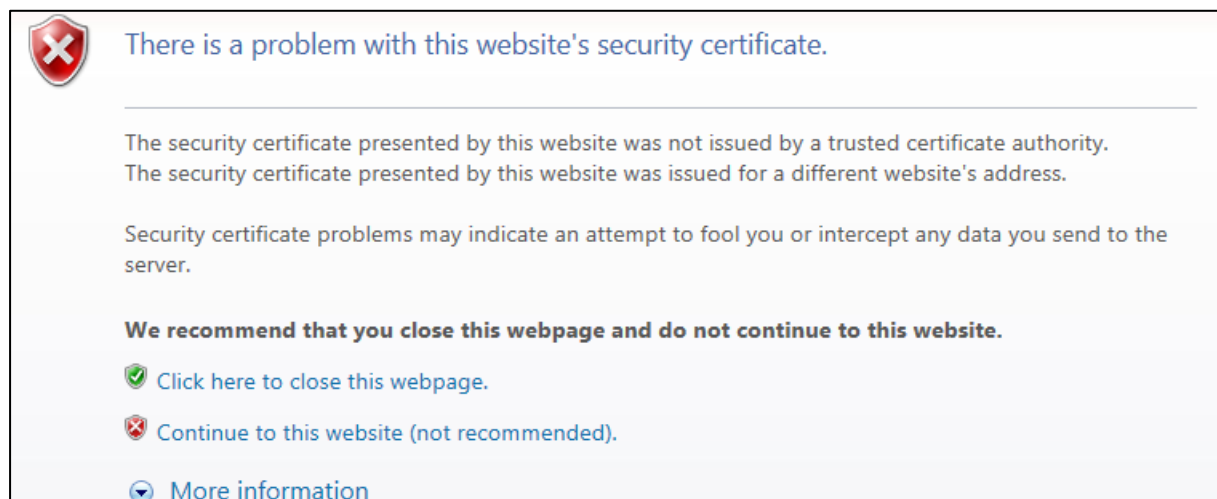
1. In the Web interface, open the Sign-In page (**Configuration** tab > **Lync sign in** > **Sign in**).

Figure 4-39: Sign-in – Content Blocked Page



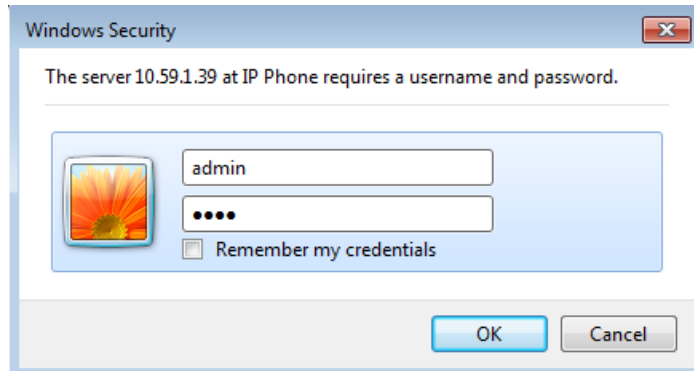
2. Click the **open it** link and then click **Show content**.

Figure 4-40: Sign-in – Windows Security Prompt



3. Click the **Continue to this website (not recommended)** link.

Figure 4-41: Windows Security Prompt



4. In the Windows Security prompt, enter the username and password and then click **OK**.

Figure 4-42: Sign-in with PIN Code

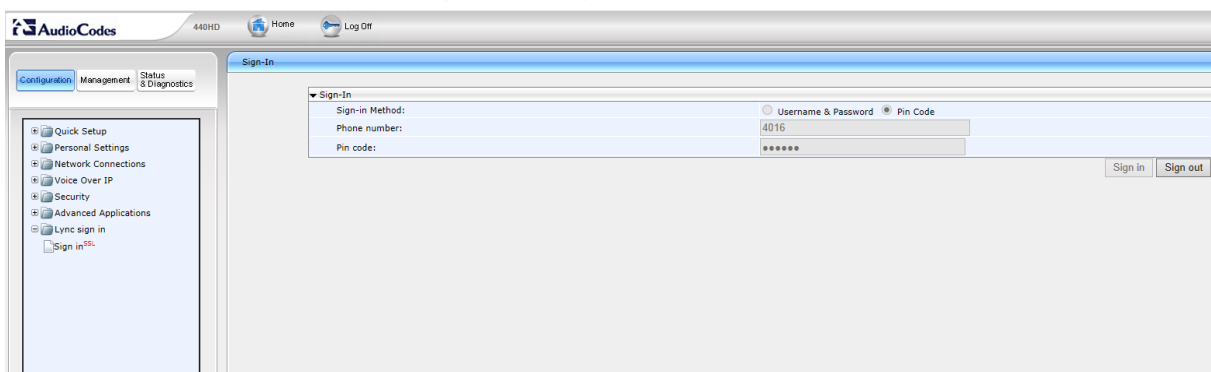
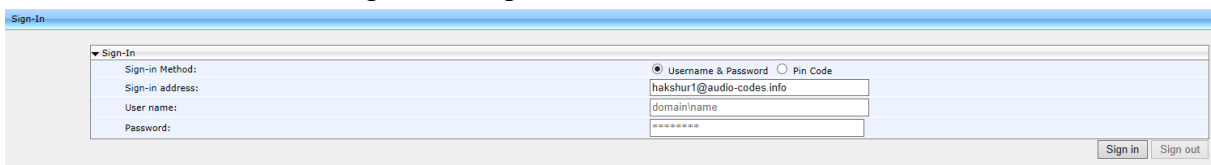


Figure 4-43: Sign-in with Username & Password



5. Select the Sign-in Method. Choose either **Username & Password** or **Pin Code**.
6. In the ' Phone Number' field, enter the number of the phone.
7. [Only applies to signing in with Username & Password] In the 'User name' field, enter the domain name and username.
8. In the 'Pin code' field, enter the PIN code.
9. Click **Sign in / Sign out**
 - a. If the phoned is signed out, click the activated **Sign in** button.
 - b. If the phoned is signed in, click the activated **Sign out** button.

4.24 Signing in and Authenticating with Microsoft's Cloud PBX

The phones feature the capability to sign in to (connect to) and authenticate with Microsoft's Cloud PBX, Microsoft's cloud-hosted version of enterprise voice. AudioCodes' phone features two new sign-in method options, allowing users to connect to Microsoft's Cloud PBX:

- OrgID (Organizational ID), which is the default authentication method in 2016. In 2017, the ADAL method will become the default (see the next option).
- ADAL (Azure AD Authentication Library). Enables the phone to authenticate using OAuth. In 2017, OAuth will replace OrgID, which will deprecate. OAuth 2.0 was implemented in the phone wrapped in ADAL, as described in [RFC 6749](#).

4.25 Initiating a Skype for Business Server Based Phone Conference

The phone supports Multi-Party Skype for Business Remote Conferencing utilizing CCCP (Centralized Conference Control Protocol). Using the new 'Meet Now' option or pressing the **Conf** softkey during an ongoing call, users can initiate, join or be added to a multi-party conference call while having full control and viewing capability. Users can view the roster – see other participants and their status (like the Mute option, Hold status), mute/unmute other participants, manage the conference status as lock/unlock, manage the lobby for conference calls that lobby is defined, admit/deny other participants, and add users into the conference.

The **Meet Now** softkey is defined by default; it enables users to easily initiate remote Skype for Business conference calls.

In versions prior to 3.0, supported conference capability was *locally based* (*phone based*) and limited to two more users, or *remote based*, with more than two parties from the Skype for Business client, using the BToE feature.

4.26 Provisioning the Server for Downloading Contacts Pictures

The network administrator must provision inband provisioning parameters for downloading contacts pictures from the Skype for Business Address Book Server (ABS) or from the Exchange Web Services (EWS).

To provision for downloading contacts pictures from the ABS or EWS:

- Use the table below as reference.

Table 4-16: Inband Provisioning Parameters for Downloading Contacts Pictures to Phones

Parameter	Description
PhotoUsage	Configure either: <ul style="list-style-type: none"> ■ AllPhotos (Default) [All contacts pictures can be downloaded] ■ NoPhoto [Contacts pictures will not be downloaded] ■ PhotoFromADOnly [Contacts pictures can only be downloaded from Microsoft's Active Directory]
AbsWebServiceEnabled	<ul style="list-style-type: none"> ■ True (Default) [Contacts pictures can be downloaded to the phone from Microsoft's Active Directory] ■ False [Contacts pictures cannot be downloaded to the phone from Microsoft's Active Directory]
<absInternalServerUrl>	Defines the Address Book Service (ABS) URL for downloading contacts pictures from the Active Directory. This URL points to an <i>internal ABS server</i> . Example: <i>https://sippoolAM30E06.infra.lync.com:9999/abs/handler</i>
<absExternalServerUrl>	Defines the Address Book Service (ABS) URL for downloading contacts pictures from the Active Directory. This URL points to an <i>external ABS server</i> . Example: <i>https://webpoolAM30E06.infra.lync.com:443/abs/handler</i>

4.26.1 Disabling Contacts Pictures

The screens of the 450HD phone, 450HD + Expansion Module, C450HD phone, C450HD + Expansion Module, 445HD phone and the HRS by default display contacts pictures. Contacts pictures are displayed with idle screen Speed Dials (including presence statuses), Favorites, Corporate Directory, Personal Directory, Exchange Contacts, other contacts lists, incoming calls, outgoing calls, conference calls, visual voice mail and call logs. Enterprises typically won't disable the feature but if enterprises or employees want it disabled, the network administrator can disable it locally on the phone.

To disable the phone from displaying contacts pictures:

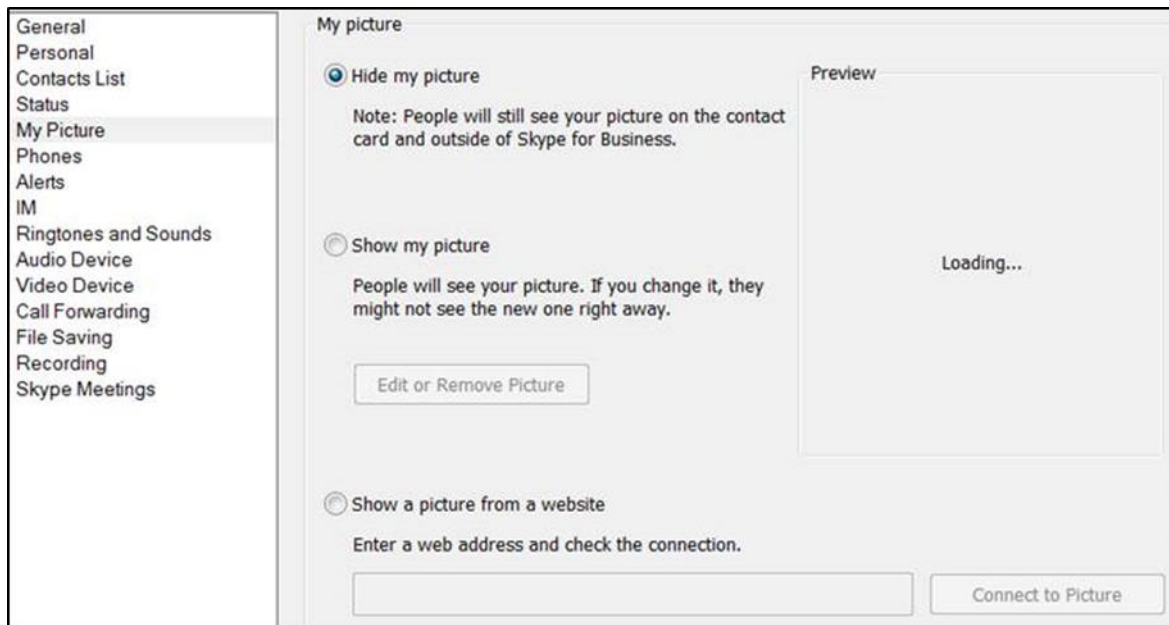
- Use the table below as reference.

Table 4-17: Local Phone Parameters for Downloading Contact Pictures

Parameter	Description
lync/ContactPicture/IPPhotoUsage	<p>[INBAND] (Default) [Phone performs according to the inband provisioning parameter]</p> <p>[NOPHOTO] [No contacts pictures are displayed; overrides the inband provisioning parameter]</p> <p>[ALLPHOTOS] [All contacts pictures can be displayed; overrides the inband provisioning parameter]</p>



In the Skype for Business client (see the figure below), users can reserve their right to hide their pictures so even when both parameters above are set to **All photos**, if user B uses the client to hide their picture, others won't be able to see it.

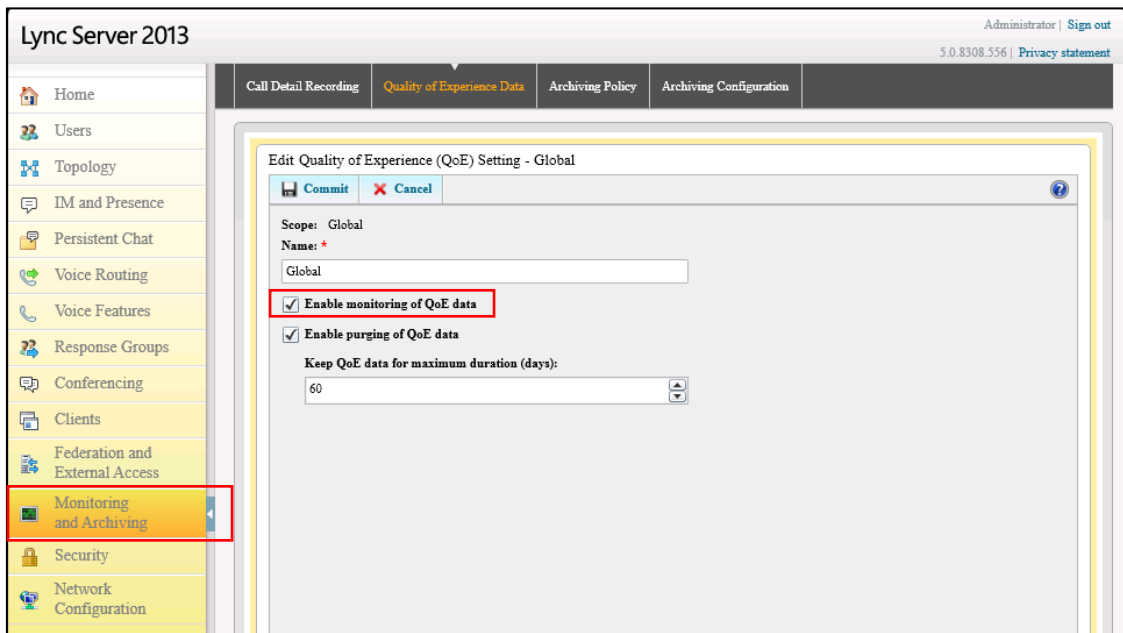


4.27 Enabling QoE Reports to be Sent to Microsoft's SQL Server

Quality of Experience (QoE) reports can be sent to Microsoft's SQL server. A SIP Service message containing a QoE .xml report is sent inband from the phone to Microsoft's FE server at the end of every phone call. The FE server then sends it to Microsoft's SQL server from which third-party applications such as AudioCodes' Session Experience Manager (SEM), in addition to Microsoft's Report Server, can pull and present the information graphically for network administrators to use to optimize and enhance enterprise telephony.



To enable QoE reports, the Lync/Skype for Business server must be configured to enable QoE monitoring, as shown in the figure below.



To enable the feature:

- Open the Configuration File page (**Management tab > Manual Update > Configuration File**) and configure the parameter using the table below as reference.

Table 4-18: Enabling QoE Reports using the Configuration File

Parameter Name	Description
voip/rtcp_xr/vq_statistics/mode	Enables / disables QoE reports to be sent to Microsoft's SQL server. <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)



The RX50 conference phone supports Voice Quality reports in compliance with the IETF's RFC 6035, except for the following VQ local metrics that are not provided:

- Jitter buffer statistics
- Burst and Gapp loss
- Signal and noise levels
- Voice Quality estimation

4.28 Enabling Malicious Call Tracing

Phone users can report a malicious call if the (new) parameter option 'Enable malicious call tracing' on the Skype for Business server is selected, as indicated in the figure below.

The screenshot shows the Lync Server 2013 administration console. The left-hand navigation pane is expanded to 'Voice Routing'. The main area displays the 'Edit Voice Policy - ChinaLync2013' dialog box. The 'Calling Features' section is expanded, and the 'Enable malicious call tracing' checkbox is checked and highlighted with a red box. Other checked options include 'Enable call forwarding', 'Enable delegation', 'Enable call transfer', 'Enable call park', 'Enable simultaneous ringing of phones', 'Enable team call', and 'Enable PSTN reroute'. The 'Associated PSTN Usages' table is also visible.

PSTN usage record	Associated routes
CH local route	LocalRoute, AC Lab Route
Internal	China
Local	China
Long Distance	China

If a user gets a malicious call and wants to report it, the option allows them to send a report to the Skype for Business server (see the *User's Manual* for more information).

4.29 Disabling the C450HD IP Phone Screen Saver

The C450HD phone features a screen saver displaying a digital clock. The feature allows future customization of the phone. By default, the feature is enabled, but the network administrator can disable it on request.

To disable the feature:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-19: Disabling the C450HD IP Phone Screen Saver

Parameter Name	Description
personal_settings/ScreenSaverEnabled	Enables / disables the C450HD phone screen saver. <ul style="list-style-type: none"> ■ [0] Disable ■ [1] Enable (default)
personal_settings/ScreenSaverAwakeTimeout	The timeout of the screen saver is triggered after 300 seconds by default but it can be configured to 0-600 seconds using this parameter.

4.30 Registering the Phone on Azure Cloud

The phone supports a client ID for OAuth 2.0 modern authentication in compliance with IETF RFC 6749 and in compliance with Microsoft's request to register the phone application on the Azure cloud service portal and to apply permissions.

The network administrator can enable the new client ID to be used after it's approved. See also <https://online.audiocodes.com/oauth-2-0-appid>.

To enable the client ID:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 4-20: Enabling the Client ID using the Configuration File

Parameter Name	Description
lync/sign_in/azure/Enable_new_client_id	<ul style="list-style-type: none"> ■ [0] The phone will use the previous client_id as part of the Oauth2.0 process. ■ [1] The phone will use a new client_id as part of the Oauth2.0 process (default).

5 Maintenance

This section shows how to upgrade the phone firmware, perform administration tasks, and enable remote management.

- See under Section 4.9 for information on how to automatically update the phone's firmware from the Skype for Business server.
- See Section 5.1 below for information on how to upgrade the phone's firmware with the firmware file received from AudioCodes.
- See under Section 4.9.3 for information on how to manually check if the firmware on the phone is different to the firmware file located on the provisioning server.
- See Section 5.2 for information on how to enable automatically checking for firmware updates using the Configuration File.

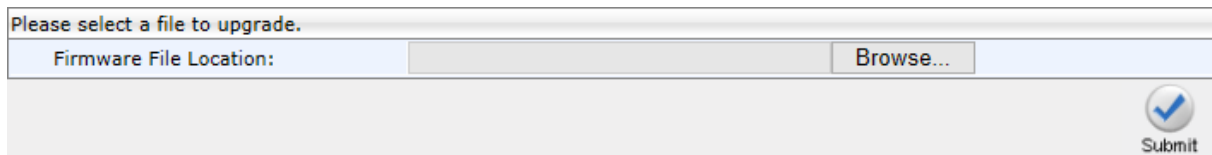
5.1 Upgrading Phone Firmware

This section shows how to upgrade the phone firmware.

To upgrade the phone firmware:

1. After receiving the new img firmware file from AudioCodes, save it to a location on your PC.
2. Open the 'Manual firmware upgrade' page (**Management** tab > **Manual Update** > **Manual firmware upgrade**).

Figure 5-1: Manual Firmware Upgrade



The screenshot shows a web form for manual firmware upgrade. At the top, it says "Please select a file to upgrade." Below this is a text input field labeled "Firmware File Location:" followed by a "Browse..." button. In the bottom right corner, there is a "Submit" button with a blue checkmark icon.

3. Click **Browse...**, navigate to the img file on your PC, and then click **Submit**; the phone screen displays the upgrade process (see the *User's Manual* for details).
4. On the phone, press the MENU key and select **Status** > **Firmware Version**.
5. Make sure the firmware is the version of the img file you received from AudioCodes, applicable to the phone model.

5.2 Enabling/Disabling Device Update

The phone checks for firmware updates when it boots up and once every timeperiod defined in its Configuration File.

Default: **Once every 24 hours.**

The phone checks for firmware updates using the HTTP POST web service. The URL is extracted from the inband provisioning information under:

- **updatesServerInternalUrl**
- updatesServerExternalUrl

Two in-band provisioning parameters enable the device update feature: 'updatesServerEnabled' and 'EnableDeviceUpdate'.

If 'updatesServerEnabled' is set to **true** and 'EnableDeviceUpdate' is set to any value except **false**, the phone will enable the device update feature.

In addition to these in-band provisioning parameters, the phone has a local configuration parameter 'SfBDeviceUpdate'. This parameter allows the administrator to disable the automatic device update feature even if the feature is enabled by the in-band provisioning parameters.

To enable/disable the device update feature:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table below as reference.

Table 5-1: Automatically Checking for Updates Using the Configuration File

Parameter Name	Description
lync/SfBDeviceUpdate	Enables or disables the device update feature: <ul style="list-style-type: none"> ■ 0] The phone will get firmware updates from the device update service only if the phone didn't get a firmware URL from DHCP Options or from Static URL configuration, and if the in-band provisioning parameters enable the feature (default). ■ 1] The phone will get firmware updates from the device update service if the in-band provisioning parameters enable the feature.

5.3 Administration

5.3.1 Managing Users

You can change the phone's login user name and password. This is the login required to access the Web interface and the **Administration** menu in the phone's screen.



- For the Administrator account, the default 'Username' and 'Password' is **admin** and **1234** respectively. It's advisable for the network administrator to change it to prevent unauthorized access.
- For the User account, the default 'Username' and 'Password' is **user** and **1234** respectively.

To change the login username and password:

- Use the tables below as reference.

Table 5-2: Administrator account - Username and Password

Parameter	Description
Note: To add a value to these parameters, enter system/ followed by the parameter name, equal sign and then the value (e.g. <code>system/user_name=admin</code>).	
system/user_name	The phone user name. The default value is admin. If this parameter value is unconfigured in the configuration file, users can log in to the Web interface using the same Microsoft password/PIN they used to sign in to the IP phone (to maintain backward compatibility). Note: This parameter is applicable only to the Web and Telnet interfaces.
system/password	The encrypted phone password. The default value is 1234. If this parameter value is unconfigured in the configuration file, users can log in to the Web interface using the same Microsoft password/PIN they used to sign in to the IP phone (to maintain backward compatibility). To generate an encrypted password, see Section 3.5. Note: This parameter applies to the Web and Telnet interfaces, and to the screen display.

Table 5-3: User account - Username and Password

Parameter	Description
system/web_user_name	The phone user name. Default: user. Applies only to Web and Telnet interfaces.
system/web_user_password	The encrypted phone password. Default: 1234. Applies only to Web and Telnet interfaces, and phone screen. It's advisable for the network administrator to change the default to prevent unauthorized access.

5.3.2 Managing the Web Login Sign-in Option

The Web Login method of signing in to the phone features a secure HTTPS protocol between the web browser and the phone. The Device Manager server intermediates between the user's internet browser and the phone. Version 7.4.3000 and later of the Device Manager supports the feature. If

the user has a version that's earlier than this, the Device Manager falls back to the previous Web Login and allows the user to sign-in by browsing directly to the server.

Network administrators can enable or disable the feature using a new configuration file parameter 'ems_server/EMS_WEB_Login'.

- [1] Enable (Default)
- [2] Disable

5.3.3 Allowing / Disallowing Management via the Web Interface

Network administrators can allow / disallow management via the phone's Web interface without requiring a phone reboot. The configuration file parameter 'system/web/enabled' supports the feature.

- 0 disallows management via the phone's Web interface
- 1 (default) allows management via the phone's Web interface

5.3.4 Restoring Defaults

See Section 8.7.1.2 on page 195, under [General Corrective Actions](#).

5.3.5 Restarting the Phone

See Section 8.7.4.2 on page 198, under [General Corrective Actions](#).

5.4 Enabling Remote Management

5.4.1 Enabling Telnet Access

Telnet access can be enabled using the Configuration File.



Opening a Telnet connection in an external network is strongly inadvisable due to the widely recognized vulnerability of the protocol.

To configure Telnet:

1. Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameter using the table as reference.

Table 5-4: Telnet Parameters

Parameter	Description
Note: To add a value to these parameters, enter management/ followed by the parameter name, equal sign and then the value (e.g. <code>management/telnet/enabled=0</code>).	
management/telnet/enabled	<p>Enables telnet access to the phone.</p> <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable <p>The user name and password for telnet access are according to the parameters: system/user_name and system/password.</p>

5.4.2 Enabling SSH Access

Secure Shell (SSH) protocol can be configured for secure remote login to the 450HD, C450HD and 445HD phones and the HRS. Network administrators can use configuration file parameter 'management/ssh/enabled' to enable the feature (by default, it is set to **0**, i.e., disabled).

6 Status and Performance

6.1 Viewing Network Status

This section shows how to view network status from the Web interface.

6.1.1 Viewing LAN Status

This section shows how to view LAN status information.

To view LAN status information:

- Open the Network Status page (**Status & Diagnostics** tab > **System Status** menu > **Network Status**).

Figure 6-1: Web Interface - LAN Information

LAN Information	
Type:	DHCP Client
IP Address:	10.16.2.162
Subnet Mask:	255.255.0.0
Default Gateway Address:	10.16.0.1
Primary DNS:	10.1.1.11
Secondary DNS:	10.1.1.10
MAC Address:	00:90:8F:1E:DB:3E

6.1.2 Viewing Port Mode Status

This section shows how to view the Port Mode status.

To view port mode status:

- Open the Network Status page (**Status & Diagnostics** tab > **System Status** menu > **Network Status**).

Figure 6-2: Web Interface - Port Mode Status

Port Mode Status		
Attribute	LAN Port	PC Port
Link State:	Up	Down
Negotiation:	Automatic	Automatic
Speed:	100Mbps	N/A
Duplex:	Full	N/A

6.1.3 Viewing 802.1X Status

This section shows how to view 802.1X status.

To view 802.1X status:

- Open the Network Status page (**Status & Diagnostics** tab > **System Status** menu > **Network Status**).

Figure 6-3: Web Interface - 802.1X Status

802.1X Status	
EAP Type:	EAP-TLS
Status:	Failure: No certificates

6.2 Viewing VoIP Status

This section shows how to view VoIP status using the Web interface.

6.2.1 Viewing Phone Status

This section shows how to view the phone status.

To view the phone status:

- Open the VoIP Status page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**) and locate the section 'Phone Status'.

Figure 6-4: Web Interface - Phone Status

Phone Status	
Hook State	On Hook
Audio Device	Ringer

6.2.2 Viewing Line Status

This section describes how to view the line status.

To view the line status:

- Open the VoIP Status page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**) and locate the section 'Line Status'.

Figure 6-5: Web Interface - Line Status

Line Status	
Line Number	Line 1
SIP Registration	Registered
DnD	On
Mute	Off
Forward State	Disabled
Forward Destination	N/A

6.2.3 Viewing Call Information

The Web interface displays call information *of a currently established call*.

To view call information after establishing a call:

- Open the VoIP Status page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**) and locate the 'Call Information' section.

Figure 6-6: Web Interface - Call Information

Line 1 Call Information	
Call Number	Call 1
Call State	Connected
Origin	Outgoing
Remote Number	+97239764232
Remote ID	-
Duration	00:00:21
Codec	PCMU
Packets Sent	6104
Packets Received	4223
Bytes Sent	976640
Bytes Received	675680
Packets Lost	0
Fraction Lost	N/A
Jitter	0
Round Trip Delay	0

6.3 Viewing Call History

The Web interface displays received and missed calls, dialed numbers and call duration.

To view call history:

1. Open the Call History page (**Status & Diagnostics** tab > **History** > **Call History**).

Figure 6-7: Web Interface - Call History

Call History					
Type: Missed Calls Page: 1					
No.	Name	Number		Time	Delete
1	420HD	1000	Dial	06/01/2000 Thursday 21:21:31	<input type="checkbox"/>
2	420HD	1000	Dial	06/01/2000 Thursday 21:17:38	<input type="checkbox"/>
3	Alan_2	2000	Dial	06/01/2000 Thursday 21:14:26	<input type="checkbox"/>
4	420HD	1000	Dial	06/01/2000 Thursday 19:24:49	<input type="checkbox"/>
5	420HD	1000	Dial	06/01/2000 Thursday 19:13:29	<input type="checkbox"/>
6	Alan_2	2000	Dial	06/01/2000 Thursday 19:13:22	<input type="checkbox"/>

2. From the 'Type' dropdown, select the call history type, i.e., Missed Calls, Received Calls, or Dialed Numbers that you want to view; the table lists the call history according to the call history type you select.
3. To delete an entry, select the entry's 'Delete' option and click **Delete**.

6.4 Viewing Phone Model / Firmware Version

This section shows how to view the phone model and the phone's firmware version from the the phone's screen.

6.4.1 Viewing from the Phone's Screen

This section shows how to view phone model and firmware version from the phone's screen.

To view the phone's model and firmware version from the screen:

- Open the Firmware Version screen (MENU key > **Status** > **Firmware Version**).

6.4.2 Viewing Release Information

This section shows how to view release information in the Web interface.

To view release information in the Web interface:

- Open the Release Information page (**Status & Diagnostics** tab > **System Information** > **Release Information**).

Figure 6-8: Web Interface - System Information - Release Information

Release Information	
BLVERSION	3.3.10
BUILD_TIME	2018-03-13_17:21:37
DSPFWVERSION	494E002ce2.720.32
HW_TYPE	450HD
LOG	0
SWVERSION	UC_3.1.0.296
SW_TYPE	LYNC

7 Diagnostics

This section shows how to perform diagnostics.

7.1 Logging

7.1.1 Analyzing and Debugging Traffic using Syslog

This section shows how to use the System Logging (Syslog) feature which allows administrators to track and monitor syslog information, facilitating traffic analysis and debugging the phone.

The feature includes one centralized log in the Web interface's System Logging page, shown in the figure below.

For each log module, a log level can be configured: **None**, **Basic** or **Detailed**. The feature can be configured using the Configuration File.

To configure system logging:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.



If you disable Syslog after enabling it, it's important to revert all parameter settings back to **None**.

Table 7-1: Syslog Parameters

Parameter	Description
system/syslog/log_level	Defines the System Logging feature's log level. Possible values are: <ul style="list-style-type: none"> • None = make unavailable / disable • Basic = basic debug level • Detailed = detailed debug for developers (debug version required)
system/syslog/mode	Defines the System Logging feature's destination. Possible values are: <ul style="list-style-type: none"> • Local = No Syslog, i.e., the phone's flash memory (default). • Network = a.k.a. Syslog server. Basic debug level. • Serial = a.k.a. Console. You'll need to connect a serial cable to view the logs. • All = Syslog is sent to the Syslog server <i>and</i> the phone console (Network <i>and</i> Console).
system/syslog/server_address	Only displayed when 'Log Destination' is Network or All . Defines the IP address (in dotted-decimal notation) of the PC host you are using to run the Syslog server (e.g. Wireshark), to where the Syslog messages should be sent. The Syslog server is an application designed to collect the logs and error messages generated by the phone. Default: 0.0.0.0 .

Parameter	Description
system/syslog/server_port	Defines the log module which generates Syslog messages related to the UDP port of the Syslog server. Range: 0 to 65,535. Default: 514. Note: This parameter is applicable when Log Destination (see above) is set to Network or Both .
Process - nxphone	Defines the log module process executed on the phone which generates Syslog messages related to the phone application responsible for user interface representation (front end) on the screens (main screen, BLF screen and sidecar).
Process - voip_task	Defines the log module which generates Syslog messages related to the multi-layer VoIP application. Default: None.
system/syslog/component/control_center	Defines the log module process executed on the phone which generates Syslog messages related to networking. Default: None.
Process - b2goe	Defines the log module process executed on the phone which generates Syslog messages related to AudioCodes' B2GoE USB driver. Default: None.
Process - lighttpd	Defines the log module process executed on the phone which generates Syslog messages related to the lighttpd webserver. Default: None.
Process - ac_watchdog	Defines the log module process executed on the phone which generates Syslog messages related to Watchdog process. Default: None.
system/syslog/component/sip_call_control	Defines the log module process executed on the phone which generates Syslog messages related to Multimedia Terminal Framework (MTF) responsible for VoIP standards. Default: None
system/syslog/component/sip_stack	Defines the log module process executed on the phone which generates Syslog messages related to SIP (RFC 3261). Default: None
system/syslog/component/ice_stack	Defines the log module which generates Syslog messages related to ICE (Interactive Connectivity Establishment). Default: None
system/syslog/component/lcd_display	Defines the log module which generates Syslog messages related to the phone screen display. Default: Debug
system/syslog/component/web_server	Defines the log module which generates Syslog messages related to the phone's Web server. Default: None
system/syslog/component/ieee802_1x	Defines the log module which generates Syslog messages related to the 802.1X security protocol. Default: None
system/syslog/component/kernel	Defines the log module which generates Syslog messages related to the operating system core.
system/syslog/component/dsp	Defines the log module which generates Syslog messages related to the phone's DSP (voice engine) commands.
system/syslog/component/lib	Defines the log module which generates Syslog messages related to the internal library of the IP phone. Default: None.
system/syslog/component/sipe	Defines the log module which generates Syslog messages related to the SIPE Project's third-party Pidgin plugin for Microsoft Skype for Business client.
system/syslog/component/cgi	Defines the log module which generates Syslog messages related to the services for the Web server.

7.1.2 Analyzing and Debugging Traffic using Syslog

A syslog logging mechanism allows you to perform phone logging without affecting phone performance.

To enable the Lightweight Syslog:

1. In the Web interface, open the phone's System Logging page (**Status & Diagnostics** tab > **Diagnostics** > **Syslog Config**).
2. Change the 'Log Destination' parameter from its default **Local** to **Network**.
3. Provide a valid IP address and server port.
4. Do not set any of the options (keep all as **None**).
5. Click **Submit**.

7.2 Enabling Recording to Debug Voice

This section shows how to use recording capability to debug voice activity on the phone. You can enable the capability using the Configuration File.

To enable recording to debug voice:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 7-2: Packet Recording Parameters

Parameter	Description
voip/packet_recording/remote_ip	The IP address (in dotted-decimal notation) of the remote computer to which the recorded packets are sent. The recorded packets should be captured by a network sniffer (such as Wireshark). The default value is 0.0.0.0.
voip/packet_recording/remote_port	Defines the UDP port of the remote computer to which the recorded packets are sent. The valid range is 1024 to 65535. The default value is 50000.
voip/packet_recording/enabled	Activates the packet recording mechanism. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable Note: DSP packet recording can be enabled on the fly, without requiring the network administrator to reset the phone.
voip/packet_recording/rtp_recording/enabled	Only displayed in the Web interface if 'Enable DSP Recording' is enabled. Enables RTP recording. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable

Parameter	Description
voip/packet_recording/ec_debug_recording/enabled	Activates the Echo Canceller Debug recording. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable
voip/packet_recording/cng_debug_recording/enabled	Activates the generic Comfort Noise Generation debug recording. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable
voip/packet_recording/noise_reduction_recording/enabled	Traffic on the network stops when the MUTE key is activated. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable
voip/packet_recording/network_recording/enabled	Activates the DSP network (TDM Out) recording. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable
voip/packet_recording/tdm_recording/enabled	Activates the DSP TDM (TDM In) recording. <ul style="list-style-type: none"> ■ [0] Disable (default) ■ [1] Enable

7.3 Downloading a Tombstone Dump

This section shows how to download a tombstone dump using the Web interface. If a crash occurs, a crash dump file of firmware exceptions such as incorrect flow, a bug, a NULL pointer, etc., is written. The file contains data about the crashed process. IP phone developers can use it to debug a problem.

To download a tombstone using the Web interface:

1. Open the Crash Dump page (Status & Diagnostics tab > Diagnostics menu > Tombstone Dump).

Figure 7-1: Web Interface - Crash Dump

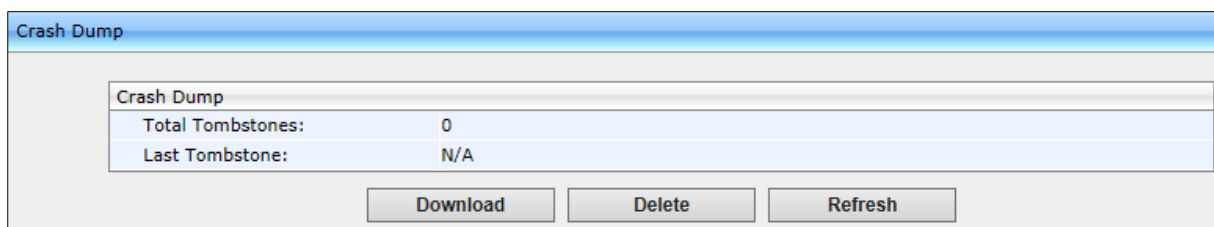


Table 7-3: Crash Dump Parameters

Parameter	Description
Total tombstones	The number of crashes on the phone.
Last tombstone	The date and time of the last crash (the exact time of the crash).

2. Click **Download** to save the crash dump file on your computer.

7.4 Activating Core Dump

The phone can perform a core dump providing detailed information related to a firmware exception on the phone. The core dump facilitates problem diagnosis and debugging. The recorded contents of the phone's main memory are stored at a specific time, usually after the phone crashes or is terminated abnormally, and made available for further examination.



The Core Dump feature is by default enabled on the 445HD, 450HD and C450HD phones. On all other phones, it is by default disabled.

To enable core dump:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and enable core dump using the table below as reference.

Table 7-4: Core Dump Parameter

Parameter	Description
kernel/cfg/enable_core_dump	Enables core dump. <ul style="list-style-type: none">■ [0] Disable■ [1] Enable (default)

If a phone issue is encountered, for example, if the phone crashes or is terminated abnormally, you can download the core dump to examine dumps of all exceptions encountered and resolve the issue.

7.5 Monitoring: Traceroute

For effective troubleshooting and diagnosis, it's recommended to set up the phone to store trace messages. This section shows how to perform traceroute using the Web interface.



During regular phone operation, it is recommended to *disable* debug tracing for improved performance.

Traceroute is a diagnostic you can use

- to display the route of packets across your network
- to measure transit delays

Traceroute computes the sum of the mean times it takes for the packets to transit each hop (from host to host) in the route. [Ping, by contrast, computes the final round-trip times from the destination point].

To perform traceroute using the Web interface:

1. Open the Monitoring page (**Status & Diagnostics** tab > **Diagnostics** menu > **Monitoring**).

Figure 7-2: Web Interface - Monitoring - Traceroute

2. In the 'Destination' field, enter the IP of the device on the remote side to traceroute.
3. Click **Go** to perform diagnostics.

7.6 Enabling Port Mirroring

Port Mirroring when enabled changes the NIC from SWITCH to HUB (L2 to L3) so that network traffic on the LAN port is reflected in the PC port for debugging purposes.

To enable Port Mirroring:

- Use the table below as reference.

Table 7-5: Port Mirroring Parameters

Parameter	Description
network/pc_port_mirroring/enabled	Enables port mirroring. <ul style="list-style-type: none"> ■ [0] Disable (default) - The LAN/PC Network interfaces operate in SWITCH mode. ■ [1] Enable - The LAN/PC Network interfaces operate in HUB mode.

8 Troubleshooting

This section provides various troubleshooting procedures.

8.1 Unable to Sign in to Skype for Business using Username/Password

Problem	Unable to sign in to Skype for Business using the username/password sign-in method.
LCD Message	"Invalid address, username or password"
Corrective Actions	
<ol style="list-style-type: none"> 2. Make sure you correctly entered the sign-in address, username, and password. 3. Make sure you have the correct username/password; it may have changed in the Enterprise's Active Directory. 4. Make sure you used the correct sign-in method (Sign-in softkey > Switch sign-in method > OK hard key or Select softkey). 	

8.2 Unable to Authenticate User using PIN

Problem	Unable to authenticate user when signing in to Skype for Business using PIN code.
LCD Message	"The phone number or extension is not valid"
Corrective Actions	
<ol style="list-style-type: none"> 5. Make sure you entered the phone number / PIN code correctly. 6. Make sure you have the correct PIN code; it may have changed in the Enterprise's Active Directory. 7. Make sure you used the PIN code sign-in method (Sign-in softkey > Switch sign-in method > OK hard key or Select softkey). 	

8.3 IP Phone Fails Registration Process

Problem	The phone fails to register.
LCD Message	-
Corrective Actions	
<p>Make sure:</p> <ol style="list-style-type: none"> 8. DHCP Option 43 has been configured. 9. Access is possible from the following Web site: https://YOUR_AUTHORITY_SERVER:443/CertProv/CertProvisioningService.svc 10. If the environment supports more than one CA Certificate, this must be included in the CA Certificate file and loaded to the IP phone. 	

8.4 How to Verify CA Certificate is Trusted / Authorized by IP Phone

Problem	How do I know if my CA Certificate is trusted and authorized by the IP Phone?
LCD Message	-
Corrective Actions	
Verify whether your public trusted certificate is listed in Microsoft Public Trusted Certificates (http://technet.microsoft.com/en-us/library/gg398270(v=ocs.14).aspx).	

8.5 Invalid Time Server

Problem	The time server is invalid.
LCD Message	-
Corrective Actions	
Make sure NTP (DHCP Option 42) is configured in the DHCP server and is defined as NTP SRV records. If not, manually configure it.	

8.6 Invalid Time Offset

Problem	The time offset is incorrect.
LCD Message	-
Corrective Actions	
Make sure the Time Offset (DHCP Option 2) is configured in the DHCP server. If not, manually configure Daylight Saving Time (DST) values in the phone screen.	

8.7 General Corrective Actions

8.7.1 Restoring Phone Defaults

The phone's default settings can be restored from its screen or from the Web interface.

8.7.1.1 Restoring Factory Defaults from the Phone Screen

This section shows how to restore factory defaults from the phone's screen.

To restore the phone's default settings from the phone screen:

1. Open the Restore Defaults menu option (MENU key > **Administration** > **Restore Defaults**).
2. Select the **Restore Defaults** option; the phone prompts with the following warning:
Warning. Restore settings?
3. Select **Yes** to confirm or **No** to cancel.



You can restore the phone's settings to their defaults without needing access to the 'Administration' menu or (2) administrator access to the Web interface.

To restore the phone's settings to their defaults if necessary:

1. Press the OK + MENU keys simultaneously and keeping them pressed, unplug the power cable.
2. Plug the power cable back into the phone continuing to press the OK + MENU keys for +-5 seconds.
3. Release the OK + MENU keys; the phone's settings are restored to their defaults.

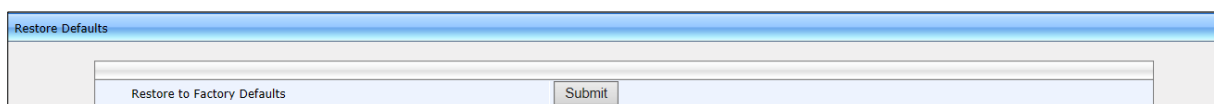
8.7.1.2 Restoring Factory Defaults from the Web Interface

This section shows how to restore the phone's factory defaults from the Web interface.

To restore the phone's factory defaults from the Web interface:

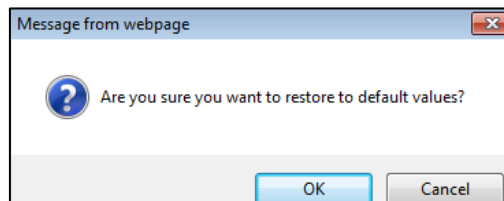
1. Open the Restore Defaults page (**Management** > **Administration** > **Restore Defaults**).

Figure 8-1: Web Interface - Restore Defaults



2. Click **Submit**:

Figure 8-2: Confirm Restore to Factory Defaults



3. Click **OK**.

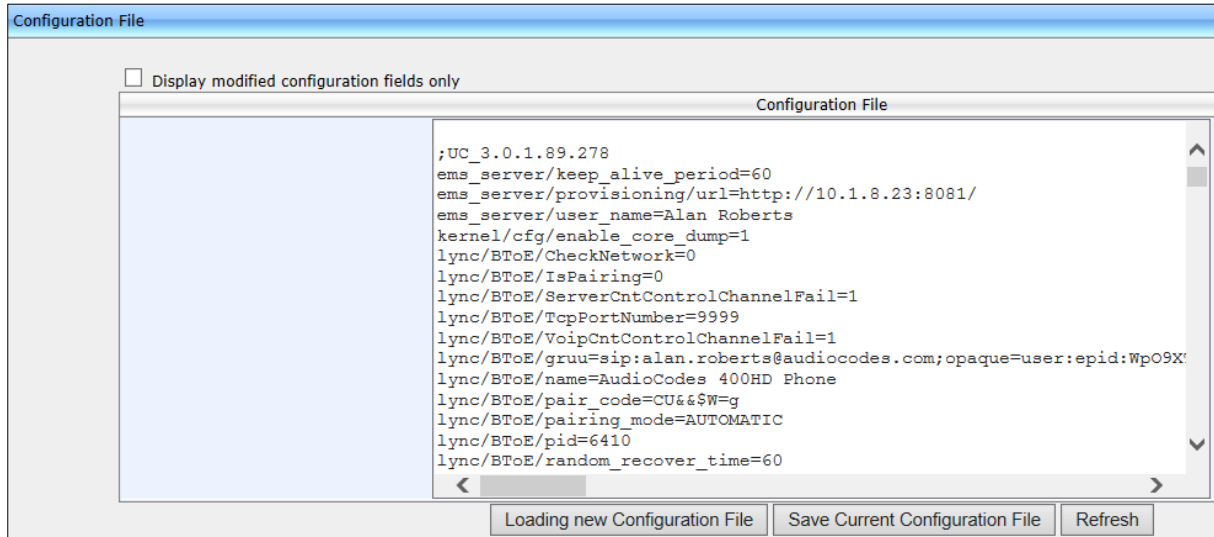
8.7.2 Loading the Configuration File Manually

This section shows how to load the cfg configuration file to the phone.

To load the cfg configuration file to the phone:

1. In the Web interface, open the Configuration File page (**Management tab > Manual Update menu > Configuration File**):

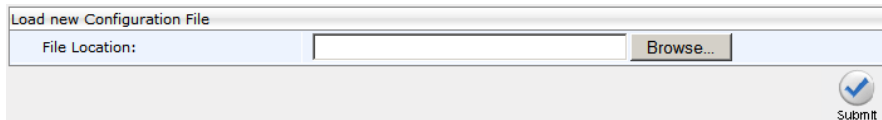
Figure 8-3: Web Interface - Configuration File



The configuration you created is displayed in the text pane.

2. Click **Loading new Configuration File**:

Figure 8-4: Web Interface - Load New Configuration File



3. Click **Browse** and select the cfg file you created; the phone verifies it's related to the phone model. The cfg is then loaded to the phone. Once loaded, the phone reboots (indicated on the screen); the phone is now loaded with the cfg file you created.

8.7.3 Recovering Firmware

If the phone is powered off for some reason during the firmware upgrade process, the phone becomes unusable.

To recover the phone firmware:

1. Ensure that your DHCP server supports Options 66 (TFTP server address) and 67 (firmware file), and that these are configurable.
2. Before connecting the phone, make sure the TFTP server is running and the firmware file for recovery is located in the correct location.



Make sure the firmware file for recovery is up to date. Make sure it's one of the latest GA firmware versions released by AudioCodes.

3. Connect your phone to the IP network and then connect the phone to the power outlet;
 - a. The phone sends a TFTP request to the IP address indicated in the DHCP Option 66 field to retrieve the firmware file indicated in the DHCP Option 67 field.
 - b. The phone, in the DHCP Discover message sends its model name in the DHCP Option 77 field. The DHCP server, according to the phone model, sets the appropriate firmware file name in the DHCP Option 67 field sent to the phone (e.g., 450HD_2.0.9.img).
 - c. The phone then upgrades to the recovery firmware.
 - d. After the firmware upgrade process completes, the phone boots up successfully.

See also Appendix B.

8.7.4 Restarting the Phone

The phone can be restarted from phone's screen or the Web interface.

8.7.4.1 Restarting the Phone from the Screen

This section shows how to restart the phone from its screen.

To restart the phone from its screen:

1. Open the Administration menu (MENU key > **Administration**).
2. Select the **Restart** option; a warning message pops up requesting you to confirm:

Warning: Restart the phone?

3. Select **Yes** to confirm phone restart or **No** to cancel.

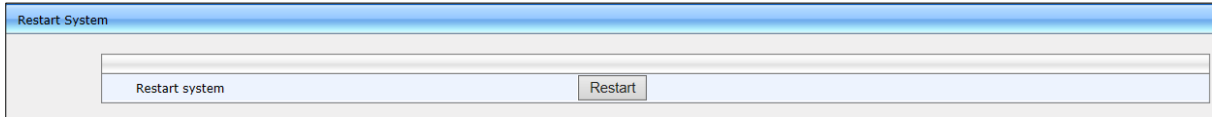
8.7.4.2 Restarting the Phone from the Web Interface

This section shows how to restart the phone from the Web interface:

To restart the phone from the Web interface:

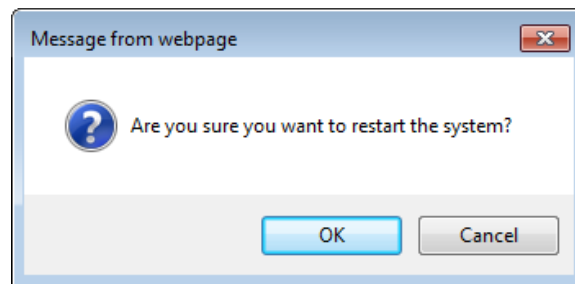
4. Open the Restart System page (**Management** tab > **Administration** menu > **Restart System**).

Figure 8-5: Web Interface - Restart System



5. Click **Restart**; you're prompted to confirm.

Figure 8-6: Confirmation Prompt



6. Click **OK**.

A Installing the Expansion Module

Before installing the Expansion Module for your phone, make sure the following items are included in the shipped box:

- Expansion Module
- Kit containing five screws



Applies to AudioCodes' 450HD and C450HD phones.

A.1 Installation Procedure



Before proceeding with the installation:

- Disconnect the phone from the Power Supply / Power over Ethernet (PoE)
- Obtain a Philips screwdriver

To connect the Expansion Module to the 450HD phone:

1. Step 1: Prepare the two units – see below
2. Step 2: Remove the phone's side panel – see [below](#)
3. Step 3: Connect the Expansion Module to the phone – see [below](#)
4. Step 4: Attach the panel removed from the phone in Step 3, to the Expansion Module – see [below](#)
5. Step 5: Secure the assembly – see [below](#)
6. Step 6: Install the Expansion Module's base stand and the phone's base stand - see [below](#)
7. Step 7: Mount the assembled unit - see [below](#)

A.1.1 Step 1: Place Phone and Module on a Table

Place the phone and the Expansion Module on a table alongside one other.



A.1.2 Step 2: Invert and Unscrew Three Screws

Invert the phone on a surface that won't scratch the screen such as a towel or printer paper. Avoid inverting the phone on the surface of a desk. Then unscrew the three screws shown below in order to remove the phone's side panel:



A.1.3 Step 3: Remove Rubber Cover and Connect

Return the phone to an upright position. Remove the Expansion Module's connector's rubber cover and then connect the Expansion Module to the phone. Note the connector and PEM direction.



A.1.4 Step 4: Attach the Panel

Attach the panel that you removed from the phone in Step 3 to the side of the Expansion Module:



A.1.5 Step 5: Secure the Side Panel

Invert the assembled unit and secure the side panel by screwing in the three screws:



A.1.6 Step 6: Secure the Connection of the Two Units

[Refer again to the figure above] Secure the connection of the two units by screwing in **these** five screws.

A.1.7 Step 7: Mount Phone on Base Stand, Expansion Module on Base Stand

With the assembly inverted, mount the phone on its dedicated base stand and the Expansion Module on its dedicated base stand, like this:



Slots in the stands are slid onto rails on the units. The figure above shows the phone mounted on the short edge of its 'L' shaped base stand, and the Expansion Module mounted on the short edge of its 'L' shaped base stand. The long edge of the 'L' can alternatively be used per user preference, depending on sources of glare in the office.

B Alternative Automatic Provisioning Methods

B.1 Static DNS Record Method

The Static DNS (Generic Domain Name) Record method is used for automatic provisioning when you are unable to manage your DHCP server. If the provisioning server does not support using SIP SUBSCRIBE and NOTIFY messages mechanism as described above and no response for the SIP SUBSCRIBE message has been received, the phone tries to retrieve firmware and configuration files using the following URL: **tftp://ProvisioningServer/<Phone Model Name>/**

For example:

- The phone tries to obtain the following firmware file:
tftp://ProvisioningServer/450HD/450HD.img
- The phone tries to obtain the following configuration file:
tftp://ProvisioningServer/450HD/<MAC address>.cfg
(e.g. tftp://ProvisioningServer/450HD/001122334455.cfg)

It is the Administrator's responsibility to configure a DNS entry called **ProvisioningServer** on the DNS server and set it to the TFTP server IP address.



If Generic Domain Name is used, the automatic provisioning mechanism periodically tries to retrieve new firmware/configuration from Provisioning Server domain name.

To configure Static DNS Record:

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table B-1: Static DNS Record Parameters

Parameter	Description
provisioning/firmware/url]	<p>The static URL for checking the firmware file. The URL must be entered using one of the following syntax options:</p> <ul style="list-style-type: none"> ■ <protocol>://<server IP address or host name> ■ <protocol>://<server IP address or host name>/<firmware file name> <p>Where <protocol> can be one of the following protocols: "ftp", "tftp", "http" or "https". For example:</p> <ul style="list-style-type: none"> ■ tftp://192.168.2.1 – retrieved firmware file is 450HD.img ■ ftp://192.168.2.1/Different_Firmware_Name.img - retrieved firmware file is Different_Firmware_Name.img <p>Note: This parameter is applicable only when method is configured to "Static".</p>
provisioning/configuration/url]	<p>The static URL for checking the configuration file. The URL must be entered using one of the following syntax options:</p> <ul style="list-style-type: none"> ■ <protocol>://<server IP address or host name> ■ <protocol>://<server IP address or host name>/<configuration file name> <p>Where <protocol> can be "ftp", "tftp", "http" or "https" and where <configuration file name> can be either:</p> <ul style="list-style-type: none"> ■ A unique configuration file, per phone, for example: <MAC>.cfg -or- ■ A global configuration file, per deployment, for example, 450HD.cfg <p><u>Unique Configuration Example</u> http://192.168.2.1/different.img;<MAC>.cfg The retrieved firmware file is <i>different.img</i> and the configuration file name is <MAC>.cfg such as 001122334455.cfg</p> <p><u>Global Configuration Example</u> http://192.168.2.1/<450HD>.cfg The configuration file name is 450HD.cfg</p> <p>Note: This parameter is applicable only when 'Method' is configured to Static.</p>

B.2 AudioCodes' HTTPS Redirect Server

AudioCodes' HTTPS redirect server can be used to direct phones to the provisioning server's URL, for downloading configuration and firmware files.

After the phone is powered up and network connectivity is established, the phone automatically requests provisioning information. If it doesn't get it according to the regular provisioning methods, it sends an HTTPS request to AudioCodes' HTTPS redirect server. The server responds to the phone with an HTTPS Redirect response containing the URL of the provisioning server where the firmware and configuration files are located. When the phone successfully connects to the provisioning server's URL, an Automatic Update mechanism begins.



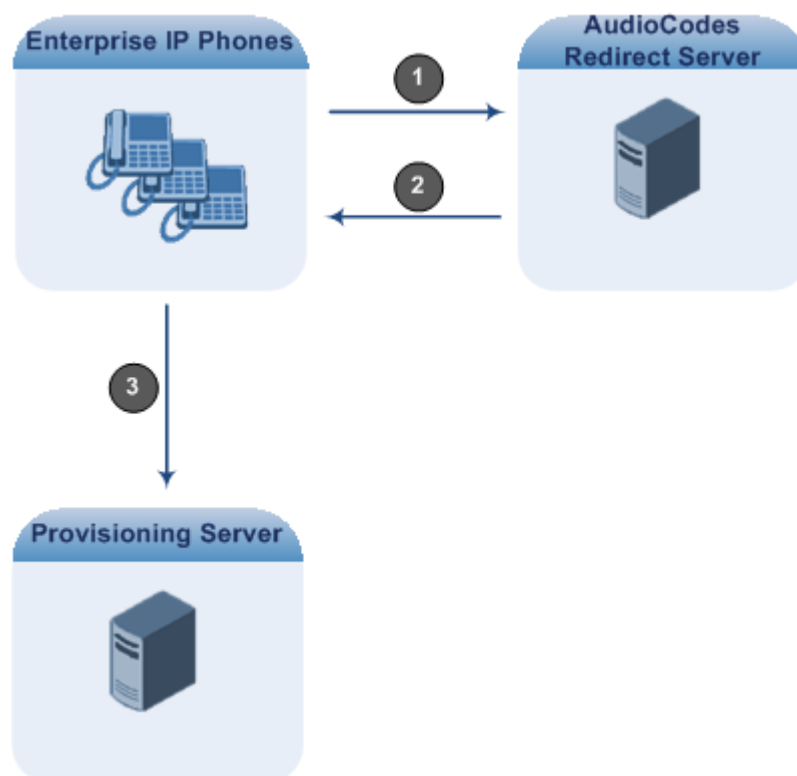
Phones' MAC addresses and the provisioning server's URL are preconfigured on the HTTPS redirect server. For more information, contact AudioCodes support.

AudioCodes' HTTPS redirect server's default URL is:

provisioning/redirect_server_url=https://redirect.audiocodes.com

This address can be reconfigured if required.

Figure A-7: HTTPS Redirect Server Directing Phones to Provisioning Server



B.2.1.1 Redirection Process

Here's how redirection is performed (refer to [Figure A-2](#)):

- 1 The phone sends an HTTPS request to the redirect server.
- 2 The redirect server sends an HTTPS response with the provisioning server's URL.
- 3 The phone sends a request for cfg and img files to the provisioning server.

Communications between the phone and the redirect server are encrypted (HTTPS) for security reasons. The phone uses the pre-installed AudioCodes factory-set certificate to authenticate itself with the redirect server and to verify the latter's authenticity. If the redirect URL (where the cfg file is located) also uses HTTPS protocol, the phone can use a regular certificate - or the AudioCodes factory-set certificate - to authenticate itself and to validate the server's certificate if a trusted root certificate (regular) is configured.



The phone repeats the redirect process whenever reset to factory defaults.

C Recovering AudioCodes' IP Phone

This appendix shows how to recover AudioCodes' IP phone.

To recover the phone, follow this procedure:

1. Identify that the phone is in recovery mode (see [below](#))
2. Recover the phone (see [below](#))
3. Make sure the phone downloaded the image file (see [below](#))

C.1 Identifying that the Phone is in Recovery Mode

This section shows how to identify that the phone is in recovery mode.

To identify that the phone is in recovery mode:

- Observe the following displayed in the phone's screen:

Figure B-1: Identifying Recovery Mode



-OR-

- Observe that the phone reboots every +-5 seconds.

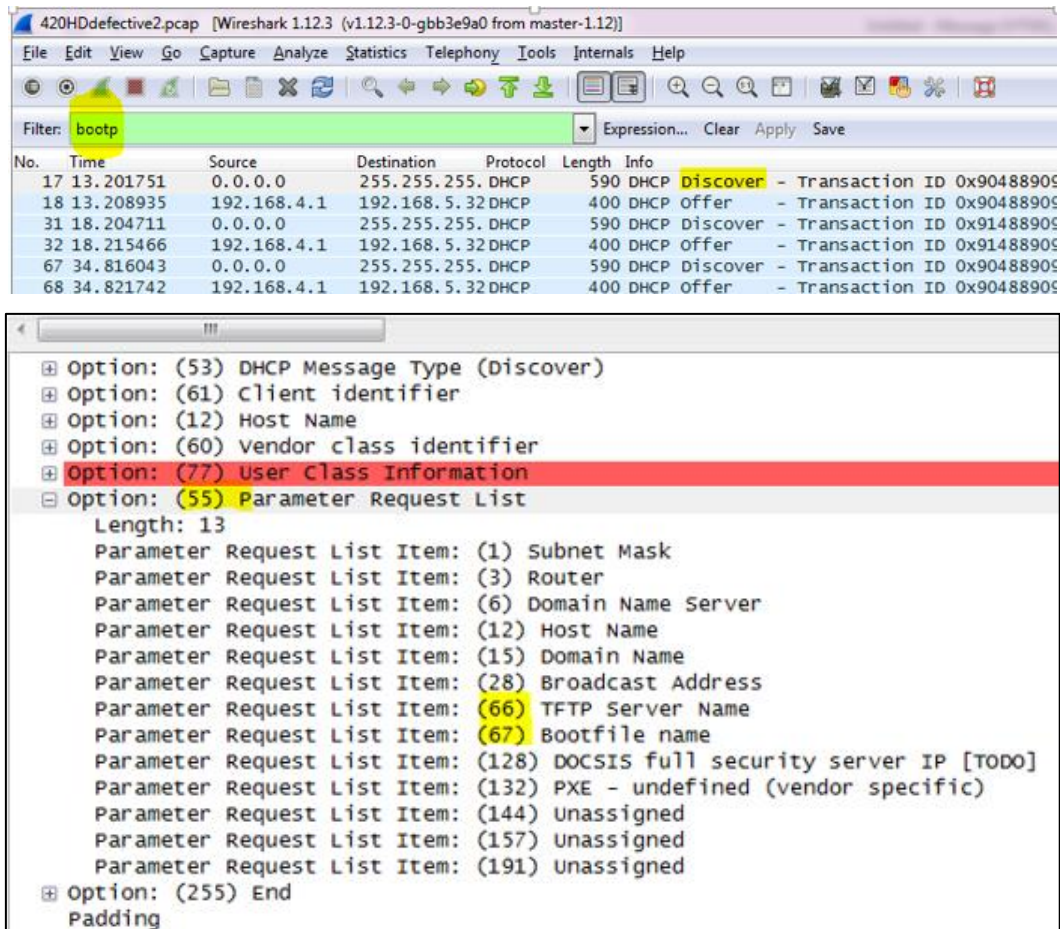
C.2 Making Sure the Phone is in Recovery Mode

You can make sure that the phone is in recovery mode.

To make sure the phone is in recovery mode:

1. Connect the phone to the PC and run Wireshark.
2. In Wireshark, filter by **bootp** and then check if the phone is requesting Option 66 (TFTP Server) & Option 67 (Bootfile) under Option 55 in the 'DHCP Discover' message, as shown in the figures below.

Figure B-2: Verifying Recovery Mode in Wireshark

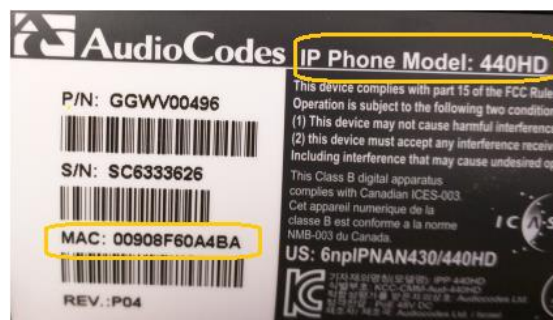


The screenshot shows the Wireshark interface with a filter set to 'bootp'. The packet list pane shows a DHCP Discover message (No. 17, Time 13.201751, Source 0.0.0.0, Destination 255.255.255.255, Protocol DHCP, Length 590). The packet details pane shows the following options:

- Option: (53) DHCP Message Type (Discover)
- Option: (61) Client identifier
- Option: (12) Host Name
- Option: (60) vendor class identifier
- Option: (77) User Class Information
- Option: (55) Parameter Request List
 - Length: 13
 - Parameter Request List Item: (1) Subnet Mask
 - Parameter Request List Item: (3) Router
 - Parameter Request List Item: (6) Domain Name Server
 - Parameter Request List Item: (12) Host Name
 - Parameter Request List Item: (15) Domain Name
 - Parameter Request List Item: (28) Broadcast Address
 - Parameter Request List Item: (66) TFTP Server Name
 - Parameter Request List Item: (67) Bootfile name
 - Parameter Request List Item: (128) DOCSIS full security server IP [TODO]
 - Parameter Request List Item: (132) PXE - undefined (vendor specific)
 - Parameter Request List Item: (144) unassigned
 - Parameter Request List Item: (157) unassigned
 - Parameter Request List Item: (191) unassigned
- Option: (255) End Padding

3. Make sure the source Ethernet MAC address is the same as that labeled on the base of the phone. For example:

Figure B-3: Source Ethernet MAC Address in Wireshark Identical to Phone Base's



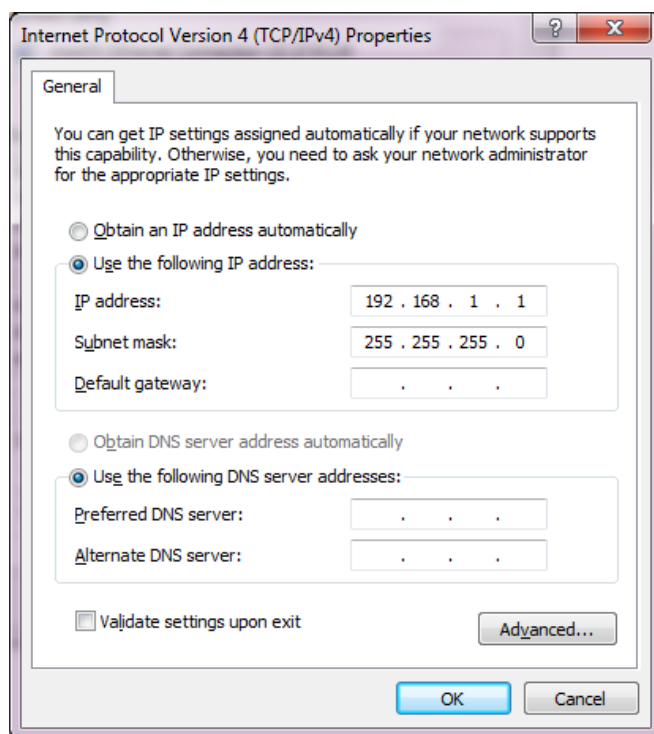
C.3 Recovering the Phone

This section shows how to recover the phone.

To recover the phone:

1. Configure the PC NIC to which the phone is connected as follows:
 - IP address: **192.168.1.1**
 - Subnet mask: **255.255.255.0**
 - [Figure B-4](#) below shows the configured settings.
2. Make sure the phone is directly connected (or via a network hub) to the PC LAN NIC.
3. Disable all other PC NICs (also wireless NICs).

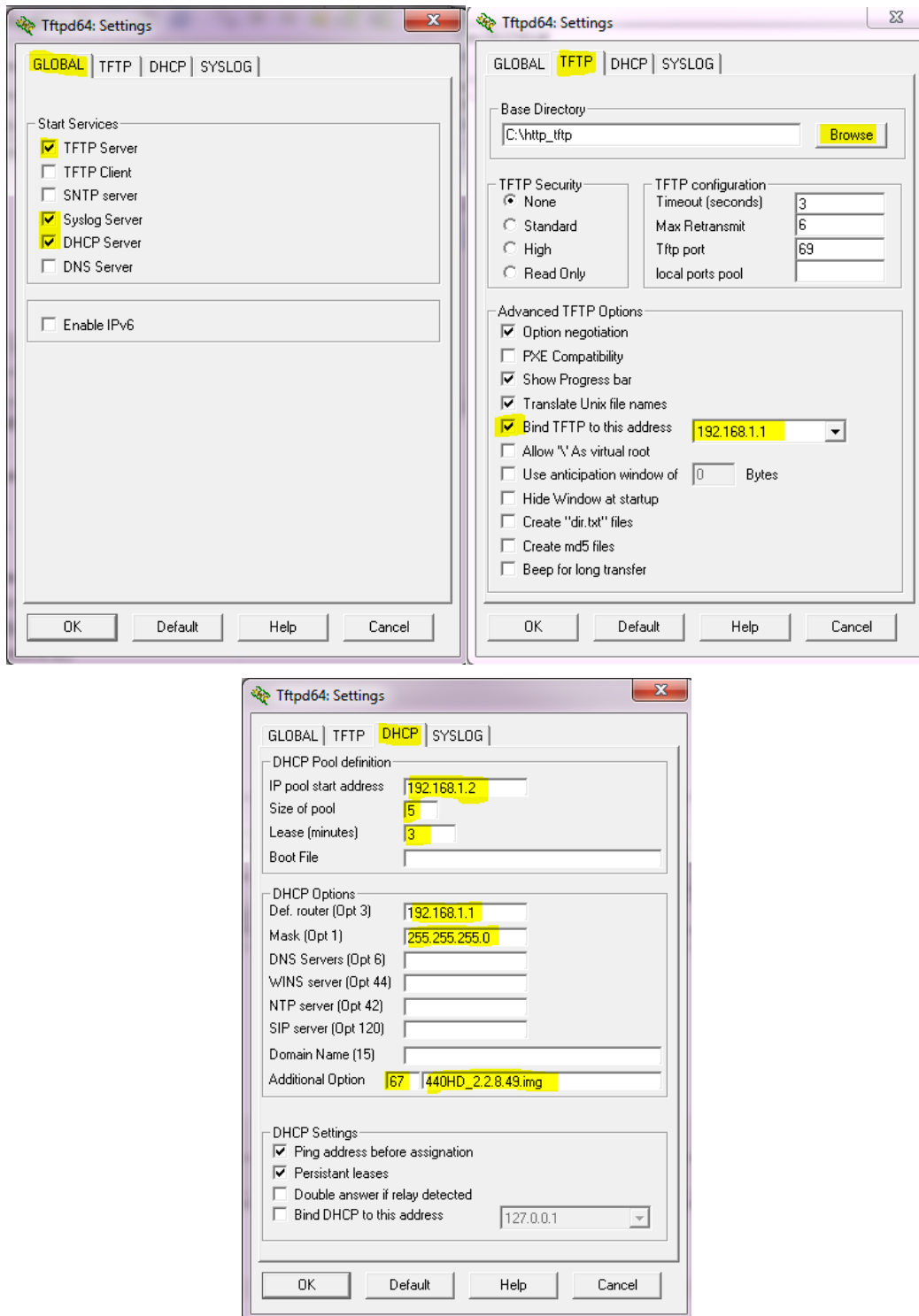
Figure B-4: Recovering the Phone - Configure the PC NIC to which the Phone is Connected



4. Download the following **tftpd64** freeware tool:
http://tftpd32.jounin.net/tftpd32_download.html
5. Run the tftpd64.exe executable.
6. Click Settings and configure the following settings:

Table C-1: Configuring tftpd64 Settings

Global	TFTP	DHCP
TFTP Server [=option66]	Browse to the directory in which the AudioCodes IP phone firmware is located.	IP pool start address: 192.168.1.2
Syslog Server	Bind the TFTP to IP address 192.168.1.1	Size of pool: 5
DHCP Server	Leave all other options at their default.	Lease: 3
		Default.router: 192.168.1.1
		Mask: 255.255.255.0
		Additional Option: 67, FW_file_name.img



7. For **tftps64** to accept the new settings, close and open **tftpd64**.

After (1) **tftpd64** is restarted, (2) the phone is directly connected to the PC, and (3) the network settings referred to above are applied, the phone immediately gets the required options [66 and 67] and begins downloading the firmware. Make sure the phone is downloading the image file as shown in the next section.

C.4 Make Sure the Phone is Downloading the Image File

This section shows how to make sure the phone is downloading the firmware image file.

To make sure the phone is downloading the image file:

- use Wireshark -or-
- use tftpd64 -or-
- use the phone screen

C.4.1 Making Sure Using Wireshark

1. In Wireshark, make sure the four DHCP 'DORA' (Discover; Offer; Request; ACK) steps are accomplished, as shown in the figure below.

Figure B-5: Make Sure with Wireshark that the Phone is Downloading Phone .img File

The screenshot shows the Wireshark interface with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
4	13.029407000	0.0.0.0	255.255.255.	DHCP	590	DHCP Discover - Transaction ID 0x9160a4ba
6	13.556598000	192.168.1.1	255.255.255.	DHCP	359	DHCP Offer - Transaction ID 0x9160a4ba
7	13.561085000	0.0.0.0	255.255.255.	DHCP	590	DHCP Request - Transaction ID 0x9160a4ba
8	13.568623000	192.168.1.1	255.255.255.	DHCP	359	DHCP ACK - Transaction ID 0x9160a4ba
61	17.427393000	192.168.1.1	255.255.255.	DHCP	330	DHCP Inform - Transaction ID 0x563d2f0

The details pane for Frame 8 (DHCP ACK) shows the following options:

- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x9160a4ba
- Seconds elapsed: 0
- Bootp flags: 0x0000 (unicast)
- Client IP address: 0.0.0.0 (0.0.0.0)
- Your (client) IP address: 192.168.1.2 (192.168.1.2)
- Next server IP address: 127.0.0.1 (127.0.0.1)
- Relay agent IP address: 0.0.0.0 (0.0.0.0)
- Client MAC address: AudioCod_60:a4:ba (00:90:8f:60:a4:ba)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (ACK)
- Option: (54) DHCP Server Identifier
- Option: (1) Subnet Mask
- Option: (3) Router
- Option: (51) IP Address Lease Time
- Option: (58) Renewal Time value
- Option: (59) Rebinding Time Value
- Option: (7) Log Server
- Option: (66) TFTP Server Name
 - Length: 9
 - TFTP Server Name: 127.0.0.1
- Option: (67) Bootfile name
 - Length: 18
 - Bootfile name: 440HD_2.2.8.49.img
- Option: (255) End

2. Filter by TFTP, as shown in the figure below.

Figure B-6: Verifying .img File Download with Wireshark – Filtering by TFTP

The screenshot displays the Wireshark network protocol analyzer interface. The filter bar at the top is set to 'tftp'. The packet list pane shows a series of TFTP packets between 192.168.1.1 and 192.168.1.2. Packet 40026 is highlighted, and its details pane is expanded to show the following information:

- Frame 40026: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface 0
- Ethernet II, Src: f8:ca:b8:52:3d:d3 (f8:ca:b8:52:3d:d3), Dst: AudioCod_60:a4:ba (00:90:8f:60:a4:ba)
- Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
- User Datagram Protocol, Src Port: 53520 (53520), Dst Port: 2000 (2000)
- Trivial File Transfer Protocol
 - [Source File: 440HD_2.2.8.49.img]
 - Opcode: Data Packet (3)
 - Block: 19954
 - Data (512 bytes)

C.4.2 Making Sure Using tftpd64

In **tftpd64**, view the indications shown in the figures below.

Figure B-7: Verifying .img File Download using tftpd64

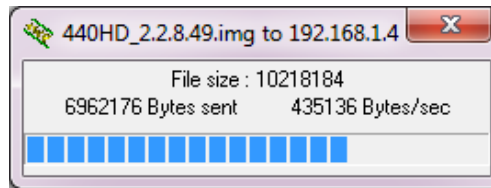
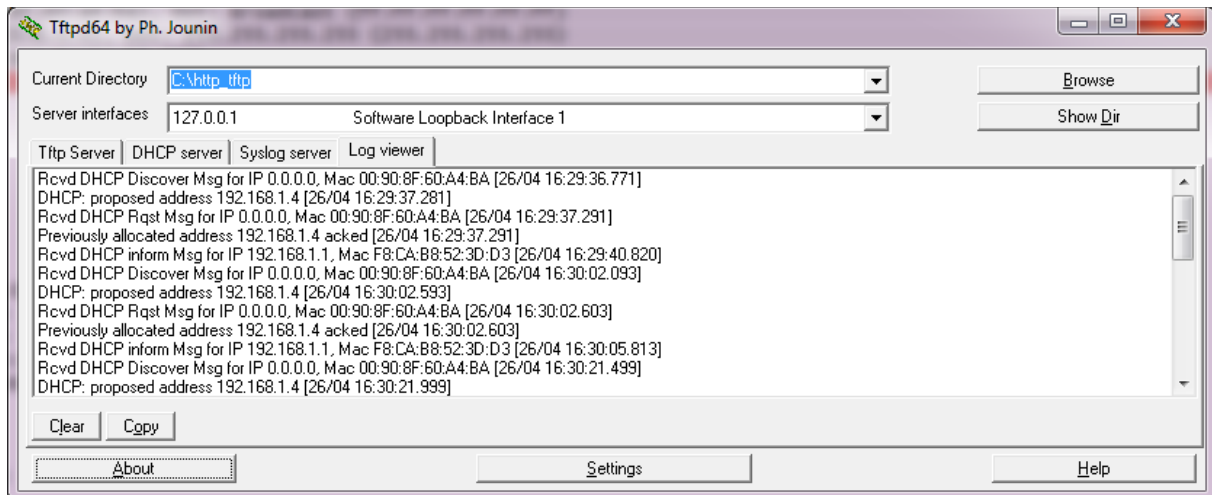


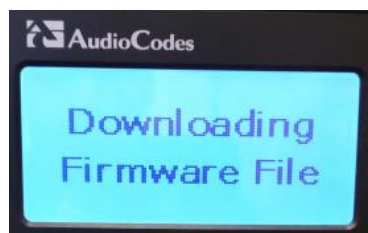
Figure B-8: Verifying .img File Download using tftpd64



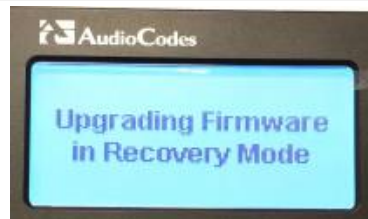
C.4.3 Making Sure Using the Phone Screen

In **tftpd64**, view the indications shown in the figures below.

Figure B-9: Verifying .img File Download from the Phone Screen



Important: Do not unplug / power-off the phone while the screen displays the message shown below.



You can disconnect the phone from the PC and connect to the network LAN *only after the firmware upgrade finishes*, that is, after the phone's screen displays the following:

Discovering CDP...Discovering LLDP...Acquiring IP...

The phone is now up, functioning, and ready to be provisioned.

D Huddle Room Solution (HRS)

This appendix describes Web interface parameters and functionalities that are unique to the HRS. *Note that the HRS does not support BToE, paging and Boss Admin (though Delegates is supported).* In the System Information page shown below, parameters 'Speaker Model Name' and 'Speaker Firmware Version' apply only to the HRS Web interface.

Figure C-10: System Information page

System Information	
Model Name	UC-HRS-457
Firmware Version	UC_3.0.2.141.3
Release Date	2017-11-06_19:50:53
Speaker Model Name	HRS_457
Speaker Firmware Version	110

These parameters are not displayed in the Web interface of the other phones. The first refers to the Jabra speaker model name. The second to its firmware version.

In the Release Information page shown below, parameters 'Conference Speaker Device type' and 'Conference Speaker Device FW version' apply only to the HRS Web interface.

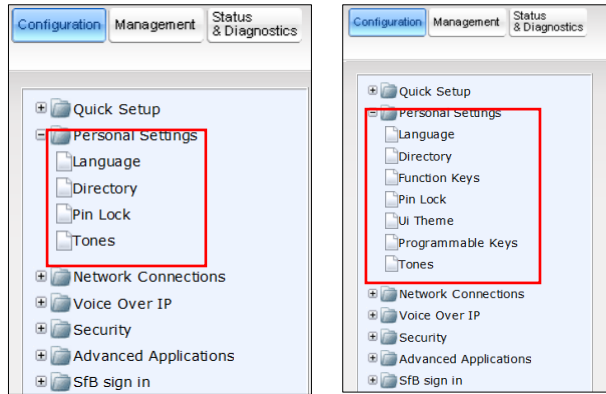
Figure C-11: Release Information page

Release Information	
BLVERSION	1.0.33
BUILD_TIME	2017-11-06_19:50:53
DSPFWVERSION	494E002ce2.720.32
HW_TYPE	UC-HRS-457
LOG	0
SWVERSION	UC_3.0.2.141.3
SW_TYPE	LYNC
Conference Speaker Device type	HRS_457
Conference Speaker Device FW version	110

These parameters are not displayed in the Web interface of the other phones. The first refers to the Jabra speaker type. The second refers to the Jabra speaker firmware version.

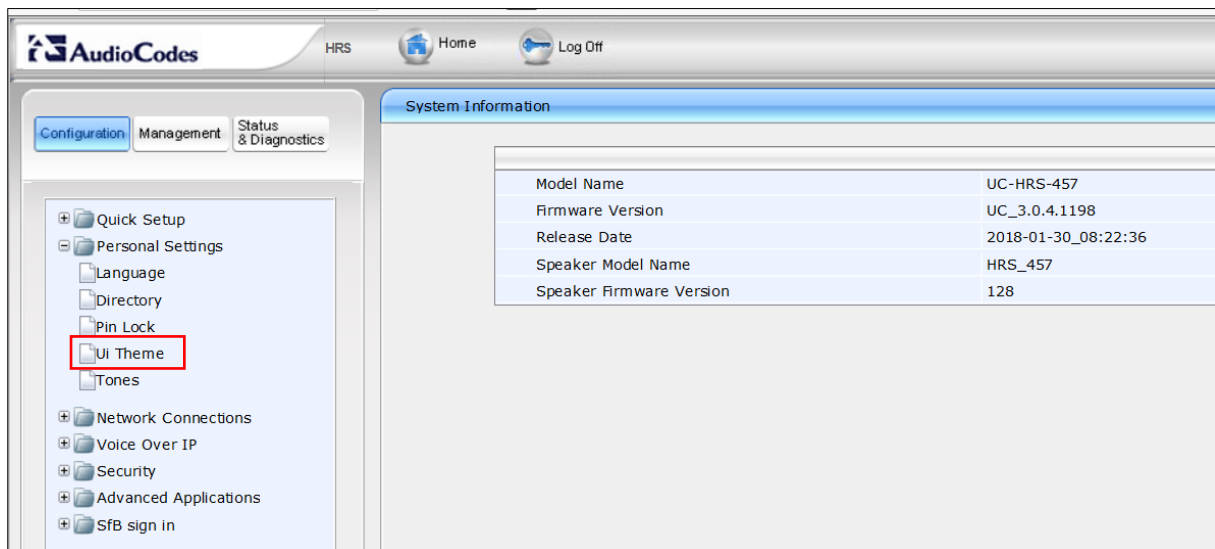
In the navigation tree under the Configuration tab, Personal Settings shown below, the HRS does not display Function Keys, UI Theme and Programmable Keys.

Figure C-12: Personal Settings (Left HRS | Right 450HD and C450HD)



The HRS' UI Theme can be changed in the Web interface. You can select MSFT (Microsoft) or AudioCodes.

Figure C-13: UI Theme



E Migrating from Skype for Business to Teams Environment

Read this appendix when migrating from Microsoft Skype for Business to Microsoft Teams. AudioCodes phones are Teams compatible and will continue operating as normal after migration. Users currently using **Exchange Username and Password** to sign in to their phones should not have issues due to this migration. Users using **Pin Code and Extension**, however, need to change their sign-in method and start using **Exchange Username and Password**. This appendix provides step-by-step instructions on how to sign in to your phone using the **Web Sign-in (Cloud)** method.



Important:

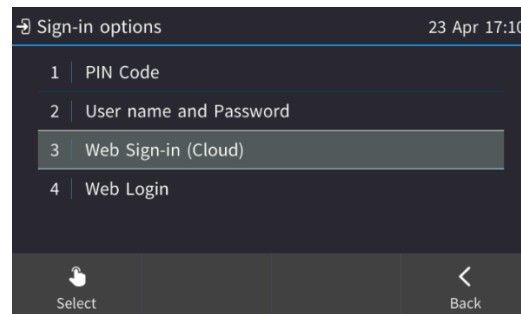
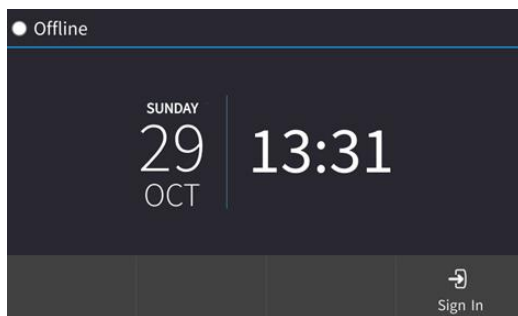
- After completing the migration procedure, your phone may lose its registration with the server and may require that you sign out before signing in through **Web Sign-in**. If this occurs, see [here](#) for instructions on how to sign out before signing in again.
- In addition, your phone may attempt to sign in repeatedly. If this occurs, use the **Cancel** softkey to cancel the sign-in attempts, and then proceed to sign in to the phone.

E.1 Signing in with Web Sign-in (Cloud)

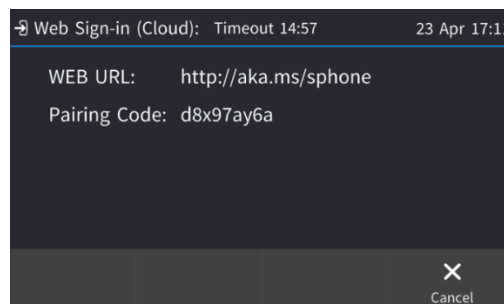
Signing in to your phone using the **Web Sign-in (Cloud)** option enables connectivity to Microsoft's Cloud PBX, which is Microsoft's cloud-hosted version for enterprise voice.

To sign in with the **Web Sign-in (Cloud)** option:

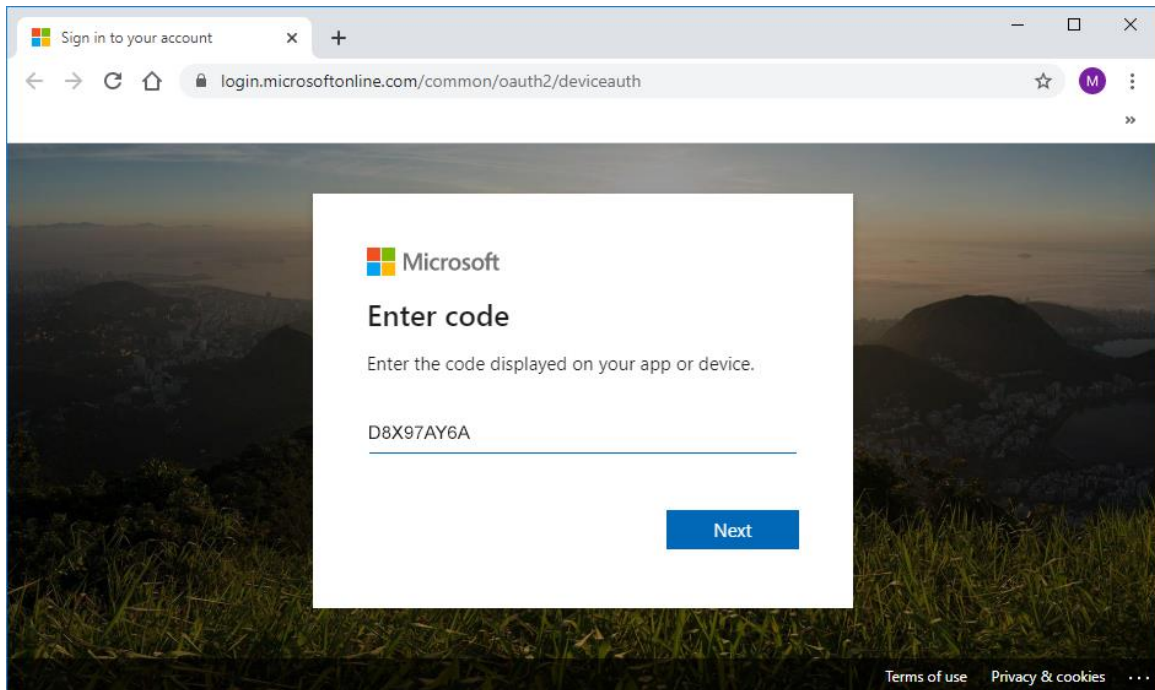
1. On your phone, select the **Web Sign-in (Cloud)** option:



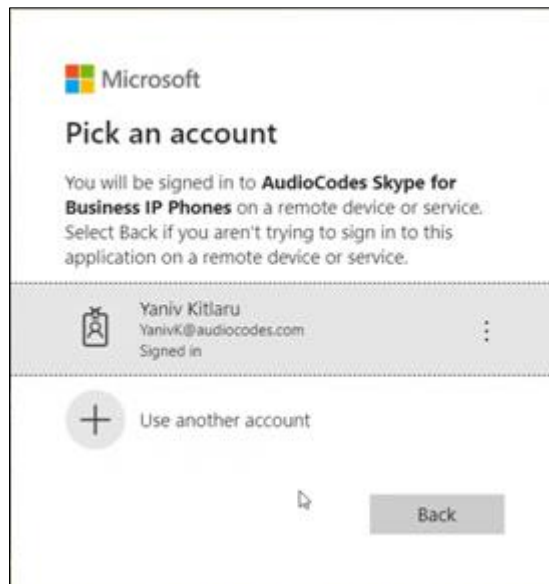
2. View in the phone screen a Web URL and Pairing Code that's displayed:



3. Using a standard web browser, go to Microsoft's Cloud PBX login page at <http://aka.ms/sphone> (i.e., URL displayed on your phone's LCD).
4. Enter the Pairing Code (as displayed on your phone's LCD):



5. Click **Next**; the following screen appears:



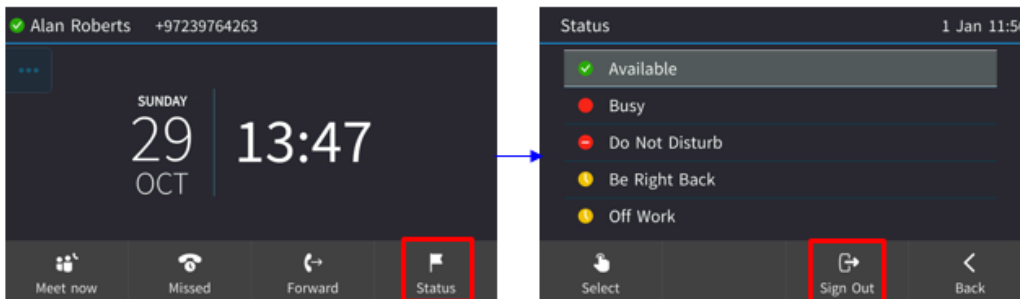
6. Select your account name; the following message appears, indicating that you have successfully signed in:



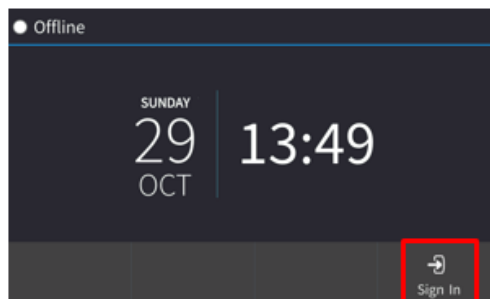
E.2 Signing Out and then Signing In Again

If your computer's password was changed, sign-out of your phone and then sign in again as follows:

1. In the idle screen, touch the **Status** softkey.
2. In the Status screen, touch the **Sign Out** softkey.
3. In the idle screen (Offline), touch the **Sign In** softkey to sign in.



You're signed out and returned to the offline screen displaying the **Sign in** softkey.



F Switching Devices from Teams Compatible to Teams Native Mode

This appendix shows how to configure a provisioning template and upload software files on the AudioCodes Device Manager or OVOC to switch devices from Teams Compatible to Teams Native mode.

F.1 Prerequisites

- Device Manager or OVOC installed on the management server
- Teams Compatible firmware file: *UCC450HD_3.4.5.2.img* or later
- Teams Native firmware file: *C450HD_TEAMS_1.8.288.android_images.zip* or later
- Teams native .md5 file: *C450HD_TEAMS_1.8.288.android_images.zip.md5*

F.2 Upload Software Files to the Device Manager

F.2.1 Enable MD5 File Uploading to the Device Manager

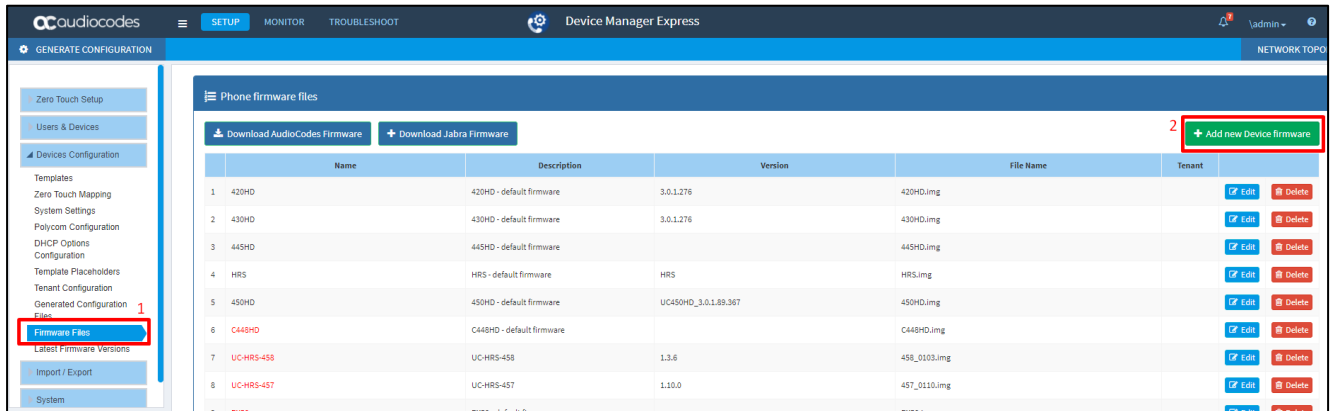
1. In the Device Manager, go to **Setup > System Settings**.
2. In the System Settings page, go to **Upload File Extensions**.
3. Add **.md5** to the 'Accept Extensions' field and click **Save**.

Upload File Extensions

Accept Extensions Note: Use ', ' as delimiter of the extensions ('.cfg,.img,.zip').

F.2.2 Upload Teams Compatible Firmware File

1. Upload the file *UCC450HD_3.4.5.2.img* to the Device Manager.
2. Go to **Setup > Devices Configuration > Firmware Files**.
3. Click **Add new device firmware**



4. Enter Name, Description, Version (without suffix .img) and Tenant.
5. Click **Continue & Upload**.

+ Add new Device firmware

Name:

Description:

Version:

Tenant:

↑ Continue & Upload

← Back

6. Click **Upload firmware file:**

Device UCC450HD_3.4.5.2 Firmware

Name:
UCC450HD_3.4.5.2

Description:
UCC450HD_3.4.5.2

Version:
UCC450HD_3.4.5.2

Tenant:
Default

Upload firmware file

Save Back

7. Browse to the file *UCC450HD_3.4.5.2.img*:

Upload Device Firmware UCC450HD_3.4.5.2

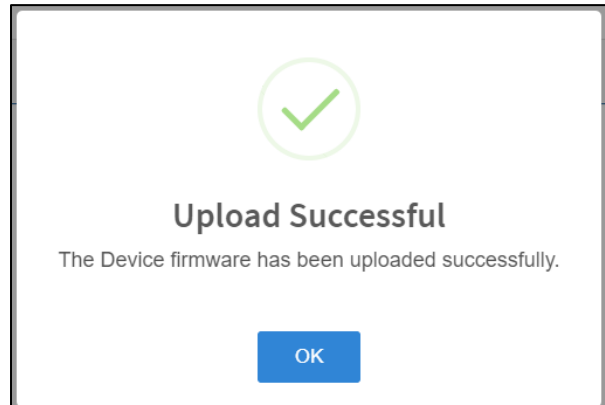
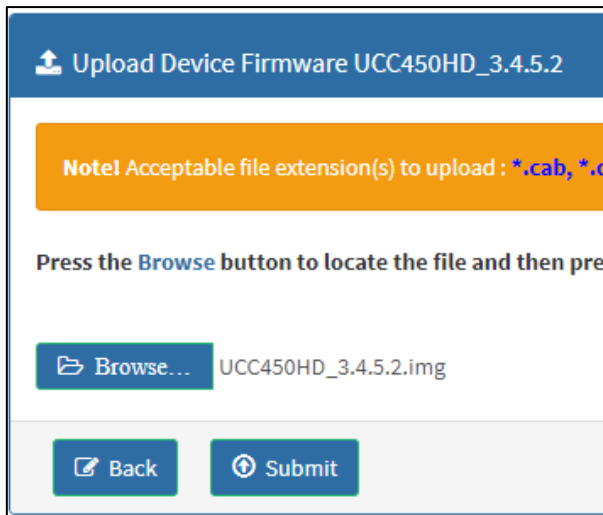
Note! Acceptable file extension(s) to upload : *.cab, *.cfg, *

Press the **Browse** button to locate the file and then press th

Browse... No file chosen

Back

8. Click **Submit**:



F.2.3 Upload Teams Native Firmware

1. Upload file C450HD_TEAMS_1.8.288.android_images.zip to the Device Manager.
2. Repeat the steps shown in the previous section for the file *C450HD_TEAMS_1.8.288.android_images.zip*.

F.2.4 Upload MD5 File

1. Upload the file C450HD_TEAMS_1.8.288.android_images.zip.md5 to the Device Manager.
2. Repeat the steps shown in the section before the previous for the file *C450HD_TEAMS_1.8.288.android_images.zip.md5*.

F.2.5 Verify Files Successful Upload

- Check the phone's firmware files to make sure all files were uploaded with the correct name and extension.

31	C450HD_TEAMS_1.8.288.android_images.zip	C450HD_TEAMS_1.8.288-.md5	C450HD_TEAMS_1.8.288.android_images.zip	C450HD_TEAMS_1.8.288.android_images.zip.md5	Default		
32	C450HD_TEAMS_1.8.288.android_images	C450HD_TEAMS_1.8.288.android_images	C450HD_TEAMS_1.8.288.android_images	C450HD_TEAMS_1.8.288.android_images.zip	Default		
33	UCC450HD_3.4.5.2	UCC450HD_3.4.5.2	C450HDUC_3.4.5.2	UCC450HD_3.4.5.2.img	Default		

C450HD_TEAMS_1.8.288.android_images.zip.md5	Default		
C450HD_TEAMS_1.8.288.android_images.zip	Default		
UCC450HD_3.4.5.2.img	Default		

F.3 Add Parameters to Provision in the Teams Phone Template

1. Go to Setup > Devices Configuration > Templates.
2. Edit the Teams IP-Phone template.
3. Add the parameters below to the template:

```
provisioning/AndroidUpdate/FirmwareUrl=https://<DM IP address>/<firmware folder>/C450HD_TEAMS_1.8.288.android_images.zip
provisioning/AndroidUpdate/AutomaticSwitchToTeams=1
```

4. Click **Save**.

Example:

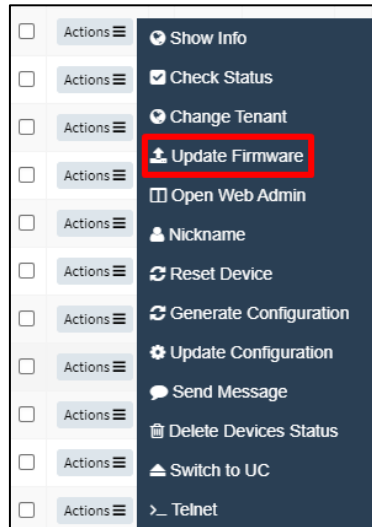
Edit template

```
<file_config>
  <type>file</type>
  <profile>user</profile>
  <encrypt_mode>0</encrypt_mode>
  <name>%ITCS_mac%.cfg</name>
  <destinationDir>%ITCS_destination%/</destinationDir>
<data><![CDATA[include Audiocodes_C450HD_global_LYNC_empty.cfg
management/telnet/enabled=1
provisioning/AndroidUpdate/FirmwareUrl=https://10.59.160.109/ipp_files/firmware/C450HD_TEAMS_1.8.288.android_images.zip
provisioning/AndroidUpdate/AutomaticSwitchToTeams=1
ems_server/keep_alive_period=1
provisioning/configuration/url=%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/configfiles/
provisioning/method=STATIC
provisioning/period/daily/time=0:00
provisioning/period/hourly/hours_interval=24
provisioning/period/type=DAILY
provisioning/period/weekly/day=SUNDAY
provisioning/period/weekly/time=0:00
provisioning/random_provisioning_time=120
provisioning/redirect_server_url=https://redirect.audiocodes.com
ems_server/user_name=%ITCS_Line1AuthName%
ems_server/user_password=%ITCS_Line1AuthPassword%
provisioning/firmware/url=%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/firmwarefiles/%ITCS_FirmwareFile%
ems_server/provisioning/url=%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/ipprest/lync_auto_prov.php
network/lan/vlan/id=%ITCS_VLANID%
network/lan/vlan/mode=%ITCS_VLANMode%
network/lan/vlan/period=30
network/lan/vlan/priority=%ITCS_VLANPriority%
```

Save Cancel

F.4 Upgrade the Phone to Teams Compatible Transition Firmware

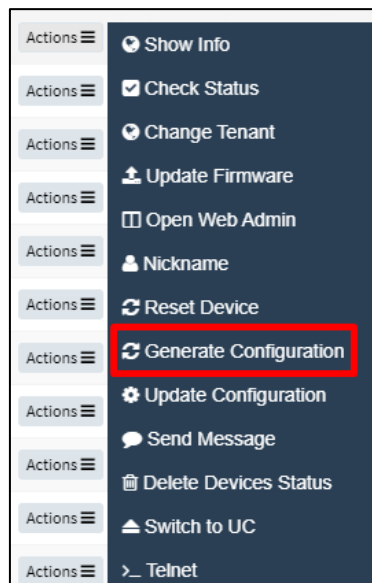
1. Go to Monitor > Device Status.
2. Upgrade the phone to firmware version *UCC450HD_3.4.5.2* (or later) by clicking **Actions** > **Update Firmware**.



F.5 Generate Configuration on the Phone



1. After the phone completes the upgrade to *UCC450HD_3.4.5.2* (or higher), set the switching provision by clicking **Actions** > **Generate Configuration**.

The phone then updates the configuration, reboots and starts the switching process to Teams Native.



F.6 Verify Successful Upgrade to Teams Native

After the phone finishes switching and upgrading to Teams Native, check that it's connected to the Device Manager/OVOC and that the firmware matches.

Model	Firmware	Tenant	Template	Report Time
  C450HD	TEAMS_1.8.288	Default		2020.11.26 08:39:10

G Specifications

See AudioCodes' *400HD IP Phone Series Release Notes* for detailed information about the phones' specifications.

G.1 SIP Support (RFC, Headers)

The following is a list of supported SIP RFCs and methods that you can use to create for the phone.

Table G-1: Supported IETF RFCs

RFC Number	RFC Title
RFC 2327	SDP
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
RFC 2782	A DNS RR for specifying the location of services
RFC 2833	Telephone event
RFC 3261	SIP
RFC 3262	Reliability of Provisional Responses in SIP
RFC 3263	Locating SIP Servers
RFC 3264	Offer/Answer Model
RFC 3265	(SIP)-Specific Event Notification
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
RFC 3326 (Partially Supported)	Reason header
RFC 3389	RTP Payload for Comfort Noise
RFC 3515	Refer Method
RFC 3605	RTCP attribute in SDP
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)
RFC 3665	SIP Basic Call Flow Examples
RFC 3711	The Secure Real-time Transport Protocol (SRTP)
RFC 3725	Third Party Call Control
RFC 3842	MWI
RFC 3891	"Replaces" Header
RFC 3892 (Sections 2.1-2.3 and 3 are supported)	The SIP Referred-By Mechanism
RFC 3960 (Partially Supported)	Early Media and Ringing Tone Generation in SIP (partial compliance)
RFC 3966	The tel URI for Telephone Numbers
RFC 4028 (Partially Supported)	Session Timers in the Session Initiation Protocol
RFC 4240	Basic Network Media Services with SIP - NetAnn

RFC Number	RFC Title
draft-ietf-sip-privacy-04.txt (Partially Supported)	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header
draft-ietf-sipping-cc-transfer-05	Call Transfer
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol



The following SIP features are not supported:

- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- S/MIME
- Outbound, Managing Client-Initiated Connections (RFC 5626)
- SNMP SIP MIB (RFC 4780)
- SIP Compression – RFC 5049 (SigComp)
- ICE (RFC 5245)
- Connected Identity (RFC 4474)

G.1.1 SIP Compliance Tables

The SIP device complies with RFC 3261 as shown in the following subsections.

G.1.1.1 SIP Methods

The device supports the following SIP methods:

Table G-2: Supported SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	Inside and outside of a dialog
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
PUBLISH	Yes	Send only
SUBSCRIBE	Yes	

G.1.1.2 SIP Headers

The device supports the following SIP headers:

Table G-3: Supported SIP Headers

Header Field	Supported
Accept	Yes
Alert-Info	Yes
Allow	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes

Header Field	Supported
Diversion	Yes
Encryption	No
Expires	Yes
Fax	Yes
From	Yes
History-Info	Yes
Join	Yes
Max-Forwards	Yes
MIN-SE	Yes
P-Asserted-Identity	Yes
P-Preferred-Identity	Yes
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Prack	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Replaces	Yes
Remote-Party-ID	Yes
Retry-After	Yes
Route	Yes
Session-Expires	Yes
Supported	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Website: <https://www.audiocodes.com>

©2021 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-09964

