# 400HD IP Phones Series for Microsoft® Skype™ for Business

Version 3.0.4

Microsoft **Partner**

Gold Communications

Skype for Business

audiocodes

# Table of Contents

# List of Figures

# List of Tables

This page is intentionally left blank.

> ## 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: Jan-22-2018

## Trademarks

AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

## WEEE EU Directive

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

## Customer Support

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

## 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 http://online.audiocodes.com/doc-feedback.

## Related Documentation

| Document Name |
| --- |
| 405HD IP Phone User's Manual |
| 420HD IP Phone User's Manual |
| 430HD and 440HD IP Phone User's Manual |
| 450HD IP Phone User's Manual |
| 405HD IP Phone Quick Guide |
| 420HD IP Phone Quick Guide |
| 430HD IP Phone Quick Guide |
| 440HD IP Phone Quick Guide |
| 450HD IP Phone Quick Guide |
| IP Phone Management Server Administrator's Manual |
| One Voice Resiliency Configuration Note |

## Regulatory Information

Compliancy and Regulatory Information can be viewed at:
http://www.audiocodes.com/library.

> **Note:** Throughout this document, where features can be configured using the Web interface or configuration file, the Web parameter is displayed in the regular font above its corresponding configuration file parameter, which is enclosed in square brackets in bold font type.

# 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' 400HD Series of IP Phones includes the 405HD, 420HD, 430HD, 440HD and 450HD models.

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

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.

This page is intentionally left blank.

# 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.

> **Note:** Instead of using DHCP as the automatic provisioning method, you can alternatively use Static DNS Record or SIP SUBSCRIBE and NOTIFY messages (see Appendix A).

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 the Microsoft Skype for Business environment.

These steps are described in detail in the following sections.

> **Note:** Automatic mass provisioning of IP phones using the DHCP provisioning method can alternatively be performed from the AudioCodes EMS Provisioning Server in the IP Phones Management Server. For detailed information, see the *IP Phone Management Server Administrator's Manual*.

**Figure 2-1: Setting up Automatic Provisioning**

**1**

Prepare the Microsoft Skype for Business environment for IP phones, e.g., configure the DHCP server with DHCP Option 160 to point to the provisioning server's URL

**2**

Without signing in, save a single phone's default configuration as a .cfg file, using the Web interface

**3**

Configure this single phone to perform according to your specific performance requirements in the enterprise

**4**

Save the phone's newly configured settings as a .cfg file

**5**

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

**6**

Load this delta .cfg file to another phone. Sign in. Test performance to see if it matches requirements.

**7**

Place the delta .cfg file on the provisioning server

**8**

Connect all IP phones to the network and power up. Phones are automatically provisioned

## 2.1 Preparing the Microsoft Skype for Business Environment for IP Phones

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

To prepare it for IP 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
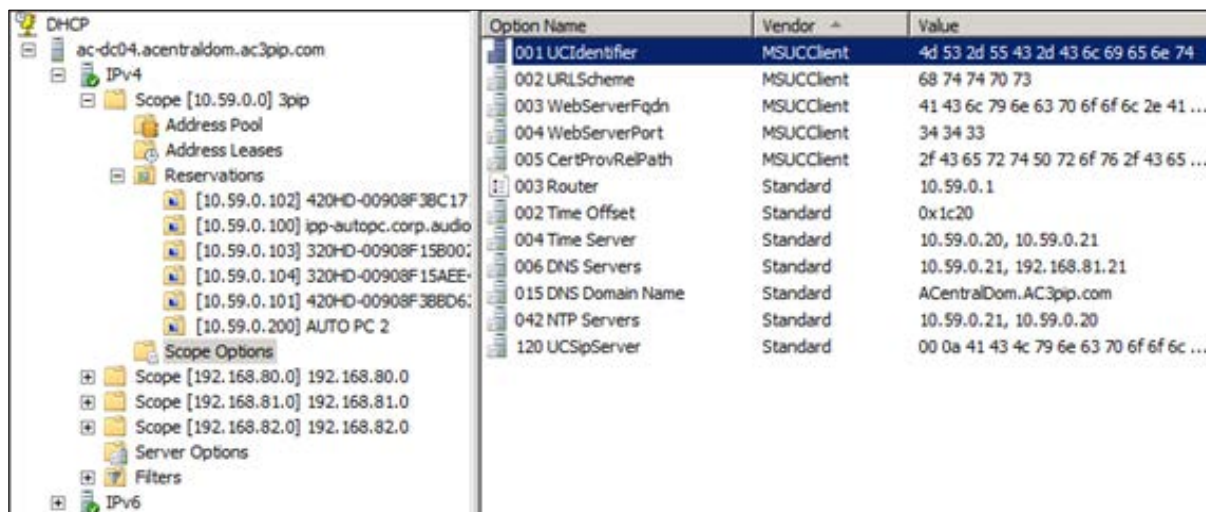
### 2.1.1 Making Sure DHCP Server Options are Correctly Configured

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

**Figure 2-2: DHCP Server Options**



Make sure:

■ DHCP Option 43 (comprising 001-005 in the figure above) is correctly configured (see Section 2.1.1.1 on page 22 below)

■ DHCP Option 120 is correctly configured (see Section 2.1.1.3 on page 22 below)

■ DHCP Option 42 is correctly configured (see Section 2.1.1.4 on page 22 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

**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 | lyncserver.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

**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 | lyncserver.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.

> **Note:**
>
> •    The examples below show DHCP server **acrtplab-ad.audiocodes.local**
> •    The examples below show IPv4 addresses

**Figure 2-3: DHCP Options Assigned to IPv4 Addresses**
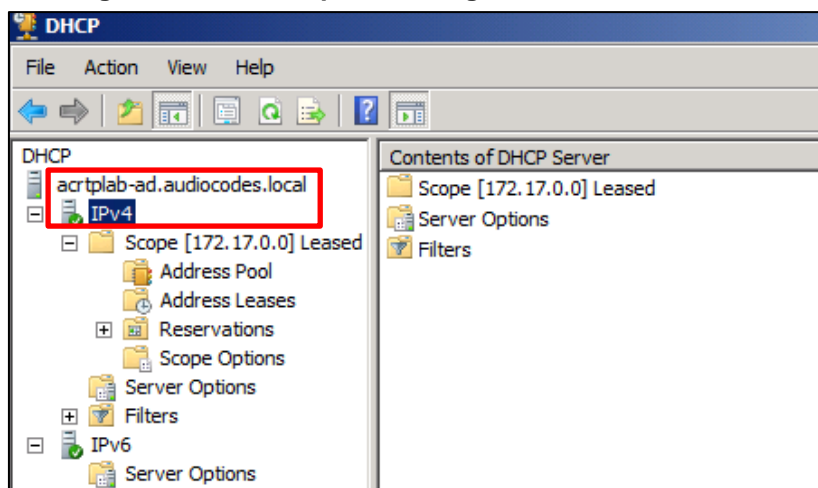


**3.**    Define a separate **User Class** for each AudioCodes phone model deployed (405HD, 420HD, 430HD, 440HD and 450HD phone models): Right-click the **IPv4** server icon and from the popup menu, select **Define User Classes…**

**Figure 2-4: Defining User Classes**
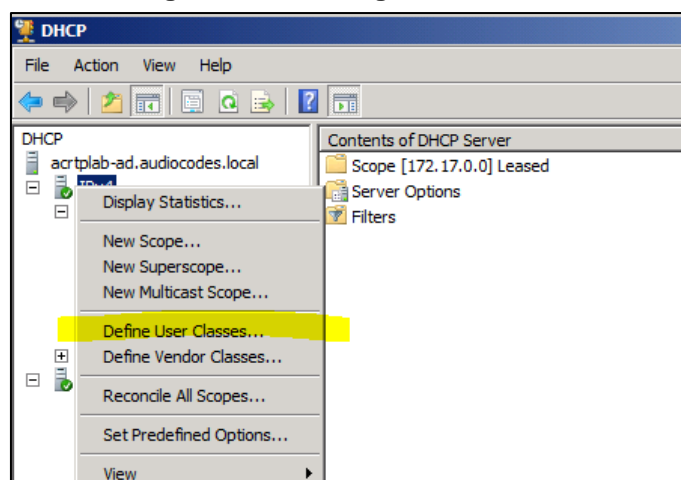
The DHCP User Classes dialog opens.

**Figure 2-5: DHCP User Classes**
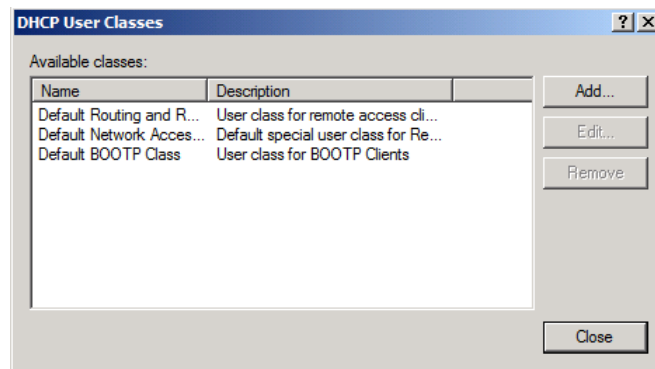


4. Click **Add…**

**Figure 2-6: New Class**
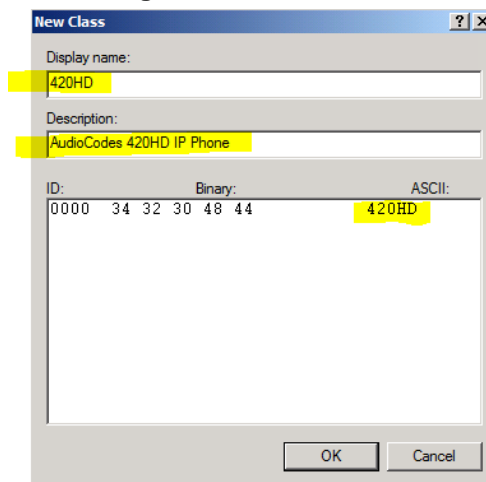


5. In the New Class dialog, enter **Display name** and **Description** as shown in the figure above, and then in the **ASCII** field, enter the **User Class Phone Type** (see the Packet Bytes window in Wireshark below for an example of the 420HD phone, and see the table below for the other AudioCodes 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 |
|---|---|---|
| 420HD | AudioCodes 420HD IP Phone | 420HD |
| 430HD | AudioCodes 430HD IP Phone | 430HD |
| 440HD | AudioCodes 440HD IP Phone | 440HD |
| 450HD | AudioCodes 450HD IP Phone | 450HD |
| 405HD | AudioCodes 405HD IP Phone | 405HD |

**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**
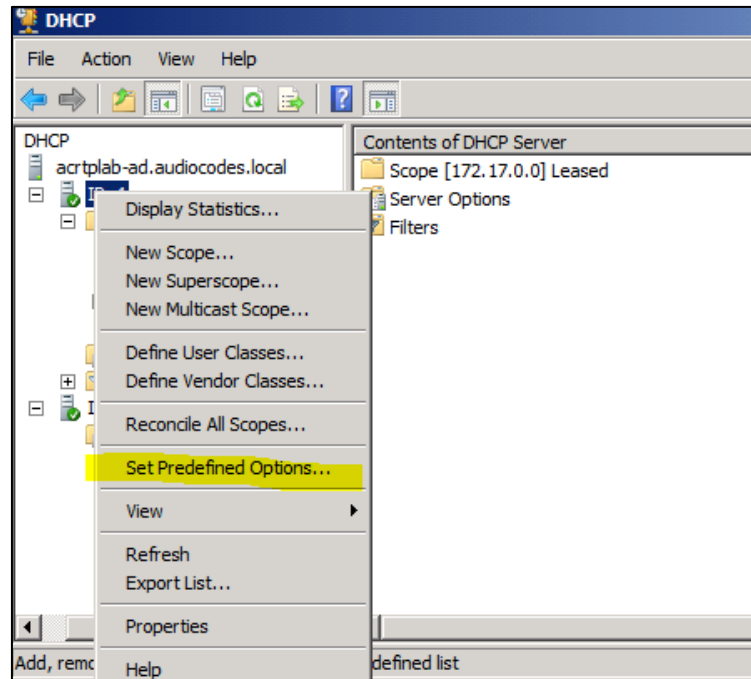


**8.** From the 'Option class' dropdown, select **DHCP Standard Options**, and then click **Add…**

**Figure 2-10: Predefined Options and Values**
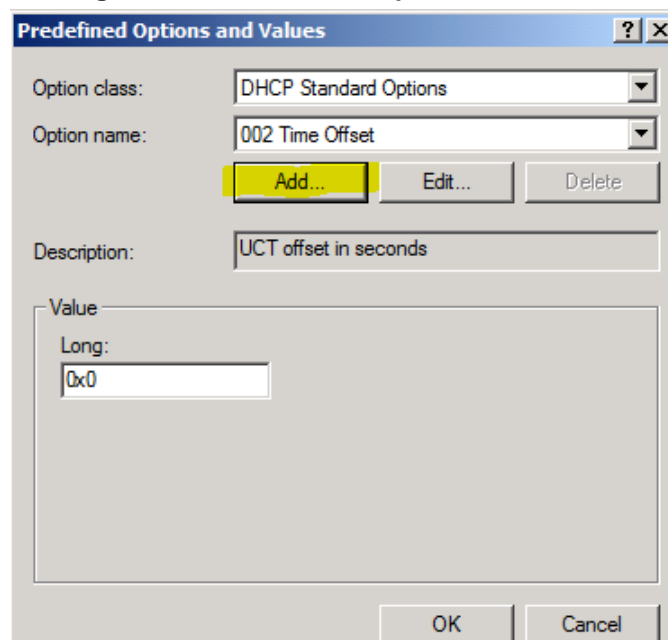


**9.** Add the **AudioCodes 160 Option** as shown below, and then click **OK**.

**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/dhcpoption160.cfg**. See the *IP Phone Management Server Administrator's Manual* for detailed information.

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



> **Note:** Ensure you defined **http://<EMS IP address>/firmwarefiles;ipp/dhcpoption160.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**
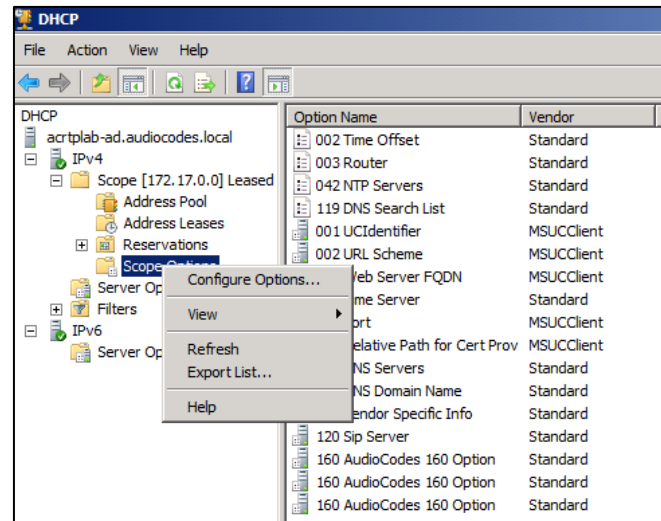


**-OR-**

**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**
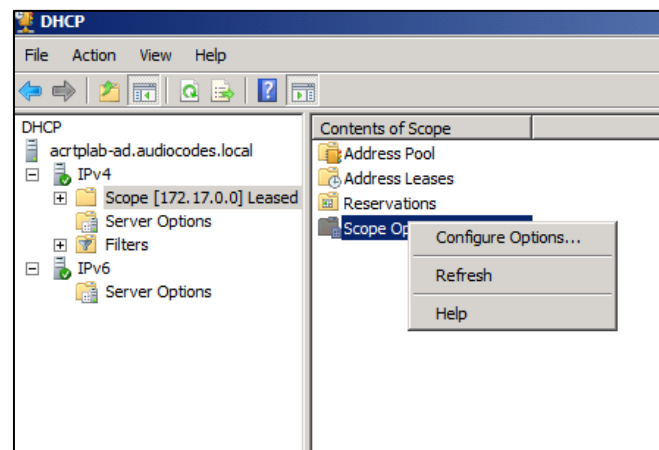


**-OR-**

**Server Option**

**13.** If assigning to the entire server (acrtplab-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**
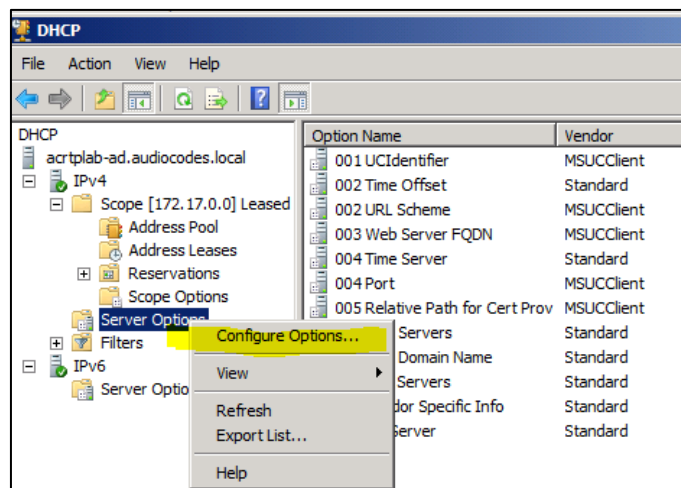


**14.** In the Server Options page (or Scope Options page) that opens, select the **Advanced** tab, ensure that **DHCP Standard Options** remains selected, and select **420HD User Class** for the first phone model to be defined. Scroll through the Available Options (all are cleared) and select only **160 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.
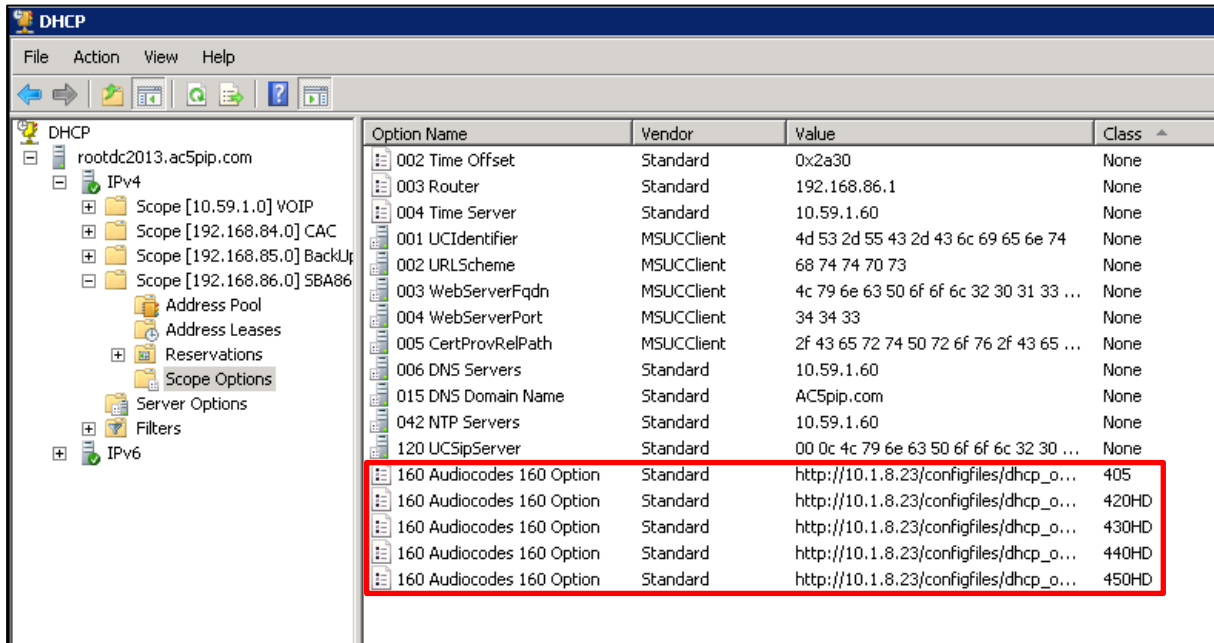
**Figure 2-16: Server Options**
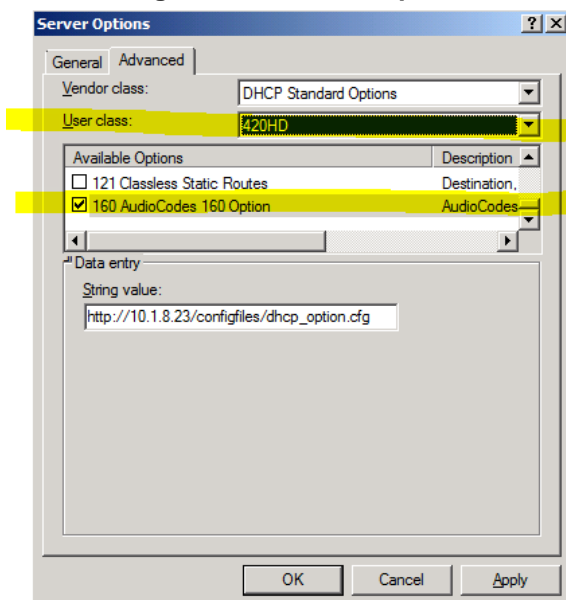


**15.** Click **Apply** and then follow the same procedure to add the **405HD, 420, 430HD**, **440HD** and **450HD** User Classes. After adding them, click **OK**.

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

**Figure 2-17: Five Scope Options Created**



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

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

**Figure 2-18: New Policy**
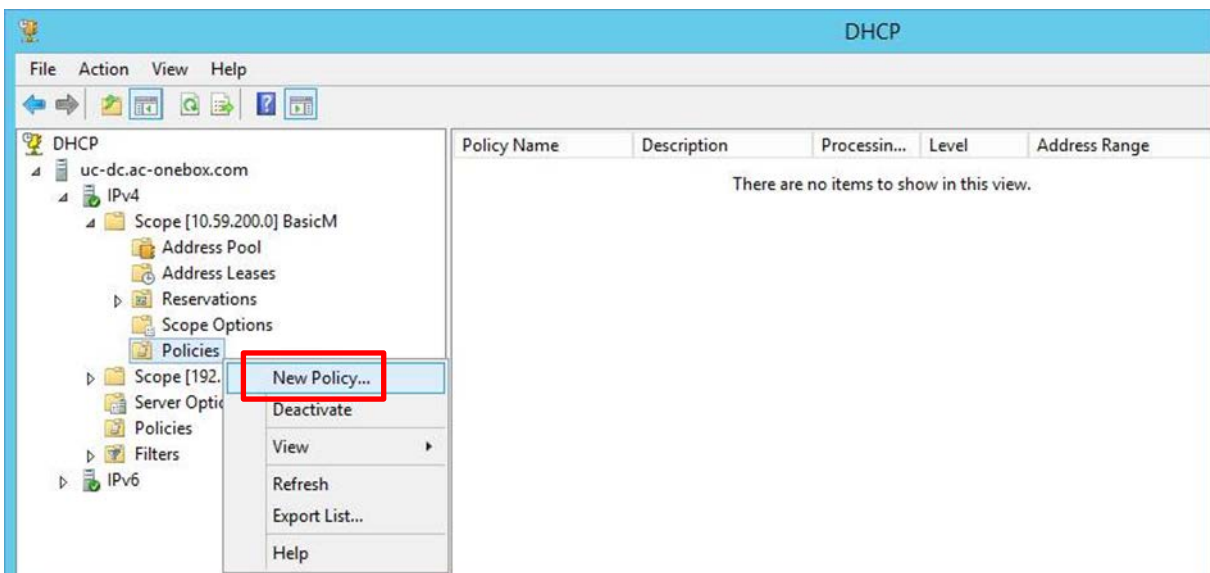
**Figure 2-19: DHCP Policy Configuration Wizard – Policy Name**



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

**Figure 2-20: DHCP Policy Configuration Wizard - Add**

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

**Figure 2-21: Add/Edit Condition**



**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 (**420HD** / **430HD** / **440HD** / **450HD** / **405HD**) 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:
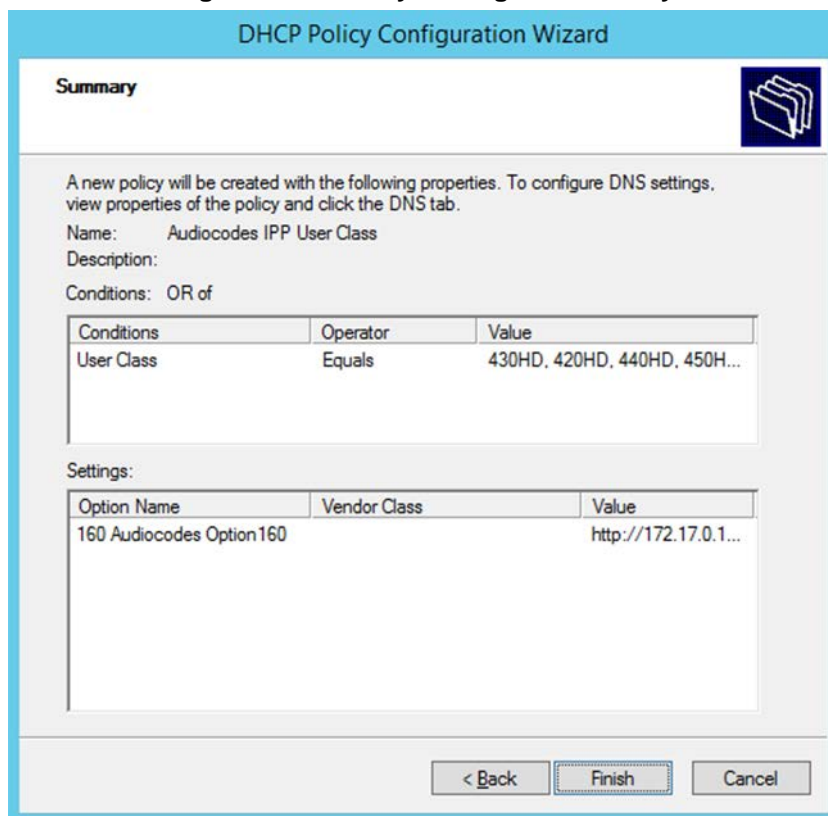
**Figure 2-24: Policy Settings – Available Options**



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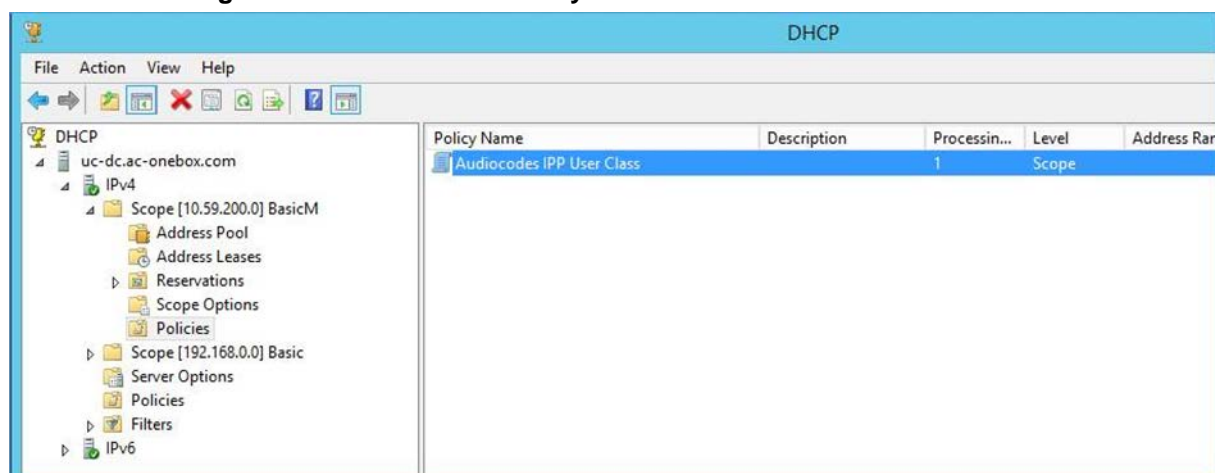
## 2.1.2 Making Sure the DHCP Server is Correctly Configured for Auto Provisioning

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:

   - &lt;protocol&gt;://&lt;server IP address or host name&gt;/&lt;firmware file name&gt;;&lt;configuration file name&gt;
   - &lt;protocol&gt;://&lt;server IP address or host name&gt;
   - &lt;protocol&gt;://&lt;server IP address or host name&gt;/&lt;firmware file name&gt;
   - &lt;protocol&gt;://&lt;server IP address or host name&gt;/;&lt;configuration file name&gt;

   Where &lt;protocol&gt; 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.

---

**Note:**

- 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., 420HD). 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 185).

---

## 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**
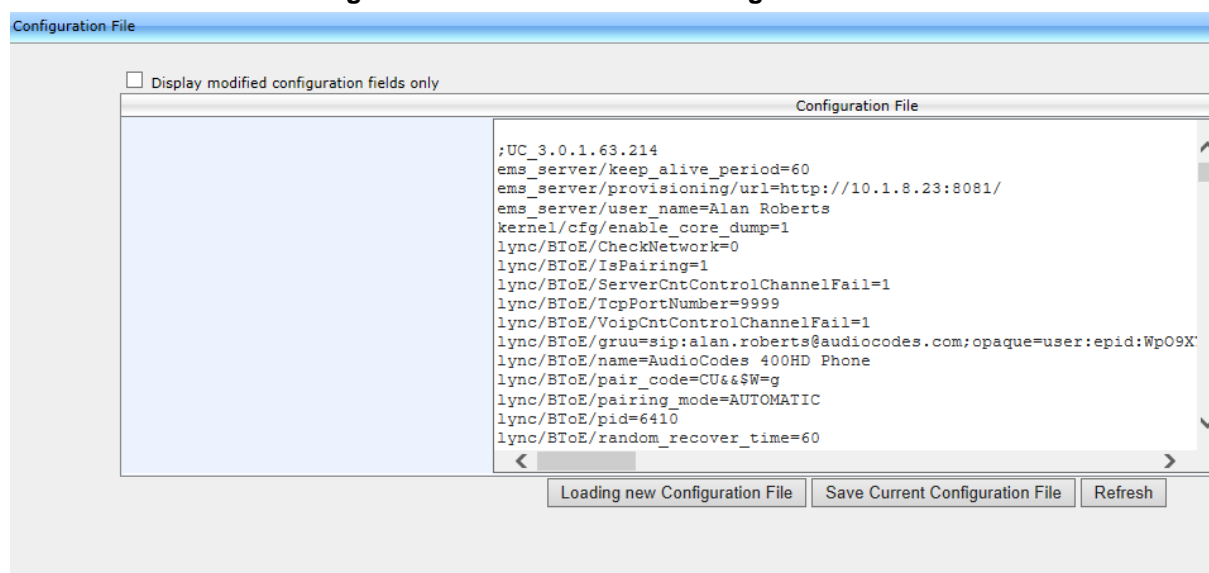


4. Click **Save Current Configuration File** and save the .cfg file in a folder on your PC.

## 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**

**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 4.21.

### 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 using the Configuration File:**

**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.<br>▪ **[0]** (Default) Allows sign-in with user credentials and with user extension number and PIN code.<br>▪ **[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.

> **Note:** 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.

> **Note:** 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 using the Configuration File:**

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]** | Determines which online sign-in method option is used.<br>▪ **[0]** The phone uses the OrgID method option to sign in.<br>▪ **[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]** | ▪ **[0]** Disabled.<br>▪ **[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.

> **Note:** 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<br>Phone Screen Notification:<br>"Failed to validate certificate" -or-<br>"Failed to obtain user certificate" | Three possible actions:<br><ul><li>Make sure DHCP Option 43, sub-option 5, was enabled in the DHCP server. If it wasn't, enable it.</li><li>Make sure you can access the Skype for Business Web service URL:<br>https://lyncsvrWebPoolFQDN:443/CertProv/CertProvisioningService.svc</li><li>Query the LDAP server:<br>_ldap._tcp.<DOMAIN name><br>Make sure it was enabled. If it wasn't, enable it in order to get the root certificate.</li></ul> |
| Synchronization problem.<br>Phone Screen Notification:<br>"Failed to connect to time server" -or-<br>"PIN internal error" | <ul><li>Make sure *at least one* of the following was configured to enable synchronization:<ul><li>✓ NTP server, via DNS SRV record (_ntp._udp.<SIP domain>pointing to NTP server)</li><li>✓ NTP server, returned via DHCP Option 42</li><li>✓ Time.windows.com</li><li>✓ Time.nist.gov</li><li>✓ Configuration Parameter (manually)</li></ul></li></ul> |
| Phone not initializing | Make sure DHCP is enabled. |
| Cannot find SIP server for 'Domain name'. Phone can't perform registration.<br>Phone Screen Notification:<br>"Failed to connect <domain> server"<br>-or-<br>"Cannot find Lync server at <>" | <ul><li>Make sure *at least one* of the following is enabled in the DNS server:</li><li>_sipinternaltls._tcp.<domain> (for TLS)</li><li>DHCP results (Option 120) (for TLS)</li><li>_sipinternal._tcp.<Domain> (for TCP)</li><li>DHCP results (Option 120) (for TCP)</li><li>_sip._tls.<Domain> (for TLS)</li><li>_sip._tcp.<Domain> (for TCP)</li></ul> |
| Phone Screen Notification: | <ul><li>Make sure 'Location look up' is configured by the</li></ul> |

| Problem / Phone Screen Notification | Corrective Action |
|---|---|
| "Location look-up failed. Please enter your address." | management shell in the Skype for Business server. |
| 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.<br>▪ 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.<br>▪ Make sure the correct information was entered in the phone screen and in the Skype for Business server interface, and that they tally.<br>▪ 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" | ▪ Make sure in the Skype for Business server interface that a PIN was configured for this user account.<br>▪ If it wasn't, create a PIN for the account. |
| Phone Screen Notification: "PIN expired" | ▪ In the Skype for Business server interface, renew the PIN expiration policy. |
| Phone Screen Notification: "PIN account disabled" | ▪ 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" | ▪ Test the PIN Authentication process on the Skype for Business server: Run in the server shell the emulate cmdlet:<br>**Test-CsPhoneBootstrap -PhoneOrExt nnnn -PIN nnnn**<br>▪ 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:<br>http://technet.microsoft.com/en-us/library/gg412852.aspx |

**Note:**

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

## 2.5.2    Using the Web Interface

This section shows how to use the Web interface to troubleshoot problems.

➢ **To use the Web interface to troubleshoot:**

1. Obtain the phone's IP address if the DHCP server successfully automatically provided one: Press the MENU key on the dial pad and in the phone's screen, navigate to and select **Status** > **Network Status**.

2. Scroll down to the IP Address and note it.

3. Open your browser and use the IP address to access the phone's Web interface.

4. Select the **Status & Diagnostics** tab > **Diagnostics** > **Tracing**:

**Table 2-10: Web Interface – Status & Diagnostics - Tracing**

# 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 7.6 on page 204 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.

> **Note:**
> •      The default password is **1234**.
> •      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** as you did **IP Address**.

➢ **To change LAN Connection Type in the Web interface:**

1. Open the Network Settings page (**Configuration** tab > **Network Connections** menu > **Network Settings**) and select the **Static IP** option:

**Figure 3-1: Web Interface - Network Settings – Static IP**

| Network Settings | |
|---|---|
| IP Type: | ◉ Static IP ○ Automatic IP (DHCP) |
| Domain Name: | [                    ] ☑ Manual |
| IP Address: | 0.0.0.0 ☑ Manual |
| Subnet Mask: | 0.0.0.0 ☑ Manual |
| Default Gateway Address: | 0.0.0.0 ☑ Manual |
| Primary DNS: | 0.0.0.0 ☑ Manual |
| Secondary DNS: | 0.0.0.0 ☑ Manual |
| MAC Address: | 00:90:8F:47:FD:E0 |
| LAN Port Mode: | Auto Negotiation ▾ |
| PC Port Mode: | Auto Negotiation ▾ |

2. Configure the parameters using the table below as reference and click **Submit**.

➢ **To change the LAN Connection Type using the Configuration File:**

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. `network/lan_type`=DHCP). | |
| IP Type<br>**[network/lan_type]** | Defines the IP addressing method:<br>▪ **[STATIC]** Static IP - IP address defined manually<br>▪ **[DHCP]** Automatic IP DHCP (default) - IP address is acquired automatically from a DHCP server |
| IP Address<br>**[network/lan/fixed_ip/ip_address]** | The LAN IP address |
| Subnet Mask<br>**[network/lan/fixed_ip/netmask]** | The subnet mask address |
| Default Gateway Address<br>**[network/lan/fixed_ip/gateway]** | The IP address of the default gateway. |
| Domain Name<br>**[network/lan/fixed_ip/domain_name]** | The domain name. |
| **Domain Name Server (DNS)** | |
| Primary DNS<br>**[network/lan/fixed_ip/primary_dns]** | The primary DNS server address. |
| Secondary DNS<br>**[network/lan/fixed_ip/secondary_dns]** | The secondary DNS server address. The phone connects to this server if the primary DNS server is unavailable. |

- Select the **Automatic IP (DHCP)** option:

**Figure 3-2: Web Interface - Network Settings - Automatic IP (DHCP)**



The following parameters can be configured:

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

| Parameter | Description |
|---|---|
| IP Type<br>**[network/lan_type]** | Defines the IP addressing method:<br>▪ **[STATIC]** Static IP - Phone's IP address is defined manually<br>▪ **[DHCP]** Automatic IP DHCP (default) - Phone's IP address is acquired automatically from a DHCP server |
| Domain Name - Manual<br>**[network/lan/dhcp/domain_name/enabled]** | Enables setting the domain name manually.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** If enabled, **network/lan/fixed_ip/domain_name** must also be set. |
| IP Address - Manual<br>**[network/lan/dhcp/ip_address/enabled]** | Enables setting the IP address manually.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** If enabled, **network/lan/fixed_ip/ip_address** must be set. |
| Subnet Mask - Manual<br>**[network/lan/dhcp/netmask/enabled]** | Enables setting the network mask manually.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** If enabled, **network/lan/fixed_ip/netmask** must be set. |
| Default Gateway Address – Manual<br>**[network/lan/dhcp/gateway/enabled]** | Enables setting the default gateway manually.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** If enabled, **network/lan/fixed_ip/gateway** must be set. |

| Parameter | Description |
|---|---|
| Primary DNS - Manual<br>**[network/lan/dhcp/primary_dns/enabled]** | Enables setting the primary DNS manually.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** If enabled, **network/lan/fixed_ip/primary_dns** must be set. |
| Secondary DNS - Manual<br>**network/lan/dhcp/secondary_dns/enabled** | Enables setting the secondary DNS manually.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** If enabled, **network/lan/fixed_ip/secondary_dns** must be set. |

## 3.1.2    Configuring LAN Port / PC Port

Port settings can be configured using the Web interface or Configuration File.

**Note:** The optional values of the configuration file parameters are enclosed in square brackets while its corresponding Web interface values are written outside the square brackets, for example, [1] Enable.

➢ **To define phone port settings using the Web interface:**

1.   Open the Network Settings page (**Configuration** tab > **Network Connections** > **Network Settings**):

**Figure 3-3: Web Interface – LAN Port Mode / PC Port Mode**

| LAN Port Mode: | Auto Negotiation |
|---|---|
| PC Port Mode: | Auto Negotiation |

2.   Configure using the table below as reference and click **Submit**.

➢ **To define phone port settings using the Configuration File:**

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 |
|---|---|
| LAN Port Mode<br>**[network/lan/port_mode]** | Sets the LAN port mode.<br>Valid values are :<br>[AUTOMATIC] = Auto negotiation.<br>[FULL_10] = 10Mbps + full duplex<br>[FULL_100] = 100Mbps + half duplex<br>[HALF_10] = 10Mbps + full duplex<br>[HALF_100] = 100Mbps + half duplex |
| PC Port Mode<br>**[network/pc/port_mode]** | Sets the computer port mode.<br>See valid values above. |

### 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 using the Web interface:**

1. Open the Network Settings page (**Configuration** tab > **Network Connections** menu > **Network Settings**).

**Figure 3-4: Web Interface - VLAN Settings**



2. Configure using the table below as reference and click **Submit**.

➢ **To configure the phone's VLAN settings using the Configuration File:**

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 |
|---|---|
| VLAN Discovery Mode<br>**[network/lan/vlan/mode]** | Determines the VLAN mode of operation.<br>▪ [Disable] Disable<br>▪ **[Manual]** Manual Configuration of LAN - Static configuration of VLAN ID and priority<br>▪ **[CDP]** Automatic Configuration of VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol (CDP)<br>▪ **[LLDP]** Automatic Configuration of VLAN - VLAN discovery mechanism based on LLDP.<br>▪ **[CDP_LLDP]** Automatic Configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol (CDP). LLDP protocol is with higher priority. |
| Period<br>**[network/lan/vlan/period]** | The time period in seconds between discovery messages when configured to CDP, LLDP or CDP and LLDP.<br>The default value is 30. |
| VLAN ID<br>**[network/lan/vlan/id]** | Only displayed when the 'VLAN Discovery Mode' parameter (above) is configured to **Manual**.<br>The valid range is 0 to 4096. The default VLAN ID is 0. |
| VLAN Priority<br>**[network/lan/vlan/priority]** | Only displayed when the 'VLAN Discovery Mode' parameter (above) is configured to **Manual**.<br>Defines the priority of traffic pertaining to this VLAN.<br>The valid range is 0 to 7 (where 7 is the highest priority). The default VLAN priority is 0. |

➢ **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
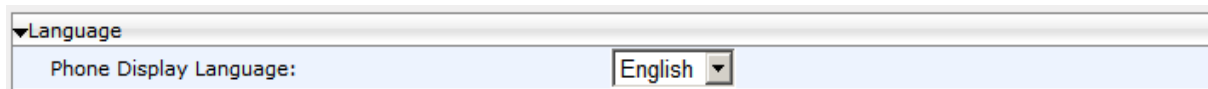
### 3.2.1 Configuring Language

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

➢ **To choose a language using the Web interface:**

1. Open the Language page (**Configuration** > **Personal Settings** > **Language**).

**Figure 3-5: Language**

2. Select the language according to the parameter in the table below, and then click **Submit**; the phone reboots and changes the screen display language accordingly.

➢ **To choose a language using the Configuration File:**

• Use the table below as reference.

**Table 3-5: Language Display Parameters**

| Parameter | Description |
|---|---|
| Phone Display Language<br>**[personal_settings/language]** | Determines the phone screen language.<br>▪ [English] English (default)<br>▪ [Spanish] Spanish<br>▪ [Russian] Russian<br>▪ [Portuguese] Portuguese<br>▪ [German] German<br>▪ [Ukraine] Ukrainian<br>▪ [French] French<br>▪ [Italian] Italian<br>▪ [Hebrew] Hebrew<br>▪ [Polish] Polish<br>▪ [Korean] Korean<br>▪ [Finnish] Suomalainen<br>▪ [Chinese] Chinese Simplified<br>▪ [Chinese] Chinese Traditional<br>▪ [Magyar] Hungarian<br>▪ [Japanese] Japanese<br>▪ Slovak<br>▪ Czech |

## 3.2.2    Configuring a Personal Directory

This section shows how to configure the Personal Directory.

➢ **To configure a Personal Directory:**

1.    Open the Directory page (**Configuration** tab > **Personal Settings** > **Directory**).

**Figure 3-6: Web Interface – Personal Directory**

**Note:** The Corporate Directory is automatically managed by the Skype for Business server.

2.    Use the 'Directory Page' field to quickly navigate to a user. This is useful if the directory extends over multiple pages.

3.    You can add, edit, or delete directory contacts. A contact's address can be a telephone number, IP address, or domain name. You can also download a personal directory file using the **Save Personal Directory** button or upload a personal directory file using the **Load Personal Directory** button.

➢ **To add a contact to the Personal Directory using the Web interface:**

1.    In the Directory page, click the **Add Contact** link above the Personal Directory section; the section expands:

**Figure 3-7: Web Interface – Directory – Add Contact**

2.    In the 'Name' field, enter the name of the contact.

3.    In the 'Office', 'Home' and/or 'Mobile' fields, enter the contact's telephone numbers. The contact's number can be defined with an IP address or domain name (e.g. <number>@<IP address or domain name>).

4.    Click **Submit**; the contact's name is displayed in the Directory list of contacts.

➤ **To edit a contact:**

1. If the contact does not appear in the displayed Directory list, then from the 'Directory Page' drop-down list, select the page in the directory that you want displayed.

2. In the Directory list, click the number that appears in the 'No.' column corresponding to the contact you want to edit; the contact's attributes appear in the **Edit Phone** group above.

3. Edit the contact as required, and then click **Submit**; the contact's new attributes are updated in the Directory list.

➤ **To delete a contact:**

1. In the Directory list, mark the 'Select' check box corresponding to the contact you want to delete.

2. Click **Delete**. (To delete all contacts, click **Delete All**).

## 3.2.3    Configuring Function Keys

> **Note:** Function Keys do not apply to the 450HD phone.

### 3.2.3.1    405HD and 420HD Phones

On the 405HD and 420HD phones you can configure Function Keys as Speed Dials, or you can configure Function Keys for Paging. You can use the Web interface or Configuration File to do it.

The Function Keys are the dial pad keys labeled **1**-**9**. Long-pressing a dial pad key activates its Function Key, if a Function Key is configured on that key. In the Web interface, they're labeled **1**-**9** and in the Configuration File **0**-**8**.

#### 3.2.3.1.1 Configuring a Function Key as a Speed Dial using the Web Interface

This section shows how to configure a function key as a Speed Dial. Up to nine can be configured.

➢ **To configure a Function Key as a Speed Dial using the Web interface:**

1. Open the Function Keys page (**Configuration** tab > **Personal Settings** menu > **Function Keys**).

**Figure 3-8: Web Interface - Function Keys**



2. In the 'Number' field corresponding to the 'Key' column, enter the telephone number to which to assign a Speed Dial, and click **Submit**.

### 3.2.3.1.2 Configuring a Function Key as a Speed Dial using the Configuration File

⚠️ **Note:** 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 using the Configuration File:**

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

**Table 3-6: Speed Dial Parameter**

| Parameter Name | Description |
|---|---|
| **[provisioning/speed_dial_uri]** | The URI for retrieving the speed dial list. The speed dial list must be included in a separate file that can be downloaded to the phone during provisioning.<br>For example:<br>**provisioning/speed_dial_uri=speed_dial_list.txt**<br><br>**Note:**<br>▪ The speed dial file is downloaded after boot up and periodically.<br>▪ If the speed dial file is new, the phone reboots.<br>▪ For creating a Speed Dial file, see Section 3.2.3.1.2. |

#### 3.2.3.1.3 Configuring a Function Key for Paging using the Web Interface

This section shows how to configure a function key as a Speed Dial. Up to nine can be configured for paging, allowing the user to page up to nine paging groups.

➢ **To configure a Function Key for paging using the Web interface:**

1. Open the Function Keys page (**Configuration** tab > **Personal Settings** menu > **Function Keys**).

**Figure 3-9: Web Interface - Function Keys - Paging**



2. From the 'Type' dropdown corresponding to the 'Key' column, select **Paging**, as shown in the figure above. This option will only be available if the paging feature is enabled as shown in Section 3.3.15. The page shown in the figure below opens.

**Figure 3-10: Web Interface - Function Keys – Paging Parameters**



3. In the 'Paging Group' field, enter the name of the group, to be displayed in the phone's screen when there's an incoming paging call. For phones to be in a group, all must be configured with the same name.

**4.** In the 'Paging Multicast' field, 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.

**5.** In the 'Paging Port' field, enter the group's port. Default: 8888. For phones to be in a group, all must be configured with the same port.

**6.** Click **Submit**.

### 3.2.3.2    430HD and 440HD Phones

On the 430HD and 440HD phones, the Function Keys are on the sidecar on the right side of the phone's physical interface (covered on the 430HD).

In the Web interface they're labeled **1**-**12**. In the Configuration File they're labeled **0**-**17**.

You can configure Function Keys as Speed Dials, or as Speed Dials + BLFs (Presence) (440HD phone only), using the Web interface or Configuration File to do it.

#### 3.2.3.2.1    Configuring a Function Key as Speed Dial / Speed Dial+BLF using the Web Interface

This section shows how to configure a function key as Speed Dial / Speed Dial+BLF using the Web interface or the Configuration File.

➢    **To configure a Function Key as Speed Dial / Speed Dial+BLF using the Web interface:**

**1.** Open the Function Keys page (**Configuration** tab > **Personal Settings** menu > **Function Keys**).

**Figure 3-11: Web Interface - Function Keys**



**2.** In the 'Number' field corresponding to the 'Key' column, enter the telephone number to which to assign a Speed Dial.

**3.** Enter a 'Label' (applies only to the 440HD phone).

**4.** Click **Submit**.

### 3.2.3.2.2 Configuring a Function Key for Paging using the Web Interface

You can configure a Function Key in order to page a group (see Section 3.3.15 for detailed information about the paging feature). Up to 12 Function Keys can be configured for paging, allowing the user to page up to 12 paging groups. This section shows how to configure a Function Key for paging, using the Web interface.

➢ **To configure a Function Key for paging using the Web interface:**

**1.** Open the Function Keys page (**Configuration** tab > **Personal Settings** menu > **Function Keys**).

**Figure 3-12: Web Interface - Function Keys - Paging**



**2.** From the 'Type' dropdown corresponding to the 'Key' column, select **Paging**, as shown in the figure above; the page shown in the figure below opens.

**Figure 3-13: Web Interface - Function Keys – Paging Parameters**



**3.** In the 'Paging Group' field, enter the name of the group, to be displayed in the phone's screen when there's an incoming paging call.

**4.** In the 'Paging Multicast' field, 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.

**5.** In the 'Paging Port' field, enter the group's port. Default: 8888. For phones to be in a group, all must be configured with the same port.

**6.** Click **Submit**.

### 3.2.3.2.3 Saving Configured Speed Dials in a cfg File

In the Web interface, 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:**

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

### 3.2.3.2.4 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.

### 3.2.3.2.5 Deleting a Speed Dial

➢ **To delete speed dials, either:**

• **Deleting selected speed dial entries:** select the 'Delete' check boxes corresponding to the speed dials that you want to delete and click **Submit**.

• **All speed dials:** Click **Delete All** and at the prompt click **OK**.

• **To clear (unselect) all selected 'Delete' check boxes:** click **Reset**.

## 3.2.4    Configuring Programmable Keys using the Web Interface

⚠️ **Note:** Not applicable to the 405HD and 420HD phones.

### 3.2.4.1    430HD and 440HD Phones

Six programmable keys, located next to the phone screen, three on each side, are labelled **1**-**6** in the Web interface and **12**-**17** in the Configuration File.

- ■ Line Key **1** can only be **SfB Account** (Skype for Business Account)
- ■ Line Key **2**-**6** can be configured as Speed Dial / Speed Dial+BLF, Paging or Key Event
- ■ Line Key **6** (only) can be configured as **VocaNOM**

#### 3.2.4.1.1    Configuring a Programmable Key as a Speed Dial / Speed Dial+BLF in the Web Interface

Speed Dials let users quickly access and dial numbers they use often. BLF allows the user to determine others' presence status.

➢ **To configure a Programmable Key in the Web interface as a Speed Dial / Speed Dial+BLF:**

1. Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).

**Figure 3-14: Web Interface – Programmable Keys**



2. From the 'Line Key' dropdown, select **2**-**6**.

**Figure 3-15: Web Interface – Programmable Key – Speed Dial / Speed Dial+BLF**



3. From the 'Key Type' dropdown, select **Speed Dial** / **Speed Dial+BLF**; the page extends to display the 'Key Label' and 'Line Speed Dial Number' fields.
4. Choose a Key Label, i.e., the name of the person to whose phone number this speed dial will dial.
5. Enter the phone number of the person to whom this speed dial will dial.
6. Click **Submit**. Make sure the label is displayed in the phone's screen.

### 3.2.4.1.2 Configuring a Programmable Key for Paging using the Web Interface

The key lets you page (make a live announcement) 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.

> **Note:**
> - Before configuring a programmable key for paging, you need to enable the paging feature (see Section 3.3.15).
> - You can configure up to five programmable keys for paging on the 430HD, 440HD and 440+HD phones.
> - Paging is not allowed if a user is configured as a delegate in a Boss-Admin scenario.

➢ **To configure a Programmable Key for paging using the Web interface:**

1. Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).

**Figure 3-16: Web Interface - Programmable Keys**



> **Note:** Line Key **1** is reserved for the extension line. Only **2-6** can be selected from the 'Line Key' dropdown.

2. From the 'Line Key' dropdown, select **2-6**.
3. From the 'Key Type' dropdown, select **Paging**, as shown in the figure below.

**Figure 3-17: Web Interface - Programmable Keys – Line Settings - Paging**



4. In the 'Key Label' field, enter the group's label, to be displayed in the phone's screen when there's an incoming paging call.
5. In the 'Paging Group' field, enter the name of the group, to be displayed in the phone's screen when there's an incoming paging call.
6. In the 'Paging Multicast' field, 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.
7. In the 'Paging Port' field, enter the group's port. Default: 8888. For phones to be in a group, all must be configured with the same port.
8. Click **Submit**.

**3.2.4.1.3  Configuring a Programmable Key as a Key Event in the Web Interface**

Key Events let users quickly access Calendar, Dialed numbers, Missed Calls, Received Calls, Directory, DnD All, and/or Forward All.

➢ **To configure a Programmable Key as a Key Event in the Web interface:**

1. In the Programmable Keys page, select **2**-**6** from the 'Line Key' dropdown under Line Settings.
2. From the 'Key Type' dropdown, select **Key Event**.
3. In the 'Key Event' field now displayed, choose either **Calendar** (default), **Dialed Calls**, **Missed Calls**, **Received Calls**, **Directory**, **DnD All** and/or **Forward All**.

**Figure 3-18: Web Interface – Programmable Line Keys – Selecting a Key Event**



4. In the 'Key Label' field, enter a Label reflecting the key event, for example, enter **Dialed** if you're configuring a Dialed Calls key event.
5. Click **Submit**. Make sure the label is displayed in the phone screen adjacent to the key you configured.

**3.2.4.1.4  Configuring Programmable Key #6 as VocaNOM in the Web Interface**

Lets users vocalize a destination to call, instead of manually dialing a number. Only key **6** can be configured as VocaNOM.

➢ **To configure Programmable Key #6 as VocaNOM with the Web interface:**

1. Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).
2. From the 'Line Key' dropdown, select **6**; 'Key Type' is automatically configured as **VocaNom** and 'VocaNOM Number' is configured as **4444** (the default number to dial in order to receive the VocaNOM voice service).

**Figure 3-19: Web Interface - Programmable Keys – Line Key 6**



3. Click **Submit**; the VocaNOM key is displayed in the phone's screen.

### 3.2.4.2 450HD Phone

Eight programmable keys (**1**-**8**) can be configured using the Web interface. You can configure *any* one as:

■ VocaNOM

■ Speed Dial / Speed Dial+BLF

■ Paging

■ Key Event (see below). Lets the user quickly access Dialed numbers, Missed Calls, Received Calls, Directory, DnD All and/or Forward All.

#### 3.2.4.2.1 Configuring a Programmable Key as VocaNOM using the Web Interface

Lets the user vocalize a destination number to call, instead of manually dialing the number.

➢ **To configure a programmable key as VocaNOM using the Web interface:**

**1.** Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).

**2.** From the 'Line Key' dropdown, select any (**1**-**8**).

**3.** From the 'Key Type' dropdown, select **VocaNom**.

**Figure 3-20: Web Interface – Programmable Keys**



**4.** In the 'Key Label' field that opens, enter a label such as **VocaNOM**.

**5.** In the 'VocaNOM Number' field, enter the number of the service, e.g., 4444.

**6.** Click **Submit**; VocaNOM is displayed in the phone's screen.

#### 3.2.4.2.2 Configuring a Programmable Key as a Speed Dial / Speed Dial+BLF using the Web Interface

Speed Dials let the user quickly access and dial numbers they use often. Speed Dial+BLF is the same as a Speed Dial but also allows the user to determine presence status.

➢ **To configure a programmable key in the Web interface as a Speed Dial / Speed Dial+BLF:**

**1.** Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).

**2.** From the 'Line Key' dropdown, select **1**-**8**.

**Figure 3-21: Web Interface – Programmable Keys – Speed Dial**

**3.** From the 'Key Type' field, select **Speed Dial**; the page extends to display the 'Key Label' and 'Line Speed Dial Number' fields.

**4.** Enter a Key Label, i.e., the name of the person to whose phone number this speed dial will dial.

**5.** Enter the phone number of the person to whom this speed dial will dial.

**6.** Click **Submit**.

**7.** Make sure the label is displayed in the phone's screen. If you configured Speed Dial+BLF, you'll view their presence status next to their label.

### 3.2.4.2.3 Configuring Programmable Keys for Paging using the Web Interface

> **Note:**
>
> - Before configuring a programmable key for paging, you need to enable the paging feature (see Section 3.3.15).
> - You can configure up to eight programmable keys for paging on the 450HD phone.
> - Paging is not allowed if a user is configured as a delegate in a Boss-Admin scenario.

The key allows you to make a live announcement (page) 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.

➢ **To configure a Programmable Key for paging using the Web interface:**

**1.** Open the Programmable Keys page (**Configuration** tab > **Personal Settings** menu > **Programmable Keys**).

**2.** From the 'Line Key' dropdown, select **1**-**8**.

**3.** From the 'Key Type' dropdown, select **Paging**.

**Figure 3-22: Web Interface - Programmable Keys**



**4.** In the 'Key Label' field, enter the group's label, to be displayed in the phone's screen when there's an incoming paging call.

**5.** In the 'Paging Group' field, enter the name of the group, to be displayed in the phone's screen when there's an incoming paging call.

**6.** In the 'Paging Multicast' field, 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.

**7.** In the 'Paging Port' field, enter the group's port. Default: 8888. For phones to be in a group, all must be configured with the same port.

**8.** Click **Submit**.

#### 3.2.4.2.4 Configuring a Programmable Key as a Key Event using the Web Interface

➢ **To configure a Programmable Key as a Key Event in the Web interface:**

1. From the 'Line Key' dropdown in the Programmable Keys page, select any value from **1**-**8**.
2. From the 'Key Type' dropdown, select **Key Event**.
3. From the 'Key Event' dropdown now displayed, select **Calendar**, **Dialed Calls**, **Missed Calls**, **Received Calls**, **Directory**, **DnD All** or **Forward All**.

**Figure 3-23: Web Interface – Programmable Keys – Key Event**



4. In the 'Key Label' field, enter a label for the key reflecting the event, for example, enter **Dialed** if you're programming a Dialed Calls key event.
5. Click **Submit**.
6. Make sure the label is displayed in the screen.

## 3.2.5    Configuring Programmable Keys using the Configuration File

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

⚠️ **Note:** Not applicable to the 405HD and 420HD phones.

### 3.2.5.1    430HD and 440HD Phones

This section shows how to configure a programmable key on the 430HD and 440HD Phones using the Configuration File.

➢ **To configure a Programmable Key using the Configuration File:**

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

**Table 3-7: Programmable Key Parameters in the Configuration File - 430HD and 440HD Phones**

| Parameter Name | Description |
|---|---|
| **[personal_settings/functional_key/12-17/shared_line_index]** | Defines the line.<br>**Note:**<br>▪ Line index **12** can *only* be **SfB Account** (Skype for Business Account) (default)<br>▪ Line index **13**–**17** can be configured as **Speed Dial**, **Speed Dial+BLF** (only 440HD) or **Key Event** which can be configured as Calendar, Dialed Numbers, Missed Calls, Received Calls, Directory, DnD All, and/or Forward All.<br>▪ The Key Event **Calendar** can only be configured on line index **13**.<br>▪ The Key Event **VocaNOM** can only be configured on line index **17**. |
| **[personal_settings/functional_key/13-17/type]** | Configure either:<br>▪ SPEED_DIAL<br>▪ SPEED_DIAL_BLF (440HD only)<br>▪ PAGING<br>▪ KEY_EVENT<br>  ✓ The Key Event **Calendar** can only be configured on line index **13**.<br>  ✓ The Key Event **VocaNOM** can only be configured on line index **17**. |
| **[personal_settings/functional_key/13-17/key_label]** | Configure a label for the key, e.g., the name of the person to whose phone number the speed dial will dial. The label is displayed in the phone's screen next to the hard key. Does not apply to the Key Event **VocaNOM** whose label is automatically displayed after it is configured. |
| **[personal_settings/functional_key/13-17/speed_dial_number]** | The phone number of the person to whom the speed dial will dial. Also allows you to configure the number which the key must dial to reach the **VocaNOM** service, e.g., **4444**. |

### 3.2.5.2    450HD Phone

This section shows how to configure a programmable key on the 450HD phone using the Configuration File.

➢ **To configure a Programmable Key using the Configuration File:**

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

**Table 3-8: Programmable Key Parameters in the Configuration File - 450HD Phone**

| Parameter Name | Description |
|---|---|
| [personal_settings/functional_key/12-19/shared_line_index] | Eight line keys, indexed **12-19**, can be configured. Each can be configured as Key Type **VocaNOM**, **Speed Dial**, **Speed Dial+ BLF**, **Paging** or **Key Event**.<br>**VocaNOM** is a service that lets users vocalize a destination number to call, instead of manually dialing it.<br>**Speed Dial** lets users quickly access and dial numbers they use often. **Speed Dial+BLF** indicates the presence status of people for whom speed dials are configured.<br>**Key Event** lets users quickly access Calendar (default), Dialed Numbers, Missed Calls, Received Calls, Dialed Calls, Directory, DnD All or Forward All. |
| [personal_settings/functional_key/12-19/type] | Each Line Key can be configured as type:<br>▪ VOCANOM<br>▪ SPEED_DIAL<br>▪ SPEED_DIAL_BLF<br>▪ PAGING<br>▪ KEY_EVENT |
| [personal_settings/functional_key/12-19/key_label] | 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. |
| [personal_settings/functional_key/12-19/speed_dial_number] | Displayed in the Web interface only if 'Key Type' is configured as **Speed Dial** or **Speed Dial+BLF**. Configure the telephone number which the speed dial will dial.<br>Also allows you to configure the number which the key must dial to reach the **VocaNOM** service, e.g., **4444**. |
| Key Event<br>[voip/line_key/12-19/key_event] | Lets users quickly access **CALENDAR** (default), **Dialed** numbers, **Missed Calls**, **Received Calls**, **Dialed Calls**, **Directory**, **DnD All** or **Forward All**. |

#### 3.2.5.2.1 Saving Configured Programmable Keys in a cfg File

After configuring Speed Dials or Speed Dials+BLFs (presence) in the Web interface, you can save the configuration in a cfg file on your computer and load it to other phones.

➢ **To save Speed Dials / Speed Dials+BLFs 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.

#### 3.2.5.2.2 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.

## 3.2.6 Configuring Tones

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

### 3.2.6.1 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 your region using the Web interface:**

1. Open the Tones page (**Configuration** tab > **Personal Settings** > **Tones**).

**Figure 3-24: Web Interface - Tones - Regional Settings**



2. From the 'Current Location' drop-down list, select the country in which your phone is located. Use the table below as reference.
3. Click **Submit**.

➢ **To configure regional location using the Configuration File:**

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

**Table 3-9: Regional Parameters**

| Parameter | Description |
|---|---|
| Current Location<br>**[voip/regional_settings/selected_country]** | 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:<br>▪ [Israel] Israel<br>▪ [China] China<br>▪ [France] France<br>▪ [Germany] Germany<br>▪ [Netherlands] Netherlands<br>▪ [UK] UK<br>▪ [Brazil] Brazil<br>▪ [Italy] Italy<br>▪ [Argentina] Argentina<br>▪ [Portugal] Portugal<br>▪ [Russia] Russia |

| Parameter | Description |
|---|---|
| | ▪ [Australia] Australia<br>▪ [USA] USA<br>▪ [India] India |
| [voip/regional_settings/use_config_file_values] | 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.<br>▪ **[0]** - Disable (default)<br>▪ **[1]** - Enable |
| **Call Progress Tones (CPT)**<br>**Note:** Up to 10 CPTs can be configured (**voip/regional_settings/call_progress_tones/0…9**). ||
| [voip/regional_settings/call_progress_tones/%d/enabled] | Enables the specific CPT.<br>▪ **[0]** - Disable<br>▪ **[1]** - Enable |
| [voip/regional_settings/call_progress_tones/%d/name] | Defines the name of the CPT. |
| [voip/regional_settings/call_progress_tones/%d/cadence] | ▪ Defines the cadence type of the tone.<br>▪ **[0]** - Continuous signal<br>▪ **[1]** - Cadence signal<br>▪ **[2]** - Burst signal |
| [voip/regional_settings/call_progress_tones/%d/frequency_a] | Defines the low frequency (in Hz) of the tone.<br>Range: 300 - 1980 Hz, in steps of 1 Hz.<br>Unused frequencies must be set to zero. |
| [voip/regional_settings/call_progress_tones/%d/frequency_b] | Defines the high frequency (in Hz) of the tone.<br>Range: 300 - 3000 Hz, in steps of 1 Hz.<br>Unused frequencies must be set to zero. |
| [voip/regional_settings/call_progress_tones/%d/frequency_a_level] | Output level of the low frequency tone (in -dBm) in Call Progress generation. Range: 0 - 63, where 63 is mute. |
| [voip/regional_settings/call_progress_tones/%d/frequency_b_level] | Output level of the low frequency tone (in -dBm) in Call Progress generation. Range: 0 - 63, where 63 is mute. |
| [voip/regional_settings/call_progress_tones/%d/tone_on_0] | tone_on_0 to tone_on_3.<br>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. |
| [voip/regional_settings/call_progress_tones/%d/tone_off_0] | tone_off_0 to tone_on_3.<br>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. |

### 3.2.6.2 Uploading Ring Tones

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

> **Note:**
> - 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 upload a ring tone using the Web interface:**

1. Open the Tones page (**Configuration** tab > **Personal Settings** menu > **Tones**) and scroll down to the Upload Ringing Tone section.

**Figure 3-25: Web Interface - Upload Ringing Tone**



2. In the 'Ringing Tone Name' field, enter the name of the ring tone file to upload. If you do not enter a name, the phone assigns the tone's file name (without the .wav file extension) as the name of the tone.
3. Click **Browse**, navigate to the folder in which the ring tone file is located, select the file, and then click **Open**; the file name and path is displayed in the 'File Location' field.
4. Click **Submit**; the file is loaded to the phone and displayed in the Ringing Tone Name pane.

➢ **To delete Ring Tones using the Web interface:**

- Select the 'Delete' check boxes corresponding to the ring tone that you want to delete, and then click **Submit**.

➢ **To define the Ring Tone File URI in the Configuration File:**

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

**Table 3-10: Ring Tone File URI in the Configuration File**

| Parameter | Description |
|---|---|
| Ringing Tone Name File Location **[provisioning/ring_tone_uri]** | 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. <br> For example: **provisioning/ring_tone_uri=tones.tgz** <br> **Note:** <br> ▪ The ringtone file is downloaded only after boot up, and not periodically. <br> ▪ If the tones file is new, the phone updates the information, but does not reboot. |

➢ **To select Ring Tones using the Configuration File:**

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

**Table 3-11: Ring Tones Parameter in the Configuration File**

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

## 3.2.7 Configuring Phone Screen Settings

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

➢ **To configure phone screen settings using the Configuration File:**

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

**Table 3-12: Phone Screen Contrast Parameters**

| | |
|---|---|
| **[personal_settings/lcd_contrast]** | Determines the phone screen contrast. 430HD / 440HD: Range: 55-90. Default: 69. 420HD: Range 0-63. Default: 18. |
| **[personal_settings/enhanced_lcd_contrast]** | [440HD+ only] Determines the phone screen contrast. Range: 285-325. Default: 305. |
| **[personal_settings/blf_lcd_contrast]** | [440HD and 440HD+ only) Determines BLF screen contrast. Configure to a level that is comfortable for the user. Range: 100-200. Default: 140. |

Table 3-13 on the next page shows the 450HD screen contrast parameters.

**Note:** The 450HD 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 Busingess 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' timout if in working hours.
- The third determines 'active mode' timout 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.

**Table 3-13: Screen Contrast Parameters – 450HD Only**

| 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 dialpad, etc.<br>• LOW<br>• MEDIUM<br>• 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).<br>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:<br>• LOW<br>• MEDIUM (default)<br>• 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. |
| **[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).<br>Either: 30, 60 (default), 90 or 120 minutes. |

| Parameter | Description |
|---|---|
| **[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:<br>• LOW (default)<br>• MEDIUM<br>• HIGH<br> 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    Configuring VoIP Settings

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

### 3.3.1    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 using the Configuration File:**

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

**Table 3-14: TLS/SSL over SIP Parameters**

| Parameter | Description |
|---|---|
| **[voip/signalling/sip/tls_method]** | Possible values:<br>• **ssl_2**<br>• **ssl_3**<br>• **ssl_2_3** (default)<br>• **tls_1**<br>• **tls_1_1**<br>• **tls_1_2**<br>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. |
| **[voip/signalling/sip/tls_disable]** | Possible values: space separated list of values from above list. For example:<br>• " **ssl_2 ssl_3** " (default)<br>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. |

## 3.3.2 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 using the Configuration File:**

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

**Table 3-15: TLS/SSL over SIPE Parameters**

| Parameter | Description |
|---|---|
| **[voip/signalling/sipe/tls_method]** | Possible values:<br>• **ssl_2**<br>• **ssl_3**<br>• **ssl_2_3** (default)<br>• **tls_1**<br>• **tls_1_1**<br>• **tls_1_2**<br>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. |
| **[voip/signalling/sipe/tls_disable]** | Possible values: space separated list of values from above list. For example:<br>• " **ssl_2 ssl_3** " (default)<br>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. |

### 3.3.3    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).

> **Note:** 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 using the Web interface:**

1.  Open the Signaling Protocol page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**) and scroll down under SIP Proxy and Registrar.

**Figure 3-26: Web Interface – Signaling Protocol – Use Hosting Outbound Proxy**



2.  Configure the parameters using the table below as reference and then **Submit**.

➢ **To configure using the Configuration File:**

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

**Table 3-16: Proxy and Registrar Parameters**

| Parameter | Description |
|---|---|
| Use Hosting Outbound Proxy<br>**[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).<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |
| Outbound Proxy IP Address or Host Name<br>**[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. |
| Outbound Proxy Port<br>**[voip/signalling/sip/sip_outbound_proxy/port]** | Displayed when the 'Use Hosting Outbound Proxy' parameter is enabled.<br>Defines the port on which the outbound proxy listens. Range: 1024 to 65535. Default: 5060. |

## 3.3.4 Configuring Dialing

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

### 3.3.4.1 Adjusting the DTMF Level

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

➢ **To adjust the DTMF level using the Configuration File:**

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

**Table 3-17: Automatic Dialing Parameters**

| Parameter | Description |
|---|---|
| **[voip/audio/gain/dtmf_tone_signal_level]** | Range: 1-32. Default: 16 |

### 3.3.4.2 Configuring Automatic Dialing

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

➢ **To activate automatic dialing using the Web interface:**

1. Open the Dialing page (**Configuration** tab > **Voice Over IP** menu > **Dialing**).

**Figure 3-27: Web Interface - Dialing - Automatic Dialing**



2. Configure the Automatic Dialing section parameters using the table below as reference, and then click **Submit**.

➢ **To activate automatic dialing using 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 3-18: Automatic Dialing Parameters**

| Parameter | Description |
|---|---|
| Activate **[voip/dialing/auto_dialing/enabled]** | Determines whether automatic dialing is enabled (i.e., phone number is automatically dialed when you off-hook the phone). <br> ▪ **[0]** Disable (default) <br> ▪ **[1]** Enable |

| Parameter | Description |
|---|---|
| Timeout<br>**[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.<br>▪ The valid range is 0 to 120. The default value is 15. |
| Destination Phone Number<br>**[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.<br>The valid value can be up to 32 characters. |

### 3.3.4.3 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 requried 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 "," or "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 using 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 3-19: 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]. |

### 3.3.4.4 Configuring Default Audio Device

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

➢ **To configure the default Audio Device using the Web interface:**

1. Open the Dialing page (**Configuration** tab > **Voice Over IP** menu > **Dialing**) and scroll down to the Default Audio Device section.

**Figure 3-28: Web Interface - Dialing - Default Audio Device**



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

➢ **To select the default Audio Device using the Configuration File:**

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

**Table 3-20: Default Audio Device Parameter**

| Parameter | Description |
|---|---|
| Audio Device<br>**[voip/answer_device]** | Sets the default audio device to answer or initiate a new call when no explicit audio device is set.<br>For example:<br>▪ When pressing the **Answer** softkey.<br>▪ When initiating a call by speed dial key, call history or phone directory.<br>▪ Answering talk event or auto-answer.<br>▪ When starting to dial in "on hook" mode.<br>Valid values are:<br>▪ [SPEAKER] (default)<br>▪ [HEADSET] |
| **[voip/headset_only/enabled]** | Lets you control audio device usage. Lets you enable headset only, and disable the phone hook and the SPEAKER button.<br>▪ **[0]** Headset only (default)<br>▪ **[1]** Disables the phone hook and the SPEAKER button. Leaves the headset as the only possible audio device that can be used. |

## 3.3.5    Enabling Direct Voice Dialing

Users can use the AudioCodes Voca 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 Function Key which they can press and then vocalize the name of the party to whose number the Voca service will directly dial.

> **Note:** Applies to the 450HD, 440HD, 430HD, 420HD and 405HD phone models.

➢ **To enable voice dialing using 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 3-21: Enabling Voice Dialing**

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

> **Note:** All parameters must be configured for the user's **Voca** Functional Key to be activated.

## 3.3.6 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 using the Configuration File:**

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

**Table 3-22: Disable Microphone Parameter**

| Parameter | Description |
|---|---|
| **['voip/audio/microphone/enable]** | Enables/disables the phone's microphone functionality.<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |

### 3.3.7 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 using the Configuration File:**

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

**Table 3-23: 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.<br>▪ **[0]** TRANSFER hard key performs Consultative Transfer<br>▪ **[1]** TRANSFER hard key performs Blind Transfer (default) |

### 3.3.8 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 using the Configuration File:**

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

**Table 3-24: Semi-Consultative Transfer Parameter**

| Parameter | Description |
|---|---|
| **[system/semi_attended/enable]** | Enables semi-consultative transfer.<br>▪ **[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.<br>▪ **[1]** A calls C and presses the **Trans** softkey when A hears the ringback from C. |

## 3.3.9 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 using the Configuration File:**

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

**Table 3-25: Blind Transfer Softkey Parameter**

| Parameter | Description |
|---|---|
| **[voip/signalling/sip/sk_blind_transfer/enable]** | Enables display / removes display of the **BXfer** softkey in the phone screen when in a call.<br>▪ **[0]** Removes display of the **BXfer** softkey when in a call; the **Hold** softkey is displayed instead.<br>▪ **[1]** Enables display of the **BXfer** softkey when in a call (default). |

## 3.3.10  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 Web interface or 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 the EHS using the Web interface:**

1. Open the Services page (**Configuration** tab > **Voice Over IP** menu > **Services**) and scroll down to the General Parameters section.

**Figure 3-29: Web Interface - VoIP- Services – General Parameters**



2. Configure the 'Electronic Hook Switch' parameter using the table below as reference, and then click **Submit**.

➢ **To enable EHS using the Configuration File:**

• Configure the EHS parameter using the table below as reference, and then click **Submit**.

**Table 3-26: EHS Parameter**

| Parameter | Description |
|---|---|
| Electronic Hook Switch<br>**[voip/services/electronic_hook_switch/enabled]** | Enables the EHS DHSG-standard feature.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>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.<br>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. |

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.

## 3.3.11  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 in the Web interface:**

**1.** Open the Services page (**Voice over IP** > **Services**), scroll to the Call Waiting section and from the 'Generate Tone' dropdown, select **Disable**.

**Figure 3-30: Web Interface - Voice over IP – Services – Generate Tone**



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

➢ **To disable Call Waiting audial indication using the Configuration File:**

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

**Table 3-27: Call Waiting Audial Indication Parameter**

| Parameter | Description |
|---|---|
| Generate Tone<br>**[voip/services/call_waiting/generate_tone/enabled]** | Enables a call waiting audial indication (beep progress tone), which can interrupt a phone conversation.<br>▪ **[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.<br>▪ **[1]** Enabled (default) |

## 3.3.12 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 in the Web interface:**

1.  Open the Services page (**Voice over IP** > **Services**) and under the Call Waiting section, select the option **Busy on Busy** from the 'Mode' dropdown, as shown in the figure below.

**Figure 3-31: Web Interface - Voice over IP – Services – Mode – Busy on Busy**



2.  Click **Submit**.

## 3.3.13 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 using the Configuration File:**

- Use the table below as reference.

**Table 3-28: 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. <br> ▪ [**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. <br> ▪ [**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. |

## 3.3.14 Configuring Media Streaming

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

### 3.3.14.1 Configuring Quality of Service

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

➢ **To configure QoS using the Web interface:**

1. Open the Media Streaming page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

**Figure 3-32: Web Interface – Media Streaming - Quality of Service Parameters**



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

➢ **To configure QoS using the Configuration File:**

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

**Table 3-29: QoS Parameters**

| Parameter | Description |
|---|---|
| Type of Service (ToS) <br> **[voip/media/media_tos]** | Defines DS (Differentiated Services) containing a DSCP (Differentiated Services Code Point) value and an ECN (Explicit Congestion Notification) value. <br> DSCP is backwards compatible with ToS. ECN is not. <br> 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). <br> See *RFC 3168* for detailed information. |

### 3.3.14.2 Configuring Codecs

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

➢ **To configure the codecs using the Web interface:**

1. Open the Media Streaming page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

**Figure 3-33: Web Interface – Media Streaming - Codecs**

| Codec Priority | Codec Type | Packetization Time (milliseconds) |
|---|---|---|
| 1st Codec | G.722/16000 ▾ | 20 ▾ |
| 2nd Codec | G.711, 64 Kbps, u-Law ▾ | 20 ▾ |
| 3rd Codec | G.711, 64 Kbps, A-Law ▾ | 20 ▾ |
| 4th Codec | G.729, 8 Kbps ▾ | 20 ▾ |
| 5th Codec | G.722/16000 ▾ | 20 ▾ |

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

➢ **To define the codecs using 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 3-30: Codec Parameters**

| Parameter | Description |
|---|---|
| **[voip/codec/codec_info/%d/enabled]** | 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. |
| | 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. |
| | The *%d* variable stands for the priority: |
| | ▪ **[0]** - Disabled |
| | ▪ **[1]** (default) - Enabled |

| Parameter | Description |
|---|---|
| Codec Type<br>**[voip/codec/codec_info /%d/name]** | Name of the codec. The variable *%d* 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:<br>▪ **[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.<br>  ✓ Compatible with Skype for Business<br>  ✓ Flexible bit rate<br>  ✓ High quality<br>  ✓ Variety of sampling frequencies<br>  ✓ Inband FEC and good resilience to packet loss<br>**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 first priority vocoder, 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.<br>▪ **[G722]** G.722 (default)<br>▪ **[PCMA]** G.711 A-Law<br>▪ **[PCMU]** G.711 Mu-Law<br>▪ [G729] G.729<br>For example, **voip/codec/codec_info/0/name=G722**.<br>**Note**: Specific codecs require specific firmware files. For more information, refer to the *Release Notes*. |
| Packetization Time<br>**[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. |
| G.723 Bitrate<br>**[voip/codec/g723_bitrate]** | Low or high bit rate for G.723.<br>▪ [LOW] Low<br>▪ **[HIGH]** High (default) |
| **[voip/codec/g722_bitrate]** | G.722 bit rate.<br>▪ [G722_64K] (default)<br>▪ [G722_56K]<br>▪ [G722_48K]<br>**Note:** Currently, only 64bps is supported. |
| **[system/activation_keys/amr_coder]** | Activation key (string) required to unlock AMR coder (relevant for supporting firmware only). |

### 3.3.14.3  Configuring Real Time Protocol (RTP) Port Range

This section shows how to configure the RTP port range using the Web interface.

➢ **To configure the RTP port range using the Web interface:**

1.  Open the Media Streaming page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**) and scroll down to the parameter 'RTP Port Range'.

**Figure 3-34: Web Interface – Media Streaming - RTP Port Range**

| Media Streaming Parameters | |
| --- | --- |
| RTP Port Range - Contiguous Series of 4 Ports Starting From: | 50020 |

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

**Table 3-31: Media Streaming - RTP Port Range**

| Parameter | Description |
| --- | --- |
| RTP Port Range | Defines the base port for the range of RTP ports which the enterprise network administrator must open on the network's firewall. Default: 50020. Valid possible ports (if the default is selected as base port): 50020-50140. If, for example, 6000 is selected as base port, the valid possible ports will be 6000-60120. |

### 3.3.14.4 Configuring RTCP Extended Report

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

➢ **To configure RTCP-XR using the Web interface:**

1. Open the Media Streaming page (**Configuration** tab > **Voice Over IP** menu > **Media Streaming**).

**Figure 3-35: Web Interface – Media Streaming - RTCP-XR**

| RTCP-XR | |
|---|---|
| RTCP-XR Voice Quality Statistics Mode: | Disable |

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

➢ **To configure RTCP_XR using the Configuration File:**

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

**Table 3-32: RTCP_XR Parameter**

| Parameter | Description |
|---|---|
| RTCP-XR Voice Quality Statistics Mode<br>**[voip/rtcp_xr/vq_statistics/mode]** | Sets RTCP_XR working mode.<br>Select either:<br>▪ [**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).<br>▪ [**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).<br>▪ [**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). |

### 3.3.14.5 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.

## 3.3.15 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.

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.

> **Note:** Applies to all phones. Does not apply to the HRS.

➢ **To enable paging using the Web interface:**

1. Open the Services page (**Configuration** > **Voice Over IP** > **Services**) and scroll down to 'Paging'.

**Figure 3-36: Web Interface – Services - Paging**



2. From the dropdown, select **Enable**.

**Figure 3-37: Web Interface – Services – Enabling Paging**



[See the next section for details about the 'Barge-in' feature].

3. Click **Submit** and then make sure 'Paging' is displayed in the:
   ♦ Web interface, in the Function Keys page (see under Section 3.2.3)
   ♦ In the 430HD and 440HD phone screen (MENU key > **Keys Configuration** > **Function Keys** > press the **Select** softkey > navigate to 'Paging')
   ♦ In the 420HD and 405HD phone screen (long-press dialpad key **1**-**9** > navigate to 'Paging')

➢ **To enable Paging using 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 3-33: 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 3.3.14.2 for supported codecs. Default: G722_8000. |
| **[voip/services/group_paging/enabled]** | Enables or disables the paging feature.<br>▪ **[0]** = Disabled [Default]<br>▪ **[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.<br>▪ **[0] =** Deactivated [Default]. Paging was deactivated for the key configured as paging dial, so the key will be a regular speed dial.<br>▪ **[1] =** Activated. Paging was activated for the key configured as paging dial.<br>**Note**:<br>▪ On the 405HD and 420HD, **n-n** are the nine Functional Keys indexed **0-8** in the Configuration File.<br>▪ On the 430HD and 440HD, **n-n** are the 12 Functional Keys indexed **0-11** in the Configuration File. |
| **[voip/services/group_paging/group/n-n/multicast_addr]** | Displayed in the Web interface 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.<br>**Note**:<br>▪ On the 405HD and 420HD, **n-n** are the nine Functional Keys indexed **0-8** in the Configuration File.<br>▪ On the 430HD and 440HD, **n-n** are the 12 Functional Keys indexed **0-11** in the Configuration File. |

| Parameter | Description |
|---|---|
| **[voip/services/group_paging/group/n-n/name]** | 405HD and 420HD: Defines the name of the group displayed in the phone's screen when there's an incoming paging call. Label is not supported.<br><br>430HD, 440HD and 450HD: 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.<br><br>**Note**:<br>• On the 405HD and 420HD, **n-n** are the nine Functional Keys indexed **0-8** in the Configuration File.<br>• On the 430HD and 440HD, **n-n** are the 12 Functional Keys indexed **0-11** 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).

## 3.3.16 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.

> **Note:** Applies to all phones except the 450HD for which support is pending.

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 using the Web interface:**

1. Open the Services page (**Configuration** > **Voice Over IP** > **Services**) and scroll down to 'Paging'.

**Figure 3-38: Web Interface – Services - Paging**



2. From the dropdown, select **Enable**:

**Figure 3-39: Web Interface – Services – Paging Enabled – Barge-in**



3. From the 'Barge-in' dropdown, select **Enable** (by default, it's **Disable**) and then click **Submit**.

➢ **To enable Barge-in using the Configuration File:**

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

**Table 3-34: 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. <br> ▪ **[0]** = [Default] Those in regular calls are prompted whether or not to accept an incoming paging call. <br> ▪ **[1]** = Incoming paging calls interrupt (barge in on) regular calls that are in progress. |

## 3.3.17 Enabling VocaNOM on the 405HD and 420HD Phones

VocaNOM must be enabled on the 420HD and 405HD phones before you can configure a VocaNOM softkey.

➢ **To enable VocaNOM using the Web interface:**

1. Open the Services page (**Configuration** tab > **Voice over IP** menu > **Services**) and scroll down until the VocaNOM section.

**Figure 3-40: Web Interface – Enabling VocaNOM – 420HD and 405HD Phones**



2. Select **Enabled** if it isn't already, enter the VocaNOM service's number to dial, and then click **Submit**; the **VCNM** softkey is displayed in the phone's screen.

➢ **To enable VocaNOM using the Configuration File:**

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

**Table 3-35: VocaNOM SIP URI Parameter**

| Parameter Name | Description |
|---|---|
| **[lync/VocaNom/sip_uri]** | Defines the number to dial to get the VocaNOM service. Default: 4444. |

## 3.3.18 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:**

    **1.** Open the Services page (**Configuration** tab > **Voice Over IP** menu > **Services**) and scroll down to 'Message Waiting Indication (MWI)'.

**Figure 3-41: Web Interface – Services - MWI**

| Message Waiting Indication (MWI) | |
|---|---|
| Voice Mail Number: | |
| Activate: | Enable |
| Subscribe To MWI: | Disable |

    **2.** From the 'Activate' dropdown, select **AUDC_VM** (AudioCodes voicemail).

    **3.** From the 'Subscribe to MWI' dropdown, select **Enable**.

**Figure 3-42: Web Interface – Dedicated Voicemail Server**

| Message Waiting Indication (MWI) | |
|---|---|
| Voice Mail Number: | |
| Activate: | AUDC_VM |
| Subscribe To MWI: | Enable |
| MWI Server IP Address or Host Name: | 0.0.0.0 |
| MWI Server Port: | 5060 |
| MWI Subscribe Expiry Time: | 3600 Seconds |

    **4.** Configure the parameters using the table below as reference.

➢ **To configure a dedicated voicemail server using 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 3-36: Dedicated Voicemail Server - Parameters**

| Parameter | Description |
|---|---|
| Voice Mail Number<br>**[voip/services/msg_waiting_ind/voice_mail _number]** | Enter the number of the service to dial in order to retrieve voicemail. |
| Activate<br>**[voip/services/msg_waiting_ind/enabled]** | Configure either:<br>▪ **[0] Disabled** if a voicemail service isn't required.<br>▪ **[1] Enabled** (default) in order to use Microsoft Exchange Server for voicemail.<br>▪ **AUDC_VM** in order to use a dedicated voicemail server other than Microsoft Exchange Server for voicemail. |

| Parameter | Description |
|---|---|
| Subscribe to MWI<br>[voip/services/msg_waiting_ind/subscribe] | • **[0] Disabled** (default) configure this option if you chose in the previous parameter to use Microsoft Exchange Server for voicemail.<br>• **[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. |
| MWI Server IP Address or Host Name<br>[voip/services/msg_waiting_ind/subscribe _address] | Enter the IP address of the AudioCodes gateway or PBX on which the voicemail application is located. |
| MWI Server Port<br>[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. |
| MWI Subscribe Expiry Time<br>[voip/services/msg_waiting_ind/expiraition _timeout] | Defines how often the voicemail application is updated (refreshed) for new mail. Default: Every **3600** seconds (i.e., every hour). |

## 3.3.19    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 using the Configuration File:**

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

**Table 3-37: Securing Voicemail Access by PIN Code Authentication Parameter**

| Parameter | Description |
|---|---|
| [voip/services/vm_skip_pin_code/enabled] | Configure:<br>• **[0] Disable** in order 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.<br>• **[1] Enable** (default) for the phone to skip PIN code authentication and allow the user direct access to voicemail. |

## 3.3.20    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 3-43: Exchange Admin Center - Unified Messaging**
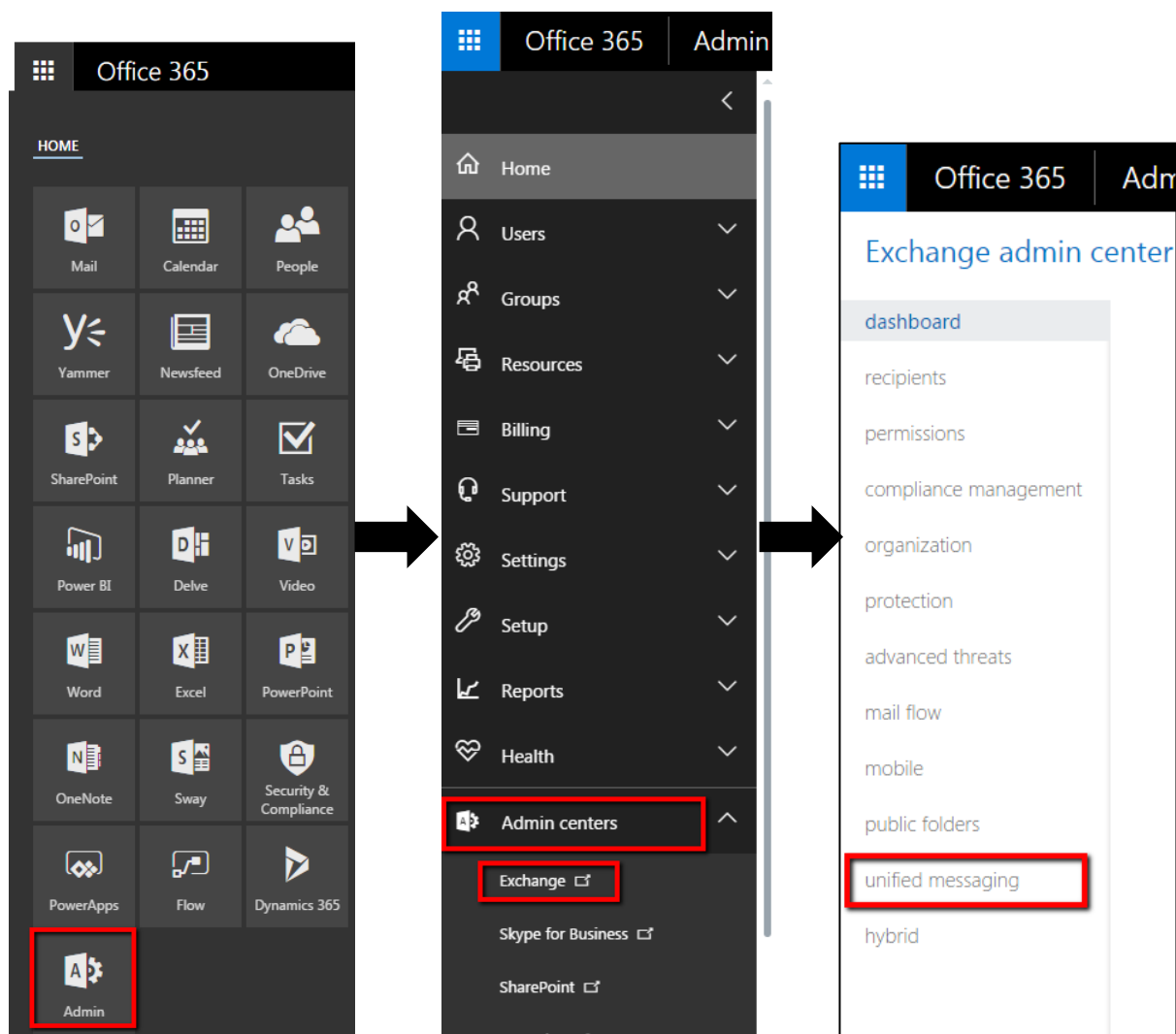


2.   In the Exchange Admin Center – Unified Messaging screen (see the figure below), click the **+** icon to set up a dial plan.

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

**Figure 3-44: Setting up a Dial Plan**
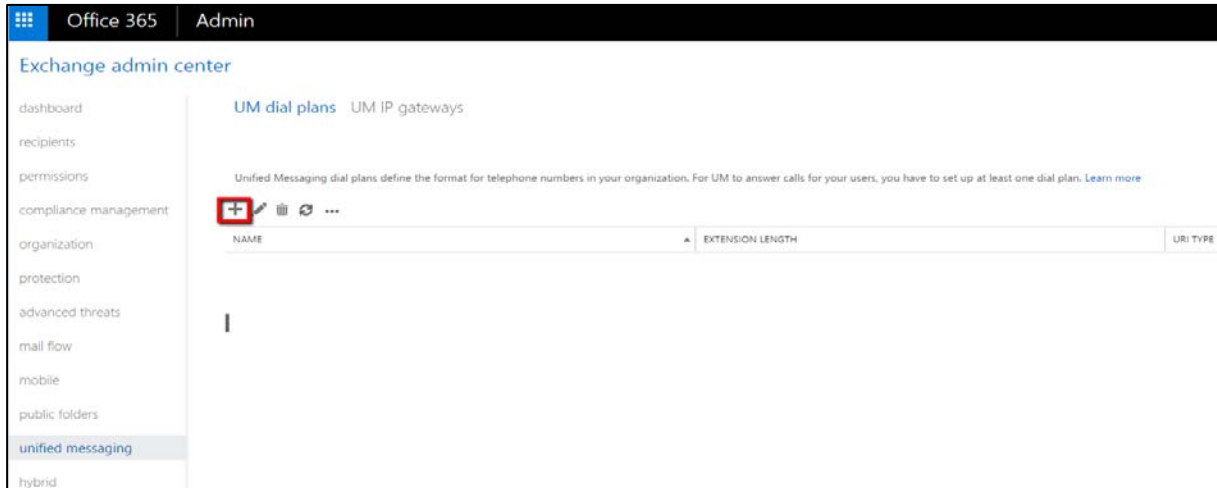


3. Set up the new Dial Plan with URI TYPE = SIP URI, as shown in the figure below.

**Figure 3-45: New Dial Plan: URI Type = SIP URI**

**4.** Click **Save**.

**Figure 3-46: Dial Plan: Rules and Settings**



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

**Figure 3-47: Edit**

**6.** Make sure the MWI option is selected.

**Figure 3-48: Enabling UM for Users**



### 3.3.20.1 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 3-49: 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 3-50: Browse to the UM Dial Plan**
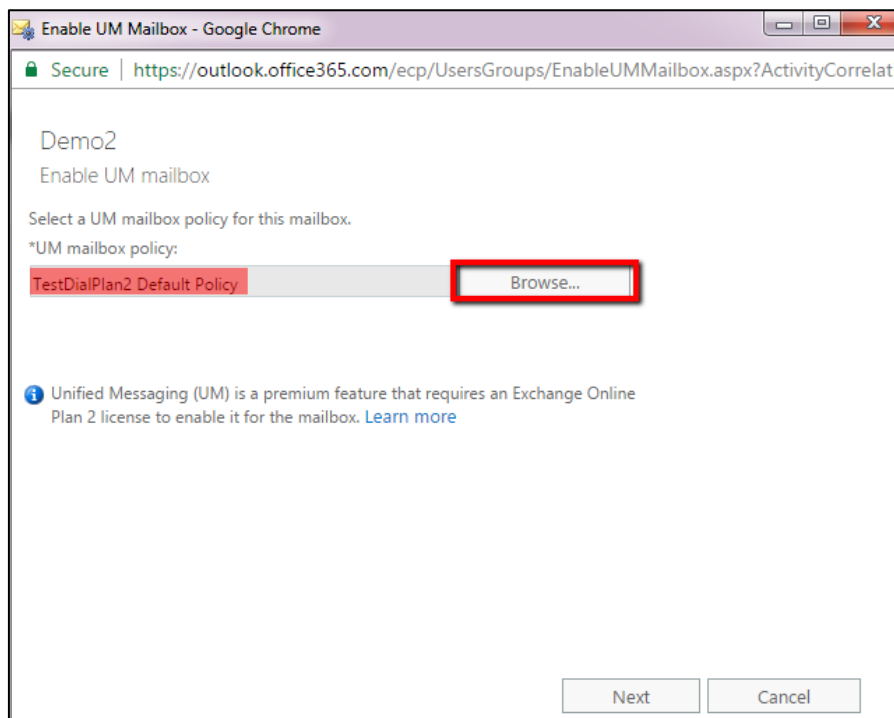


**7.** Click **Next** and enter the user's SIP address and/or Extension Number, and enter the PIN if the checkbox is selected.

**Figure 3-51: User's SIP Address and/or Extension Number, and PIN**
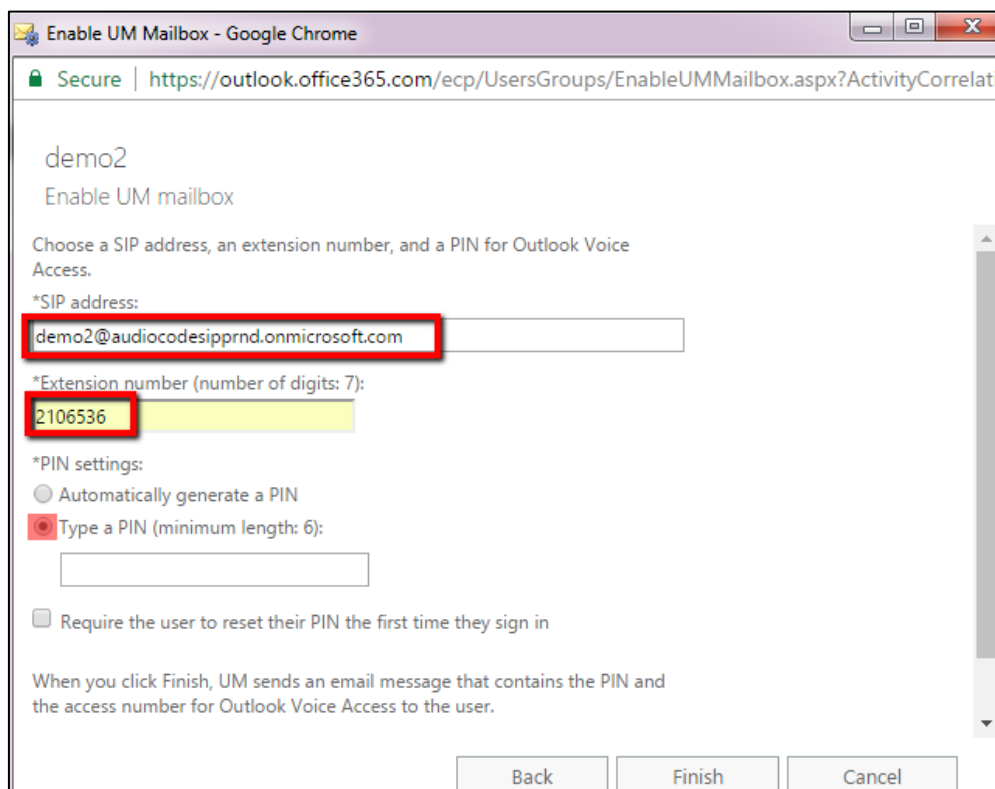
**8.** After the user is enabled and configured with a UM Dial Plan for VoiceMail indicator, the phone must be rebooted - or signed out and then signed back in again.

### 3.3.20.2 Troubleshooting

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

**Figure 3-52: Troubleshooting – Protected Voice Mail**

# 3.4 Configuring Security

## 3.4.1 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.

### 3.4.1.1 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').

## 3.4.2 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="}
```

> **Note:** 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.

## 3.4.3    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.

### 3.4.3.1    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:**

1. Open the Root CA Certificate page (**Configuration** tab > **Security** menu > **Root CA Certificate**).

**Figure 3-53: Web Interface – Root CA Certificate**



2. Click **Browse** to navigate to the certificate file, and then click **Load** to upload it to the phone. The maximum number you can load to the phone is 5. Click **Del** to delete a load if necessary. Click **Display** to display the certificate if you require viewing it.

**Table 3-38: Root CA Certificate Parameters**

| Parameter | Description |
|---|---|
| Root CA 1<br>**[security/ca_certificate/0/uri=]** | The first root CA certificate loaded to the phone. |
| Root CA 2<br>**[security/ca_certificate/1/uri=]** | The second root CA certificate loaded to the phone. |
| Root CA 3<br>**[security/ca_certificate/2/uri=]** | The third root CA certificate loaded to the phone. |
| Root CA 4<br>**[security/ca_certificate/3/uri=]** | The fourth root CA certificate loaded to the phone. |
| Root CA 5<br>**[security/ca_certificate/4/uri=]** | The fifth root CA certificate loaded to the phone. |

### 3.4.3.2 Loading the Client Certificate to the Phone

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

➢ **To load the Client Certificate to the phone:**

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

**Figure 3-54: Web Interface – Client Certificate**



2.  Refer to the table below. You can also load the file/s to the phone using the Configuration File. In the table below, the Configuration File parameters are in square parenthesis in bold.

**Table 3-39: Client Certificate Parameters**

| Parameter | Description |
|---|---|
| Certificate<br>**[security/sip_certificate_uri=]** | Loads the Client Certificate for SIP TLS (SIP calls with Transport Layer Security) to the phone. |
| Private Key<br>**[security/sip_private_key_uri]** | Loads the Client Private Key for SIP TLS (SIP calls with Transport Layer Security) to the phone. |
| Certificate<br>**[security/ieee802_1x_certificate_uri=]** | Loads the Client Certificate for 802.1X Authentication to the phone. The certificate must be in .pem format. |
| Private Key<br>**[security/ieee802_1x_private_key_uri=]** | Loads the Client Private Key for 802.1X Authentication to the phone. The certificate must be in .pem format. |

### 3.4.3.3 Generating a Certificate Signing Request

The section shows how to generate a certificate signing request (CSR) to send to the Certifcate 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 3-55: Web Interface – Certificate Signing Request**
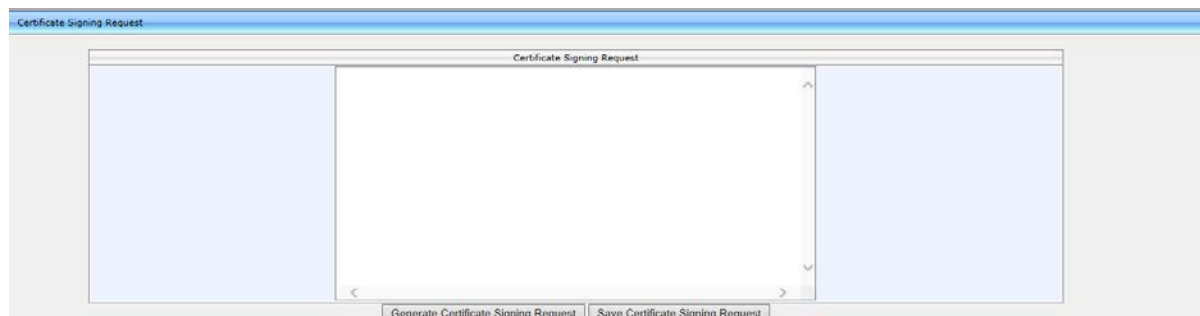


2. Click **Generate Certificate Signing Request**; the phone creates a CSR file.
3. Click **Save Certificate Signing Request** and download the CSR file to your PC.
4. Send the CSR file to the Certificate Authority to sign the Client Certificate.
5. You can load the Client Certificate to the phone for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

## 3.4.4    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.

### 3.4.4.1    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 3.4.4.2

● **EAP-TLS** - see Section 3.4.4.3

### 3.4.4.2    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**.

### 3.4.4.3    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.

## 3.4.5 Using the Web Interface / Configuration File

This section shows how to configure 802.1X from the Web interface or using the Configuration File.

### 3.4.5.1 EAP MD5 Mode

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

➢ **To configure the phone's 802.1X settings for EAP MD5 using the Web interface:**

1. Open the 802.1X Settings page (**Configuration** tab > **Network Connections** > **802.1X Settings**) and from the 'EAP Type' dropdown, select **EAP-MD5**.

**Figure 3-56: Web Interface - 802.1X Settings - EAP MD5**



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

➢ **To configure EAP MD5 using 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 3-40: EAP MD5 Parameters**

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

### 3.4.5.2 EAP TLS Mode

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

➢ **To configure 802.1X settings for EAP TLS using the Web interface:**

1. Open the 802.1X Settings page (**Configuration** > **Network Settings** > **802.1X Settings**) and from the 'EAP Type' dropdown, select **EAP-TLS**.

**Figure 3-57: Web Interface - 802.1X Settings – EAP-TLS**

| ▼802.1X Settings | |
|---|---|
| EAP Type: | EAP-TLS ▼ |

2. Click **Submit**.

➢ **To configure EAP TLS using 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 3-41: EAP TLS Parameters**

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

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

## 3.4.6 Configuring HTTPS

This section shows how to access the Web interface using HTTPS, for example, https://10.16.2.40, to secure provisioning.

Firmware and configuration files will then be loaded to the phone from the HTTPS server. The Firmware URL and Configuration URL parameters in the page below show how HTTPS is defined:

**Figure 30-1: Web Interface – HTTPS**



**Note:**

- To implement secure provisioning using HTTPS, the HTTPS server on the far end (from where you are loading the files) must also support HTTPS.
- The connection between the phone and the AudioCodes IP Phone Management Server is now fully secured using HTTPS.
- To increase the security level, it's advisable to block any HTTP connection using the Configuration File parameter *security/web/https_only*.

## 3.4.7 Supported Encryption Ciphers and TLS Version

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

## 3.5    Configuring Advanced Applications

### 3.5.1    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 Web interface or Configuration File.

➢   **To configure DHCP using the Web interface:**

   **1.**   Open the Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

**Figure 3-58: Web Interface - Automatic Provisioning – Dynamic URL**



   **2.**   Configure the parameters using the table below as reference and click **Submit**.

➢   **To configure DHCP using 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 3-42: 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. `provisioning/method=dynamic`). | |
| Provisioning Method<br>**[provisioning/method]** | Defines the provisioning method:<br><br>▪  **[Disable]** Disable - Automatic update is disabled. The phone attempts to upgrade its firmware and configuration<br>▪  **[Dynamic]** DHCP Options (Dynamic URL) (default) - Using DHCP options 160 or 66/67 for provisioning<br>▪  **[Static]** Static URL - Using Static URL for provisioning |
| DHCP Option Value<br>**[provisioning/url_option_value]** | Determines the DHCP option number to be used for receiving the URL for provisioning.<br>The default value is 160.<br>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.<br>The following syntax is available for DHCP option 160: |

| Parameter | Description |
|---|---|
| | ▪ \<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\> |
| | Where \<protocol\> can be either "ftp", "tftp", "http" or "https" and where \<configuration file name\> can be either: |
| | ▪ A unique configuration file, per phone, for example: \<MAC\>.cfg <br> -or- |
| | ▪ A global configuration file, per deployment, for example, 420HD.cfg |
| | <u>Unique Configuration Example</u> |
| | **http://192.168.2.1/different.img;\<MAC\>.cfg** |
| | The retrieved firmware file is *different.img* and the configuration file name is *\<MAC\>.cfg* such as *001122334455.cfg* |
| | <u>Global Configuration Example</u> |
| | **http://192.168.2.1/\<420HD\>.cfg** |
| | The configuration file name is *420HD.cfg* |
| | The following syntax is available for DHCP Options 66/67: |
| | ▪ Option 66 must be a valid IP address or host name of a TFTP server only. |
| | ▪ Option 67 must be the firmware name. |
| | If Option 67 is absent, the phone requests for the 420HD.img image file. For example: |
| | ▪ **Option 66:** 192.168.2.1 or myTFTPServer |
| | ▪ **Option 67:** 420HD_2.0.9.img |
| | **Note:** |
| | ▪ 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. |
| Random Provisioning Time <br> **[provisioning/random_provisioning_time]** | Defines the maximum random number to start the provisioning process. |
| | 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. |
| | The valid range is 0-65535. The default value is 120. |

| Parameter | Description |
|---|---|
| Check Period<br>**[provisioning/period/type]** | Defines the period type for automatic provisioning:<br>▪ **[hourly]** Hourly **-** Sets an interval in hours.<br>▪ **[daily]** Daily (default) - Sets an hour in the day.<br>▪ **[weekly]** Weekly - Sets a day in the week and an hour in the day.<br>▪ **[powerup]** On Power-up Only - The phone tries to upgrade only after power-up. |
| Every (Check Period = Hourly)<br>**[provisioning/period/hourly/hours_interval]** | The interval in hours for automatically checking for new firmware and configuration files.<br>The valid range is 1 to 168. The default is 24.<br>**Note:** This parameter is applicable only when `type` is configured to "hourly". |
| Every day at<br>**[provisioning/period/daily/time]** | The hour in the day for automatically checking for new firmware and configuration files.<br>The format of this value is **hh:mm**, where **hh** is hour and **mm** is minutes. For example, `00:30.`<br>The default time is **00:00**.<br>**Note:** This parameter is applicable only when **type** is configured to "daily". |
| Every (Check Period = Day)<br>**[provisioning/period/weekly/day]** | The day in the week for automatically checking for new firmware and configuration files.<br>▪ **[Sunday]** Sunday (default)<br>▪ [Monday] Monday<br>▪ [Tuesday] Tuesday<br>▪ [Wednesday] Wednesday<br>▪ [Thursday] Thursday<br>▪ [Friday] Friday<br>▪ [Saturday] Saturday<br>**Note:** This parameter is applicable only when **type** is configured to "weekly". |
| Every (Check Period = Weekly)<br>**[provisioning/period/weekly/time]** | The hour in the day for automatically checking for new firmware and configuration files.<br>The format of this value is: **hh:mm**, where **hh** is hour and **mm** is minutes. For example: `00:30`<br>The default time is **00:00**.<br>**Note:** This parameter is applicable only when **type** is configured to "weekly". |

### 3.5.1.1 DHCP Option 160

DHCP Option 160 can be configured using the Web interface.

➢ **To configure DHCP Option 160 using the Web interface:**

1. Open the Automatic Provisioning page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

**Figure 3-59: Web Interface - Automatic Provisioning - DHCP Option 160**



2. From the 'Provisioning Method' drop-down list, select **DHCP Option (Dynamic URL)**.
3. In the 'DHCP Option Value' field, enter **160**.
4. Configure the remaining parameters and click **Submit**.
5. After reboot, confirm that the firmware and configuration files have been updated.

### 3.5.1.2 DHCP Options 66 and 67

DHCP Options 66 and 67 can be configured using the Web as shown below.

➢ **To configure DHCP Options 66 and 67 using the Web interface:**

1. Open the Automatic provisioning page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

**Figure 3-60: Web Interface – Automatic Provisioning - DHCP Options 66/67**



2. From 'Provisioning Method', select **DHCP Option (Dynamic URL)**.
3. In the 'DHCP Option Value' field, enter **0**.
4. Configure the remaining parameters and click **Submit**.
5. After the reboot, confirm that the firmware and configuration files were updated.

## 3.5.2 Configuring Date and Time

> **Note:** 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.

Date and time can also be *manually* configured using the Web interface.

➢ **To manually configure date and time using the Web interface:**

■ Open the Date and Time page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**).

**Figure 3-61: Web Interface - Date and Time**



### 3.5.2.1 Configuring Daylight Saving Time

You can configure Daylight Saving Time using the Web interface or Configuration File.

➢ **To configure Daylight Saving Time using the Web interface:**

1. In the Date and Time page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**) shown above, set the 'Active' parameter to **Enable**; the page section shown below opens.

**Figure 3-62: Web Interface – Daylight Saving Time**



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

➢ **To configure Daylight Saving Time using the Configuration File:**

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

**Table 3-43: Daylight Saving Time Parameters**

| Parameter | Description |
|---|---|
| Active<br>**[system/daylight_saving/activate]** | Determines whether the phone automatically detects the Daylight Saving Time for the selected Time Zone.<br>▪ **[DISABLE]** Disable (default)<br>▪ [ENABLE] Enable |
| Date Format<br>**[system/daylight_saving/mode]** | Configures the date format. Valid values are:<br>**FIXED=** Date is specified as: Month, Day of month.<br>**DayOfWeek =** Date is specified as Month, Week of month, Day of week. |
| Start Time<br>**[system/daylight_saving/start_date]** | This subsection defines the starting day for the daylight saving offset.<br>▪ **[month]** - defines specific month in year<br>▪ **[day]** - defines specific day in month<br>▪ **[hour]** - defines specific hour in day<br>▪ **[minute]** - defines specific minute in hour<br>Example: To configure the phone to start daylight savings with a specific offset on February 22nd at 14:30, set the following:<br>**system/daylight_saving/start_date/month=2**<br>**system/daylight_saving/start_date/day=22**<br>**system/daylight_saving/start_date/hour=14**<br>**system/daylight_saving/start_date/minute=30** |
| Start Time<br>**[system/daylight_saving/start_date/month]** | The month in a year.<br>The valid range is 1 to 12. |
| Start Time<br>**[system/daylight_saving/start_date/day]** | The day in a month.<br>The valid range is 1 to 31. |
| Start Time<br>**[system/daylight_saving/start_date/hour]** | The hour in the day.<br>The valid range is 0 to 23. |
| Start Time<br>**[system/daylight_saving/start_date/minute]** | The minute in an hour.<br>The valid range is 0 to 59. |

| Parameter | Description |
|---|---|
| End Time<br>**[system/daylight_saving/end_date]** | This subsection defines the ending day for the daylight saving offset.<br>▪ **[month]** - defines the specific month in a year<br>▪ **[day]** - defines the specific day in a month<br>▪ **[hour]** - defines the specific hour in a day<br>▪ **[minute]** - defines the specific minute in an hour<br>For example: To configure the phone to end the daylight savings on July 16<sup>th</sup> at 22:15, set the following:<br>**system/ntp/daylight_saving/end_date/month=7**<br>**system/ntp/daylight_saving/end_date/day=16**<br>**system/ntp/daylight_saving/end_date/hour=22**<br>**system/ntp/daylight_saving/end_date/minute=15** |
| End Time<br>**[system/daylight_saving/end_date/month]** | The month in a year.<br>The valid range is 1 to 12. |
| End Time<br>**[system/daylight_saving/end_date/day]** | The day in a month.<br>The valid range is 1 to 31. |
| End Time<br>**[system/daylight_saving/end_date/hour]** | The hour in the day<br>The valid range is 0 to 23. |
| End Time<br>**[system/daylight_saving/end_date/minute]** | The minute in an hour.<br>The valid range is 0 to 59. |
| Offset<br>**[system/daylight_saving/offset]** | The offset value for the daylight saving.<br>The valid range is 0 to 180. The default offset is 60. |
| **[system/daylight_saving/start_date/week]** | Relevant to 'Day of week' mode:<br>The week of month (values 1-5) for start of daylight saving time. |
| **[system/daylight_saving/start_date/day_of_week]** | Relevant to 'Day of week' mode:<br>The day of week for daylight saving time start<br>Valid values :<br>**[SUNDAY]**<br>**[MONDAY]**<br>**[TUESDAY]**<br>**[WEDNESDAY]**<br>**[THURSDAY]**<br>**[FRIDAY]**<br>**[SATURDAY]** |
| **[system/daylight_saving/end_date/week]** | Relevant to 'Day of week' mode:<br>The week of month (values 1-5) for end of daylight saving time. |

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

### 3.5.2.2 Configuring NTP Server

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

➢ **To configure the NTP server using the Web interface:**

1. Open the Date and Time page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**).
2. Configure the parameters under the NTP & Time Settings section using the table below as reference, and then click **Submit**.

**Figure 3-63: Web Interface - NTP & Time Settings**



➢ **To configure the NTP server using the Configuration File:**

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

**Table 3-44: NTP Server Parameters**

| Parameter | Description |
|---|---|
| Active<br>**[system/ntp/enabled]** | Enables the NTP server from which the phone retrieves the date and time.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable – obtains the time information from a configured NTP server |
| Primary Server<br>**[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**.<br>You can select from the dropdown or leave the dropdown as **User defined and manually** define your domain in the adjacent field. |
| Secondary Server<br>**[system/ntp/secondary_server_address]** | Defines the address of the secondary NTP server. |
| Update Interval<br>**[system/ntp/sync_time]** | This sub-section defines how often the phone must perform an update with the NTP server.<br>▪ **[days]** - defines the number of days<br>▪ **[hours]** - defines the number of hours<br>For example: To configure the phone to perform an update with an NTP server every 1 day and 6 hours, set the following:<br>**system/ntp/sync_time/days=1**<br>**system/ntp/sync_time/hours=6** |
| Update Interval<br>**[system/ntp/sync_time/days]** | The number of days.<br>The valid range is 0 to 7. The default of days is 0. |
| Update Interval<br>**[system/ntp/sync_time/hours]** | The number of hours.<br>The valid range is 0 to 24. The default is 12. |
| Time Display Format<br>**[system/ntp/time_display_format]** | The format of the time displayed on the phone screen.<br>▪ **[24Hour]** (default)<br>▪ [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.

### 3.5.2.3 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).

⚠️ **Note:** 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 using Web interface:**

1. Open the Date and Time page (**Configuration** tab > **Advanced Applications** menu > **Date and Time**).

2. From the 'Obtain Time Zone From DHCP' drop-down list, select **Disable**; the page below is shown.

**Figure 3-64: Web Interface - NTP and Time Settings**



3. Configure the NTP and Time Settings using the table below as reference, and then click **Submit**.

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

**Table 3-45: NTP Server and GMT Parameters**

| Parameter | Description |
|---|---|
| Time Zone<br>**[system/ntp/gmt_offset]** | Default is **00:00**<br>Enables the NTP server from which the phone retrieves the date and time.<br>▪ **[0]** Disable<br>▪ **[1]** Enable – obtains the time information from a configured NTP server |
| **network/lan/dhcp/ntp/server_list/enabled** | 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**).<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |
| **network/lan/dhcp/ntp/gmt_offset/enabled** | Enables prioritization of the NTP GMT offset information received from the DHCP server (Option field 2), over the static configuration (**system/ntp/gmt_offset**).<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |

**Table 3-46: 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 |

## 3.5.3    Configuring Contacts (LDAP)

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

> **Note:** 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 using the Web interface:**

1. Open the Contacts page (**Configuration** tab > **Advanced Applications** > **Contacts**) and select **LDAP** from the 'Contact Search Method' dropdown list (the default is **SfB Contacts**).

**Figure 3-65: Web Interface – Contact Search Method**

Contacts

▼Contacts
| Contact Search Method: | SfB Contacts ∨ |
| T9 Mode: | Enable ∨ |

↓

| Contact Search Method: | LDAP ∨ | |
| Server Address: | | |
| Port: | 389 | |
| User Name: | | |
| Password: | | |
| Base: | | |
| Name Filter: | (\|(sn=%)(givenname=%)(displayname | |
| Name Attributes: | sn givenname displayname | |
| Number Filter: | (\|(telephoneNumber=%)(Mobile=%)(h | |
| Number Attributes: | telephoneNumber Mobile homePhon | |
| Display Name: | %displayname | |
| Max Hits: | 50 | (1~1000) |
| Country Code: | | |
| Area Code: | | |
| Sort Result: | Enable ∨ | |
| Search Timeout: | 5 | seconds |
| Call Lookup: | Enable ∨ | |

2. Configure the parameters using the table below as reference and click **Submit**.

➢ **To configure LDAP using 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 3-47: LDAP Parameters**

| Parameter Name | Description |
|---|---|
| Active<br>**[system/ldap/enabled]** | Enables or disable LDAP. |
| Server Address<br>**[system/ldap/server_address]** | Defines the IP address or URL of the LDAP server. |
| Port<br>**[system/ldap/port]** | Defines the LDAP service port. |
| User Name<br>**[system/ldap/user_name]** | Defines the user name used for the LDAP search request. |
| Password<br>**[system/ldap/password]** | Defines the password of the search requester. |
| Base<br>**[system/ldap/base]** | Defines the access point on the LDAP tree. |
| Name Filter<br>**[system/ldap/name_filter]** | Specifies your search pattern for name look ups.<br>For example:<br>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.<br>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.<br>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. |
| Name Attribute<br>**[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.<br>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. |
| Number Filter<br>**[system/ldap/number_filter]** | Specifies your search pattern for number look ups.<br>When you type in the following field, for example, *(\|(telephoneNumber=%)(Mobile=%)(ipPhone=%))*, the search result is all LDAP records which have the "telephoneNumber" OR "Mobile" OR "ipPhone"field match the number being searched.<br>When you type in the following field: *(&(telephoneNumber=%)(sn=*)),* the search result is all LDAP records which have the "sn" |

| Parameter Name | Description |
|---|---|
| | field set and the "telephoneNumber" match the number being searched. |
| Number Attributes<br>**[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.<br><br>When you type in the following field, for example, *Mobile telephoneNumber ipPhone*, you must specify 'Mobile', 'telephoneNumber' and 'ipPhone' fields for each LDAP record. |
| Display Name<br>**[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.<br><br>When you type in the following field, for example:**%sn, %givenName**, the displayed result returned should be "Black, Mike". |
| Max Hits<br>**[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). |
| Sort Result<br>**[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. |
| Search Timeout<br>**[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. |
| Call Lookup<br>**[system/ldap/call_lookup]** | Performs an LDAP search during call (search the display name for a number). |
| Country Code<br>**[system/ldap/country_code]** | Defines the country code prefix added for number search. |
| Area Code<br>**[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). |

## 3.5.4 Configuring T9
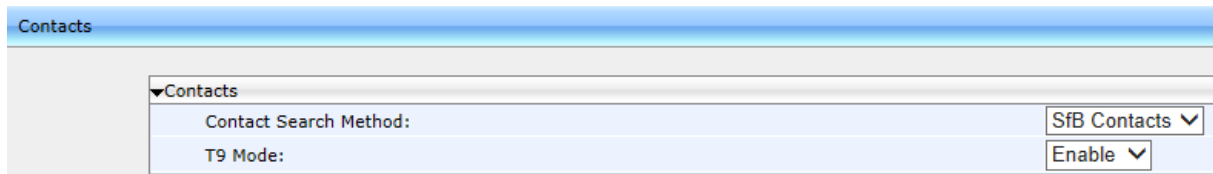
When searching for a contact in the Corporate Directory, users can press dial pad keys *to input letters*. Only a single press on any key, regardless of the letter's position on the key, is necessary

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

➢ **To configure T9 using the Web interface:**

■ Open the Contacts page (**Configuration** tab > **Advanced Applications** > **Contacts**) and make sure T9 is enabled (default). If it isn't, select **Enable** from the 'T9 Mode' dropdown list.

**Figure 3-66: Web Interface – T9 Mode**



➢ **To configure T9 using the Configuration File:**

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

**Table 3-48: T9 Parameter**

| Parameter Name | Description |
|---|---|
| T9 Mode<br>**[lync/contact_search_t9_enabled]** | Enables or disable T9 mode. Default=**Enable**. |

# 4    Configuring Microsoft Skype for Business Features

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

## 4.1    Microsoft Screen Theme

> ⚠️ **Note:** Applies only to the 450HD 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    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.

## 4.3    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
```

2. 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).



3. 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:**

1. Open the ini configuration file in an editor like Notepad.

2. 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

3. Save and close the file and load it to the phone.

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

## 4.4    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'<br><br>Min: 300 seconds (5 minutes) (default); Max: 2678400 seconds (31 days) |
| [lync/presence/state_inactive_timeout] | Configures how long it will take for presence status to change from 'Inactive' to 'Away'<br><br>Min: 300 seconds (5 minutes) (default); Max: 2073600 seconds (24 days) |

## 4.5    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.

## 4.6    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

## 4.7 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.

   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
```

## 4.8 Updating Device Firmware from the Skype for Business Server

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

⚠️ **Note:** 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**



### 4.8.1 Enabling Automatic Firmware Updates from the Server in the Web Interface

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.

> ➢ **To enable automatic firmware updates from the Skype for Business server using the Web interface:**

1. Open the Automatic provisioning page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

**Figure 4-3: Web Interface – Automatic Provisioning – Firmware Provisioning**

| Automatic Provisioning | | |
| --- | --- | --- |
| **Firmware Provisioning** | | |
| Firmware Version : | | UC_3.0.1.63.240 |
| Provisioning Method : | SfB Update | |
| SfB Update Server : | Enabled | Check Now |
| SfB Update Server URL : | https://lyncweb2013.audiocodes.com:443/RequestHandlerExt/ucdevice.upx<br>https://aclpool2013.corp.audiocodes.com:443/RequestHandler/ucdevice.upx | |

2. From the 'Provisioning Method' dropdown, select **SfB Update**.
3. In the Check Period screen section shown below, select how frequently you want the server to perform the check.

**Figure 4-4: Web Interface – Automatic Provisioning – Check Period**

| Check Period | |
| --- | --- |
| Check Period : | Daily |
| Every day at : | 00:00 |
| Random Provisioning Time : | 120 minutes |

4. Click **Submit**.

## 4.8.2 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 using the Configuration File:**

■ 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.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |

## 4.8.3 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 4-5: 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.

## 4.9 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.

> **Note:**
> - 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 in the Web interface:**

1. Open the Pin Lock page (**Configuration** > **Personal Settings** > **Pin Lock**).

**Figure 4-6: Pin Lock**



2. From the 'Pin Lock' dropdown, select the **Enable** option if it isn't selected already and click **Submit**.

➢ **To enable the feature using the Configuration File:**

- 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 |
|---|---|
| Pin Lock<br>**[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.<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |

> **Note:** If a user's phone was automatically paired (see Section 4.11.7) 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.

### 4.9.1    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

#### 4.9.1.1    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 | Determines handset functionality when the phone is locked.<br>[**0**] Allows incoming and outgoing calls when the phone is locked<br>[**1**] Allows only incoming calls when the phone is locked<br>[**2**] Disallows incoming and outgoing calls when the phone is locked<br>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. |

#### 4.9.1.2    Allowing Users to Make/Receive Incoming/Outgoing Calls

Network administrators can configure a local phone parameter 'AllowCallsInLockState' to determine whether or not 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 | Determines whether or not users can make/receive incoming/outgoing calls if the phone locks.<br>[**GET_FROM_INBAND**] The phone's capabilities when locked are set by inband provisioning parameter (default)<br>[**ALLOW_BOTH**] Allows users to make/receive incoming/outgoing calls when the phone is locked<br>[**ALLOW_INCOMING_ONLY**] Allows users to make/receive incoming/outgoing calls when the phone is locked<br>[**DENY_BOTH**] Disallows users from making/receiving incoming/outgoing calls when the phone is locked<br>If set to **ALLOW_BOTH** or **ALLOW_INCOMING_ONLY** or **DENY_BOTH**, this parameter overrides the 'DisableHandsetOnLockedMachine' inband provisioning parameter. |

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

Network administrators can configure a local parameter 'AnswerDelegateIncomingCalls' to determine whether or not 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 'AnswerDelegateIncomingCalls'**

| Parameter Name | Description |
|---|---|
| AnswerDelegateIncomingCalls | Determines whether or not users can answer second-hand (Share Line Appearance and Delegation) incoming calls when the phone is locked.<br><br>[**0**] Users cannot answer incoming Delegate calls when the phone is locked (default)<br><br>[**1**] Users can answer incoming Delegate calls when the phone is locked.<br><br>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. |

## 4.10    Exchange Server Features

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

> **Note:** 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.

### 4.10.1    Configuring Calendar Displayed in the Phone's Screen

[Applies to all phones except the 420HD] 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.<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |
| **[lync/calendar/mode]** | Determines which Microsoft Exchange Calendar meetings will be displayed in the phone's screen.<br>▪ **[24H]** (Default) Displays meetings scheduled to commence<br>  ✓ between now and 24 hours from now<br>  ✓ before now but scheduled to end after now<br>  ✓ before 24 hours from now but scheduled to end after 24 hours from now<br>▪ **[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. |

## 4.10.2 Configuring Meeting Reminders Popping up in the Phone's Screen

[Applies to all phones except the 420HD] 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 using the Configuration File:**

■ 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]** | Determines for which types of meetings reminders will automatically pop up in the phone's screen. |
| | ▪ **[ALL]** (Default) Enables reminders for *all* 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 *all* 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. |

## 4.10.3    Visual Voicemail

[Applies to all phones except the 420HD]

> **Note:**
>
> - 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.

## 4.10.4    Skype for Business 'Favorites' Contacts & Outlook Contacts

[Applies to all AudioCodes phones except the 420HD model). 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 in order to optimize phone resources.

> ➢ **To configure the maximum number of Outlook contacts to display in the phone's screen using the Configuration File:**

- 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]** | Determines the maximum number of Outlook contacts to display in the phone's screen. <br> **[50]** (Default) = the phone will be capable of retrieving and displaying up to 50 Outlook contacts in the screen. <br><br> **[0]** = an unlimited number of Outlook contacts can be displayed in the phone's screen, i.e., as many contacts as there are defined in Outlook can be retrieved and displayed. <br><br> **[500]** = The maximum number of Outlook contacts that the phone can retrieve and display. |

## 4.11    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 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*).

### 4.11.1   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.

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

## 4.11.2  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.

---

**Note:**

- 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 4.11.3 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:
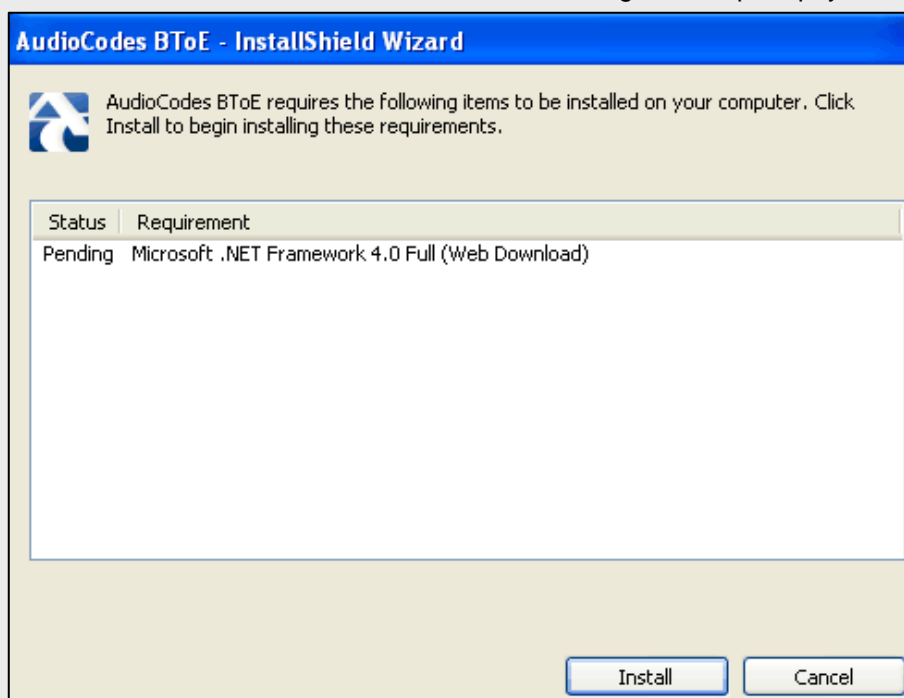


When installing the BToE PC/laptop application using the installation file *AudioCodes BToE.msi*, you won't be prompted to install .Net 4.0 and the network administrator should make the necessary preparations prior to installation of the BToE PC application.

---

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 4-7: InstallShield Wizard – Preparing to Install**
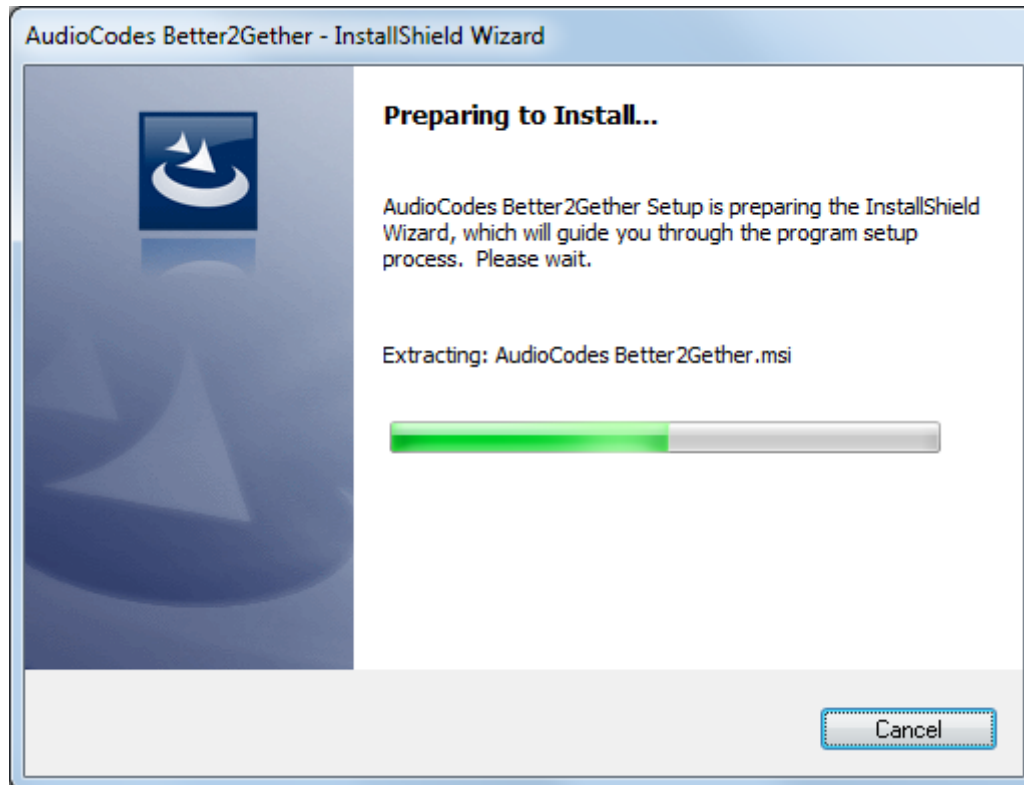


**Figure 4-8: Welcome to the InstallShield Wizard**
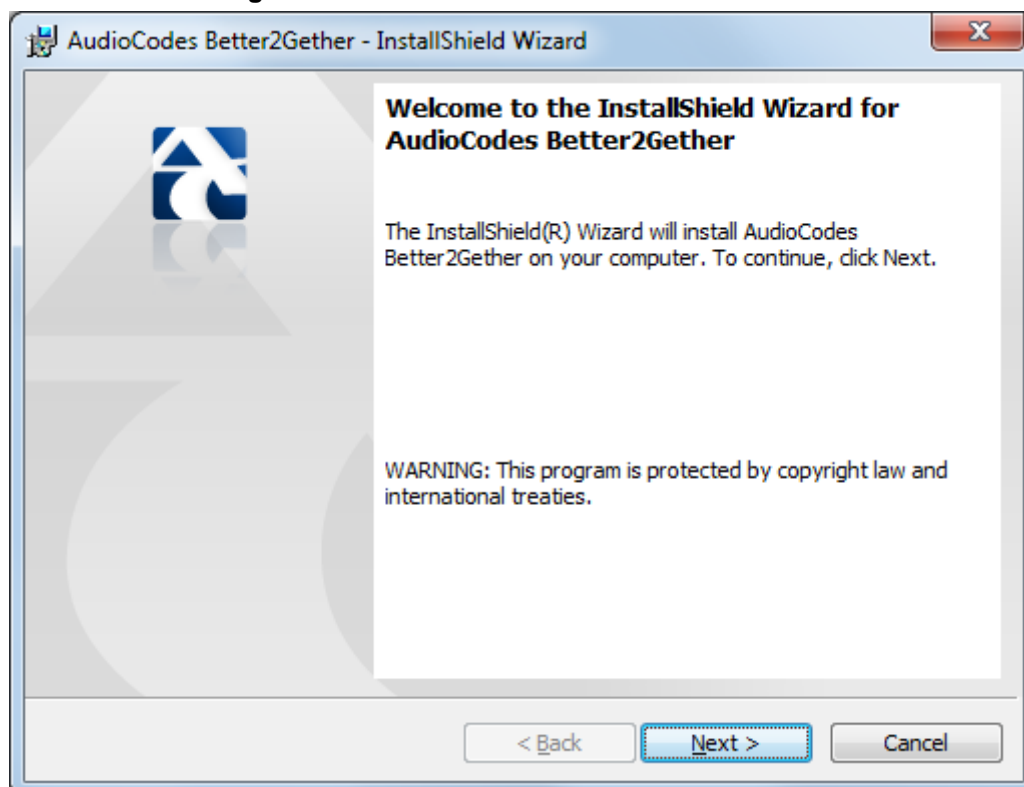


**2.** Click **Next**; the License Agreement dialog opens.

**Figure 4-9: License Agreement**
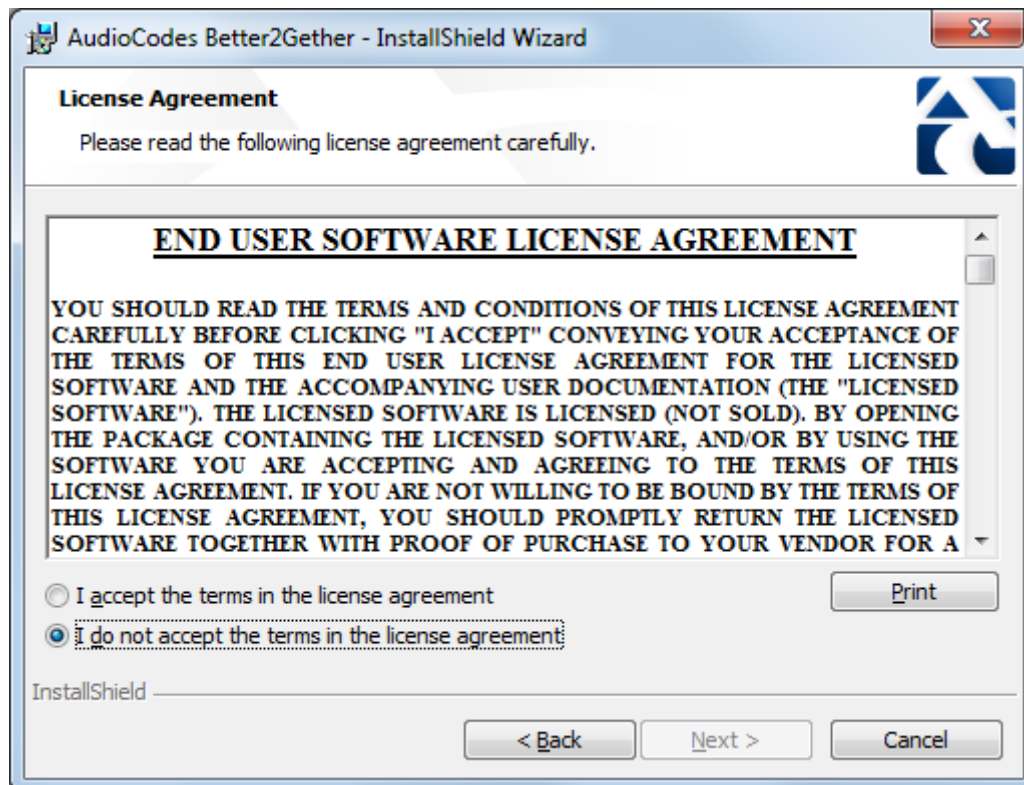


3. Select the **I accept…** option and click **Next**.

**Figure 4-10: License Agreement**



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

**Figure 4-11: Destination Folder**
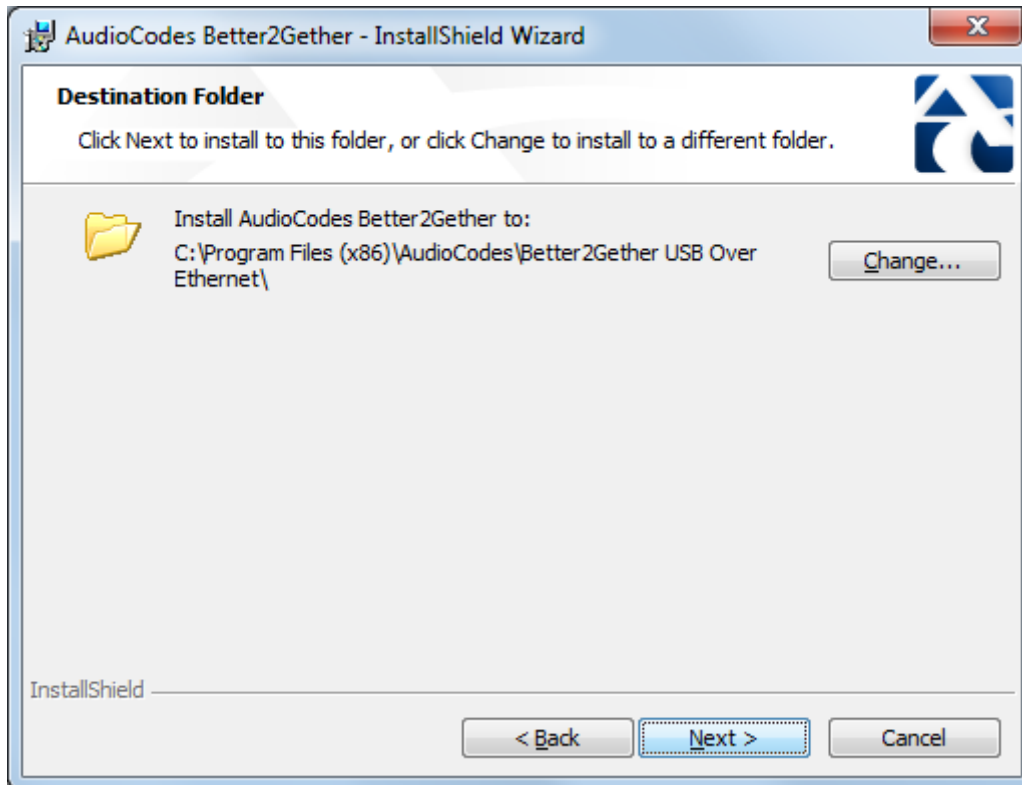


5.   To change the default Destination Folder, click **Change** and proceed to step 6. To leave the Destination Folder at its default, click **Next** and proceed to step 7.

**Figure 4-12: Change Current Destination Folder**
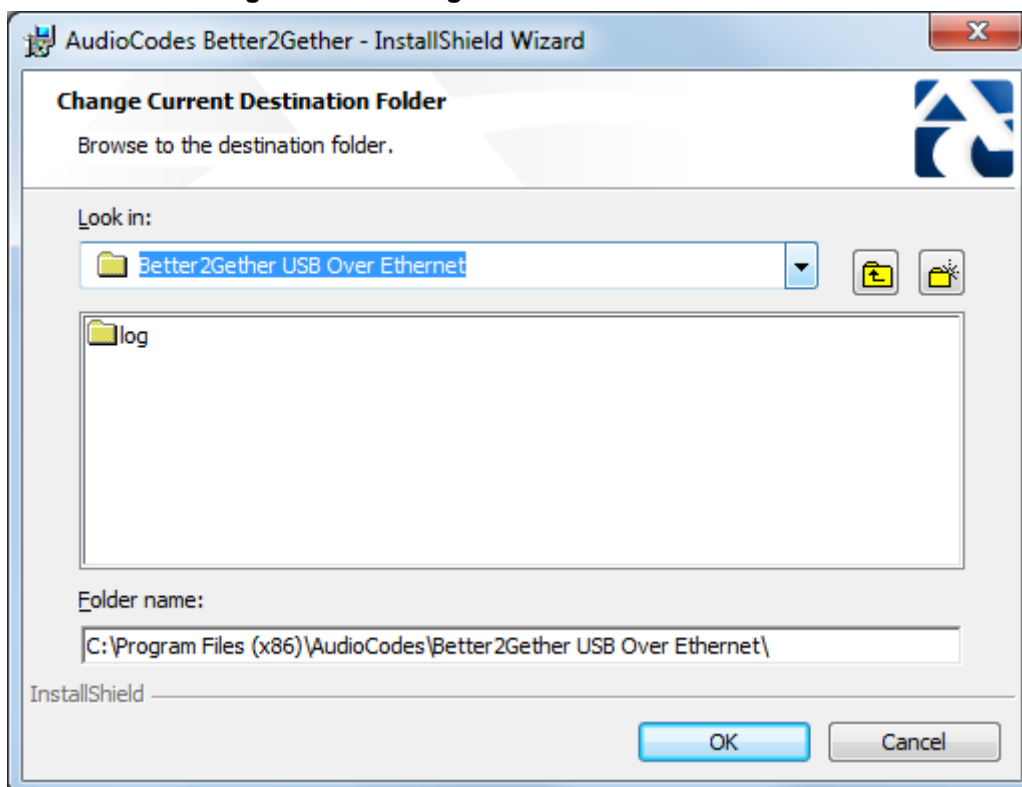
**6.** Click **OK**; you're returned to the Destination Folder dialog.

**7.** Click **Next**; the Ready to Install dialog opens.

**Figure 4-13: Ready to Install**
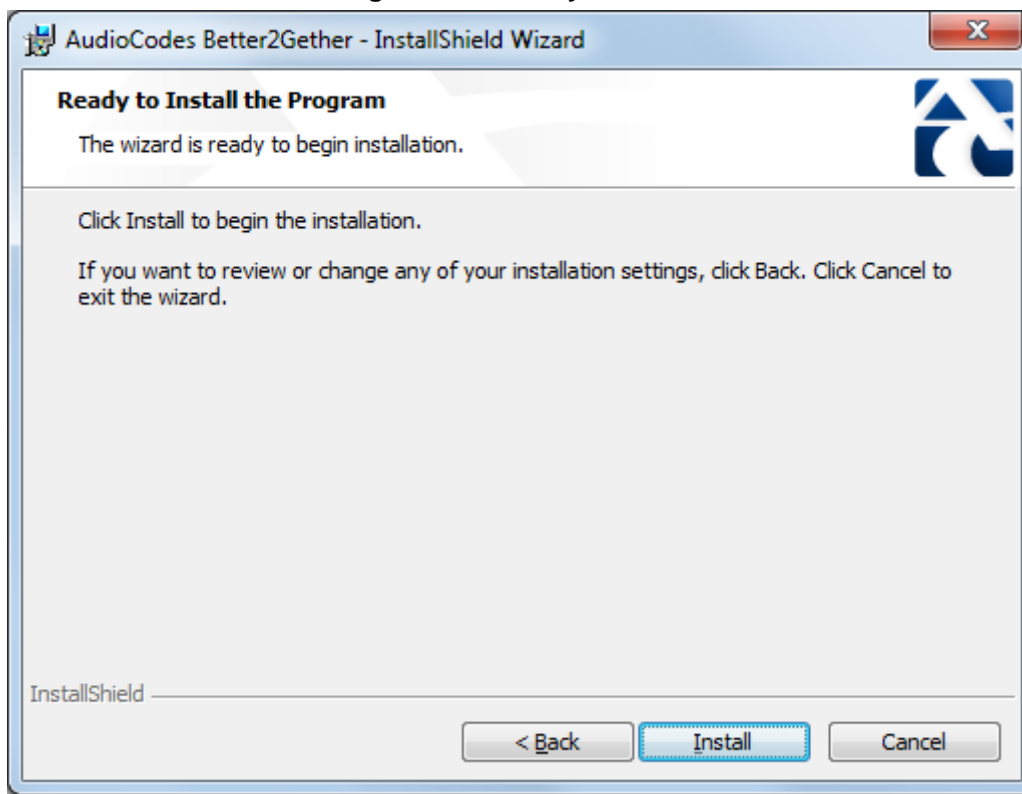


**8.** Click **Install**; the Installing AudioCodes Better2Gether dialog opens indicating installation progress status.

**Figure 4-14: Installing AudioCodes Better2Gether**
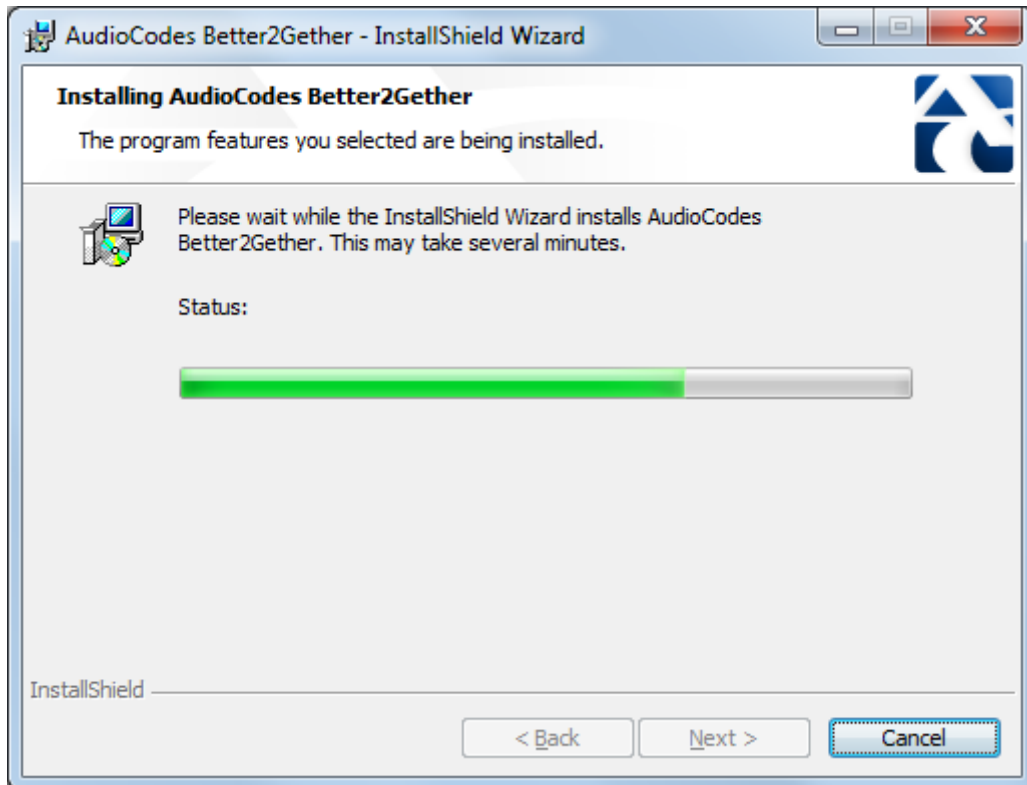


9. Wait until the following dialog is displayed:

**Figure 4-15: InstallShield Wizard Completed**
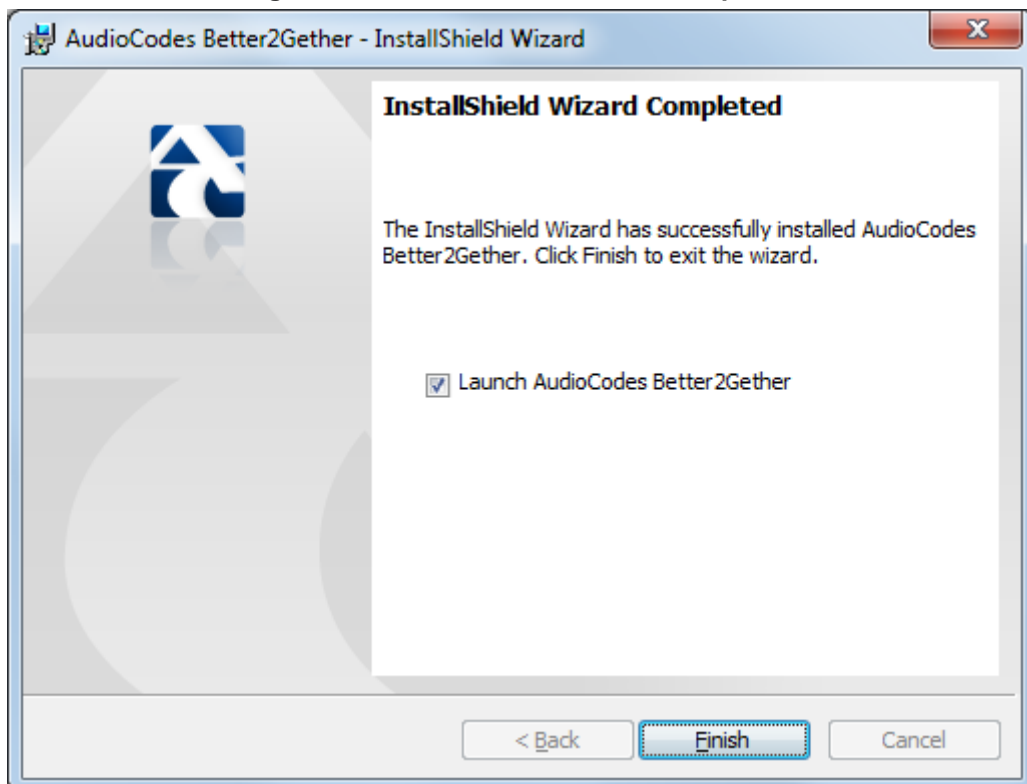
**10.** Click **Finish** and then check your Windows taskbar and locate the newly displayed AudioCodes icon (AC) as shown below:

**Figure 4-16: AudioCodes Icon in Taskbar**
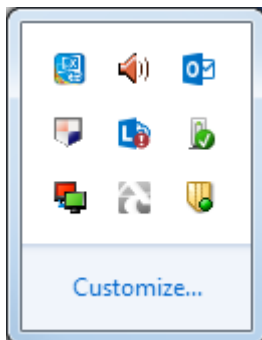


**11.** Wait until the "Installing device driver software" process completes:



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

**Figure 4-17: Control Panel>Programs>AudioCodes Better2Gether**
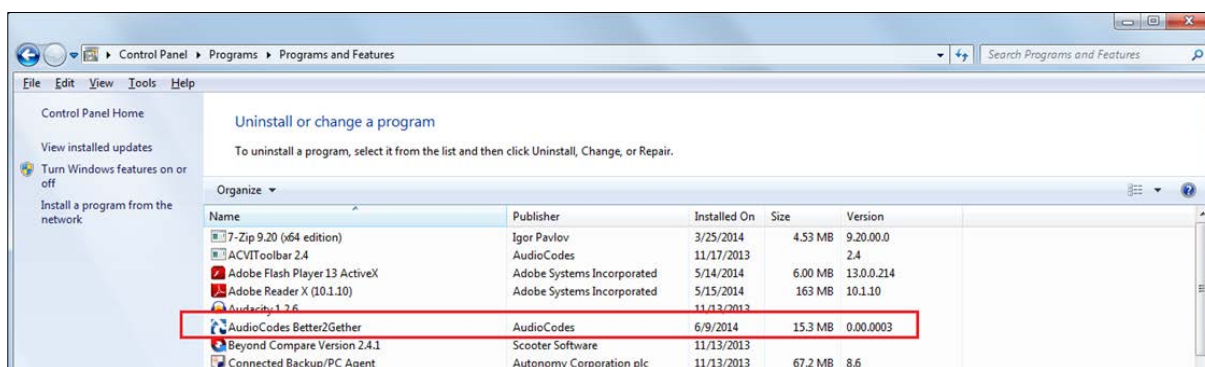


> ⚠️ **Note:** You can use this entry in the Control Panel > Programs to uninstall.

**13.** Access Computer Management > Services and Applications and locate BToE:

**Figure 4-18: Computer Management > Services and Applications**
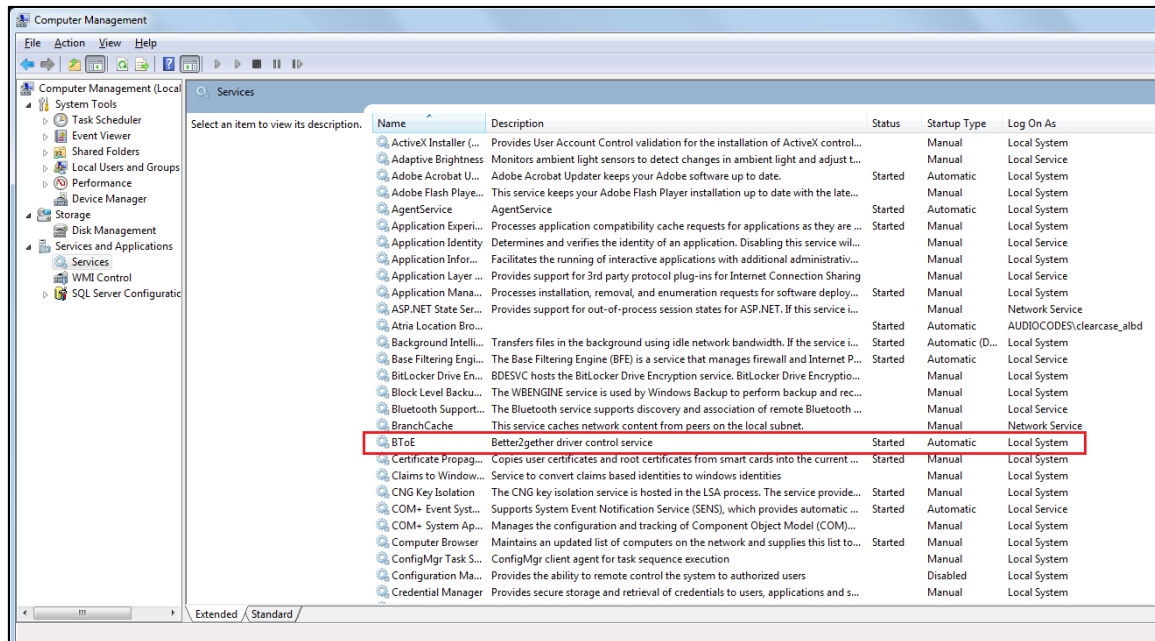


**14.** Access the Device Manager and locate 'AudioCodes B2GoE USB driver'.

**Figure 4-19: Device Manager > AudioCodes B2GoE USB Driver**
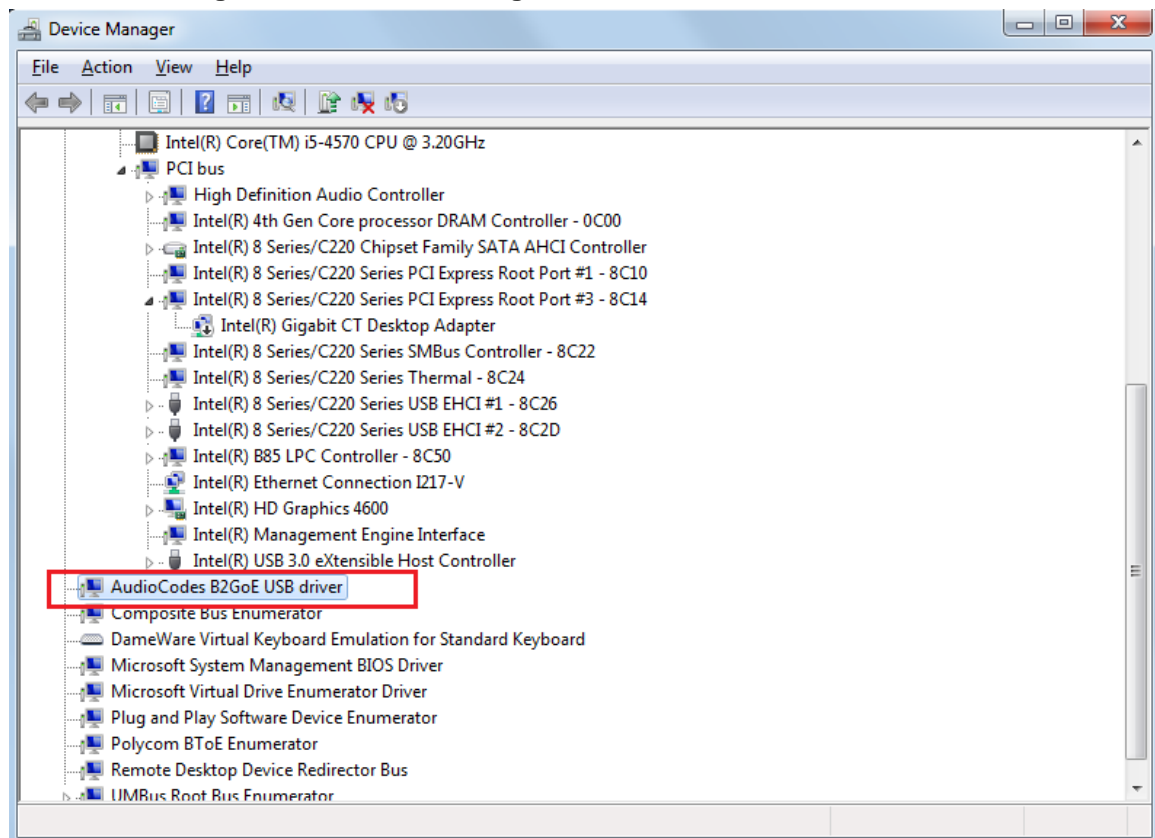


You've successfully installed the program.

## 4.11.3  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*.

> **Note:** Do not change the file name. Changing it is disallowed.

➢ **To distribute the BToE PC application *msi* package:**

**1.** Use the following command to install the *msi* package:
```
msiexec /I "AudioCodes BToE.msi" /qn
```

**2.** 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:**

**1.** 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
```

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

## 4.11.4 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 4-20: Popup Menu**
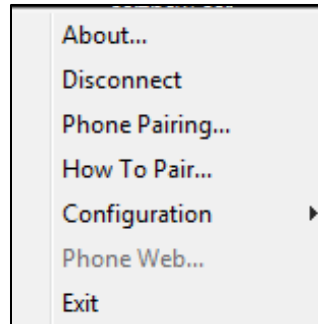


**2.** Select the **About…** menu option to verify the DLL and BToE version:

**Figure 4-21: About AC BToE**
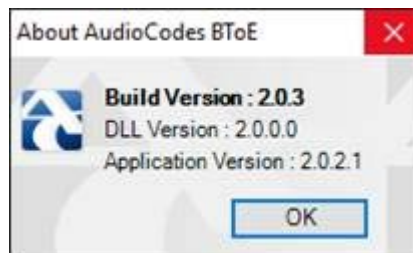


## 4.11.5 Enabling BToE for Online Users in the Skype for Business Server

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:**

**1.** 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

**2.** 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

## 4.11.6   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.

> **Note:** 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:**

**3.** Click the **AC** (AudioCodes) taskbar icon; the menu shown in Figure 4-20 pops up.

**4.** Select **Disconnect** in the popup menu and then select **Configuration** > **TCP Port**.

**Figure 4-22: TCP Port**
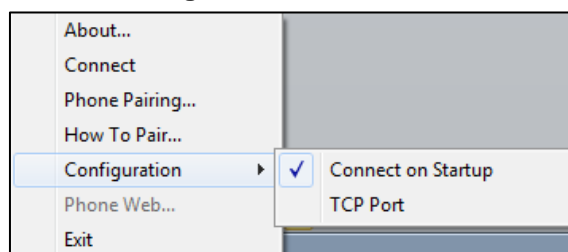


**5.** From the AC BTOE TCP Port dialog that opens, configure the TCP Port:

**Figure 4-23: 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**.

### 4.11.7 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.

> **Note:** 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*.

## 4.11.8    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 4.11.8.1)

**2.**    Connect the phone and BToE PC/laptop application using the pair code (see Section 4.11.8.2)

> **Note:**
> - 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.

### 4.11.8.1    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:

> **Note:**
> - 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.

### 4.11.8.2    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 4-24: Popup Menu**
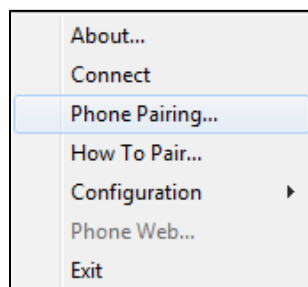
**2.** Select the **Phone Pairing** option

**Figure 4-25: Phone Pairing**
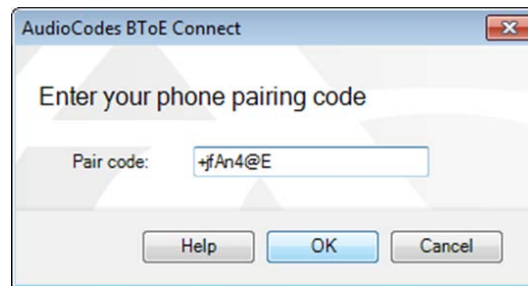


**3.** In the 'Enter your phone pairing code' dialog, enter the pair code that you generated as shown in Section 4.11.8.1; the **OK** button is activated after 8 characters are entered.

**3.** Click **OK**; BToE is activated.

**4.** If a communication error occurs or the wrong pair code was entered, the following icon indication appears:

**Figure 4-26: AC BToE Failed Indication**
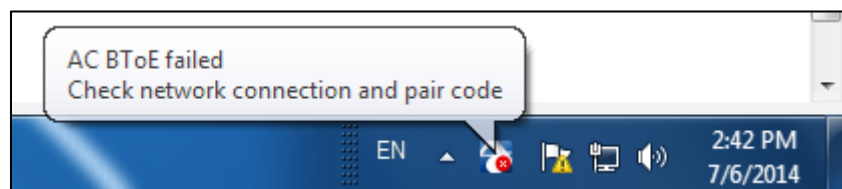


**5.** When BToE is successfully connected, view the following icon indication:

**Figure 4-27: AC BToE is Connected Indication**
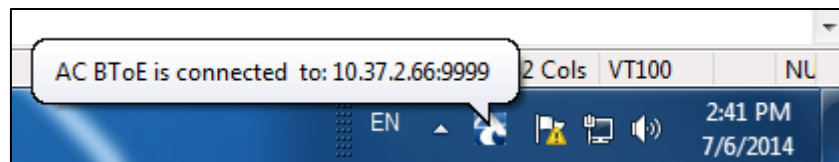


**6.** When BToE is in 'Connected' state, the popup menu shows the **Disconnect** menu item and the **Phone Pairing** menu item is deactivated:

**Figure 4-28: Popup Menu: 'Disconnect' Enabled, 'Phone Pairing' Disabled**
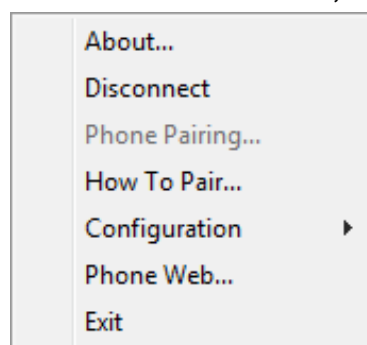


**7.** After selecting the **Disconnect** menu option, the 'AC BToE Disconnected' indication is displayed:

**Figure 4-29: BToE Disconnected**
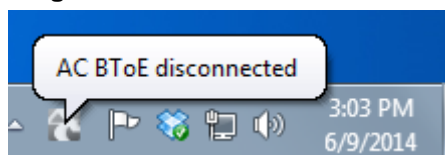


8.    From the popup menu as well you can see if BToE is disconnected:

**Figure 4-30: Popup Menu: BToE Disconnected**
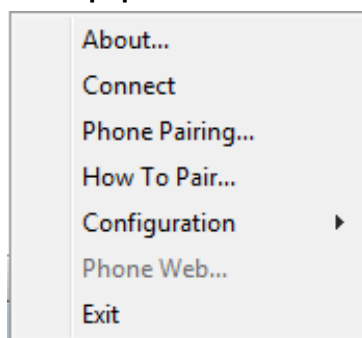


> ⚠️ **Note:** When BToE is connected, you can select the **Phone Web** menu option to open the phone's Web interface.

9. 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. |

10. 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 4-31: Start > Programs > AudioCodes > BToE Controller**
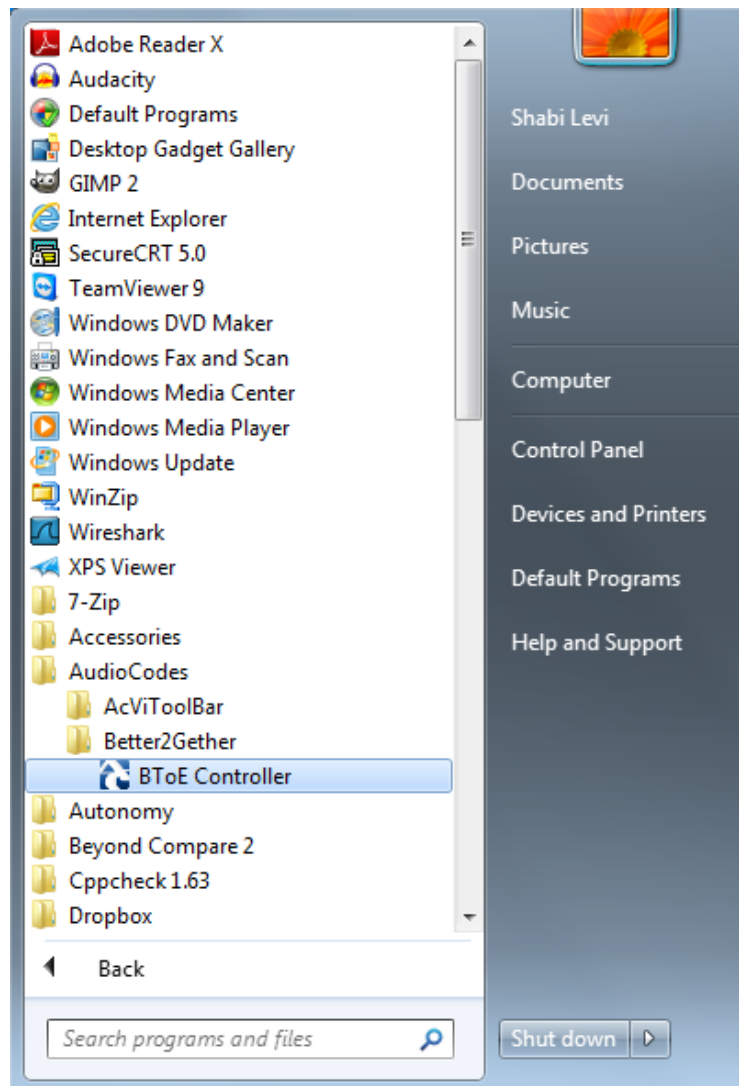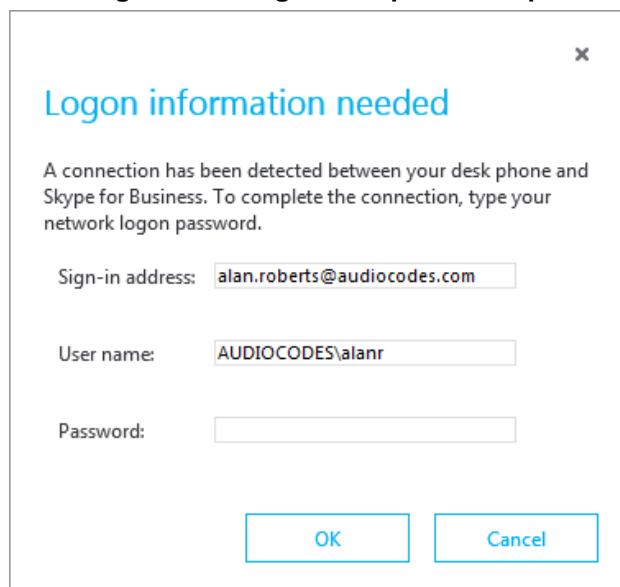
## 4.11.9    Connecting the Skype for Business Client with the IP Phone

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 4-32: Sign-in Request Prompt**



⚠️ | **Note:** Primary Device cannot be changed in 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. See the *Release Notes*.

## 4.11.10  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.

### 4.11.10.1 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:
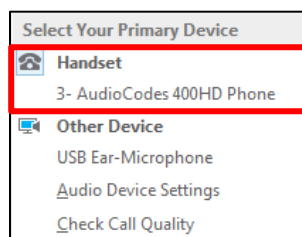
**2.** Make sure **Handset AudioCodes 400HD Phone** is selected.

---

**Note:**

- 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*.

---

## 4.11.10.2 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.

---

**Note:** The icon shown above is that displayed in the 450HD 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.

## 4.11.11 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 using the Configuration File:**

■ 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]** | ▪ **AUTOMATIC** mode<br>When the PC port of the phone is connected directly to the PC, the phone is *automatically* paired with the PC<br>-OR-<br>▪ **BOTH** mode<br>✓ 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 *manually* paired<br>-or-<br>✓ When the PC port of the phone is connected directly to the PC, the phone is *automatically* 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).

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

## 4.11.12 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 4-33: Web Interface - Configuration File**
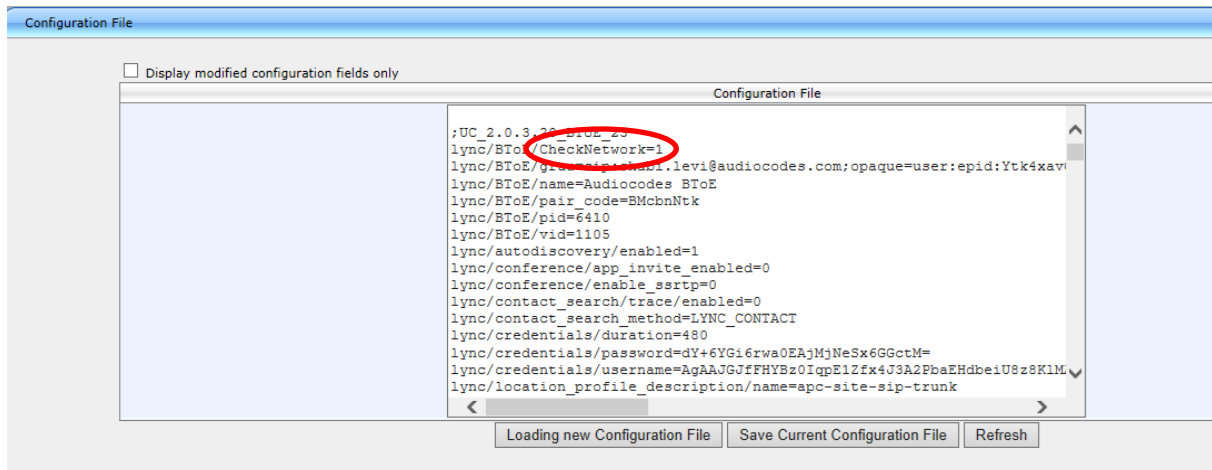


2. Locate the 'CheckNetwork' field. Make sure it is set to its default of **0**.

   **0** = pairing across different subnets enabled
   **1** = pairing across different subnets disabled

## 4.11.13 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.

## 4.12    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.*

---

**Note:**

- The Boss Admin feature applies to the 430HD, 440HD and 450HD phone models. It 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.

---

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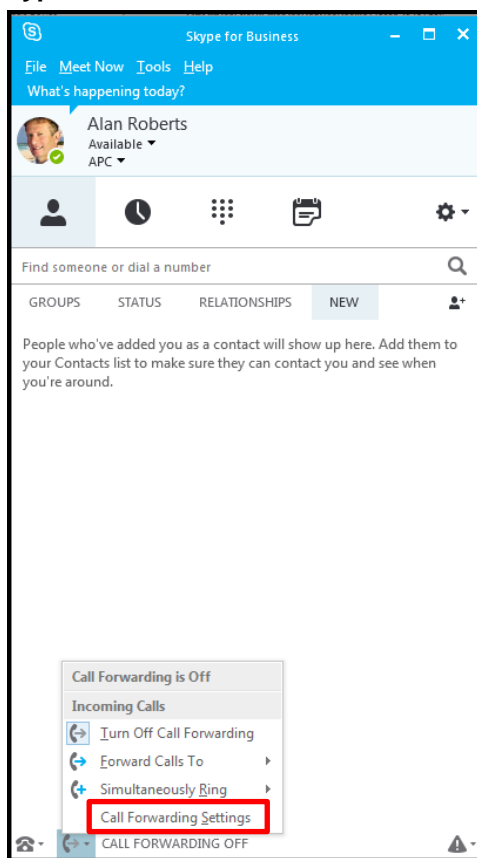
**2.** In the screen that opens, shown below, click the **Edit my delegate members** link.

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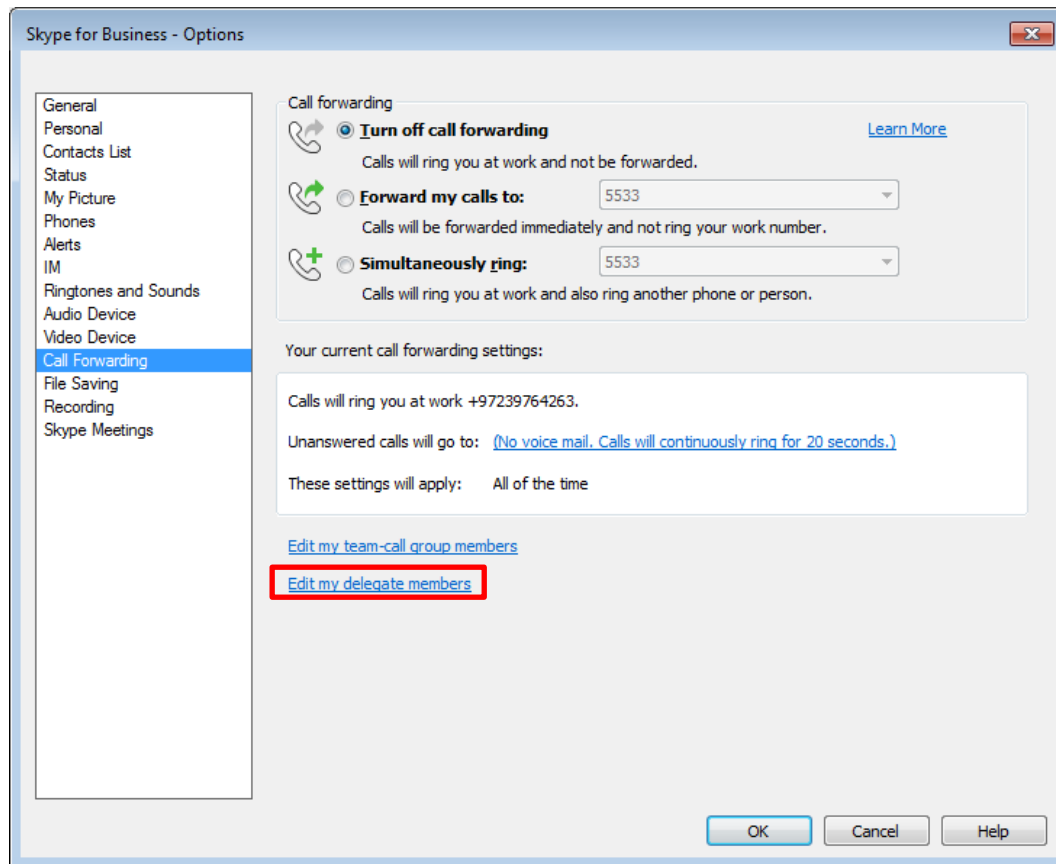


**3.** In the screen that opens, shown below, click **Add** and add a contact from the list.

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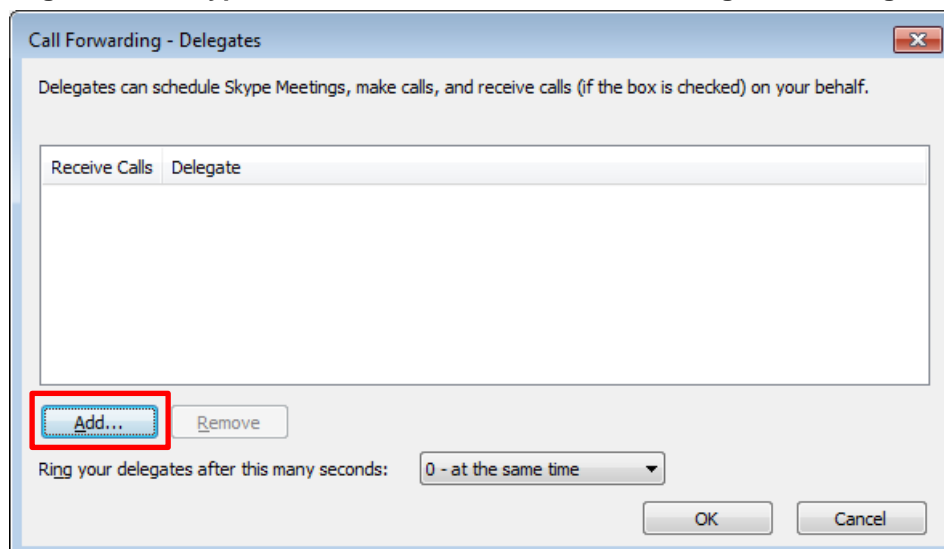


**4.** Adjacent to the added delegate in the screen that opens (Mike Dubb, shown below), make sure the **Receive Calls** option is selected:

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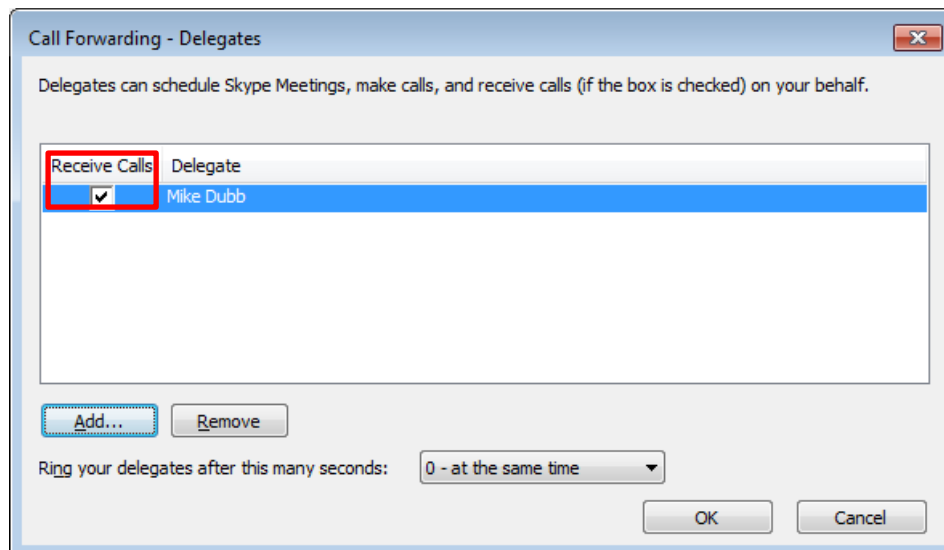


**5.** Click **OK**.

**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**
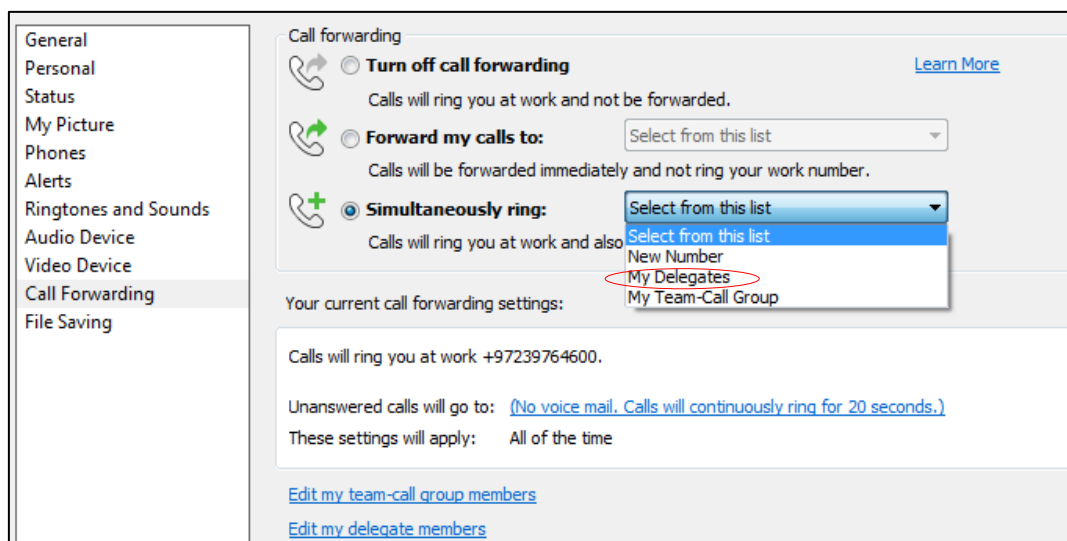


**7.** Click **OK**; you're returned to the Skype for Business client main screen.

> ⚠️ **Note:** 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.

### 4.12.1 Viewing Admin Lines on Boss's Phone

After setting up the feature, you'll view on Boss's phone (**Alan Roberts**, below) the Admin line **mike.d.** that you configured previously.
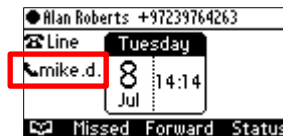


- Configure another Admin in the same way as that described previously.
- On Boss's phone, view both configured Admin lines **mike.d.** and **brad.b.**
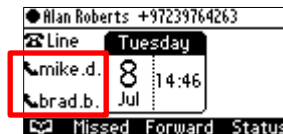


> **Note:** 440HD / 440HD phone screens are shown here. The 450HD phone screen is different in terms of size, color and presence status, but the concept is identical.

### 4.12.2 Viewing Boss's Line on Admin's Phone

- On Admin's phone (**Mike Dubb** below), you'll view Boss's line **Alan R** from whose Skype for Business client you configured the Admin:
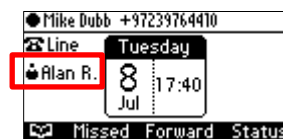


> **Note:** The 440HD / 440HD phone screen is shown here. The 450HD phone screen is different in terms of size, color and presence status, but the concept is identical.

## 4.12.3    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 using the Configuration File:**

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

**Table 4-11: Boss Privacy Mode Parameter**

| Parameter Name | Description |
|---|---|
| **[boss_privacy_enable]** | **[0] =** Admin sees a remote caller's ID when they call (Default). |
| | **[1]** = A call from a remote caller indicates 'Private Call' on the Admin's phone instead of caller ID. |
| | The Boss's phone indicates the remote side's caller ID for all calls. |

**Note:**

- 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.

## 4.13    Enabling the Delegated Line Feature

[Applies only to the 440HD phone for Lync 2013] 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.

---

**Note:**

- 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.

## 4.13.1    Configuring Boss Admin Delegated Line

### 4.13.1.1    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.

### 4.13.1.2  Configuring Boss-Admin Sidecar Functionality

> **Note:** Applies exclusively to the 440HD 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.

> **Note:** 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 13$^{th}$ call and up are unmanageable in the sidecar (no appearance, no pick up). Even if an index becomes free, the 13$^{th}$ call and up will not occupy the free index. A newly free index will be occupied by the next incoming call.

## 4.14  Configuring Phones to Operate in an OVR Deployment

Network administrators can configure phones to operate in an OVR (One Voice Resiliency) deployment, supporting dhcpoption160.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.

## 4.15 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 using the Configuration File:**

■ Use the table below as reference.

**Table 4-12: Removing Local 3-Way Conferencing Capability from Users - Parameter**

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

## 4.16 Disabling User Sign-Out on Common Area Phones

You can remove the **Sign out** softkey from phones in Common Areas (lobbies, cafeterias, lounges, meeting rooms, etc.).

> **Note:** Common Area phone menus do not display DND (Do not Disturb) and Call Forward softkeys for the same reason - to prevent users from making the phone 'unavailable'..

➢ **To remove the 'Sign out' softkey:**

■ Use the table below as reference.

**Table 4-13: Disabling Sign-Out on Common Area Phones - Parameter**

| Parameter | Description |
|---|---|
| **[voip/common_area/enhanced_mode]** | **[0]** = displays the **Sign out** softkey in the screen (default)<br>**[1]** = removes the **Sign out** softkey in the screen |

Users can, however, sign out using the Web interface. See Section 4.18.

## 4.17 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 4-14: Blocking All Users from Signing out - Parameter**

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

## 4.18    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                              :
CustomLinkInErrorMessages                      :
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
```

## 4.19 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**.

## 4.20 Enabling an IP Phone Voice Quality Check

IP phone voice quality can be tested through the phone's Device Status menu.
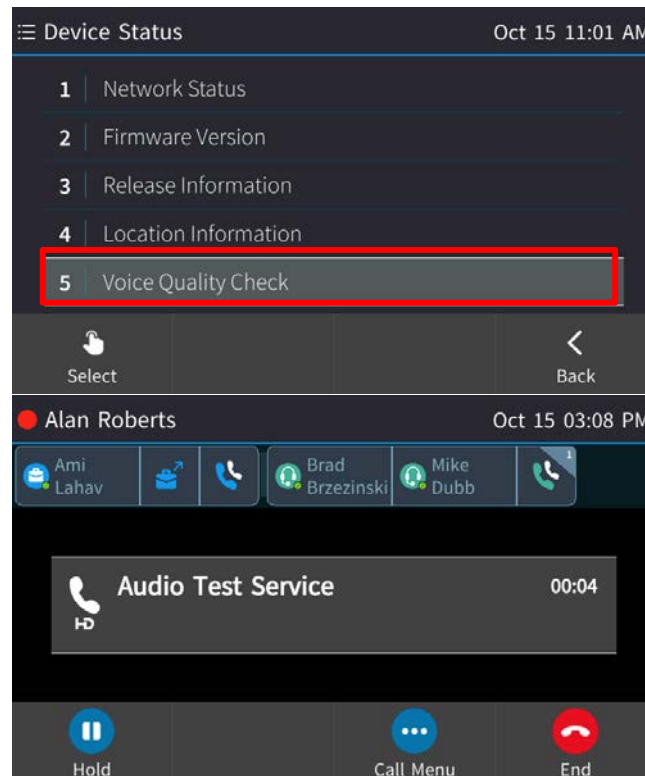


If selected, an invitation is played to "Record a short message after the tone then wait to hear how you sound". To enable the feature, the network administrator must enter the following command on the Skype for Business server:

```
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>**

# 4.21    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**
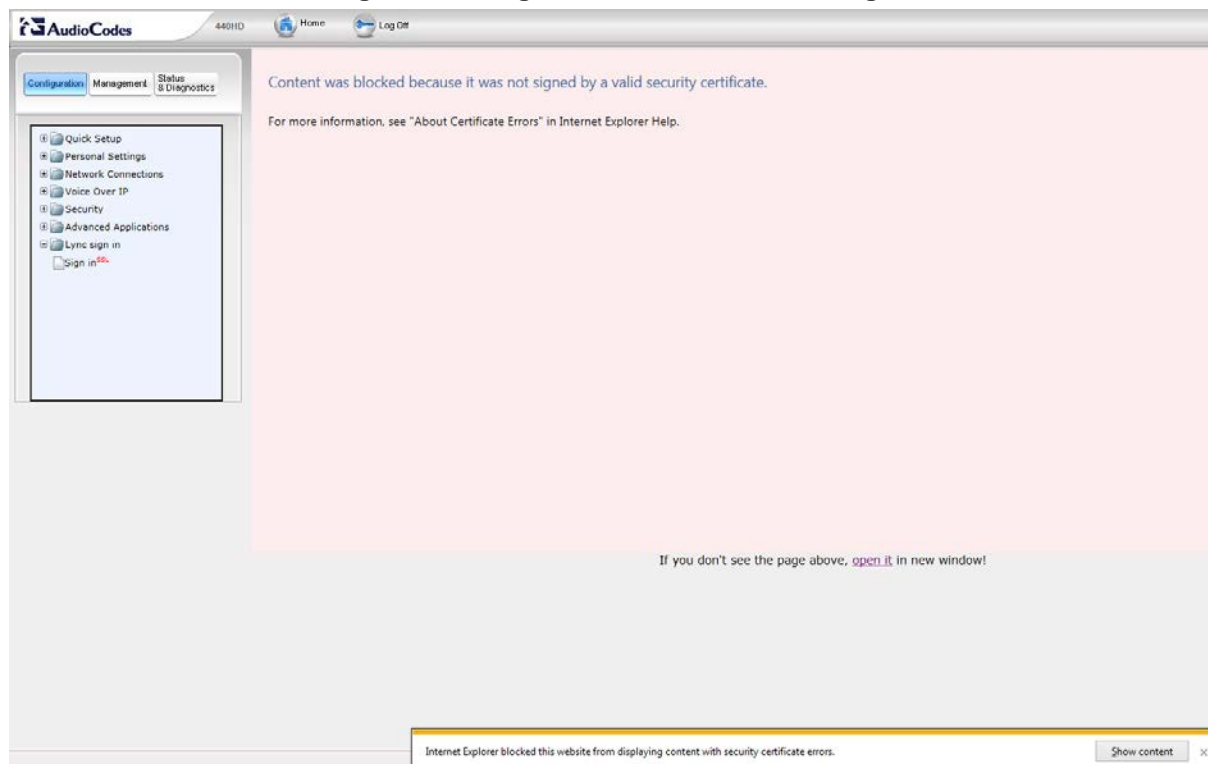


2. Click the **open it** link and then click **Show content**.

**Figure 4-40: Sign-in – Windows Security Prompt**
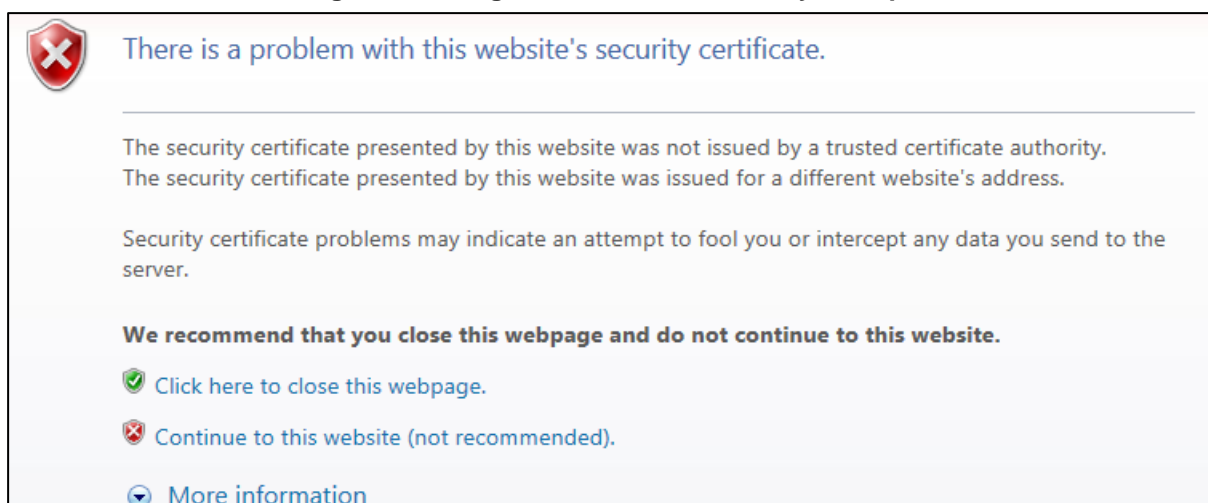


3. Click the **Continue to this website (not recommended)** link.

**Figure 4-41: Windows Security Prompt**
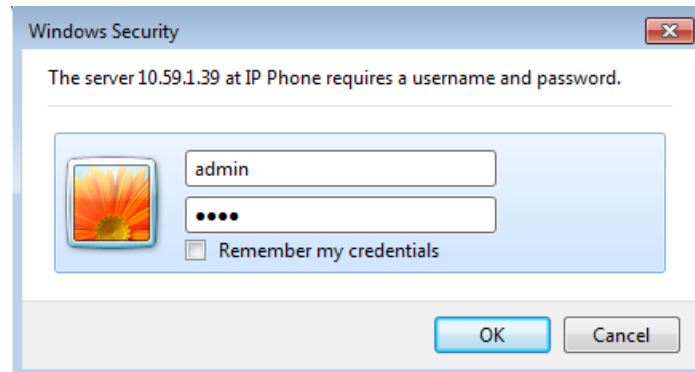


4. In the Windows Security prompt, enter the username and password and then click **OK**.

**Figure 4-42: Sign-in with PIN Code**
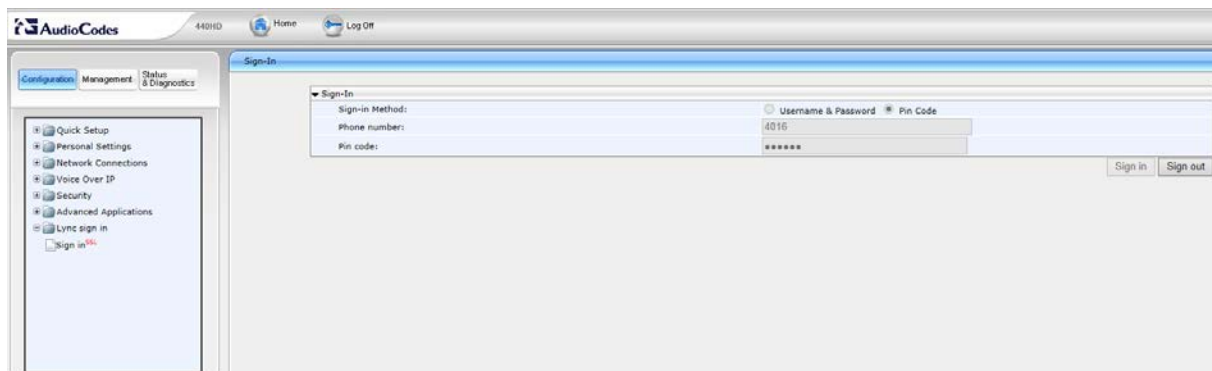


**Figure 4-43: Sign-in with Username & Password**
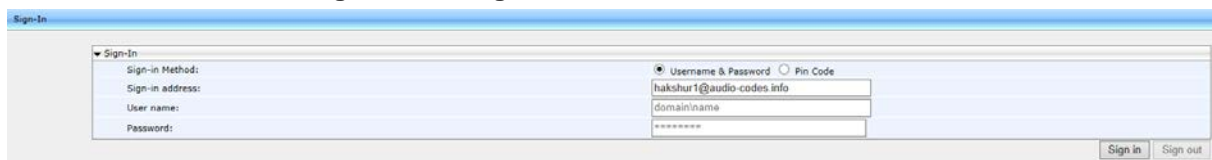


5. Select the Sign-in Method. Choose either **Username & Password** or **Pin Code**.
6. In the ' Phone Number' field, enter the number of the phone.
7. [Only applies to signing in with Username & Password] In the 'User name' field, enter the domain name and username.
8. In the 'Pin code' field, enter 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.

# 4.22 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, OAth will replace OrgID, which will deprecate. OAuth 2.0 was implemented in the phone wrapped in ADAL, as described in RFC 6749.

## 4.23 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.

## 4.24 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 the feature using the Web interface:**

1. In the Web interface, open the Media Streaming page (**Configuration** > **Voice over IP** > **Media Streaming**).

**Figure 4-44: Media Streaming - 'RTCP-XR Voice Quality Statistics Mode'**



2. From the 'RTCP-XR Voice Quality Statistics Mode' dropdown, select the option **REMOTE_AND_EVENTS** and then click **Submit**.

**Figure 4-45: Media Streaming – REMOTE_AND_EVENTS**



**Note:** To enable QoE reports, the Lync/Skype for Business server must be configured to enable QoE monitoring, as shown in the figure below.

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

**Table 4-15: 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.<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |

# 4.25 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.
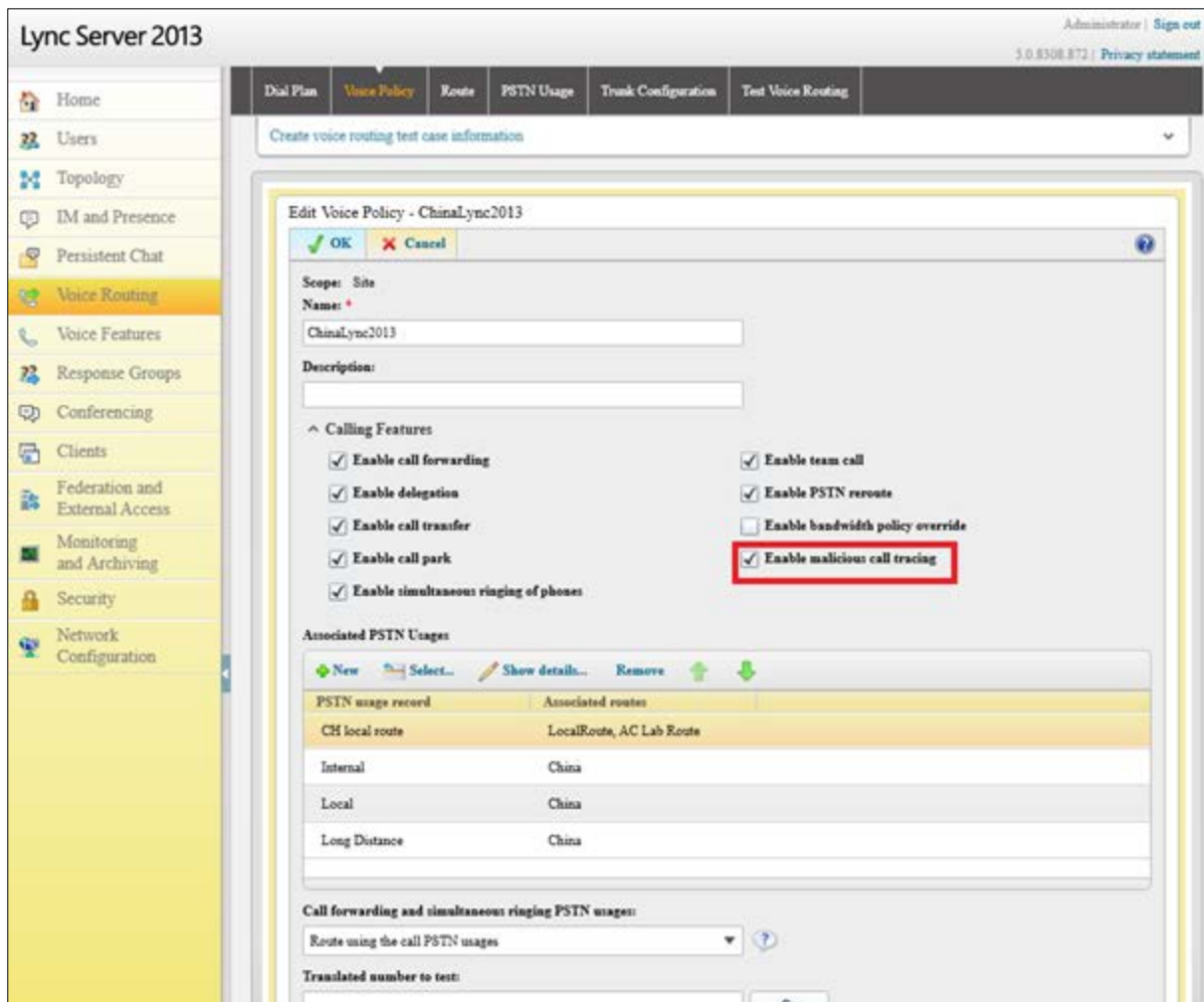


If a user gets a malicious call and wants to report it, the option allows them to send a report to the Skype for Business server (see the *User's Manual* for more information).

# 5    Maintenance

This section shows how to upgrade the phone firmware, perform administration tasks, and enable remote management.

- See under Section 4.8 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 5.2 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 5.3 for information on how to enable automatically checking for firmware updates using the Configuration File.
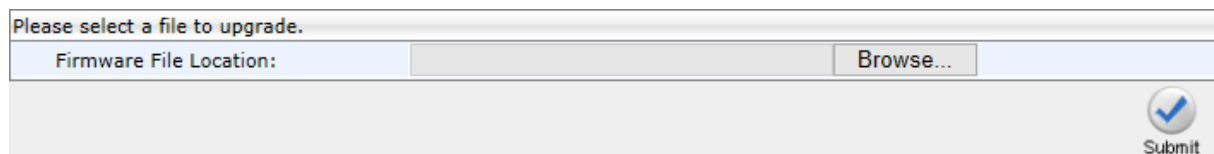
## 5.1    Upgrading Phone Firmware

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**



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    Manually Checking Phone Firmware vs Firmware on Provisioning Server

You can use the phone's Web interface to manually check if the firmware on the phone is different to the firmware file located on the provisioning server.

- If you're using the 'DHCP Options (Dynamic URL)' provisioning method to provision the phone, the firmware file on your provisioning server is checked.
- If you're using the 'Static URL' provisioning method to provision the phone, the phone's static internal firmware version is compared to the firmware on your HTTP, HTTPS, FTP or TFTP server located on a static URL provided by you, e.g., AudioCodes' IP Phone Management Server.
- If you're using the Microsoft Skype for Business server as your provisioning server, see under Section 4.8 for detailed information.

➢ **To manually check if the firmware on the phone is different to the firmware file located on the server:**

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

**Figure 5-2: Web Interface – Check Now**



2. Click the **Check Now** button; the figure below shows an example of the resulting prompt:

**Figure 5-3: Web Interface – Check Now**
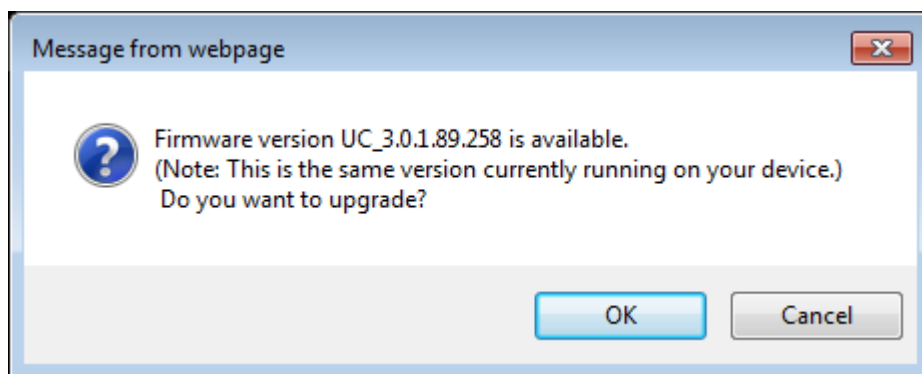
## 5.3    Enabling/Disabling Device Update

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 using the Configuration File:**

- 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:<br>• **[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).<br>• **[1]** The phone will get firmware updates from the device update service if the in-band provisioning parameters enable the feature. |

## 5.4 Administration

### 5.4.1 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.

➢ **To change the login username and password using the Web interface:**

1. Open the Users page (**Management** tab > **Administration** menu > **Users**).

**Figure 5-4: Web Interface – Users**



2. In the 'Username' field, enter a user name. Use the table below as reference.
3. In the 'Password' field, enter a new password, and then in the 'Confirm Password' field, re-enter this new password. Use the table below as reference.

> **Note:**
> - For the Administrator account, the default 'Username' and 'Password' is **admin** and **1234** respectively.
> - For the User account, the default 'Username' and 'Password' is **user** and **1234** respectively.

4. Click **Submit**; a confirmation box appears.
5. Click **OK**.

➢ **To change the login username and password using the Configuration File:**

- 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. `system/user_name=admin`). | |
| Username **[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. |
| Password **[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 3.4 on page 111. **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. |

## 5.4.2    Restoring Defaults

See Section 8.7.1.2 on page 209, under General Corrective Actions.

## 5.4.3    Restarting the Phone

See Section 8.7.4.2 on page 211, under General Corrective Actions.

## 5.5 Enabling Remote Management

### 5.5.1 Enabling Telnet Access

Telnet access can be enabled using the Web interface or the Configuration File.

> ⚠️ **Note:** Opening a Telnet connection in an external network is strongly inadvisable due to the widely recognized vulnerability of the protocol.

➢ **To enable Telnet using the Web interface:**

1. Open the Telnet page (**Management** tab > **Remote Management** menu > **Telnet**).

**Figure 5-5: Web Interface - Telnet**

2. Enable Telnet according to the parameter in the table below, and then click **Submit**.

➢ **To configure Telnet using the Configuration File:**

1. Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**).
2. Configure the parameter using the table below 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. `management/telnet/enabled=0`). | |
| Activate<br>**[management/telnet/enabled]** | Enables telnet access to the phone.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>The user name and password for telnet access are according to the parameters: **system/user_name** and **system/password**. |

# 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 Network Status page (**Status & Diagnostics** tab > **System Status** menu > **VoIP 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 Network Status page (**Status & Diagnostics** tab > **System Status** menu > **VoIP 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 Network Status page (**Status & Diagnostics** tab > **System Status** menu > **VoIP Status**).

**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 calls history:**

**1.**    Open the Call History page (**Status & Diagnostics** tab > **History** > **Call History**).

**Figure 6-7: Web Interface - Call History**

| No. | Name | Number | | Time | Delete |
|---|---|---|---|---|---|
| 1 | 420HD | 1000 | Dial | 06/01/2000 Thursday 21:21:31 | ☐ |
| 2 | 420HD | 1000 | Dial | 06/01/2000 Thursday 21:17:38 | ☐ |
| 3 | Alan_2 | 2000 | Dial | 06/01/2000 Thursday 21:14:26 | ☐ |
| 4 | 420HD | 1000 | Dial | 06/01/2000 Thursday 19:24:49 | ☐ |
| 5 | 420HD | 1000 | Dial | 06/01/2000 Thursday 19:13:29 | ☐ |
| 6 | Alan_2 | 2000 | Dial | 06/01/2000 Thursday 19:13:22 | ☐ |

**2.**    From the 'Type' drop-down list, select the type of call history (i.e., missed calls, received calls, and dialed numbers) that you want to view; the table lists the call history according to the chosen call history type.

**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 Web interface or from the phone's screen.

### 6.4.1 Viewing from the Web Interface

➢ **To view the phone's model and firmware version from the Web interface:**

■ Open the phone's Web interface; the System Information page opens by default:

**Figure 6-8: Web Interface - System Information**

| System Information | |
|---|---|
| Model Name | 405 |
| Firmware Version | UC_3.0.0.63 |
| Release Date | 2016-04-04_16:41:48 |

To access the page from another page in the Web interface:
**Status & Diagnostics** tab > **System Information** menu > **General**

### 6.4.2 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**).

### 6.4.3 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 6-9: Web Interface - System Information - Release Information**

| Release Information | |
|---|---|
| BLVERSION | 1.0.32 |
| BUILD_TIME | 2017-03-14_09:13:47 |
| DSPFWVERSION | 494E002ce2.720.28 |
| HW_TYPE | 450HD |
| LOG | 0 |
| SWVERSION | UC_3.0.1.89.278 |
| 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: **Network**, **Console** or **Both**. The feature can be configured using the Web interface or Configuration File.

➢    **To configure system logging using the Web interface:**

   **1.**    Open the System Logging page (**Status & Diagnostics** tab > **Diagnostics** menu > **Logging**).

**Figure 7-1: Web Interface - System Logging**



   **2.**    Configure the parameters using Table 7-1 on the next page as reference, and then click **Submit**.

➢ **To configure system logging using the Configuration File:**

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

> **Note:** 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 |
|---|---|
| Activate<br>**[system/syslog/mode]** | Defines the System Logging feature's log level. Possible values are:<br>• **Disable** = No Syslog, i.e., the phone's flash memory (default).<br>• **Network** = a.k.a. Syslog server. Basic debug level.<br>• **Console** = a.k.a. Serial. You'll need to connect a serial cable to view the logs, which causes delays in the phone's operation. Intended for developers; requires a unique firmware version.<br>• **Both** = Syslog is sent to the Syslog server *and* the phone console (Network *and* Console). |
| Server IP Address or Host Name<br>**[system/syslog/server_address]** | Only displayed when 'Activate' is **Network** or **Both**. 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**. |
| Server Port<br>**[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.<br>**Note:** This parameter is applicable when Log Destination (see above) is set to **Network** or **Both**. |
| VoIP Application<br>**[system/syslog/component/voip_application]** | Defines the log module which generates Syslog messages related to the multi-layer VoIP application. Default: None |
| SIP Call Control<br>**[system/syslog/component/sip_call_control]** | Defines the log module which generates Syslog messages related to MTR layer. Default: None |
| SIP Stack<br>**[system/syslog/component/sip_stack]** | Defines the log module which generates Syslog messages related to the SIP Stack. Default: None |
| ICE Stack<br>**[system/syslog/component/ice_stack]** | Defines the log module which generates Syslog messages related to ICE (Interactive Connectivity Establishment). Default: None |
| Control Center<br>**[system/syslog/component/control_center]** | Defines the log module which generates Syslog messages related to networking. Default: None |

| Parameter | Description |
|---|---|
| LCD Display<br>**[system/syslog/component/lcd_display]** | Defines the log module which generates Syslog messages related to the phone screen display.<br>Default: Debug |
| Web<br>**[system/syslog/component/web_server]** | Defines the log module which generates Syslog messages related to the phone's Web server.<br>Default: None |
| Watchdog<br>**[system/syslog/component/watchdog]** | Defines the log module which generates Watchdog-related Syslog messages. Watchdog is responsible for keeping other processes running. Default: None |
| 802.1X<br>**[system/syslog/component/ieee802_1x]** | Defines the log module which generates Syslog messages related to the security protocol.<br>Default: None |
| Kernel<br>**[system/syslog/component/kernel]** | Defines the log module which generates Syslog messages related to the operating system core. |
| DSP<br>**[system/syslog/component/dsp]** | Defines the log module which generates Syslog messages related to the phone's DSP (voice engine) commands. |
| lib<br>**[system/syslog/component/lib]** | Defines the log module which generates Syslog messages related to the internal library of the IP phone. |
| SIPE<br>**[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. The parameter is displayed only when 'Activate' is set to **Network** or **Console** (see above). May help with the investigation of cases related to Exchange integration. See also Section 7.1.2 below. |
| **[system/syslog/component/cgi]** | Defines the log module which generates Syslog messages related to the services for the Web server. |

## 7.1.2 Configuring SIPE using the Configuration File

This section shows how to configure parameters related to the SIPE Project's third-party Pidgin plugin for Microsoft Skype for Business client. The parameters are relevant only when 'Log Destination' is Network / Serial (see above). The logging level may help with the investigation of cases related to Exchange integration.

➢ **To configure SIPE using the Configuration File:**

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

**Table 7-2: SIPE Parameters**

| Parameter | Description |
| --- | --- |
| **[lync/sipe/read_timeout]** | Defines the idle time allowed during a SIPE read operation, in seconds. Default: 90 seconds. |
| **[lync/sipe/write_timeout]** | Defines the idle time allowed during a SIPE write operation, in seconds. Default: 90 seconds. |
| **[lync/sipe/connect_timeout]** | Defines the idle time allowed during a SIPE connect operation, in seconds. Default: 90 seconds. |

## 7.1.3 Analyzing and Debugging Traffic using 'Lightweight Syslog'

A 'Lightweight Syslog' logging mechanism allows you to perform phone logging without affecting phone performance.

➢ **To enable the Lightweight Syslog:**

■ In the Web interface, open the phone's System Logging page (**Status & Diagnostics** tab > **Diagnostics** > **Logging**), set the 'Activate' parameter to **Network** and provide a valid IP address and server port. Do not set any of the options (keep all as **None**).

# 7.2    Monitoring: Pinging & Traceroute

This section shows how to perform pinging and traceroute using the Web interface.

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 monitoring using the Web interface:**

1.    Open the Monitoring page (**Status & Diagnostics** tab > **Diagnostics** menu > **Monitoring**).

**Figure 7-2: Web Interface - Monitoring**

| Ping (ICMP Echo) | | |
|---|---|---|
| Destination: | | Go |
| Number of pings: | 4 | |

| Traceroute | | |
|---|---|---|
| Destination: | | Go |

2.    In the 'Destination' field, enter the IP of the device on the remote side to ping.

3.    In the 'Number of pings' field, configure how many pings you want to send. You can configure multiple pings for (for example) constant communication tests.

4.    Click **Go** to perform these diagnostics.

## 7.3 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 Web interface or Configuration File.

➢ **To enable recording to debug voice, using the Web interface:**

**1.** Open the Recording page (**Status & Diagnostics** tab > **Diagnostics** menu > **Recording**).

**Figure 7-3: Web Interface - Recording**



**2.** Configure the parameters using the table below as reference and click **Submit**.

➢ **To enable recording to debug voice, using 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 7-3: Packet Recording Parameters**

| Parameter | Description |
|---|---|
| Remote IP Address or Host Name<br>**[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).<br>The default value is 0.0.0.0. |
| Remote Port<br>**[voip/packet_recording/remote_port]** | Defines the UDP port of the remote computer to which the recorded packets are sent.<br>The valid range is 1024 to 65535. The default value is 50000. |
| Enable DSP Recording<br>**[voip/packet_recording/enabled]** | Activates the packet recording mechanism.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable<br>**Note:** DSP packet recording can be enabled on the fly, without requiring the network administrator to reset the phone. |

| Parameter | Description |
|---|---|
| Enable RTP Recording<br>**[voip/packet_recording/rtp_recording/enabled]** | Only displayed in the Web interface if 'Enable DSP Recording' is enabled. Enables RTP recording.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |
| Enable EC Debug Recording<br>**[voip/packet_recording/ec_debug_recording/enabled]** | Activates the Echo Canceller Debug recording.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |
| Enable Noise Reduction Debug Recording<br>**[voip/packet_recording/noise_reduction_recording/enabled]** | Traffic on the network stops when the MUTE key is activated.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |
| Enable Network Recording<br>**[voip/packet_recording/network_recording/enabled]** | Activates the DSP network (TDM Out) recording.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |
| Enable TDM Recording<br>**[voip/packet_recording/tdm_recording/enabled]** | Activates the DSP TDM (TDM In) recording.<br>▪ **[0]** Disable (default)<br>▪ **[1]** Enable |

## 7.4    Creating a Crash Dump File

This section shows how to create a crash dump file using the Web interface. Crash dump copies historical processes to a file. You can create the file at the time the problem occurs. You can use the file to debug the problem.

➢ **To create a crash dump file using the Web interface:**

1.    Open the Crash Dump page (**Status & Diagnostics** tab > **Diagnostics** menu > **Crash Dump**).

**Figure 7-4: Web Interface - Crash Dump**
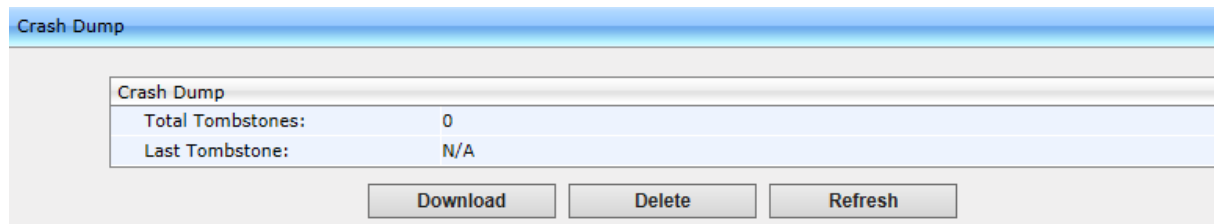


**Table 7-4: Crash Dump Parameters**

| 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.

## 7.5    Enabling Tracing

For effective troubleshooting and diagnosis it's recommended to set up the phone to store trace messages. See also Section 2.5.2 on page 44.

> **Note:** During regular phone operation, it is recommended to *disable* debug tracing for improved performance.

> ➢  **To enable tracing:**

1.  Log in to the Web management tool of the IP Phone, using HTTPS (e.g., https://172.17.0.103) through your Web browser. The phone's IP address can be obtained from the DHCP server, or from the phone's screen (press the MENU button > press **5** for the **Status** menu > press the OK button for the **Network Status** menu > press the OK button > press the Navigation key to scroll down to the IP address).

2.  Open the Tracing page (**Status & Diagnostics** tab > **Diagnostics** menu > **Tracing**).

3.  Set the 'Max File Size' field to **1024**.

4.  Set the 'Trace Level' field to **Debug** to activate tracing to debug level.

5.  Click **Submit**.

6.  Click **Clean log**, and then power up the phone.

7.  After the phone completes the power-up process, click **Save log**.

8.  Send the saved logged trace to AudioCodes Customer Technical Support for troubleshooting.

**Figure 7-5: Configuring Tracing**

## 7.6    Configuring Port Mirroring

Port mirroring facilitates network traffic monitoring enabling administrators to analyze and debug data or diagnose errors on a network, manage network performance and be alerted to problems. Inbound or outbound traffic (or both) can be mirrored on single or multiple interfaces. Port mirroring can be activated using the Web interface or Configuration File.

➢ **To configure port mirroring using the Web interface:**

1.  Open the Recording page (**Configuration** tab > **Network Connections** menu > **Network Settings**).

**Figure 7-6: Web Interface - Port Mirroring**

2.  Configure using the table below as reference and click **Submit**.

➢ **To configure port mirroring using the Configuration File:**

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

**Table 7-5: Port Mirroring Parameters**

| Parameter | Description |
|---|---|
| Activate<br>**[network/pc_port_mirroring/enabled]** | Enables port mirroring.<br>▪ **[0]** Disable (default) **-** The LAN/PC Network interfaces operate in SWITCH mode.<br>▪ **[1]** Enable **-** The LAN/PC Network interfaces operate in HUB mode. The network traffic on the LAN port is reflected in the PC port. |

## 7.7    Configuring Core Dump

The phone performs core dump to facilitate 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.

➢ **To configure core dump using the Web interface:**

1.  Open the Core Dump page (**Status & Diagnostics** > **Diagnostics** > **Core Dump**).

**Figure 7-7: Web Interface – Core Dump**

2. From the Core Dump dropdown, select **Enable** (default) if it isn't already, and then click **Submit**.

➢ **To configure core dump using the Configuration File:**

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

**Table 7-6: Core Dump Parameter**

| Parameter | Description |
|-----------|-------------|
| **[kernel/cfg/enable_core_dump]** | Enables core dump.<br>▪ **[0]** Disable<br>▪ **[1]** Enable (default) |
| **[system/watchdog/CoreDump_Handling_Enabled]** | Core dump files are compressed under /tmp directory and backed up on the flash under /phone/etc/core. The feature can be enabled/disabled.<br>▪ **[0]** Archive core does not dump files<br>▪ **[1]** Archive core dumps files (default) |
| **[system/watchdog/max_core_dump_on_flash]** | Defines the number of the latest core dump files to be saved on flash. You should limit the number of the first compressed core dump on the flash under /phone/etc/core. The limit is per process. Valid values: 0-5. Default for 440HD / 430HD phones: 2 per process. Default value for the 420HD phone: 0 per process.<br>If exceeded, the new core will not be copied to the flash.<br>If 0, the core dump will be compressed but will not copy to the flash. |

## 7.7.1 Downloading Core Dump

If a phone issue is encountered (for example, it crashes or is terminated abnormally), you can download the core dump in order to examine the issue and resolve it.

➢ **To download the core dump:**

■ In the Core Dump page shown in Figure 7-7, open the 'Download Core Dump' dropdown and select the dump to analyze.

## 7.7.2 Downloading Core Dump Archive

You can download the core dump archive in order to examine dumps of previously encountered issues that may help resolve the current issue.

➢ **To download the core dump archive:**

■ In the Core Dump page shown in Figure 7-7, open the 'Download Core Dump Archive' dropdown and select the archived dump to analyze.

This page is intentionally left blank.

# 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** | |

1   Make sure you correctly entered the sign-in address, username, and password.
2   Make sure you have the correct username/password; it may have changed in the Enterprise's Active Directory.
3   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** | |

1   Make sure you entered the phone number / PIN code correctly.
2   Make sure you have the correct PIN code; it may have changed in the Enterprise's Active Directory.
3   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** | |

Make sure:
1   DHCP Option 43 has been configured.
2   Access is possible from the following Web site:
    https://YOUR_AUTHORITY_SERVER:443/CertProv/CertProvisioningService.svc
3   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 420HD IP Phone.

# 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.

> **Note:** 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' 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**

| Restore Defaults | |
|---|---|
| Restore to Factory Defaults | Submit |

**2.** Click **Submit**:

**Figure 8-2: Confirm Restore to Factory Defaults**

Message from webpage

Are you sure you want to restore to default values?

OK        Cancel
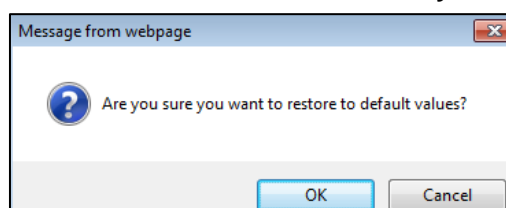
**3.** Click **OK**.

## 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**
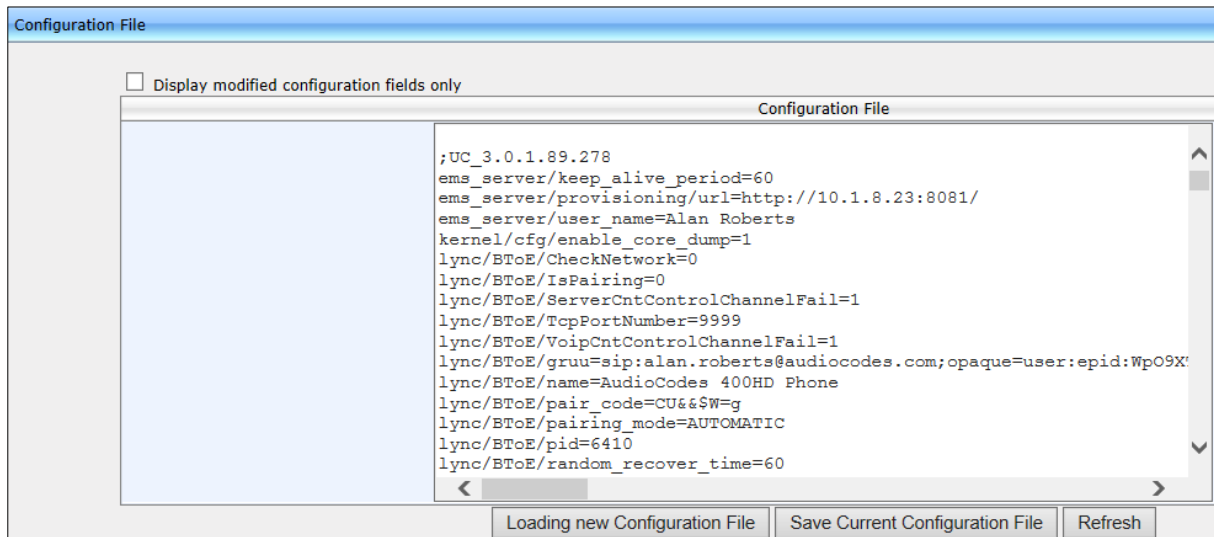


The configuration you created is displayed in the text pane.

2. Click **Loading new Configuration File**:

**Figure 8-4: Web Interface - Load New Configuration File**
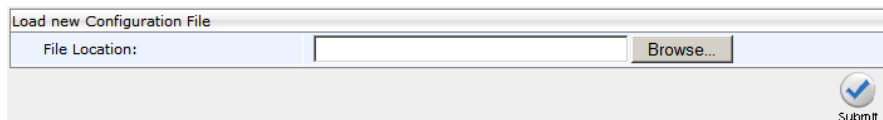


3. Click **Browse** and select the cfg file you created; the phone verifies it's related to the phone model. The cfg is then loaded to the phone. Once loaded, the phone reboots (indicated on the screen); the phone is now loaded with the cfg file you created.

## 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.

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., 420HD_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:

<div align="center">

**Warning: Restart the phone?**

</div>

**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:**

**1.** Open the Restart System page (**Management** tab > **Administration** menu > **Restart System**).

<div align="center">

**Figure 8-5: Web Interface - Restart System**

</div>



**2.** Click **Restart**; you're prompted to confirm.

<div align="center">

**Figure 8-6: Confirmation Prompt**

</div>
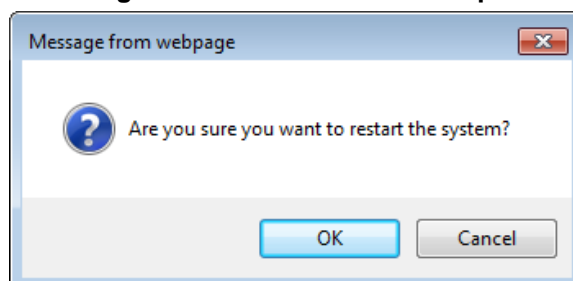


**3.** Click **OK**.

This page is intentionally left blank.

# A    Alternative Automatic Provisioning Methods

## A.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/420HD/420HD.img**

■    The phone tries to obtain the following configuration file:
**tftp://ProvisioningServer/420HD/<MAC address>.cfg**

   (e.g. tftp://ProvisioningServer/420HD/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.

---

**Note:** 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 using the Web interface:**

**1.**    Open the Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

**Figure A-1: Web Interface - Static DNS Record**

| | |
|---|---|
| Firmware Version : | UC_3.0.0.82 |
| Provisioning Method : | Static URL |
| Firmware URL : | Check Now |
| Configuration URL : | Check Now |
| Check Period : | Daily |
| Every day at : | 00:00 |
| Random Provisioning Time : | 120    minutes |

**2.**    Configure using the table below as reference and click **Submit**.

➢ **To configure Static DNS Record using 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 A-1: Static DNS Record Parameters**

| Parameter | Description |
|---|---|
| Firmware URL<br>**[provisioning/firmware/url]** | The static URL for checking the firmware file. The URL must be entered using one of the following syntax options:<br>▪ <protocol>://<server IP address or host name><br>▪ <protocol>://<server IP address or host name>/<firmware file name><br>Where <protocol> can be one of the following protocols: "ftp", "tftp", "http" or "https". For example:<br>▪ tftp://192.168.2.1 – retrieved firmware file is 420HD.img<br>▪ ftp://192.168.2.1/Different_Firmware_Name.img - retrieved firmware file is Different_Firmware_Name.img<br>**Note:** This parameter is applicable only when **method** is configured to "Static". |
| Configuration URL<br>**[provisioning/configuration/url]** | The static URL for checking the configuration file. The URL must be entered using one of the following syntax options:<br>▪ <protocol>://<server IP address or host name><br>▪ <protocol>://<server IP address or host name>/<configuration file name><br>Where <protocol> can be "ftp", "tftp", "http" or "https" and where <configuration file name> can be either:<br>▪ A unique configuration file, per phone, for example: <MAC>.cfg<br>-or-<br>▪ A global configuration file, per deployment, for example, 420HD.cfg<br>Unique Configuration Example<br>**http://192.168.2.1/different.img;<MAC>.cfg**<br>The retrieved firmware file is *different.img* and the configuration file name is *<MAC>.cfg* such as *001122334455.cfg*<br>Global Configuration Example<br>**http://192.168.2.1/<420HD>.cfg**<br>The configuration file name is *420HD.cfg*<br>**Note:** This parameter is applicable only when 'Method' is configured to **Static**. |

## A.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.

> **Note:** 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-2: HTTPS Redirect Server Directing Phones to Provisioning Server**
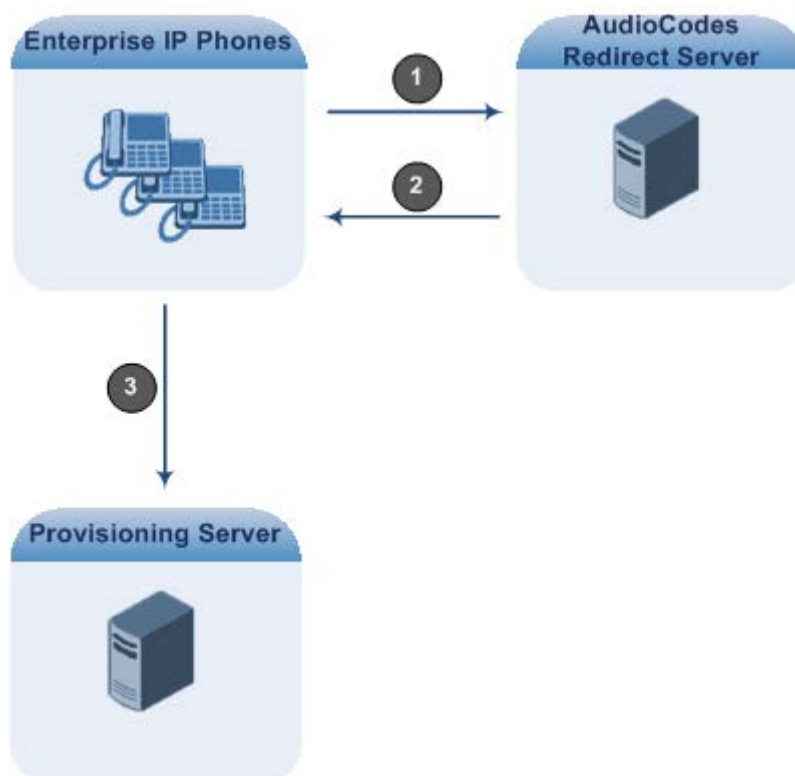
### A.2.1.1 Redirection Process

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.

> **Note:** The phone repeats the redirect process whenever reset to factory defaults.

# B        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)

## B.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.

## B.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**

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**
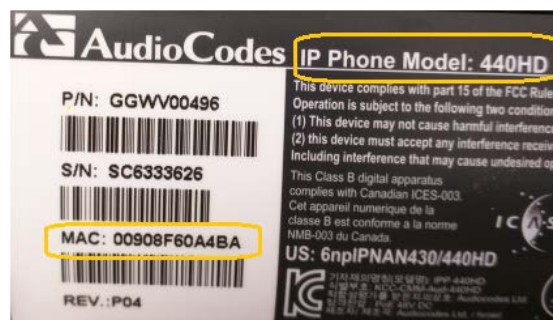


## B.3 Recovering the Phone

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**
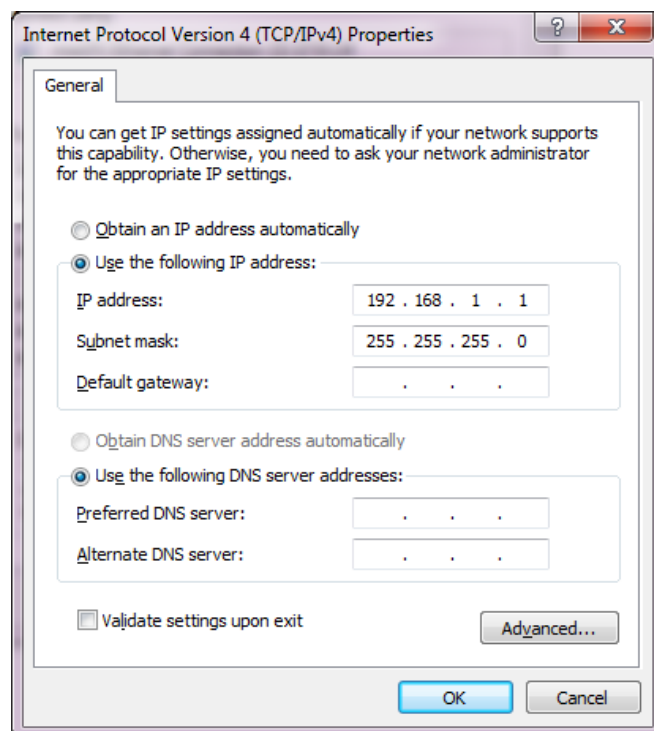


4. Download the following **tftpd64** freeware tool:
   http://tftpd32.jounin.net/tftpd32_download.html

5. Run the **tftpd64.exe** executable.

6. Click **Settings** and configure the following settings:

**Table B-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 |
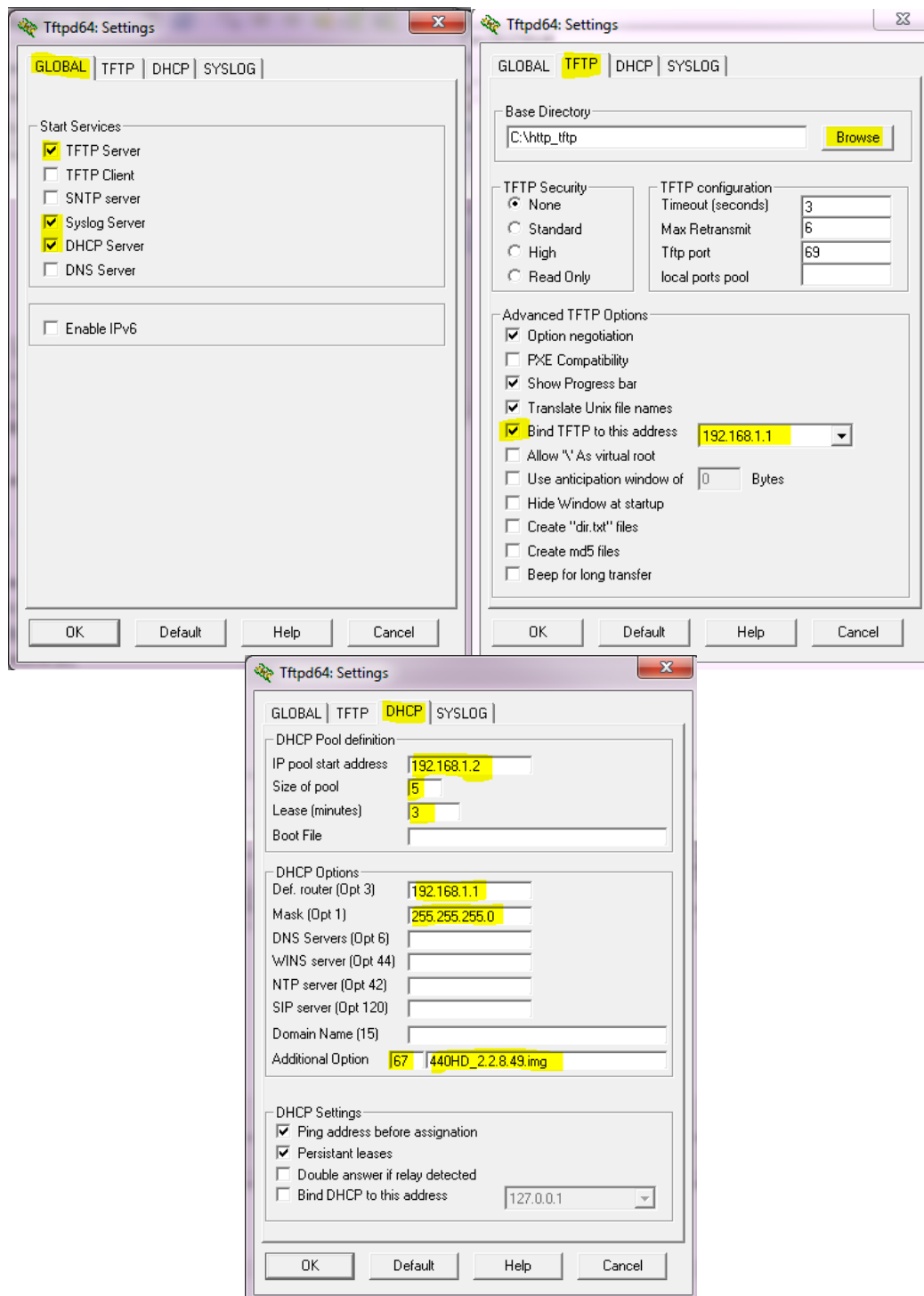
7.  For **tftps64** to accept the new settings, close and open **tftpd64**.

    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.

# B.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

## B.4.1    Making Sure Using Wireshark

**1.** In Wireshark, make sure the four DHCP 'DORA' (**D**iscover; **O**ffer; **R**equest; **A**CK) steps are accomplished, as shown in the figure below.

**Figure B-5: Make Sure with Wireshark that the Phone is Downloading Phone .img File**
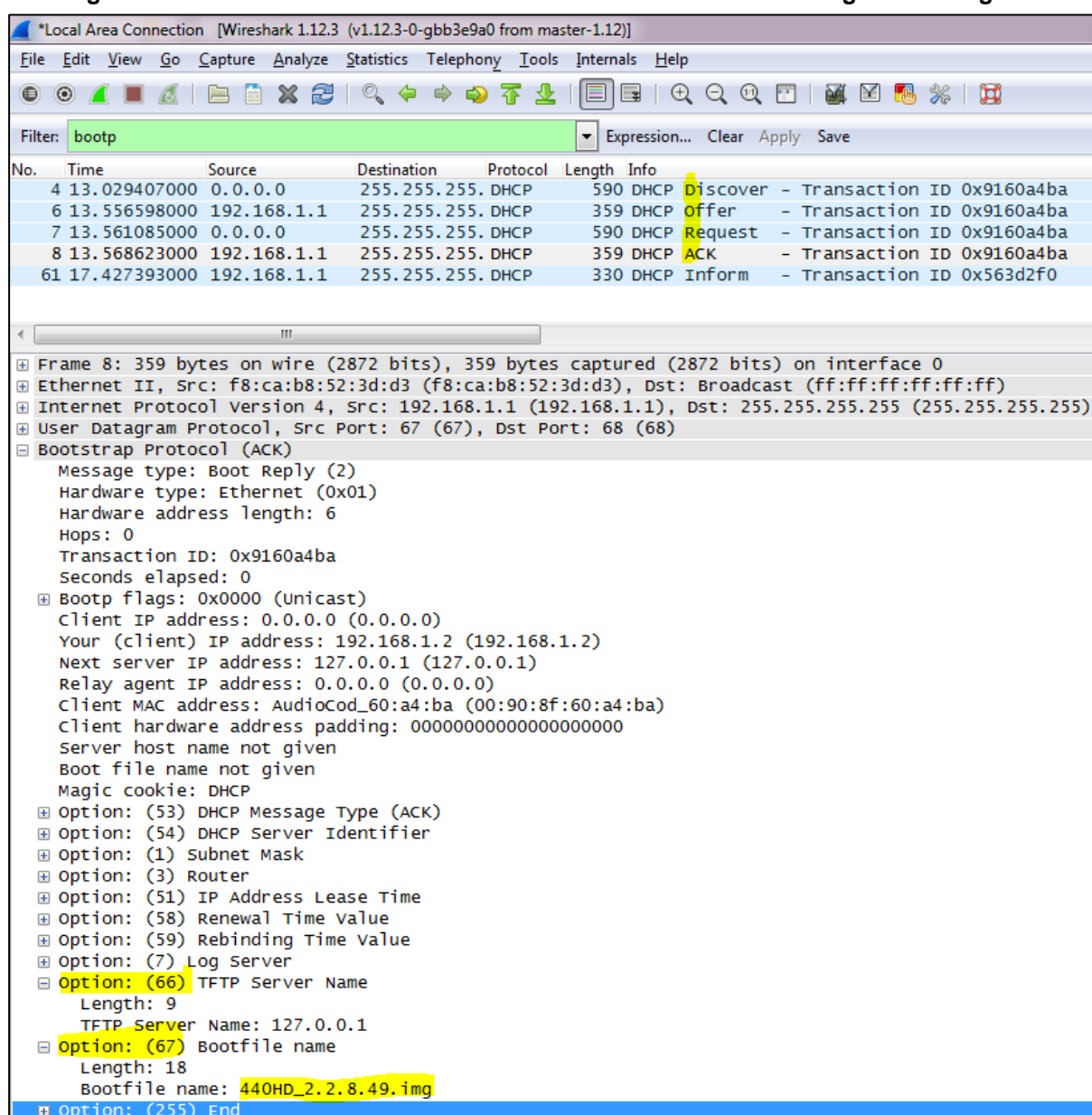
**2.** Filter by **TFTP**, as shown in the figure below.

**Figure B-6: Verifying .img File Download with Wireshark – Filtering by TFTP**
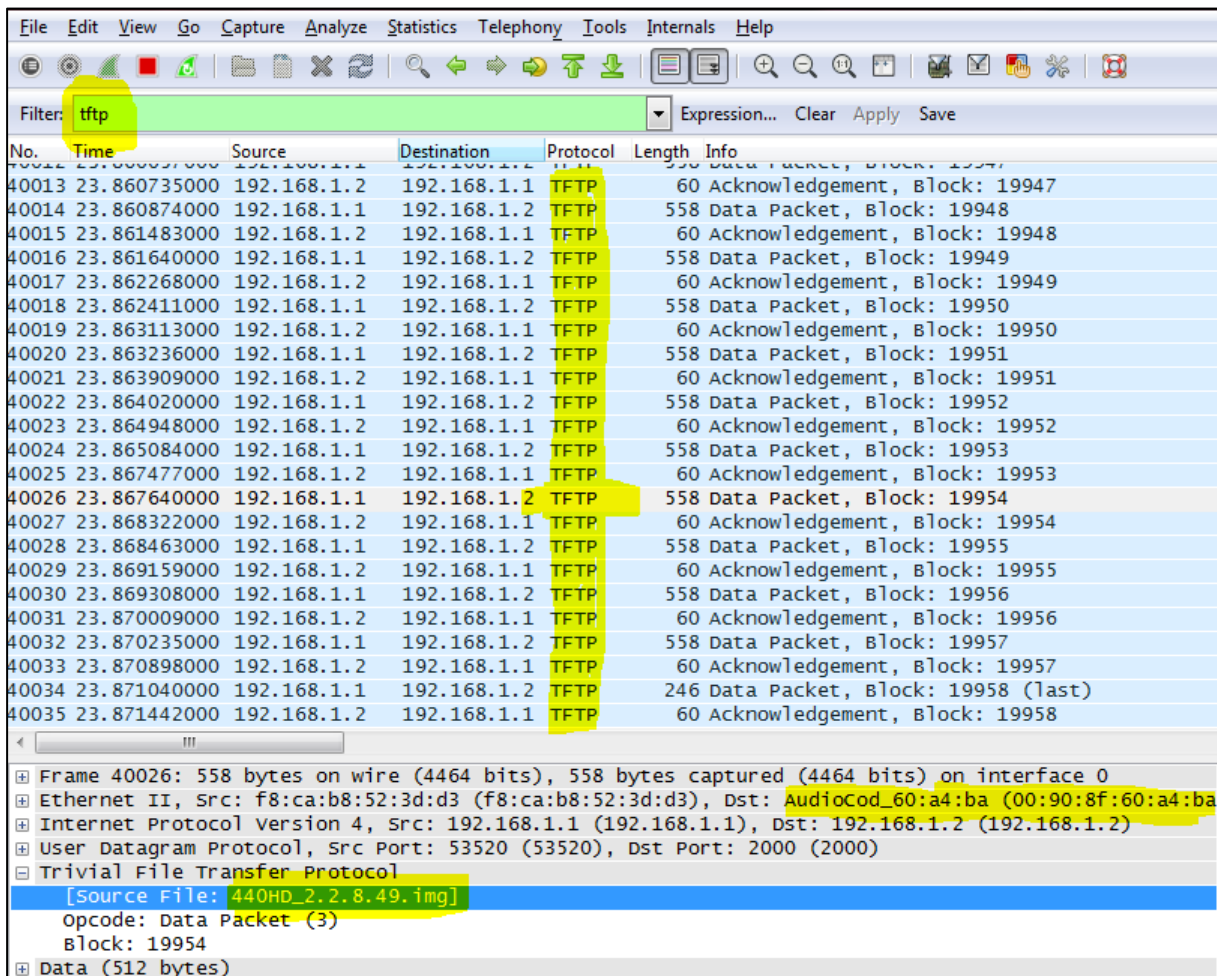


## B.4.2   Making Sure Using tftpd64

In **tftpd64**, view the indications shown in the figures below.

**Figure B-7: Verifying .img File Download using tftpd64**
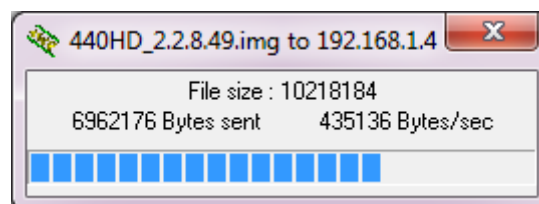
**Figure B-8: Verifying .img File Download using tftpd64**
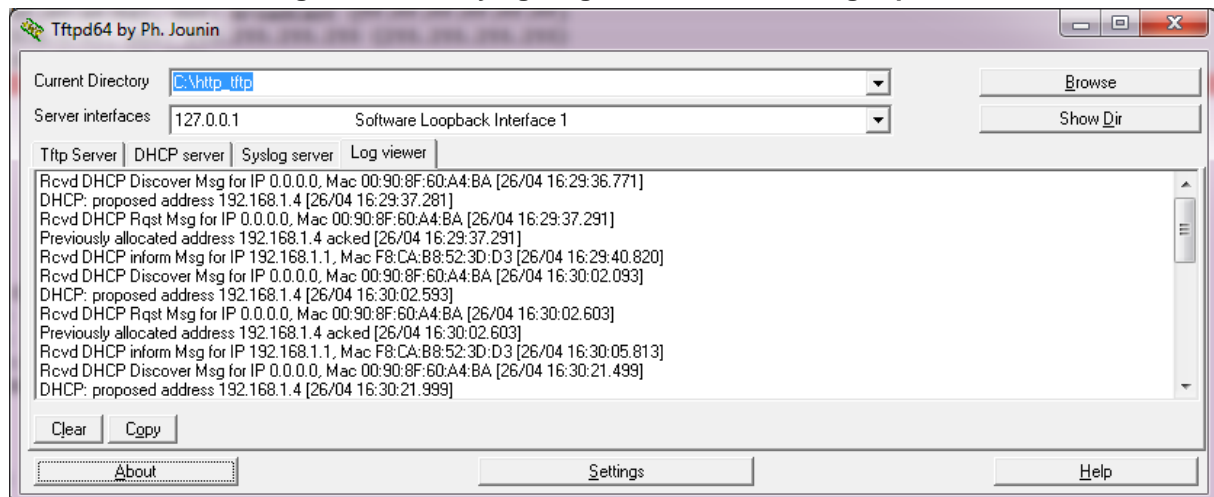


### B.4.3 Making Sure Using the Phone Screen

In tftpd64, view the indications shown in the figures below.

**Figure B-9: Verifying .img File Download from the Phone Screen**
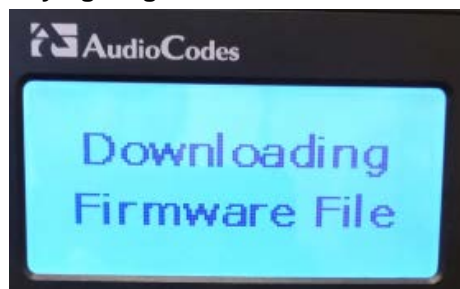


> ⚠️ **Important:** Do not unplug / power-off the phone while the screen displays the message shown below.
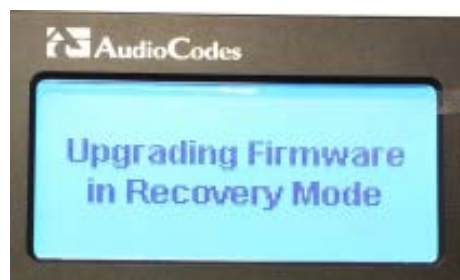


You can disconnect the phone from the PC and connect to the network LAN *only after the firmware upgrade finishes*, that is, after the phone's screen displays the following:

**Discovering CDP…Discovering LLDP…Acquiring IP…**

The phone is now up, functioning, and ready to be provisioned.

This page is intentionally left blank.

# C     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 *call forwarding.* 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**



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**



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)**
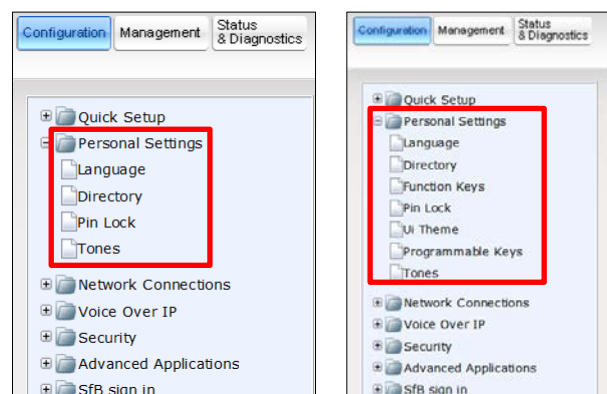
The HRS' UI Theme can be changed in the Web interface. You can select MSFT (Microsoft) or AudioCodes.

**Figure C-13: UI Theme**
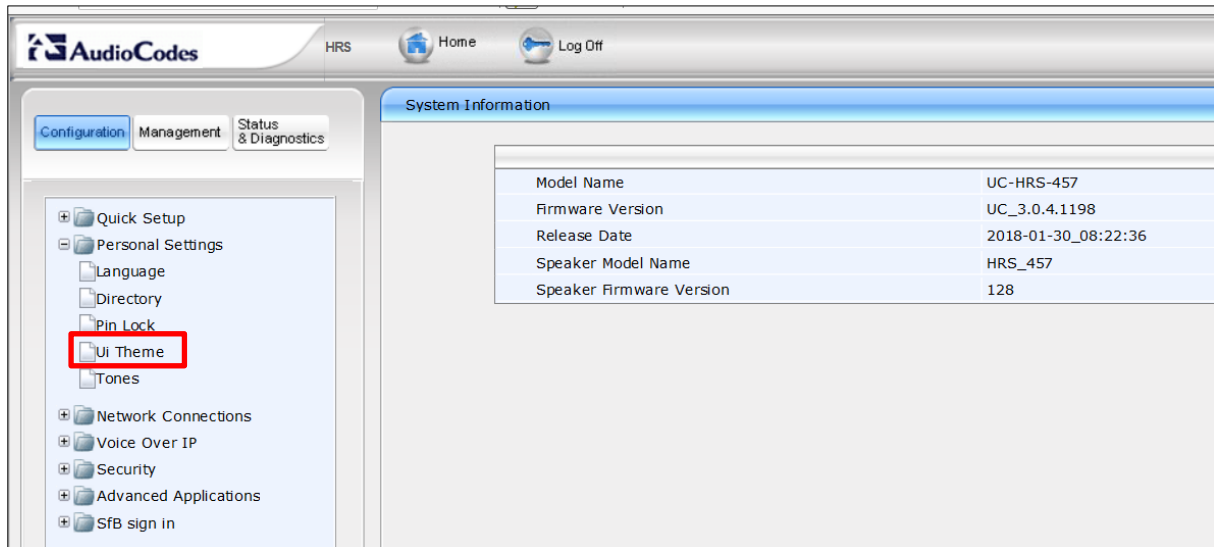
# D    Specifications

See AudioCodes' *400HD IP Phone Series Release Notes* for detailed information about the phones' specifications.

## D.1    405HD Model IP Phone

The table below details the 405HD model IP phone specifications.

**Table D-1: 405HD Model IP Phone Specifications**

| Feature | Details |
|---|---|
| **VoIP Signaling Protocols** | ▪ SIP: RFC 3261, RFC 2327 (SDP) |
| **Data Protocols** | ▪ IPv4, TCP, UDP, ICMP, ARP, DNS and DNS SRV for SIP Signaling<br>▪ SIP over TLS (SIPS)<br>▪ 802.1x<br>▪ 802.1p/Q for Traffic Priority and QoS<br>▪ VLAN Discovery Mechanism (CDP, LLDP and LLDP-MED)<br>▪ ToS (Type of Service) field, indicating desired QoS DHCP Client<br>▪ NTP Client<br>▪ Microsoft Skype for Business (previously Microsoft Lync)<br>▪ MS-ICE2<br>▪ Open SSL 1.0.1 integrated with TLS 1.2, compliant with Skype for Business security requirements<br>▪ OpenSSL 1.0.1m, supporting SHA2 algorithms<br>▪ OVR (One Voice Resiliency) |
| **Media Processing** | ▪ Voice Coders: G.711, G.729A/B, G.722, and RTA<br>▪ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length<br>▪ Adaptive Jitter Buffer 300 msec<br>▪ Voice Activity Detection<br>▪ Comfort Noise Generation<br>▪ Packet Lost Concealment<br>▪ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)<br>▪ DTMF Relay (RFC 2833) |
| **Telephony Features** | ▪ Busy on Busy<br>▪ Call Park<br>▪ Group Call Pickup<br>▪ Call Hold / Un-Hold<br>▪ Call Transfer; the TRANSFER hard key's default functionality (blind transfer) can be changed to consultative transfer.<br>▪ Redial<br>▪ Caller ID Notification<br>▪ Call Waiting Indication, including Caller ID<br>▪ Message Waiting Indication (including MWI LED)<br>▪ Local and Corporate Directories<br>▪ Automatic On-hook Dialing<br>▪ Automatic Answering (Alert-Info header and "talk" event)<br>▪ Call Logs: Missed/Received Calls/Dialed; all devices that users sign into are synchronized with Microsoft Exchange server. |

| Feature | Details |
|---|---|
| | ▪ URL Dialing<br>▪ 1-9 Speed Dials (dial pad keys)<br>▪ Call Forward (Do not forward, Forward to voice mail, Forward to a number)<br>▪ Dial plan (supports normalization rules downloaded from the Skype for Business server via in-band provisioning)<br>▪ Inputting Text to Dial (T9)<br>▪ Paging w/without Barge-in and configurability of Function Keys as paging group dials<br>▪ Better Together over Ethernet (BToE) compatible with Microsoft Skype for Business<br>▪ Voicemail (including capability to secure user access with PIN code) |
| Configuration/ Management | ▪ LCD Display User Interface Language Support (Various Languages)<br>▪ Web-based Management (HTTP/HTTPS) with fully integrated login<br>▪ Auto-Provisioning (via TFTP, FTP, HTTP and HTTPS) for firmware and configuration file upgrade<br>▪ In-Band Provisioning<br>▪ DHCP options (66, 67, and 160) for auto-provisioning<br>▪ DHCP options (120, 60, and 77) for device information<br>▪ DHCP option (42 or 4) for the NTP server<br>▪ DHCP option (43) for the URL of the Certificate Provisioning service<br>▪ DHCP option (2) for the Time Zone Offset<br>▪ Skype for Business Contacts<br>▪ Outlook Contacts<br>▪ LDAP (Lightweight Directory Access Protocol)<br>▪ Private labeling mechanism<br>▪ Configuration file encryption (entire file and individual parameters) |
| Debugging Tools | ▪ IPP Tracing<br>▪ Syslog mechanism<br>▪ DSP recording<br>▪ Port mirroring<br>▪ VoIP Status Web page |

| Feature | Details |
|---|---|
| **Hardware** | ▪ **LCD screen:** Graphic LCD (128 X 48)<br>▪ Connectors interfaces:<br>  ✔ 2 x RJ-45 ports (10/100BaseT Ethernet) for WAN and LAN<br>  ✔ RJ-9 port (jack) for Headset<br>  ✔ RJ-9 port (jack) for Handset<br>▪ Mounting:<br>  ✔ Wall and desktop mounting options<br>  ✔ One angle for desktop mount, another angle for wall mount<br>▪ Power:<br>  ✔ DC jack adapter 12V<br>  ✔ Power supply AC 100 ~ 240V<br>  ✔ PoE Class 1: IEEE802.3af (optional)<br>▪ Keys:<br>  ✔ 4 x softkeys<br>  ✔ VOICE MAIL message hotkey<br>  ✔ 4-way navigation keys with ENTER Key<br>  ✔ MENU<br>  ✔ REDIAL<br>  ✔ HOLD<br>  ✔ MUTE<br>  ✔ VOLUME control key<br>  ✔ HEADSET<br>  ✔ SPEAKER |
| **Headset Compatibility** | ▪ For a comprehensive list of supported Jabra headsets, see the Jabra Headset Compatibility Guide<br>▪ For a comprehensive list of supported Plantronics headsets headsets see http://www.plantronics.com/us/compatibility-guide/#/search/<br>▪ These include:<br>  ✔ Jabra UC-150<br>  ✔ Jabra Speak 510+<br>  ✔ Jabra Speak 410<br>  ✔ Jabra MOTION OFFICE<br>  ✔ Jabra PRO 9470<br>  ✔ Microsoft LX-3000<br>  ✔ Plantronics C-310M<br>  ✔ Plantronics C-320M<br>  ✔ Plantronics HW720<br>  ✔ Jabra Pro 920 EHS wireless headset<br>  ✔ Jabra Pro 9450 EHS wireless headset<br>Note that the 405HD phone doesn't support USB headsets. |

## D.2    430HD and 440HD IP Phones

The table below details the 430HD and 440HD IP Phones specifications.

**Table D-2: 430HD and 440HD IP Phone Specifications**

| Feature | Details |
|---|---|
| **VoIP Signaling Protocols** | ▪ SIP: RFC 3261, RFC 2327 (SDP) |
| **Data Protocols** | ▪ IPv4, TCP, UDP, ICMP, ARP, DNS and DNS SRV for SIP Signaling<br>▪ SIP over TLS (SIPS)<br>▪ 802.1x<br>▪ 802.1p/Q for Traffic Priority and QoS<br>▪ VLAN Discovery Mechanism (CDP, LLDP and LLDP-MED)<br>▪ ToS (Type of Service) field, indicating desired QoS DHCP Client<br>▪ NTP Client<br>▪ Microsoft Skype for Business (previously Microsoft Lync)<br>▪ MS-ICE2<br>▪ Open SSL 1.0.1 integrated with TLS 1.2, compliant with Skype for Business security requirements<br>▪ OpenSSL 1.0.1m, supporting SHA2 algorithms<br>▪ OVR (One Voice Resiliency) |
| **Media Processing** | ▪ Voice Coders: G.711, G.729A/B, G.722, and RTA.<br>▪ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length<br>▪ Adaptive Jitter Buffer 300 msec<br>▪ Voice Activity Detection<br>▪ Comfort Noise Generation<br>▪ Packet Lost Concealment<br>▪ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)<br>▪ DTMF Relay (RFC 2833) |
| **Telephony Features** | ▪ BLF presence on buttons; capability for 18 Multiple Points of Presence (MPOPs), including Skype for Business clients.<br>▪ Busy on Busy<br>▪ Call Park<br>▪ Group Call Pickup<br>▪ Call Hold / Un-Hold<br>▪ Call Transfer (including Blind Transfer option during calls)<br>▪ 3-Way Conferencing (with local mixing)<br>▪ Redial<br>▪ Caller ID Notification<br>▪ Call Waiting Indication, including Caller ID<br>▪ Message Waiting Indication (including MWI LED)<br>▪ Local and Corporate Directories<br>▪ Automatic On-hook Dialing<br>▪ Automatic Answering (Alert-Info header and "talk" event)<br>▪ Call Logs: Missed/Received Calls/Dialed; all devices that users sign into are synchronized with Microsoft Exchange server.<br>▪ 5 programmable keys, each configurable as a Speed Dial or as Key Event (Missed Calls, Received Calls, Dialed Calls, Directory, DnD |

| Feature | Details |
|---|---|
|  | All, Forward All) |
|  | ▪ 12 Function Keys, each configurable as a Speed Dial, with presence monitoring |
|  | ▪ URL Dialing |
|  | ▪ Call Forward (Do not forward, Forward to voice mail, Forward to a number) |
|  | ▪ Boss Admin (applies only to the 430HD and 440HD phones) |
|  | ▪ Dial plan (supports normalization rules downloaded from the Skype for Business server via in-band provisioning) |
|  | ▪ T9 predictive text for Corporate Directory search |
|  | ▪ Paging w/without Barge-in and configurability of Function Keys and programmable keys (430HD/440HD) as paging group dials. |
|  | ▪ Better Together over Ethernet (BToE) compatible with Microsoft Skype for Business |
|  | ▪ Voicemail (including capability to secure user access with PIN code) |
| **Configuration/ Management** | ▪ LCD Display User Interface Language Support (Various Languages) |
|  | ▪ Web-based Management (HTTP/HTTPS) with fully integrated login |
|  | ▪ Auto-Provisioning (via TFTP, FTP, HTTP, and HTTPS) for firmware and configuration file upgrade |
|  | ▪ In-band Provisioning |
|  | ▪ DHCP options (66, 67, and 160) for auto-provisioning |
|  | ▪ DHCP options (120, 60, and 77) for device information |
|  | ▪ DHCP option (42 or 4) for the NTP server |
|  | ▪ DHCP option (43) for the URL of the Certificate Provisioning service |
|  | ▪ DHCP option (2) for the Time Zone Offset |
|  | ▪ Skype for Business contacts |
|  | ▪ Outlook contacts |
|  | ▪ LDAP (Lightweight Directory Access Protocol) |
|  | ▪ Private labeling mechanism |
|  | ▪ Configuration file encryption (entire file and individual parameters) |
| **Debugging Tools** | ▪ IPP Tracing |
|  | ▪ Syslog mechanism |
|  | ▪ DSP recording |
|  | ▪ Port mirroring |
|  | ▪ VoIP Status Web page |

| Feature | Details |
|---|---|
| **Hardware** | ▪ **LCD screen:** Graphic LCD (132x64) monochrome (a 440HD phone hardware revision featuring an LCD resolution of 256x128 is supported from v2.0.13)<br>▪ **BLF screen:** Graphic LCD (60x376) monochrome (applies only to the 440HD model)<br>▪ Connectors interfaces:<br> ✔ 2 x RJ-45 ports (10/100/1000BaseT Ethernet) for WAN and LAN<br> ✔ RJ-9 port (jack) for Headset<br> ✔ RJ-9 port (jack) for Handset<br> ✔ USB interface for USB headset support<br> ✔ RJ-11 interface for DHSG<br>▪ Mounting:<br> ✔ Wall and desktop mounting options<br> ✔ One angle for desktop mount, another angle for wall mount<br>▪ Power:<br> ✔ DC jack adapter 12V<br> ✔ Power supply AC 100 ~ 240V<br> ✔ PoE Class 2: IEEE802.3af (optional)<br>▪ Keys:<br> ✔ 4 x softkeys<br> ✔ VOICE MAIL message hotkey (including LED)<br> ✔ 4-way navigation keys with ENTER Key<br> ✔ MENU<br> ✔ REDIAL<br> ✔ HOLD<br> ✔ MUTE (including LED)<br> ✔ TRANSFER<br> ✔ VOLUME control key<br> ✔ HEADSET (including LED)<br> ✔ SPEAKER (including LED) |
| **Headset Compatibility** | ▪ For a comprehensive list of supported Jabra headsets, see the Jabra Headset Compatibility Guide<br>▪ For a comprehensive list of supported Plantronics headsets headsets see http://www.plantronics.com/us/compatibility-guide/#/search/<br>▪ For a comprehensive list of supported VXi products, see http://www.vxicorp.com/compatibility_guide/<br>▪ Also the following which aren't documented online yet:<br> ✔ Jabra UC-150<br> ✔ Jabra Speak 510+<br> ✔ Jabra Speak 410<br> ✔ Jabra MOTION OFFICE<br> ✔ Jabra PRO 9470<br> ✔ Microsoft LX-3000<br> ✔ Plantronics C-310M<br> ✔ Plantronics C-320M<br> ✔ Plantronics HW720<br> ✔ Jabra UC-550<br> ✔ Jabra Pro 920 EHS wireless headset<br> ✔ Jabra Pro 9450 EHS wireless headset |

## D.3    450HD IP Phone

The table below details the 450HD IP phone specifications.

**Table D-3: 450HD IP Phone Specifications**

| Feature | Details |
|---|---|
| **VoIP Signaling Protocols** | ▪ SIP: RFC 3261, RFC 2327 (SDP) |
| **Data Protocols** | ▪ IPv4, TCP, UDP, ICMP, ARP, DNS and DNS SRV for SIP Signaling<br>▪ SIP over TLS (SIPS)<br>▪ 802.1x<br>▪ 802.1p/Q for Traffic Priority and QoS<br>▪ VLAN Discovery Mechanism (CDP, LLDP and LLDP-MED)<br>▪ ToS (Type of Service) field, indicating desired QoS DHCP Client<br>▪ NTP Client<br>▪ Microsoft Skype for Business (previously Microsoft Lync)<br>▪ MS-ICE2<br>▪ Open SSL 1.0.1 integrated with TLS 1.2, compliant with Skype for Business security requirements<br>▪ OpenSSL 1.0.1m, supporting SHA2 algorithms<br>▪ OVR (One Voice Resiliency) |
| **Media Processing** | ▪ Voice Coders: G.711, G.729A/B, G.722, and RTA.<br>▪ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length<br>▪ Adaptive Jitter Buffer 300 msec<br>▪ Voice Activity Detection<br>▪ Comfort Noise Generation<br>▪ Packet Lost Concealment<br>▪ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)<br>▪ DTMF Relay (RFC 2833) |
| **Telephony Features** | ▪ BLF presence on buttons; capability for 18 Multiple Points of Presence (MPOPs), including Skype for Business clients.<br>▪ Busy on Busy<br>▪ Call Park<br>▪ Group Call Pickup<br>▪ Call Hold / Un-Hold<br>▪ Call Transfer (including Blind Transfer option during calls)<br>▪ 3-Way Conferencing (with local mixing)<br>▪ Redial<br>▪ Caller ID Notification<br>▪ Call Waiting Indication, including Caller ID<br>▪ Message Waiting Indication (including MWI LED)<br>▪ Local and Corporate Directories<br>▪ Automatic On-hook Dialing<br>▪ Automatic Answering (Alert-Info header and "talk" event)<br>▪ Call Logs: Missed/Received Calls/Dialed; all devices that users sign into are synchronized with Microsoft Exchange server.<br>▪ 5 programmable keys, each configurable as a Speed Dial or as Key Event (Missed Calls, Received Calls, Dialed Calls, Directory, DnD |

| Feature | Details |
|---|---|
| | All, Forward All)<br>▪ 12 Function Keys, each configurable as a Speed Dial, with presence monitoring<br>▪ URL Dialing<br>▪ Call Forward (Do not forward, Forward to voice mail, Forward to a number)<br>▪ Boss Admin (applies only to the 430HD and 440HD phones)<br>▪ Dial plan (supports normalization rules downloaded from the Skype for Business server via in-band provisioning)<br>▪ T9 predictive text for Corporate Directory search<br>▪ Paging w/without Barge-in and configurability of Function Keys and programmable keys (430HD/440HD) as paging group dials.<br>▪ Better Together over Ethernet (BToE) compatible with Microsoft Skype for Business<br>▪ Voicemail (including capability to secure user access with PIN code) |
| **Configuration/ Management** | ▪ LCD Display User Interface Language Support (Various Languages)<br>▪ Web-based Management (HTTP/HTTPS) with fully integrated login<br>▪ Auto-Provisioning (via TFTP, FTP, HTTP, and HTTPS) for firmware and configuration file upgrade<br>▪ In-band Provisioning<br>▪ DHCP options (66, 67, and 160) for auto-provisioning<br>▪ DHCP options (120, 60, and 77) for device information<br>▪ DHCP option (42 or 4) for the NTP server<br>▪ DHCP option (43) for the URL of the Certificate Provisioning service<br>▪ DHCP option (2) for the Time Zone Offset<br>▪ Skype for Business contacts<br>▪ Outlook contacts<br>▪ LDAP (Lightweight Directory Access Protocol)<br>▪ Private labeling mechanism<br>▪ Configuration file encryption (entire file and individual parameters) |
| **Debugging Tools** | ▪ IPP Tracing<br>▪ Syslog mechanism<br>▪ DSP recording<br>▪ Port mirroring<br>▪ VoIP Status Web page |

| Feature | Details |
|---|---|
| **Hardware** | ▪ **LCD screen:** Graphic LCD (132x64) monochrome (a 440HD phone hardware revision featuring an LCD resolution of 256x128 is supported from v2.0.13)<br>▪ **BLF screen:** Graphic LCD (60x376) monochrome (applies only to the 440HD model)<br>▪ Connectors interfaces:<br>  ✔ 2 x RJ-45 ports (10/100/1000BaseT Ethernet) for WAN and LAN<br>  ✔ RJ-9 port (jack) for Headset<br>  ✔ RJ-9 port (jack) for Handset<br>  ✔ USB interface for USB headset support<br>  ✔ RJ-11 interface for DHSG<br>▪ Mounting:<br>  ✔ Wall and desktop mounting options<br>  ✔ One angle for desktop mount, another angle for wall mount<br>▪ Power:<br>  ✔ DC jack adapter 12V<br>  ✔ Power supply AC 100 ~ 240V<br>  ✔ PoE Class 3: IEEE802.3af (optional)<br>▪ Keys:<br>  ✔ 4 x softkeys<br>  ✔ VOICE MAIL message hotkey (including LED)<br>  ✔ 4-way navigation keys with ENTER Key<br>  ✔ MENU<br>  ✔ REDIAL<br>  ✔ HOLD<br>  ✔ MUTE (including LED)<br>  ✔ TRANSFER<br>  ✔ VOLUME control key<br>  ✔ HEADSET (including LED)<br>  ✔ SPEAKER (including LED) |
| **Headset Compatibility** | ▪ For a comprehensive list of supported Jabra headsets, see the Jabra Headset Compatibility Guide<br>▪ For a comprehensive list of supported Plantronics headsets headsets see http://www.plantronics.com/us/compatibility-guide/#/search/<br>▪ For a comprehensive list of supported VXi products, see http://www.vxicorp.com/compatibility_guide/<br>▪ Also the following which aren't documented online yet:<br>  ✔ Jabra UC-150<br>  ✔ Jabra Speak 510+<br>  ✔ Jabra Speak 410<br>  ✔ Jabra MOTION OFFICE<br>  ✔ Jabra PRO 9470<br>  ✔ Microsoft LX-3000<br>  ✔ Plantronics C-310M<br>  ✔ Plantronics C-320M<br>  ✔ Plantronics HW720<br>  ✔ Jabra UC-550<br>  ✔ Jabra Pro 920 EHS wireless headset<br>  ✔ Jabra Pro 9450 EHS wireless headset |

## D.4    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 D-4: 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 |
| **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 |

| RFC Number | RFC Title |
|---|---|
| **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 |

> **Note:** 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)

## D.4.1    SIP Compliance Tables

The SIP device complies with RFC 3261 as shown in the following subsections.

### D.4.1.1    SIP Methods

The device supports the following SIP methods:

**Table D-5: 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 | |

### D.4.1.2   SIP Headers

The device supports the following SIP headers:

**Table D-6: 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 |
| 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 |

| Header Field | Supported |
|---|---|
| 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.**
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

**Contact us**: https://www.audiocodes.com/corporate/offices-worldwide
**Website**: https://www.audiocodes.com/

Document #: LTRT-09944