

AVAYA MESSAGING™

Feature Description Guide

Release 11.0 SP4
Issue 12
October 2026

AVAYA MESSAGING Feature Description Guide

Avaya Messaging is a feature rich application which offers a solution for virtually any organization or situation. The productivity enhancing nature of Avaya Messaging derives from the dynamic environment of all the features which can be fully customized and mixed-and-matched to meet the specific needs of an organization.

Since the feature library of Avaya Messaging platform is vast, it is easy to become overwhelmed by the large number of settings and options available to you as an administrator or an end user. To simplify both the configuration and usage of the common features within Avaya Messaging, this guide separates each feature and explains in detail how they can be implemented.

Having to consult vast amounts of technical documentation to implement a single feature can be time consuming and inefficient. By organizing all the necessary materials for you, the Feature Description Guide will make the administration process a breeze and will also offer you end user training materials which you may utilize during training sessions or distribute directly to the end users.

© 2014-2026, Avaya LLC
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products.

Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End users agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/ legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A

CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE

IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER

OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.

ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual

property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow https//support.avaya.com/css/P8/documents/100161515.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties.
Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

Contents

Chapter 1: AUTOMATIC SPEECH RECOGNITION (ASR) 10

Introduction 10

Visual Guide 10

Requirements 10

Server configuration 11

Avaya Messaging Admin Configuration 11

License Confirmation 13

ASR Configurator 13

MRCP Configurator 15

Chapter 2: ENHANCED CALL CONTROL 17

Introduction 17

Requirements 18

Server Configuration 18

Company 18

Feature Group 19

User Guide 20

ECC Command List 20

Chapter 3: SPEECH COMMANDS 21

Introduction 21

Visual Guide 21

Requirements 21

Server Configuration 21

Company Properties 22

Feature Group Properties 22

Mailbox Properties 23

Customize TUI Configuration 24

User Guide 24

Basic TUI Navigation 24

Temporarily Disable Speech Command 25

Chapter 4: SPEECH CONTACTS 26

Introduction 26

Visual Guide....26
Requirements....26
Server Configuration....27
Procedure....27
User Guide....30
Enabling Speech Contacts....30
Chapter 5: WEB LINKS....32
Introduction....32
Configuration Process....32
Configuration with IIS 7....33
Configuration with IIS 6....34
Avaya Messaging Configuration....36
Weblinks Example....38
Chapter 6: EMAIL ACTION SCHEMA....40
Introduction....40
Enable Action Schema....40
Email Buttons....42
Chapter 7: MUTARE TRANSCRIPTION SERVICE....48
Introduction....48
Visual Guide....48
Requirements....49
Licensing....49
Upgrading the License....49
Avaya Messaging Server Configuration....52
Transcription Configuration Tool....52
Verification....54
User Guide....54
Chapter 8: GOOGLE INTEGRATION....55
Guidelines....55
Introduction....55
Synchronization Directions....56
Implementation Example....56
Requirements....56
Install and configure OAuth2.0....58
OAuth 2.0 Setup....58
Domain Setup....71

User Guide 81
Reconfiguring Synchronization Components for Gmail 85
Restart Services 87
Chapter 9: EXCHANGE 2019/2016 INTEGRATION: USING EWS 88
Guidelines 88
Introduction 88
Visual Guide 88
Requirements 89
Server Configuration 89
Exchange Superuser Creation/Configuration 89
AM Admin Configuration 94
Contact and Calendar Sync 101
User Guide 106
Chapter 10: OFFICE 365 INTEGRATION WITH MICROSOFT GRAPH 108
Guidelines 108
Introduction 108
Pre-requisites 108
Connecting Through Microsoft Graph 108
User Configurations 117
Reconfiguring Synchronization Components for Graph 118
Restart Services 121
Note After Upgrading or Updating 121
Chapter 11: AVAYA MESSAGING TO OFFICE 365 INTEGRATION WITH EWS 122
Guidelines 122
Introduction 122
Pre-requisites 122
Office 365 Configuration 123
Avaya Messaging Server Configuration 131
Connecting Through EWS Using OAuth 2.0 133
Verify Configuration Setting 141
Chapter 12: FIND ME FOLLOW ME ON CTI INTEGRATION 144
Introduction 144
Visual Guide 145
Requirements 145
User Guide 145
Find me Follow me with CTI Integration 145

Chapter 13: MULTIPLE TIME ZONE SUPPORT 155
Introduction 155
Visual Guide 155
Requirements 156
Server Configuration 156
General Settings 156
Chapter 14: REMOTE ADMINISTRATION 158
Introduction 158
Visual Guide 158
Requirements 158
Installing Remote Admin 159
Connecting to Remote Admin 161
Chapter 15: REMOTE PRINTER 162
Introduction 162
Remote Printer Host Installation and Setup 162
Avaya Messaging Voice Server Remote Printer Setup 163
Chapter 16: AVAYA MESSAGING FAXING 165
Introduction 165
Requirements 165
Fax via Windows Fax Services (Windows 7) Configuration 165
Fax via Windows Fax Services (Windows XP) Configuration 172
Chapter 17: DIALOGIC SR140 FAX INTEGRATION 182
Introduction 182
Prerequisites 182
Configuration 183
License Manager 183
Configuration Manager 189
Avaya Messaging Configuration 192
Monitoring Channel Activity 199
Fax Detect and Deflect 200
Single DID for Fax and Voice 202
Avaya Messaging Server Configuration 206
Communication Manager Configuration 207
Chapter 18: DIALOGIC SR140 SECURE FAX 210
Introduction 210
Pre-requisites 210

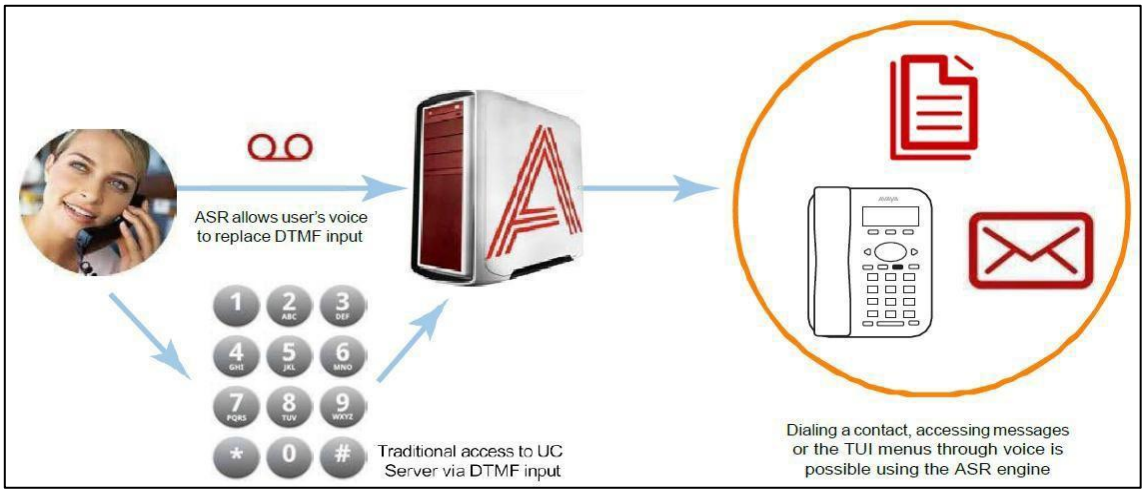
Configuration 211
License Manager 211
Configuration Manager 218
Avaya Aura Communication Manager Configuration 224
Avaya Aura System Manager Setup 226
Avaya Messaging Configuration 235
Chapter 19: WEB ACCESS 237
Introduction 237
Getting Started 237
Navigation 238
Chapter 20: PASSWORD RESET 239
Chapter 21: WEB UM MONITOR 241
Introduction 241
Getting Started 241
The Channels Tab 242
The View Status Tab 243
The View Trace Tab 244
Sending Commands 245
Display License Details 246
Chapter 22: INTEGRATION WITH AVAYA CPaaS 247
Introduction 247
Pre-requisites 247
Avaya CPaaS Configuration 247
Avaya Messaging Voice Server Configuration 250
Avaya Messaging User Configuration 251
One-to-one 251
Any-to-many 255
Addressing SMS Messages 259
Chapter 23: ACCESSIBILITY 263
Introduction 263
508 Compliance 263
TTY Integration 265
Voice Recordings and TTY 266

Chapter 1: AUTOMATIC SPEECH RECOGNITION (ASR)

Introduction

Automatic Speech Recognition (ASR) is a vital component of the UC system. ASR allows the system to recognize human speech, so that users speak contact names and menu selections, instead of entering them through the telephone keypad. Avaya Messaging uses Media Resource Control Protocol (MRCP) for communications with the ASR services provider.

Visual Guide



ASR provides the base for all speech recognition functions, such as Speech Contacts and Speech Commands. ASR interprets a user's voice input as a number or a character (e.g., alphabet) based on the grammar settings on the server.

This allows users to speak the name of the contact they want to dial, or to say a number instead of pressing the digit on the telephone keypad. By replacing traditional input with speech, users can efficiently find what they were looking for. It also gives users easy access to the system without having to use their hands.

For specific features such as Speech Commands, please refer to the appropriate chapters in this guide.

Requirements

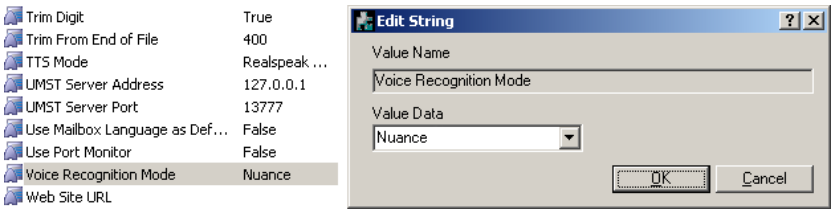
Requirements	Details
License	ASR License
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher

Server configuration

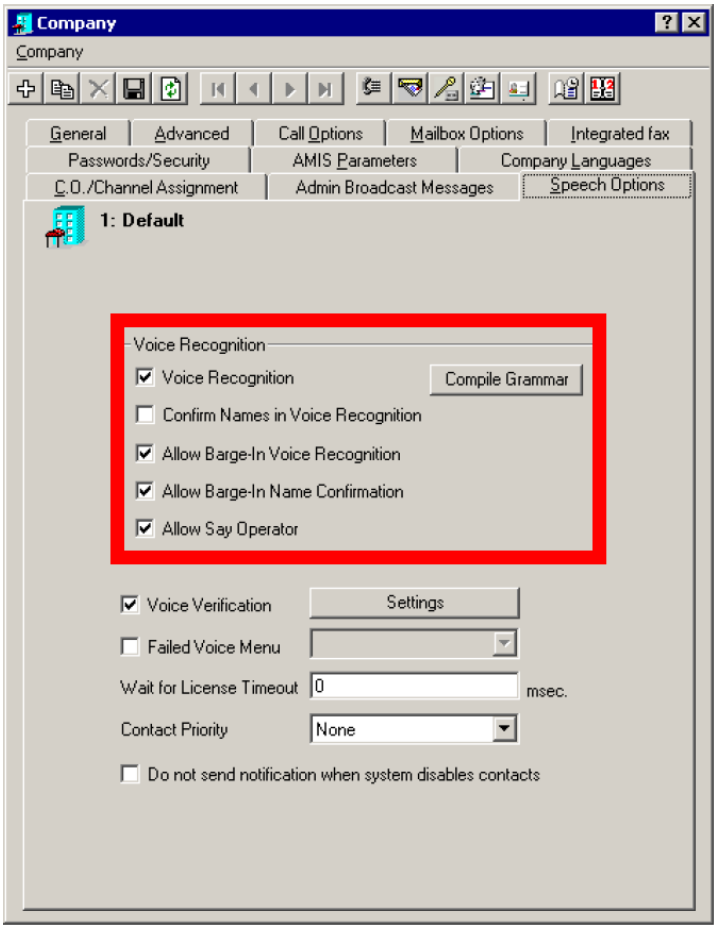
Server configuration for ASR is completed in several steps.
First, verify the Avaya Messaging license that you have. To use ASR, you must have the ASR license. Once the license is confirmed, make the necessary settings in the Avaya Messaging Administrator and from the ASR Configurator.

Avaya Messaging Admin Configuration

1. Open Avaya Messaging Admin and go to **Configuration > Advanced**. In the right pane, set Voice recognition mode to Nuance.

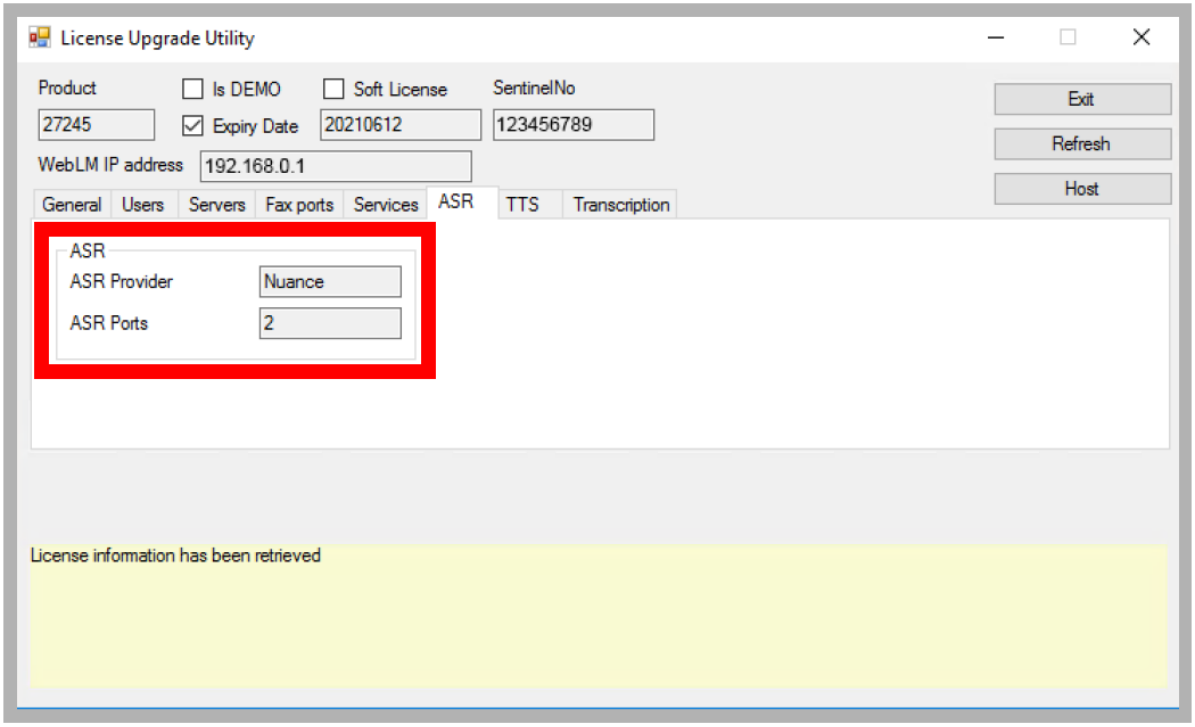


2. Once this option has been set, go to **Company Properties**.
3. Right+-click on the company that will use ASR. Choose Properties.
4. Go to the **Speech Options** tab and enable **Voice Recognition**. Enable the other features as required.
   Confirm names in voice recognition: The system will confirm a recognized name no matter what.
   Allow barge-in voice recognition: This allows you to say a name while the system is playing a greeting or a prompt.
   Allow barge-in confirm names: The system will allow you to interrupt it to confirm that a name that it found is correct.
   Allow Say Operator: For the systems with a default operator defined, it will recognize the word “Operator” as a dial request for the operator.


Company
Company
General
Advanced
Call Options
Mailbox Options
Integrated fax
Passwords/Security
AMIS Parameters
Company Languages
C.O./Channel Assignment
Admin Broadcast Messages
Speech Options
1: Default
Voice Recognition
Voice Recognition
Compile Grammar
Confirm Names in Voice Recognition
Allow Barge-In Voice Recognition
Allow Barge-In Name Confirmation
Allow Say Operator
Voice Verification
Settings
Failed Voice Menu
Wait for License Timeout
0
msec.
Contact Priority
None
Do not send notification when system disables contacts

License Confirmation

Setting up ASR begins by making sure that you have purchased and installed the license. ASR is provided under an add-on to the standard license and must be purchased separately.



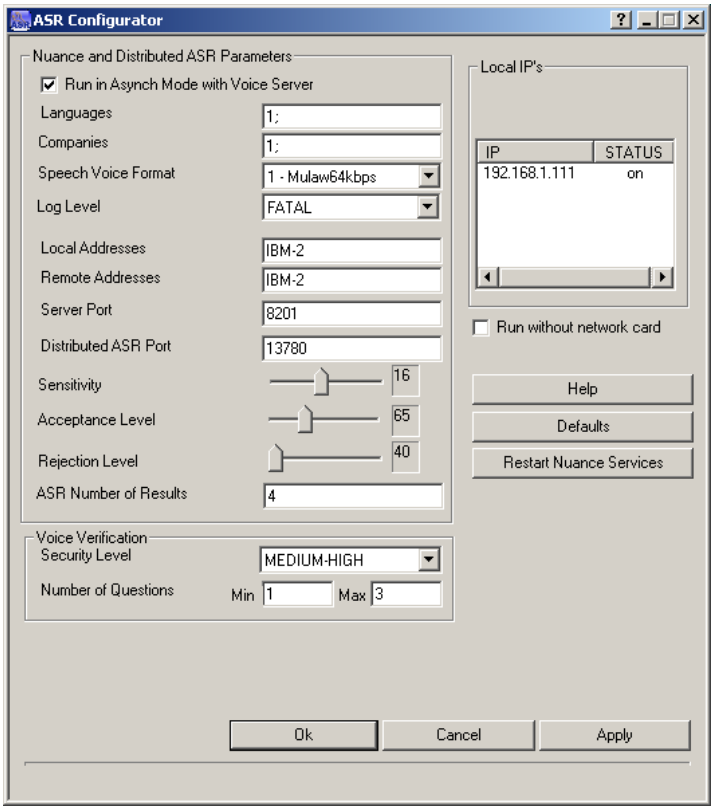
Check the **UCLicenseWebLM** under **Start>Programs>Avaya Messaging**.
Go to the **ASR** tab and ensure that the information contains the appropriate details.
With the license confirmed, launch the Avaya Messaging Administrator to configure the application.

ASR Configurator

From the Voice Verification section of the interface, you can specify the sensitivity level for the feature via **Security Level**. The number of questions the voice server will ask during login can also be controlled through **Number of Questions**.

Security Level has 5 levels to choose between. These range from **Very- High** to **Medium Low**. Refer to the chart below to see the difference between each level, along with the typical **False Acceptance** rate (the rate in which the system will log in a wrong person to the mailbox).

Since the FA rate for **Very-High** is the lowest, it may seem logical to always choose this option. However, while the number of FAs decreases, the number of **FR**s (**False Rejection**) increases. At the highest security setting, people may have problems logging into their mailbox if their voice changes even slightly. This might be caused by a sore throat, added environmental noise or using a different device. It is up to the site administrator to choose the setting which best fits the company's requirements.



Number of Questions: Choose the number of random questions that the system will ask when verifying the user's voice print. The system can be set up to ask between **1** and **3** questions. There are three types of questions that the system will ask at random.

- **Full Name**: The system will ask the user to speak out their full name associated with the mailbox.
- **Recognition Keywords**: The system will randomly choose a keyword from the database (defined by the administrator) and ask the user to repeat the word.
- **Random 4 Digit Number**: The system will generate a random 4 digit number and ask the user to repeat the numbers.

The default setting will ask a minimum of 1 and maximum of 3 questions. This means that if the answer to the first question was satisfactory, the user will be logged. If not, the system will ask a second question. If the answer to the second question was satisfactory, the user will be logged in.

If not, the system will ask the final question. If the answer to the final question was satisfactory, the user will be logged in. If not, the verification process will fail, and the user will either be disconnected from the system or be asked to manually enter their password through DTMF keys depending on the security settings of the site.

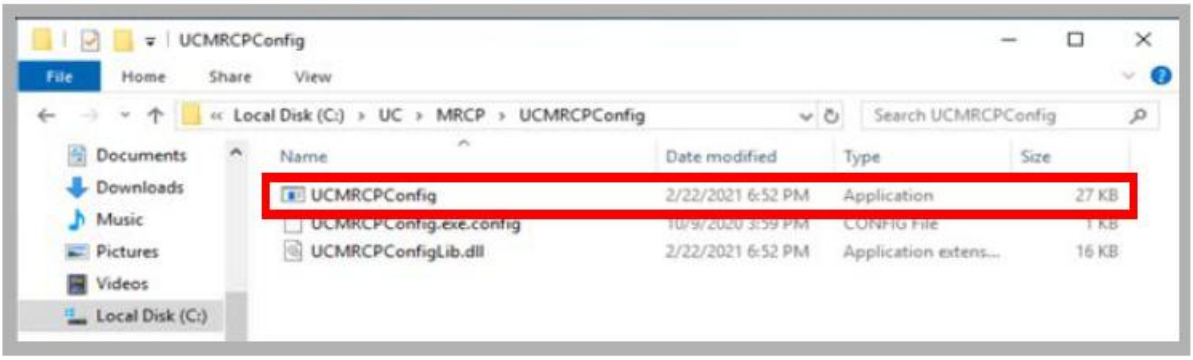
Security Level	Typical Usage Recommendation	FA Rate
Very-High	Access to mailbox accounts with critical information	0.1Internet to 0.2Internet
High	Access to mailbox accounts with high privilege	0.2Internet to 1.5Internet
Medium-High	Access to typical mailbox accounts	1.5Internet to 3Internet
Medium	Access to typical mailbox accounts in open environment	3Internet to 5Internet
Medium-Low	Generic access where Voice Verification is used for convenience	5Internet to 7Internet

Caution: The Voice Verification feature will shortly be discontinued.

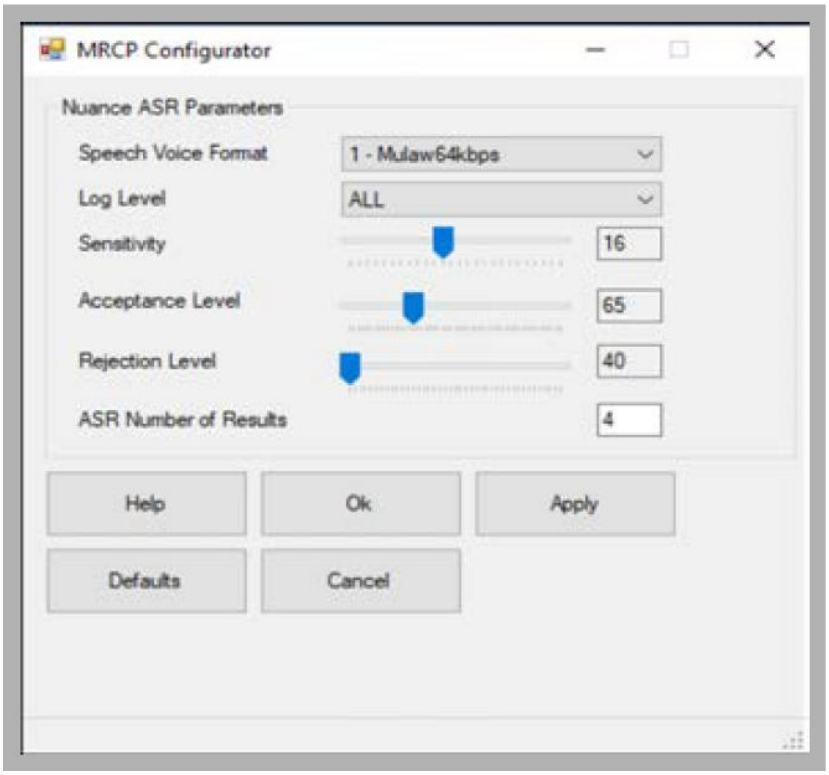
MRCP Configurator

The ASR feature should work well immediately after installation. However, if there are issues with the feature, such as excessive requests to “Please repeat that,” the administrator can adjust the program settings.

1. On the hard drive where Avaya Messaging is installed, open the **\UC\MRCP** folder and run UCMRCPConfig**.**



2. The ASR parameters are shown. Change these settings as necessary to correct any issues with the feature.



Speech Voice Format: Select the desired format for voice traffic:
0 - Linear 128kbps, **1** - Mulaw 64kbps, or **2** Alaw 64kbps. **Mulaw** is recommended.

Log Level: Provides control over the amount of information collected by the system regarding ASR. The amount of detail in the log increases with the selection as follows: **FATAL** (least data collected), **ERROR**, **WARN**, **USER_ERROR**, **USER_WARN**, **STATUS**, **INFO**, **D_INFO**, **VD_INFO** and **ALL** (most data collected). Choosing **NONE** disables logging.

Sensitivity: This adjusts the ability of the system to handle line noise. Drag the slider to select a value between
5 and **30**. Higher settings make ASR less sensitive to noise.
For TAPI/Dialogic boards, set this to **14**. For Rhetorex boards, set to **20**.

Acceptance Level: Drag the slider to select a value between **50** and **100**. The ASR server receives the voice stream and returns a score (as a %) regarding how certain it is that it understood. Scores at or above the value selected here are processed normally. Scores below this minimum are compared to the Rejection Level.

Rejection Level: Drag the slider to select a value between **40** and **80** (must be lower than the Acceptance Level). Scores below the Acceptance level but above the Rejection Level mean that the ASR server is uncertain whether it understood. The caller will be prompted to verify the result. Scores below the Rejection level are unusable and stop the process.

Click **Defaults** to return all values to their base values.

When ready, click **Apply**.

Chapter 2: ENHANCED CALL CONTROL

Introduction

When a call is made through the auto attendant to your external number, or if you dialed a person from an external number through the auto attendant, you will now perform basic call control actions right from your external number. This allows you to take advantage of the call control features without having to be tied down to your workstation or a specific telephone system. Any telephone that is capable of DTMF input will be able to send commands to the Avaya Messaging server if the call itself was connected through the Avaya Messaging server. ECC (Enhanced Call Control) also includes the Call Handoff feature which will supplement the transfer features.

Requirements

Requirements	Details
License	---
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher

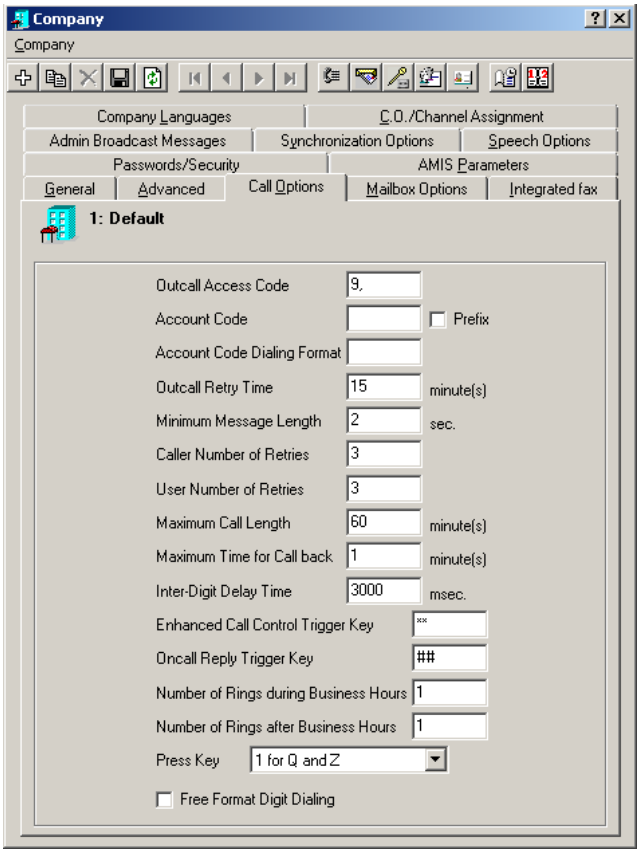
Server Configuration

The server-side configuration for enabling Enhanced Call Control is very simple. The administrator must enable the service on a Feature Group, then the mailboxes within that FG will have access to the feature. The administrator may also change the ECC trigger key from the Company settings as well.

Company

From **Company > Call Options** tab, modify the **Enhanced Call Control Trigger Key** as desired. The trigger can consist of any DTMF keys. This key is set to ** by default.

Note: Please ensure that Enhanced Call Control Trigger Key does not overlap with any other keys.

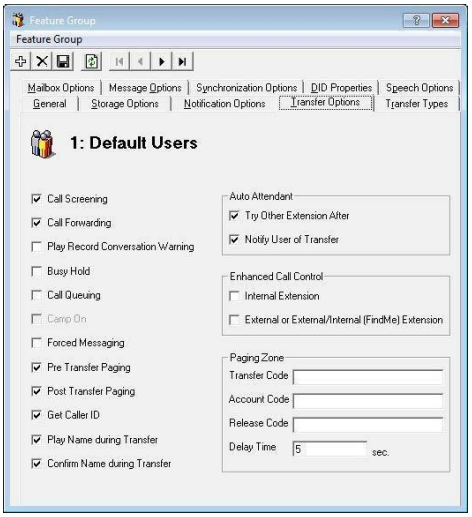


Feature Group

From **Feature Group > Transfer Options** tab, enable either or both of **Internal Extension** or **External or External/Internal (FindMe) Extension** checkbox from the **Enhanced Call Control** section.

Internal Extension will enable the ECC for user's dedicated internal device only.

External or External/Internal (FindMe) Extension will enable the ECC for both internal and external device if the call is made to the user through auto attendant.



User Guide

When the correct command key is pressed, you will hear the menu options available to you and the other person on the line will be on hold and will hear the hold music. While ECC allows you to control the call from the phone itself, the Call Handoff feature can also be managed. Refer to the section at the end of this guide for more information.

When the ECC is available for your current call, you will hear an audio indicator at the beginning of the call. If you do not hear this at the beginning of the call, you will not have access to ECC.

ECC Command List

Default Access Code. Push ** to enter the ECC menu. The other party will automatically be put on hold. This access code may be changed by the system administrator.

- **1** - Retrieve the current call (stop the hold)
- **2** - Transfer the current call to another number
- **3** - Hand off the current call to another device
- **4** - Disconnect the other person on hold and return you to the Auto Attendant
- **#** - Disconnect the current call for both parties

Chapter 3: SPEECH COMMANDS

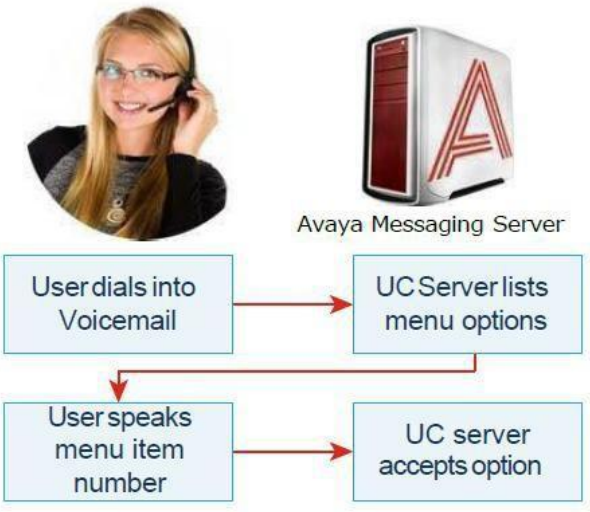
Introduction

Navigating through the Voice Menu or the TUI can sometimes be difficult when you cannot freely enter the DTMF keys. When you're on a cellphone, for example, it is often difficult to navigate through DTMF input due to the ergonomics of cell phones.

Avaya Messaging now supports a Voice Navigation function where the users may speak the numerical choice rather than to enter it on their phone. This will allow the users to freely navigate through the entire system without having to enter a single key.

Visual Guide

The user will dial into the system as he/she would normally do. Once connected, the system will list all the menu options as usual. The user speaks the menu item number of his/her choice. The system accepts Speech Command as a valid entry and performs the action associated with the number.



Requirements

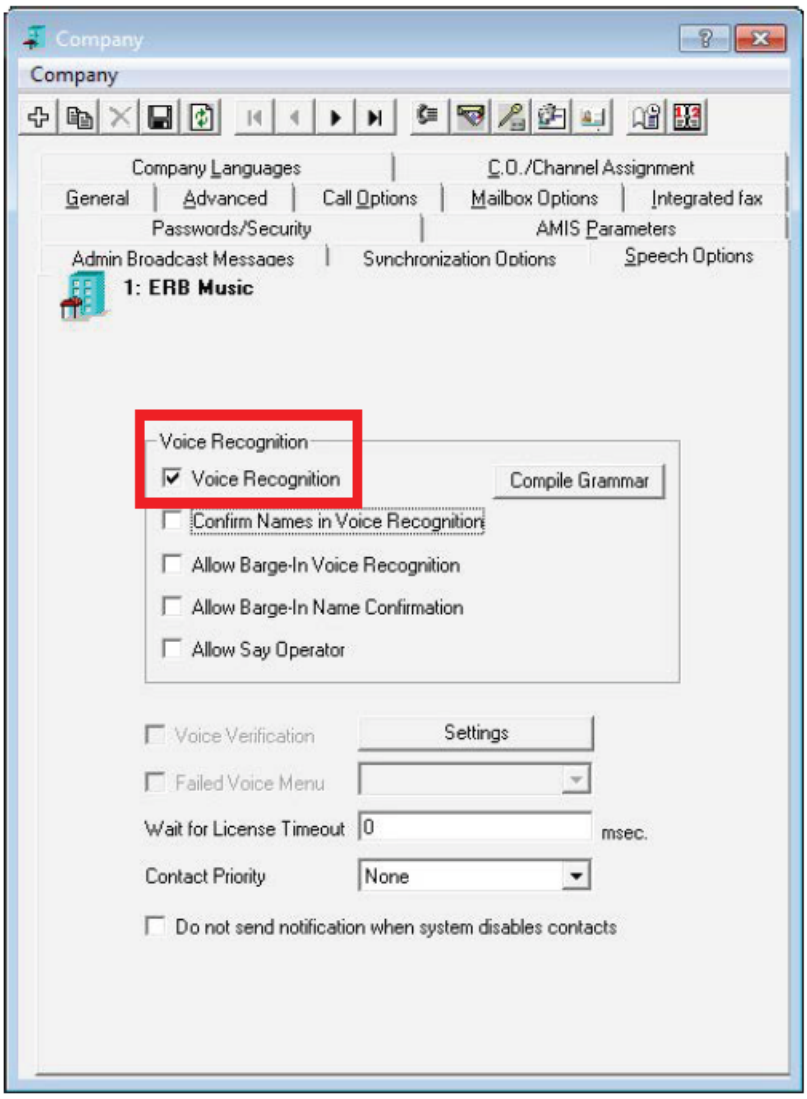
Requirements	Details
License	---
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher

Server Configuration

To enable Speech Commands for the users, Speech Recognition must be turned on at the Company level. This requires an ASR license. Then give permission to the FG and the Mailboxes as appropriate.

Company Properties

Go to **Avaya Messaging Admin > Company,** and on the **Speech Options** tab, ensure that **Voice Recognition** is enabled for the company.

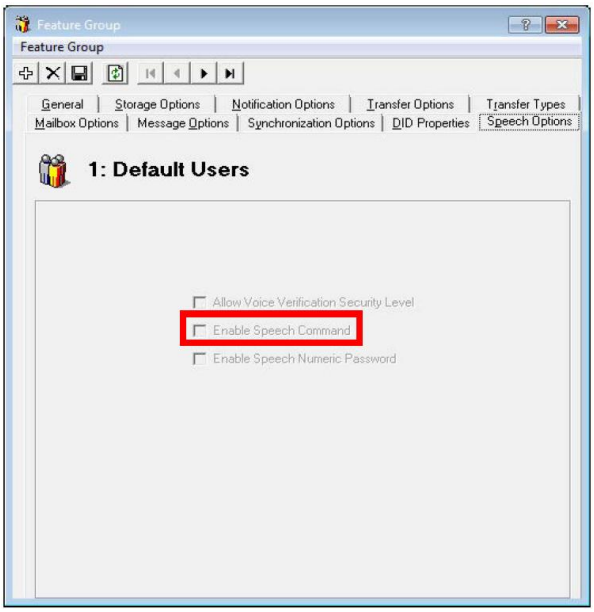


Note: All users that wish to use Speech Commands must be setup under a company that has ASR capabilities.

Feature Group Properties

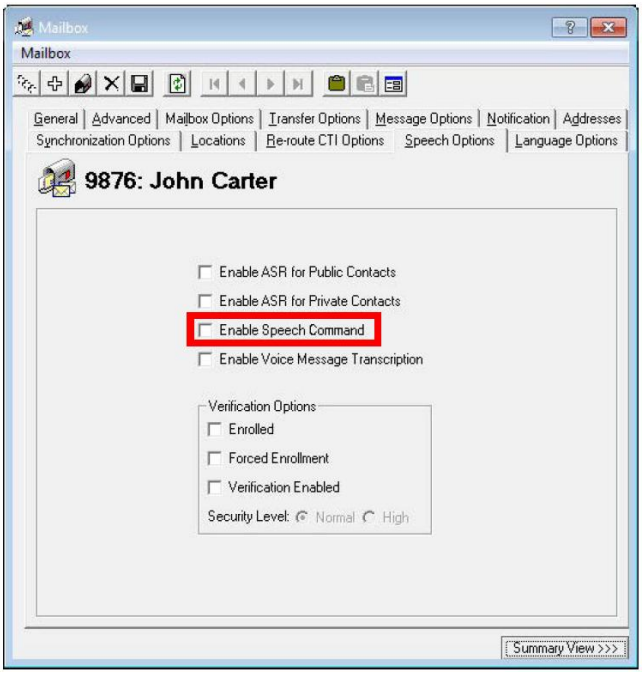
From **Avaya Messaging Admin > Feature Group**, on the **Speech Options** tab, enable the **Enable Speech Command** checkbox.

With this option enabled, individual mailboxes associated with this FG will be able to turn Speech Commands on and off.



Mailbox Properties

From **Avaya Messaging Admin > Mailbox**, on the **Speech Options** tab, enable the **Enable Speech Command** checkbox to allow this mailbox user to use the Speech Command feature. You must repeat this step for all users that wish to use this feature.

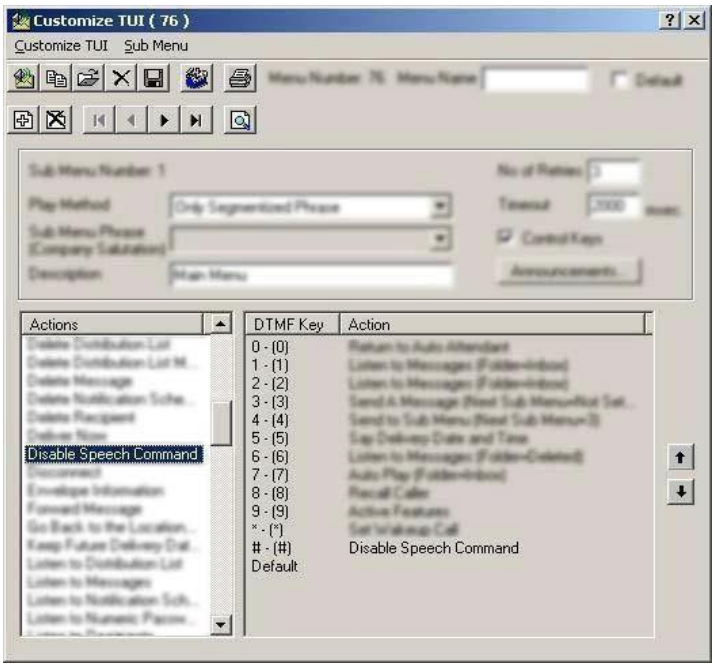


Customize TUI Configuration

Users may occasionally need to turn off the Speech Command temporarily if they are in an environment with too much noise. Voice selection of menu items can be interrupted, or another person's loud voice may be accepted as an entry instead.

To allow callers to temporarily disable this function, add the disabled **Speech Command** action to the TUI that the caller will be using. When a user selects this action from the TUI, the Speech Command feature will be disabled for that session. Users will be able to use Speech Command again the next time they log into the system. Using this action only temporarily disables the feature.

Note: If a user doesn't have access to Speech Command feature, this action will be a null action for them.



User Guide

When you log into the phone system, you may sometimes find it difficult to navigate through the menus using the telephone keypad. For example, if you are using a hands-free head set while driving, having to press the keys on your cell phone can be a dangerous distraction.

To avoid this situation, you can utilize the Speech Command feature which allows you to navigate through the phone system menus without having to press any keys. You speak the number of the commands you wish to send instead of pressing the corresponding button. This allows access to all the options available on your phone system without having to press a single button, giving you a true hands-free telephone experience.

Basic TUI Navigation

When you are given a choice of menu items, simply say the number of the corresponding action.

Warning: **Do not repeat the actual name of the action**. You must say the number of the action instead. It is vital that you clearly say the number. The system will automatically match the sound with a number without confirmation, so to properly navigate through the menus, you must pronounce the numbers as clearly as possible.

Note: Control keys can only be accessed through DTMF input. It is not compatible with speech commands.

Temporarily Disable Speech Command

You may wish to disable the Speech Command from time to time due to the high amount of background noise. If you have the Disabled Speech Command action in your TUI, you will be able to disable the Speech Command feature for a single session. When you select this action, Speech Command will become invalid right away, and the system will only accept telephone key input. The feature will remain disabled until you are disconnected from the system.

Note: When you log into the system again, the Speech Command feature will be available again.

Note: Location of the disabled action will vary depending on the TUI associated with your mailbox.

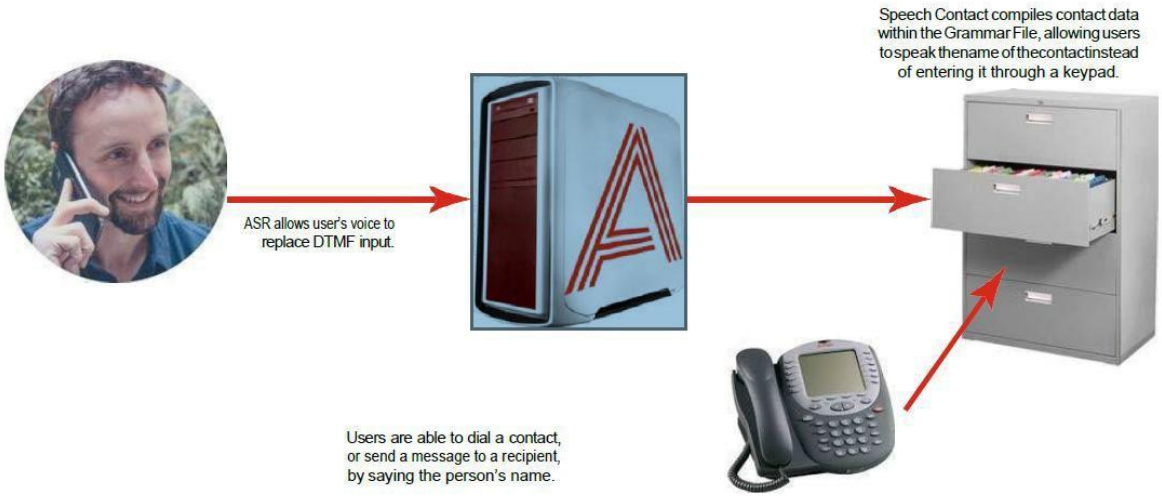
Chapter 4: SPEECH CONTACTS

Introduction

For many business users, their list of contacts can easily grow to such a length that finding any one person can be difficult. To make this easier, the contact list can be speech enabled to allow finding a person through voice alone.

For a user to use this feature, configuration changes must be made on both the server and the client applications. Please follow this guide exactly as explained to enable the speech contact function on your system.

Visual Guide



Having easy access to contacts is essential for people on the go. Spending a few minutes just to select someone to call or to send a message to is not very efficient. **Speech Contacts** makes it easy for users to locate a contact by enabling voice searches. Once the user sets a contact to be speech enabled, they will be able to find that person within the TUI.

Requirements

Requirements	Details
License	ASR
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher

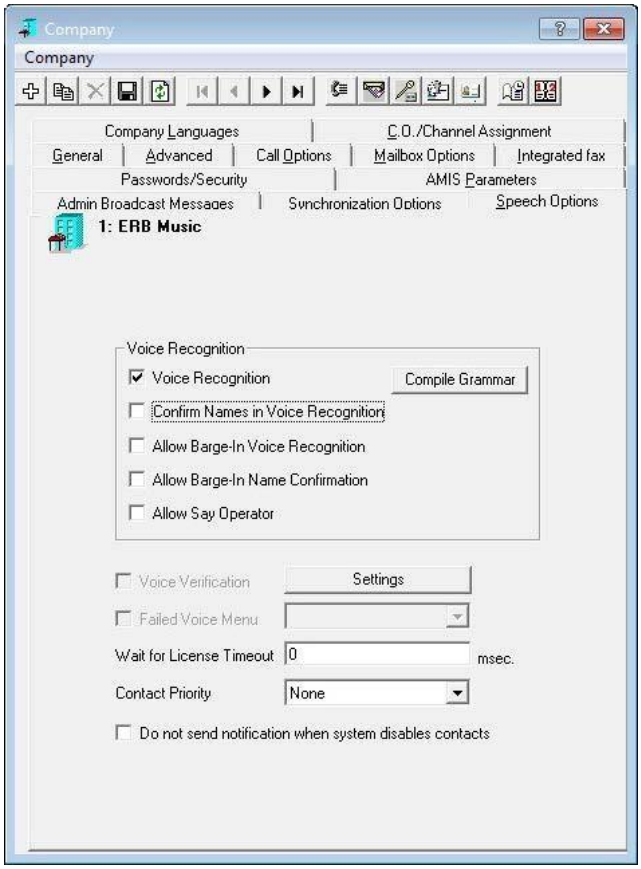
Server Configuration

For the following steps, launch the Avaya Messaging Admin program.

Procedure

1. Go to **Company** properties, and open the **Speech Options** tab. Specify the following:

   - **Voice Recognition**: Enable to activate the ASR engine in the automated attendant.
   - **Confirm Names in Voice Recognition**: Allows the confirmation of the name spoken by the caller.
   - **Allow Barge-In in Voice Recognition**: The caller can interrupt the system (e.g., say "Yes" or "No") during voice recognition.
   - **Allow Barge-In in Name Confirmation**: This allows the caller to interrupt the system (e.g say "Yes" or "No") as it performs name confirmation.
   - Allow Say Operator: The caller can say “Operator” to be transferred to the operator if one has been setup on the system.



2. From the **Contact Priority** dropdown list, select which of your contacts (Public, Private or None) are **more** important when doing speech recognition of contacts.

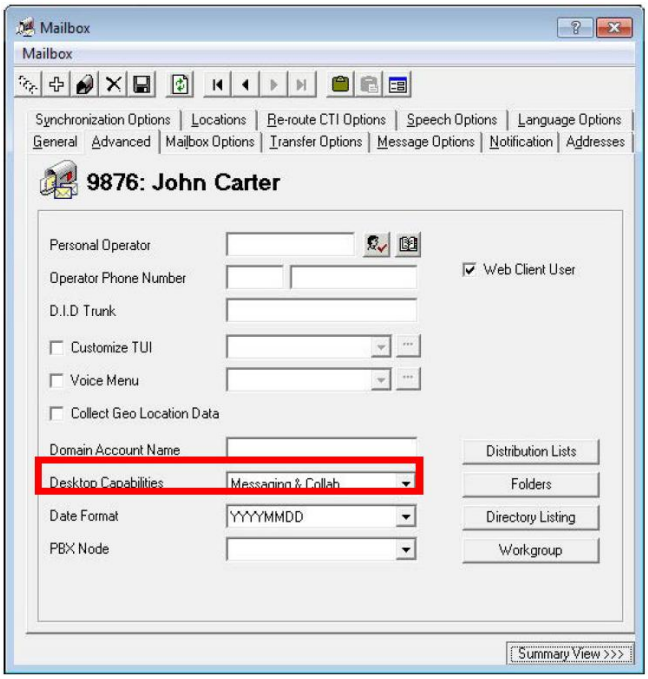
   For example, if in a mailbox you choose to make speeches enable both Public and Private contacts (**Mailbox > Mailbox Options** screen) and the number of users (company mailboxes + private contacts + public contacts) exceeds the number of allowable users on the license; you must disable either **Enable ASR for Public Contacts** or **Enable ASR for Private Contacts** according to the selection you have made in this dropdown list.

For example, selecting **Private** in this dropdown list and disabling **Enable ASR for Private Contacts** on the **Mailbox > Mailbox Options** screen will give priority to public contacts.

3. Save any changes.
4. Open the **Mailbox** of the person who will use this feature. Go to the **Speech Options** tab and specify the following:
   Enable ASR for Public Contacts: Enable to implement ASR capabilities for public contacts.
   Enable ASR for Private Contacts: Enable to implement ASR capabilities for private contacts.



5. Move onto the **Advanced** tab. Ensure that **Messaging & Collab** is selected under Desktop Capabilities.
6. Save the Mailbox settings.


Mailbox
Mailbox
Synchronization Options
Locations
Re-route CTI Options
Speech Options
Language Options
General
Advanced
Mailbox Options
Transfer Options
Message Options
Notification
Addresses
9876: John Carter
Personal Operator
Operator Phone Number
D.I.D Trunk
Customize TUI
Voice Menu
Collect Geo Location Data
Domain Account Name
Desktop Capabilities
Messaging & Collab
Date Format
YYYYMMDD
PBX Node
Web Client User
Distribution Lists
Folders
Directory Listing
Workgroup
Summary View >>>

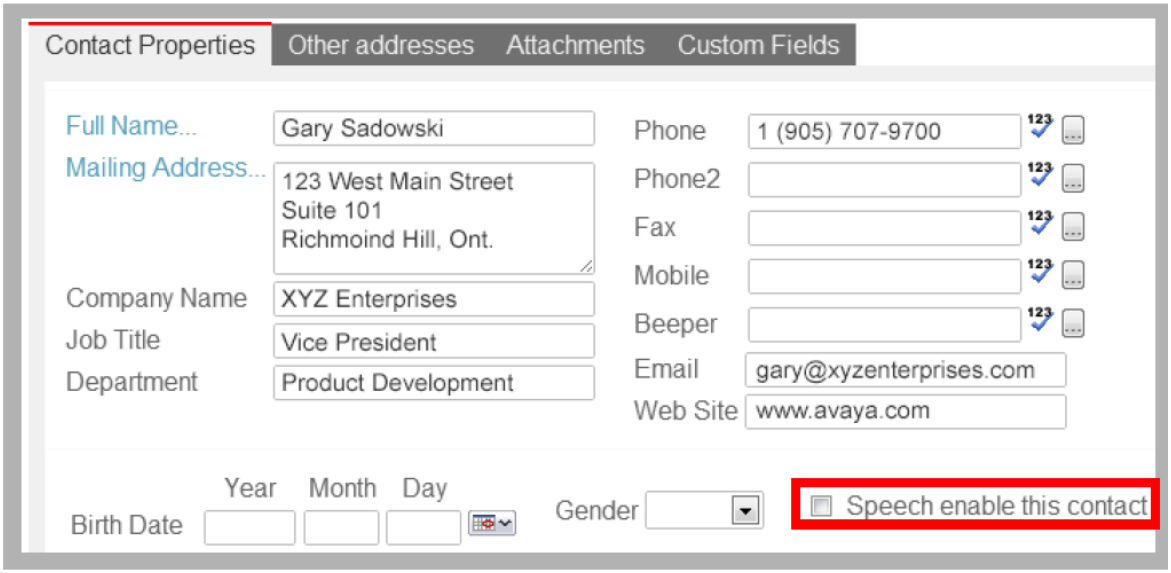
User Guide

Enabling Speech Contacts allows you to quickly and easily get in touch with your contacts through the TUI (Telephone User Interface). Instead of having to enter multiple keys to find a contact, you say the name instead.

Only speech enabled contacts may be accessed through speech. You must ensure that the contacts are enabled for speech before using the feature.

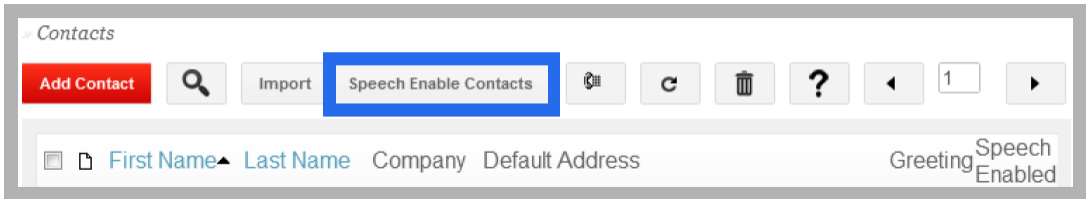
Enabling Speech Contacts

You can enable speech for your contacts individually from each contact's properties.



If you have a long list of contacts, it is quicker to use the batch function.

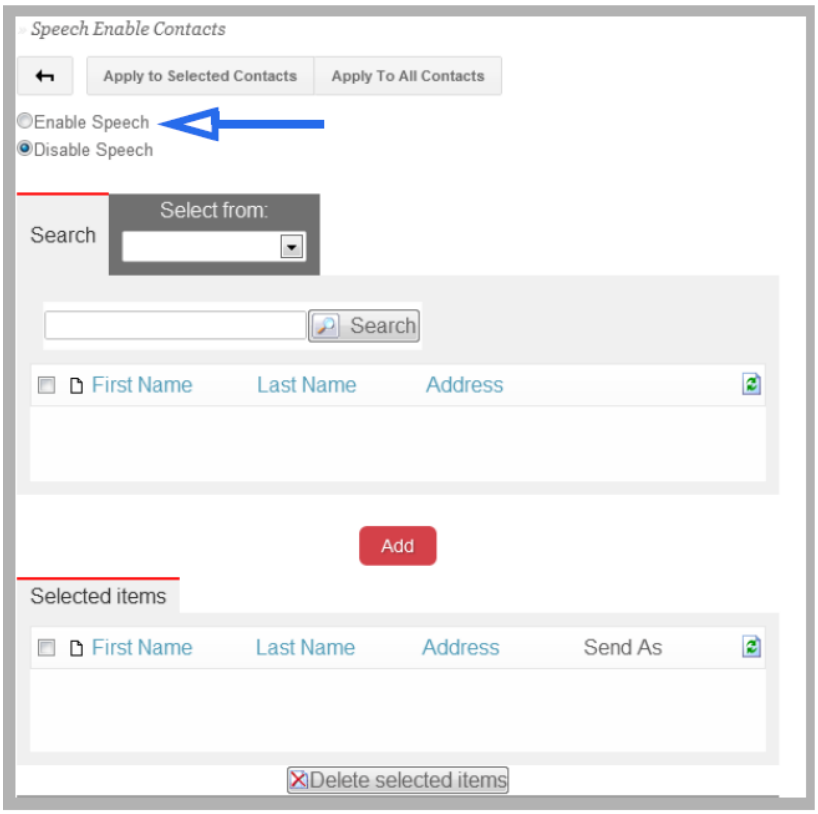
1. Click on the **Contacts** icon, then click on the **Speech Enable Contacts** button.



2. Select the **Enable Speech** radio button.
   If you wish to enable a speech for **all** your contacts, click on the **Apply To All Contacts** button.

   If you wish to enable speech for **only certain** contacts:

3. Populate the uppermost list box with contacts. Choose from the **Select from:** dropdown list, or in the Search field, enter the contact name that you want to add and click the **Search** button.
4. Add contacts from the upper list box to the bottom by enabling the checkbox beside the contact, then clicking the **Add** button.
5. When all desired contacts have been added, click on the **Apply to Selected Contacts** button to apply the changes.



Note: If you wish to disable the speech contact feature for large number of contacts, repeat the above process but choose **Disable Speech** radio button instead.

When you open a contact that has speech enabled, you will see that **Speech enables this contact** is checked. You may freely modify individual entries by enabling or disabling this checkbox.

Chapter 5: WEB LINKS

Introduction

This feature allows you to increase the security level of Voicemail and Faxes that are transferred via email by storing all the files on the server itself. Instead of the attachments being sent and received, the sender's attachment is stored on the server while the receiver gets a link to access the file.

The process below illustrates an example of how this can be implemented. Due to the variation between different sites, following these steps exactly as shown (especially with regards to the URL and folder paths) may **prevent** the feature from working properly on your own system. A professional technician with knowledge of networking knowledge who understands the process would be able to configure the settings necessary for your own system setup.

The configuration procedure will differ depending on the version of your IIS. In general, Windows 2003 and XP will use IIS 6 while Windows 2008 and Windows 7 use IIS 7.

Note: Voice messages which are listened to through the telephone using the Weblinks action link within the email will not automatically change the read status of the voice message. Therefore, listening to message in this fashion will not extinguish the message light on integrated environments. The end users have the option of marking the message as read through the options available at the bottom of the Weblinks message. Performing such an action will extinguish the message light on integrated environments if the message is the last unread message.

Configuration Process

The exact procedure to set up Weblinks depends upon which version of IIS (Internet Information Services) is installed on the server.

Warning: Only follow the procedure that is relevant to your system. Do Not perform both IIS setup procedures.

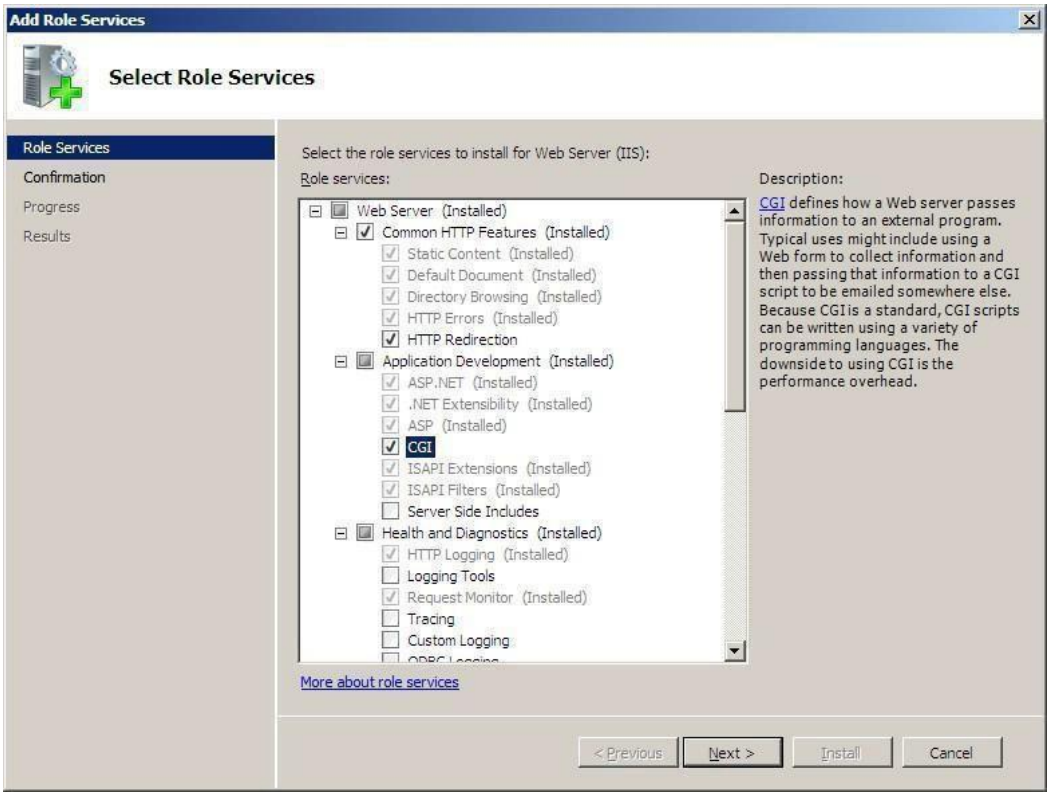
If the server has **IIS 7** installed, begin the process in the section: **Configuration with IIS 7**.
If the server has **IIS 6** installed, begin the process in the section: **Configuration with IIS 6.**

Regardless of which version of IIS is present, the Avaya Messaging setup remains the same. Once the appropriate version of IIS has been configured, continue with the Avaya Messaging setup by following the instructions in the section: **Avaya Messaging Configuration**.

Configuration with IIS 7

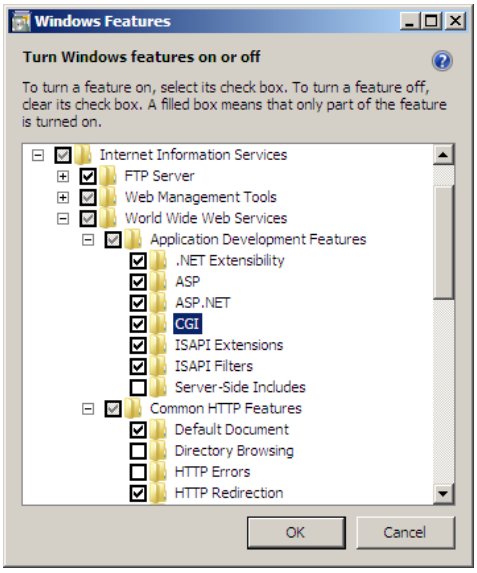
Warning: Use these instructions **only** if you have IIS 7 or later on your system. If you have IIS 6, use the section **Configuration with IIS 6**.

1. To utilize Weblinks, you must first confirm that you have the necessary Windows components installed for IIS. You will need **HTTP Redirection** and **CGI enabled** within IIS.



This image shows adding the component from Windows Server 2008, which occurs under Role **management**.

2. If you are utilizing Windows 7, you will see this screen, available from **Control Panel > Programs & Features > Windows Features.**



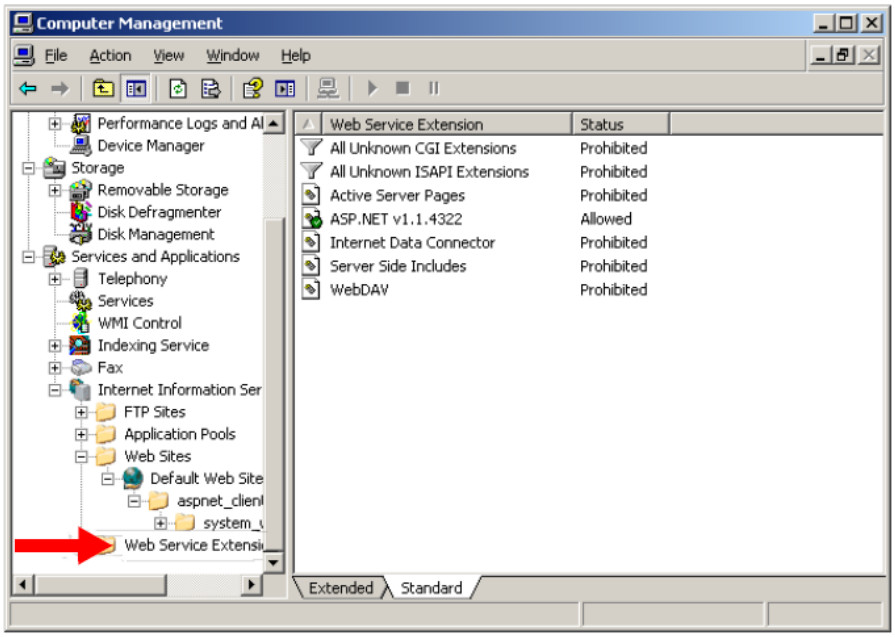
Important: Continue with the section: **Avaya Messaging Configuration**.

Configuration with IIS 6

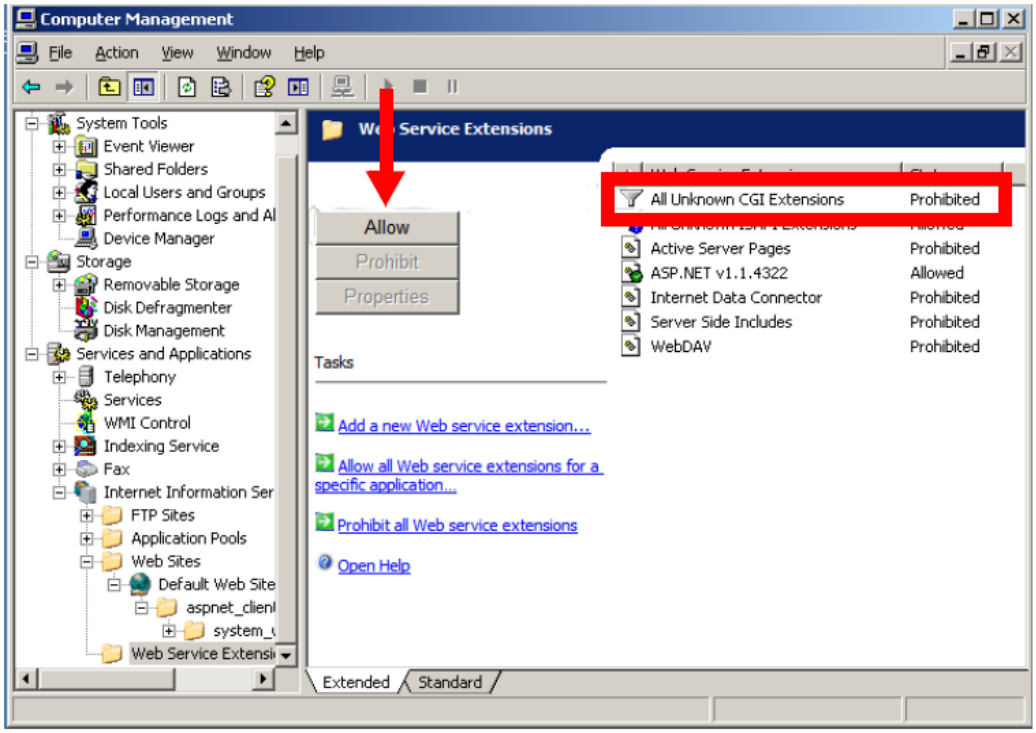
Warning: Use these instructions if you have IIS 6 on your system. If you have IIS7, then use the section: **Configuration with IIS 7.**

1. Open the Start menu.
   Right-click **My Computer** then choose **Manage**.

2. On the left-hand side, select **Web Service Extensions.**

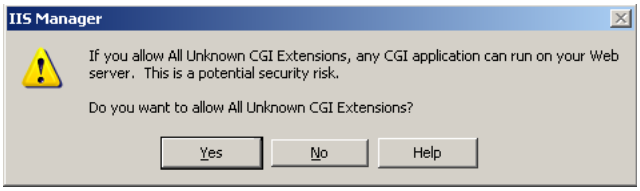


3. On the right-hand side, select **All Unknown CGI Extensions.**
   Click **Allow**.



4. You will get the following warning. Click **Yes** to accept the changes and continue.

5. Repeat steps step 1- step 4 for **All Unknown ISAPI Extensions**.

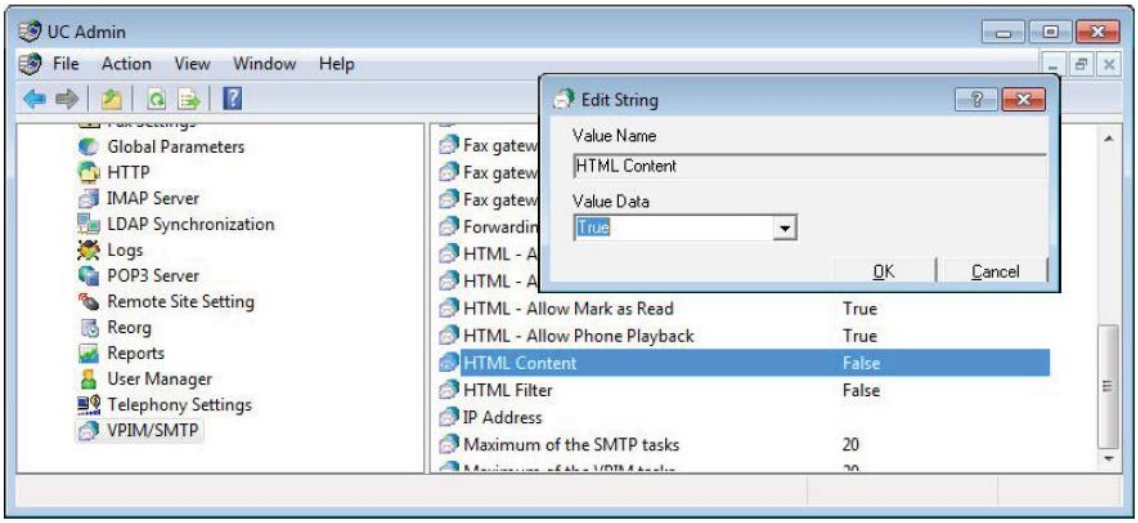


Important: Continue with the section **Avaya Messaging Configuration**.

Avaya Messaging Configuration

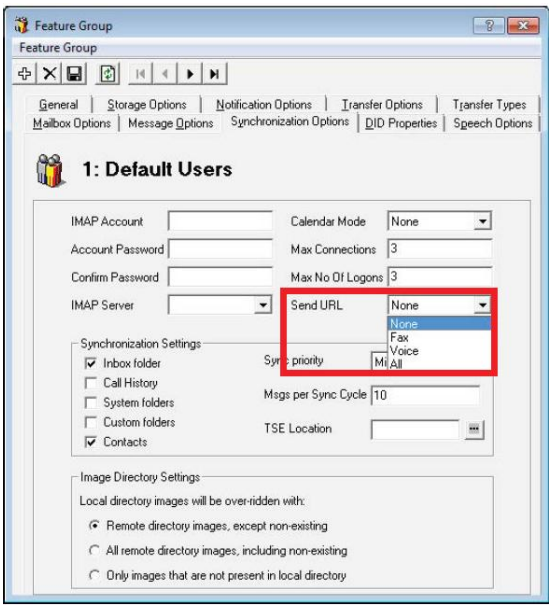
Once the appropriate version of IIS has been setup, continue with the Avaya Messaging configuration.

1. From **AM Admin > Configuration > VPIM/ SMTP**, change the value of **HTML Content** to **True**.



2. In order to utilize the Weblinks function, the **mailbox has to be associated with the Feature Group** that has the function enabled.

   From **Avaya Messaging Admin > PBX > Company > Feature Group**, go to the **Synchronization Options** tab and select the type of messages you wish to use Weblinks with from the dropdown menu.



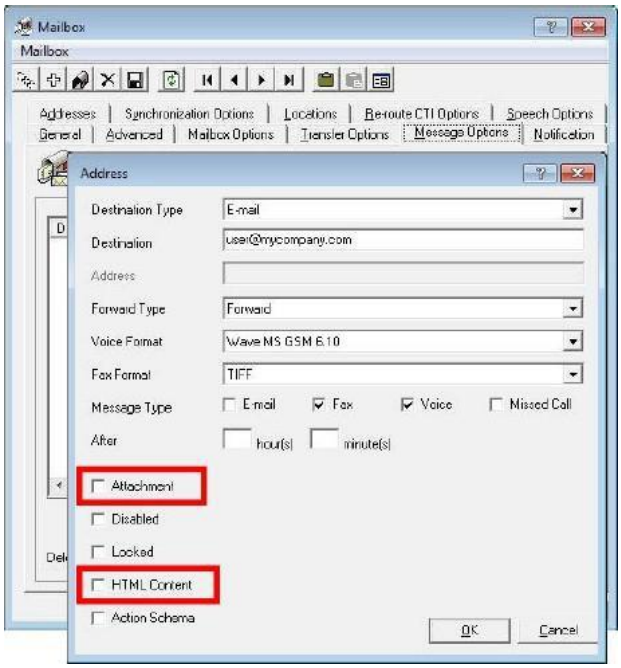
3. If a user does not utilize IMAP CSE Synchronization between their Avaya Messaging mailbox and the mail server account, you may opt for the forwarding method.

   From **Avaya Messaging Admin > PBX> Company > Mailbox**, open the properties of the mailbox

you wish to enable Weblinks for, then go to the **Message Options** tab.

Create an entry to forward the emails. When the mailbox is associated with the **Feature Group that has the Weblinks enabled**, as shown in the previous step, you can enable the **HTML Content** checkbox. Be sure to leave the **Attachment** checkbox disabled if you wish to send the URL only.

Warning: Please keep in mind that this step is **only for users who will be using email forwarding instead of IMAP CSE Synchronization**. If you configure forwarding for users who are Using IMAP CSE Synchronization, there will be an infinite loop of messages. You should either use IMAP sync or forwarding but never for the same mailbox.

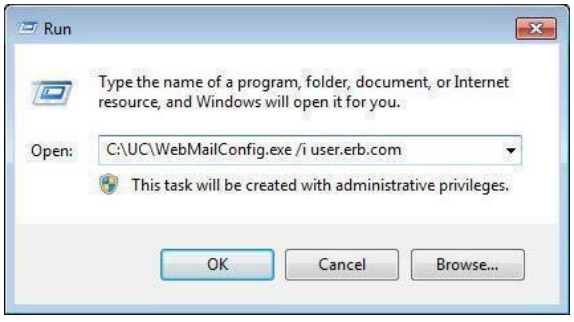


4. When all your server-side configuration has been completed, **restart the server computer**.

5. Locate the webmailconfig.exe file in the Avaya Messaging folder (by default, this is C:\UC).

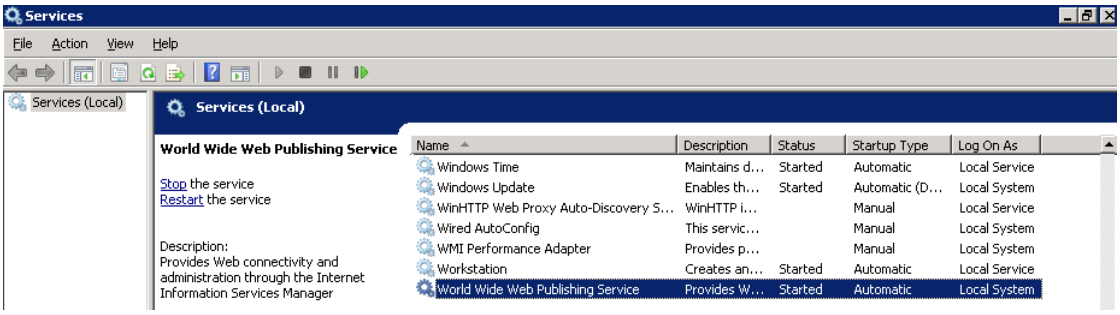
   From Windows, go to **Start > Run** and enter the full path and file name in the space provided. Add the /i parameter, and the URL of the server where the files will be kept.

   For example: **C:\UC\webmailconfig.exe /i user.erb.com**



Click **OK** and the program will automatically configure the remaining settings.

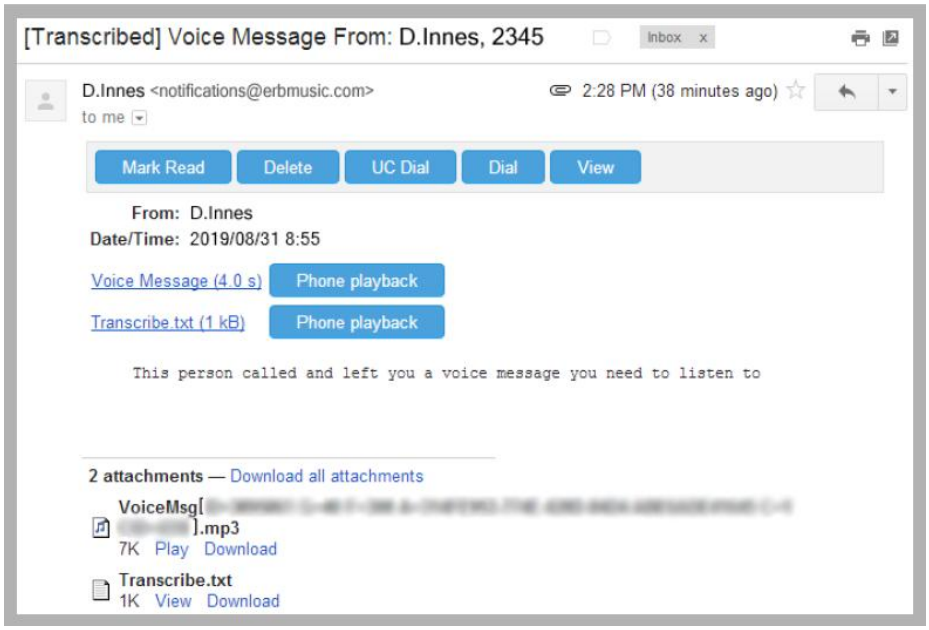
6. Stop and restart the **World Wide Web Publishing Service** on the computer to complete the setup.



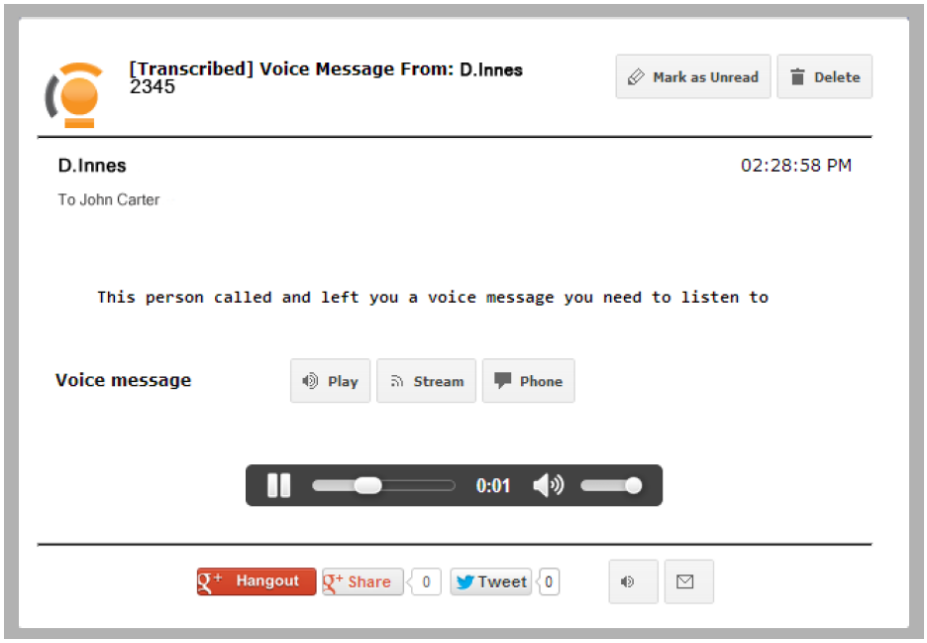
Weblinks Example

The following is an example of how the attachments are handled using this function. The email itself only contains the text of the message. The attachment is left on the server. If you were to forward this email to someone with no permission to access the mail server, they would not be able to listen to the message. While the email is forwarded, the attachment itself remains secure on the server.

By using the **Playback** buttons, the voice message can be played through the current device, or the telephone associated with the user's default extension. Additional buttons allow the message to be **Mark Read** or **Deleted** from the voice server. A call to the sender can also be initiated by clicking the **UC Dial** (dial through the Avaya Messaging voice server) or **Dial** (dial through a configured device, such as a cell phone when out of the office) buttons.



The **View** button opens a new window in the browser. This window contains playback controls for the message.



Fax messages processed through Weblinks will behave in the same manner. The attachment remains on the server while only links to view the message are sent to the user.

Chapter 6: EMAIL ACTION SCHEMA

Introduction

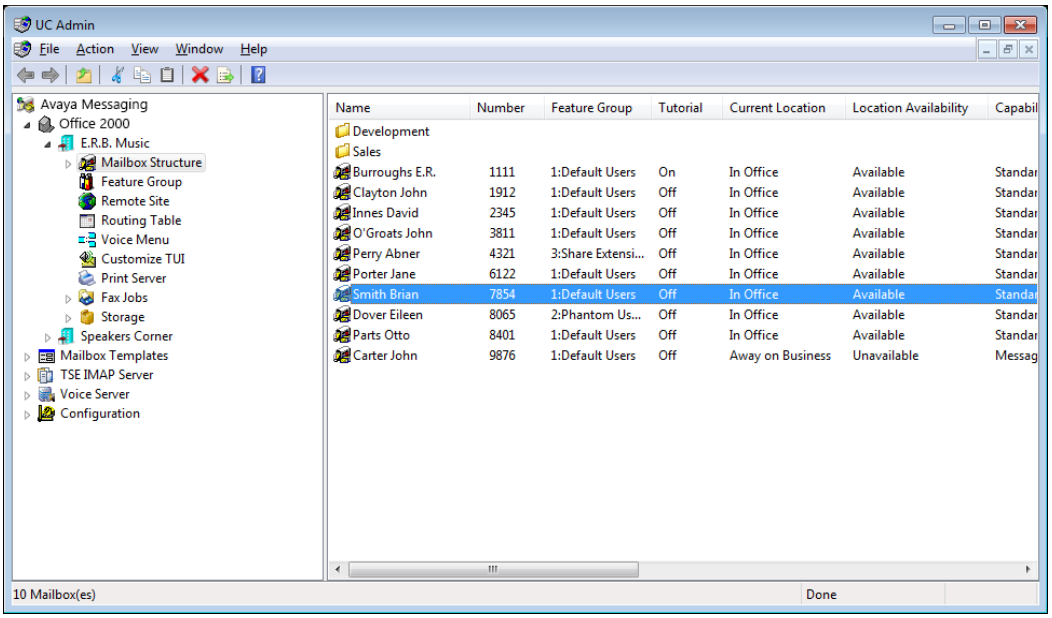
The **Action Schema** option causes tags to appear in the subject line of emails that contain voice messages, or those that denote missed calls. Users can click on these buttons to playback voice messages, or to immediately place a telephone call to the contact.

Warning: This feature is only compatible with email programs that support **DKIM verification**.
Warning: Actions Schema is not supported on systems using **IMAP Synchronization.**

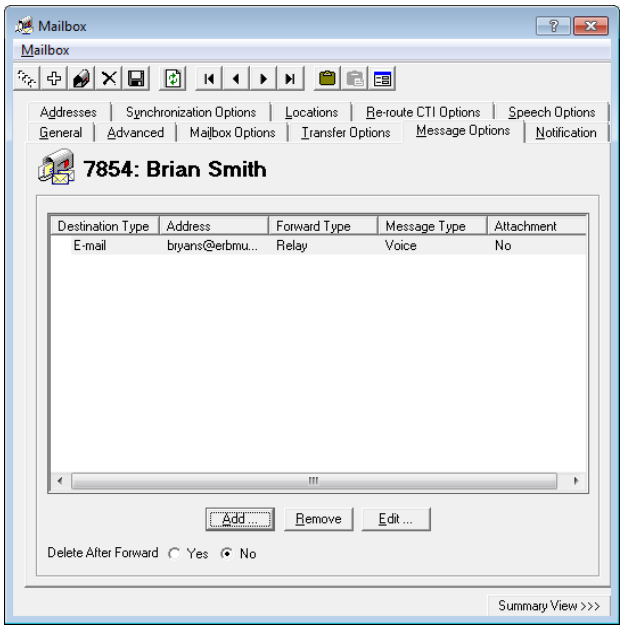
Enable Action Schema

Turn on the Action Schema option through the Avaya Messaging Admin program.

1. Start Avaya Messaging Admin and open the **Mailbox** folder.

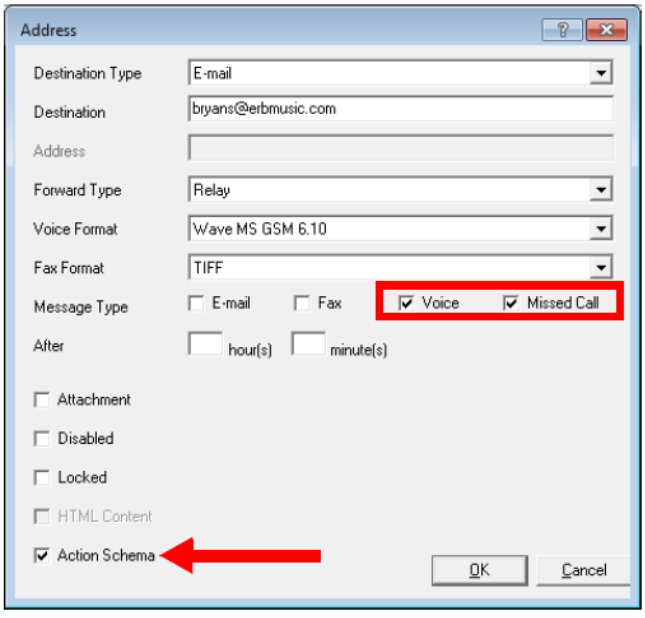


2. Double-click one of the listed mailboxes, and open the **Message Options** tab.



3. Click **Add** to create a new **Address** or select an existing address and choose **Edit**.

4. Select which **Message Types** (voice and missed calls) will add a tag to the message in the email subject line. Configure the remaining settings as required and enable the **Action Schema** checkbox.



5. Click **OK** when finished.

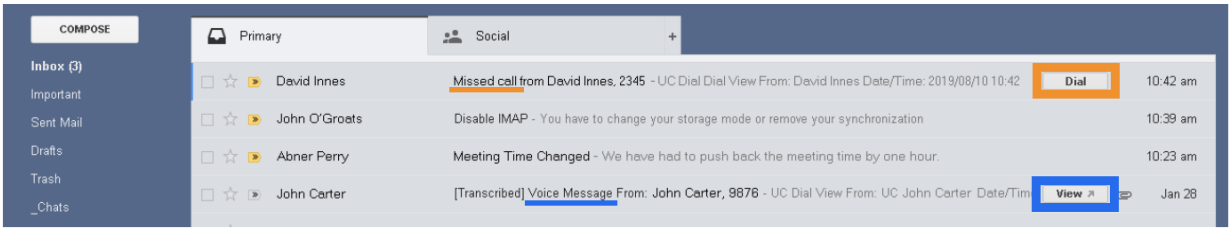
   Hint: For complete details for all of the items in the Addresses window, refer to the **Add / Edit Message Options.**

6. Save the change to the mailbox.

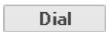
Email Buttons

Once the feature has been enabled, incoming calls that are not answered will cause a button to be added to the subject line in the email header of your client.

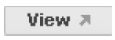
For calls where the contact leaves a voice message in the mailbox, a **View** button will appear beside the message. If the caller did not get an answer and chose not to leave a message, then the **Dial** button will appear.



Note: In the examples that follow, when initiating a telephone call to the contact, the device currently selected is used. The current device is defined within your location setup. For example, if your current location is **Mobile**, the call will ring on the device configured for that location (i.e., a cell phone). If you are **In Office**, your desktop phone may be used instead.

Dial 

The Dial button will start the dialer and place a telephone call to the contact using the currently selected device**.**

View 

Clicking the **View** button will open a window where the voice message in the inbox can be played back over any audio-enabled device.

If licensed, the transcription of the message will also be included in the playback window.

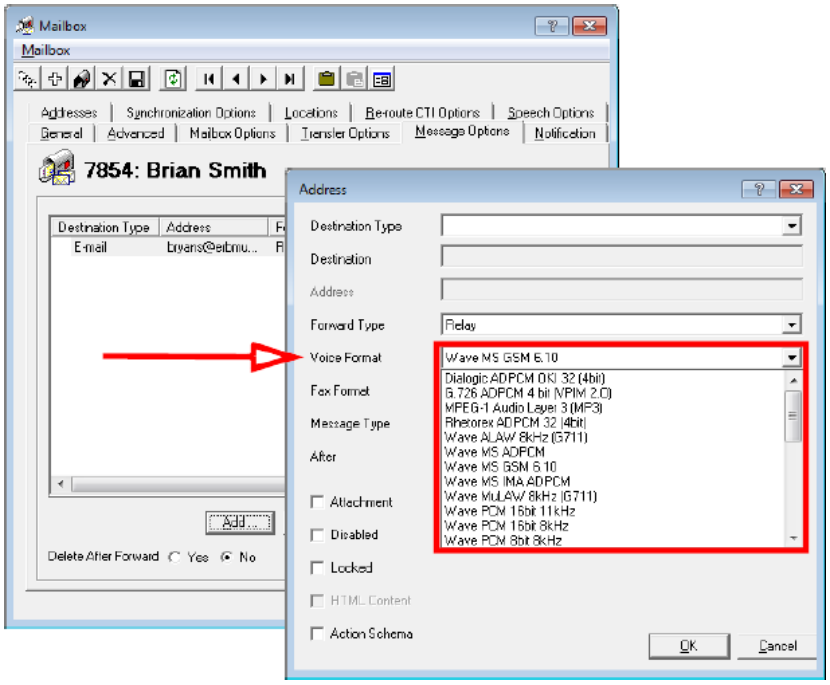


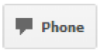
Play

Choose **Play** to have the voice message converted to MP3 format and played through the browser.

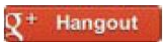
Stream

Choose Stream when the browser player does not support the MP3 format, or if a different format is preferred.
The audio file will be played using an appropriate viewer, using the **Voice Format** specified in Avaya Messaging Admin on the
Mailbox > Message Options tab under **Add/Edit**.

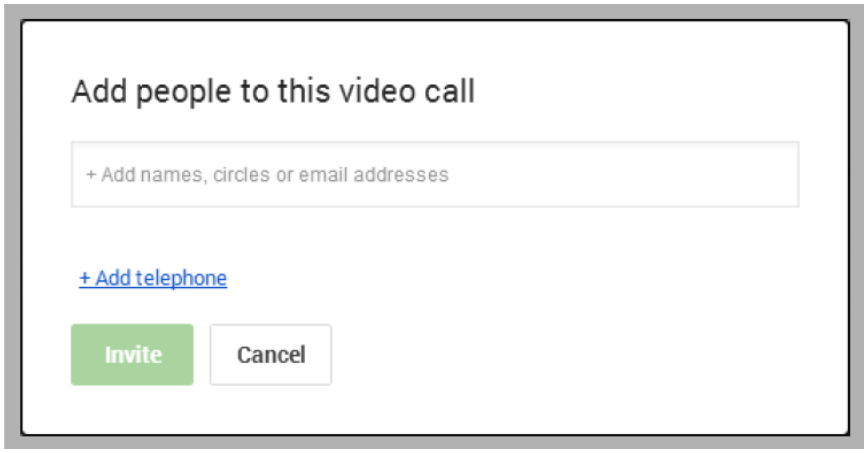


Phone 

Select this option to playback the message on the current default telephone device. The device will ring, and playback will begin through the handset/speaker.

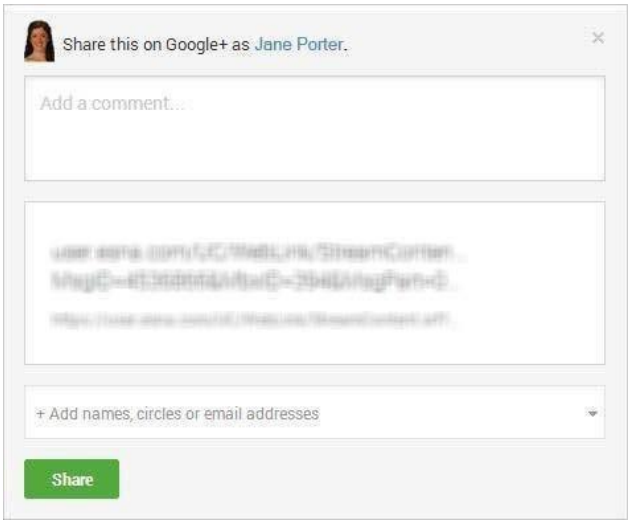
Google+ Hangout 

Click on **Google+ Hangout** to create a video call in the default browser. Enter the contact's name or number into the space provided to start the event. Click **Invite** to send an invitation to join the hangout to the contact's Google+ account. The contact must be logged into their account to receive the invitation.



Google+ Share 

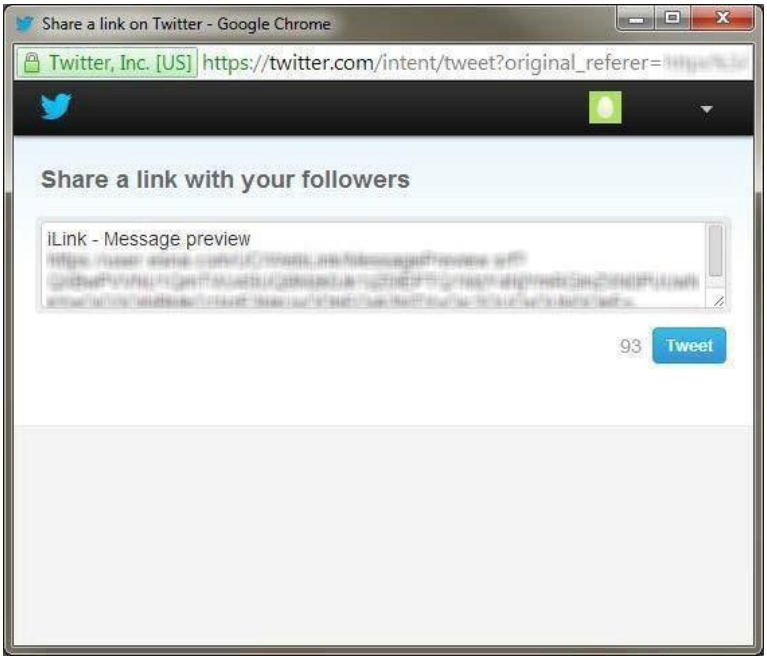
Choosing **Google+ Share** allows the user to share the message with others through their Google+ account.



Enter a comment and the contacts to share the file with. Click **Share** when ready.

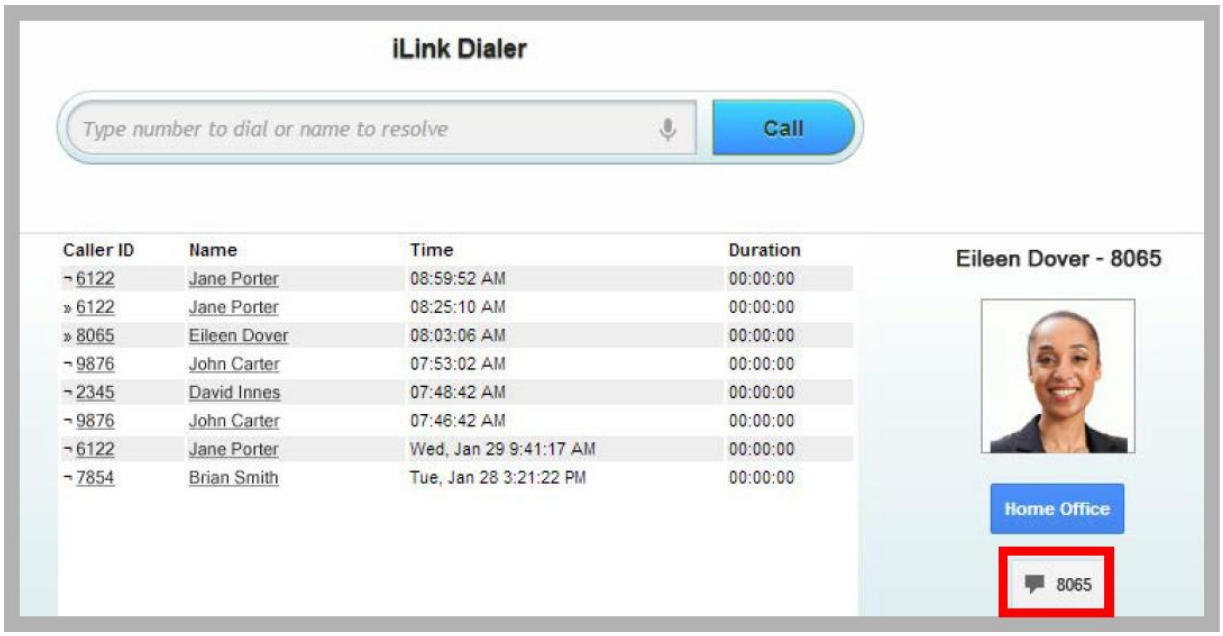
Twitter 

The **Tweet** button allows the user to share the audio file with their Twitter followers.



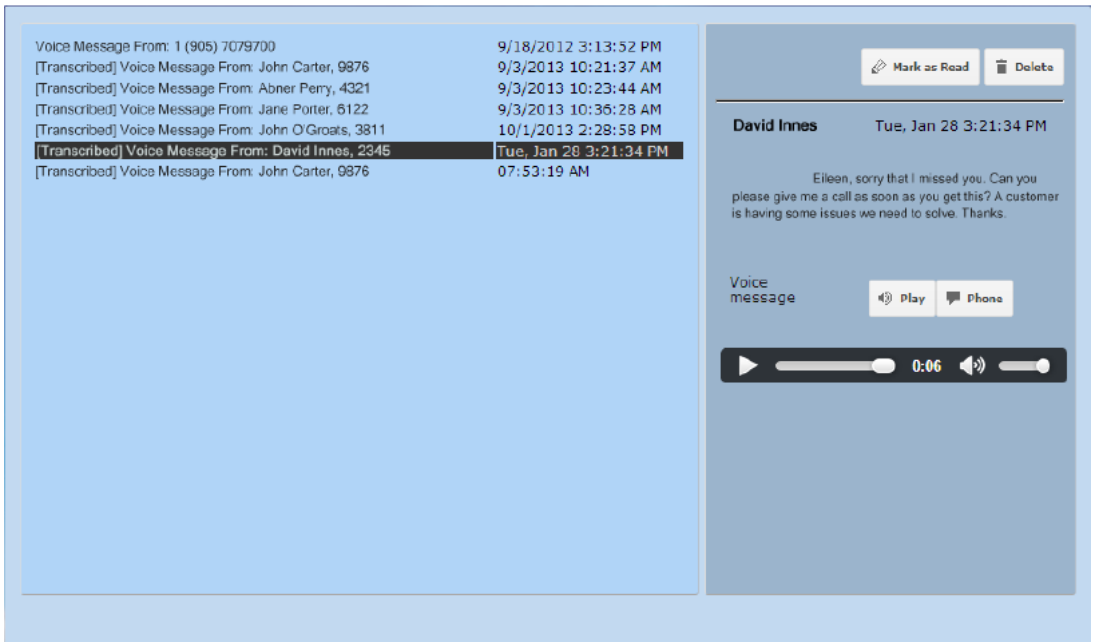
Dialer

Dialer opens a log displaying all calls made to and from the mailbox. Details include the caller's extension or phone number, the caller's name, and the time, date and length of the call.
Click on a contact or their number to open their popup card. In window, click the contact's number to place a call. Your default telephone device will ring, and you will be connected to the contact.



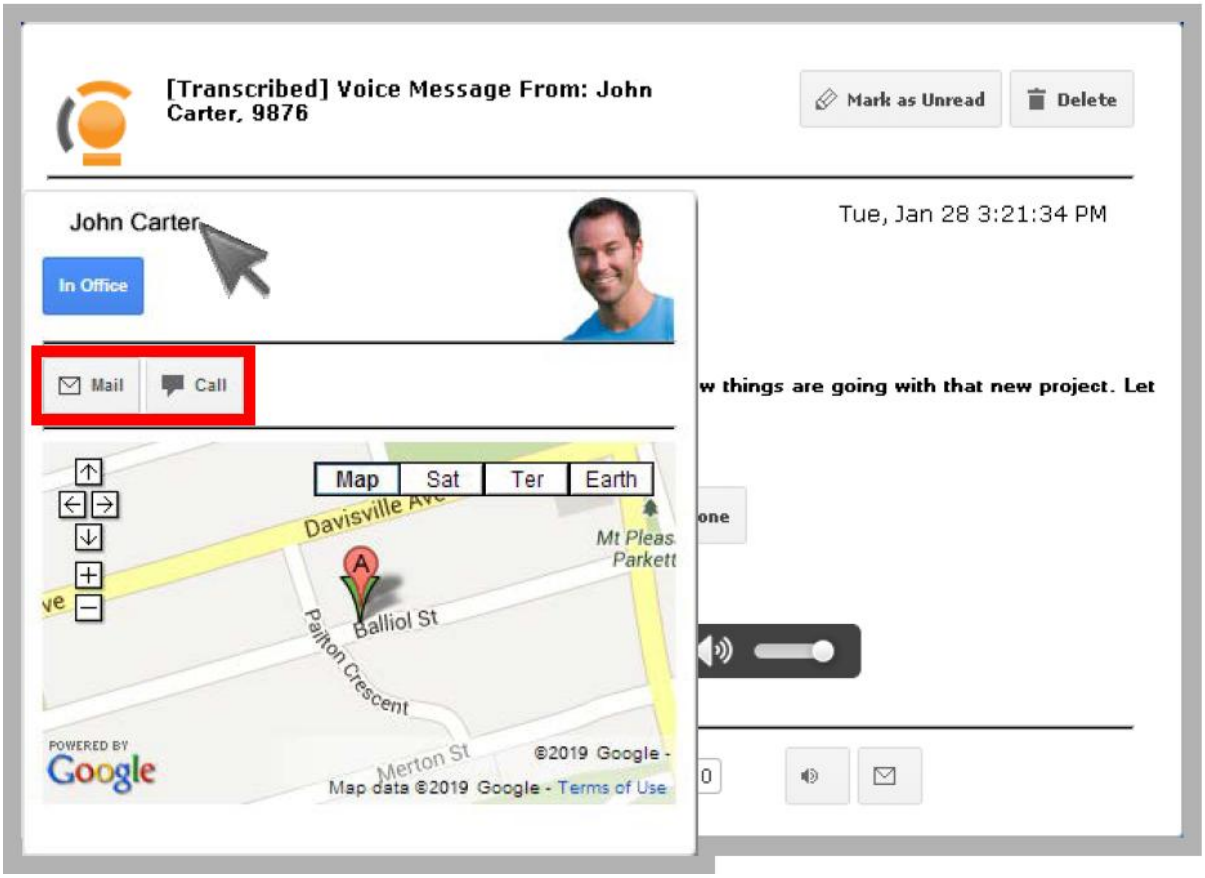
Messages

Messages opens a list of voice messages left in the mailbox. Details include the name of the contact who left the
message, their number or extension, and the date and time the message was received.
Click on an item to playback the message.



Contact Location

In various places through the window, moving the mouser over the contact's name will open a new window which shows their current location in Google Maps, if they have the Geo Location option enabled. There are also icons to contact them through email or telephone.



Mail: Opens an email client program to compose and send an email message to the contact.
Call: Places a telephone call to the contact. Your desktop telephone will ring, and you will be connected with the contact once they answer.

Chapter 7: MUTARE TRANSCRIPTION SERVICE

Introduction

Note: Transcription provides text output from voice messages left in a user's mailbox. The user will receive an email with the transcribed text of the message.

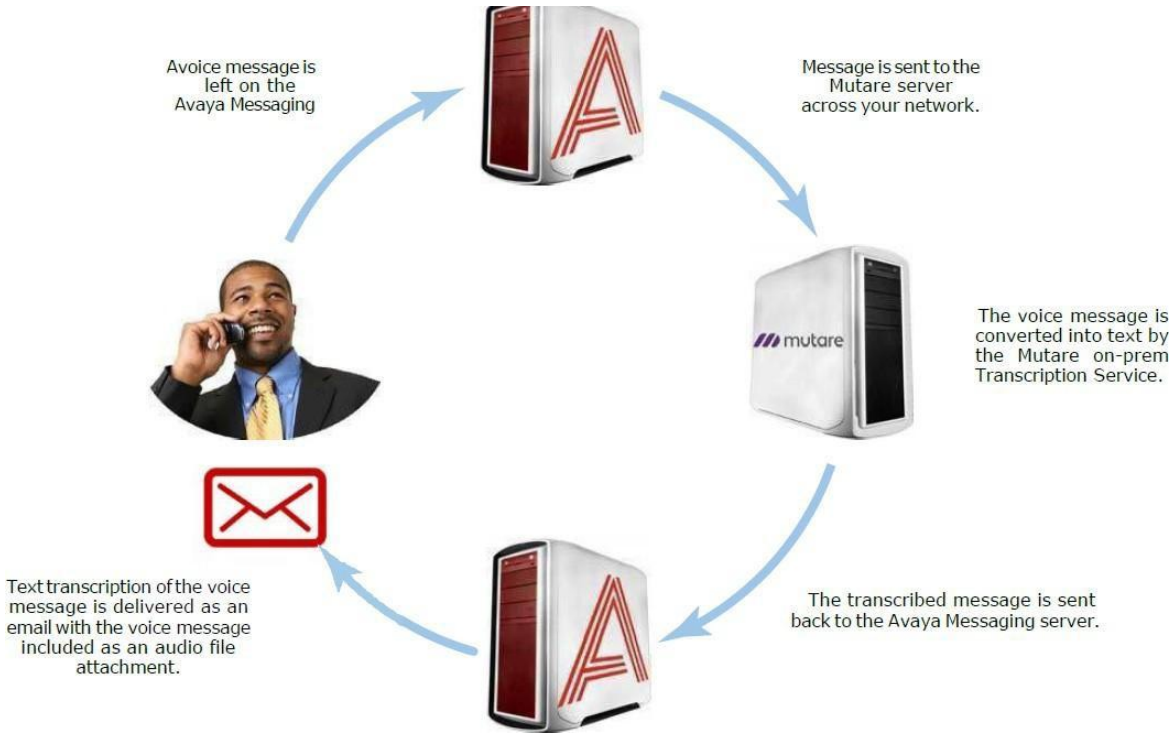
The Transcription feature allows users to receive text output from voice messages. The transcribed voice message is delivered to the user in the body of an email.

Transcription is not part of the standard Avaya Messaging license. It must be purchased separately. Licenses Mutare Transcription Services are available through Avaya.

This chapter describes the configuration for the Mutare on-premise transcription service. Mutare will provide the necessary software to the client and assist with the installation and configuration.

Important: The transcription service is available only to accounts with Messaging and Collaboration (Avaya Mainstream) Desktop Capabilities. An account with Messaging (Avaya Basic) alone will not have access to this feature. Desktop Capabilities are configured in Avaya Messaging Admin on the Advanced tab for each mailbox.

Visual Guide



When a voice message arrives on the voice server, the message is passed to the Mutare transcription server across the corporate network. The message is then returned to the voice server once the transcription has been completed. The voice and text messages are combined and delivered to the user's mailbox.

Hint: Transcribing a voice message will take some time depending upon the length of the message and the amount of traffic on the servers. If receiving a voice message immediately is critical for a user, it is recommended either that transcription is turned off for that user, or that time out settings are configured to ensure messages are delivered within an acceptable time limit.

Requirements

Requirements	Details
License	Mutare Subscription available from Avaya
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher
Hardware	A computer that meets Mutare server requirements.

A Mutare transcription service subscription.

- The Mutare software resides on the corporate network on its own machine. Ensure that a suitable computer is available to host the transcription service.

Licensing

The transcription feature is not included with the standard Avaya Messaging license but is available as an option from Avaya. These instructions are only required if a Mutare transcription license is purchased after Avaya Messaging is installed and configured.

Once you have purchased a license, it must be activated through the UC License Upgrade Utility. The service must then be configured through the Transcription Configuration Tool.

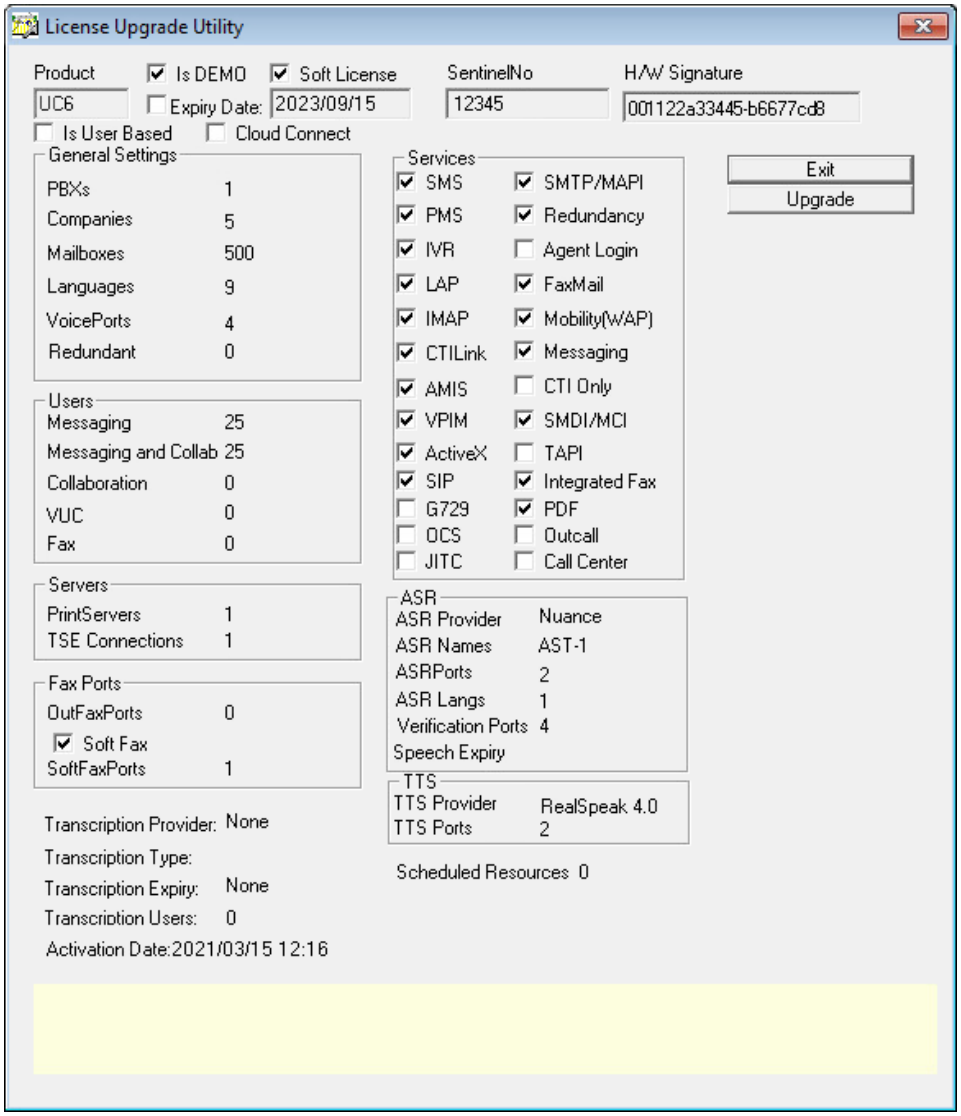
Note: If this is a first-time installation, and not an upgrade to an existing system, skip ahead to the **Avaya Messaging Server Configuration**.

Upgrading the License

If Avaya Messaging has already been installed and setup on a server, add a transcription license by following these steps. If this is a new installation, skip ahead to Avaya Messaging Server Configuration.

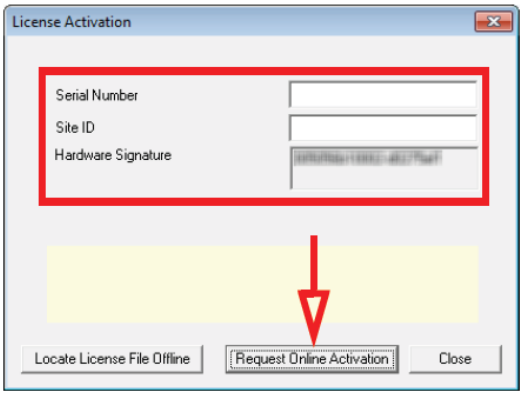
1. On the Avaya Messaging server, go to **Start > All Programs > Avaya Messaging > UCLicenseUpgrade**.

2. The **License Upgrade Utility** screen appears. Click **Upgrade**.

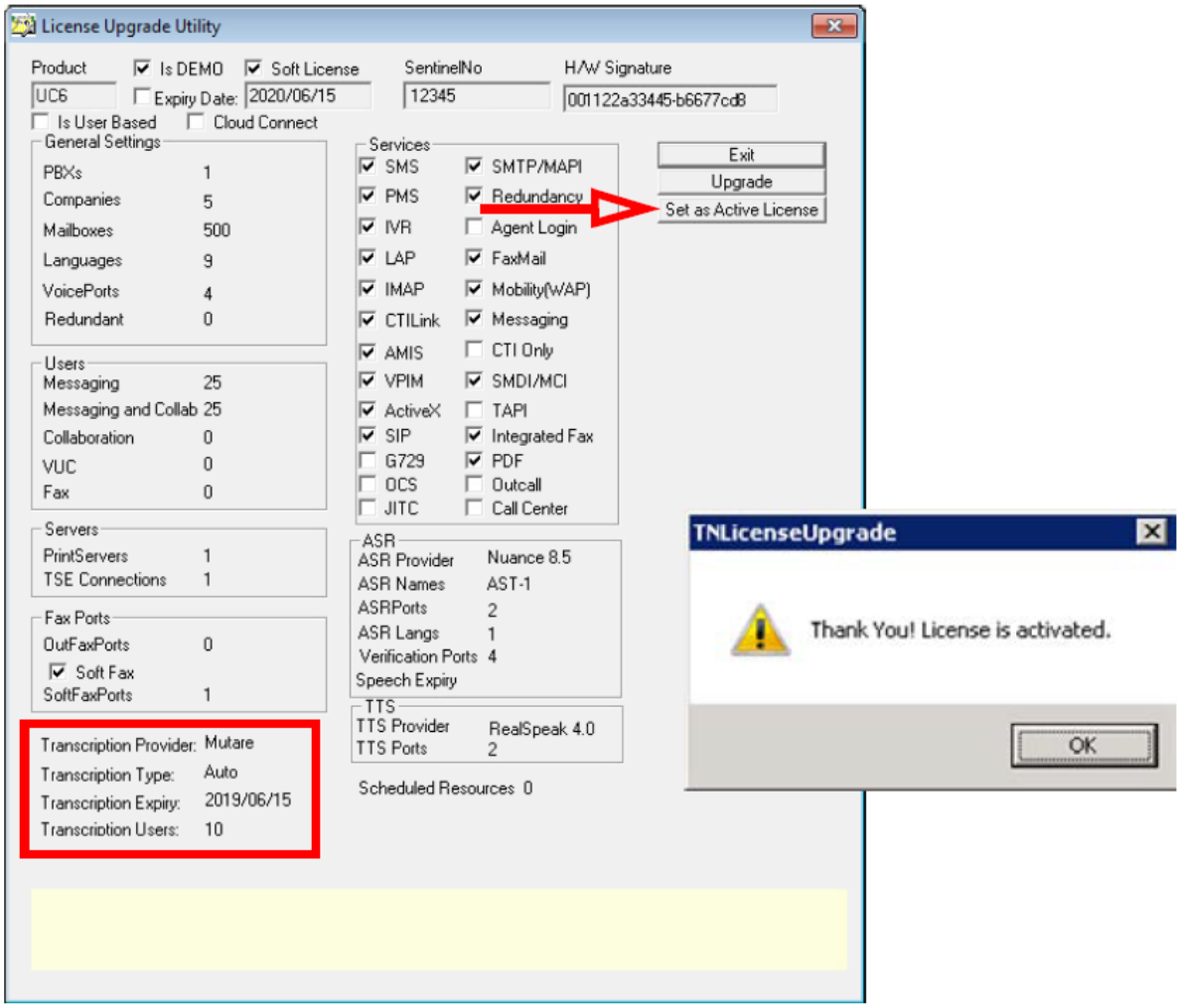


3. The Serial Number and Site ID will already be entered. If not, enter the data manually:
   Serial Number: Enter the serial number for your Avaya Messaging license.
   Site ID: Enter the site ID for your location.

   Both items are provided by Avaya as part of the initial Avaya Messaging license package



4. Click **Request Online Activation**.
5. The license will be updated from Avaya's online license server to include the latest features. Click **Set as Active License**. Click **OK.**



6. Restart the server to complete the update.
   Your transcription license is activated.

Avaya Messaging Server Configuration

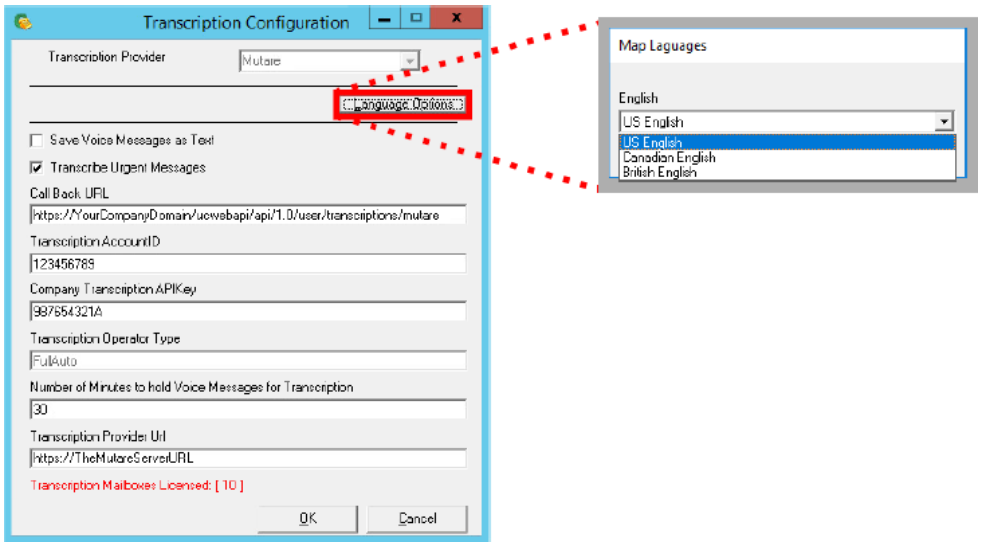
Avaya Messaging must be configured to communicate with the Mutare server over the corporate network. This applies whether this is an upgrade or first-time installation.

Note: The settings made here are system wide, applying to all accounts on all companies.

Transcription Configuration Tool

1. On the Avaya Messaging voice server (in an HA installation, on the Primary and all Secondary voice servers), go to **Start > All Programs > Avaya Messaging > UCTranscriptionConfig**.

2. Enter all required information.



Save Voice Messages as Text: Enable to mark voice messages as text messages after transcription. Leaving this unchecked will have the messages marked as voicemail in your mailbox once transcribed.

Transcribe Urgent Messages: Disable this checkbox to exclude messages flagged as Urgent from the transcription service. Transcribing a message can take several minutes so this option allows urgent messages to be delivered immediately without transcription.

Call Back URL: This is the externally (Cloud-based) or internally (On-premise) accessible URL of your Avaya Messaging server (in an HA system, this will be the Primary Consolidated server) where Mutare will send completed transcriptions. You can configure your DNS and change “YourCompanyDomain”only (i.e.from “https://YourCompanyDomain/ucwebapi/api/1.0/ user/transcriptions/mutare” you only need to change “YourCompanyDomain”) since the virtual folders and the transcription receiver applications are automatically setup.

Transcription AccountID: Enter the Mutare account information provided by your vendor.

Company Transcription APIKey: Enter the Mutare API key provided by your vendor.

Transcription Operator Type: Not applicable for a Mutare configuration.

Number of Minutes to hold... : Voice messages for selected mailboxes are put on hold until the transcription is returned from the Mutare server. This value (in minutes) tells the system when to give up waiting for a transcription and deliver the message as voice only. The default value

is 15 minutes.

Transcription Provider URL: Enter the URL to reach Mutare on-prem server on the corporate network.

3. Click **Language Options**. From the dropdown list, select a language / variation to use, then click **OK**.
   Important: This field must not be left blank. There must be a language selected here.

4. Click **OK** when it's finished.

Verification

Once all of the information has been collected and the network adjustments are made, the connection between the customer's network and the Mutare on-premises transcription server should be tested by sending a service request through Avaya Messaging and waiting for the response.

Any issues or unusual delays must be reported immediately so that the situation can be resolved.

User Guide

When a new voice message is received:

1. The system checks if the mailbox has transcription enabled.
2. If so, it uses the **UCTranscribeUploader** service to submit the voice file for transcription. The Callback URL is also sent to allow the Mutare server to reply with the results.

Note: The original message is put on hold for an amount of time defined by your administrator. The default value is 15 minutes. This means that the UC system will send the message to the transcription service and then wait for a maximum of 15 minutes for a response.

If the message has not been returned at that time, the process will time out and the transcribed voice message will be sent to the mailbox. You should be aware of the delay so that no problems arise from it.

3. Once the transcription is complete, the Mutare server will use the Callback URL to return the results to the UC system. The transcribed text will be the body of an email with the original voice message included as an audio attachment.
4. The combined message is delivered to the user's mailbox.

Note: There is no limit to the length of the message being transcribed unless set by the system administration. It is recommended that Avaya be informed if the enterprise consistently requires transcription of messages longer than 10 minutes as additional processing resources should be allocated. For example, a 60 second message may have 95% confidence score in the transcription, while a ten-minute message may drop significantly.

This is not a failing of the technology, as most voicemail systems do not record high fidelity or quality can be degraded with poor connection, voice quality, or background noise which can affect the transcription confidence.

Chapter 8: GOOGLE INTEGRATION

Guidelines

Depending upon your site's requirements and software, you have the option to integrate Avaya Messaging with several email systems. None of these are required. Where appropriate, refer to the chapter that best suits your requirements.

Introduction

Avaya Messaging transforms the way you handle online communications. With Avaya Messaging you can access voice and IM communications, presence, click-to-call, location sharing and other communication tools inside the cloud applications you work in regularly like Gmail, Google Calendar, and other Google Apps.

Avaya Messaging also offers:

- **Message Integration**: Avaya Messaging can synchronize messages with Google Apps and Gmail servers, allowing users to access a single endpoint to manage all their messages. All the user's email, voice and fax messages can be accessed through a single application through this integration. Users can listen to their Google email messages through the phone and to their voice messages from the web by logging into their Google account. Message synch is not bidirectional, so messages received directly in Google cannot be listened to in Avaya Messaging.

- **Contact & Calendar Integration**: Avaya Messaging can synchronize contact entries and calendar events with your Google Apps. Any entry that the user creates within Google will be automatically updated in Avaya Messaging. The reverse is also true. Any entry that the user creates within Avaya Messaging will be automatically updated in Google.

  Note: Repeating events in Google calendar, such as a weekly meeting, will only be synchronized with Avaya Messaging out to 7 days ahead. Previewing beyond 7 days in advance will not show the recurring event in the calendar.

  By implementing these solutions, users gain access to many new features without substantially changing their work flow. This allows for an increase in productivity without extensive retraining.
  Avaya Messaging can also forward incoming messages (voice, email, fax) to a Google Drive location making all of your communications available from anywhere in the world through the Internet.

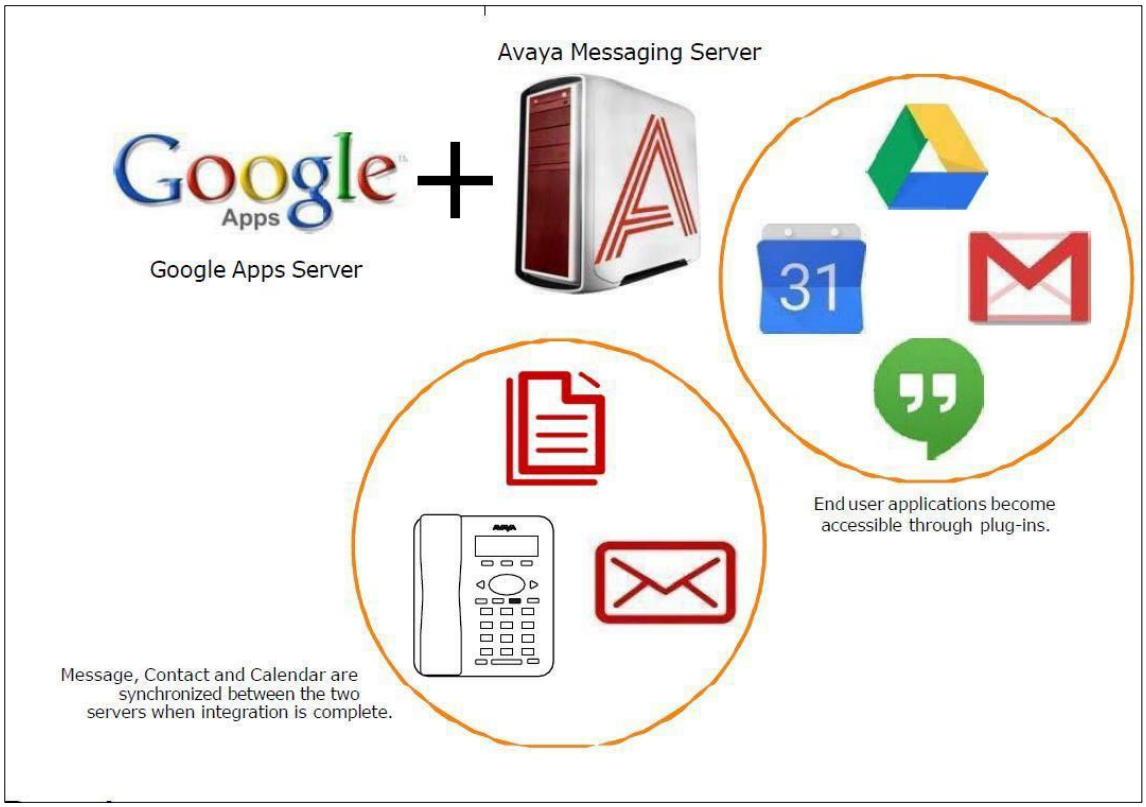
  Note: Integration with Google apps and other 3rd party applications and plug-ins may require additional licensing.

Synchronization Directions

Data synchronization between the Avaya Messaging servers and Google apps only occurs in the following directions.

ITEM	SYNCHING	FROM TO
Inbox	Avaya Messaging	Google
Contacts	Google Avaya Messaging	Avaya Messaging Google
Calendar	Google Avaya Messaging	Avaya Messaging Google

Implementation Example



Requirements

Requirements	Details
License	---
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 and higher

Server configuration of Google Integration makes extensive use of CSE and CSE.PIM for message, contact and calendar synchronization. If the web server is able communicate properly with the worldwide web, users will be able to configure all their gadgets and plug-ins on their own through the **User Guide**.

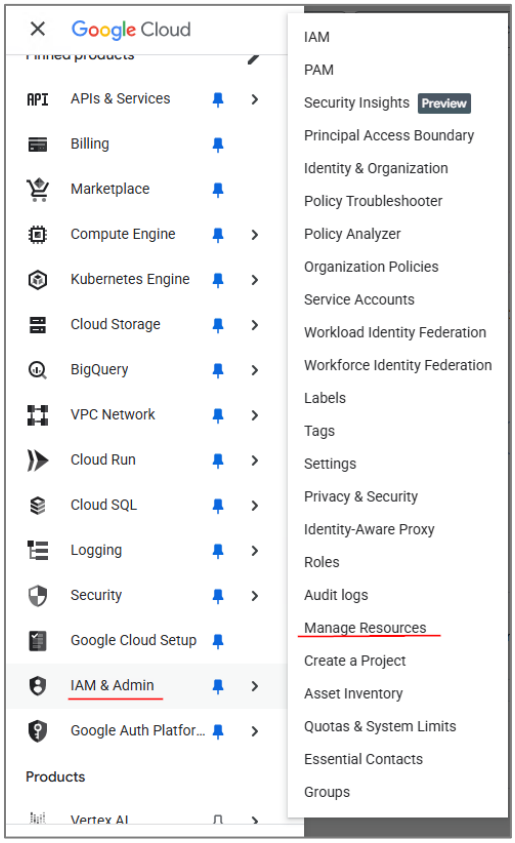
Client authentication and synchronization is handled using OAuth 2.0 and Google API.

Install and configure OAuth2.0

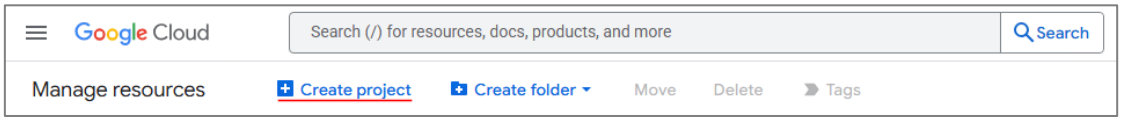
OAuth 2.0 provides secure user authentication and is required for Gmail to access the messaging servers.

OAuth 2.0 Setup

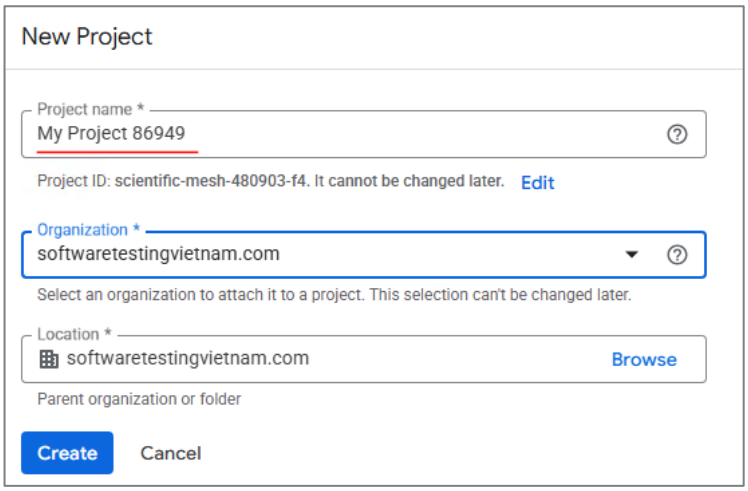
1. Open a web browser and go to https://console.cloud.google.com. Login using your Google admin account.
2. Click the **Navigation menu**. Select **IAM & Admin > Manage Resources**.



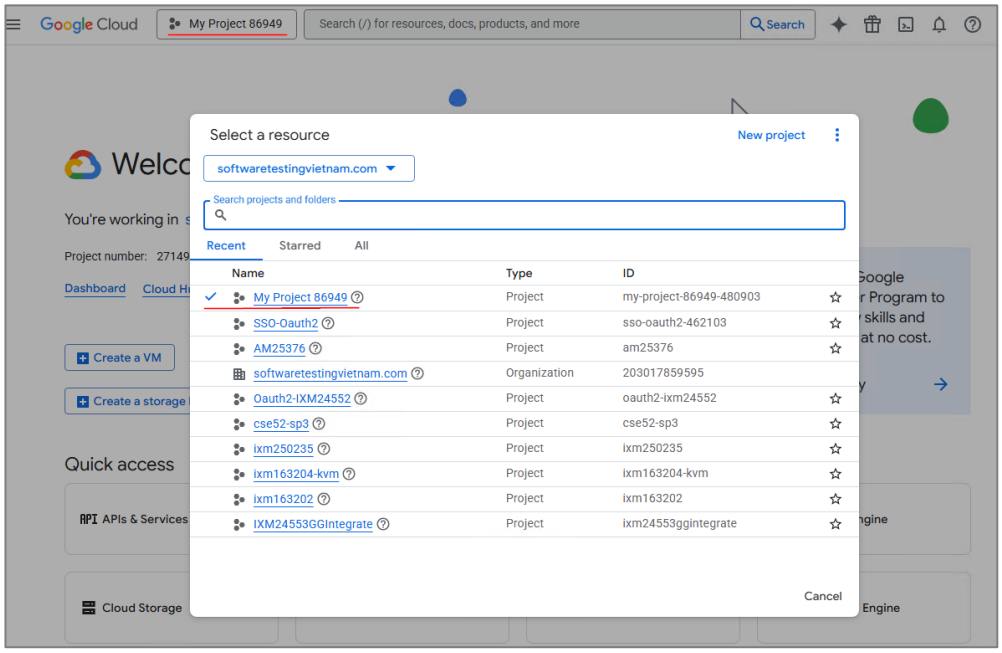
3. Click **Create Project.**



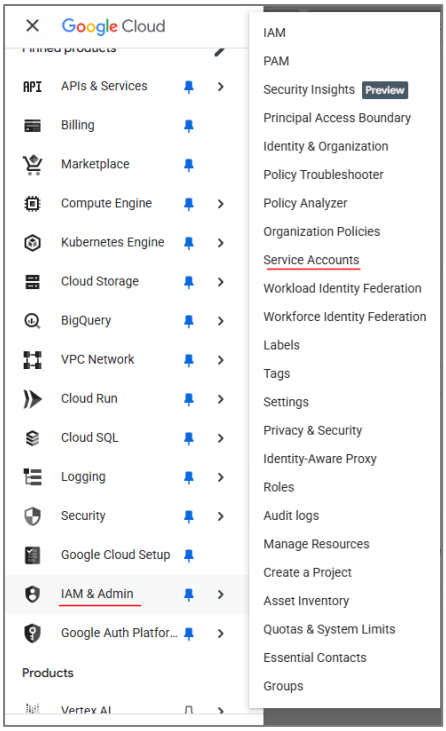
4. Give the new project a name, then click **Create**.



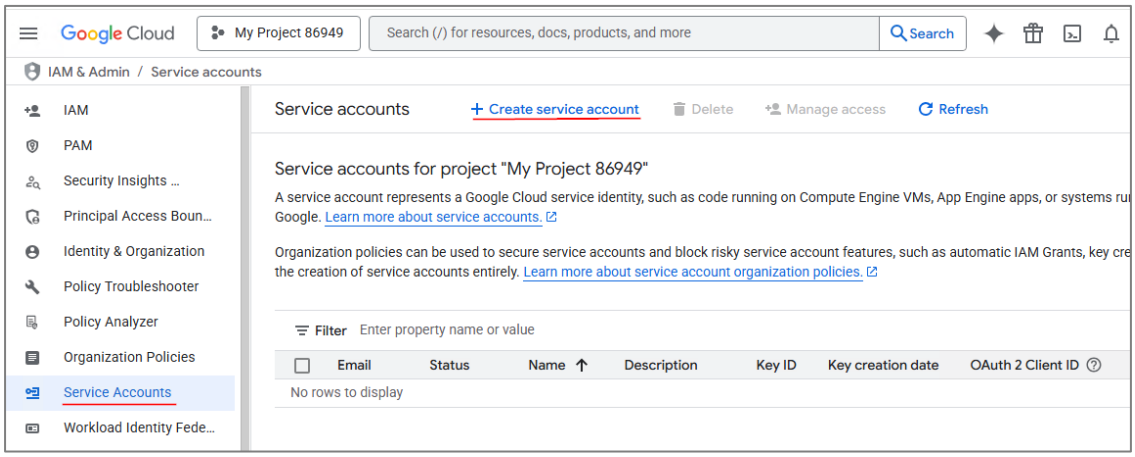
5. On the home page, click **Open project picker (Ctrl O)**. Ensure that the project you just created is chosen in the **Select Project** dropdown menu.



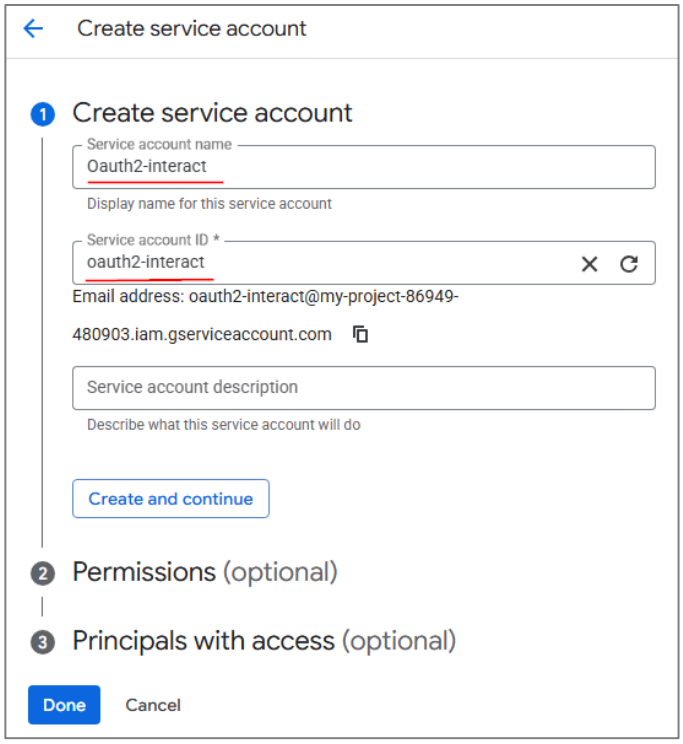
6. Click the **Navigation Menu > IAM & Admin > Service Accounts.**



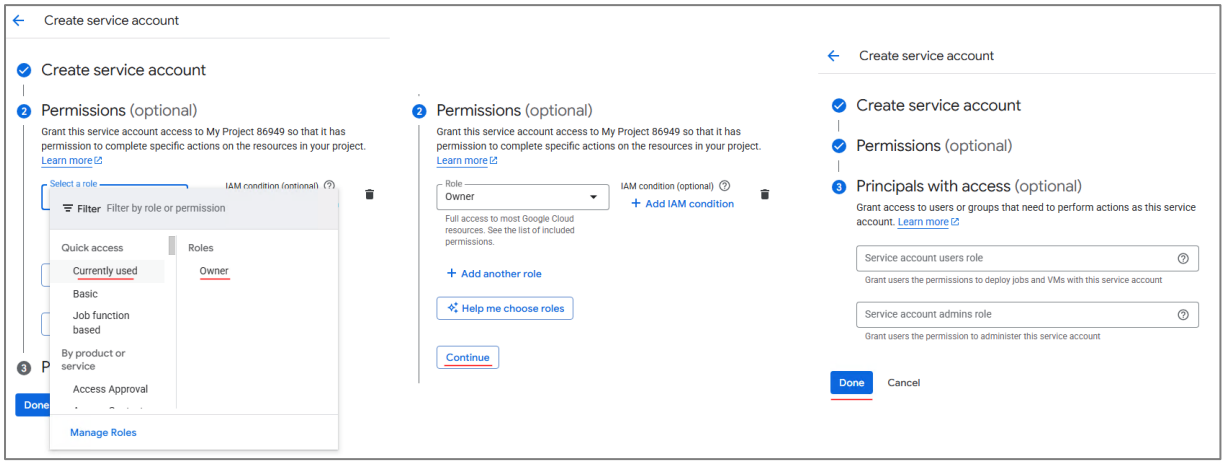
7. In the **Service accounts**. Click **Create Service Account**.



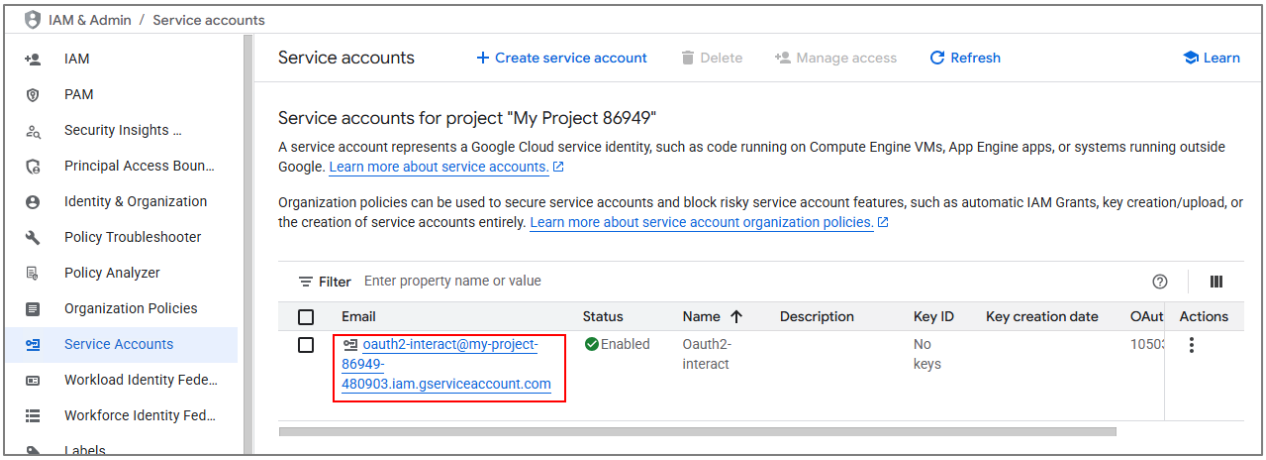
8. In **Create service account**, input a service account name, then click **Create and continue**.



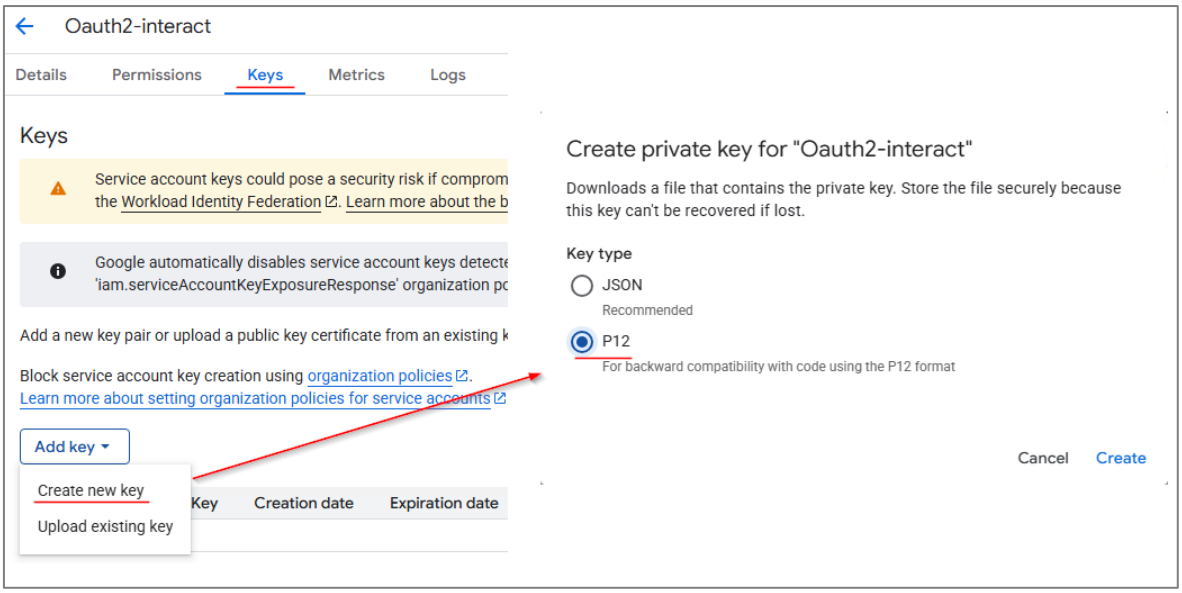
9. From the **Select a role** dropdown menu, choose **Currently used > Owner**. Click **Continue** then **Done**.



10. In **Service Accounts**, click the name of the service account you just created.

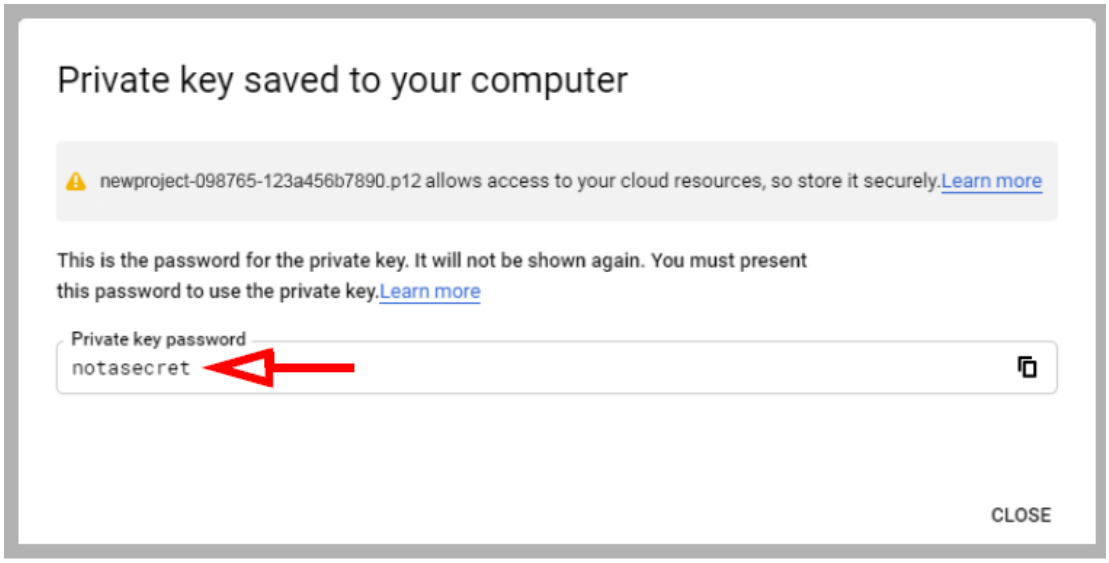


11. Open the **Keys** tab and click **Add Key > Create New Key**. Choose the **P12** option, and click **Create**.

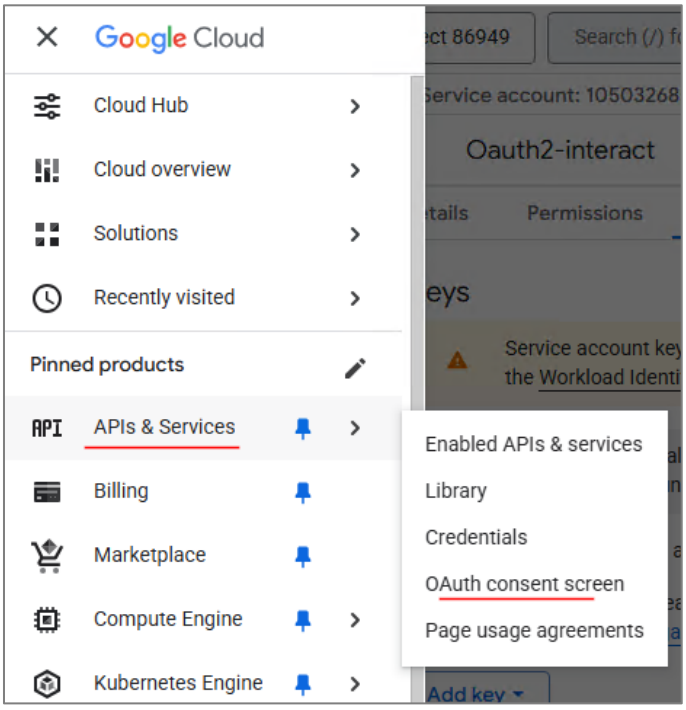


12. The private key file will be created with a .p12 extension. Make note of where the file is saved (i.e., the **Downloads** folder). Copy the file to both the **C:\UC\UCCSE and C:\UC\IMAPTSE** folders. (Change the path accordingly if your program is installed on a different drive).

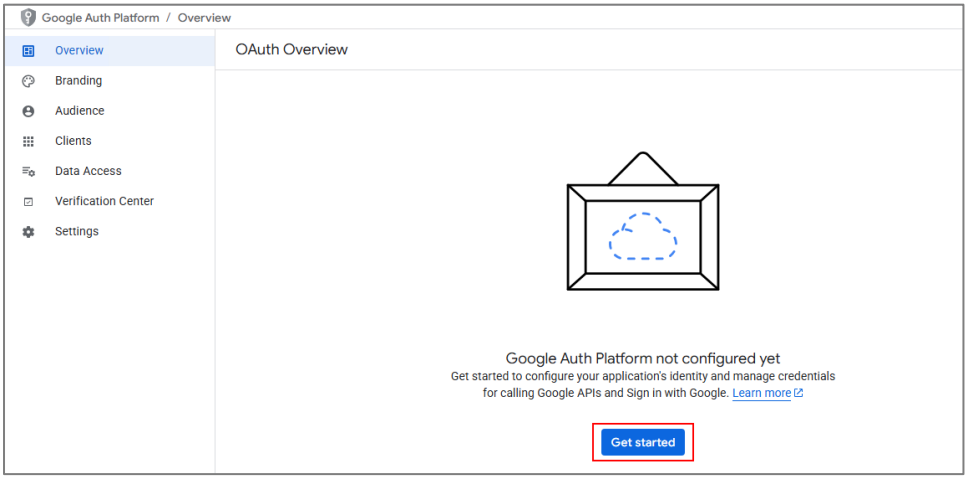
13. Record the Private key password (**`notasecret`**) and click **CLOSE**.


Private key saved to your computer
newproject-098765-123a456b7890.p12 allows access to your cloud resources, so store it securely.Learn more
This is the password for the private key. It will not be shown again. You must present this password to use the private key.Learn more
Private key password
notasecret
CLOSE

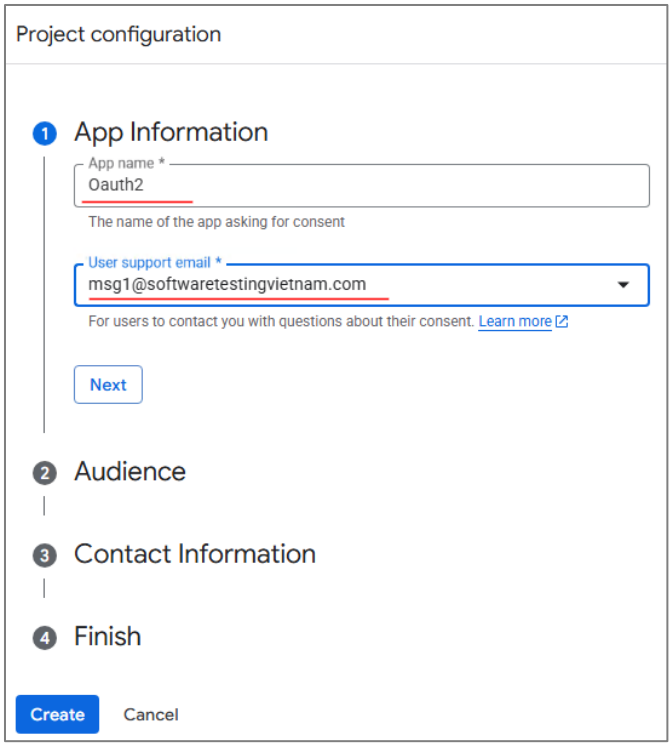
14. Open the Navigation Menu and select **APIs & Services**. Click **OAuth consent screen**.



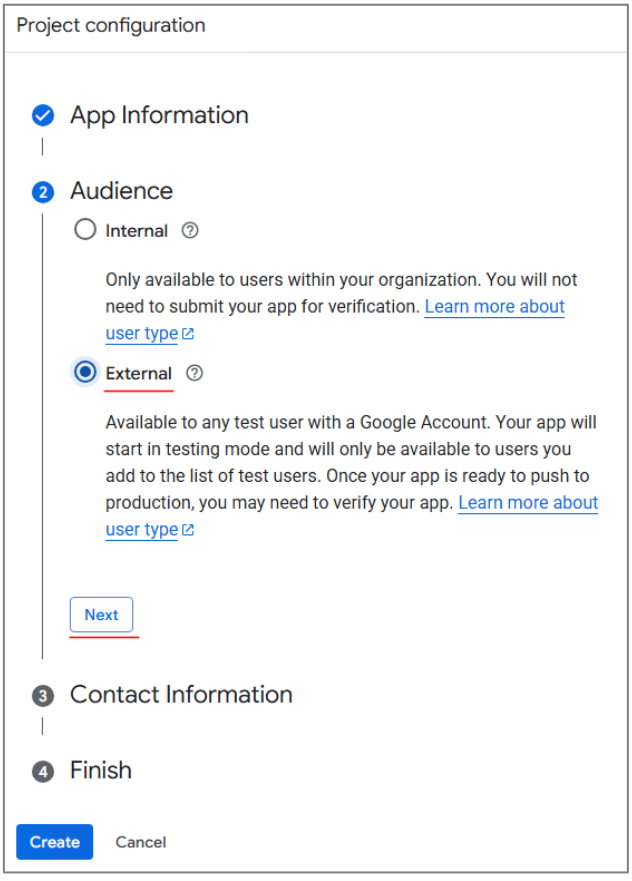
15. In **Google Auth Platform > Overview,** click **Get started.**



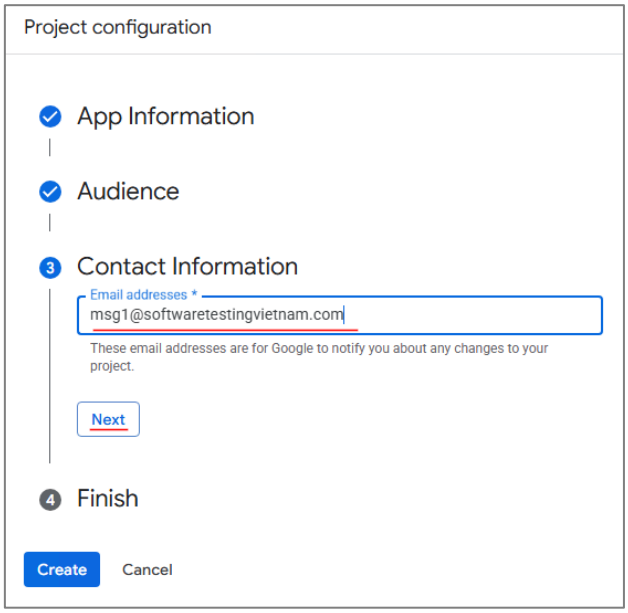
16. In Project configuration, enter **App name** and **User support email.** Then click **Next.**



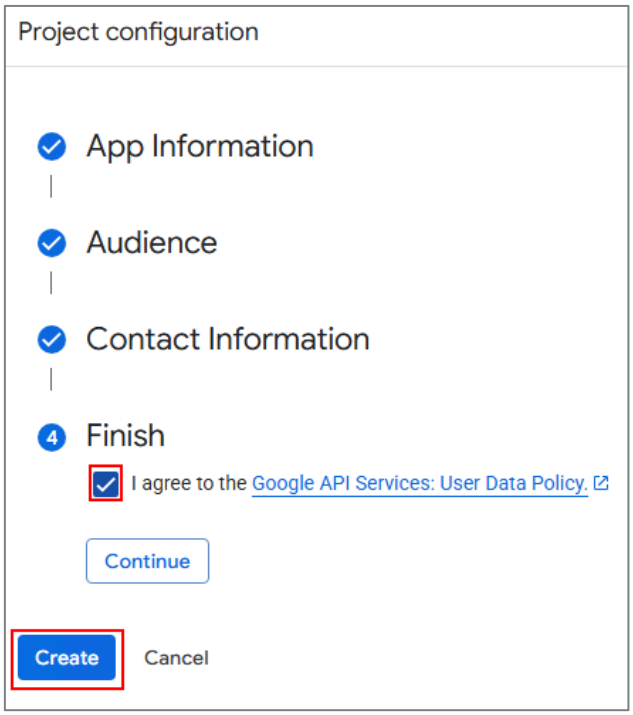
17. In **Audience**, choose **External**. Then click **Next**.



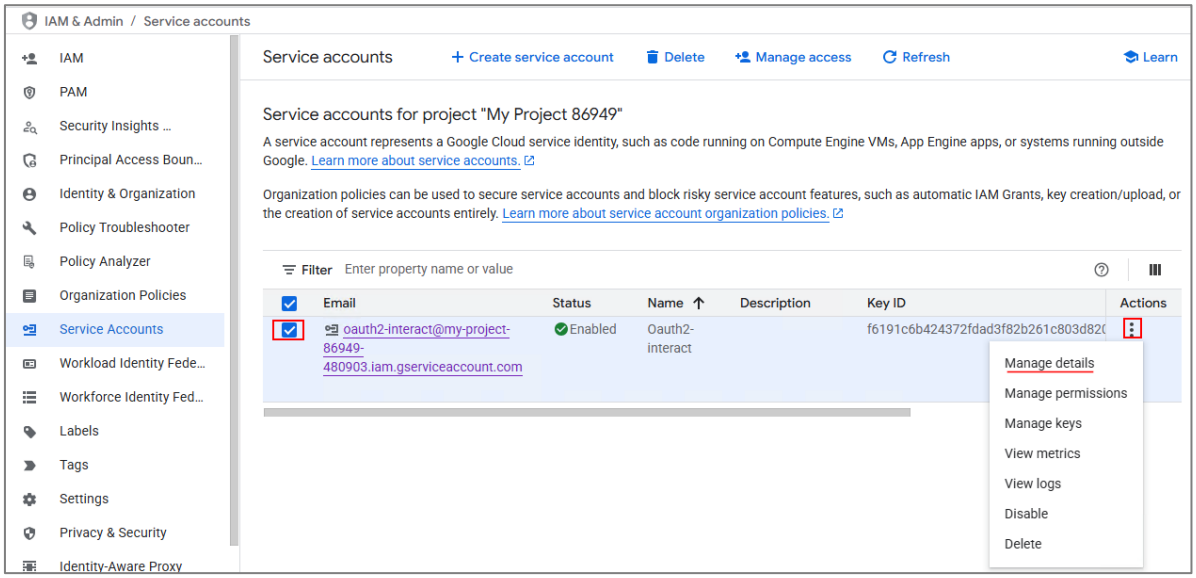
18. In Contact Information, enter your admin email address. Then click **Next.**



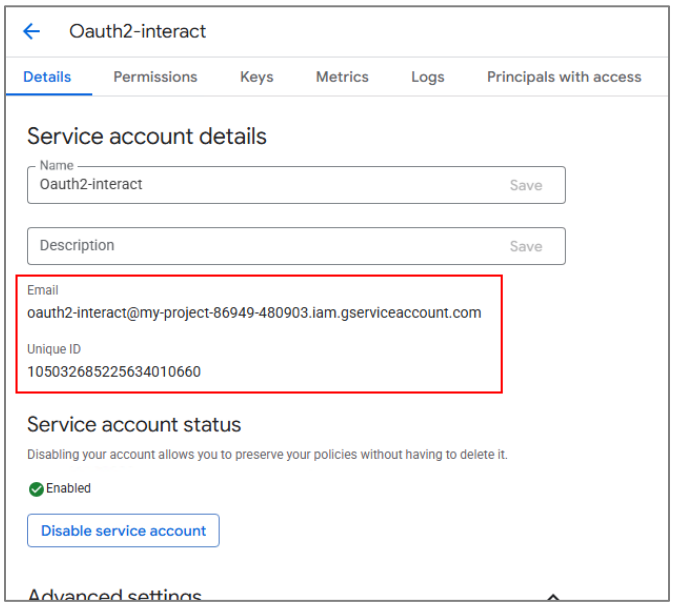
19. In Finish, tick Agree policy and then click **Create**.



20. Go back to **Service accounts**, click the **Actions** icon and choose **Manage Details**.

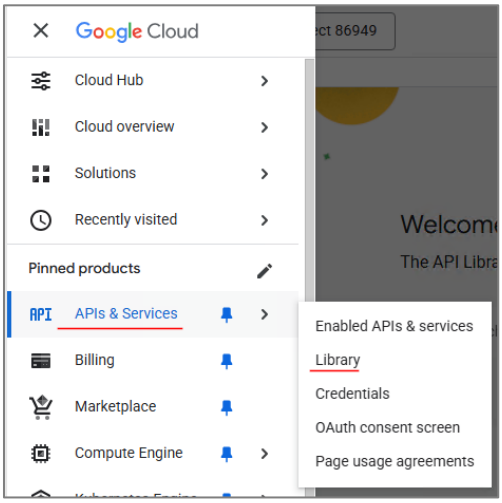


21. On this screen, record the **Email address** and the **Unique ID** (for step 31).

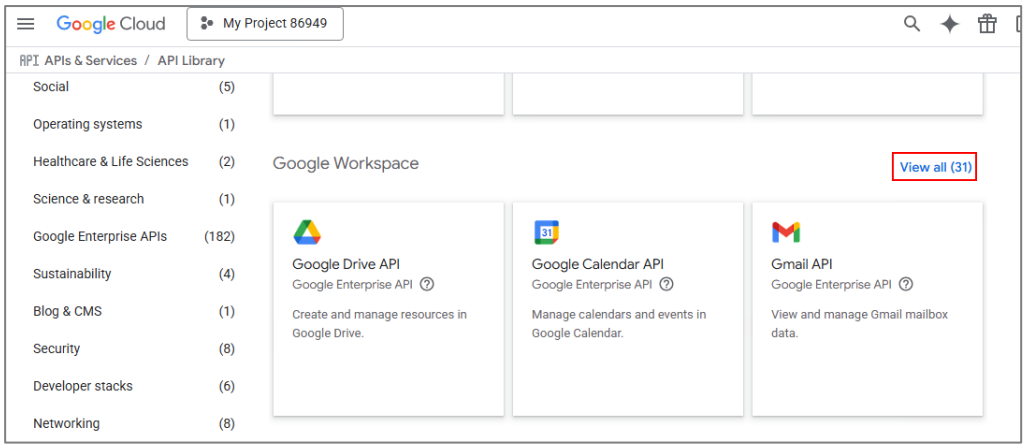


Hint: You can drag the mouse over the Unique ID value or the Email address, copy and paste the string into Notepad. This helps to prevent copy errors.

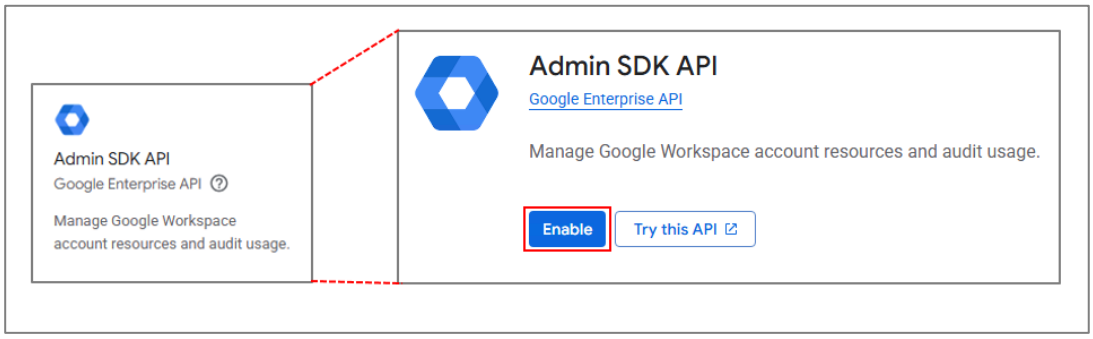
22. From the **Navigation** menu, open **APIs & Services**, and select **Library**.



23. Scroll down and click **View all** Google Workspace session.

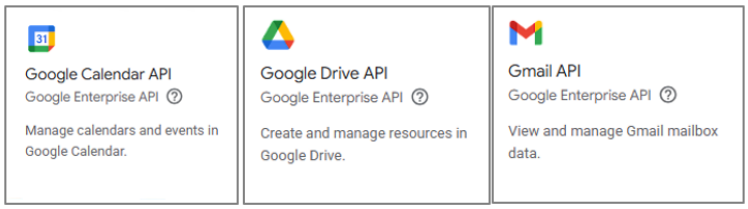


24. Under the **Google Workspace** category, select **Admin SDK API**. Click **Enable**.

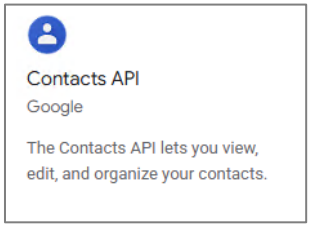


25. Once enabled, return to the Google Workspace page (**APIs & Services > Library**). Repeat to enable all of the following APIs:

    - Google Calendar API
    - Google Drive API
    - Gmail API

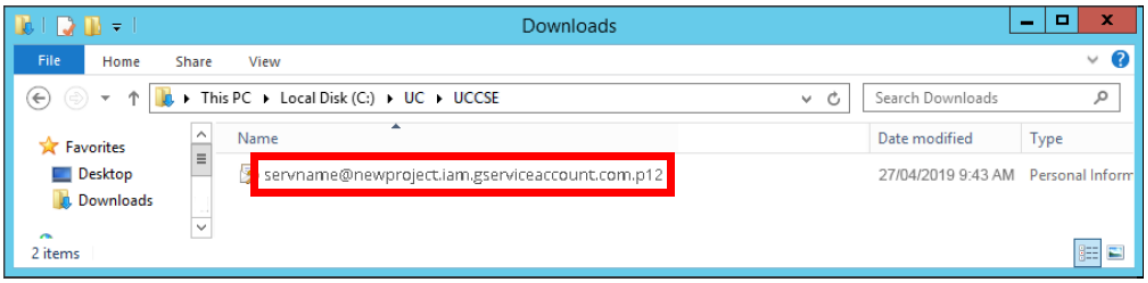


26. Return to the Library, selecting **Social** this time, then enable **Contacts API**.



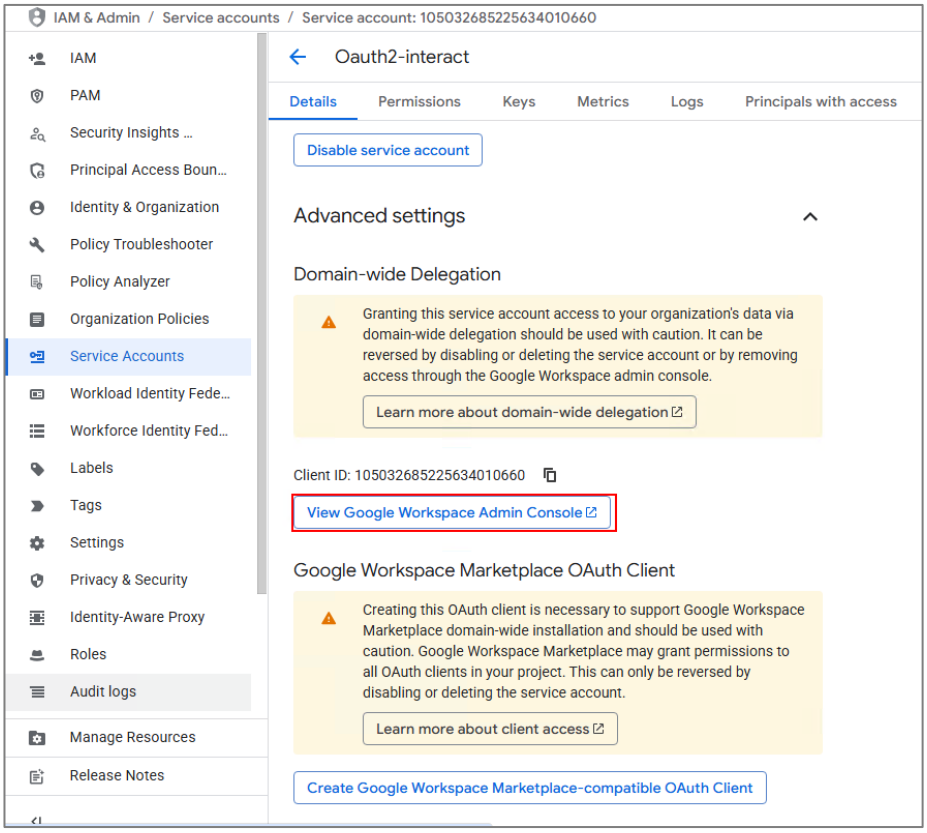
Hint: While these settings will work for most sites, not all sites will want to open all of these channels if they are not required.

27. Rename both copies of the P12 file from step 11 to match the email address recorded in step 19. Include the **domain** and the **.com** extension.

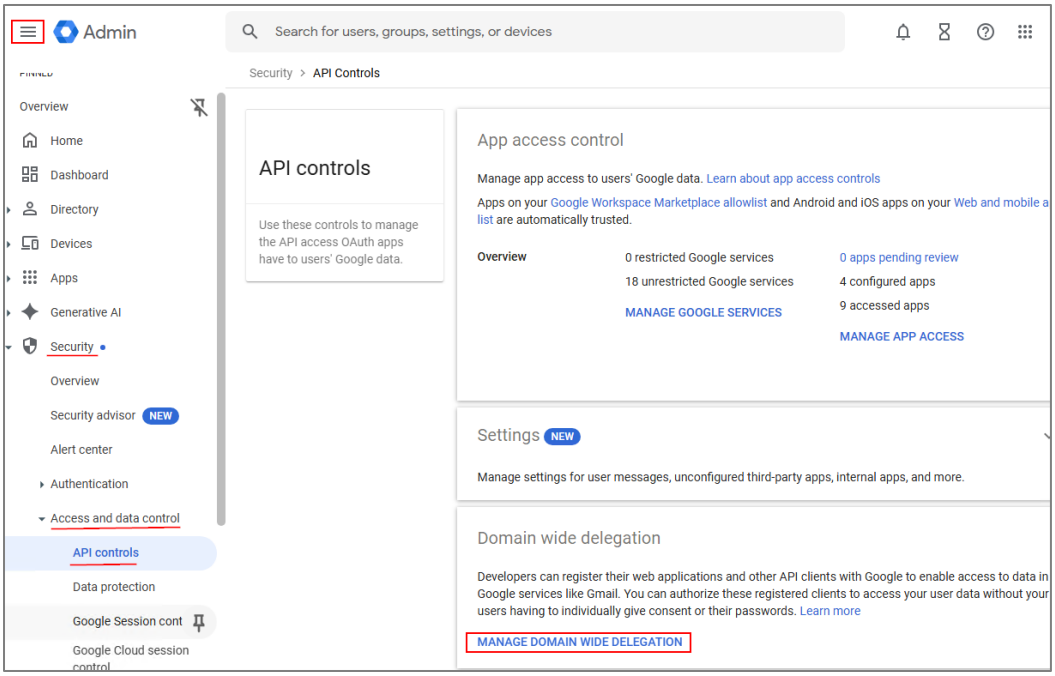


Caution: Do Not change the extension of the file. Always ensure it retains the P12 extension.

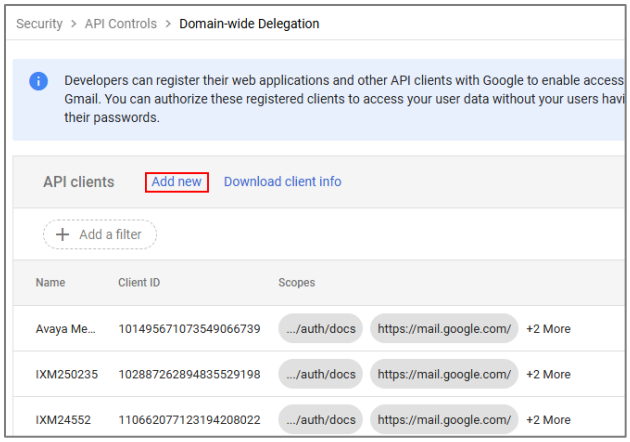
28. In Service account, extend **Advanced settings** and then click **View Google Workspace Admin Consoles**. It will redirect to **https://admin.google.com**.



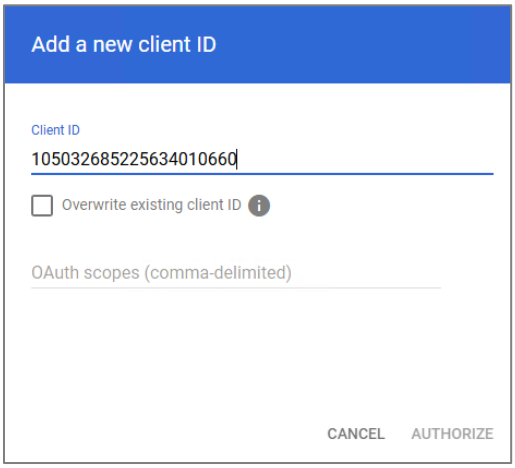
29. In page https://admin.google.com, open **Main menu > Security > Access and data control > API controls**. Then click **MANAGE DOMAIN WIDE DELEGATION.**



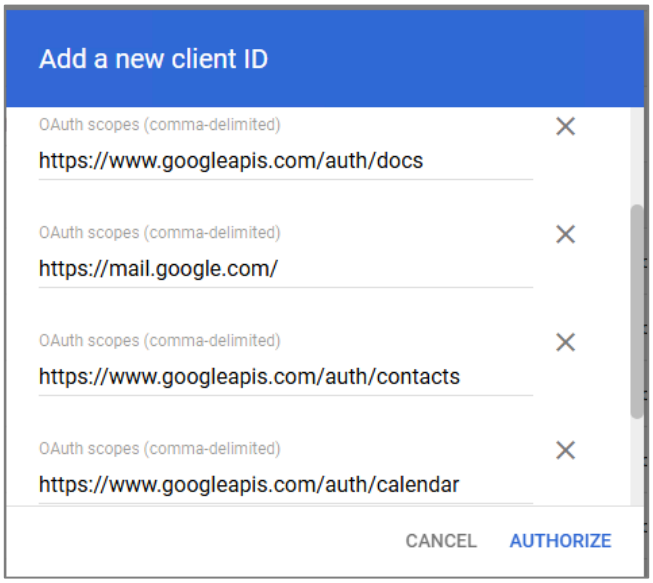
30. In Domain-wide delegation, click **Add new**.



31. In the space provided, enter the **Unique ID** from step 21.



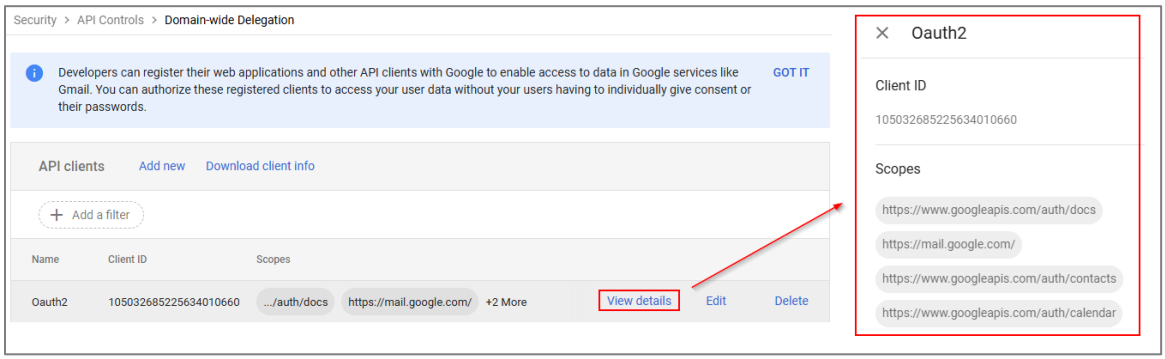
32. In the space for **OAuth scopes**, enter 4 scopes include https://www.googleapis.com/auth/docs, https://mail.google.com/, https://www.googleapis.com/auth/contacts, https://www.googleapis.com/auth/calendar



Hint: Copy and paste the string above into the field. This will greatly reduce the chance of misspelling the entry and breaking the configuration.

Important: While these settings will work for most sites, not all sites will want to open all of these channels if not required.

33. When ready, click **Authorize.**
34. Verify that the selected scopes were successfully installed.



OAuth2 and Avaya Messaging High Availability (HA)

When using OAuth2 in an HA environment, the private key must be copied to both of these locations on the Consolidated server (C:\UC\IMAPTSE and C:\UC\UCCSE).

Configuring Avaya Messaging for use with OAuth 2.0

Once OAuth 2.0 has been configured, Avaya Messaging must be setup to use it. The following procedure is conducted on the Avaya Messaging Server.

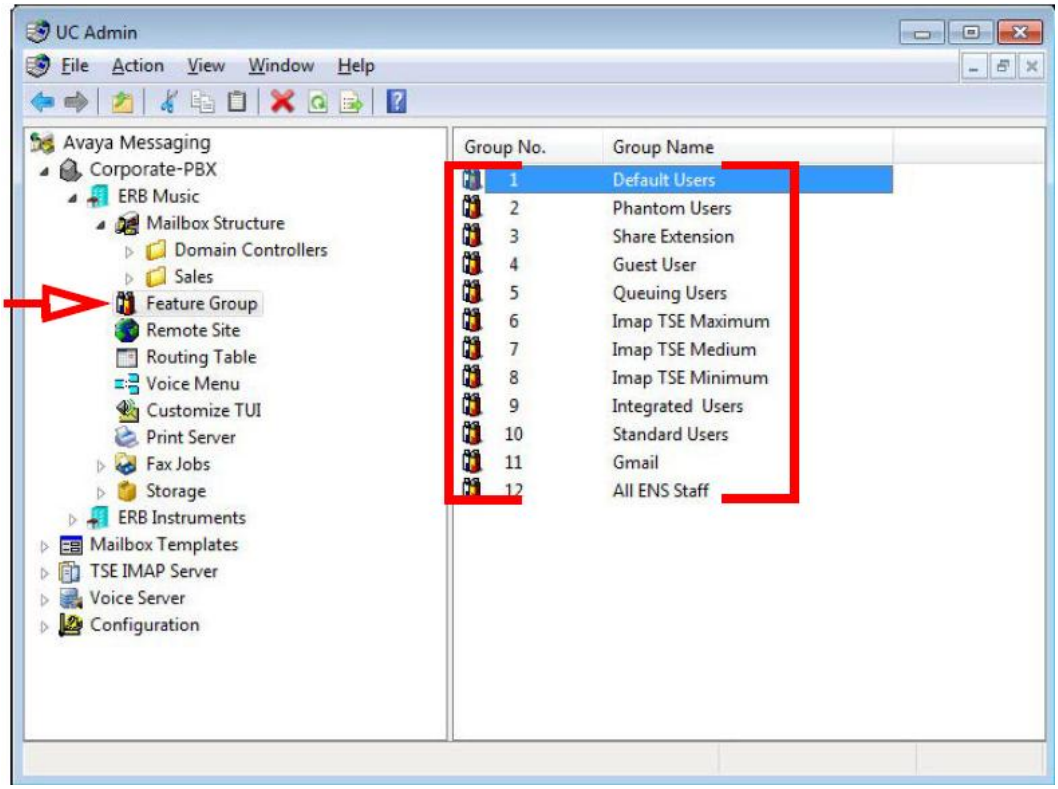
1. Open Avaya Messaging Admin.
2. Right-click on TSE IMAP Server 

and select **New > TSE IMAP Server.**
6. **IMAP Server Name**: Enter **Google** in this space. IMAP Server Address: Enter imap.gmail.com.
   IMAP Server Port: Set this value to **993**.
   Voice Format: Leave this field unchanged.

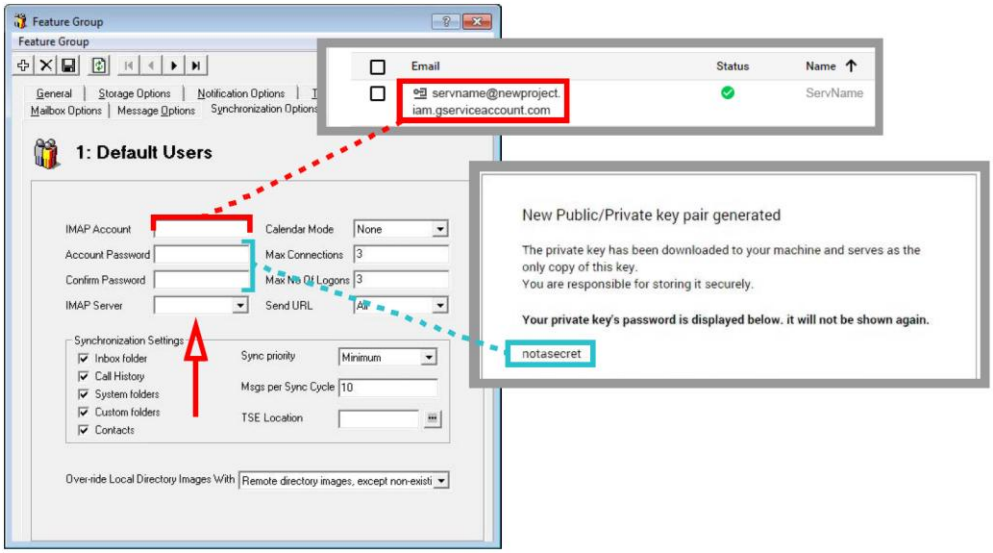
7. Click **OK** when ready.



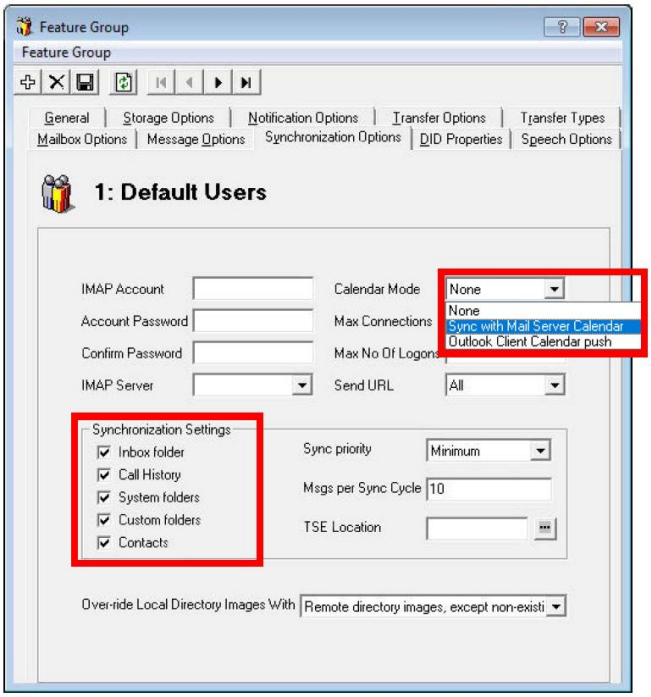
8. Click on **Feature Group** and double-click a group to modify in the right-hand pane.



9. Open the **Synchronization Options** tab. Enter values in the following fields:
IMAP Account: Enter your company domain, followed by a forward slash then the Email address from step 19. For example, yourdomain.com/avaya-secure-connection@avayacloud....
Password and Confirm Password: Type in the Private Key password for the Client ID received in step 12.
IMAP Server: From the dropdown menu, select Google.

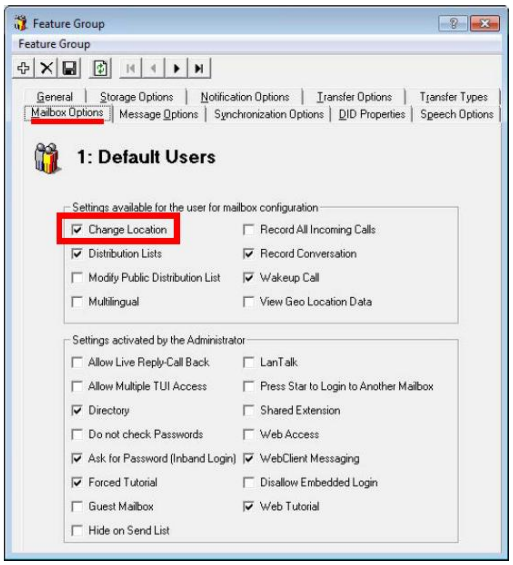


10. **Synchronization Settings:** Enable all of the items that you want to have synchronized between servers. **Calendar Mode**: If calendar synchronization is required, select **Synch with Mail Server Calendar** from the dropdown list.



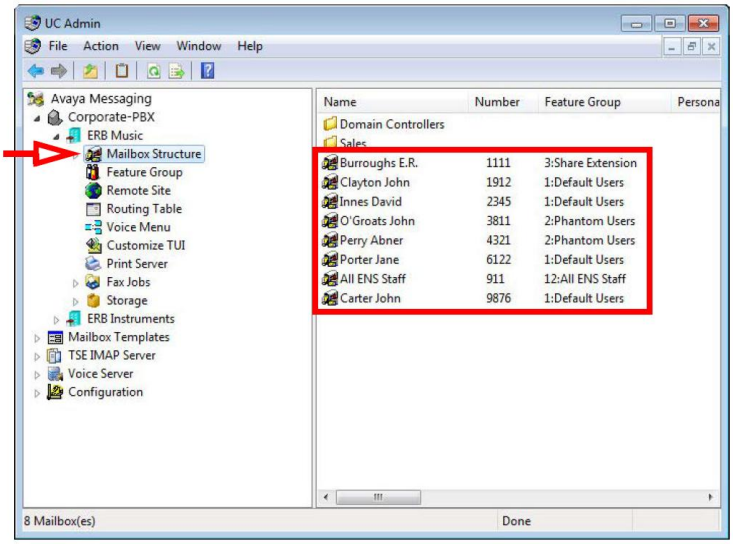
11. Click **Save**  to preserve the changes.

12. Go to the **Mailbox Options** tab and enable **Change Location** to allow an event in your mail server calendar to automatically change the UC location of the user. If this feature is not required, leave it disabled.

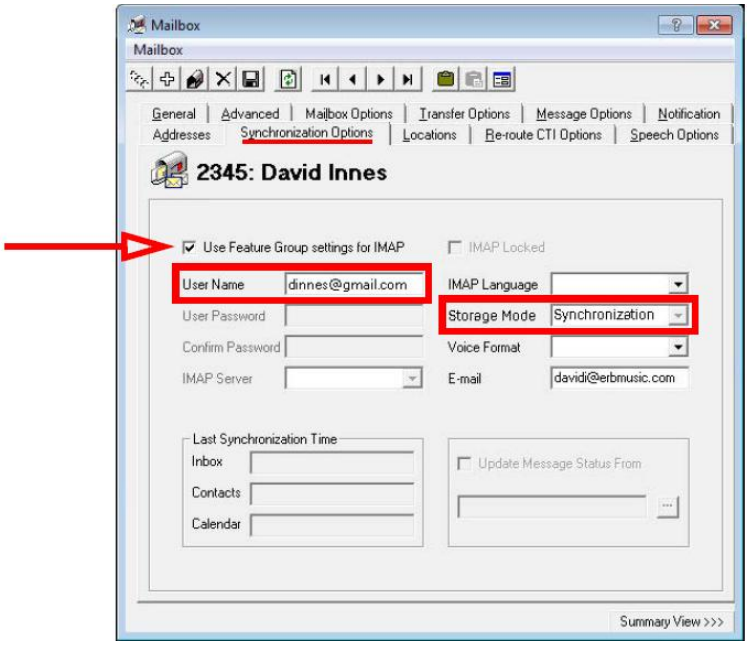


Note: Repeating events in Google calendar, such as a weekly meeting, will only be synchronized with Avaya Messaging out to 7 days ahead. Previewing beyond 7 days in advance will not show the recurring event in the Avaya Messaging calendar.

13. Click **Save** to preserve the changes.
14. In AM Admin, open **Mailbox Structure** and double-click a client to modify.



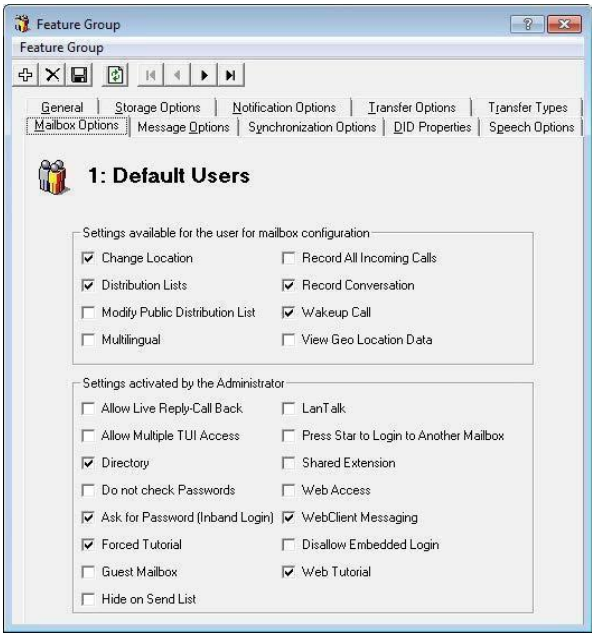
15. Open the **Synchronization Options** tab. Set **Storage Mode** to Synchronization.



16. Enable the **Use Feature Group settings for IMAP** checkbox. For **User Name**, enter the **Gmail** address for this client.

    For example, **davidi@erbmusic.com**
    janep@gmail.com
    name@yourcompany.com

    Note: Desktop Capabilities must be set to **Advanced** for these options to be configured.



Note: Repeating events in Google calendar, such as a weekly meeting, will only be synchronized with Avaya Messaging out to 7 days ahead. Previewing beyond 7 days in advance will not show the recurring event in the Avaya Messaging calendar.

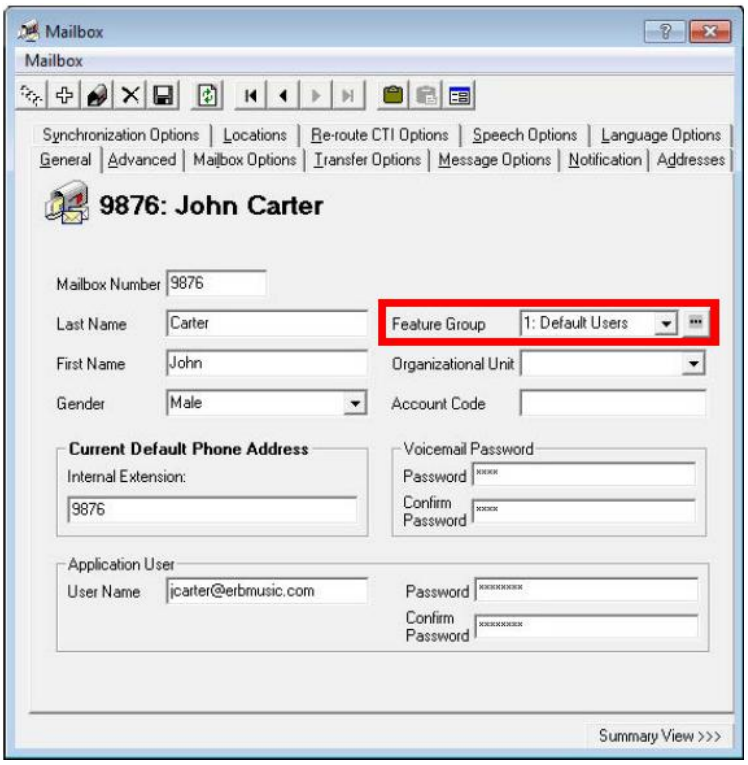
17. Click **Save** to preserve the changes.

18. Your Avaya Messaging mailbox will now synchronize contacts and/ or calendar information with the Gmail account.

    Note: To make sure that your mailboxes are associated with the right Feature Group check your Mailbox configuration window under the General tab.

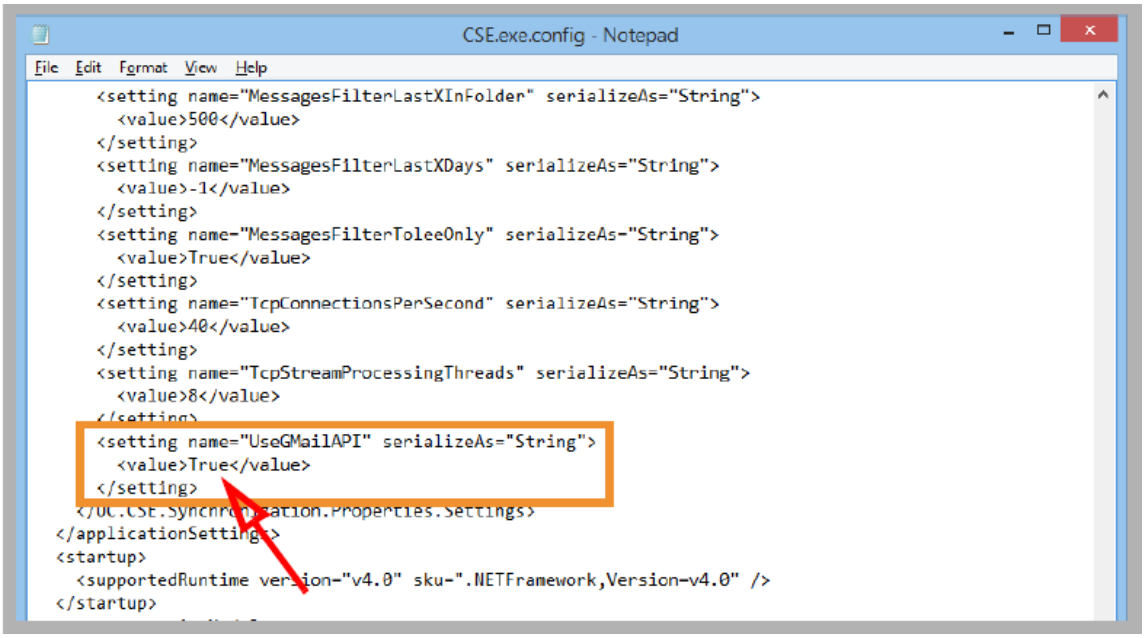
19. Repeat steps 11 through 14 for each client that requires OAuth 2.0 synchronization.

20. On the Voice Server, open the **UC/UCCSE** folder.



21. Edit the **CSE.exe.config** file using any text editor (e.g., Notepad).

22. Locate the tag **UseGMailAPI** and set its value to **True**.



23. Go to **File > Save** to complete the change.
24. Stop and start the UC Content Synchronization Engine and the UC CSE PIM Synchronization Engine services on the Voice Server or restart the server.

    Caution: If this is a High Availability system, restart these services **only on the Consolidated Server**.

    The setup is complete.

User Guide

This user guide helps you configure your message, contact and calendar synchronization between Avaya Messaging and Google Apps. While the installation and configuration related to these features are straight forward, please backup important data before configuring any synchronization.

Message Synchronization

To consolidate all messages (e.g., voice, text, fax, etc.) in a single email account, synchronize your Gmail or Google Apps email with the UC server's Web Access mailbox. If your organization is using OAuth2 authorization, you will not have to enter any details beyond the email address.

Note: If the synchronization does not work even after entering the correct credentials, your server may not be configured properly for this feature. Please contact your system administrator.

Warning: If you have a custom filter configured on your Google account, it will not apply to messages that are synchronized from the voice server (e.g., voicemail, fax, etc.).

Contact & Calendar Synchronization

When your administrator has enabled calendar and contact synchronization for you, everything will be occurring on the server side in the background, so you do not have to configure anything on your own. You can use your mail server as you normally would and your calendar and/or contact entries will be populated on your Avaya Messaging mailbox as well. The following are typical behaviors that the synchronization will follow so that you can understand exactly how your calendar and contact entries are being handled by the servers.

Note: When creating a calendar event from Google, you must ensure that the reminder time is set to **1 minute or greater**. Setting this value to 0 will cause synchronization issues. By default, the time of the memory is 10 minutes.

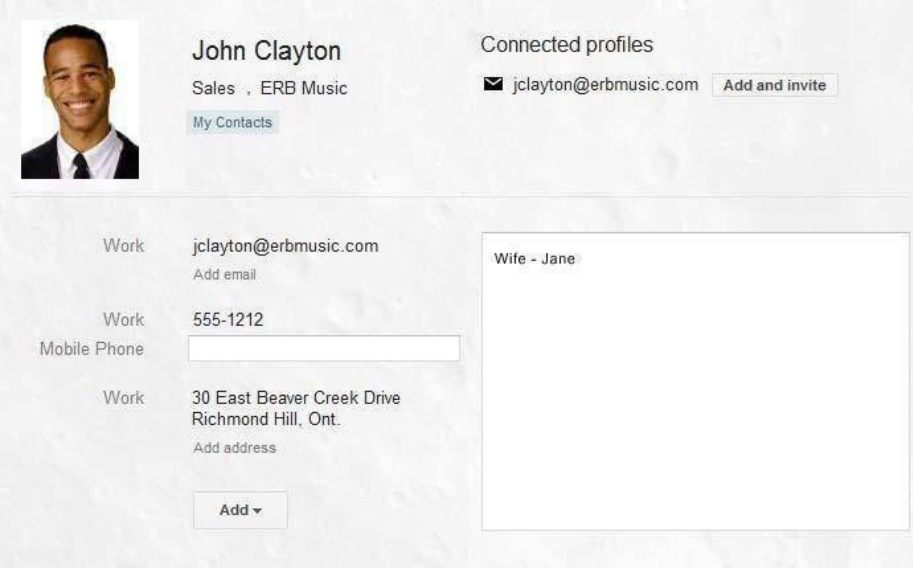
Note: All your calendar events and contacts from your current mail server will be populated into your Avaya Messaging mailbox right after your administrator finishes the configuration.

Note: You should backup your calendar events and contacts periodically as a precaution.

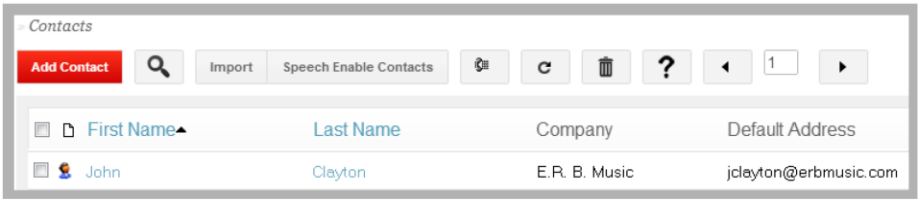
Note: Repeating events in Google calendar, such as a weekly meeting, will only be synchronized with Avaya Messaging out to 7 days ahead. Previewing beyond 7 days in advance will not show the recurring event in Google's calendar.

Contact Sync

When you create a contact entry through Gmail, the same entry will be synchronized into your Avaya Messaging contacts.



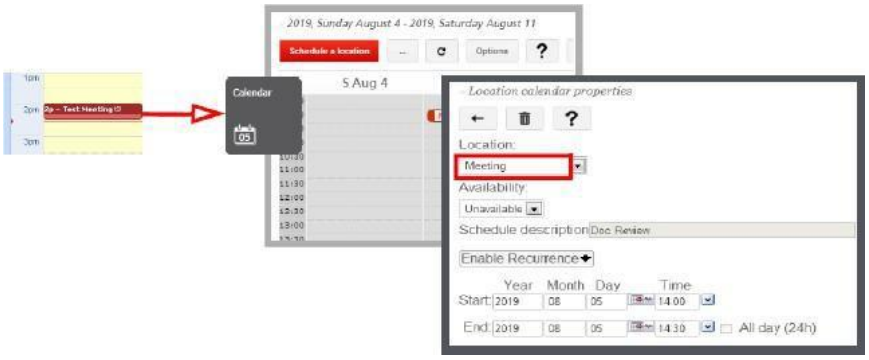
The contact information is automatically sent to the Avaya Messaging contact list.



Warning: Keep in mind that deletions are also synchronized. If you delete an entry from Gmail, it will be deleted from Avaya Messaging, and vice versa.

Calendar Sync

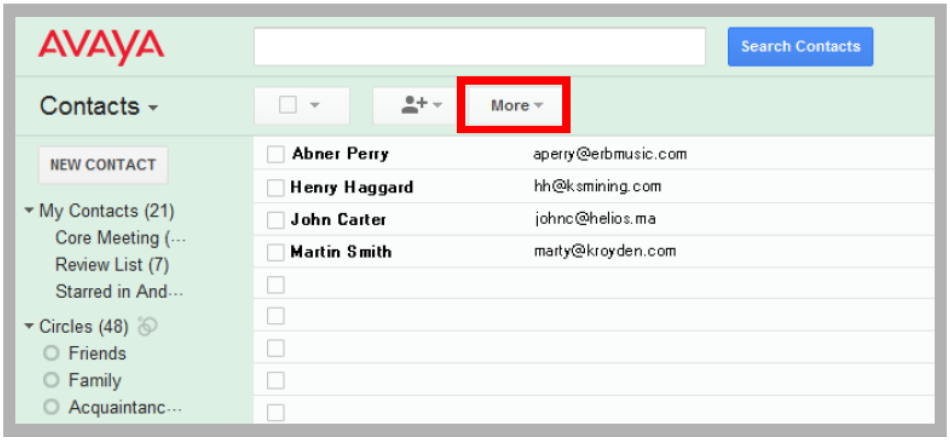
When you create a calendar entry from Google Calendar, the same entry will appear in Avaya Messaging. The time and date of the meeting is automatically sent to the Avaya Messaging mailbox. By default, the location for these events is marked as **Meeting**, but this can be changed through the Web Access **Calendar** icon.



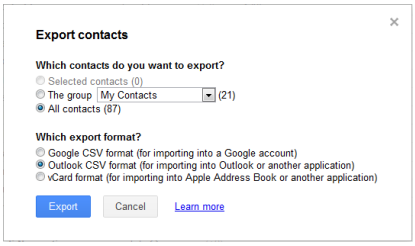
Manual Contact Importing

If synchronization is not an option for your site, you may manually copy contacts from one application to the other. Long lists of contacts can be difficult to transfer. To make this process easier, Web Access supports importing CSV (comma separated value) files that can be exported from Google Apps.

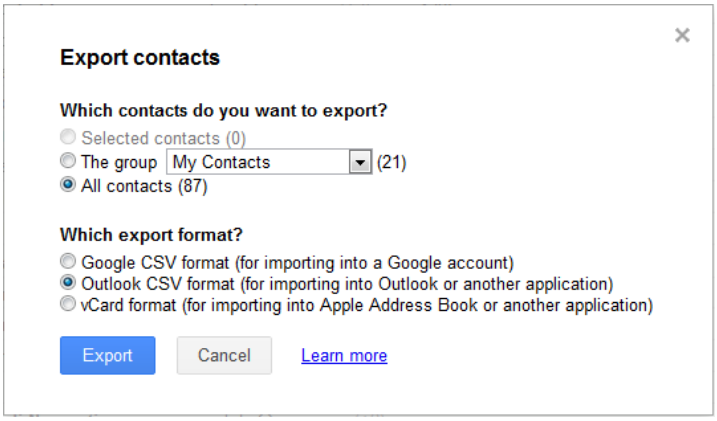
1. To export your contacts from Google Apps, log into your Google email account and open your Contacts list.
2. Click on **More**, then **Export.**
   This opens the Export contact window.



3. You can choose to export selected contacts, specific groups of contacts (e.g., My Contacts), or all contacts.
   Select **All contacts**.

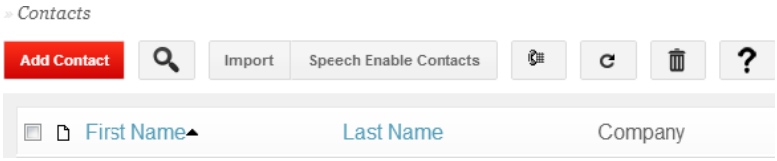


4. For **export format**, choose Outlook CSV.
   Click on **Export** when ready.

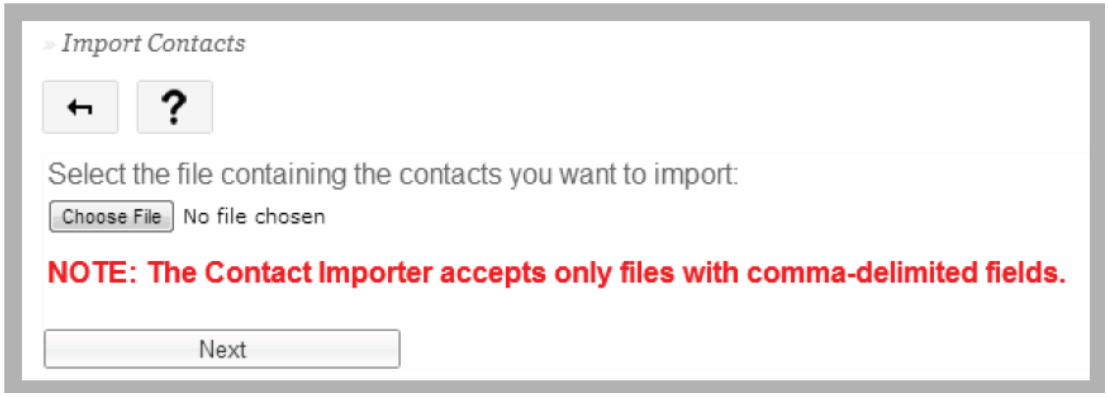


5. When prompted, specify the location where the file will be saved.

6. With the CSV file ready, open Web Access and click **Contacts**.
   Click the **Import** button.

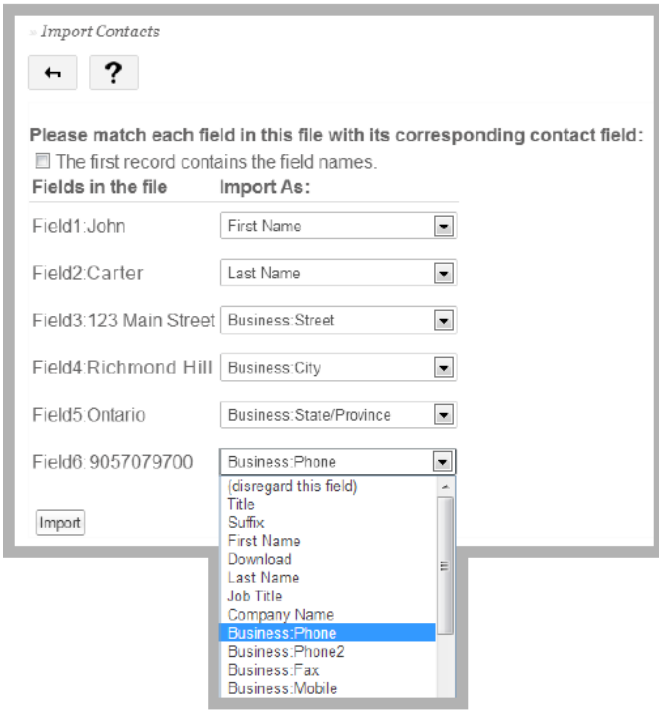


7. Click **Choose File** and select the CSV file exported from Google.
8. Click **Next** to proceed after the file has been selected.



Match the fields from the CSV file to the fields on the Web Access contact list. You will only have to match the information you require. Leave all the unnecessary fields as **(disregard this field)**.

Click **Import** when all of the required fields have been matched. The contacts will be imported from the CSV file into Web Access.

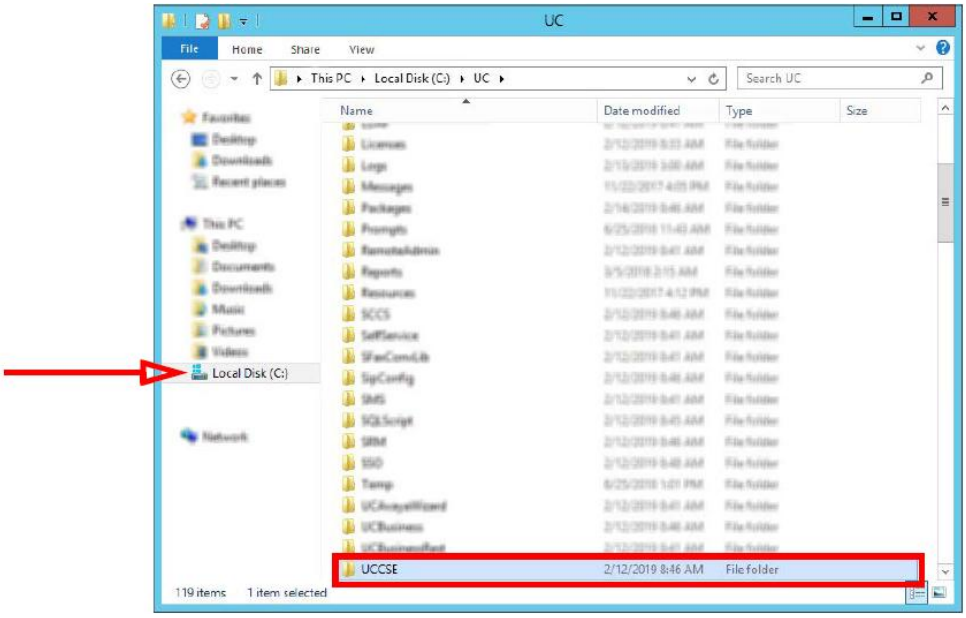


Reconfiguring Synchronization Components for Gmail

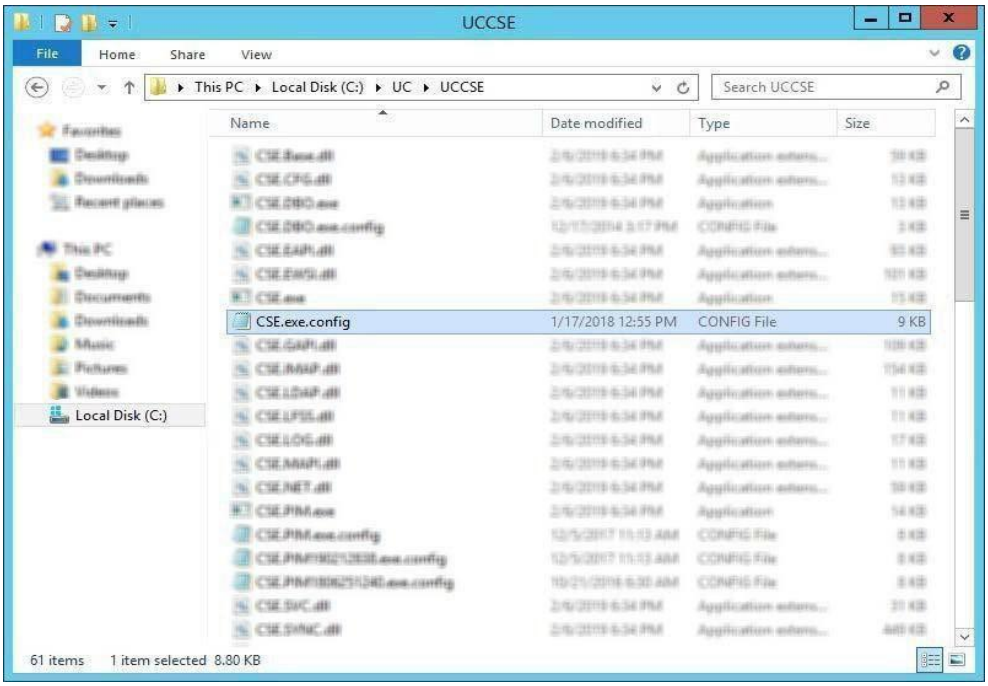
Once the installation has been completed, verify that the system configuration files are set to use GMAIL. This should be done on all servers running CSE: The voice server in a single server environment, the Consolidated server under HA, and all remote CSE servers operating.

Note: The CSE.exe.config file is used with message synchronization, while the CSE.PIM.exe.config is used for contact and calendar synchronization.

1. Open the UC/UCCSE folder on the program installation drive.

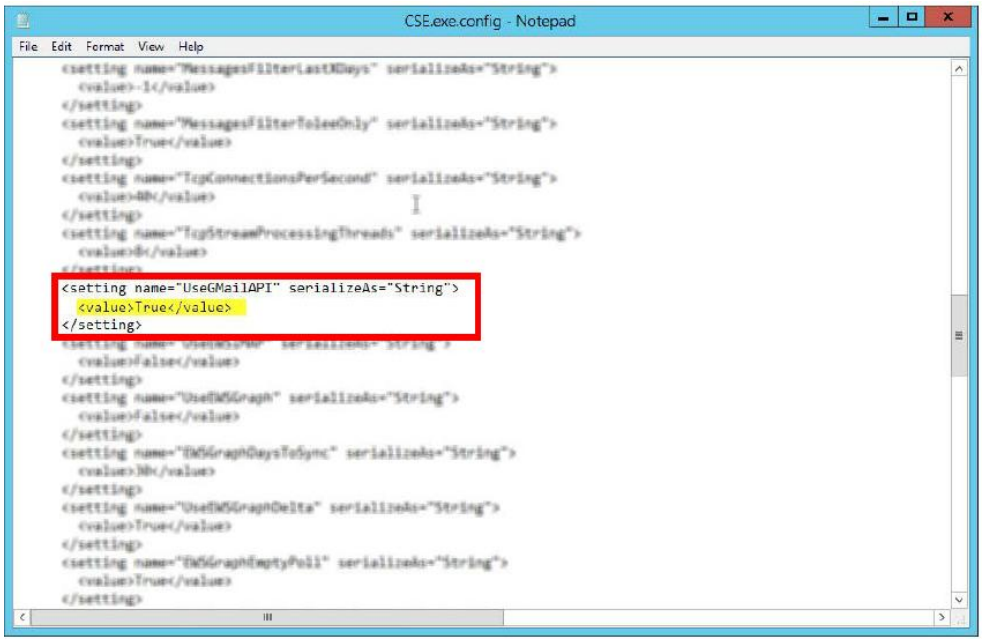


2. Within the folder, open the **CSE.exe.config** file in a text editor such as Notepad.



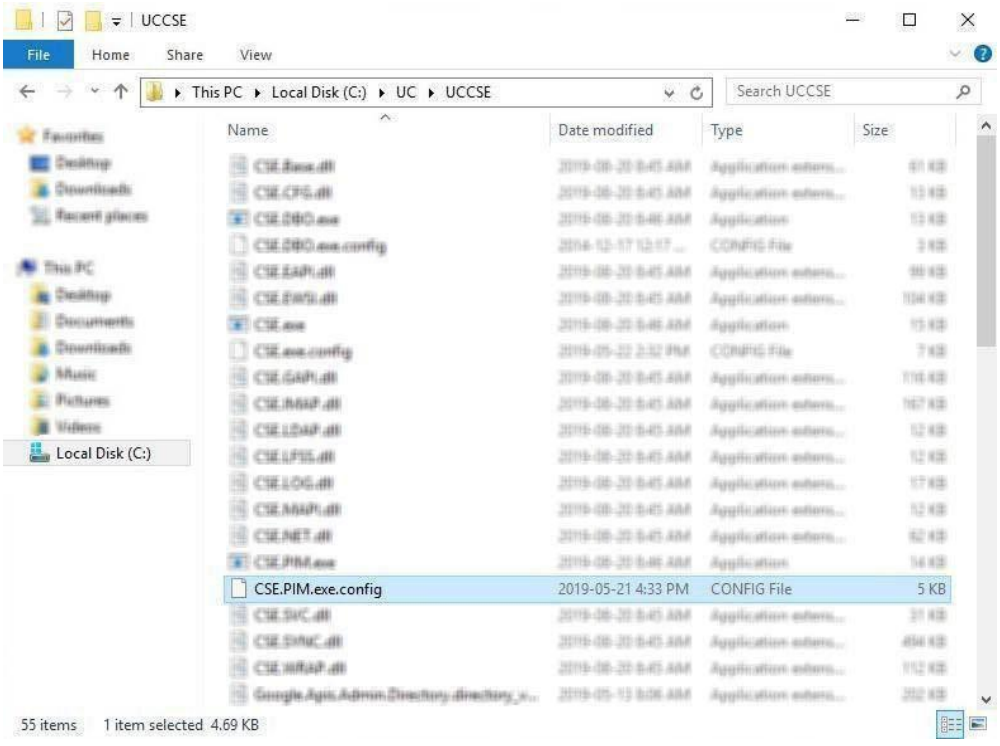
3. Scroll down to find the following lines (UseGMailAPI):

<setting name="UseGMailAPI" serializeAs="String">
<value>**True**</value>
</setting>



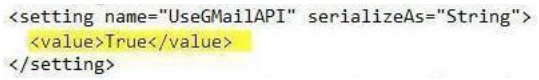
Verify that the **Value** is set to **True**. If the value is not True, change it and save the file.

4. Within the UCCSE folder, open the **CSE.PIM.exe.config** file in a text editor such as Notepad.



5. Scroll down to find the following lines (UseGMailAPI):

   <setting name=”UseGMailAPI” serializeAs=“String”>
   <value>True</value>
   </setting>



   Verify that the **Value** is set to True. If the value is not True, change it and save the file.

Restart Services

Before continuing, stop and restart the following services:

- UC Content Synchronization Engine
- UC CSE PIM Synchronization Engine

This will force Avaya Messaging to immediately update its systems. Otherwise, there will be a delay before the changes become active.

Chapter 9: EXCHANGE 2019/2016 INTEGRATION: USING EWS

Guidelines

Depending upon your site's requirements and software, you have the option to integrate Avaya Messaging with several email systems. None of these are required. Where appropriate, refer to the chapter that best suits your requirements.

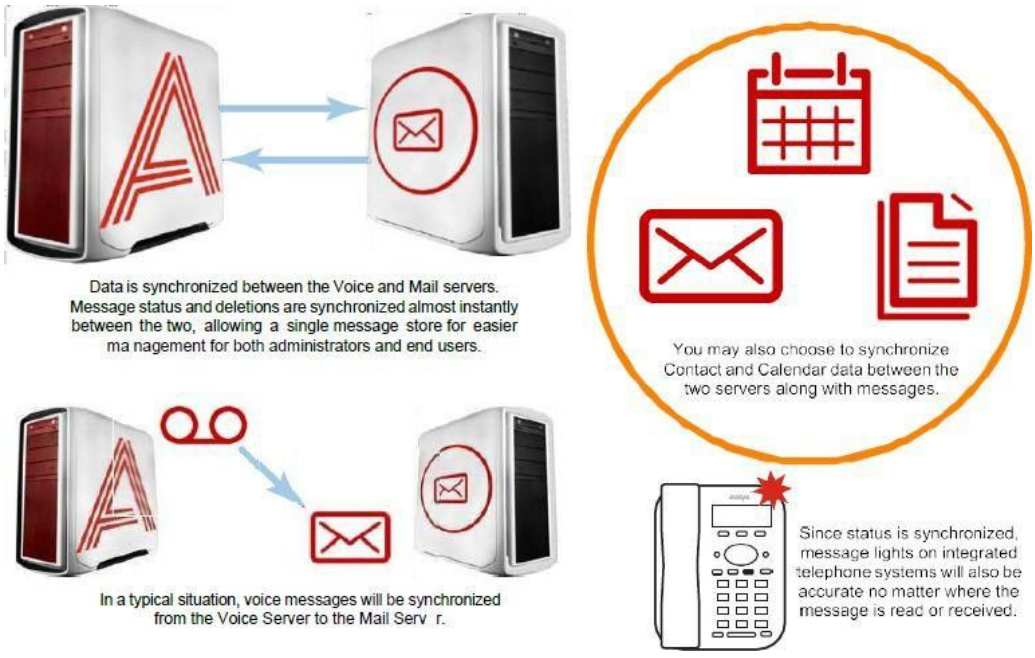
Introduction

Avaya Messaging and an Exchange server can integrate through the IMAPCSE and Exchange Web Services (EWS), providing a truly unified messaging experience. Once the configuration is complete the servers communicate and synchronize all data among themselves, eliminating the need for you to constantly manage multiple locations.

Each user's Exchange credentials are stored within the Avaya Messaging mailbox, allowing the server to synchronize messages to and from the Exchange server. End users can manage their credentials through Web Access. Administrators may also manage credentials from the admin console.

The use of EWS for Exchange 2019 and 2016 is required since IMAP is no longer supported. This chapter may be applied to both versions.

Visual Guide



When a voice server integrates with an email server, the data between the two is synchronized, allowing for accurate information regardless of the point of access. Receiving messages, and any actions performed by the users is synchronized between the two servers constantly, ensuring that your content is always up to date.

Administrators can also customize what is synchronized. A full synch includes contact and calendar entries along with messages. If the system has telephone and message light integration, MWI (message waiting lights) will also remain accurate since the status of messages are synchronized between the servers.

Requirements

Requirements	Details
License	IMAPCSE License
Software	Avaya Messaging version 10.5 or higher

Server Configuration

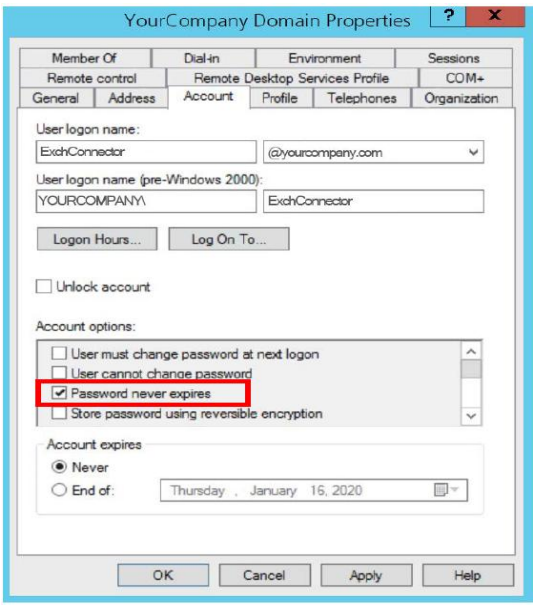
Server configuration requires the creation of a superuser account from the active directory that has the necessary permissions within the Exchange console. Once the account has been made, it must be added to the voice server configuration, and the channel of communication between the two servers must be established.
Your Exchange server must also have Exchange Web Services (EWS) enabled Avaya Messaging to communicate properly.
You must have a corporate Exchange server, either locally or virtually, configured and operating before proceeding.

Caution: Exchanges 2019 and 2016 do not support non-EWS connections. Only EWS can be used.

Exchange Superuser Creation/Configuration

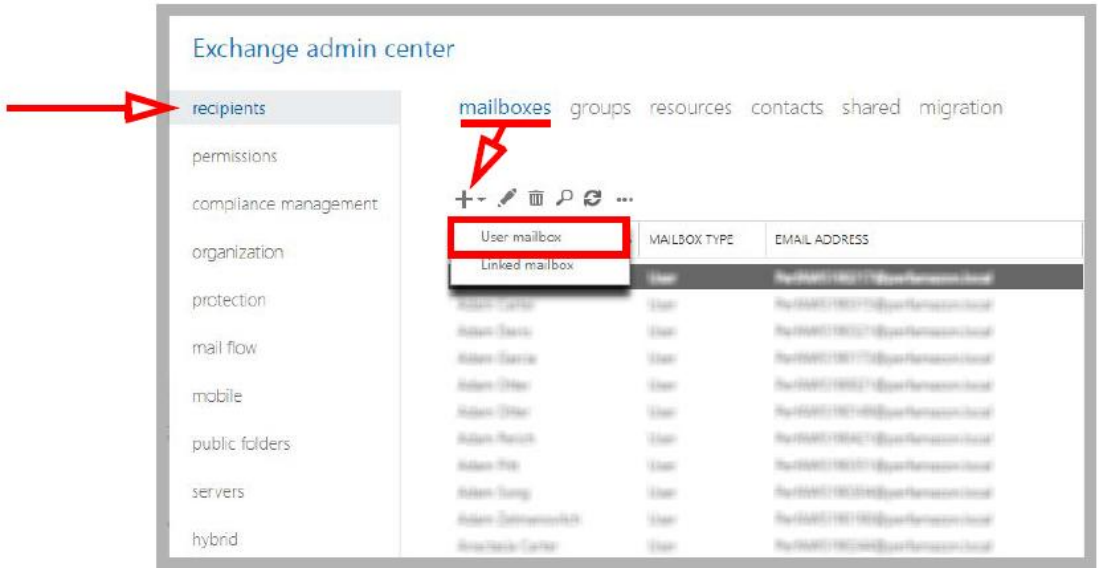
Once the superuser account is ready on Active Directory, create a mailbox for that user in the Exchange environment.

1. As an administrator, create a new user on your network using Active Directory. Configure any Organizational Units or company policies as required. This user **MUST** have **Password never expires** enabled.

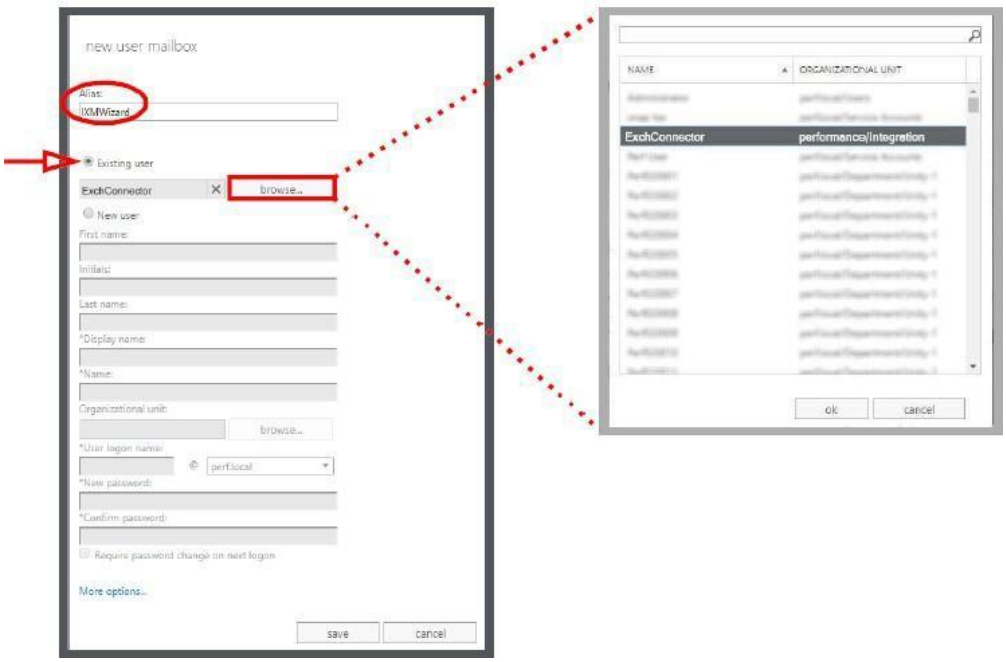


2. Open the **Exchange admin center** in a browser (e.g.,

https://IPaddressOfExchangeServer/ecp). Login with the Exchange Admin credentials. Go to the **recipients** menu at **the mailboxes** tab. Click **New**. Select **User mailbox**.

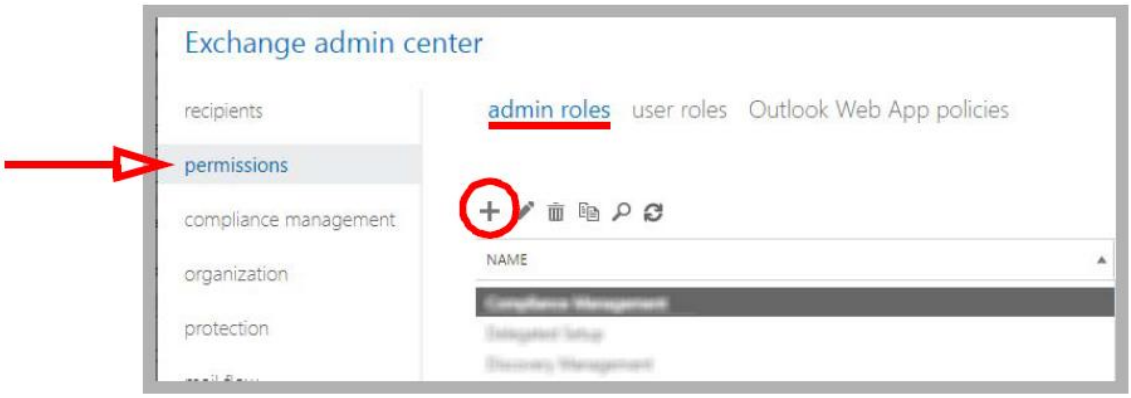


3. Enable **Existing user**. Click **browse** and select the user created in step 1. Provide a human friendly **Alias** to refer to this user.

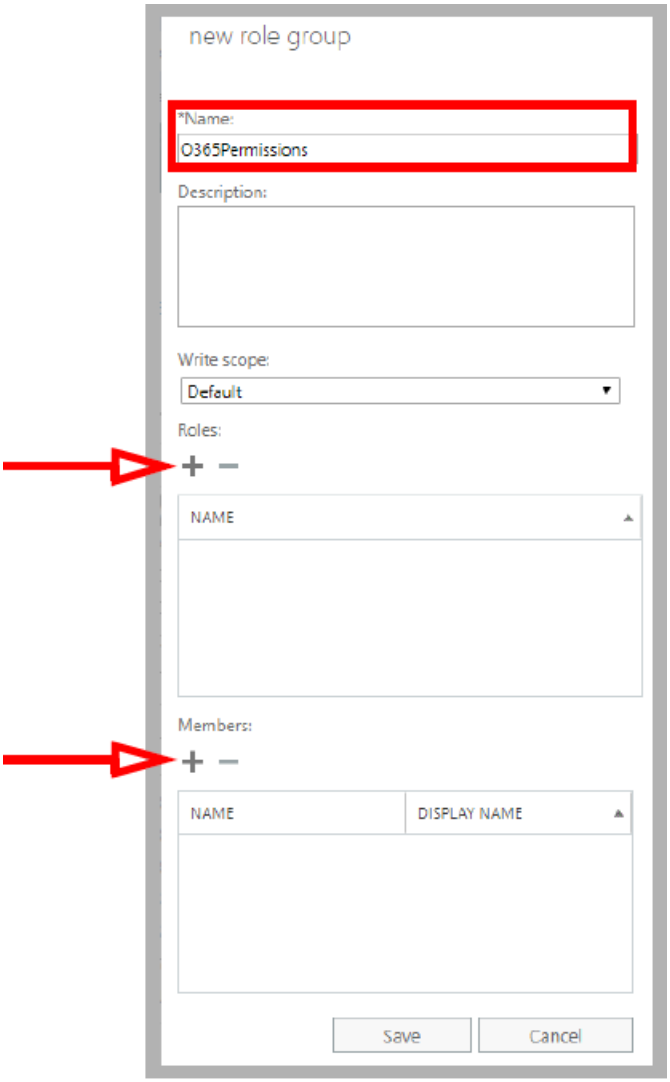


When ready, click **Save**.

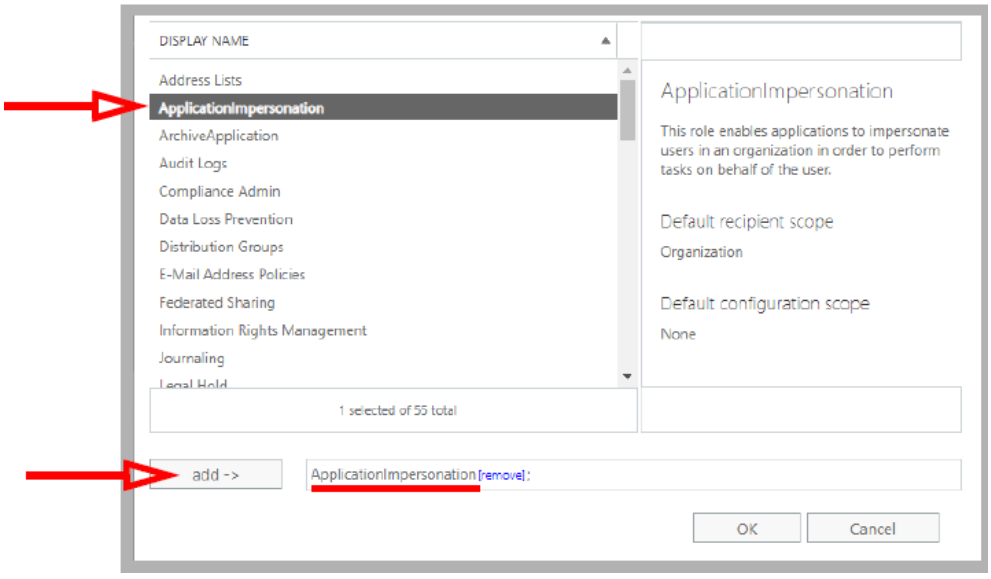
4. In the left-hand panel, select **permissions**. Under the **admin roles** tab, click **New**.



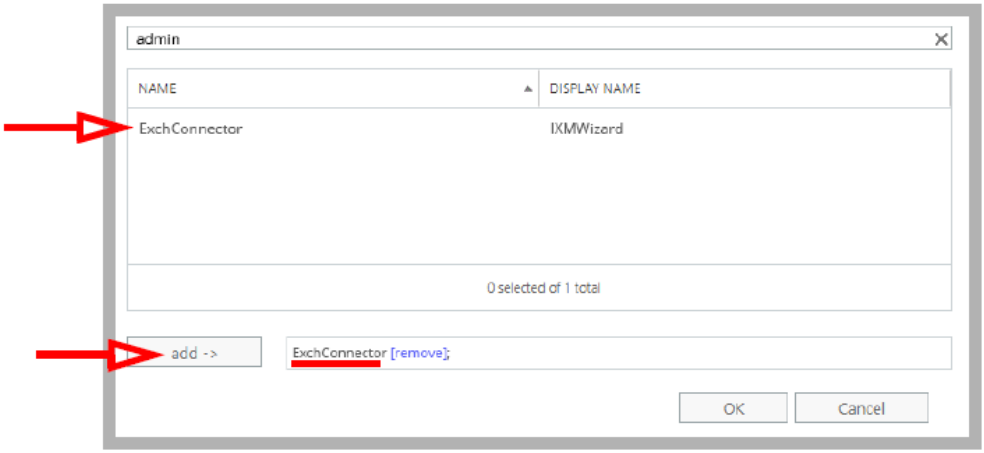
5. Give the Role a name (a Description is optional). Besides **Roles**, click **Add.**



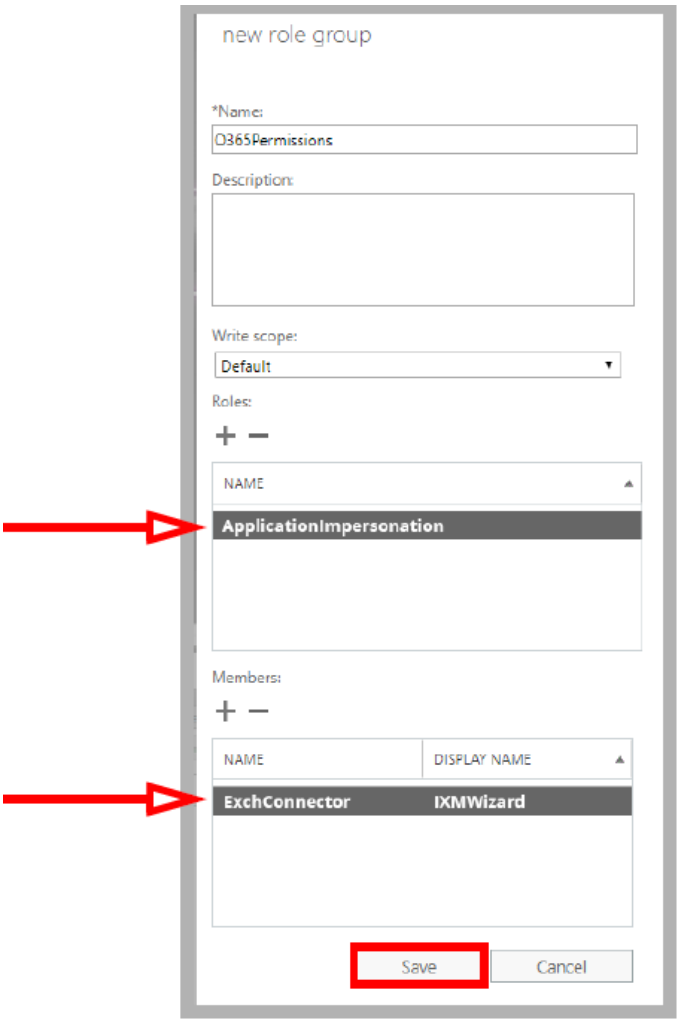
6. Select ApplicationImpersonation and click **add ->**. Click **OK**.



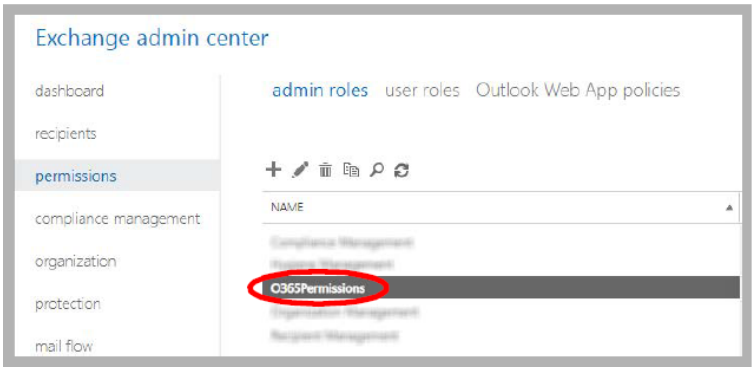
7. Below **Members**, click **Add** . Locate the account you just created, select it and click **add ->.** Click **OK**.



8. Returning to the **new role group** pane, click **Save**.



Confirm that the new role appears in the list.



A new account has been created.

AM Admin Configuration

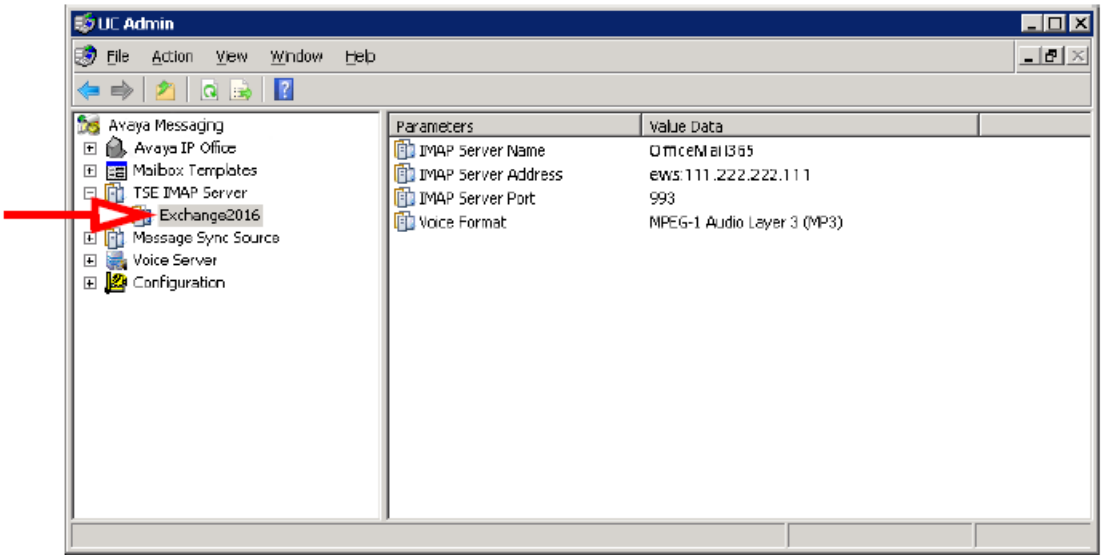
For Avaya Messaging and Exchange to be able to synchronize data, Avaya Messaging must be able to communicate with the Exchange server using the correct credentials. The superuser account streamlines this process while still enforcing individual password security protocols on each mailbox.

Adding the CSE Endpoint for EWS

For the Avaya Messaging server to recognize the Exchange server, you must configure a CSE Endpoint entry in the **Avaya Messaging Admin > TSE IMAP Server** section to use the EWS server. An entry should already be present in Avaya Messaging Admin based upon the choice of email client you made during installation.

Note: **TSE** is the previous name for **CSE** services.

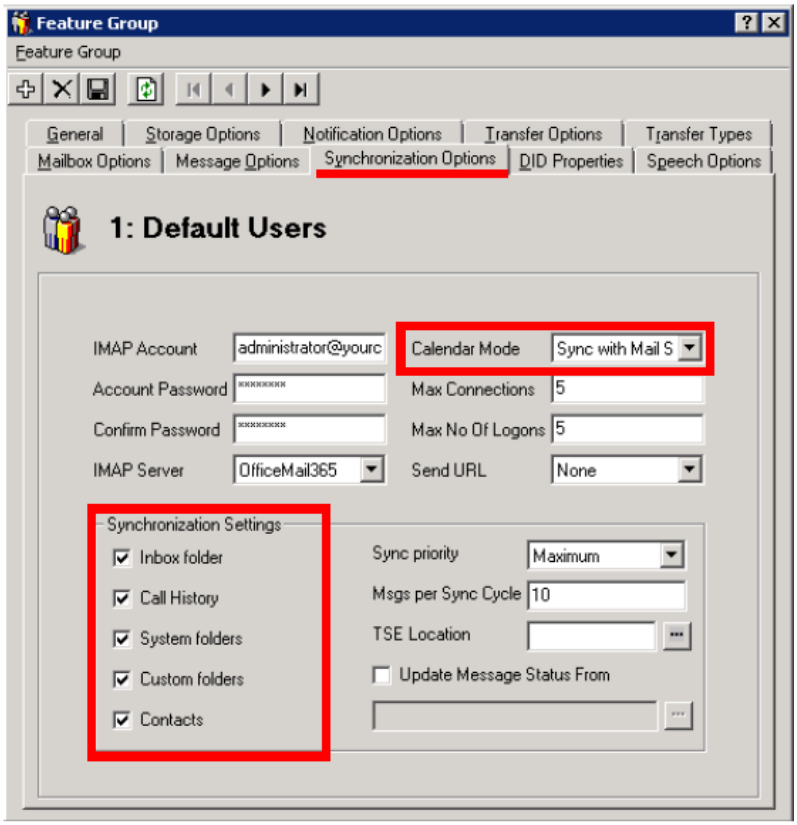
Double-click the server, or right-click and create a new one.



IMAP Server Name: This name is for your reference and does impact system performance.
IMAP Server Address: Enter the IP address of the EWS server. The address MUST be prefixed with **ews:** (all lower case, with a colon).
IMAP Server Port: Set this to the port number of the EWS server. The default is **993**.
Voice Format: Select the voice format used when sending voice messages to external voice servers.

Feature Group Configuration

Once the TSE IMAP Server entry has been created, go to **Feature Group > Synchronization Options** and modify the Office 365 user mailboxes as follows:
IMAP Account: Enter the user/service account created in step 3 above. Include the complete user@domain.com (e.g., **administrator@yourcompany.onmicrosoft.com**).
Account / Confirm Password: Enter the super user/service account password from step 3.
IMAP Server: Type in the name of the **IMAP TSE Server** created in the previous step (e.g., **OfficeMail365**).
Calendar Mode: If calendar synchronization is required, select **Sync with Mail Server Calendar** from the dropdown menu. Otherwise, select **None**.
Synchronization Settings: Set these options to specify which information will be synchronized between servers.

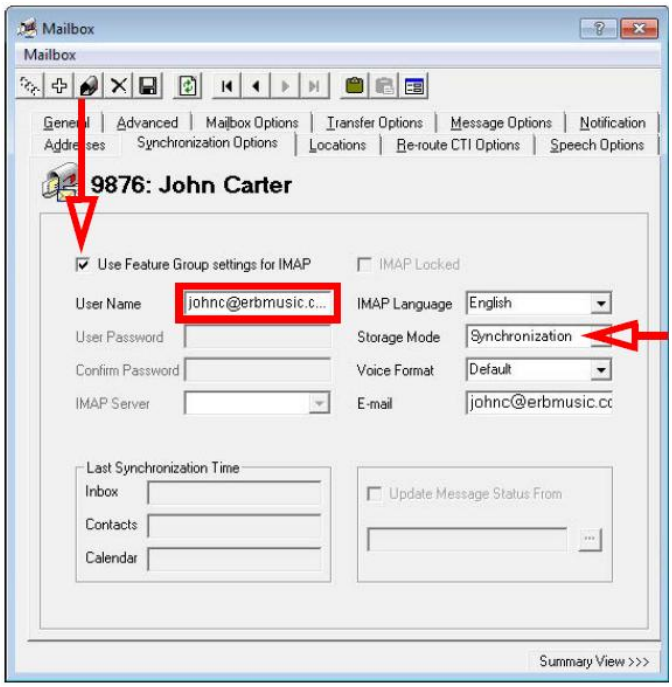


Save all changes.

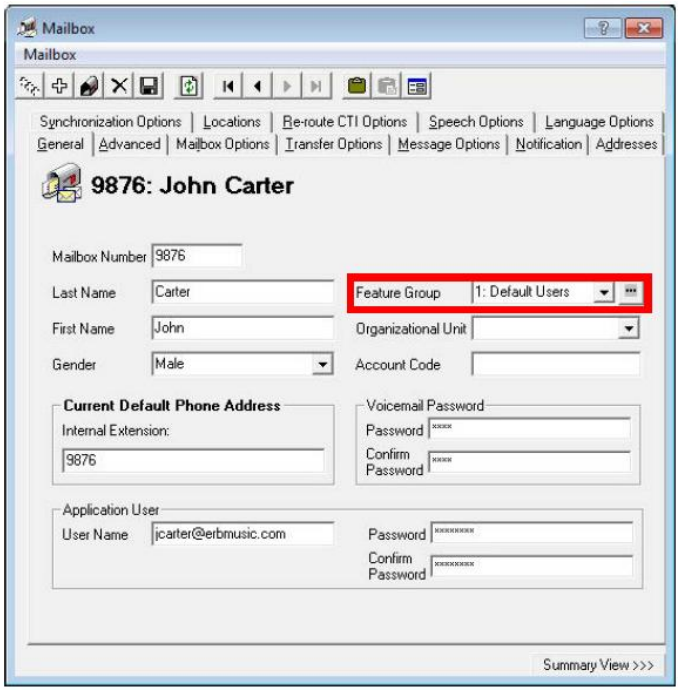
Individual Mailbox Configuration

With the superuser account, you do not have to enter the individual mailbox credentials for CSE synchronization.
Enable **Use Feature Group settings for IMAP** then enter the **User Name** in the format **user@companydomain.com**. Set the **Storage Mode** to **Synchronization**.

Note: The user must be an **Advanced** user to utilize synchronization.



Assign the mailbox to the **Feature Group** that is going to have the superuser account credentials. Save all changes and move onto Feature Group Configuration.



Certificate Configuration

To ensure that the communication between Avaya Messaging and the Exchange server is not interrupted by security measures, install the certificate from the Exchange server computer on the Avaya Messaging voice server.

For a site using High Availability, install the certificate on the Consolidated Server, and on all Remote CSE servers.

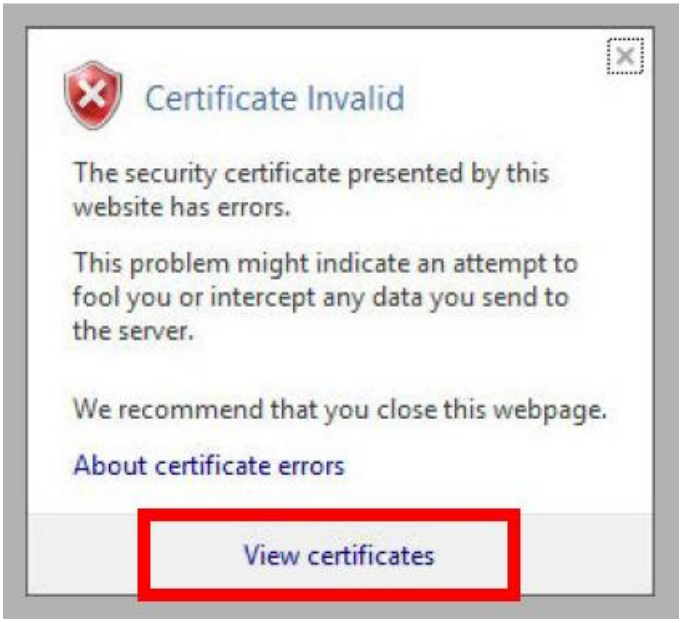
The simplest way to achieve this is to access the OWA (Outlook Web App) web page for Exchange on the voice server.

Note: This procedure may vary depending on the way in which you have the domain servers configured. **The goal of this process is to add the Exchange server as a trusted PC on the Avaya Messaging server computer**, which can be accomplished manually by the system administrator.

1. Open the **Internet Explorer** web browser, then navigate to your company's OWA web page(e.g. https://111.222.1.0/owa).
2. In the title bar, click the certificate error tab.



3. Click **View certificates.**



4. Click **Install Certificate** to launch certificate wizard.

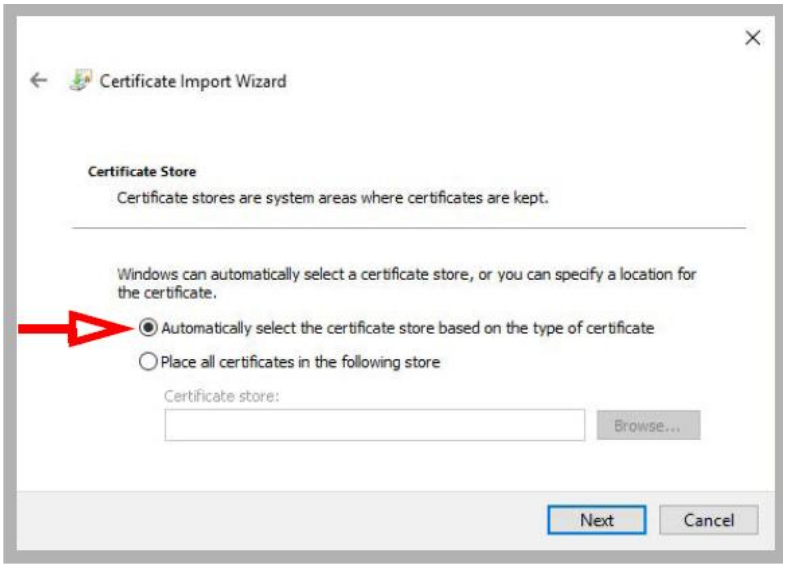
   Caution: For all certificates, always ensure that you are on the proper web page and confirm the issuer of the certificate for security purposes before proceeding with the installation.



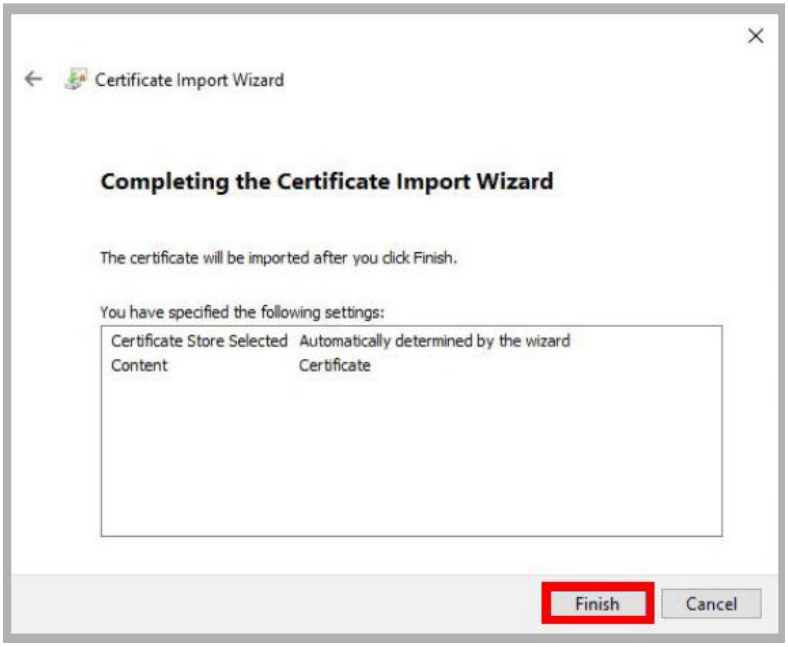
5. Enable **Current User** and click **Next**.


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel

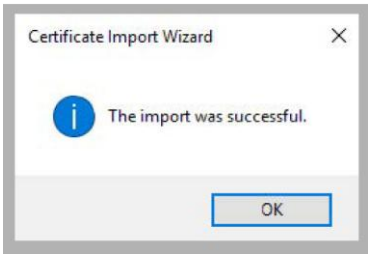
6. Enable **Automatically select the certificate store based on the type of certificate** then click **Next**.



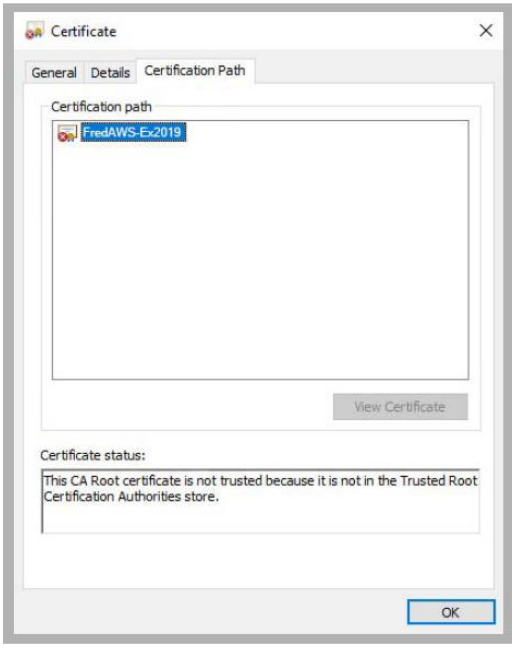
7. Confirm that the information is correct, then click **Finish.**



8. The following popup confirms the imports were successful. Click **OK**.



9. You will be able to confirm the status of the certificate through this window.
   Note: Ensure that the domain server is also certified, not just the Exchange server



   The certificate configuration is now complete. Restart the servers to ensure that the services are properly initialized.

Contact and Calendar Sync

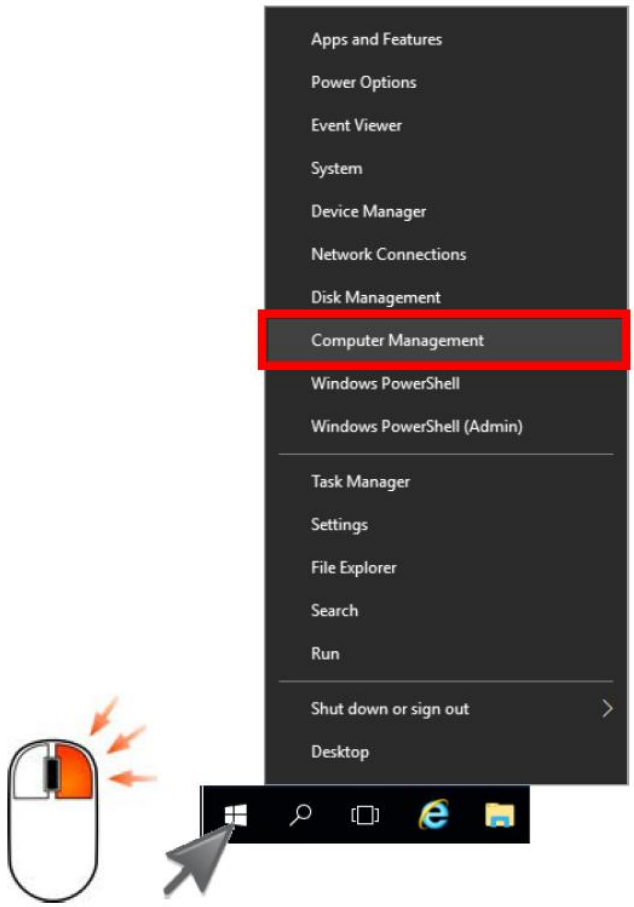
Once you have configured the IMAP CSE server with your mail server, you will be able to select the degree of synchronization from the Feature Group. Ensure that you verify all the information so that users do not lose any calendar, contact or message data during synchronization.

Warning: As a precaution, **backup the calendar and/or contact events** of your users before proceeding with the contact and calendar synchronization.

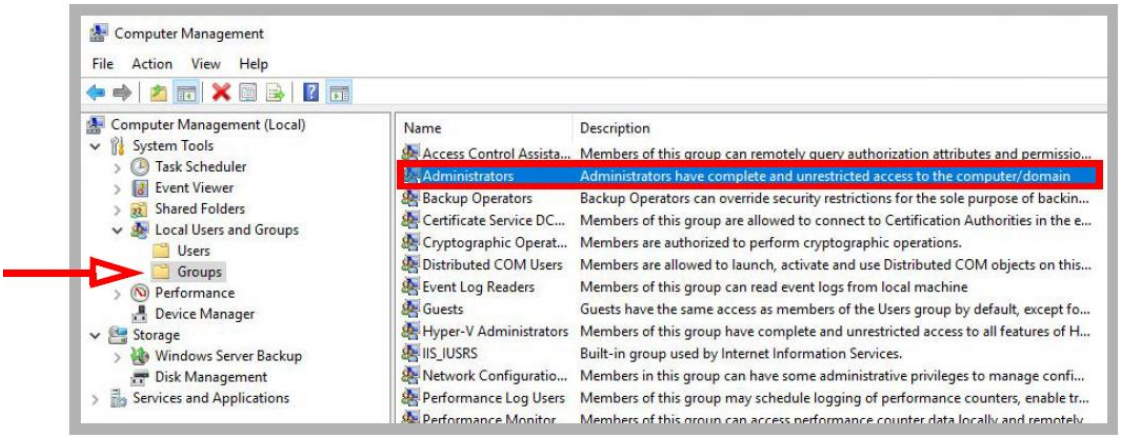
Windows Configuration

The Superuser account must be configured as a local administrator on the voice server computer.

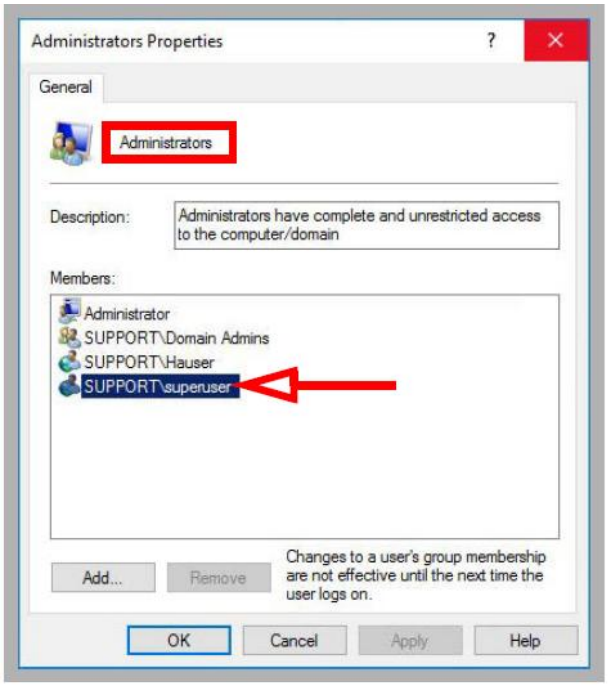
1. In Windows, right-click the Start menu and choose **Computer Management**.



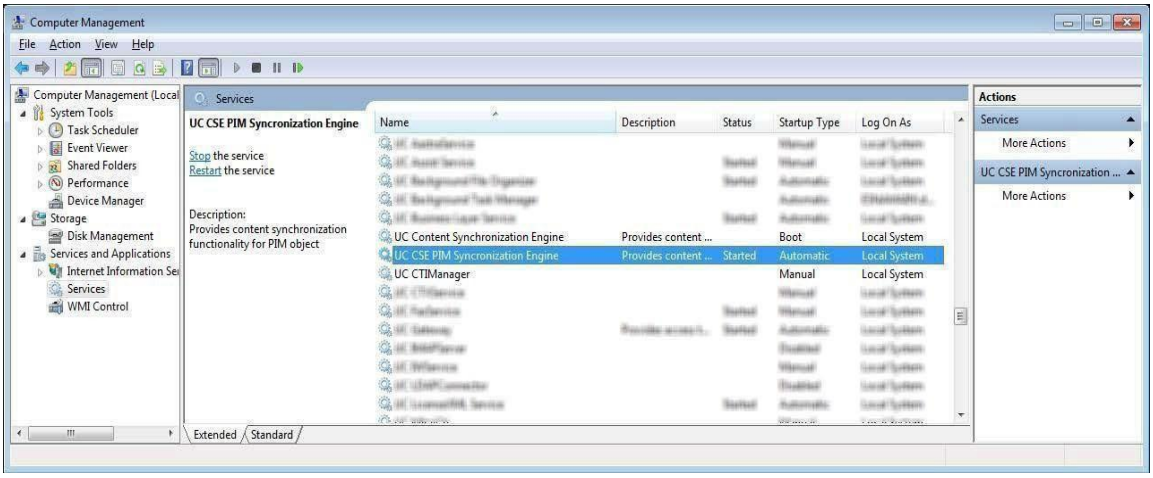
2. Go to **System Tools > Local Users and Groups > Groups**. Double-click **Administrators**.



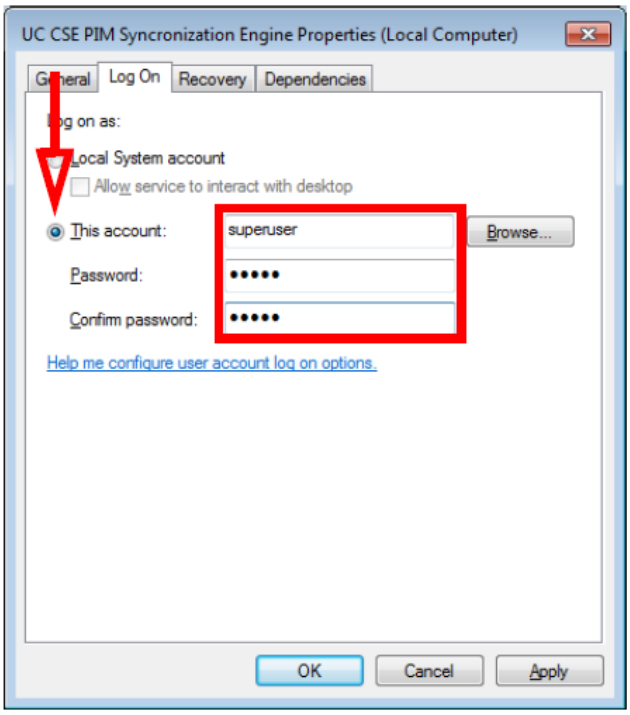
3. Ensure that the Superuser account created has the proper permissions on the Windows environment.



4. The **UC CSE PIM Synchronization Engine** service must login and run with the Superuser credentials.
Open the **Computer Management** console and select **Services**.



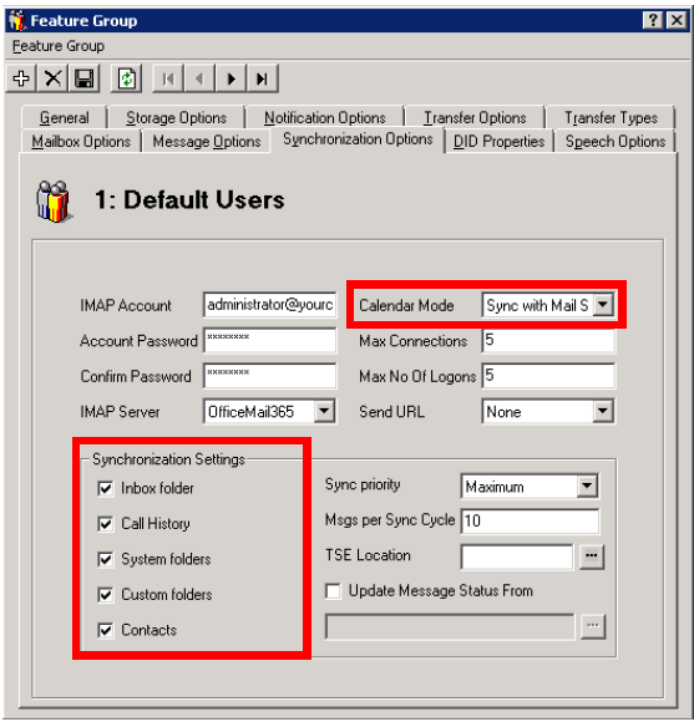
5. Right-click the service and select **Properties**.
Go to the Log On tab and enable **This Account**.
Enter the username and password for the superuser account in the spaces provided.



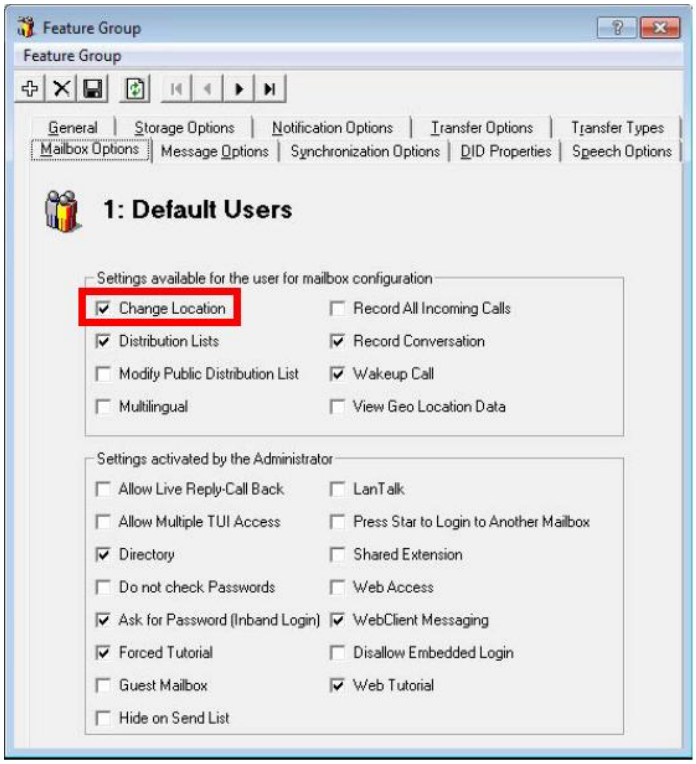
6. Click **Apply** and **OK** when finished.
7. Restart the service.

Avaya Messaging Configuration - Feature Group

Feature Group configuration requires changes on two tabs, **Synchronization Options** and **Mailbox Options**. You can define exactly what is going to be synchronized for the users from these two sections.
From the **Synchronization Options** tab, you can specify which messages are going to be synchronized between the servers.
Enable **Contacts** if you wish to enable contact synchronization between the two servers.
To enable calendar synchronization, select **Sync with Mail Server** from the **Calendar Mode** dropdown menu.
The other fields, such as Inbox Folder, are used for message synchronization between the servers. Refer to the message integration section for details.



From the **Mailbox Options** tab, **Change Location** to allow an event on the mail server calendar to automatically change the UC location of the user.



By customizing these settings you can easily segregate calendar and contact synchronization along with message synchronization when enabling features for your users, allowing you to control exactly who has access to certain features.

Once calendar and contact synchronization has been enabled, all transactions occur on the server in the background, so you do not have to configure anything on your own. Use your mail server as you normally would, and any calendar or contact entries will now be mirrored in your Avaya Messaging mailbox as well.

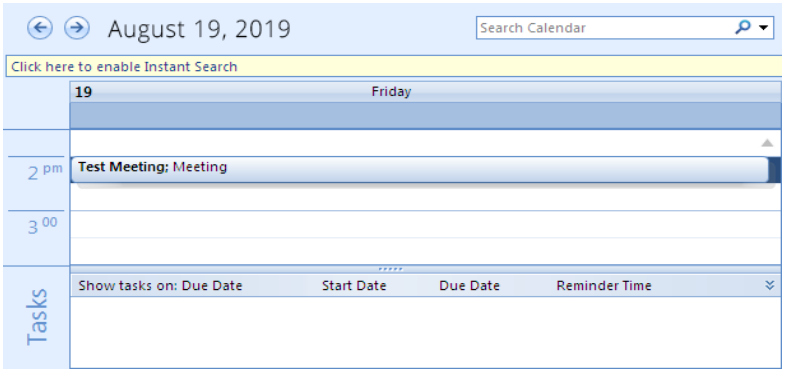
The following is typical behavior for synchronization so that you can understand exactly how your calendar and contact entries are being handled by the servers.

Note: All the calendar events and contacts from your mail server will be copied into your Avaya Messaging mailbox as soon as the administrator finishes configuring the systems.

Note: Backup your calendar events and contacts periodically as a precaution.

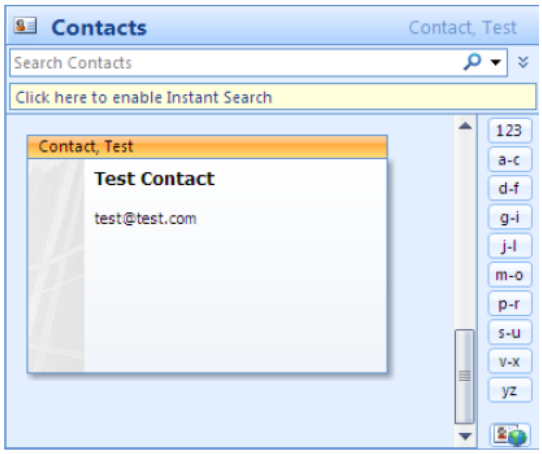
Calendar Synchronization

When you create a calendar entry in Outlook, or most other email programs, the same entry will appear in your Avaya Messaging mailbox. The time and date of the meeting is automatically sent to the Avaya Messaging mailbox. By default, the location for these events will be marked as **Meeting**.



Contact Synchronization

When you create a contact entry from Outlook, the entry will be copied into your Avaya Messaging mailbox. Contact information is automatically sent to the Avaya Messaging mailbox.



Contact information is automatically sent to the Avaya Messaging mailbox.



Caution: Deleting contacts is also synchronized. If you delete an entry from Outlook, it will also be deleted from Avaya Messaging, and vice versa.

Synchronization Limits

When using EWS with Exchange, message synchronization is one-way only, from Avaya Messaging to Exchange. Any messages created using Avaya Messaging will appear in Exchange, whereas messages created in Exchange will not appear in Avaya Messaging.

Message synchronization can place a significant burden on the voice servers which can lead to delays. Changes may take some time to appear on the other side.

MS Exchange Performance Considerations

Be aware that large numbers of items in folders can decrease the speed of operations in Exchange. This table shows the maximum number of files recommended per folder for optimum server performance.

Items in Folder	**Exchange 2016**
Messages	<100000
Contract and Calendar Entries	<10000

Chapter 10: OFFICE 365 INTEGRATION WITH MICROSOFT GRAPH

Guidelines

Depending upon your site's requirements and software, you have the option to integrate Avaya Messaging with several email systems. None of these are required. Where appropriate, refer to the chapter that best suits your requirements.

Introduction

This configuration note describes the implementation of unified messaging between Office 365 and Avaya's Avaya Messaging using Microsoft Graph as an alternative for Microsoft's Exchange Web Services.

Warning: The instructions found in this guide cannot be guaranteed to work for all installations since each site is unique. Some problems may arise even if you follow these instructions precisely. Therefore, use this document as a reference for your own configuration, making the changes appropriate to your site's specific requirements.

Note: This document describes the standard configuration for the integration of Avaya Messaging with Microsoft Office 365. For a high security connection, such as for sites requiring JITC compliance, please contact your vendor to purchase Professional Services support.

Pre-requisites

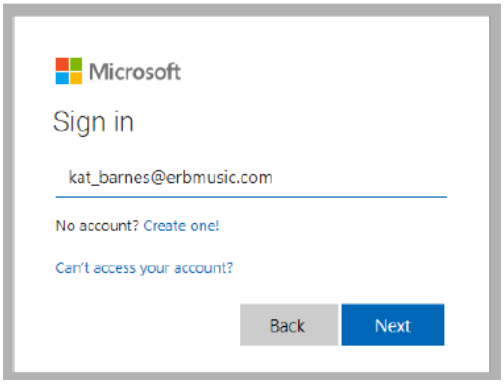
The following preliminary steps must be completed before the integration can begin:
• The Office 365 domain has been set up and deployed (requires Mid-size Business and Enterprise plan minimum, E1 or E3).
• You must have administrative access to Office 365 domain.
• Avaya Messaging Server installed and running (refer to Avaya's documentation website).

Connecting Through Microsoft Graph

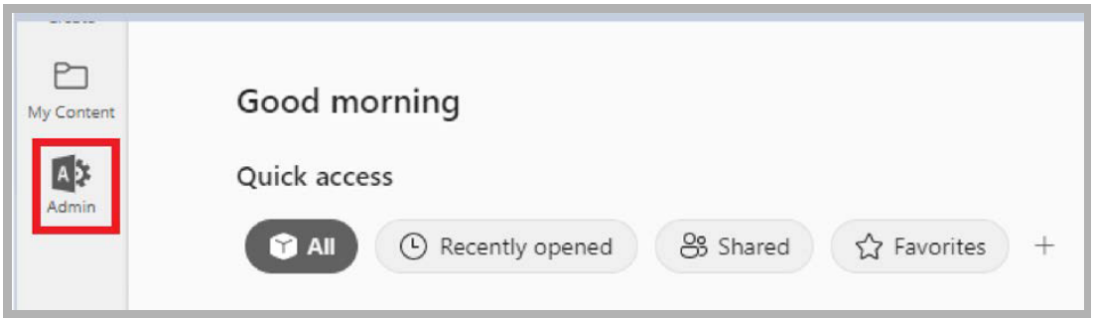
As an option, Avaya Messaging can be connected to Office 365 using Microsoft Graph. This adds an additional layer of security to your traffic flows communication.

Warning: This section contains advanced concepts and programming steps that could adversely affect operations if handled incorrectly. Read through this instruction thoroughly before proceeding. If you are not confident to follow these instructions adequately, do not continue.

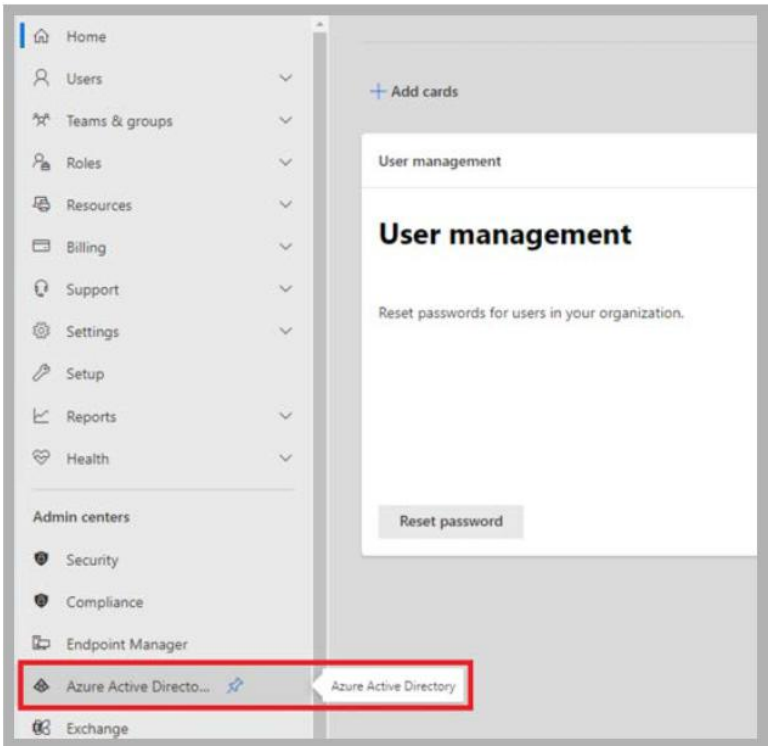
1. Open a web browser and go to Office 365 site at https://www.office.com.
   Click **Sign in** and login using your Office 365 administrator account credentials.
   Click **Next** when ready.



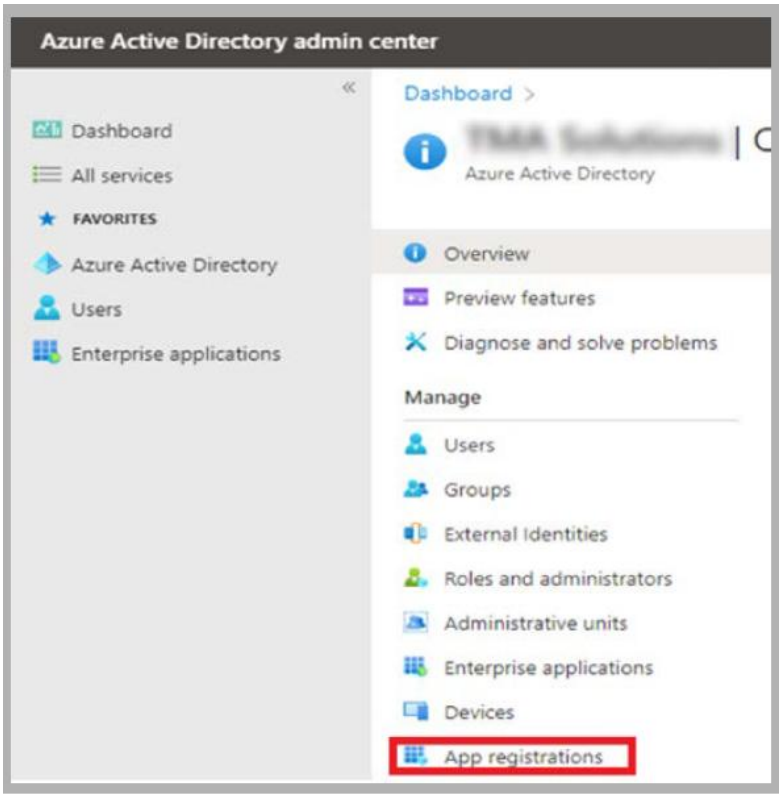
2. On the Office365 home page, click **Admin**.



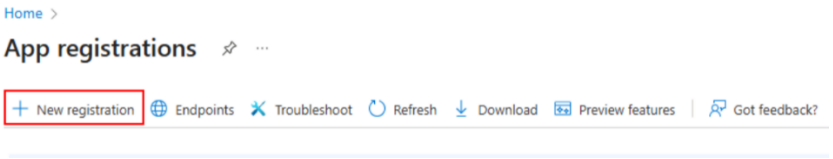
3. In the left-hand panel (**Show All**), under **Admin centers**, select **Azure Active Directory**. The Azure dashboard will appear.



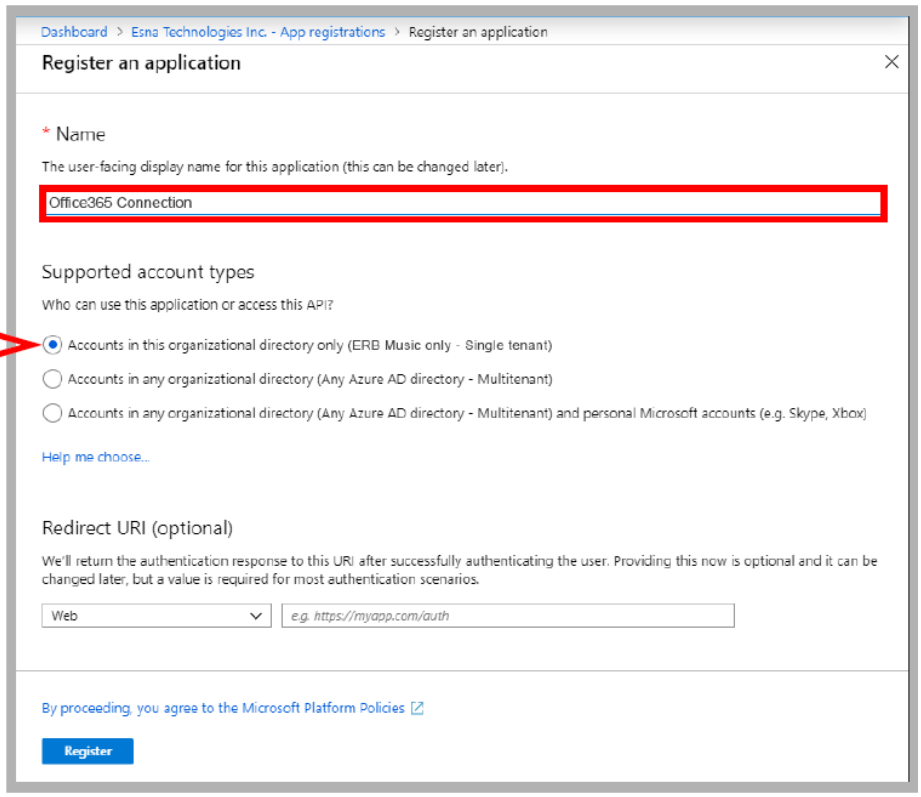
4. Open **Azure Active Directory** and select **App registrations**.



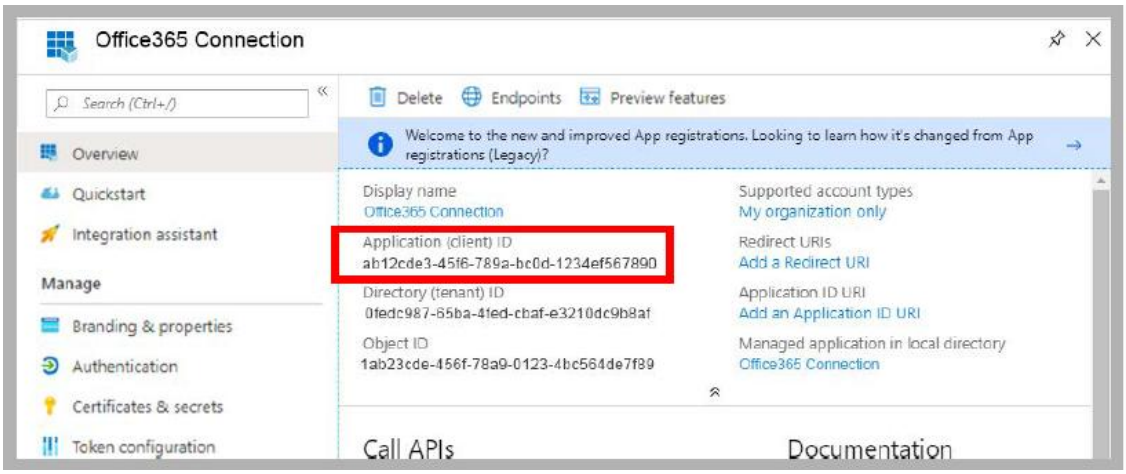
5. Click **New registration**.



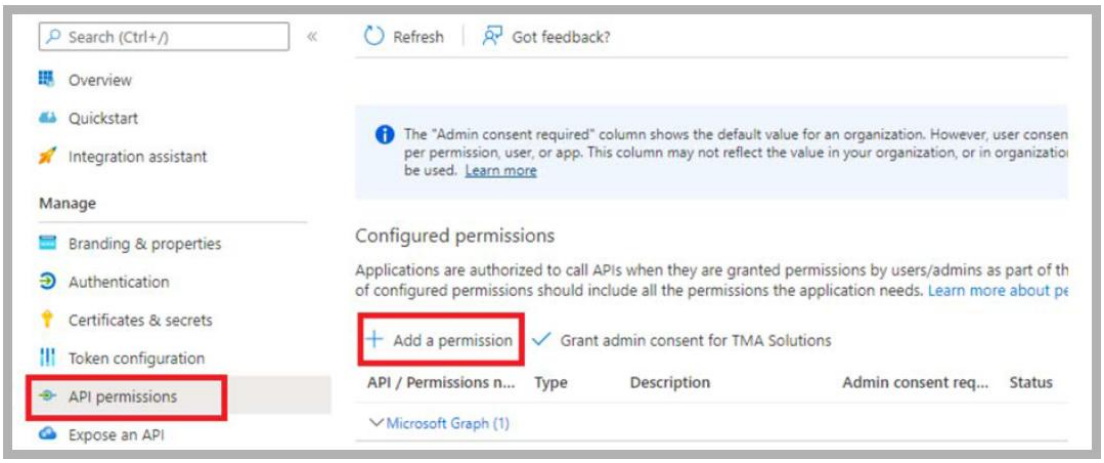
6. Provide a name for the registration. Enable **Accounts in this organizational directory only**. A redirect URI is not required. Click **Register**.



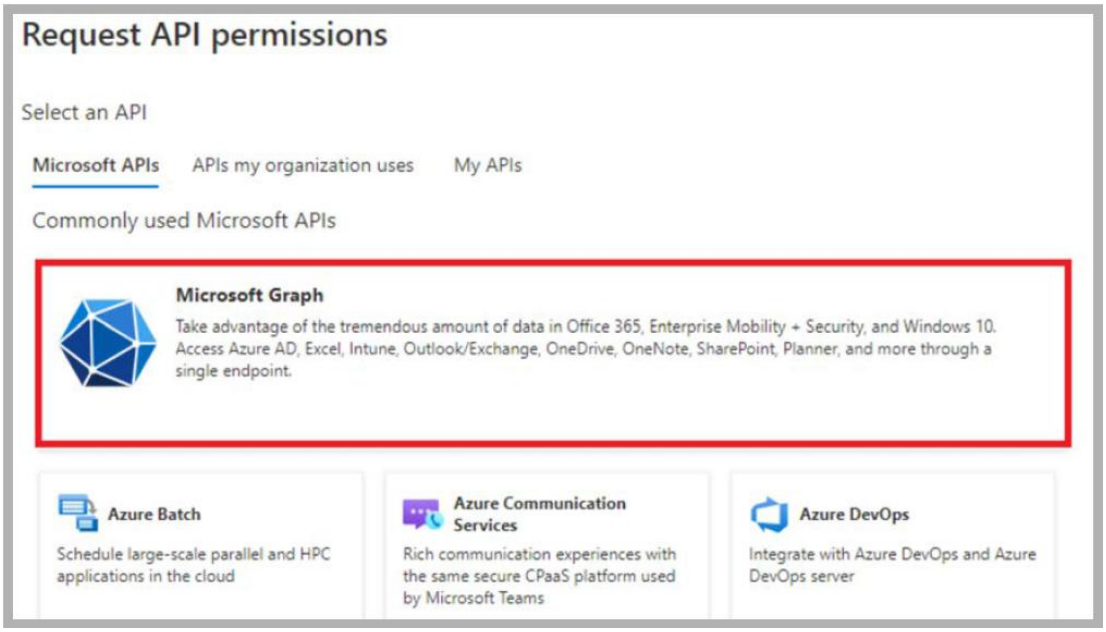
7. Record the value for **Application (client) ID**. This will become part of the username when configuring Feature Group access within Avaya Messaging.



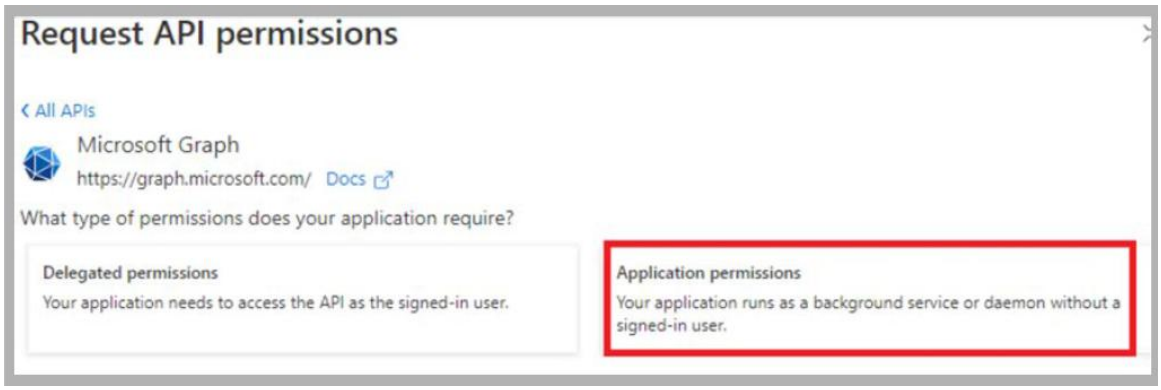
8. To configure the permissions for the application, click **API permissions > Add a permission**.



9. Under **Microsoft APIs**, select **Microsoft Graph**.



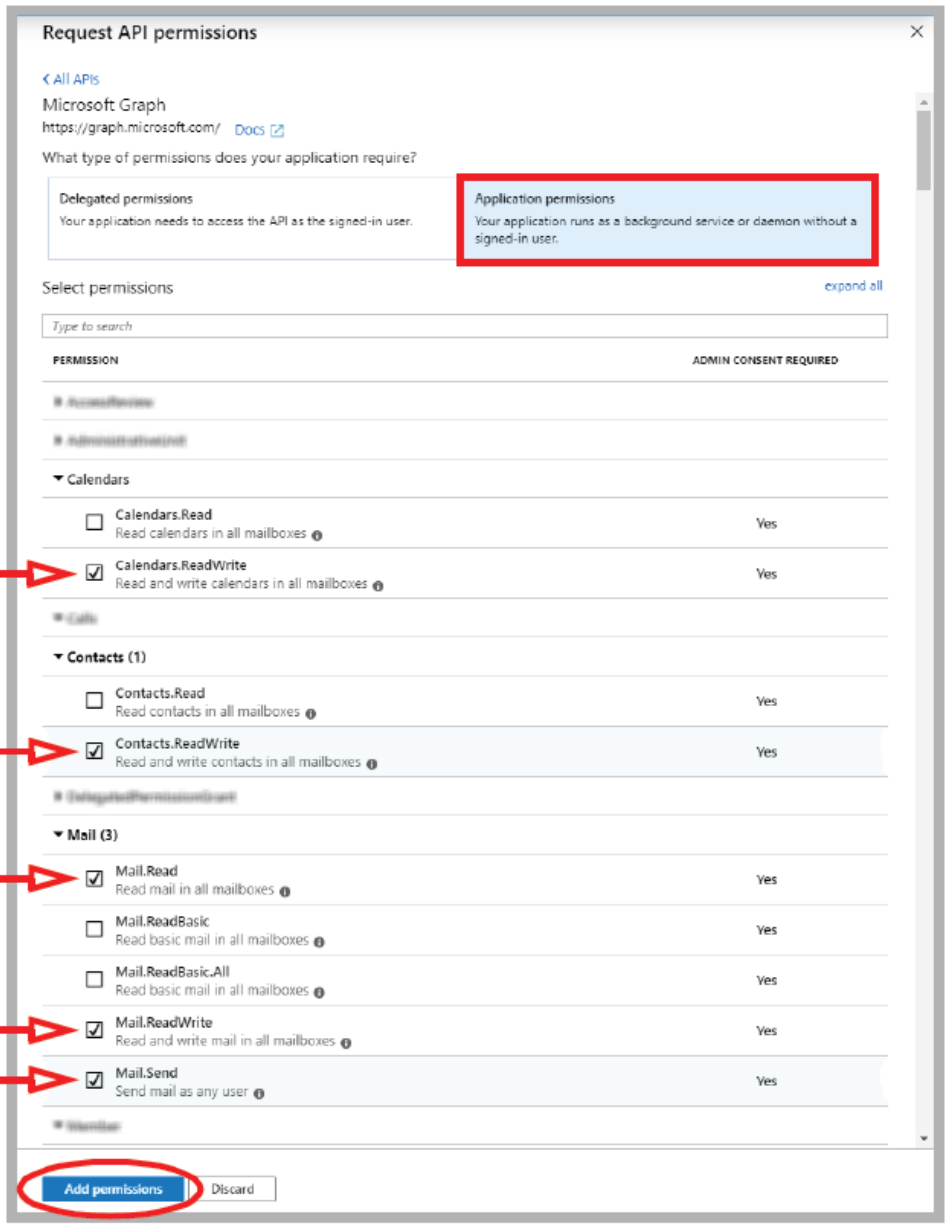
10. Choose **Application permissions**.



11. Under **Application Permissions**, enable:

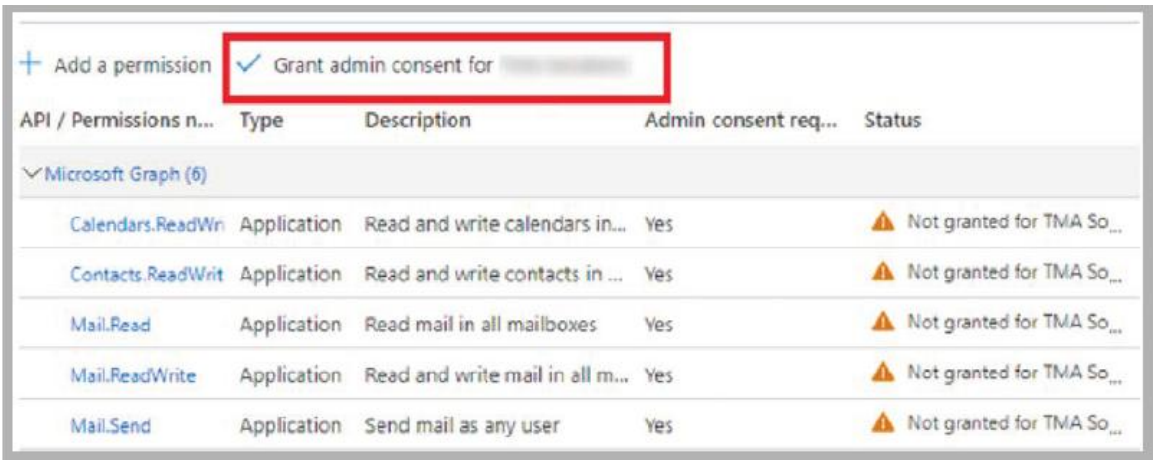
    - **Calendars.ReadWrite**
    - **Contacts.ReadWrite**
    - **Mail.Read**
    - **Mail.ReadWrite**
    - **Mail.Send**

    Click **Add permissions**.

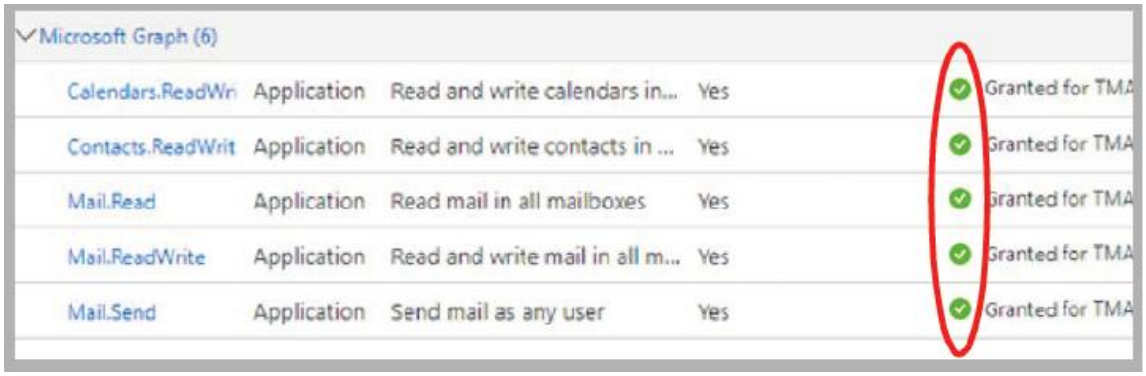


Note: The permissions that are required are based upon each site's requirements. For example, if Calendar or Contact synchronization is not necessary, then those permissions can be left out.

12. While logged in with an account with Global Admin/Privileged Role Administrators, enable Grant admin consent for your company.



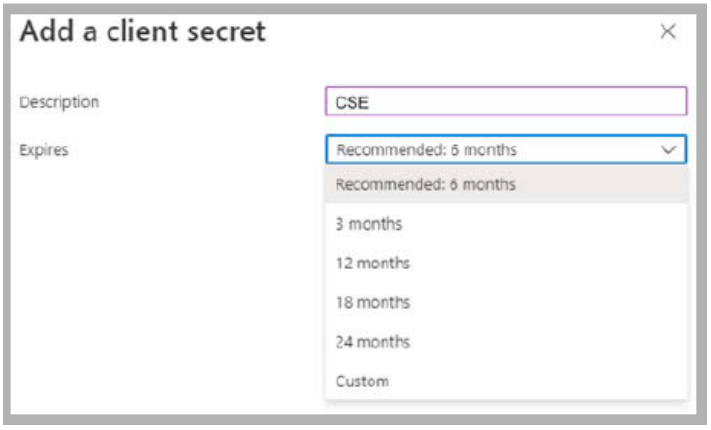
13. Ensure that all of the Status indicators are green for the permissions you just added. If not, delete them and start again.



14. Open **Certificates & secrets** and select **New client secret**.



15. Give the Secret a meaningful description. Choose when the Secret should expire. When ready, click **Add**.



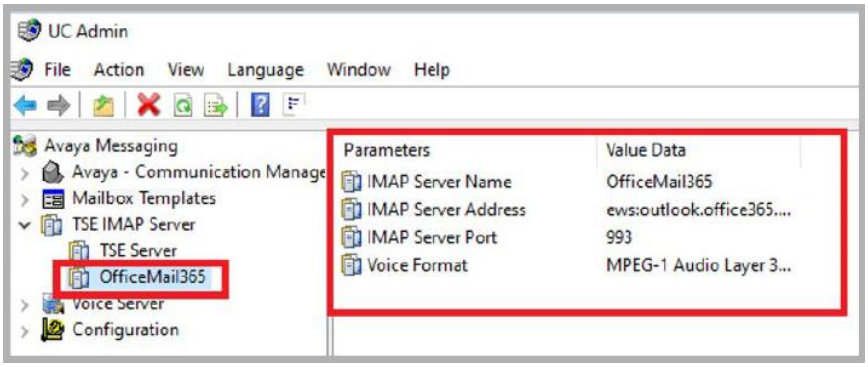
Important: Once a Secret expires, synchronization will no longer function until a new Secret is created.

16. Record the **Value** associated with the Secret. This is the password required when configuring the Feature Group in Avaya Messaging.



17. In Avaya Messaging Admin, add a new TSE IMAP server, and include the Office 365 server information.
IMAP Server Name: Enter a name for this connection (e.g., **OfficeMail365**). **IMAP Server Address**: Type in **ews:outlook.office365.com**.
IMAP Server Port: Set to **993** to enable SSL connectivity.
Voice Format: Select **MPEG-1 Audio Layer 3** (MP3) for client playback.

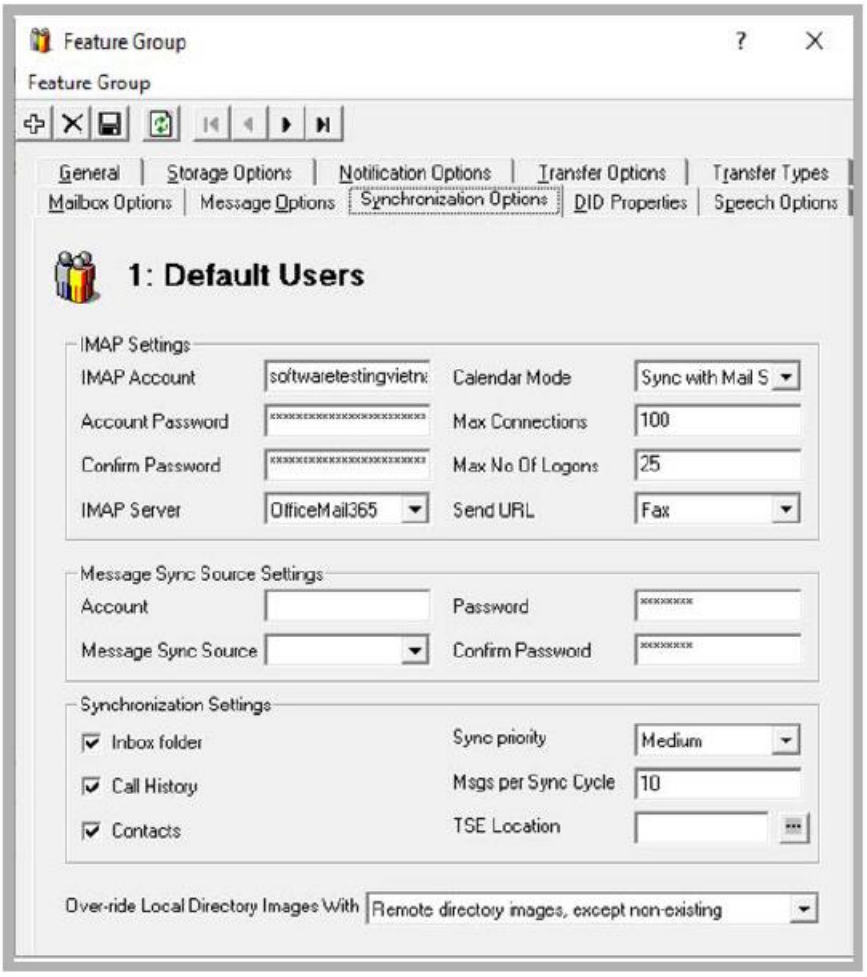
Click **OK** when ready.



18. Go to the **Feature Group> Synchronization Options** tab.

    Under **IMAP Settings**, configure:

    • **IMAP Account**: Enter your corporate Office 365 domain name, a forward slash, then the **Application (client) ID** recorded in step 7. e.g**., yourcompany.com/ab12cde3-45f6-789a-bc0d- 1234ef567890**).
    • **Account / Confirm Password**: Enter the **Client Secret Value** recorded in step 16. (e.g. **:]Ab=c1dEfGhijKlmno?pQRS2tUv3WX4**)
    • **IMAP Server**: From the dropdown menu, select the correct Office365 server. For example: **OfficeMail365**.
    • **Synchronization Settings**: Enable all of the items that you want to have synchronized between servers.
    • **Calendar Mode**: If calendar synchronization is required, select **Sync with Mail Server Calendar** from the dropdown menu. Otherwise, select **None.**

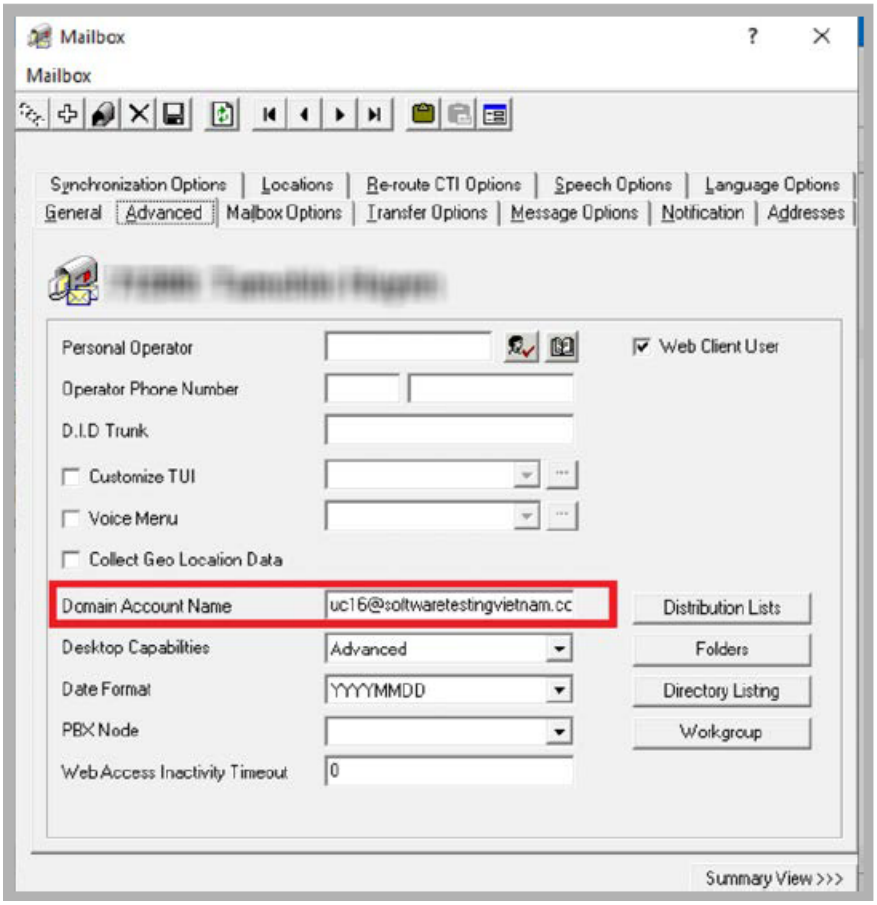


Note: The settings for the Office 365 connection through Graph can only be made to Feature Groups. These settings cannot be made at the mailbox level.

The configuration is complete.

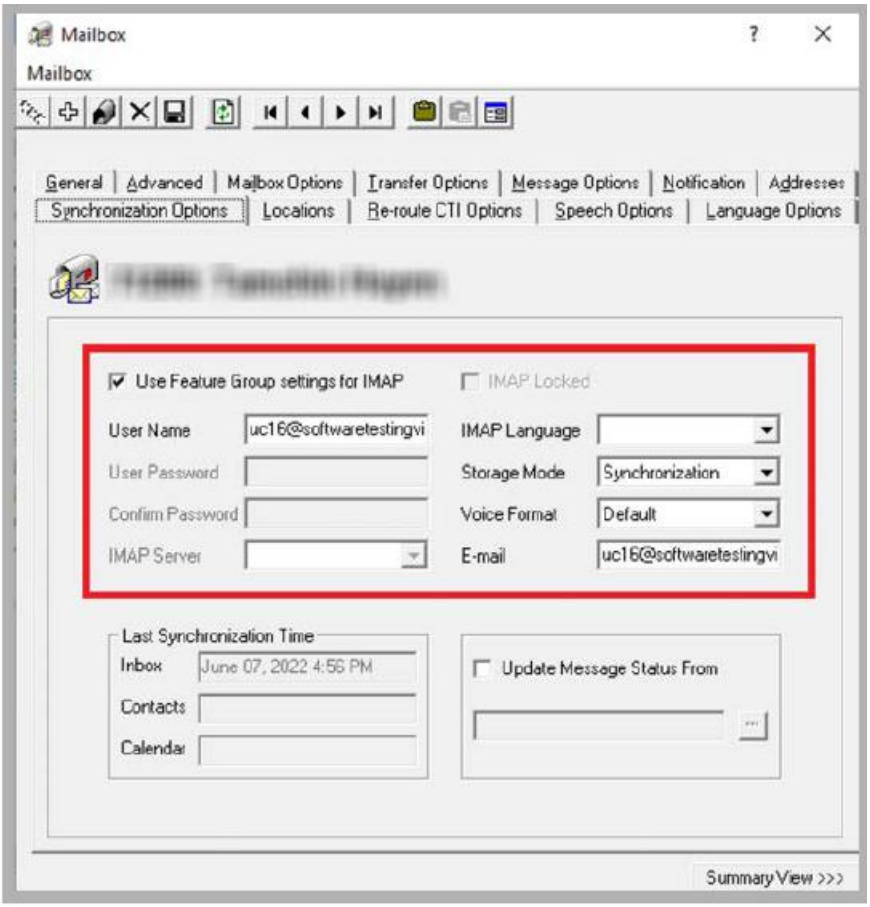
User Configurations

1. Open **Mailbox > Advanced** and enter your Office365 Account under **Domain Account Name.**



2. On the Synchronization Options tab:

   - Enable Use Feature Group settings for IMAP.
   - **UserName**: Enter you Office365 account.
   - **Storage Mode**: Set this to **Synchronization**.
   - **Voice Format**: Choose **Default.**
   - **E-mail**: Enter you Office365 email address.

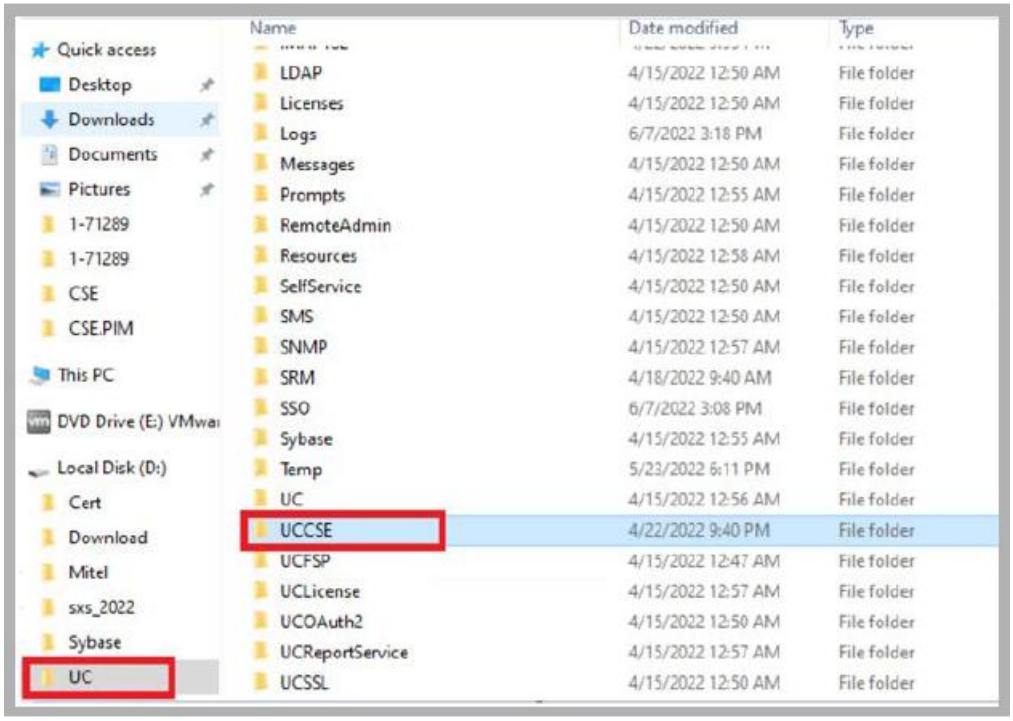


Reconfiguring Synchronization Components for Graph

Once the installation has been completed, modify the system configuration files to use EWS instead of IMAP. This should be done on all servers running CSE: The voice server in a single server environment, the Consolidated server under HA, and all remote CSE servers operating.

Note: The **CSE.exe.config** file is used with message synchronization, while the **CSE.PIM.exe.config** is used for contact and calendar synchronization.

1. Open the UC/UCCSE folder on the program installation drive.

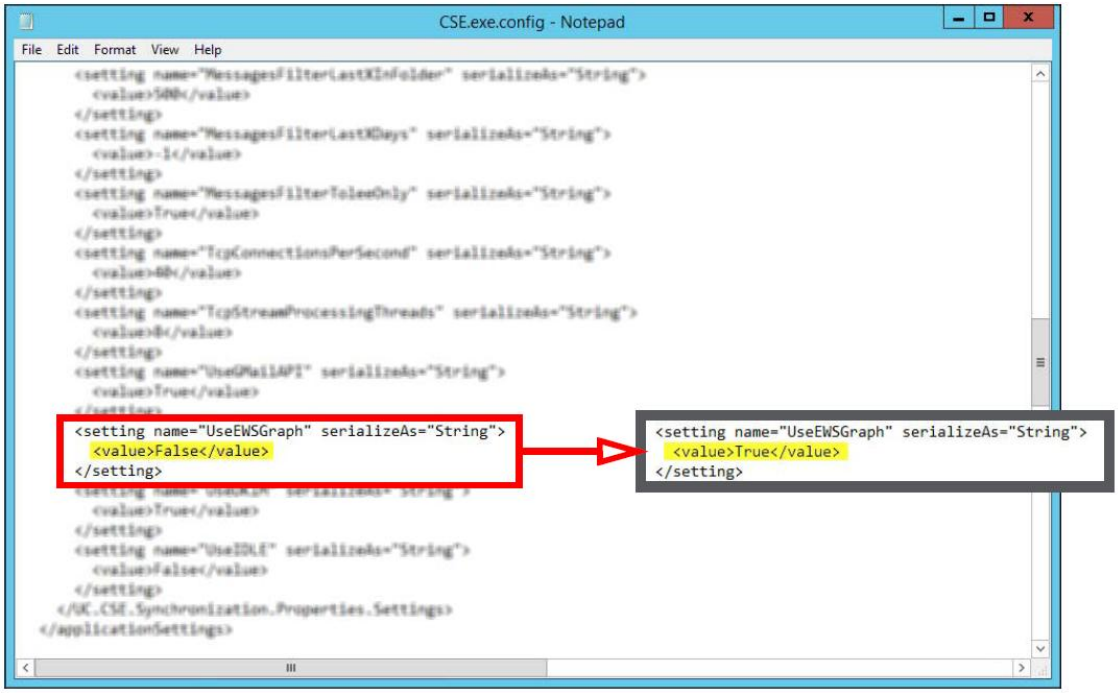


2. Within the folder, open the **CSE.exe.config** file in a text editor such as Notepad.



3. Scroll down to find the following lines (Use EWSGraph):

```
<setting name="UseEWSGraph" serializeAs="String">
<value>False</value>
</setting>
```



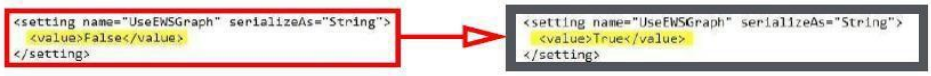
Verify that the **Value** is set to **True**. If the value is not True, change it and save the file.
<setting name="UseEWSGraph" serializeAs="String">
<value>**True**</value>
</setting>

4. Within the UCCSE folder, open the **CSE.PIM.exe.config** file in a text editor such as Notepad.



5. Scroll down to find the following lines (UseEWSGraph):

<setting name="UseEWSGraph" serializeAs="String">
<value>**False**</value>
</setting>



Verify that the **Value** is set to **True**. If the value is not True, change it and save the file.

<setting name="UseEWSGraph" serializeAs="String">
<value>**True**</value>
</setting>

IMPORTANT: If your network is setup behind a proxy server, make sure that Avaya Messaging resolves correctly and can reach these addresses: **outlook.office365.com**, **login.windows.net** (for authentication), **login.microsoftonline.com** (for authentication), and **graph.microsoft.com** (for getting API).

Restart Services

Before continuing, stop and restart the following services:
- UC Content Synchronization Engine
- UC CSE PIM Synchronization Engine

This will force Avaya Messaging to immediately update its systems. Otherwise, there will be a delay before the changes become active.

Note After Upgrading or Updating

Whenever Avaya Messaging is updated from an earlier version, it is important to check the settings configured above. During the update, these values will be overwritten with the default program settings. Repeat the steps given above to configure the software for use with MS Graph.

Chapter 11: AVAYA MESSAGING TO OFFICE 365 INTEGRATION WITH EWS

Guidelines

Depending upon your site's requirements and software, you have the option to integrate Avaya Messaging with several email systems. None of these are required. Where appropriate, refer to the chapter that best suits your requirements.

Introduction

This configuration note describes the implementation of unified messaging between Office 365 and Avaya's Avaya Messaging.

Warning: The instructions found in this guide cannot be guaranteed to work for all installations since each site is unique. Some problems may arise even if you follow these instructions precisely. Therefore, use this document as a reference for your own configuration, making the changes appropriate to your site's specific requirements.

Note: This document describes the standard configuration for the integration of Avaya Messaging with Microsoft Office 365. For a high security connection, such as for sites requiring JITC compliance, please contact your vendor to purchase Professional Services support.

Pre-requisites

The following preliminary steps must be completed before the integration can begin:

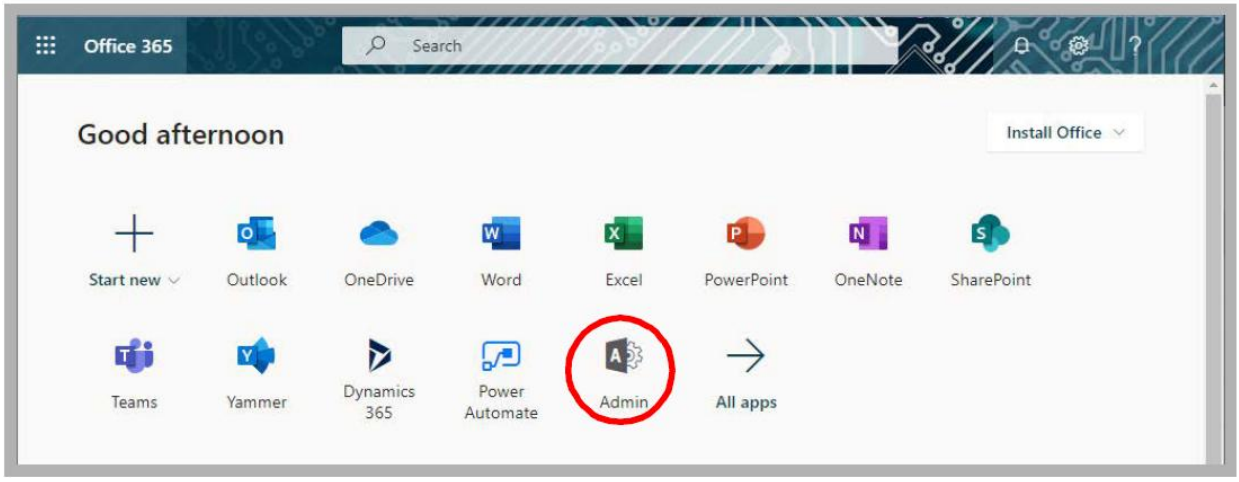
• The Office 365 domain has been set up and deployed (requires Midsize Business and Enterprise plan minimum, E1 or E3).

• Avaya Messaging Server installed and running (refer to Avaya's documentation website), either in a single server configuration, or in a High Availability environment (1 Consolidated server, 1 Primary server, 1+ Secondary servers).

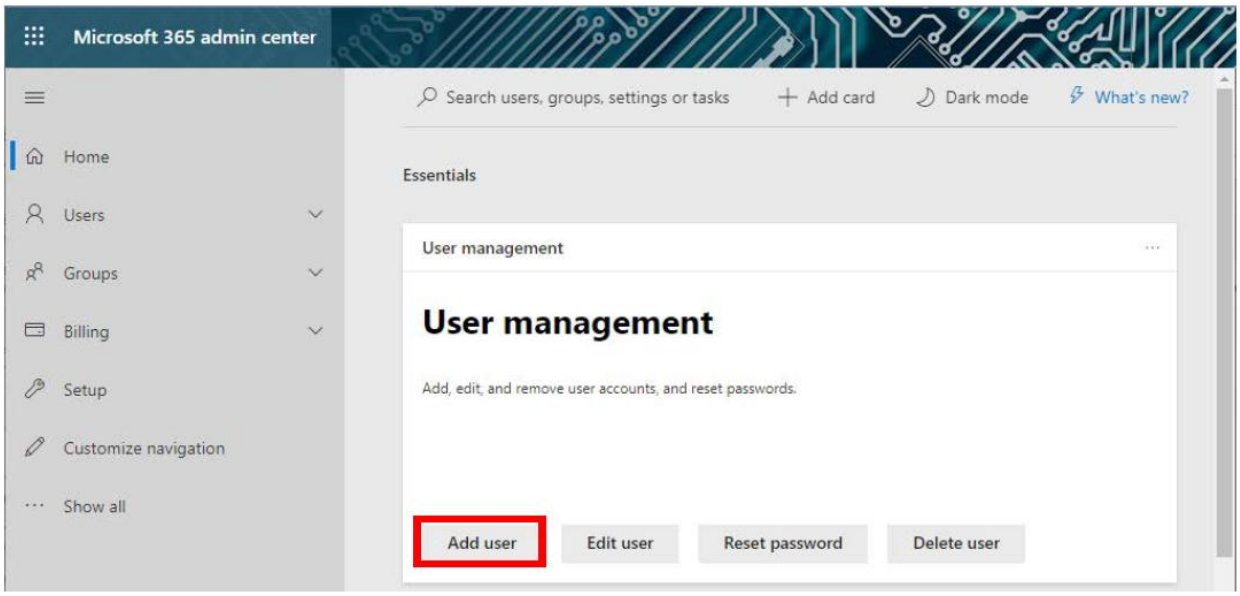
Office 365 Configuration

Web Interface Configuration

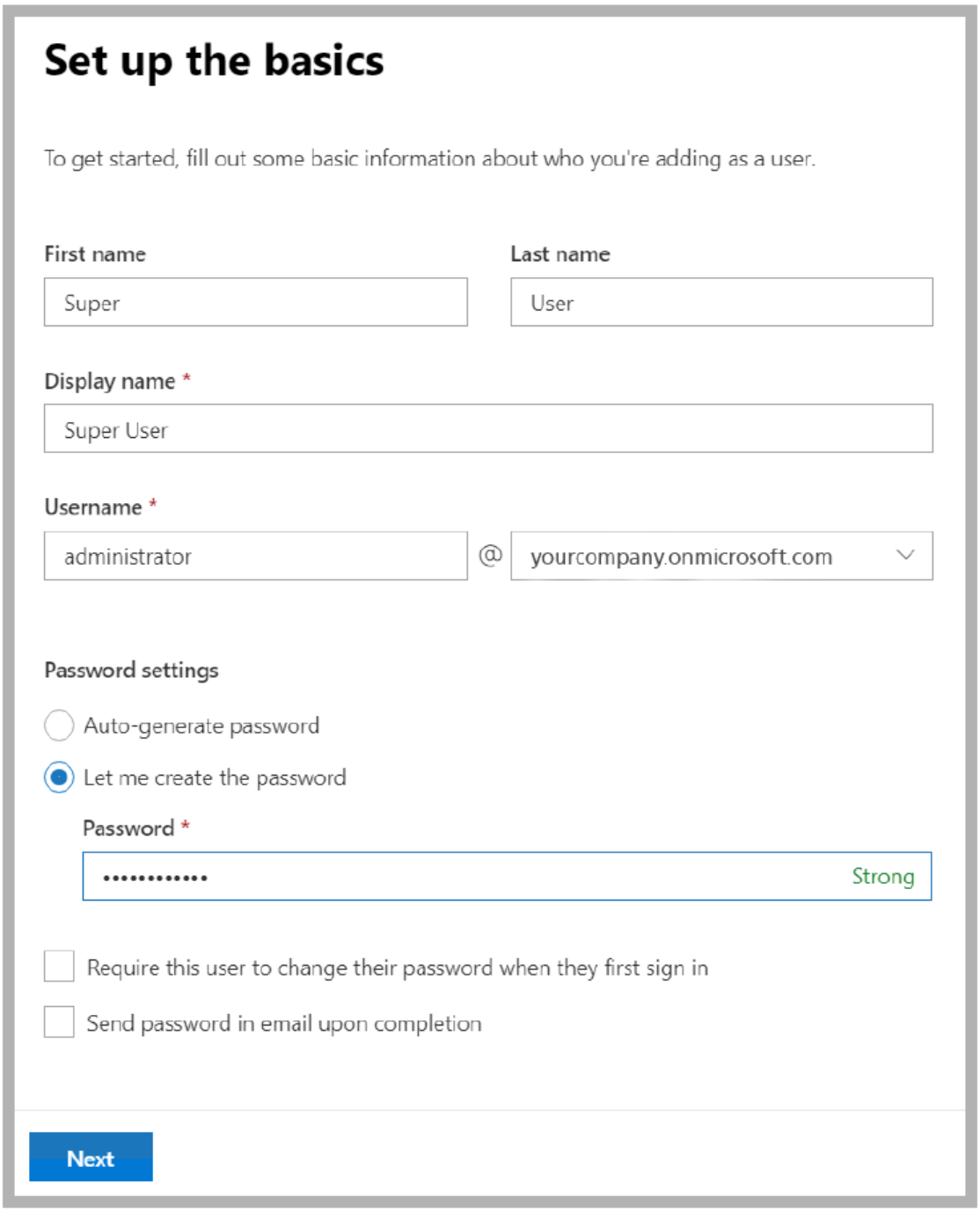
1. Log into the Office 365 Administration interface through a web browser at **https://login.microsoftonline.com/** or similar as setup by your administrator.
   Click **Admin**.



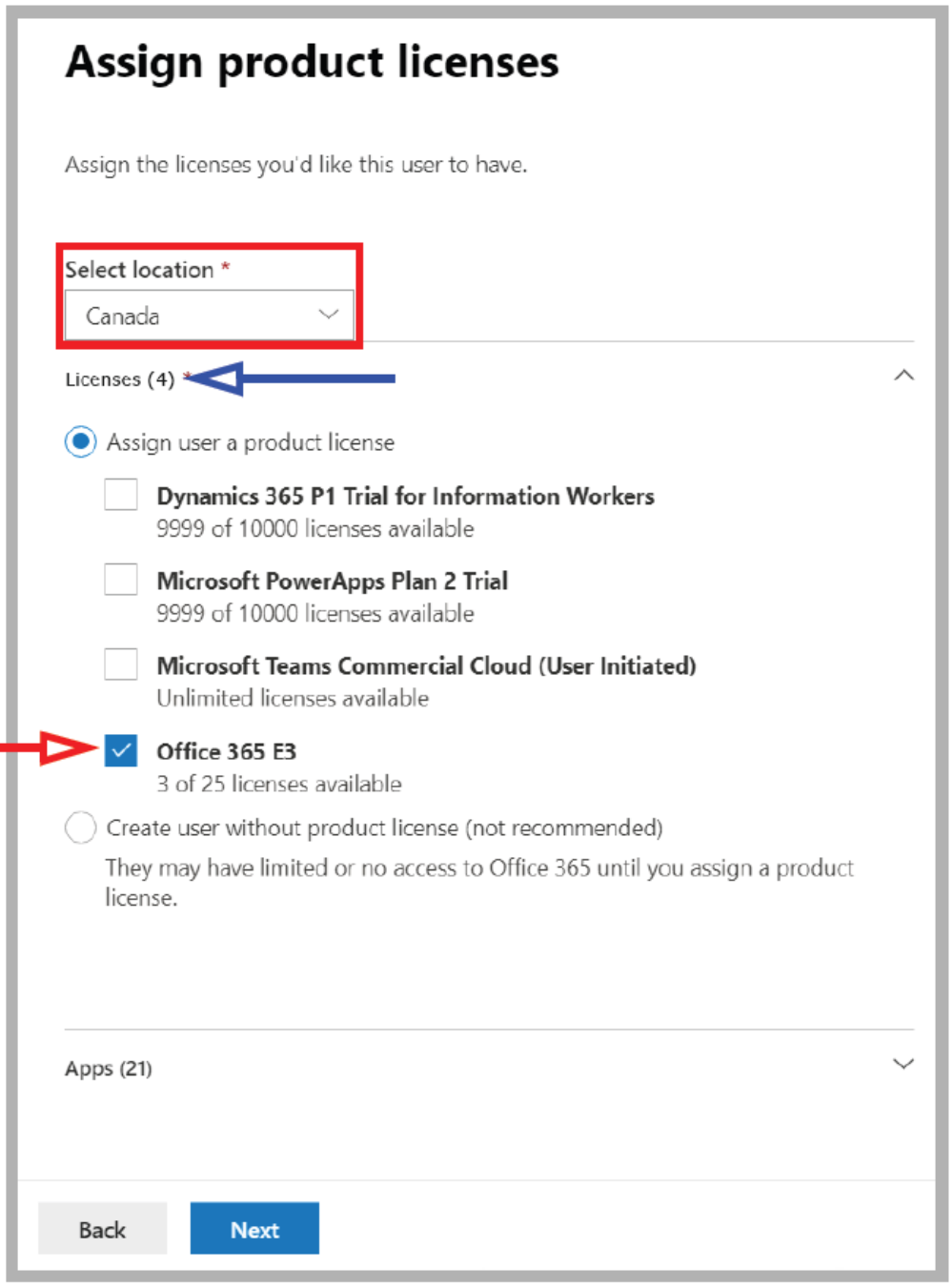
2. Under User Management, select Add User.



3. Enter a first and last name, display name, the **username** and **password** for the superuser (service) account.
   Click **Next**.

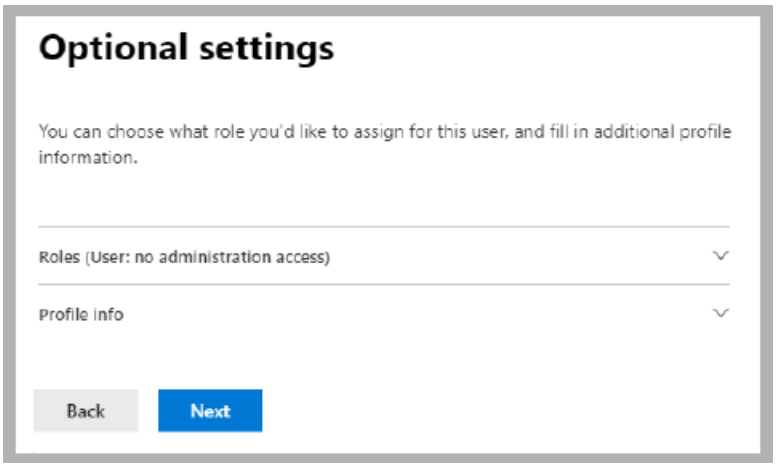

Set up the basics
To get started, fill out some basic information about who you're adding as a user.
First name
Super
Last name
User
Display name *
Super User
Username *
administrator
@
yourcompany.onmicrosoft.com
Password settings
Auto-generate password
Let me create the password
Password *
Strong
Require this user to change their password when they first sign in
Send password in email upon completion
Next

4. Set the user's geographic location on the dropdown list. Under Assign a Product License, select Office 365 E3. When ready, click Next.

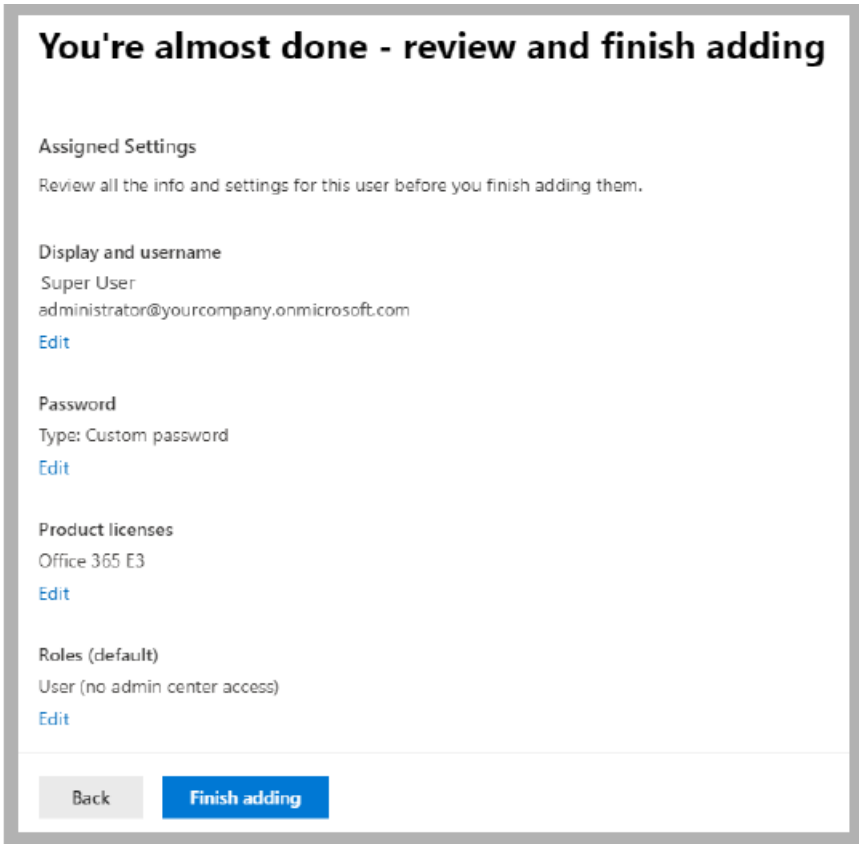


Note: A license must be available on your system for you add this user. If all licenses are already in use, delete one, or purchase additional licenses for this user.

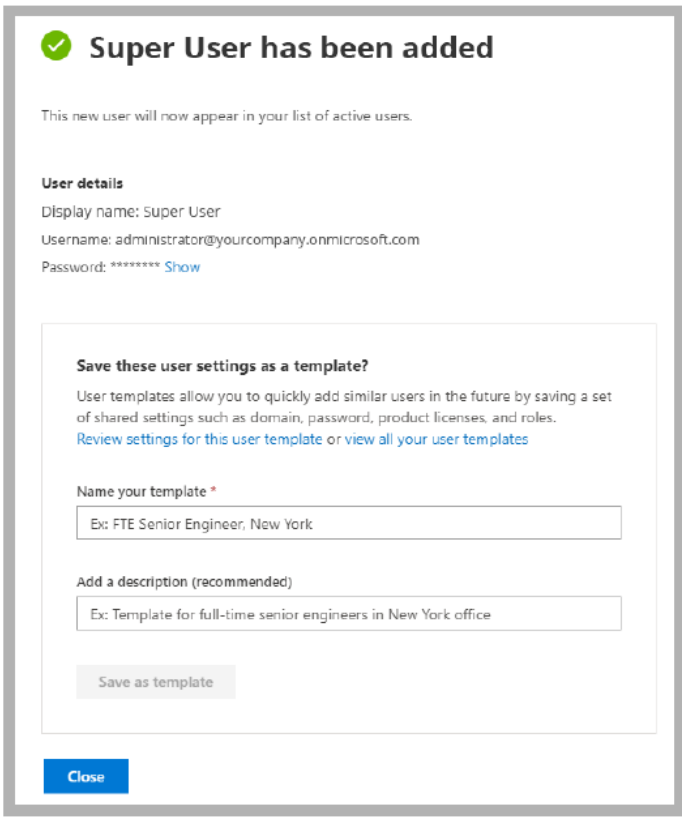
5. Make no changes here and click **Next**.



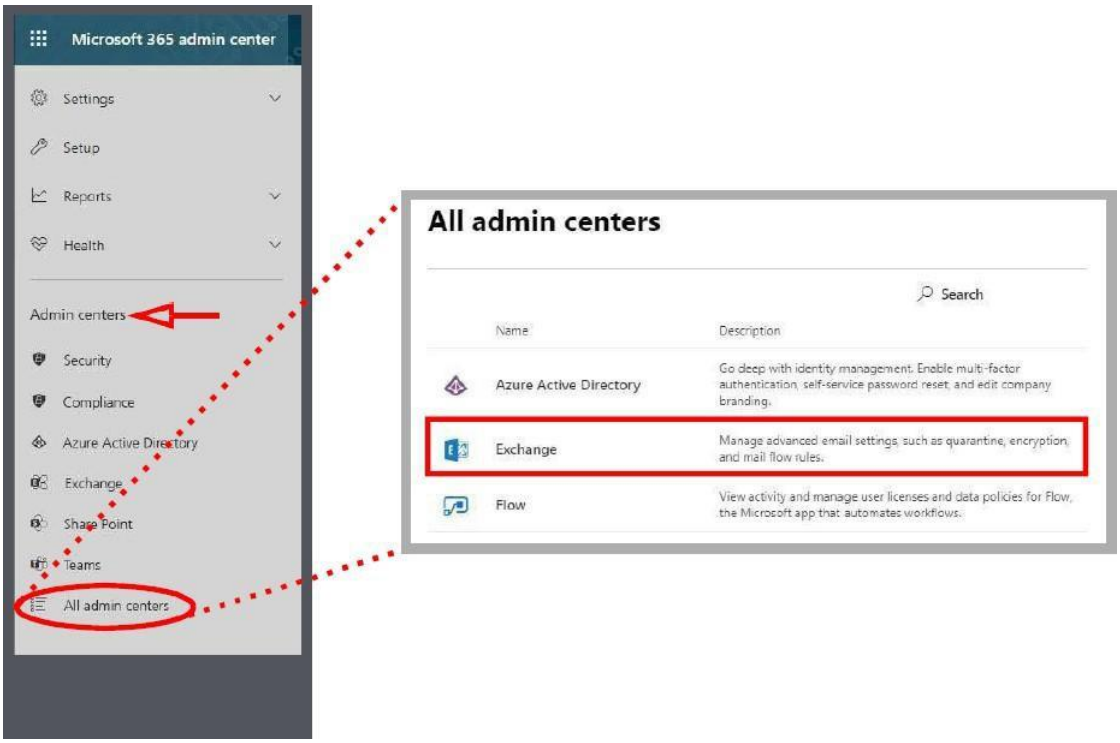
6. Review the user settings. If everything is correct, click **Finish adding**. If some elements need to change, click the Edit link beneath the incorrect item.



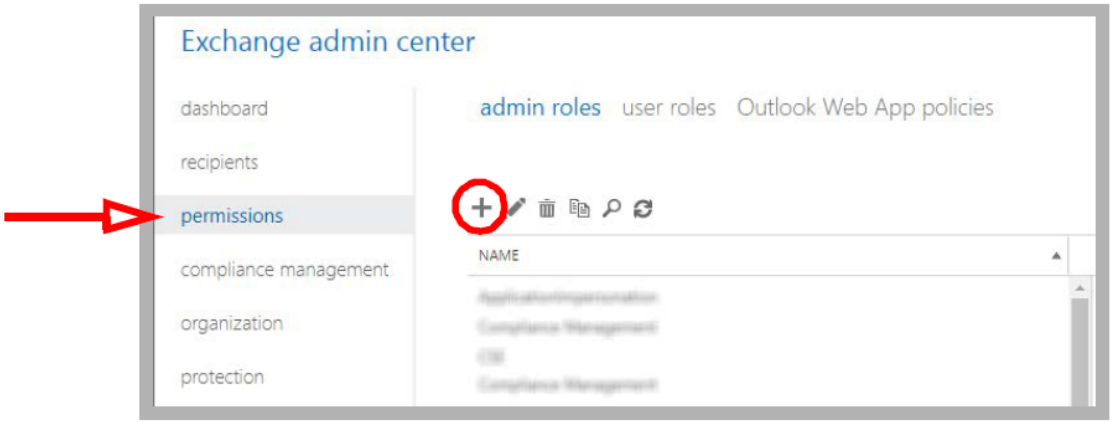
7. The user has been created. Click **Close**.



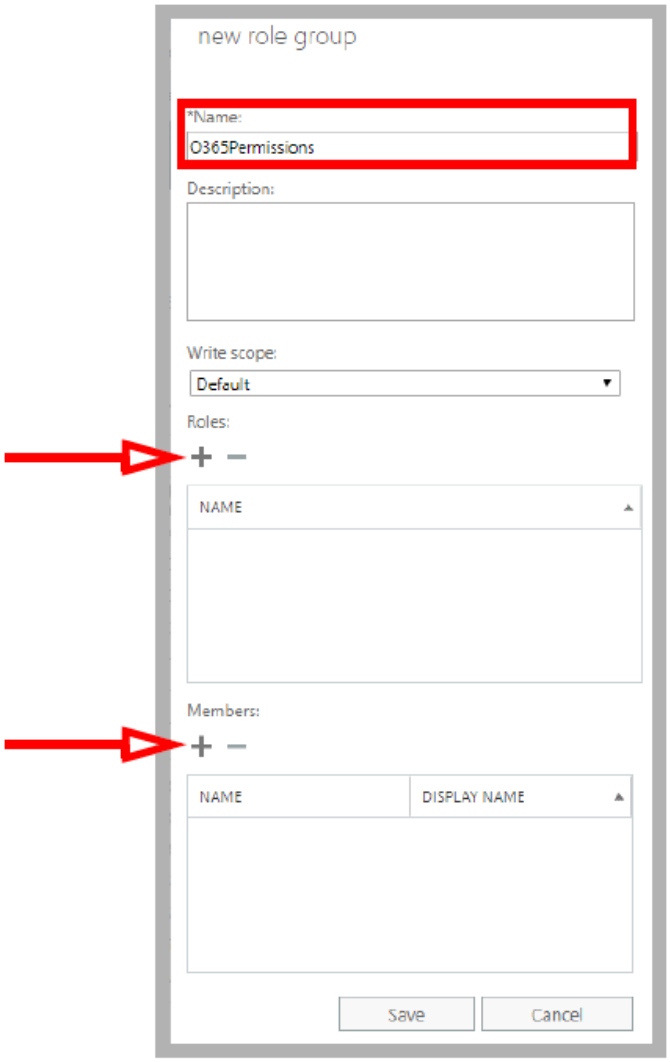
8. In the left-hand panel (**Show All**), under **Admin centers**, select **All Admin Centers**. From the list of applications, click **Exchange.**



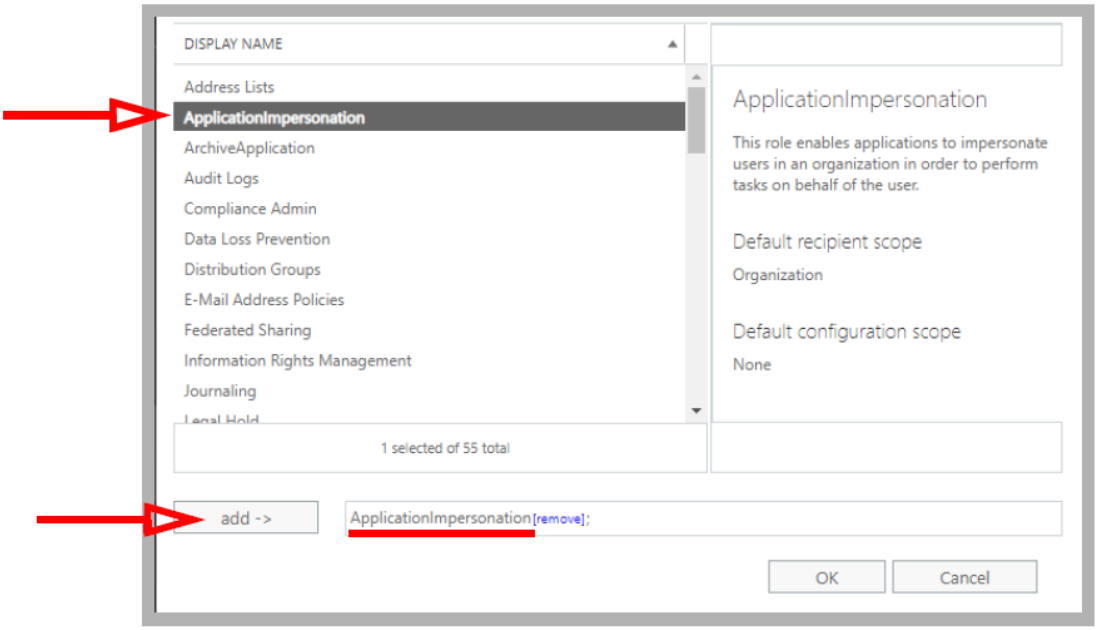
9. Select **Permissions** in the left-hand pane. Click **New.**



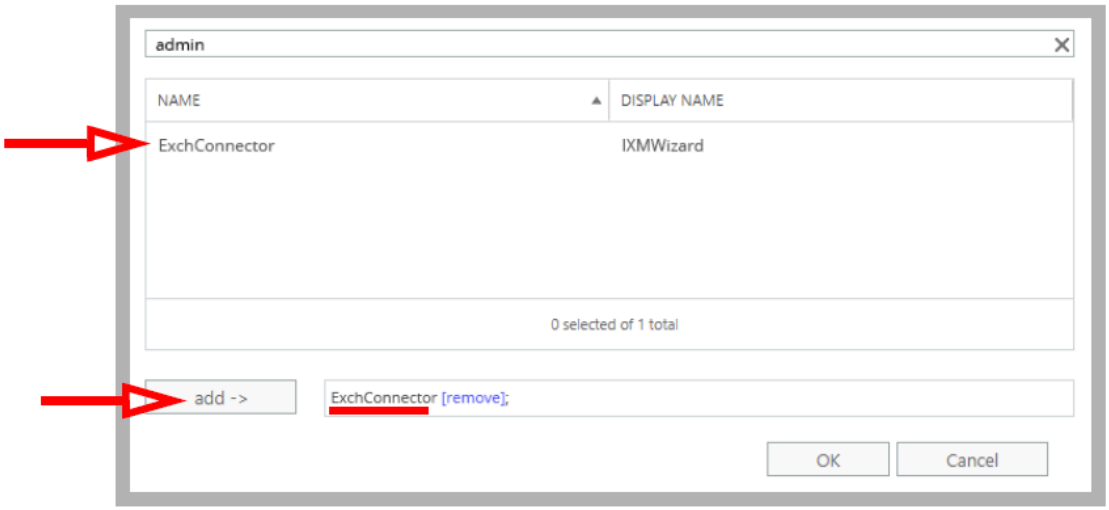
10. Give the Role a name (a Description is optional). Besides Roles, click Add.



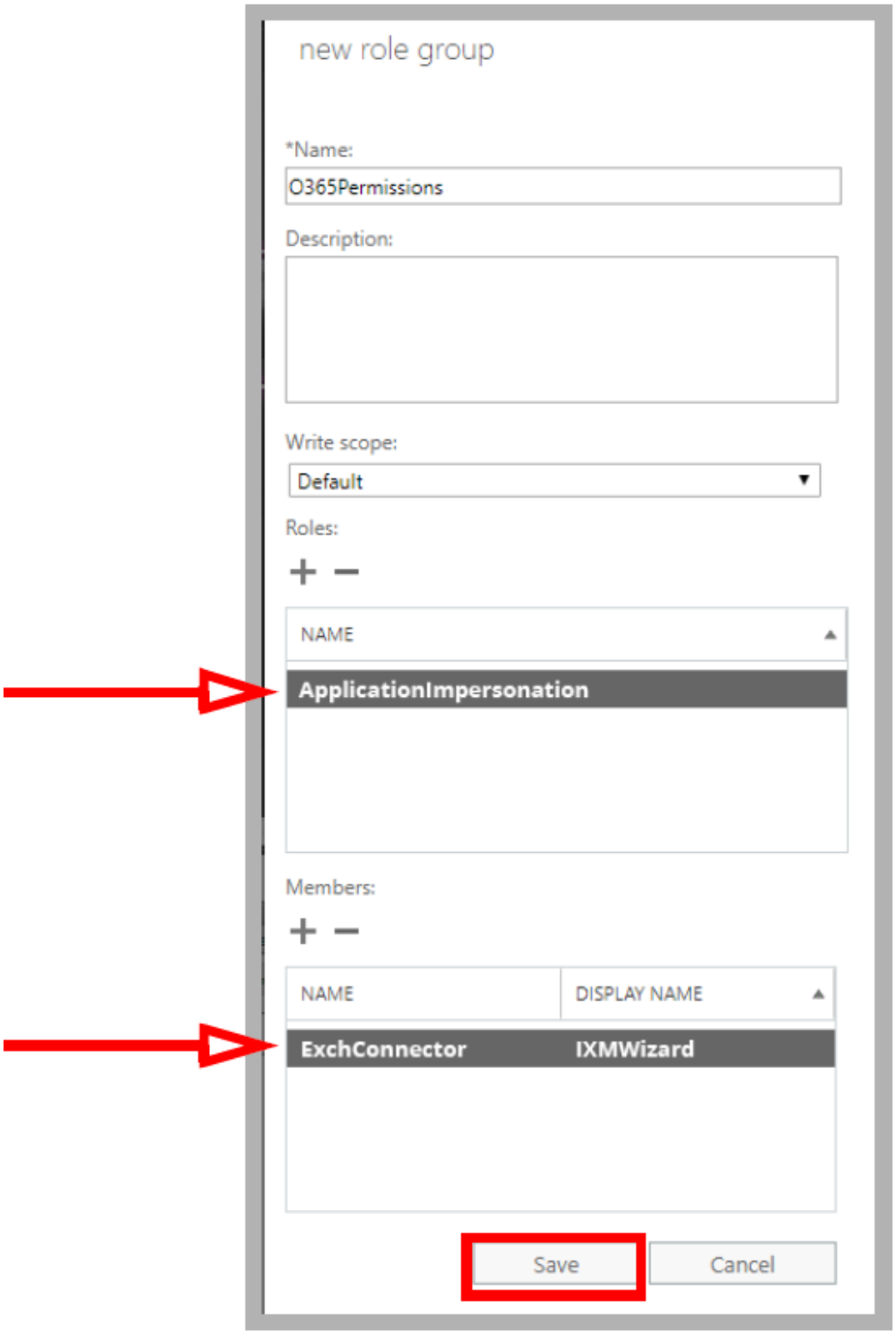
11. Select **ApplicationImpersonation** and click **add ->.** Click **OK**.



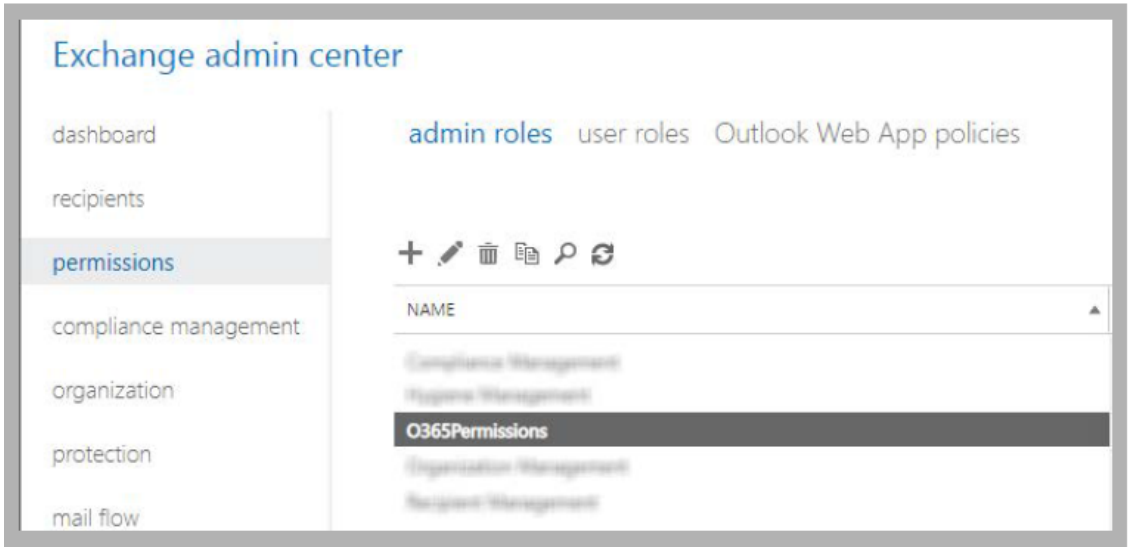
12. Below Members, click **Add**. Locate the account you just created, select it and click **add ->**. Click **OK**.



13. Returning to the **new role group** pane, click **Save**.



14. Confirm that the new role appears in the list.



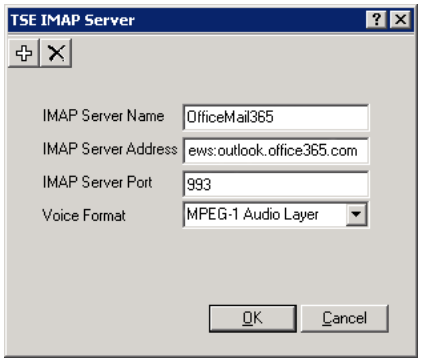
A new account has been created.

Avaya Messaging Server Configuration

Server Configuration

1. In Avaya Messaging Admin, add a new TSE IMAP server, and include the Office 365 server information.
   IMAP Server Name: Enter a name for this connection (e.g., **OfficeMail365**).
   IMAP Server Address: Type in **ews:outlook.office365.com**.
   IMAP Server Port: Set to **993** to enable SSL connectivity.
   Voice Format: Select **MPEG-1 Audio Layer 3** (MP3) for client playback.

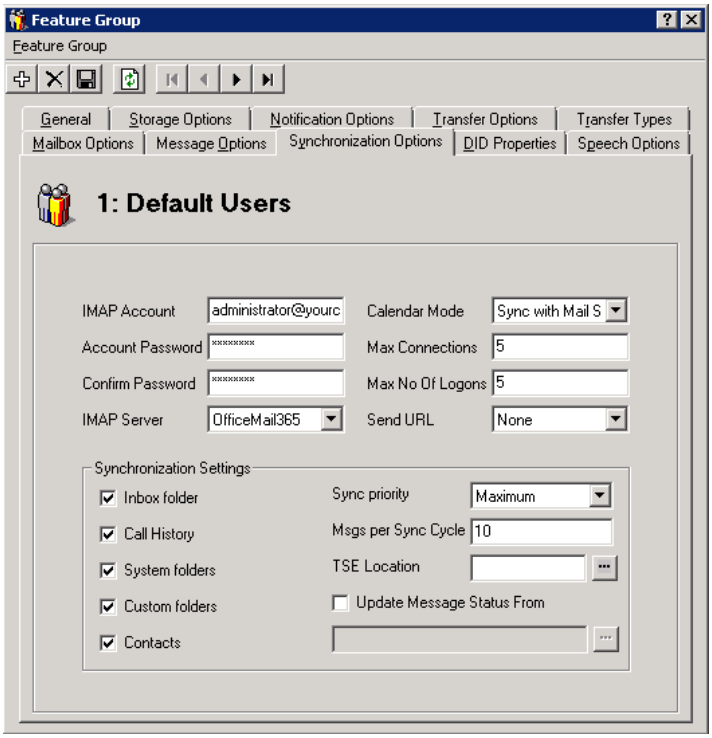
   Click **OK** when ready.



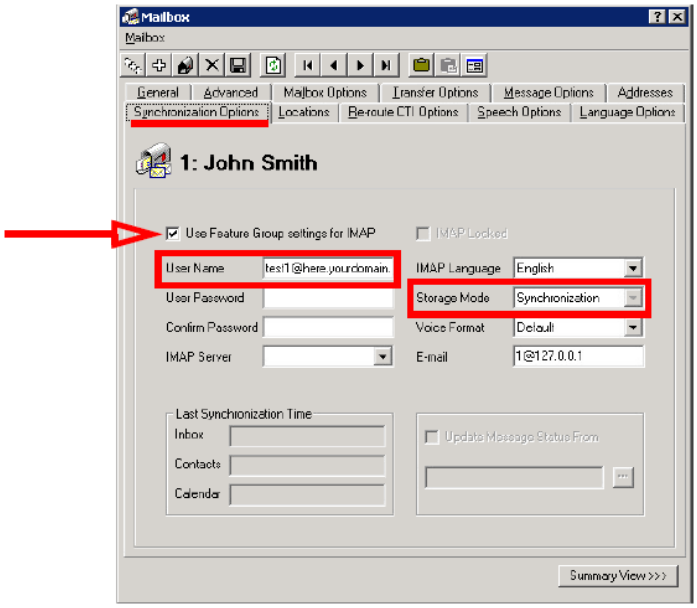
2. Once the TSE IMAP Server entry has been created, go to **Feature Group > Synchronization Options** and modify the Office 365 user mailboxes as follows:

   IMAP Account: Enter the user/service account created in step 3 above. Include the complete user@domain.com (e.g**., administrator@yourcompany.onmicrosoft.com**).
   Account / Confirm Password: Enter the super user/service account password from step 3.
   IMAP Server: Type in the name of the IMAP TSE Server created in the previous step (e.g.,

OfficeMail365).
Calendar Mode: If calendar synchronization is required, select **Sync with Mail Server Calendar** from the dropdown menu. Otherwise, select **None**.
Synchronization Settings: Set these options to specify which information will be synchronized between servers.



3. Ensure that individual mailboxes are configured under **Mailbox > Synchronization Options** with their User Name (e.g., test1@here.yourdomain.com), and that **Use Feature Group settings for IMAP** is enabled **Set Storage Mode** to Synchronization.



Connecting Through EWS Using OAuth 2.0

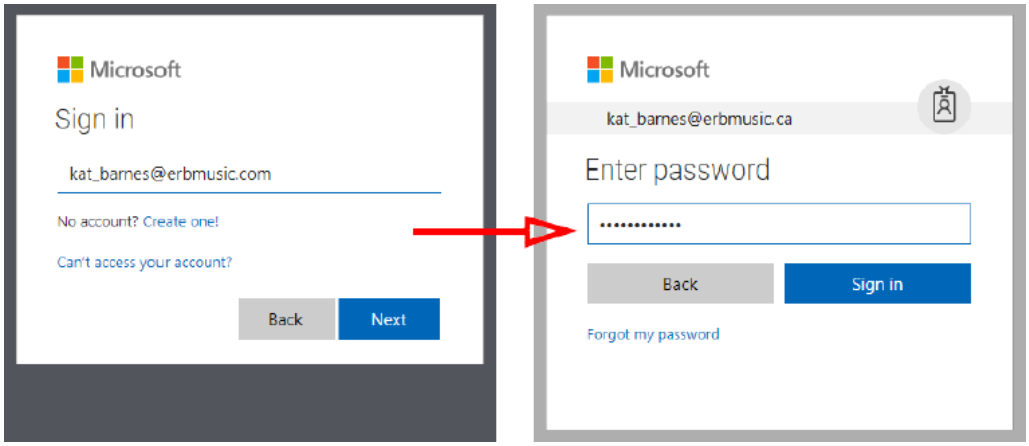
As an option, Avaya Messaging can be connected to Office 365 using Exchange Web Services. This can add an additional layer of security to your traffic flows. This section is not required.

Warning: This section contains advanced concepts and programming steps that could adversely affect operations if handled incorrectly. Read through this instruction thoroughly before proceeding. If you are not confident to follow these instructions adequately, do not continue.

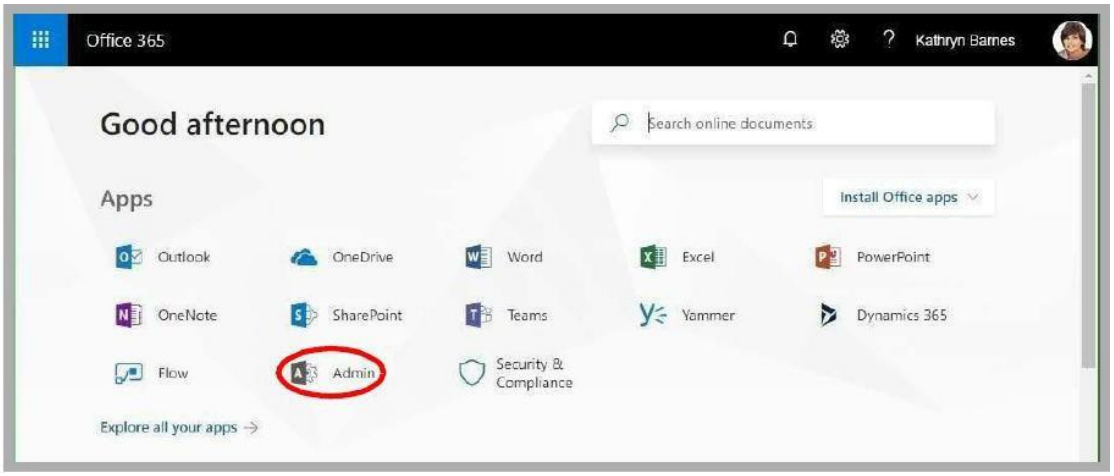
Note: You must have corporate Office 365 and EWS accounts for this configuration.

Important: These instructions require a certificate for securing the connections. It is **Strongly** advised that you purchase a certificate from a **Certification Authority (CA)** instead of using self-signed certificates. Both a Public Key and a Private Key certificate file are required.

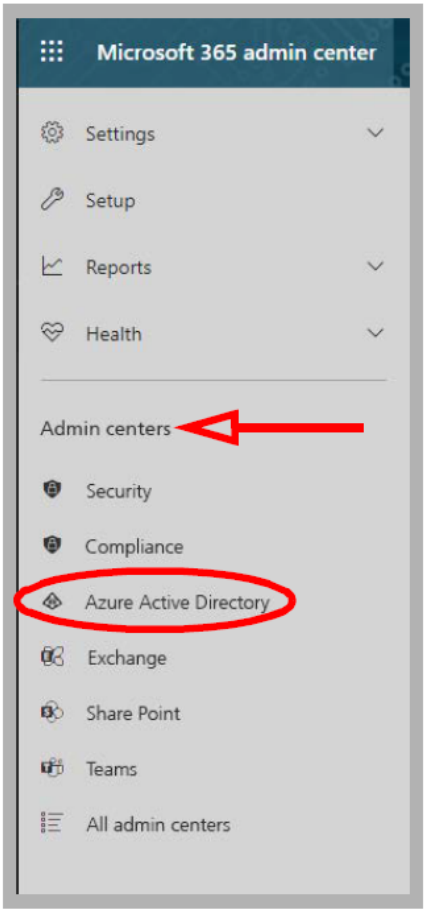
1. Open a web browser and go to the Office 365 site at **https://www.office.com**. Click **Sign in** and login using your Office 365 administrator account credentials.



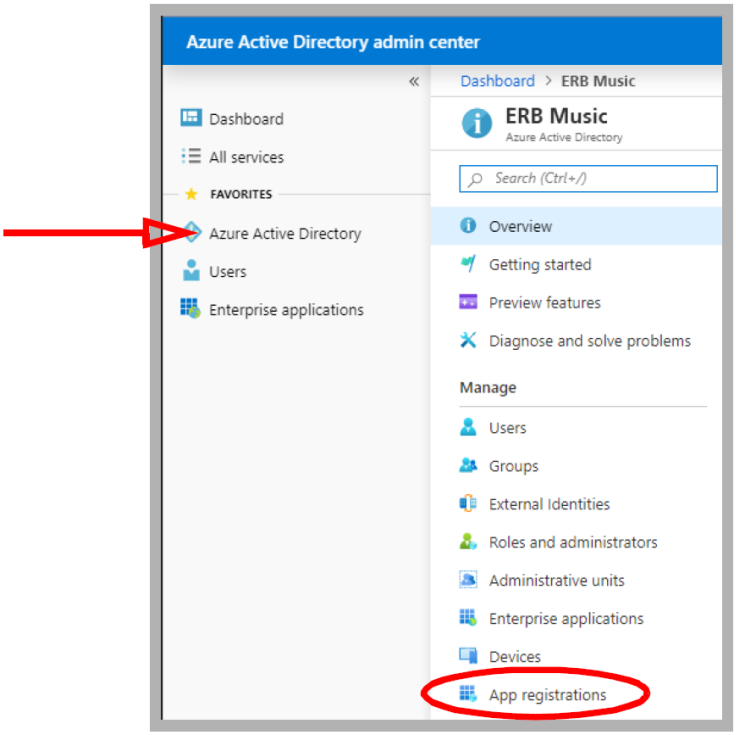
2. Click **Admin**.



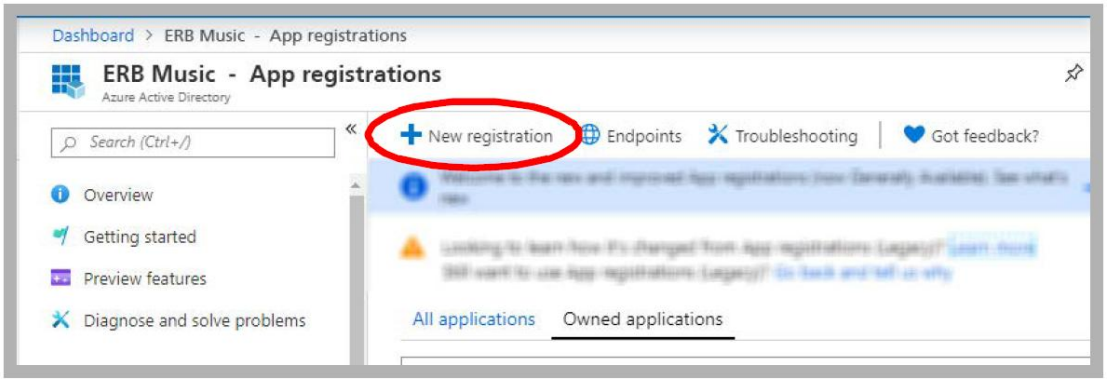
3. In the left-hand panel, open **Admin centers** (Show all) and select **Azure Active Directory**. The Azure dashboard will appear.



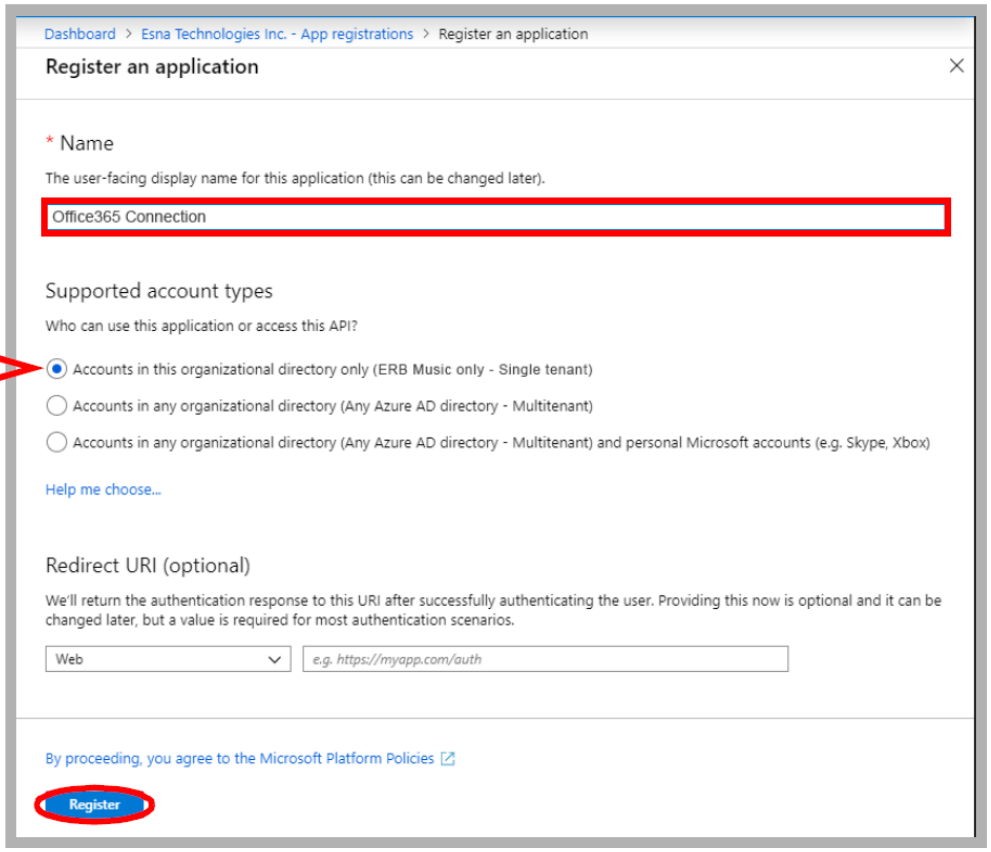
4. Click **Azure Active Directory > App registrations**.



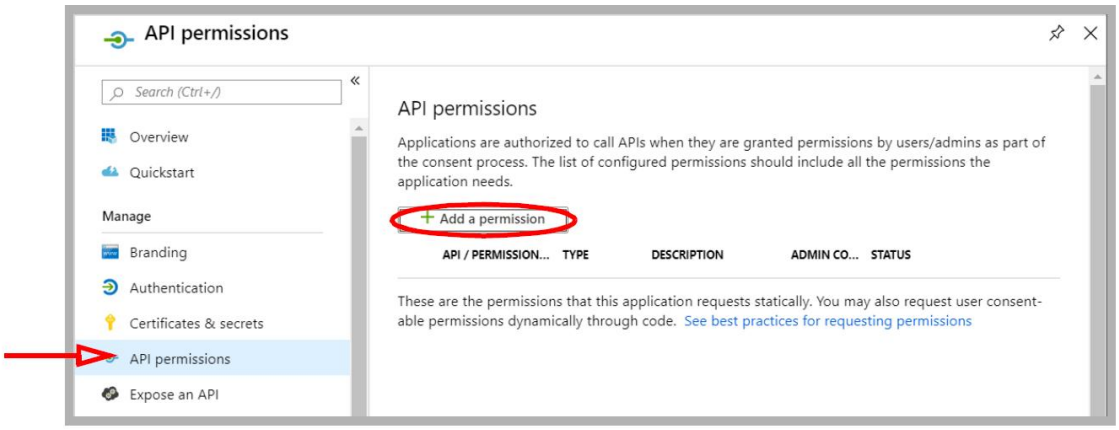
5. Click **New registration**.



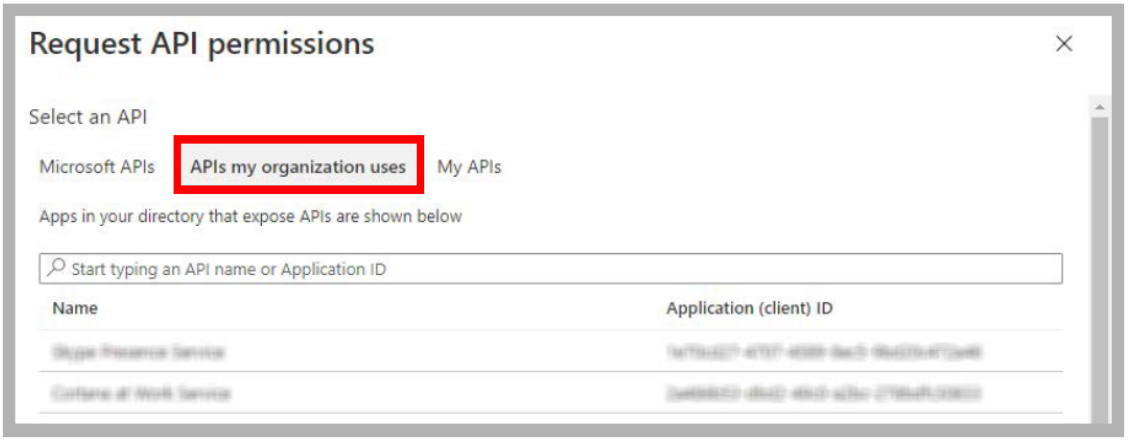
6. Provide a name for the registration. Enable Accounts in this organizational directory only. No redirect URI is required. Click Register.



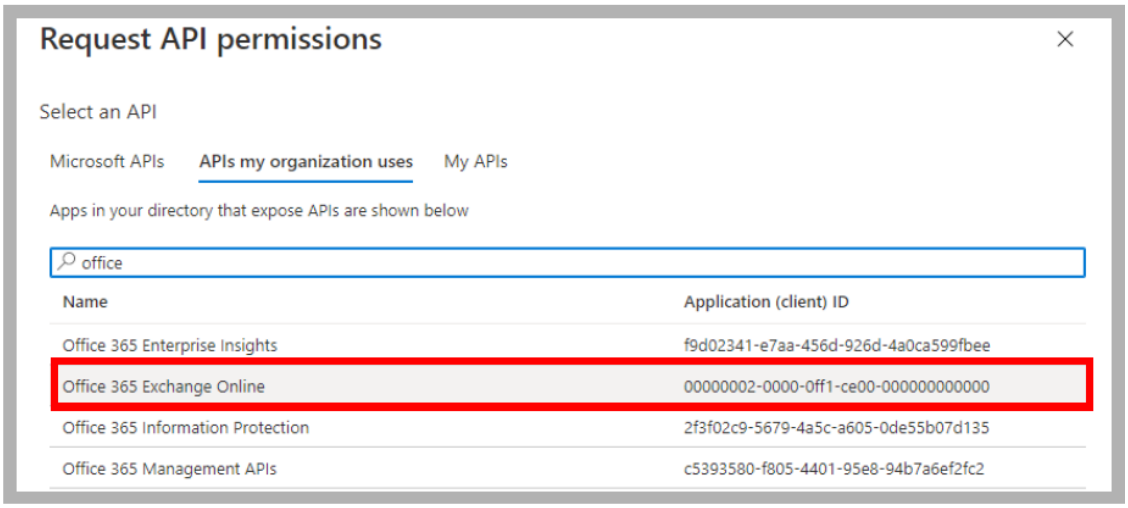
7. To configure the permissions for the application, click **API permissions > Add a permission**.



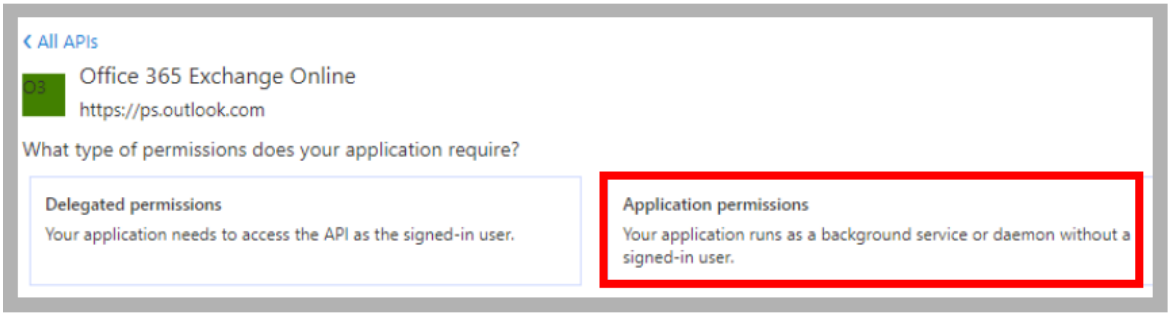
8. Under **Select an API**, go to the **APIs my organization uses** tab.



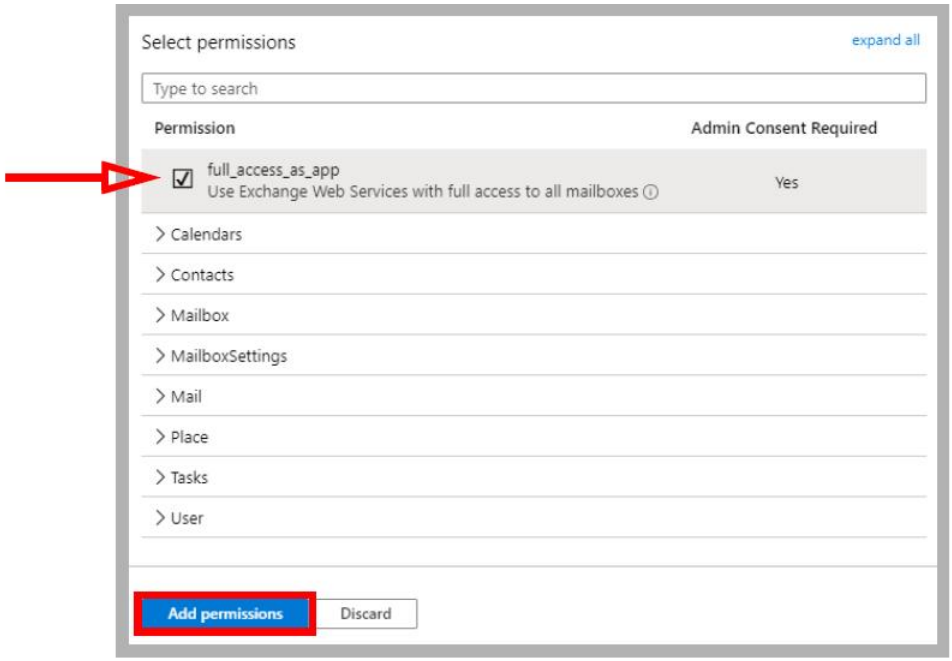
9. Find and select **Office 365 Exchange Online**.



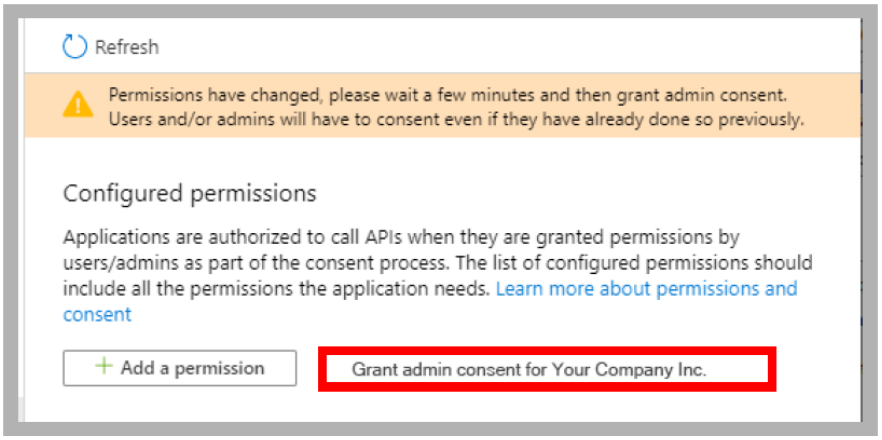
10. Click **Application permissions**.



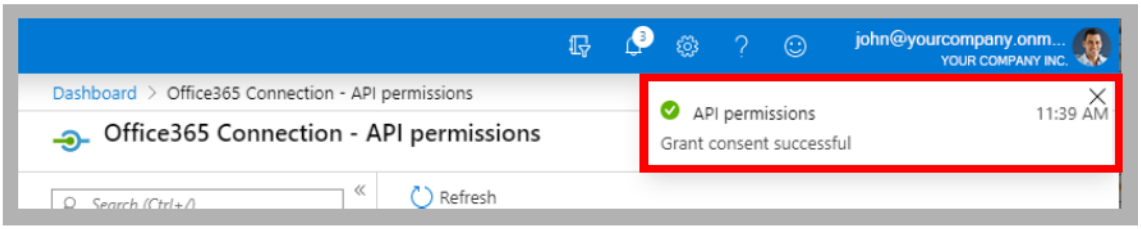
11. Enable **full_access_as_app.** Click **Add permissions**.



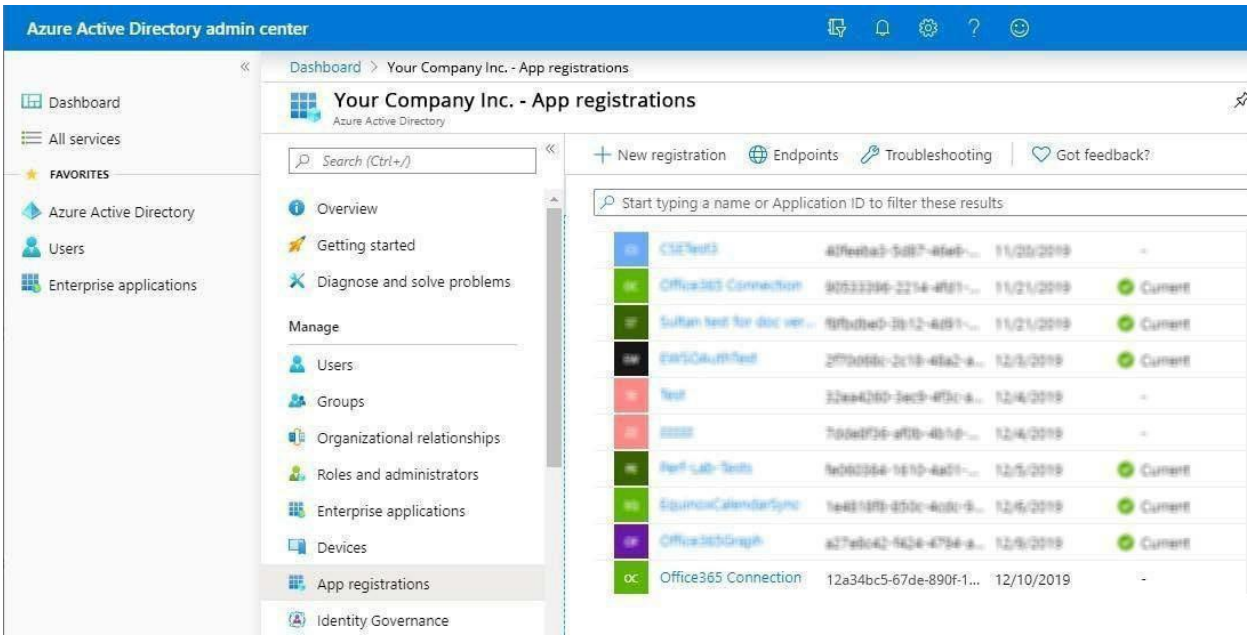
12. Wait 2-5 minutes for the updates to propagate through the system, then click **Grant admin consent for Your Company Inc.**



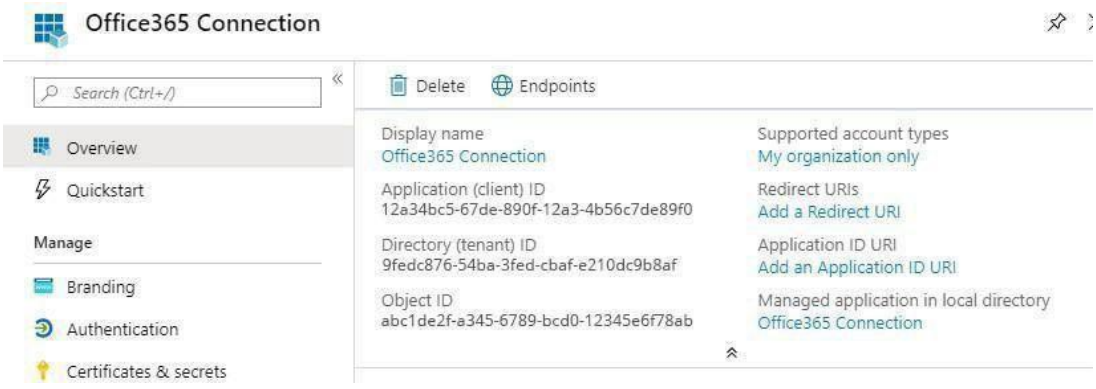
13. If the configuration was a success, a pop-up will appear in the upper right corner of the window.



14. From the Office 365 dashboard, open **Azure Active Directory > App registrations**. Click the application just created.



15. Copy the **Application (client) ID**.



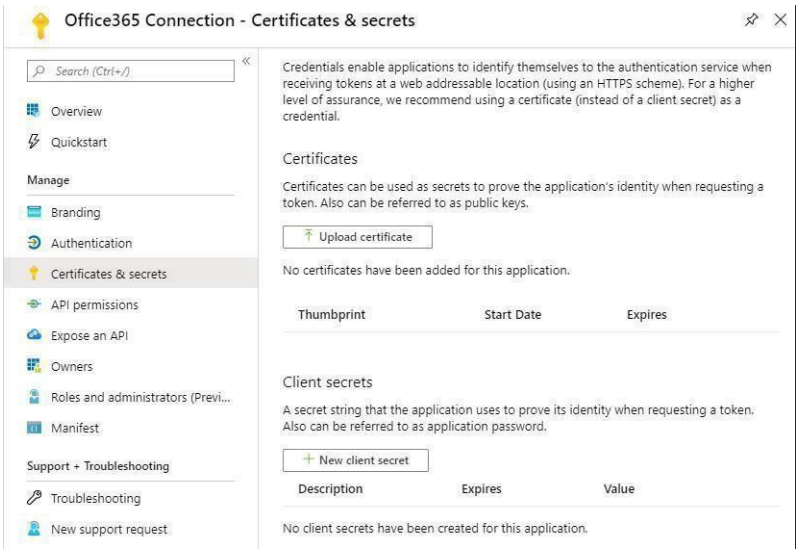
16. You will have received 2 certificate files from the Certifying Authority: one is a Public Key; the other is a Private key. Rename the **Private key**. Change the extension to .p12. Replace the name of the file with the Application (client) ID value recorded in step 15.

    For example: **0a987b654cd32.pfx ----> 12a34bc5-67de-890f-12a3-4b56c7de89f0.p12**

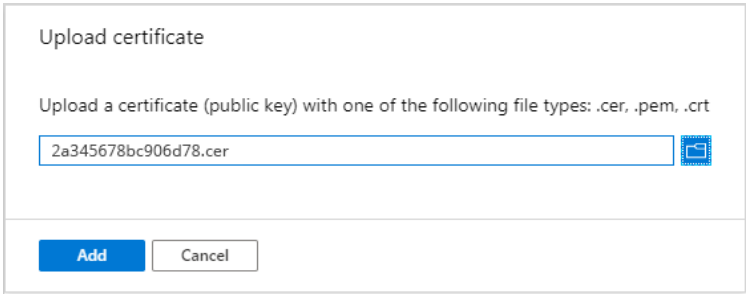
    Copy this file into both the **UC/UCCSE** and the **UC/IMAPTSE** folders on the IX Messaging voice

server. For a site using High Availability, copy the file to the same folders on the Consolidated Server, and on all Remote CSE servers.
Rename the **Public** key. Change the extension to .cer .
For example: **2a345678bc906d78.pfx--- > 2a345678bc906d78.cer**

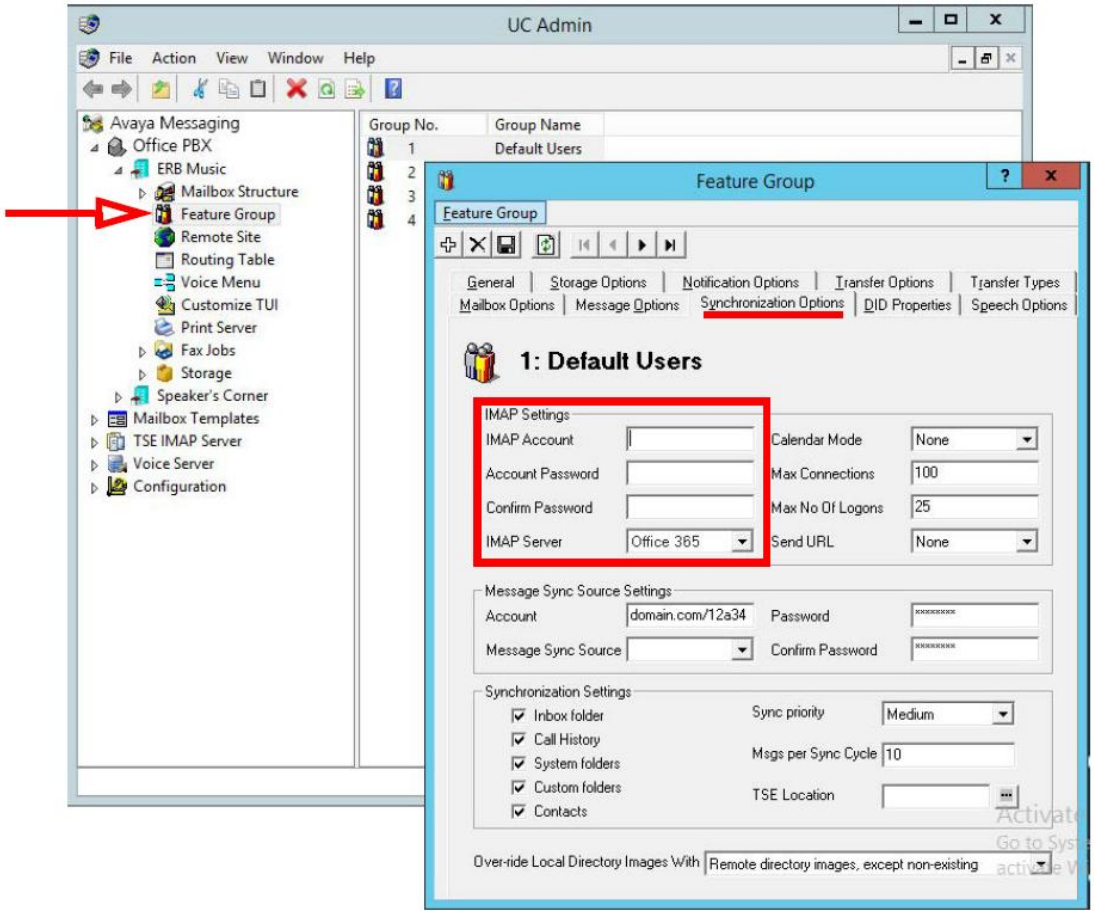
17. Click **Certificates & secrets** in the left-hand pane. Select **Upload certificate**.



18. Click **Browse** and select the **Public** certificate file on your drive. It is the one with the .cer extension. Click **Add**.

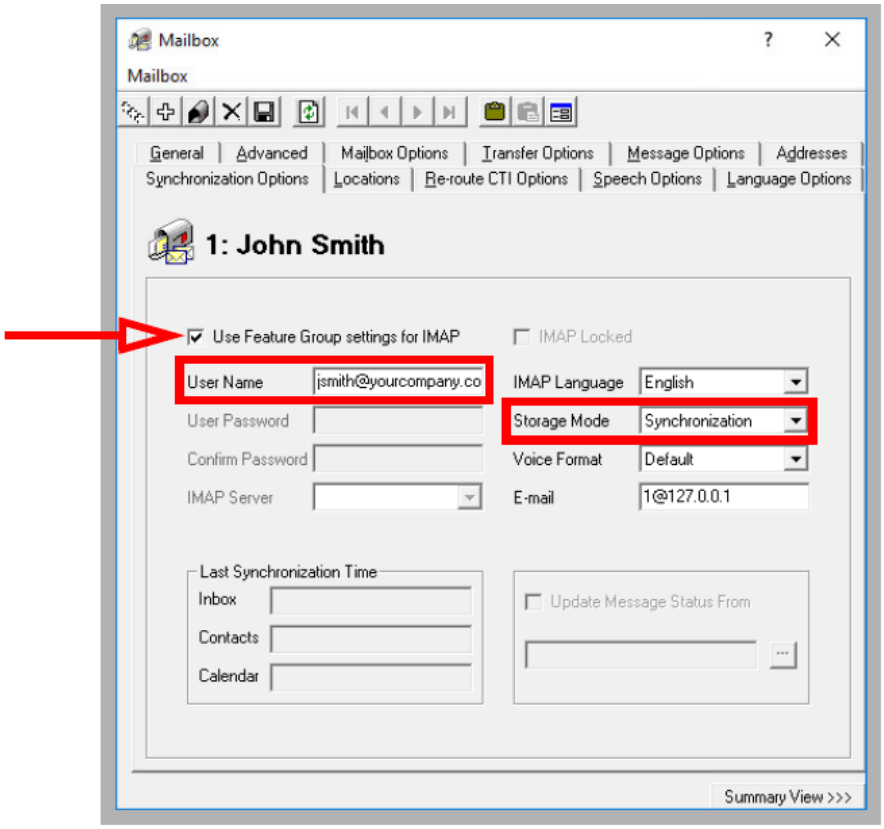


19. Open UC Admin on the Voice Server. Go to the **Feature Group > Synchronization Options** tab. Under **IMAP Settings**, configure:
IMAP Account: Enter your corporate Office 365 domain, a forward slash, then the **Application (client) ID**. (e.g., **yourcompanydomain.com/12a34bc5-67de-890f-12a3-4b56c7de89f0). Account / Confirm Password**: Type in the password used to secure the .p12 certificate file.
IMAP Server: Enter the name of your IMAP server.



Click **Save**.

20. In UC Admin, open **Mailbox Structure**. Open a person's mailbox that will use this configuration. Go to the Synchronization Options tab.
21. Enable **Use Feature Group settings for IMAP**. Type in the **User Name** for this account.
22. For **Storage Mode**, select **Synchronization**.

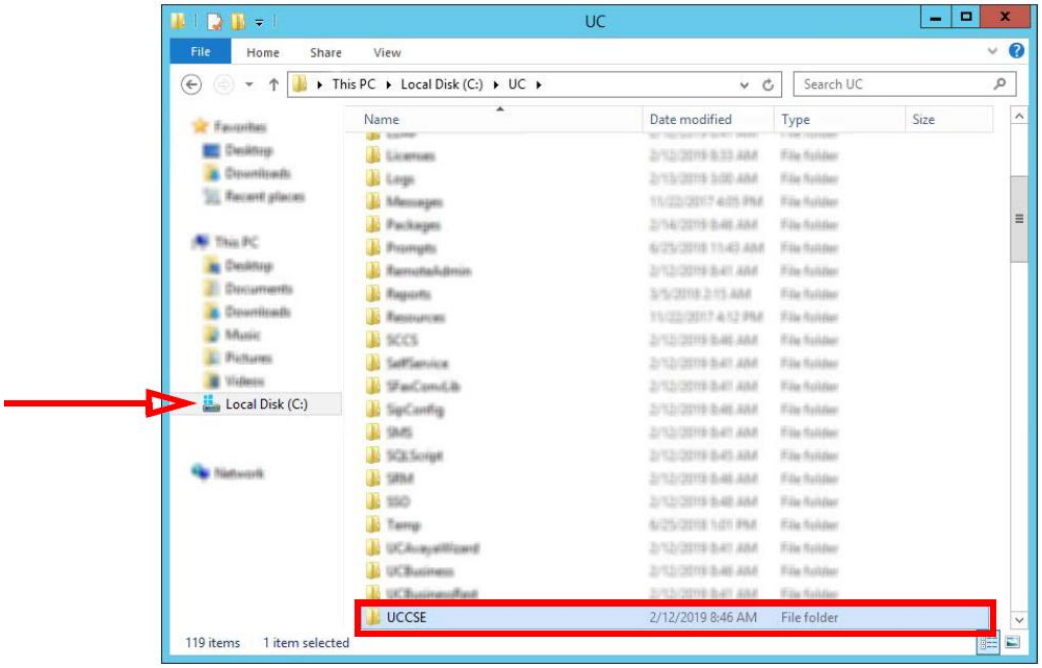


Click **Save**. The configuration is complete.

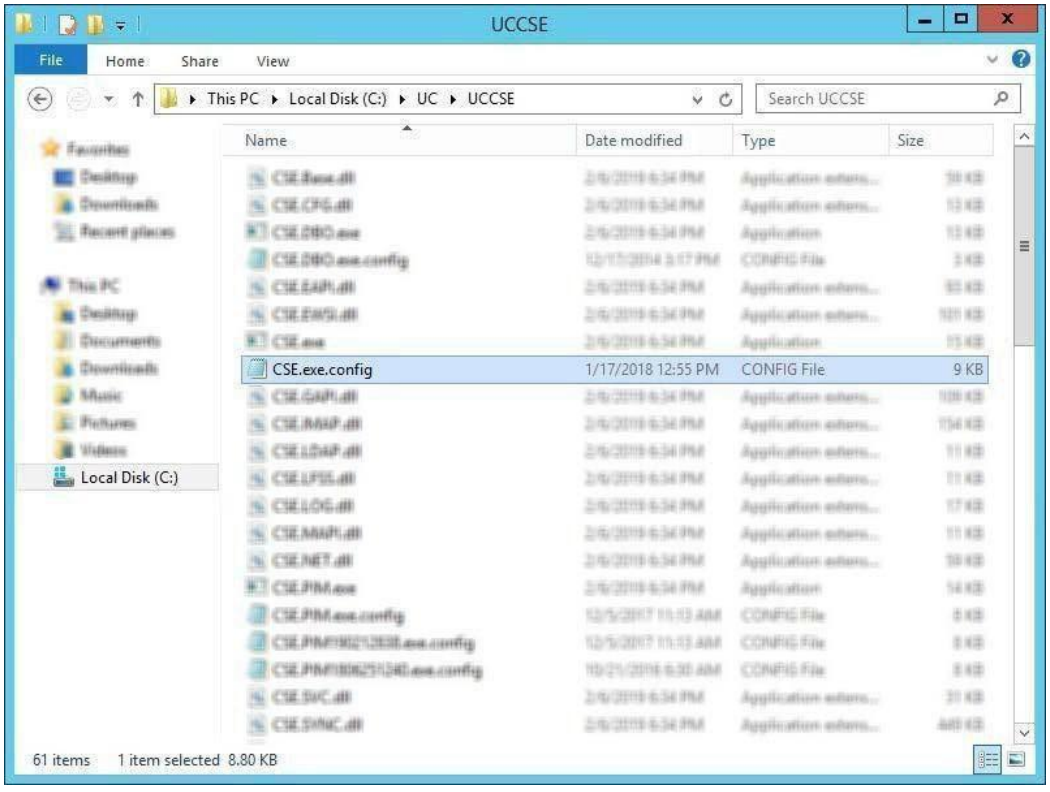
Verify Configuration Setting

Once the installation has been completed, verify that the system is configured to use EWS instead of IMAP.

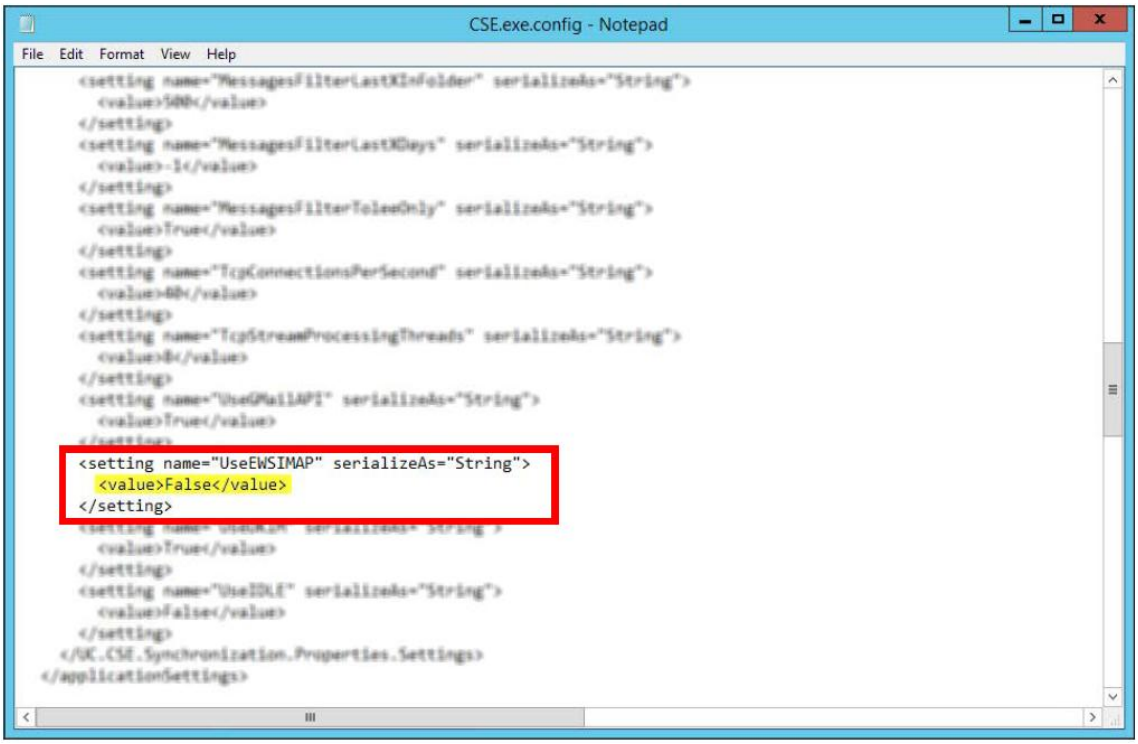
1. On a **Single Server** Installation, open the **UC/UCCSE** folder on the program installation drive. For **HA** installations, this file is found on the **Consolidated** server in the same folder.



2. Within the folder, open the CSE.exe.config file in a text editor such as Notepad.



3. Scroll down to find the following lines:
<setting name="UseEWSIMAP" serializeAs="String">
<value>**False**</value>
</setting>



4. Verify that the **Value** is set to **False**. If the value is not False, retype the text and save the file to change it to the correct value.

Chapter 12: FIND ME FOLLOW ME ON CTI INTEGRATION

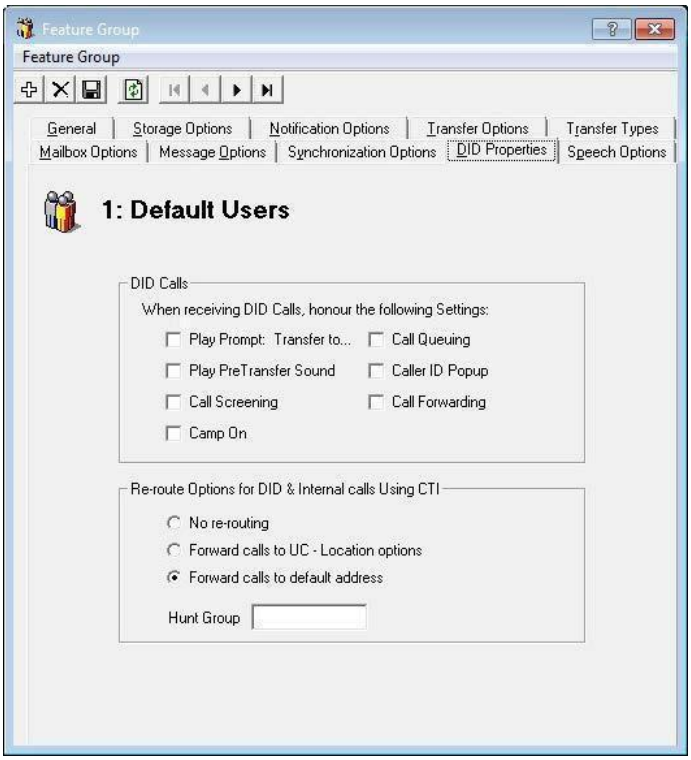
Introduction

Find me Follow me allows calls to be forwarded to one or more addresses until the user is found. The addresses can be internal or external numbers. They can be dialed sequentially, or simultaneously.

This document is intended for technicians who have some familiarity with Avaya Messaging and want a deeper understanding of what is expected of the functions and how to set up users.

The Find Me Follow Me features for DID and direct calls are only available for some PBX's.
Refer to the Technical Operating Guidelines for details on PBX's.

Note: The Hunt Group field should be left blank.



Visual Guide



If the user has configured Find Me Follow Me for their mailbox, Avaya Messaging will try to locate the user through a broadcast rather than through a single phone number or device. Whenever a call comes in, Avaya Messaging will try to locate the user through multiple devices simultaneously (or as configured). Once the user accepts the call on one device, Avaya Messaging will connect the caller with the user and terminate the other calls.

Requirements

Requirements	Details
License	---
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher.

User Guide

This guide goes over the configuration of Find me Follow using Web Access. If you have access to the admin console, this process can be completed from there as well.

Find me Follow me with CTI Integration

Note: Before you can launch Web Access, two items must be set in Avaya Messaging Admin:

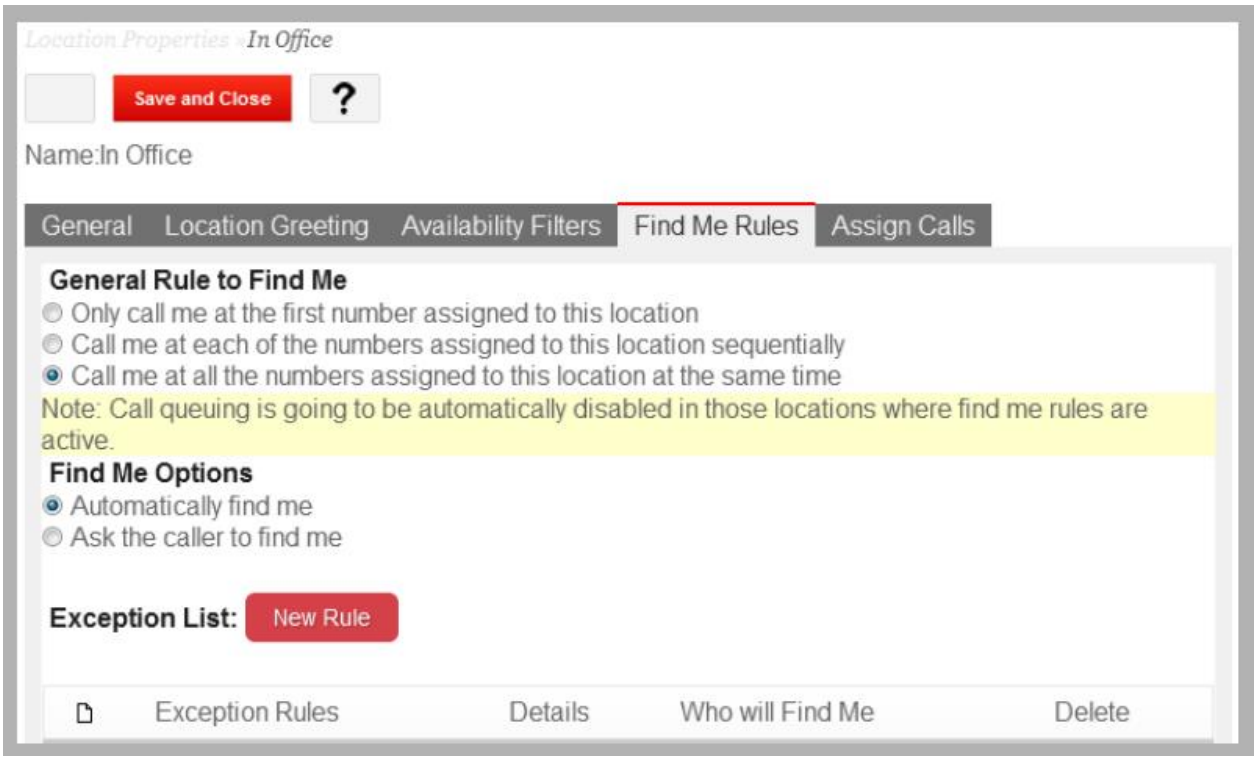
1. Enable **Web Access User** under **Mailbox > Advanced**
2. Select **Web Access** under **Feature Group > Mailbox Options**.

If you do not have access to the Avaya Messaging Admin console, please contact your System Administrator.

When you log into Web Access, the Main page will appear. Click **Locations**.



The locations page shows all the locations created for the user. From this page, the user can create a new location or edit an existing location. Click on the location to be configured, then open the **Find Me Rules** tab.

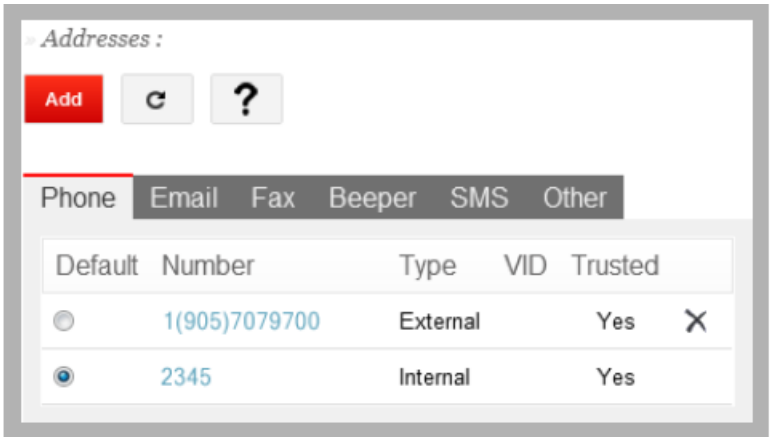


The Find Me Rules page displays all of the options available for that location. It is important to note that this section will configure how the Auto attendant will behave for incoming calls. However, it is necessary to set the current location as well as availability.

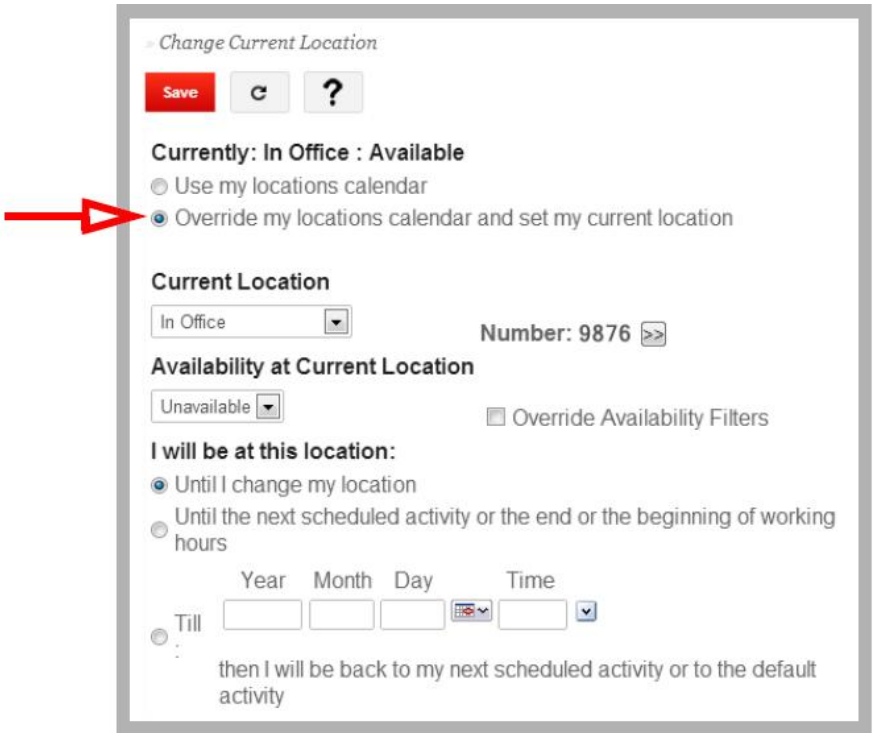
Addresses

Addresses are an important part of the finding me follow me feature, and are necessary when configuring the locations where the program will call the user. Addresses in this context refer to internal and external phone numbers where calls will be directed based on the rules and configuration selected.
It is important to first define the addresses or numbers where the user can be reached for various locations to configure the finding me follow me features.

Addresses can be added, edited and deleted on the **Addresses** page of Web Access. Addresses can be internal (such as a desk phone extension) or external (such as a cell phone or phone number off site).

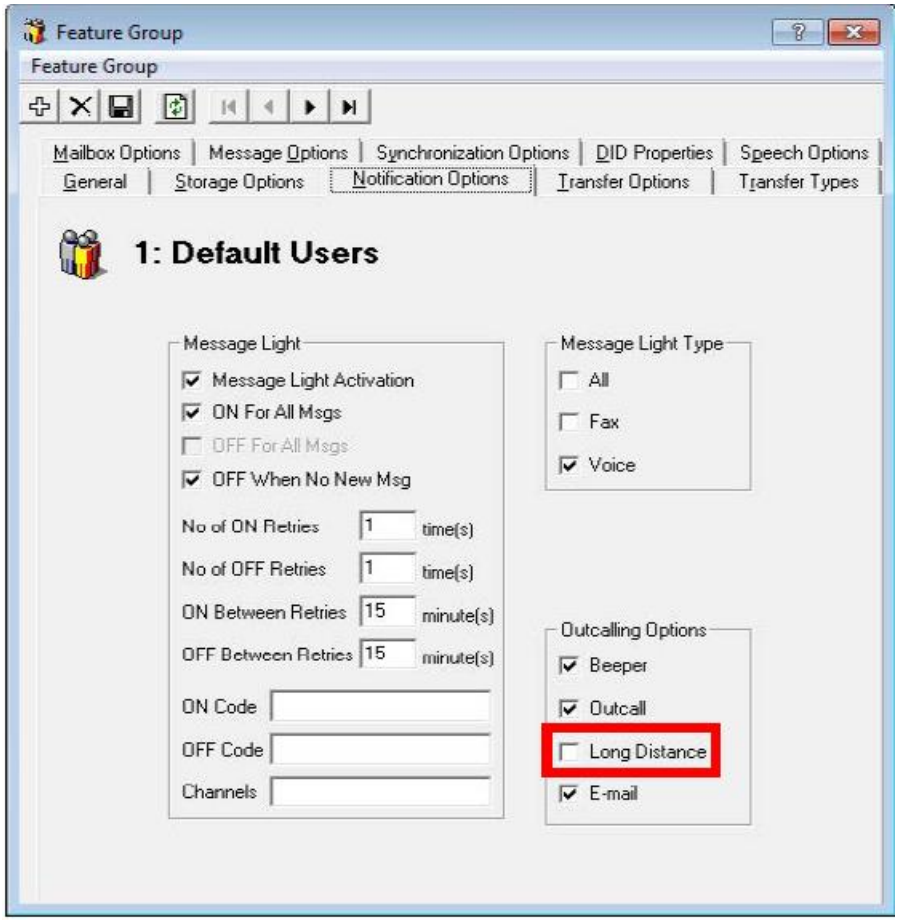


To set your current location using Web Access, click on the **Current Location** icon.
Enable **Override my locations calendar and set my current location**. Set your location and availability from the dropdown menus.



In order for outside calls to be dialed by the voice server, configure outcalling through **Windows Control Panel > Phone and Modem Options** and make sure the local area code is selected.

If the call is forwarded to a long distance number, enable **Long Distance** under **Feature Group > Notification Options > Outcalling Options** for the group containing the member.

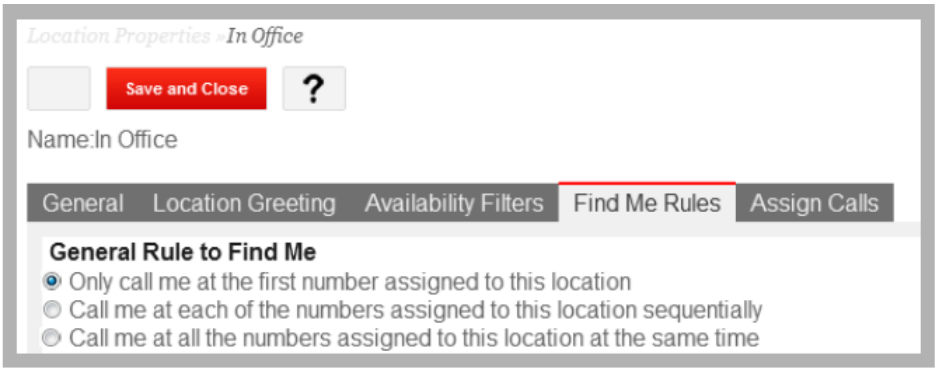


Configuring Find me Follow me features

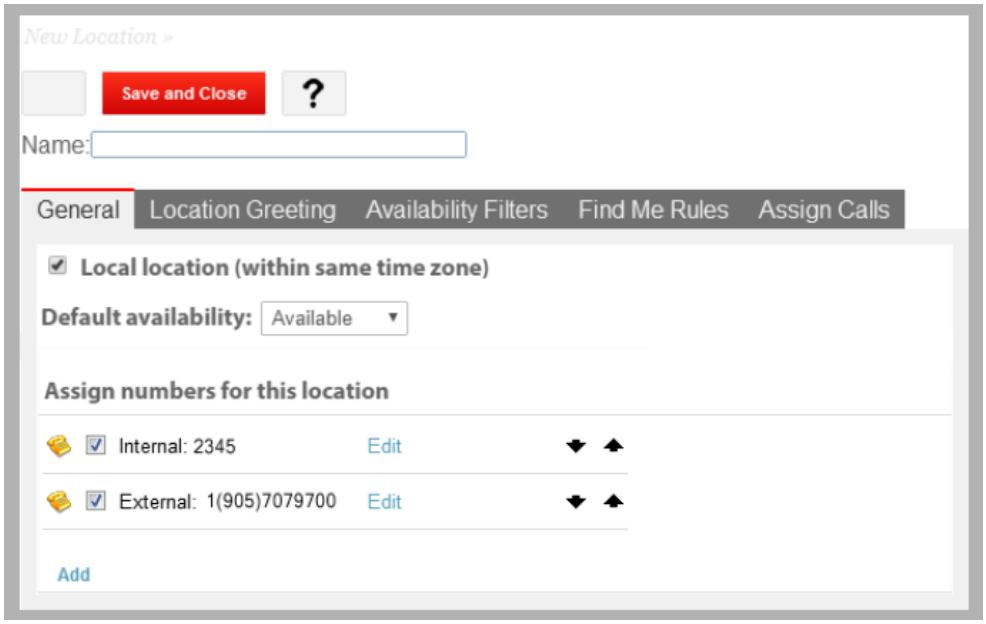
There are several pre-defined options for the Auto attendant to automatically find a user by forwarding calls to a range of numbers, either internal or external. Click on the Find me rules tab and select a rule and option:

Only call me at the first number assigned to this location

Select the option **Only call me at the first number assigned to this location** and then click on the **General** tab to go back to the list of numbers assigned to the location.



Using the up and down arrows, select the number you want calls to be forwarded to and move it to the top of the list.



Click on the **Save and Close** button.

The Auto Attendant will call only the number on top of the list of numbers assigned to that specific location. If there is no answer at that extension, the Auto attendant will play the location greeting configured. We can expect this behavior when calls are made to a DID or through the Auto attendant.

Note: In order for this feature to work, the user must be set up to be in that location and Available. If the user is Unavailable the find me follow me feature will be disabled and the Auto attendant will play the location greeting.

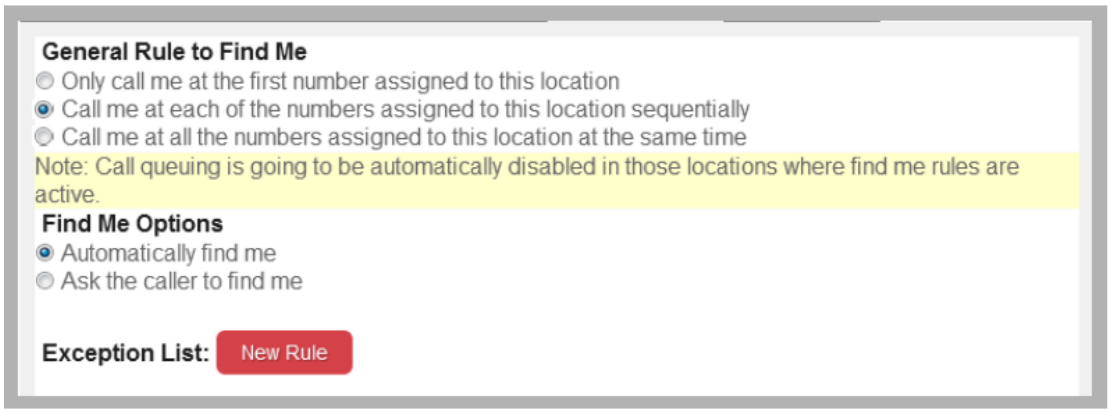
Call me at each of the numbers assigned to this location sequentially

This rule gives the user 2 options: **Automatically find me** and **Ask the caller to find me**.

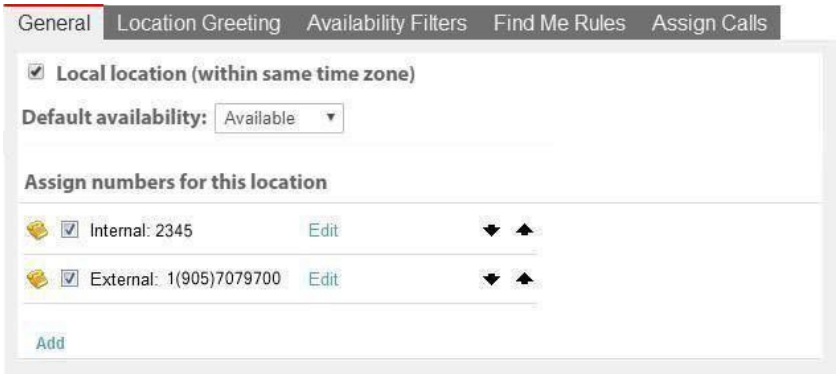
Automatically find me:

This feature will call numbers assigned to the location until it's answered or the call goes to user's voicemail if there is no answer.

On the **Find Me Rules** tab, select the appropriate options and then go to the General tab to arrange the sequence of calls:



On the **General** tab, add the addresses to the Numbers assigned to this location column and using the up/down arrows select the sequence in which you want to be found (from top to bottom).



Note: In order for this feature to work, it is necessary to have at least 2 addresses in this column, otherwise there is no sequence, and the finding feature will not be in effect

Click **Save and Close** button.

When a call is transferred by the Auto attendant or when a call is made to a DID that rings the extension directly, the Auto attendant will dial all the addresses in the list of numbers assigned to the location sequentially from top to bottom until the call is answered, if there is no answer in any of the numbers the call will be forwarded to the user's voicemail.

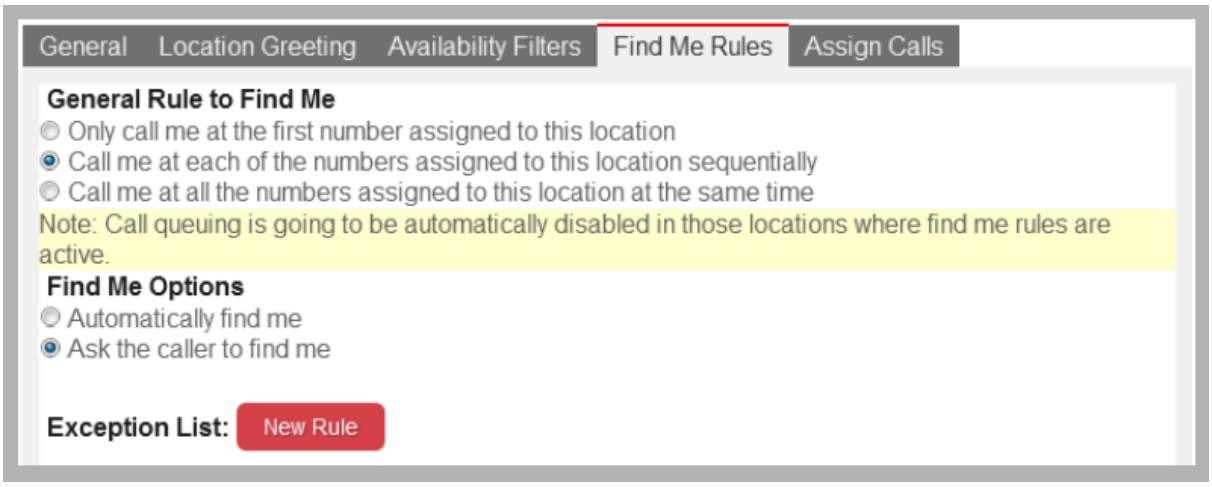
If the default internal address of that mailbox is in the list of numbers assigned to the location, calls made to a DID will always ring that extension first regardless of where it is in the list, and then the Auto attendant will dial the rest of the numbers in sequence from top to bottom (bypassing the default internal extension).

Note: For this feature to work, the user must be set up to be in that location and Available. If the user is Unavailable the find me follow me feature will be disabled, and the Auto attendant will play the location greeting. Also, if the phone is in DND, the unavailable greeting will automatically play and the finding feature will not come in effect.

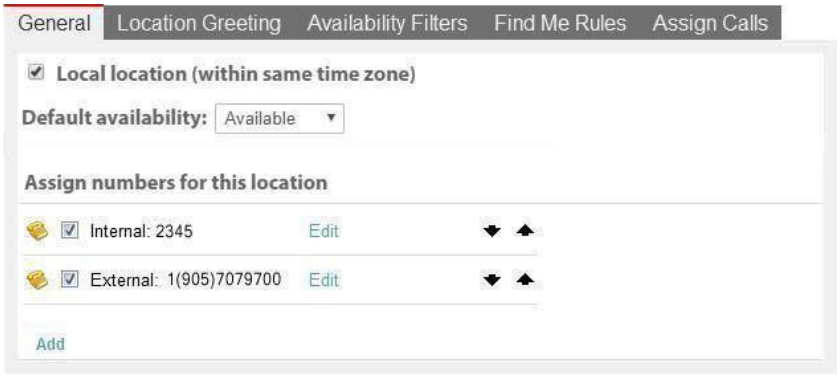
Ask the caller to find me:

This feature will play the unavailable prompt and then give the caller the option to locate the user or just leave a message.

On the **Find Me Rules** tab, select the appropriate options and then go to the General tab to arrange the sequence of calls**:**



On the General tab, add the addresses to the Numbers assigned to this location column and using the up/down arrows select the sequence in which you want to be found (from top to bottom).



Note: In order for this feature to work, it is necessary to have at least 2 addresses in this column, otherwise there is no sequence and the find me feature will not be in effect.

Click on the **Save and Close** button.

When a call is transferred by the Auto attendant or when a call is made to a DID that rings the extension directly, the Auto attendant will automatically dial the first address in the list of numbers assigned to the location, if there is no answer it will play a “no answer” and give the caller the option to locate the user or to leave a message. If the caller selects to locate the user the Auto attendant will dial the next number in the list, if there is no answer in any of the numbers the call will be forwarded to the user’s voicemail.

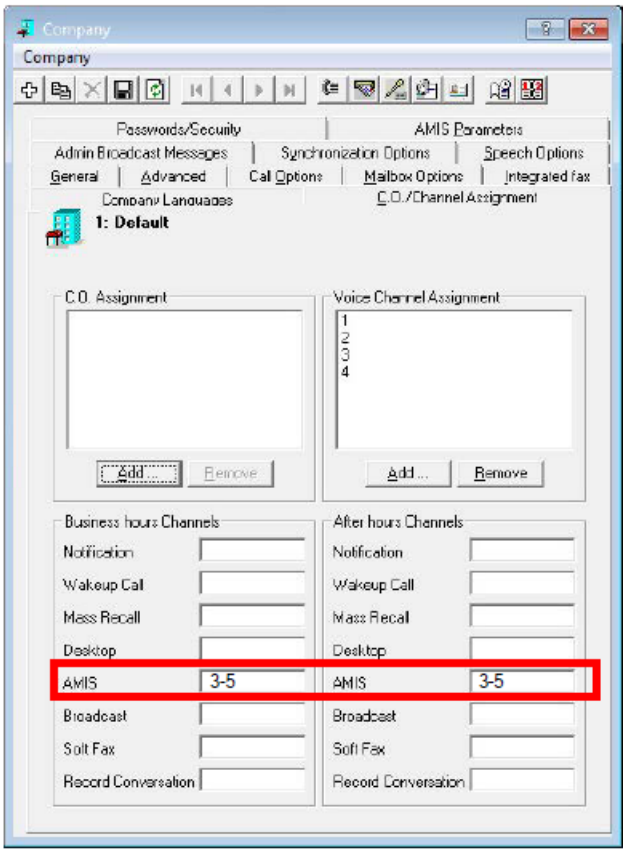
If the default internal address of that mailbox is in the list of numbers assigned to the location, calls made to a DID will always ring that extension first regardless of where it is in the list, and then the Auto attendant will dial the rest of the numbers in sequence from top to bottom (bypassing the default internal extension)

Note: For this feature to work, the user must be set up to be in that location and Available. If the user is Unavailable the find me follow me feature will be disabled and the Auto attendant will play the location greeting. Also, if the phone is in DND, the unavailable greeting will automatically play and the find me feature will not be in effect.

Call me at all the numbers assigned to this location at the same time

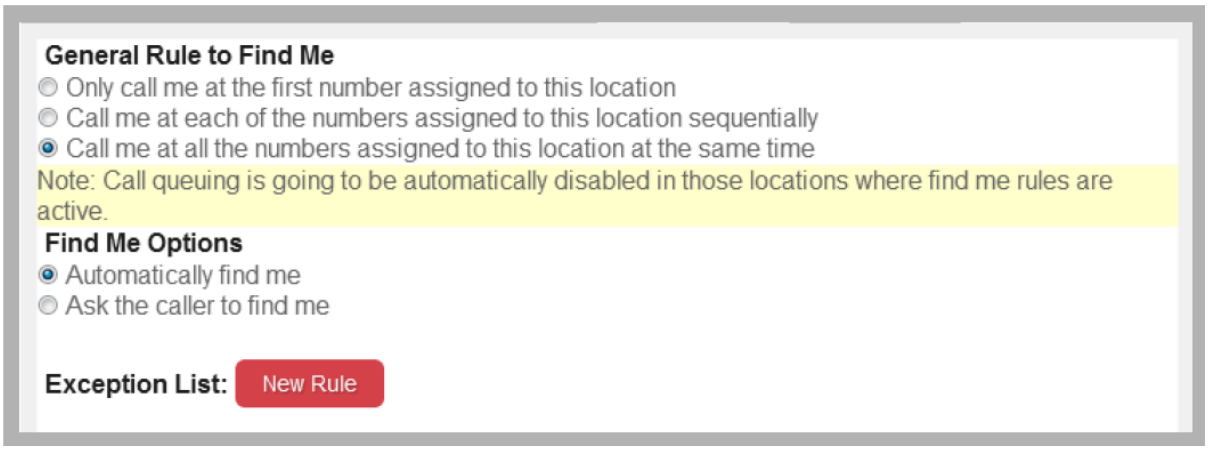
When using this Find me rule, the Auto attendant will try to find the user at all of the numbers assigned to the location at the same time, either automatically or by giving the caller the option to locate the user. The

caller will also be given the option to leave a message.
When this feature is selected it is necessary to specify the channels used for the broadcast in **Company Properties > C.O./Channel Assignment**.

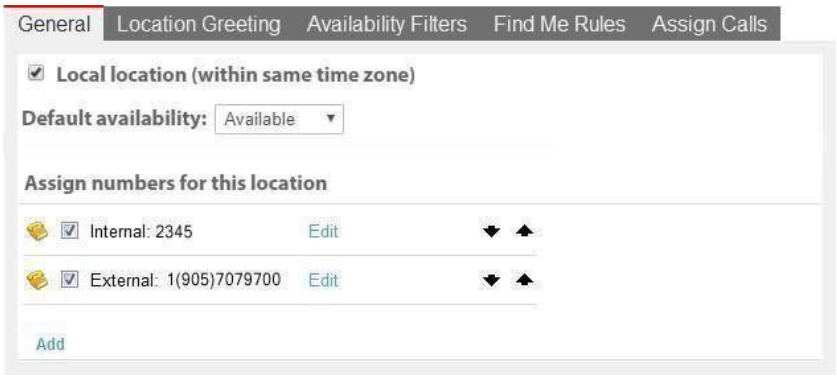


Automatically find me

On the Find me rules tab, select the **Call me at all the numbers assigned to this location at the same time** and the **Automatically find me** options, and then go to the **General** tab to choose the numbers the Auto attendant will dial:



On the **General** tab, in the right-hand column add the numbers that the Auto attendant will dial when trying to find the user.



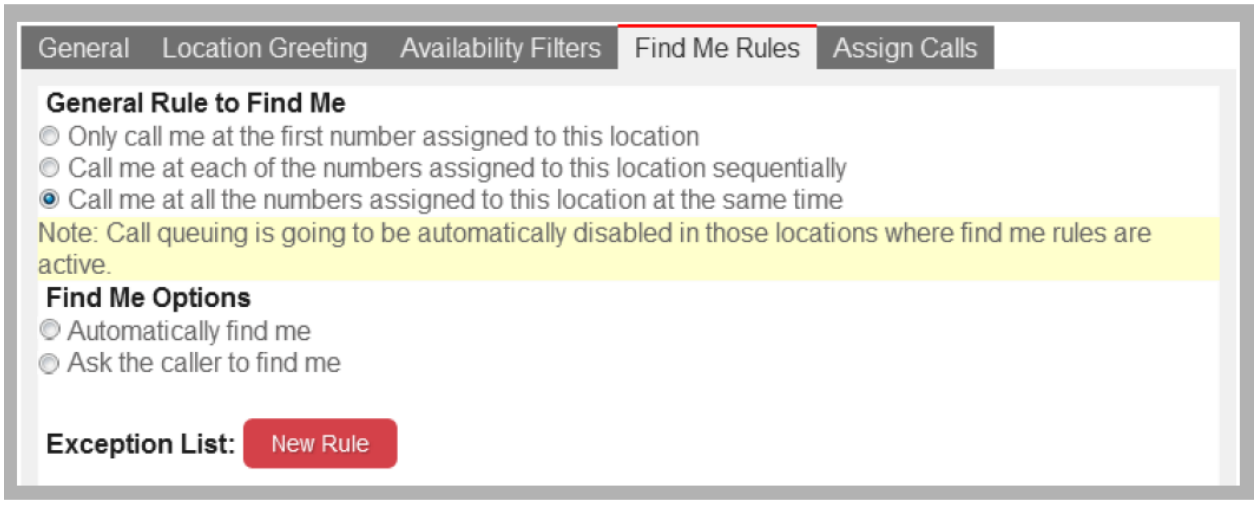
Click on the **Save and Close** button.

When a call is transferred by the Auto attendant or when a call is made to a DID that rings the extension directly, the Auto attendant will automatically dial all the addresses in the list of numbers assigned to the location simultaneously. If the call is answered and accepted in one of those numbers the calls made to the other numbers in the list will be dropped. If there is no answer in any of the numbers the call will be transferred to voicemail.
When a call is made to a DID and the default internal extension is in the list of numbers assigned to the location, that internal extension will always ring first and if there is no answer then the Auto attendant will automatically dial the rest of the numbers in the list simultaneously.

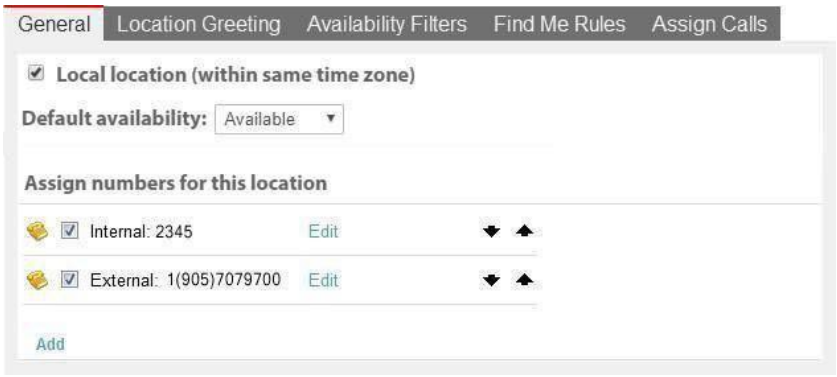
Note: For this feature to work, the user must be set up to be in that location and Available. If the user is Unavailable the find me follow me feature will be disabled and the Auto attendant will play the location greeting. Also, if the phone is in DND, the unavailable greeting will automatically play and the find me feature will not come in effect.

Ask the caller to find me

On the Find me rules tab, select the **Call me at all the numbers assigned to this location at the same time** and **Ask the caller to find me** options, and then go to the **General** tab to choose the numbers the Auto attendant will dial:



On the **General** tab, in the right-hand column add the numbers that the Auto attendant will dial when trying to find the user:



Click on the **Save and Close** button.

When a call is transferred by the Auto attendant, the first number in the list will be dialed, and if there is no answer the caller will be given the option to locate the user or leave a message. If the caller decides to locate the user, the Auto attendant will dial the rest of the numbers in the list simultaneously until one of the numbers answers and accepts the call. If the call is answered and accepted in one of the rest of the numbers, the calls made to the other addresses in the list will be dropped. If there is no answer in any of the numbers the call will be transferred to voicemail.

When a call is made to a DID we should expect the same behavior as above as long as the default internal extension is not on the list of numbers assigned to the location. If the default internal extension is in the list of numbers assigned to the location, that internal extension will always ring first (regardless of the order in the list) and if there is no answer in the internal extension, the caller will be given the option to locate the user or leave a message.

Chapter 13: MULTIPLE TIME ZONE SUPPORT

Introduction

Avaya's Avaya Messaging has built in mail capabilities, including Unified Messaging integrated to multiple mail environments. Since many of our customers have implemented Avaya's Avaya Messaging as a centralized messaging platform, it is desirable to offer users who access Avaya's mail components to be presented their messages in their time zone.
The following document outlines the steps to configure the UC Server to use this functionality.

Visual Guide



When you configure the multiple time zone support feature for your users, they will be able to access their messages anywhere around the world and see the messages in relation to local time rather than the server's time. This will reduce any confusion over when the message was received and offer the users a care-free user experience.

Requirements

Requirements	Details
License	---
Software	Officelinx/IX Messaging version 10.8 Avaya Messaging version 11.0 or higher.

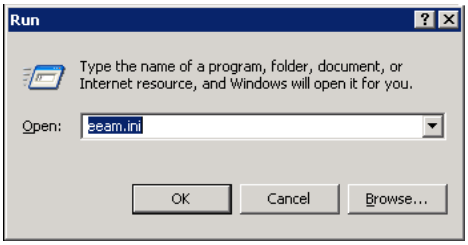
Important: In an HA installation, all servers must have the same time zone set under Windows Date / Time settings. If the servers are configured for different time zones, the timestamps will not play correctly.

Server Configuration

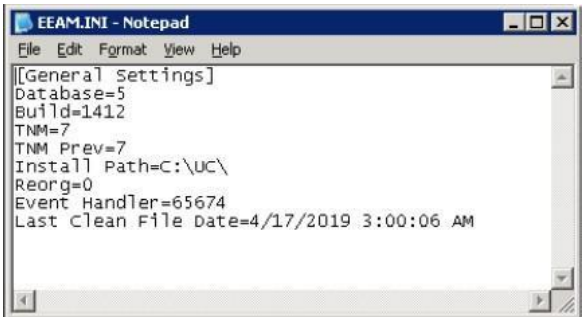
With Avaya Messaging installed on the server, you will need to edit the **EEAM.INI** file, located in the WINDOWS folder of your system.

General Settings

1. Go to **Start > RUN**, and type **EEAM.INI** in the space provided. Click **OK**. Notepad will open and display the contents of the file.



2. Add the following line to the EEAM.INI file: **Honor Timezone for Message = 1**
3. Save the file and close the editor. RESTART the PC for the change to take effect.



Your system is now ready to manage multiple time zones.

Caution: In order to specify your time zone, you will need to edit your Location Calendar. Each time you access your mailbox, either through the phone, the web or any other component, your CURRENT time zone will be determined by your active location calendar. Make sure this is specified.

Note: If the user does not have access to Web Access to specify their location calendar, an Administrator will need to set this using Avaya Messaging Admin.

The Time Zone feature supports:

All Messages presented via any device will be in the user's local time.

- Call History will be presented in the user's local time.
- Calendar events made using Outlook will be retained in the user's local time as defined by their Location Calendar.

For example, if the user's PC where Outlook is running is set for Eastern time, but the Location Calendar is defined as Pacific, then any appointment created by the client from Outlook will be offset from Eastern time to Pacific, as specified by the user's Location Calendar.

The Time Zone feature does NOT support the following:

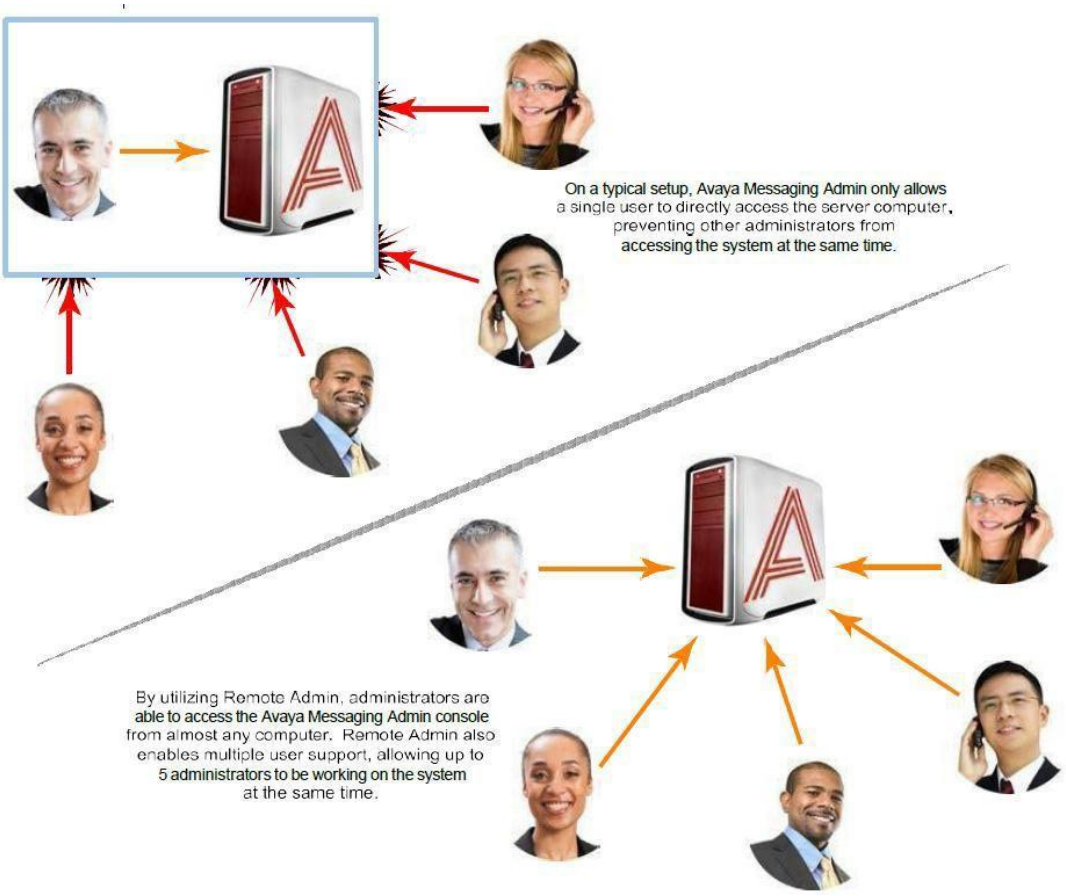
- Notification schedules – any schedule defined must be defined in the Server's time. For this reason, Web Access will now show the server's time in a window to assist the user.
- Future message delivery – message delivery must be defined in the Server's time.
- Wakeup Call – All events must be defined in the Server's time.
- Any other function where the user enters time and date.

Chapter 14: REMOTE ADMINISTRATION

Introduction

Remote Admin allows system administrators or support personnel to remotely access Avaya Messaging Admin from their own workstation, eliminating the need to be in front of the server to perform administrative functions.

Visual Guide



Requirements

Requirements	Details
Software	Microsoft Windows Server 2012,2016, 2019, 2022 and windows 7/8/10 & 11
Network	Workstations where the remote admin is installed must be in the same network as the Avaya Messaging server.

Warning: Utilizing remote admin means that more than one person may be managing the database. If two or more people make changes to the same entry; the first change may be overwritten without notification.

Note: The maximum number of people that can connect using Remote Admin is **5**.

Installing Remote Admin

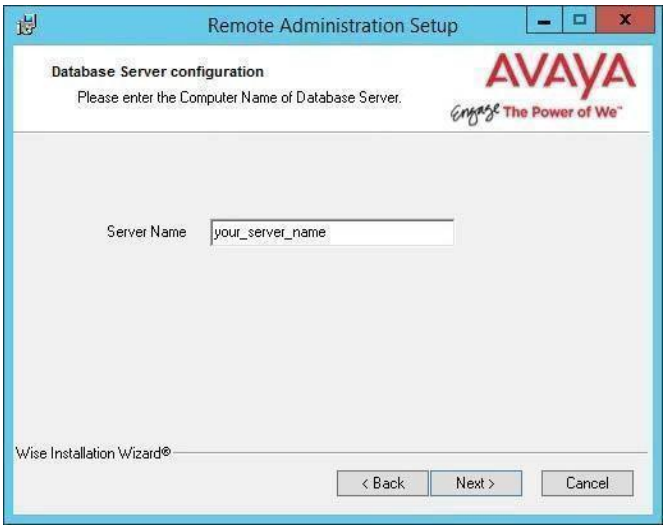
Important: Avaya Messaging must be installed and operating normally on the voice server before proceeding. Remote Admin must be installed on **the same subnet** as the Avaya Messaging voice server, or the Consolidated Server on a High Availability installation.

Remote admin must be installed on each workstation where it will be used.

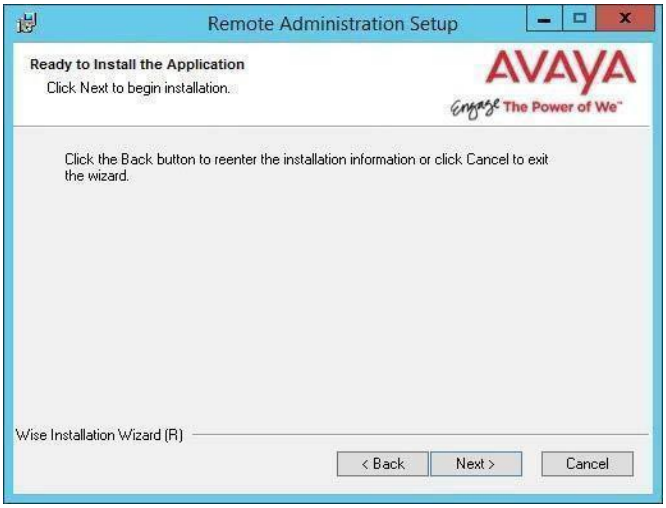
1. On the voice server, or on the Consolidated server in a high availability environment, locate the Avaya Messaging installation directory (this is **C:\UC** by default). Share the UC folder with the Windows user(s) who will be running Avaya Messaging Admin remotely.
2. On a remote workstation, login and verify that this user has access to the UC folder on the server. Go to \\ComputerName\UC and attempt to open the folder (change ComputerName to the name of the server on your system). If you can open the folder, then the share was a success, and you can continue with the installation.
3. Copy the **\UC\RemoteAdmin\RemoteAdmin.exe file** from the server to the remote machine.
4. Launch (double-click) the program and the Remote Administration Installation Wizard will start.
5. Click **Next** to begin the installation.



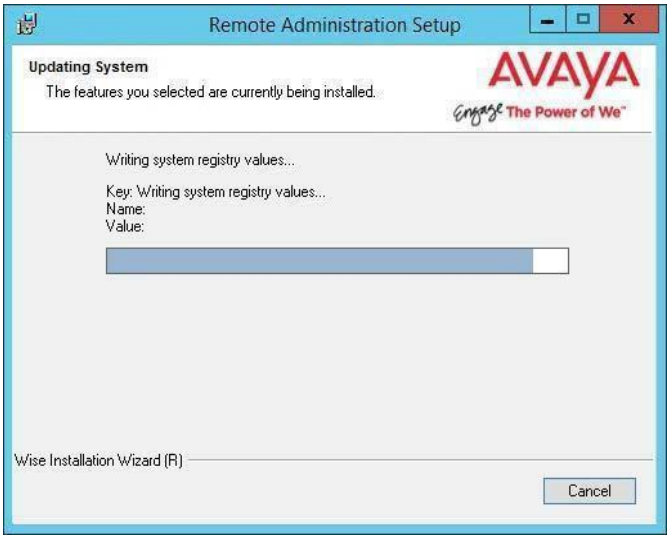
6. When prompted, enter the computer name for the Avaya Messaging voice server, or the Consolidated Server. Click **Next**.



7. The program is ready. Click **Next** to begin installing the program.



8. Remote Administrator will be installed on the system.



9. When finished, the wizard will report that the installation was successful.
10. Click **Finish** to complete the installation.



Remote admin is now ready to be used. A shortcut will be placed on your Windows desktop to access the program.



Connecting to Remote Admin

To connect to Avaya Messaging Admin remotely, you will need the login credentials.

1. Run the Avaya Messaging Admin shortcut from the desktop. The login screen appears.



2. Enter the User Name and Password in the appropriate fields. Click **Login**.

Caution: The computer launching Remote Admin must be a member of the same domain as the Avaya Messaging server to make the connection.

3. You will be remotely connected to the Avaya Messaging Admin of the remote server.

Chapter 15: REMOTE PRINTER

Introduction

The Avaya Messaging Remote Printer feature allows system administrators to remove printing functions from the voice server and move them to another computer. This reduces the demand on the voice server CPU allowing for greater speed and efficiency in processing voice data.

Remote Printer also permits the use of existing licenses for software that is not installed on the voice server. For example, MSOffice and Adobe Acrobat must be installed on the voice server if faxes are to be sent in any of their supported formats (doc, docx, pdf). Using the Remote Printer to redirect this traffic to a machine that already has the necessary software installed removes the need for additional licenses to be consumed by the voice server.

Remote Printer is included on the DVD with the standard release of Avaya Messaging. It is installed by default as part of Avaya Messaging Admin. The Remote Printer program must be installed on the host, and the settings on the voice server must be changed to point to the host machine.

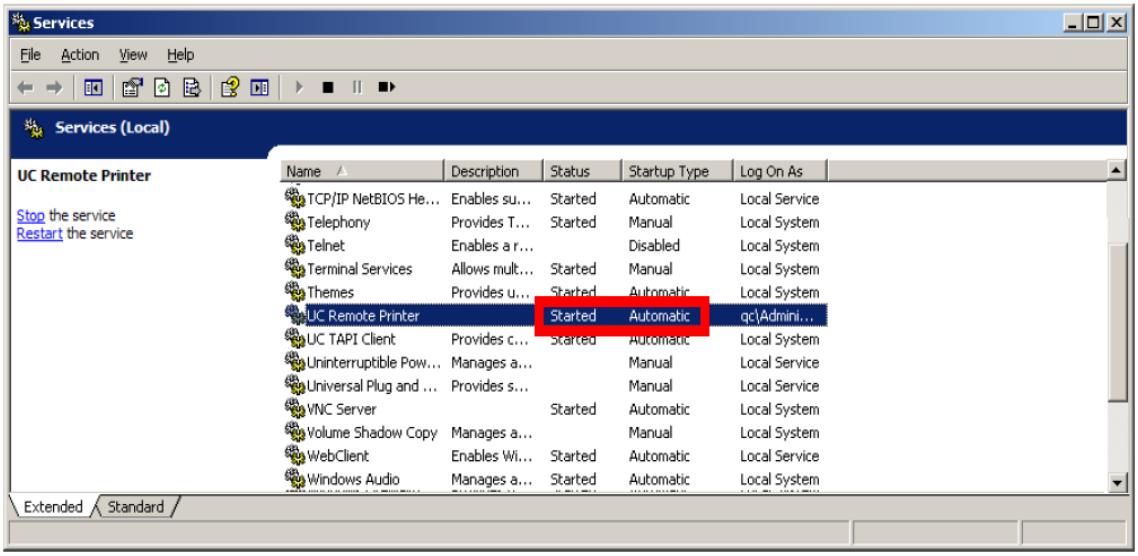
Remote Printer Host Installation and Setup

Note: Avaya Messaging must be installed and properly configured on the voice server before proceeding with the Remote Printer host installation. Refer to the Server Installation Guide and Server Configuration Guide for more information.

The following instructions must be performed on the computer that is to act as the remote printer host.

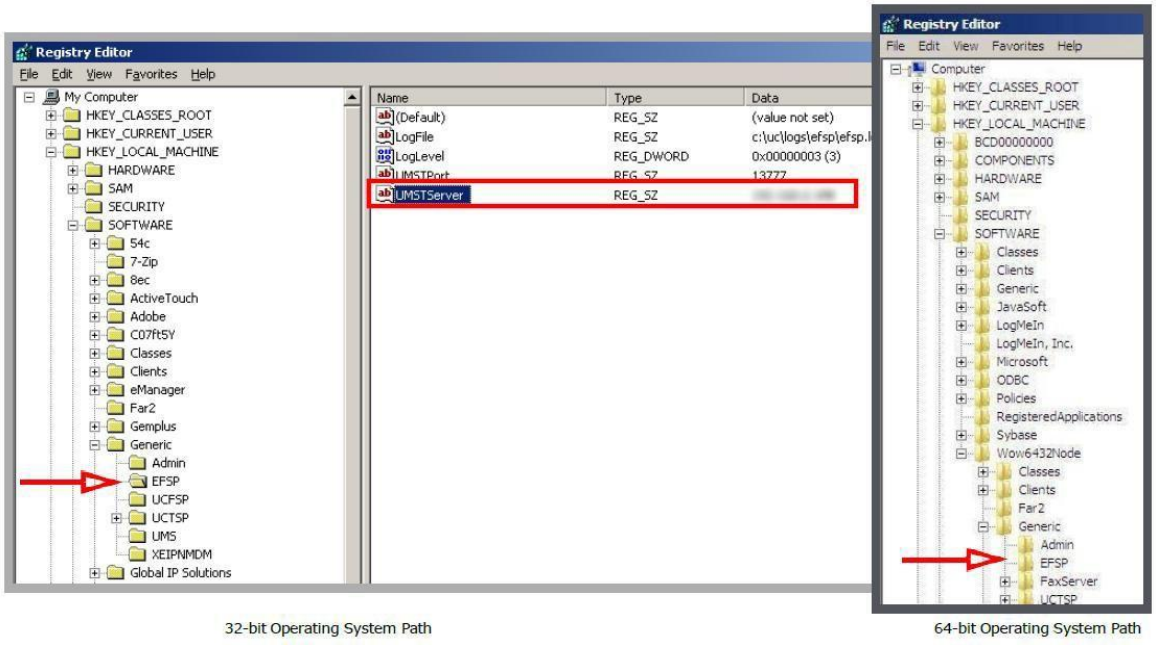
1. Run the **UCPrint.msi** program. This can be found on the Avaya Messaging DVD at: D:\UC\UCPrint (change “D:\” to the correct location of your DVD drive). Double-click this file to start the installation. The process takes a few seconds and runs silently in the background.

2. After a few moments, go to **Start > Administrative Tools > Services** and verify that the UC Remote Printer service is installed and running. This service should be configured to start automatically.



Note: The **Log On As** account should be the same as that used during the installation of MS Office or Adobe Acrobat Reader.

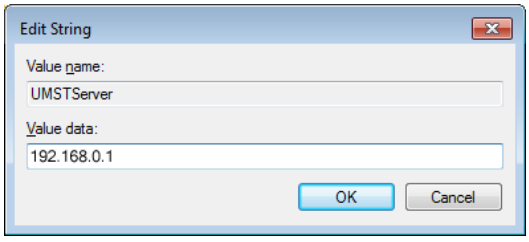
3. Go to **Start>Run** and type **regedit** in the text entry box. Click **OK**.
4. On the left pane, navigate to either:
    - HKEY_LOCAL_MACHINE>SOFTWARE>Generic>EFSP (for 32-bit operating systems), or
    - HKEY_LOCAL_MACHINE>SOFTWARE>Wow6432Node>Generic>EFSP (for 64-bit operating systems).



32-bit Operating System Path

64-bit Operating System Path

5. In the right pane, double-click **UMST Server** and enter the IP Address of the Avaya Messaging server for the value data. Click **OK** and close the regedit screen.



The client-side configuration is complete. Proceed with the setup of the Avaya Messaging voice server.

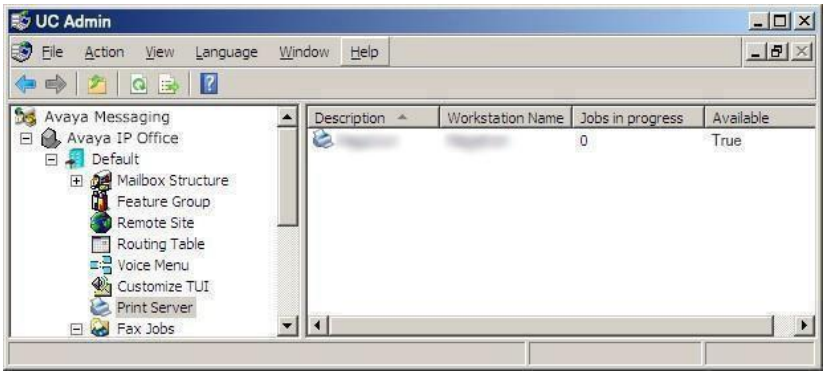
Avaya Messaging Voice Server Remote Printer Setup

The following instructions are performed on the Avaya Messaging voice server.

Note: These instructions assume that Avaya Messaging has already been installed and configured on the voice server. For details on the installation and setup of Avaya Messaging, please refer to the Server Installation Guide and the Server Configuration Guide for details.

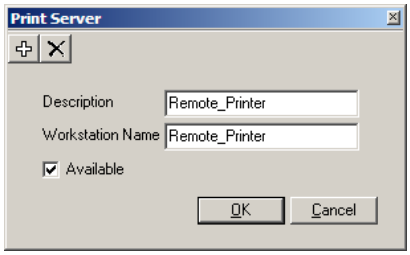
1. Go to **Start > Administrative Tools> IIS Manager**. Verify that **FTP** is installed and running. This should already be set up as part of the Avaya Messaging installation.
2. Open Avaya Messaging Admin and click **Print Server**.

3. Right-click on **Print Server** and choose **Add**.



4. Fill in the required fields.

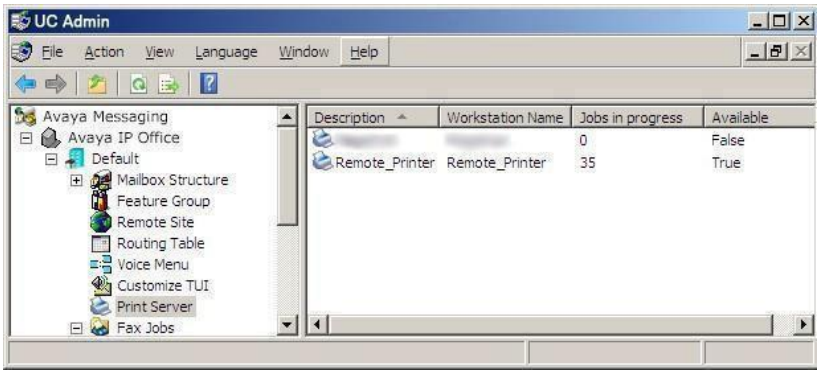
   Description: Enter a descriptive name for the remote print server.
   Workstation Name: Enter the PC name or the IP Address of the remote printer host computer.
   Available: Enable this checkbox.



   Click **OK** when finished.

5. In the right pane, double-click the local print server and disable the **Available** checkbox.

   Click **OK** when finished.



6. Go to **Start>Administrative Tools>Services** and disable the **UC Remote Printer** service.
7. Go to **Start>Administrative Tools>Services**. Stop then start the following services:
   UC Unified Messaging System Tasks Service and **UC VPIMServer**.
8. On the computer acting as the remote printer host, stop then start the **UC Remote Printer** Service.
   The setup of the Remote Printer feature is now complete.

Chapter 16: AVAYA MESSAGING FAXING

Introduction

While most business interactions occur digitally, faxing remains a required feature for many people. This is especially true when there are technical limitations or legal requirements involved. Rather than having to purchase a fax machine to handle this traffic, UC users can conveniently send faxes from their computer desktop digitally through the Avaya Messaging server with the proper license and feature set enabled.

Requirements

The fax may be sent out from your computer through these methods:

- **Windows Fax Services**: Send virtually any item as a fax as long as the software you are using to view the document or image supports printing. You can send any content as a fax by printing it through the fax services integrated with Avaya Messaging. However, this method requires some advanced configuration.

- **Email Client**: The advantage of this method is being able to send a fax from anywhere where there is access to email client. No additional configuration is required. Whether it is a web-based or a dedicated client, you can send a fax through the Avaya Messaging server as long as there is access to email. However, you can only send files types that are supported by the server. If the server does not recognize a certain type of file (i.e., docx, pdf), the fax request will fail.

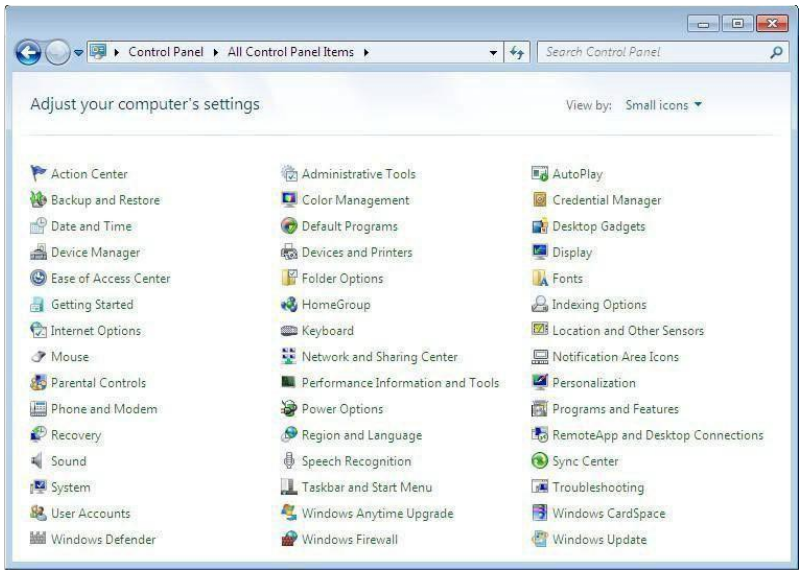
- **Fax Gadget**: This method is similar to the email client but has been streamlined for use with the Web Access interface, either accessed directly or through client applications such as UC Web Gadget.

Fax via Windows Fax Services (Windows 7) Configuration

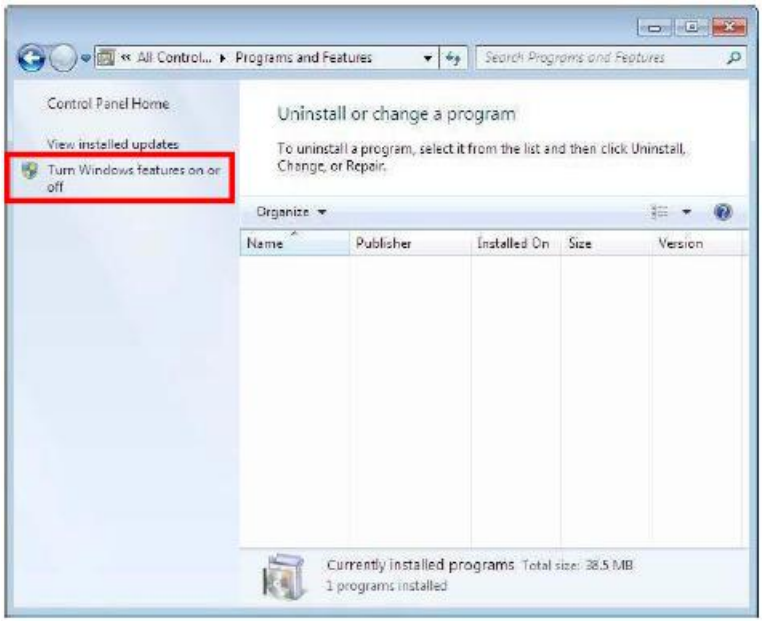
Please follow these steps to configure your client machine with the Windows Fax services.

Warning: If iPD has already been installed, remove it, enable fax services, then reinstall the application.
Warning: Only TIFF and TXT formats are supported by default. To send a fax in any other format, the computer must have the necessary program installed to support that file type (i.e., MicroSoft Office for doc and docx files, Acrobat Reader 9 (available on the Avaya Messaging DVD) or earlier for pdf, etc.). Ensure that this software is installed and working (run at least once) before attempting to send a fax using that format.

1. Launch the **Programs and Features** application within **Control Panel**.
   Note: Change your viewing style to icons to view the list of applications instead of categories.



2. Click on the **Turn Windows features on or off** link on the left-hand pane.

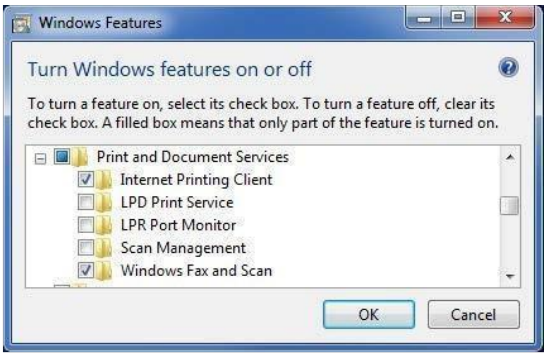


3. From the feature window, enable the following features.

Print and Document Services

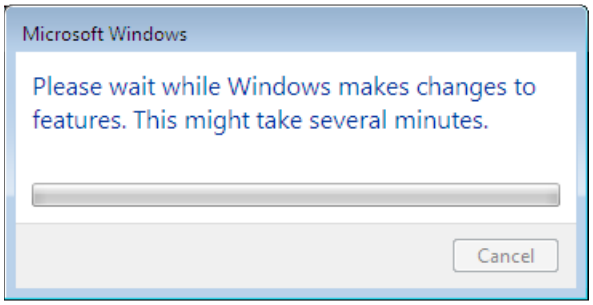
- Internet Printing Client
- Windows Fax and Scan

Click **OK** when you're done.

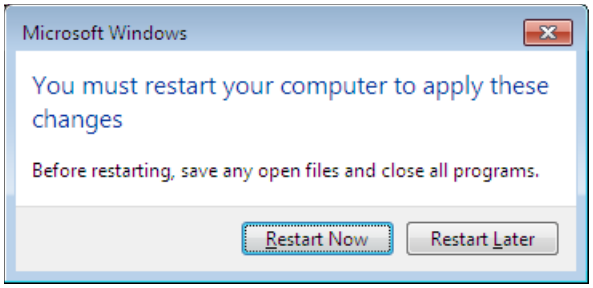


Note: If these services are already installed on your computer, skip to step 6.

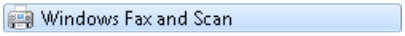
4. Windows will start to add the selected components. This process may take a while.



5. If you are asked to restart your computer, click **Restart Now** to reboot. Refer to the **Client Applications Guide** for more information.

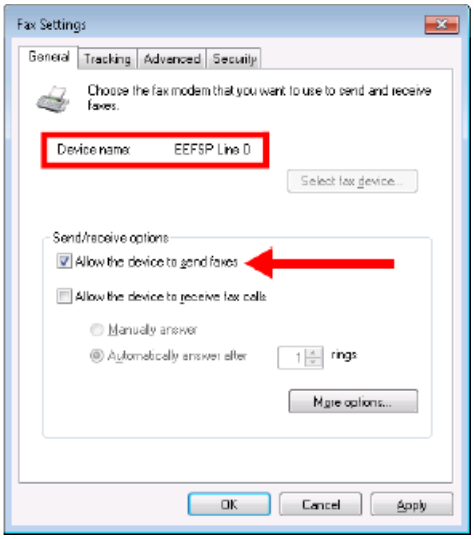


6. Go to **Start > Programs** and launch **Windows Fax and Scan**.8.Go to **Tools > Fax Settings...**

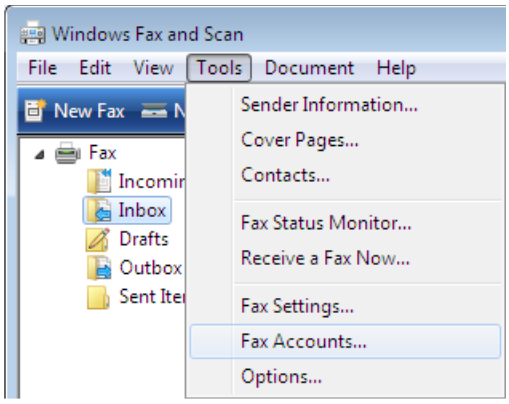




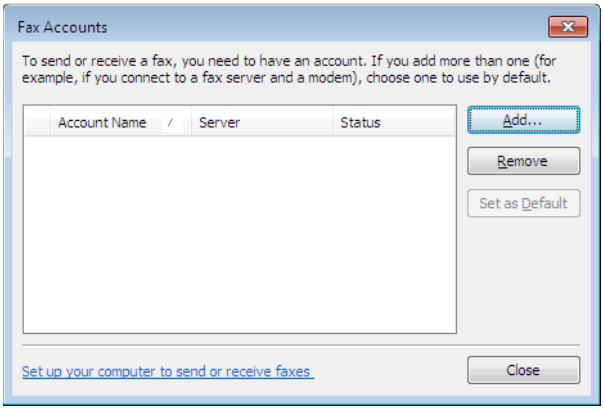
7. From the General tab, confirm that the Device name is **EEFSP**.
   If it is not, click on Select fax device... and choose it from the list.
   You must also make sure that **Allow this device to send faxes** is **enabled**. **Allow the device to receive fax calls** should be **disabled** since faxes are received through the Avaya Messaging server. Only enable this checkbox if you have a specific reason to do so.
   Click **OK** to save your changes.



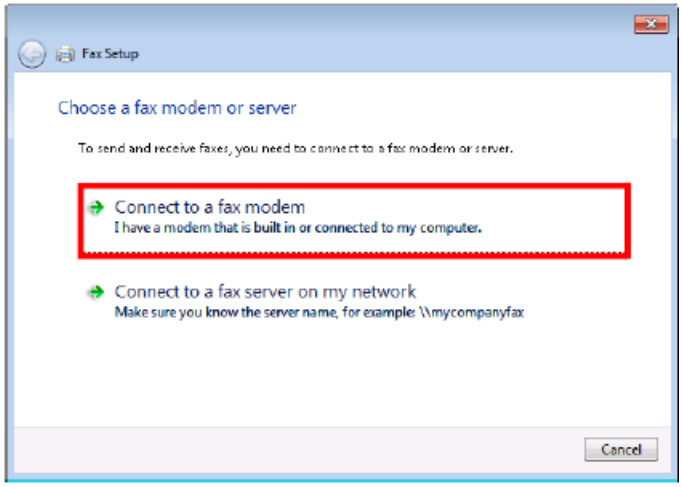
8. Open **Tools > Fax Accounts...**



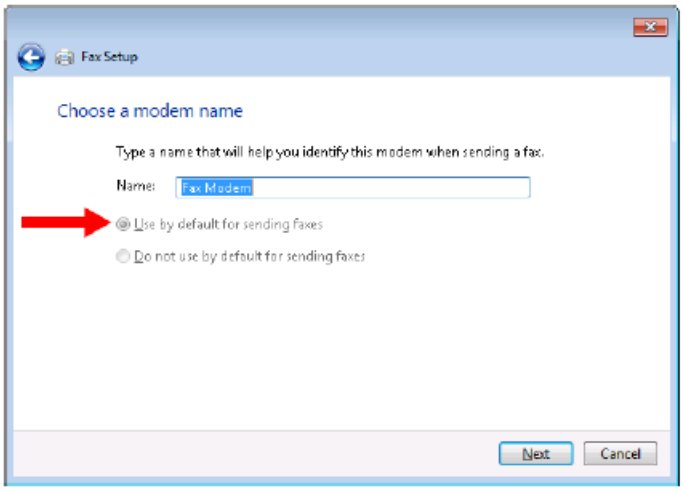
9. Click the **Add...** button.



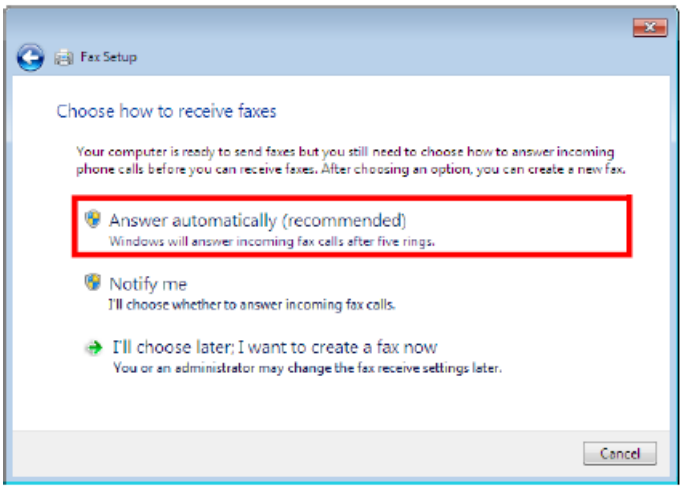
10. Select the **Connect to a fax modem** option.



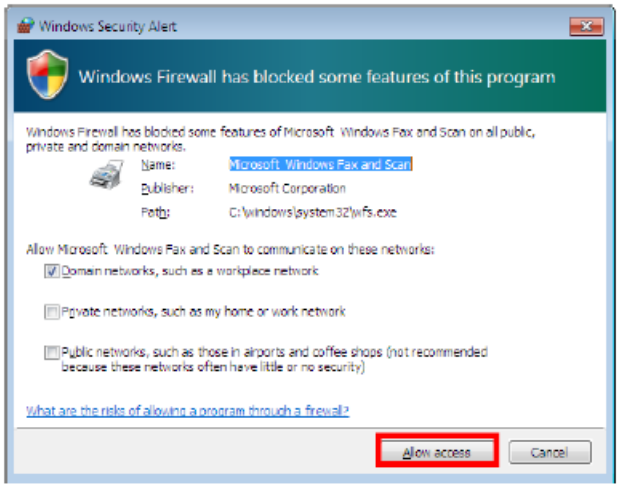
11. Give the connection a name. You may leave it at the default value, or change it according to your preference. In most cases this item should be the only device configured on your computer. If not, please ensure that **Use by default for sending faxes** radio button is enabled before continuing.
Click **Next** when ready.



12. Choose the **Answer automatically (recommended)** option.

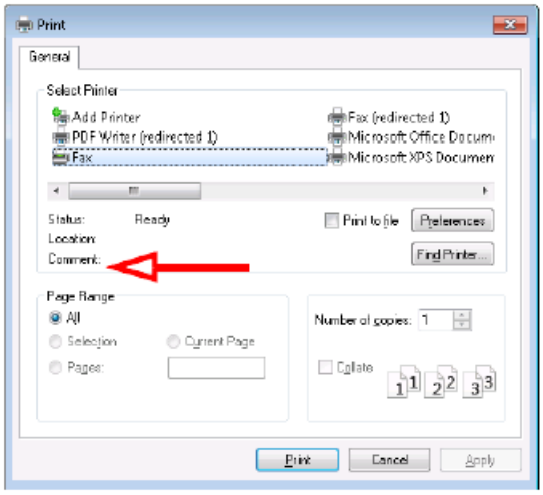


13. If you are prompted regarding your Firewall, click to **Allow access** at the bottom of the window. Your computer is now ready to send fax messages.

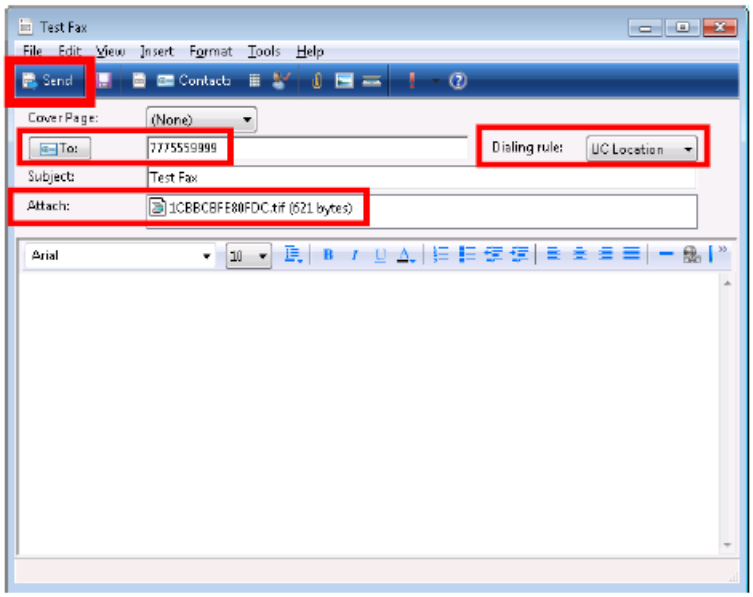


Sending Fax from an Application

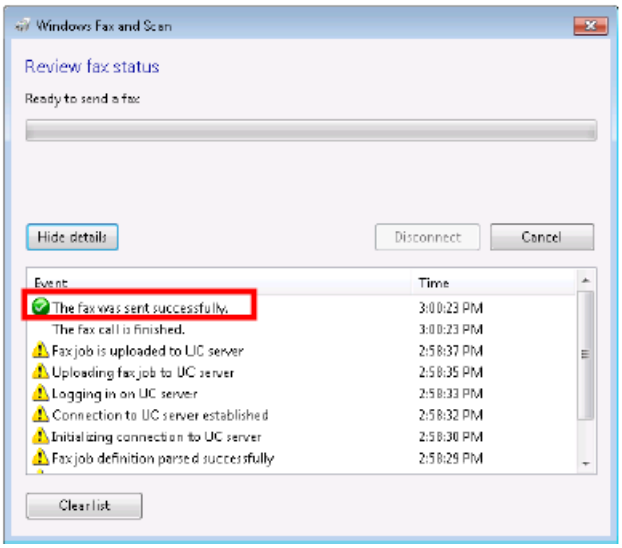
Once your computer is configured for faxing, you can send faxes from any application that can print using the Windows printing tool. To send a fax, select **Print** from the application of your choice (e.g., Microsoft Office Word, Adobe Acrobat). The Print windows appears. Select **Fax** as the print device, then click **Print**.



A new window will open to define the destination and any other components required for the fax.
The document being sent as a fax will appear as an attachment.
Ensure that you enter the correct fax number on the **To**:**field**.
Set the **Dialing rule** to **UC Location**.
All other fields, such as **Cover Page**, **Subject** and **Body** are optional fields which you can utilize to customize your fax message.
When you are ready to send the fax, click the **Send** button.



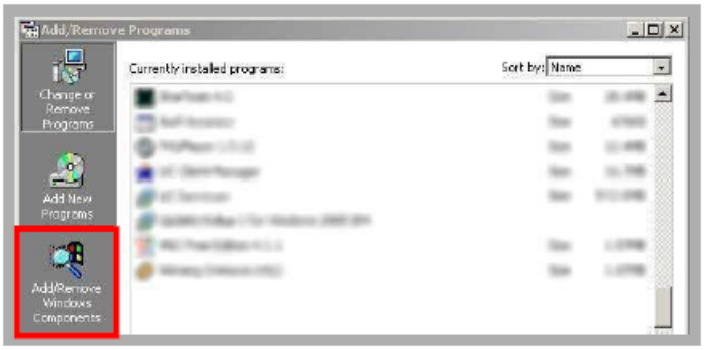
The Fax status window will appear to notify you of the fax's status. Once transmission has completed successfully, you will be notified here.
If the fax fails for any reason, the details will be shown here. Consult with your system administrator if you are having trouble sending faxes.
Note: You can track of all your outgoing faxes from the Windows Fax and Scan application available on the Start menu.



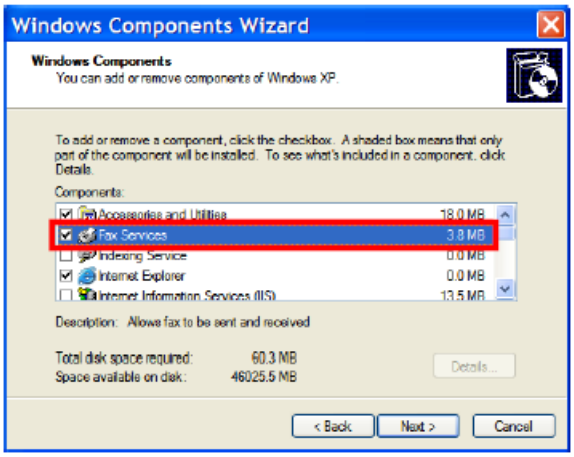
Fax via Windows Fax Services (Windows XP) Configuration

Please follow the below steps to configure your client machine for use with Windows Fax services.
Warning: Only TIFF and TXT formats are supported by default. To send a fax in any other format, the computer must have the necessary program installed to support that file type (i.e., MicroSoft Office for doc and docx files, Acrobat Reader 9 (available on the Avaya Messaging DVD) or earlier for pdf, etc.). Ensure that this software is installed and working (run at least once) before attempting to send a fax using that format.

1. Go to **Start > Settings > Control Panel**. Double-click **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.



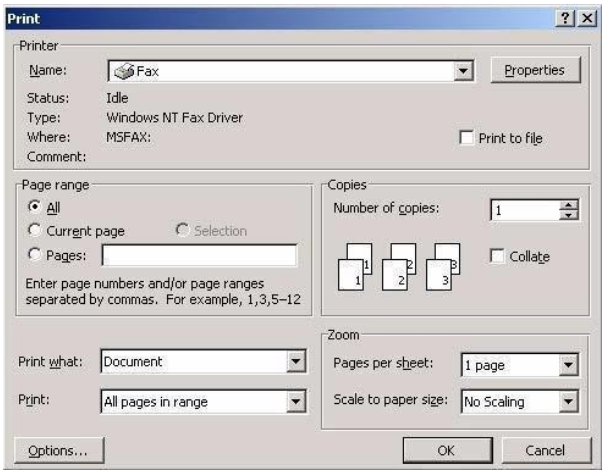
3. Enable **Fax Services**. Click **Next**.



Note: You may be asked to provide a Windows installation disc depending on the computer settings.
4. Once the process is complete, you will have the ability to send faxes from your desktop.

Sending Fax from an Application

1. Open the document or image that will be sent as a fax.
2. Print the item. This is normally under the **File > Print** menu.
3. When the print dialogue appears, select fax as the print device. Click **OK**.



4. The **Send Fax Wizard** screen appears:

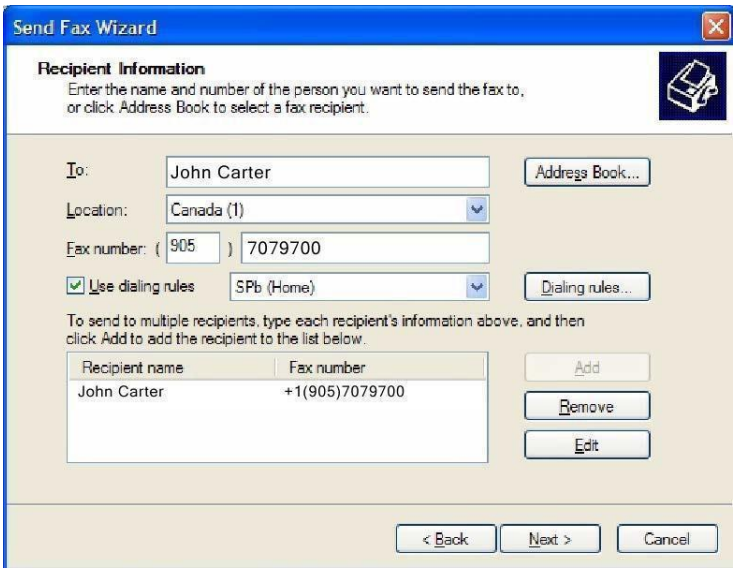


5. Click **Next**. The **Recipient Information** screen appears:
6. Specify the following:

- In the **To** field, enter the name of the intended recipient.

Hint: Click the **Address Book** button to select a recipient from your personal address book.

- From the **Location** dropdown list, select the location (country) of the intended recipient.
- In the **Fax number** fields, specify the fax area code and number for the intended recipient.
- Enable **Use dialing rules** if you want specific dialing rules to apply. Select the dialing rules from the accompanying dropdown list.



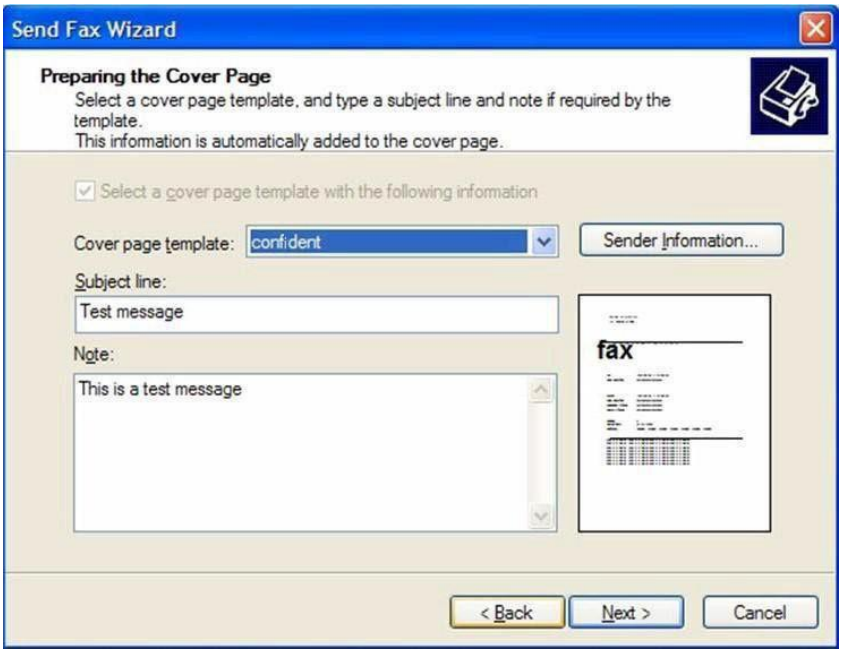
Note: To create a new set of dialing rules, click on the **Dialing rules** button.

7. Click on the **Add** button to add the recipient whose information you have just specified.

Note: You can add as many recipients as you wish.

8. Click **Next** when you have added all desired recipients. The **Preparing the Cover Page** screen appears:
9. From the **Cover page template** dropdown list, select the cover page template you want to use.

10. In the **Subject line** field, enter subject text for the fax cover page.
11. In the **Note** box, enter message text for the fax cover page.



12. Click **Next**. The **Schedule** screen appears:
13. Select one of the **When do you want to send this fax?** radio buttons:

Now - send the fax immediately
When discountrates apply - send the fax the next time discount phone rates apply
Specific time in the next 24 hours - send the fax at a specific time in the next 24 hours. If you select this radio button, you must then specify a time of day from the accompanying spin-box



14. Select one of the following **What is the fax priority**? radio buttons:

High - high priority for sending fax
Normal - normal priority for sending fax
Low - low priority for sending fax

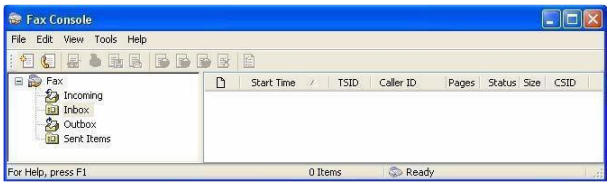
15. Click **Next**. The following screen appears:
16. If you want to preview your fax, click on the **Preview Fax** button. Otherwise, click **Finish**.

Hint: To confirm that your fax was sent successfully, check the Sent Items folder of your Fax Console application.



Viewing the Status of a Fax

1. Select **Start > All Programs > Accessories > Communications > Fax > Fax Console**.



2. In the left hand pane, click to expand **Fax**. The following list describes the folders under Fax:

   • The **Incoming** folder contains faxes that are currently being received.
   • The **Inbox** folder contains faxes that have been received.
   • The **Outbox** folder contains faxes that are scheduled to be sent.
   • The **Sent Items** folder contains faxes that have been successfully sent.

3. In the left hand pane, highlight a folder.
4. In the right hand pane right click on the fax you want and select **Properties**.
5. On the General tab, check the status of the fax under **Status**.

Note: If an item is in the Outbox folder, then the fax attempt has failed. Until all retries have been exhausted, Status will read **Pending**. If all retries have been exhausted, Status will read **Failed**.

Receiving and Viewing a Fax

1. Select **Start > All Programs > Accessories > Communications > Fax > Fax Console**. The Fax Console detects incoming faxes and stores them in your inbox.
2. To view a fax click **Inbox**, then double click on the fax you want to view.

Canceling a Fax Job

You can cancel any fax you have set up to be sent at a future time.

1. If Fax is not open, select **Start > All Programs > Accessories > Communications > Fax > Fax Console**. The Fax Console appears.
2. To cancel a fax click **Outbox**, then right click on the fax you want to cancel.
3. Click **Delete** to cancel the fax.
4. Click **Yes**.

Automatically Send Retry

You can set up Fax so that it continues trying to send your fax if the receiving fax machine is busy.
Note: Fax is automatically set up to retry three (3) times at 10-minute intervals.

1. Select **Start > Control Panel**. The Control Panel appears.
2. If your Control Panel is in **Category** View, click **Printers and Other Hardware**. Click **View installed printers or fax printers**. The **Printers and Faxes** screen appears.
   OR
   If your Control Panel is in **Classic** View, double-click the **Printers and Faxes** icon. The **Printers and Faxes** screen appears.
3. Right click **Fax** and select **Properties**. The Fax Properties dialogue box opens.
4. Click the **Devices** tab, then **Properties**. The Modem dialogue box opens.
5. Specify the number of retries and the amount of time between retries.
6. Click **OK**.

Automatically Canceling a Fax

If your PC tried to send a fax and failed to connect to a fax machine, you can automatically cancel a failed fax.

1. Select **Start > Control Panel**. The Control Panel appears.
2. If your Control Panel is in **Category** View, click **Printers and Other Hardware**. Click **View installed printers or fax printers**. The **Printers and Faxes** screen appears.

   OR,
   If your Control Panel is in **Classic** View, double-click the **Printers and Faxes** icon. The **Printers and Faxes** screen appears.
3. Right click **Fax** and select **Properties**. The Fax Properties dialogue box opens.
4. Click the **Devices** tab, then click **Properties**. The Modem dialogue box opens.
5. Click the **Cleanup** tab.
6. Click to check Automatically delete failed faxes after and specify the number of days.
7. Click **OK**.

Email to Fax

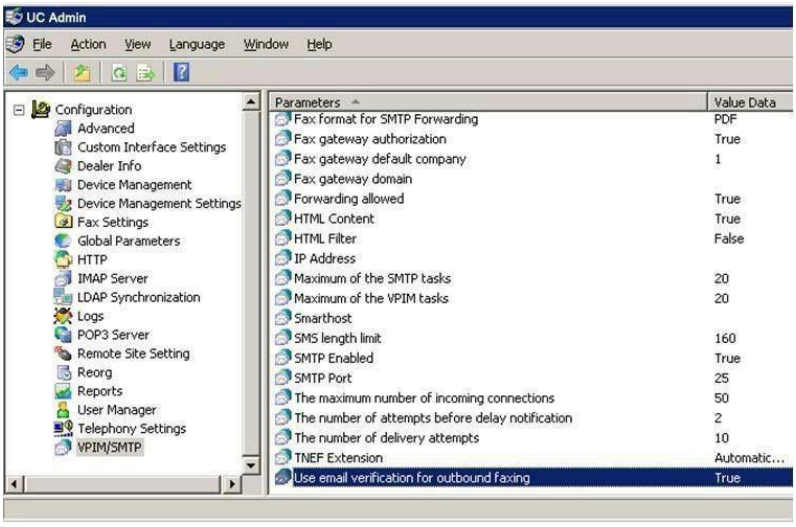
Note: The example shown in this guide uses Gmail. However, this process can be repeated with virtually any email client including web based email, MS Office 365, and MS Exchange.

Email to Fax requires no user-end configuration. The only requirement is that the fax email is sent to the correct domain using the correct format.

Administrator Setup

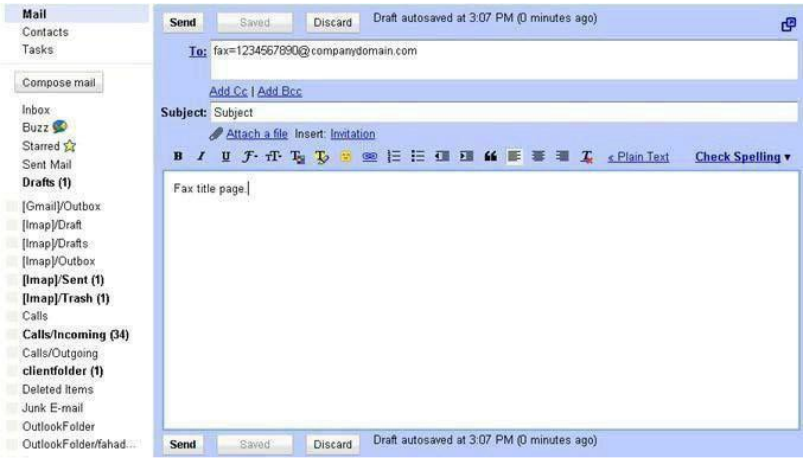
Warning: Only TIFF and TXT formats are supported by default. To send a fax in any other format, the computer must have the necessary program installed to support that file type (i.e., MicroSoft Office for doc and docx files, Acrobat Reader 9 (available on the Avaya Messaging DVD) or earlier for pdf, etc.). Ensure that this software is installed and working (run at least once) before attempting to send a fax using that format.

- The network administrator must setup an MX Record that points **vpim.*yourcompany*.com** to the Avaya Messaging voice server (or the Consolidated Server in an HA environment).
- **Send URL** must be configured and activated on the voice server (see the *Security Enhancements chapter* in *Avaya Messaging Server Configuration Guide*).
- SMTP port 25 needs to be opened on any firewall or security services.
- An active email account and client are also required.
- Under **Avaya Messaging Admin>Configuration>VPIM/SMTP**, set **Use email verification for outbound faxing** to **True**.



Sending a Fax

Create a new email message. In the **To...** field, type **fax=** followed by the number of the destination fax machine at(@) your company's server. For example, **fax=1234567890@companydomain.com**.
The Subject line and the email message body will be included with the fax as a cover page.
Include the main body of the fax as an attachment to the email.
Note: Only **TIFF** and **TXT** formats are supported by default. However, if the server has the appropriate programs installed, other formats can be used (**PDF** requires Acrobat 9 (available on the Avaya Messaging DVD), **DOC** / **DOCX** need MS Office).



Send the email when you're ready.
The message will be accepted by your server and processed into an outgoing fax job.

Fax Activation

To prevent spam, once you have clicked the **Send** button, the Avaya Messaging Server will send you an email to confirm that the fax message is to be sent.
This email includes a link which you must click on to authorize the server to send the fax message. Click on the link.

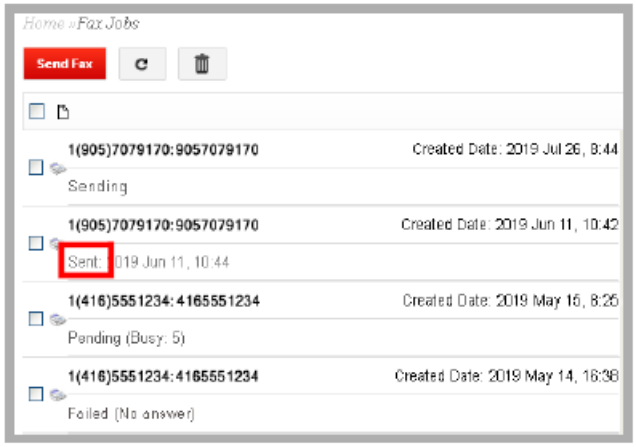


The system will respond with a message verifying that the fax has been queued for sending. The message status can now be tracked in the fax status report folders.



The fax message you've sent will now be listed under **Fax Jobs**. You will be able to easily check on the status of the fax to ensure that it has been sent out.

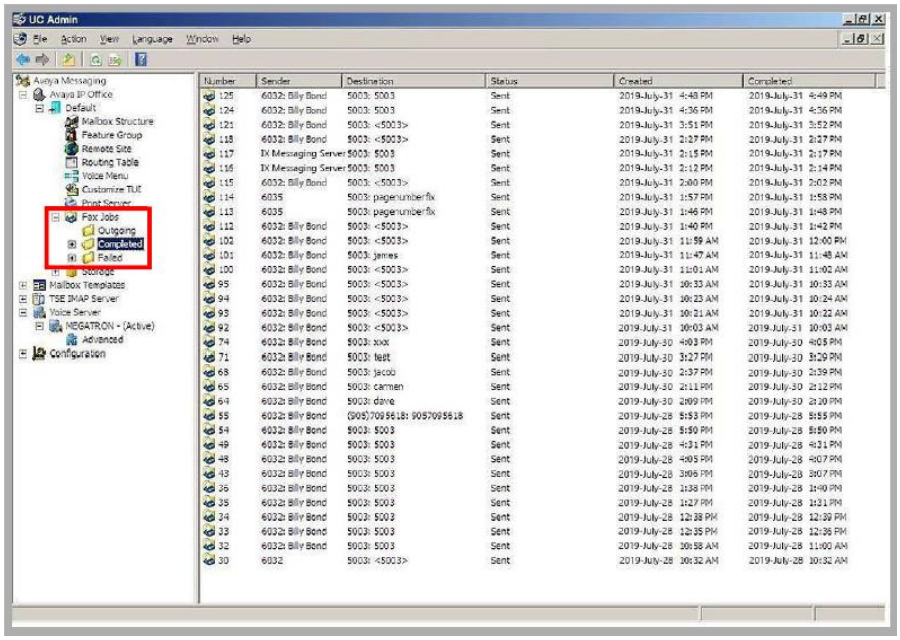
If the status doesn't change to **Sent** within a reasonable amount of time, or if the fax message fails repeatedly, please contact your system administrator for help regarding the matter.



Fax Jobs

Whenever a fax message is sent or received by the UC server, an entry will appear in **Admin > Fax Jobs** so that the administrator can easily view and manage faxing. All fax jobs will appear in one of three folders and will be moved accordingly.

Outgoing: This folder contains the details of all faxes that are currently being sent that have neither finished nor failed.
Completed: This folder contains the details of all faxes that have been successfully sent.
Failed: This folder contains the details of all faxes that could not be sent. The system has stopped trying to send the fax.



Each of these folders contains the following information for each fax message:

Number: This field displays the job number assigned to the fax.
Sender: This field displays the individual who sent the fax.
Destination: This field displays the Mailbox number to which the fax is directed.

Status: This field displays the current status of the fax (Initial / Pending / Sending / Sent / Canceled / Failed-Busy / Failed-No Answer / Failed-Other / Failed).
Created: This field displays date and time the fax was sent.
Completed: This field displays date and time when the transmission of the fax was completed.

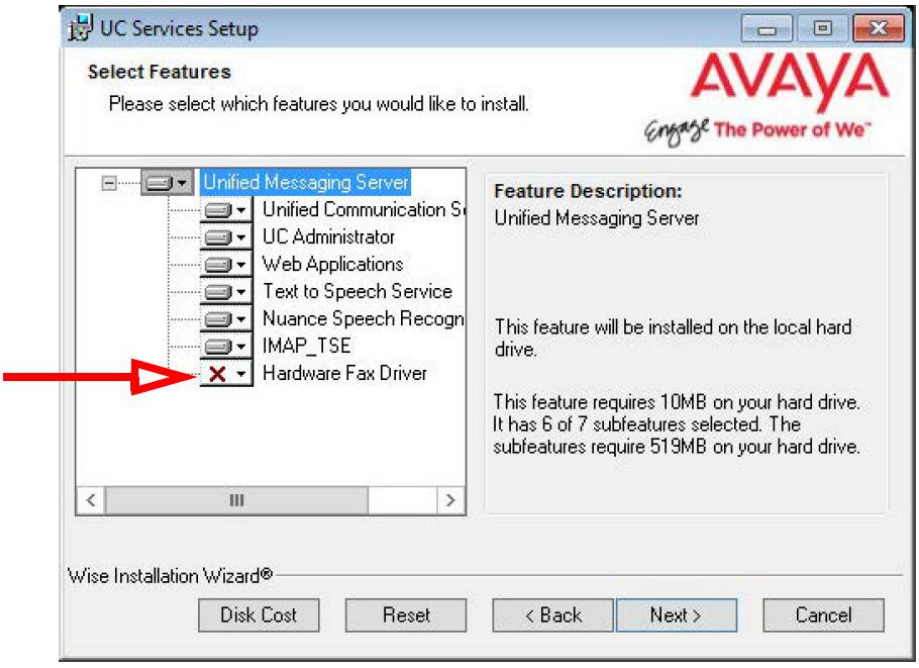
Chapter 17: DIALOGIC SR140 FAX INTEGRATION

Introduction

Avaya Messaging permits high volume fax users to integrate their Dialogic SR140 fax software with the voice server platform.

Prerequisites

Install the Avaya Messaging program onto the computer that will act as the **Voice Server**. Ensure that the **Hardware Fax Drivers** option is installed at the **Features Selection** screen during program installation. This will ensure that the necessary program elements are included with Avaya Messaging.

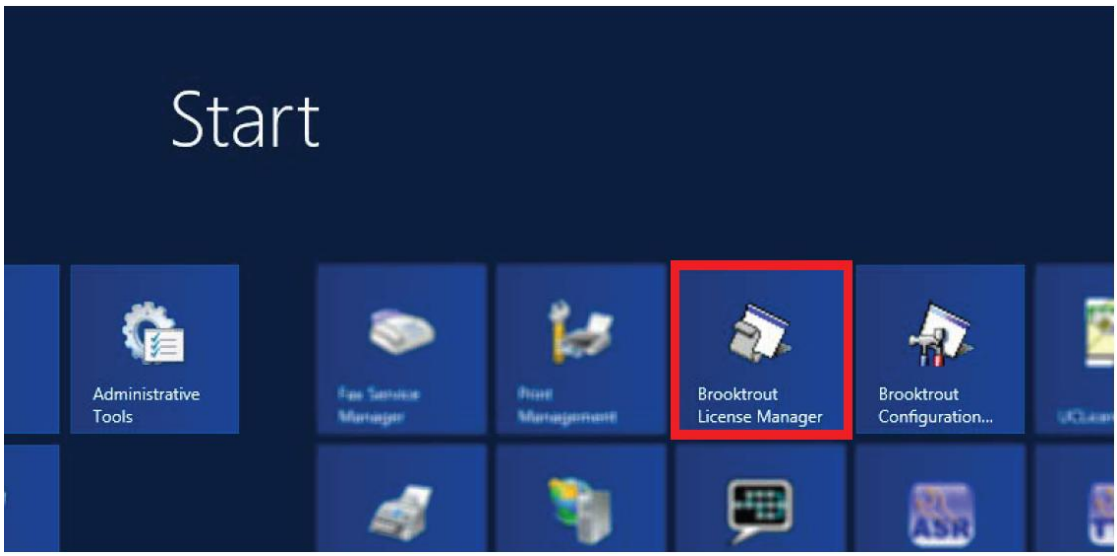


Configuration

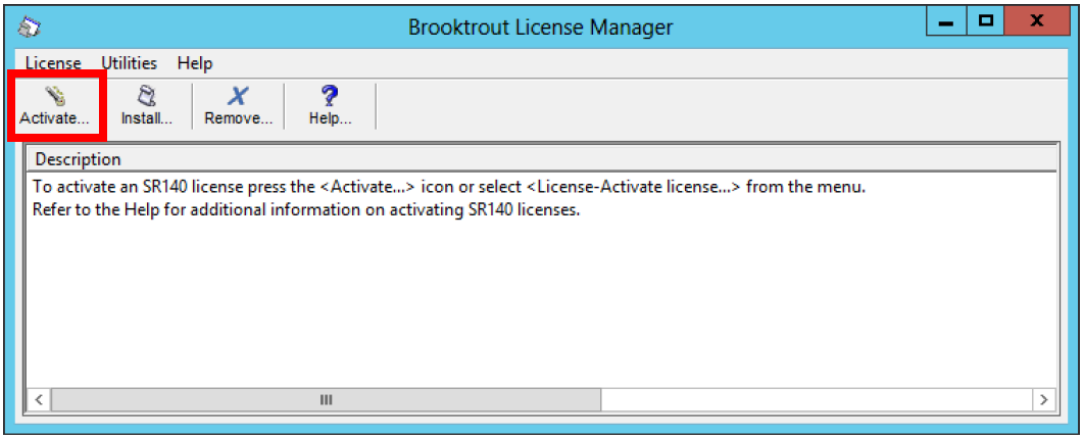
Once both the Dialogic SR140 and the Avaya Messaging voice server have both been installed, the fax software must be configured to communicate with the UC platform.
The following procedures must be performed on each computer that is running the SR140 software.

License Manager

1. Open the **Brooktrout License Manager** program.



2. Enable the SR140 license by clicking on the **Activate** button.

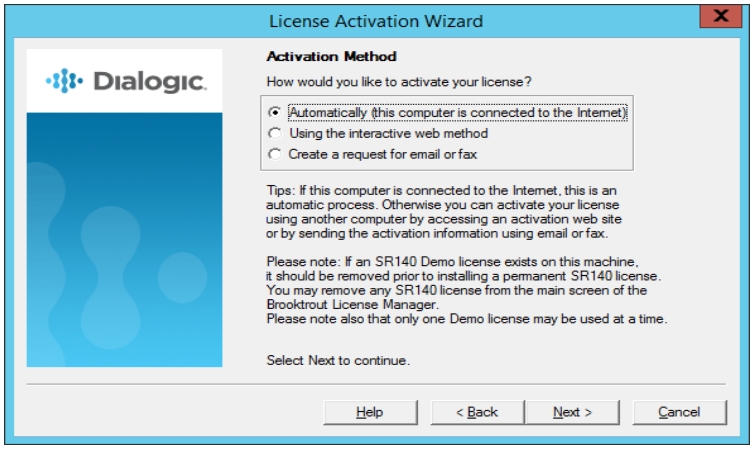


Note: The procedure shown here uses the Activation Wizard and an Internet connection.
If you have a license file, select **Install** and point the program to the file provided by your vendor.

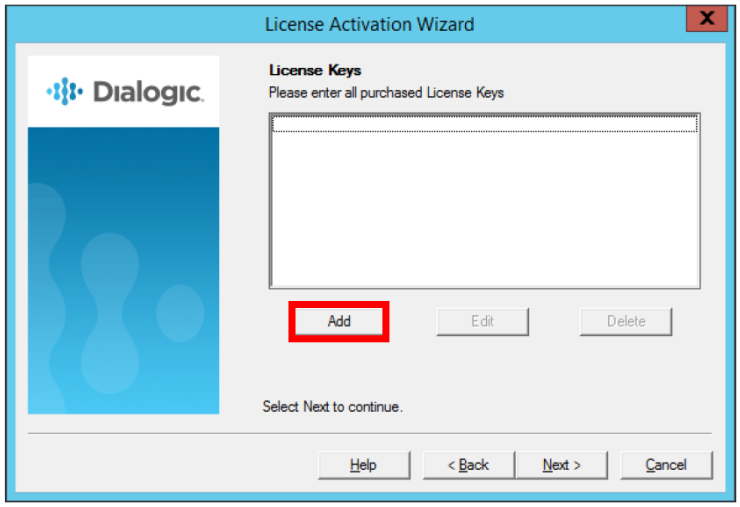
3. Click **Next**.



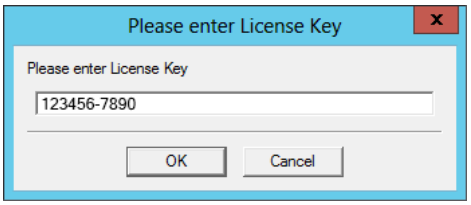
4. Make sure that **Automatically this computer is connected to the Internet** is selected as the Activation Method, then click **Next**.



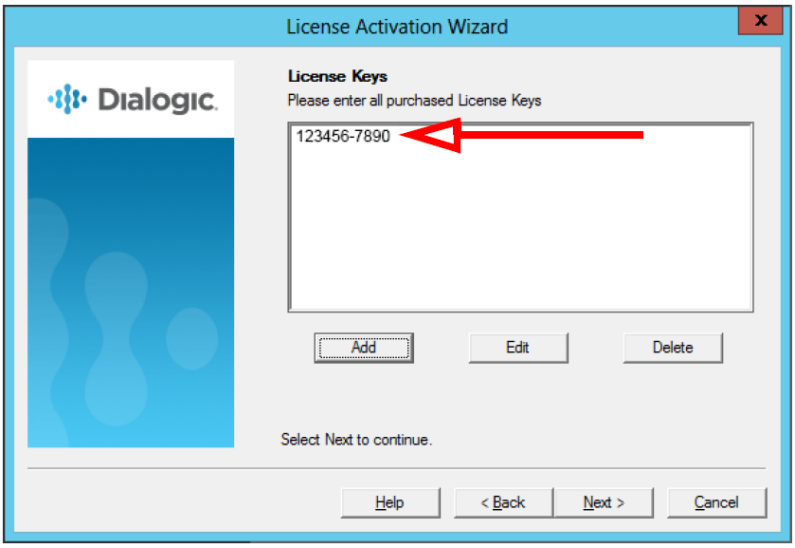
5. Currently, no **License Keys** are installed. Click **Add**.



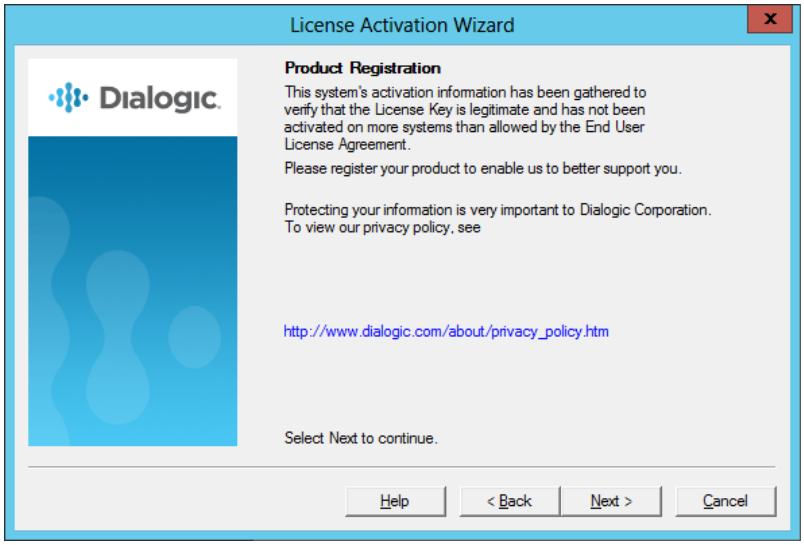
6. Enter the SR140 license key number that came with the fax software package. Click **OK** when ready.



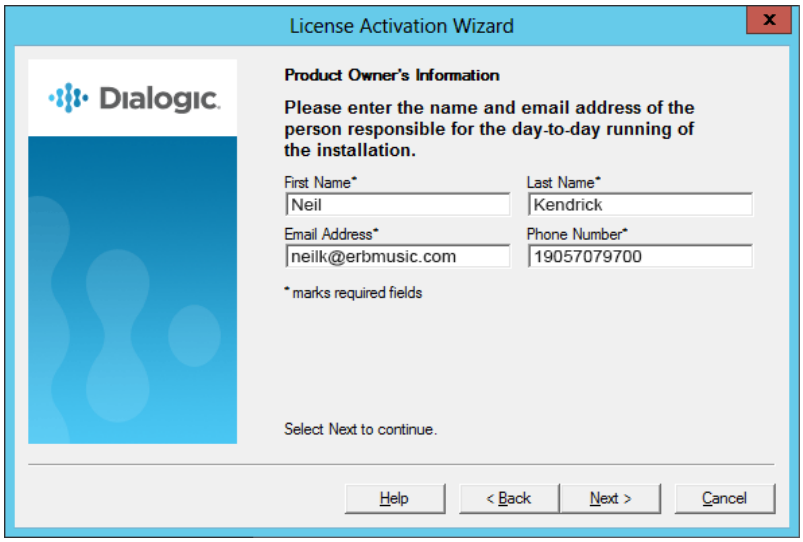
7. The new license key has been successfully added to the system. Click **Next**.



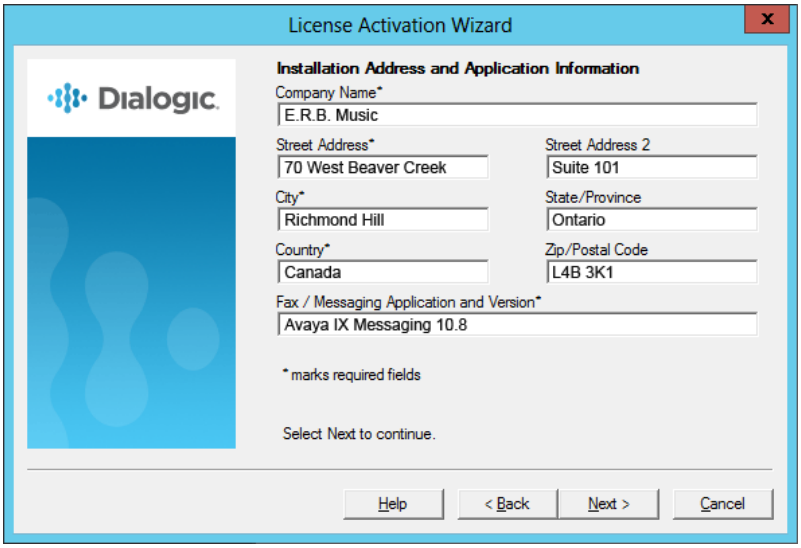
8. Click **Next** to continue to the **Product Registration** pages.



9. Enter the details of the site administrator. All fields are required for registration. Click **Next** when ready.



10. Enter the required information into the fields provided. This is the site where the software is installed. Click **Next** to continue.

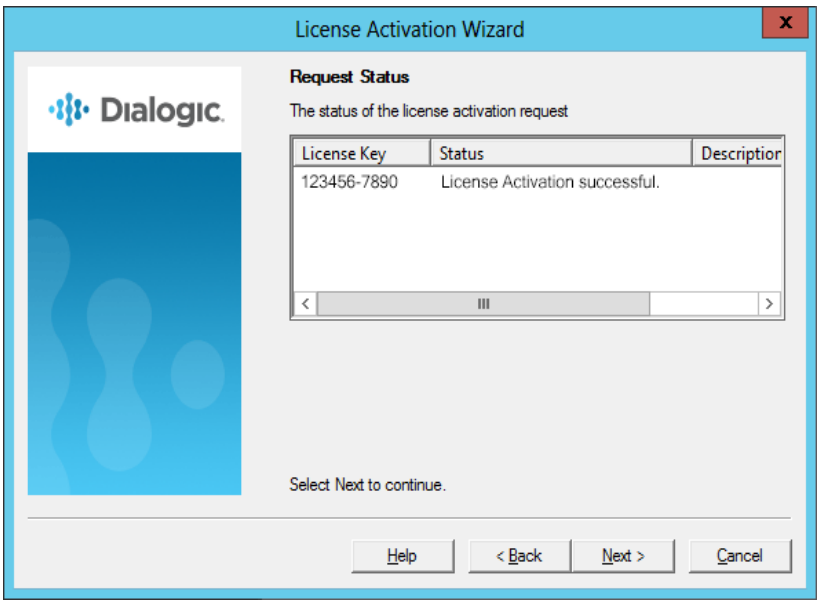


11. The program will connect to the Dialogic servers to upload the registration details. This requires a working Internet connection and must be completed successfully before the license is activated.

    When it has finished, click **Next** to continue.



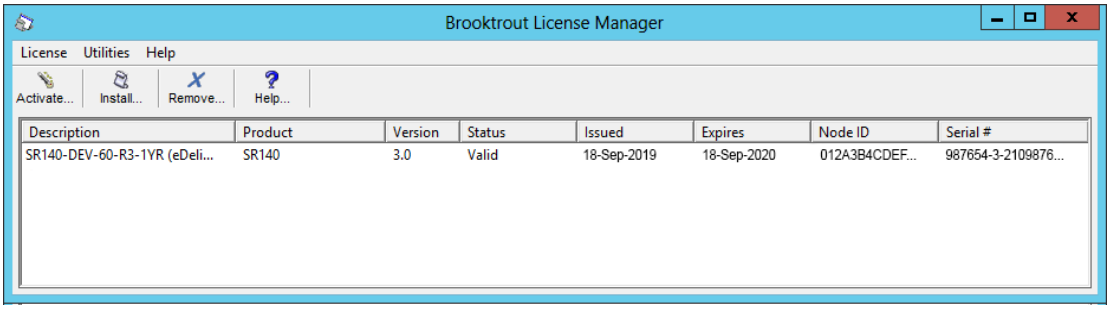
12. The new license has been added to the Wizard. Click **Next**.



13. Click **Next** to complete the activation Wizard.

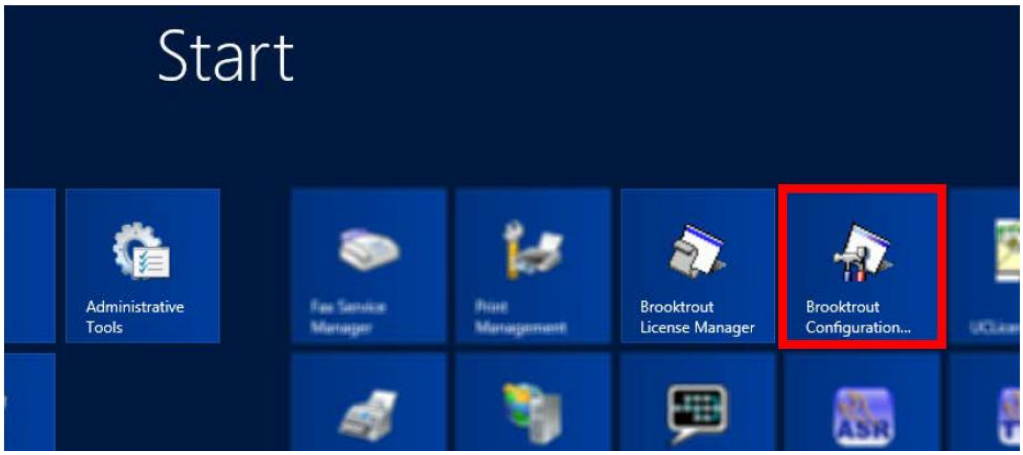


14. The added license appears in the **Brooktrout License Manager**.

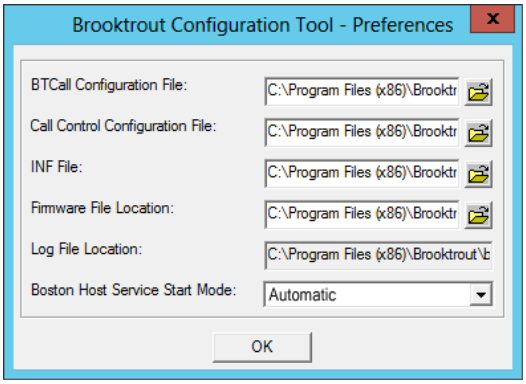


Configuration Manager

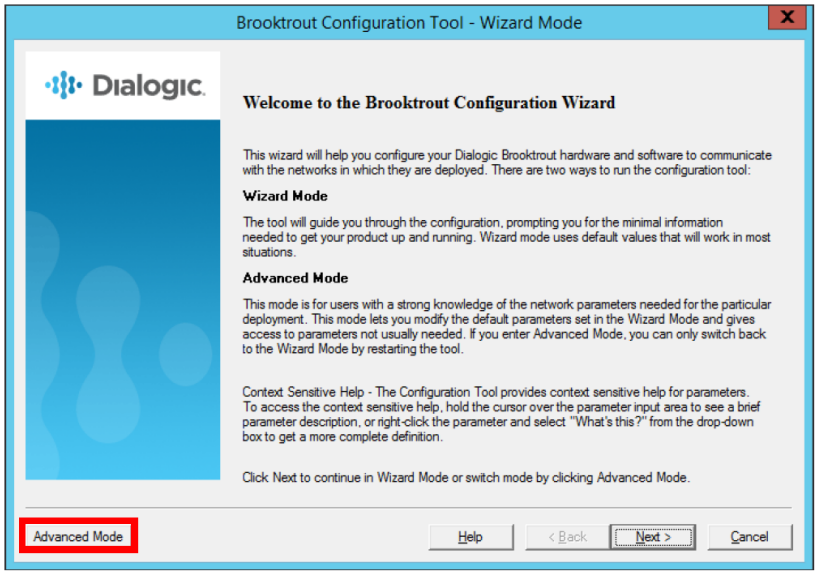
15. Open the **Brooktrout Configuration Manager** program.



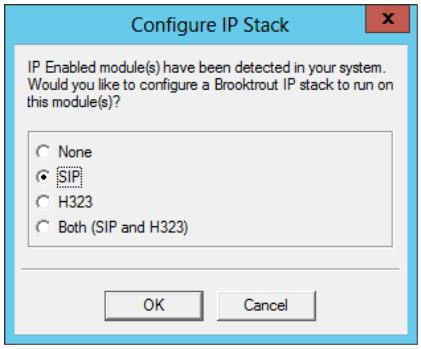
16. At **Configuration Tool - Preferences**, change **Boston Host Service Start Mode** to **Automatic** and click **OK**.



1. When the Configuration Wizard starts, choose **Advanced Mode**.



2. Enable the option for SIP. Click **OK** to continue.

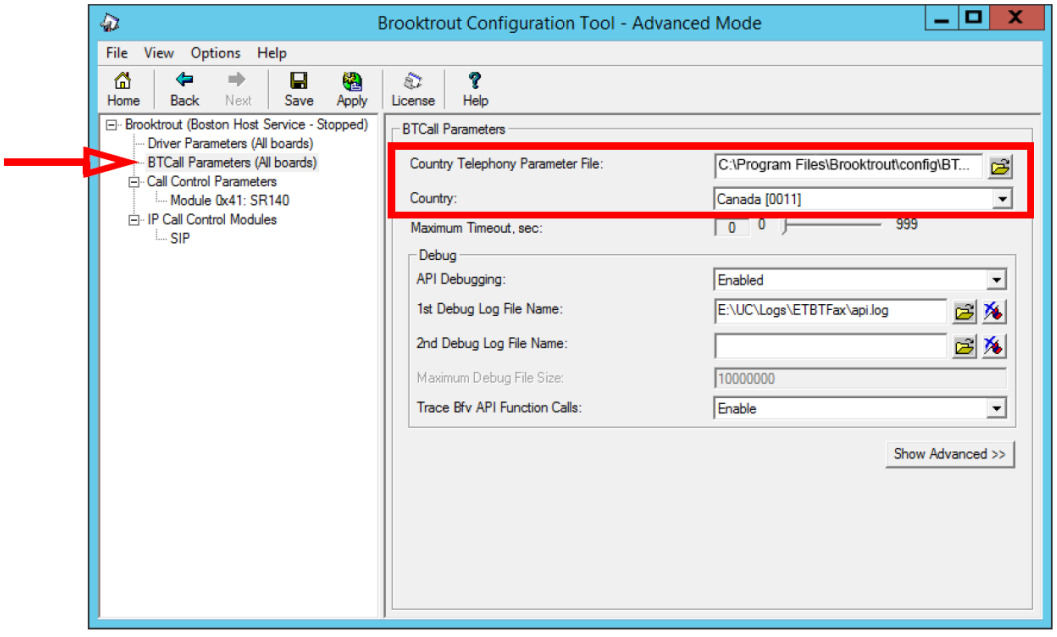


3. Select **BTCall Parameters (All boards)**.

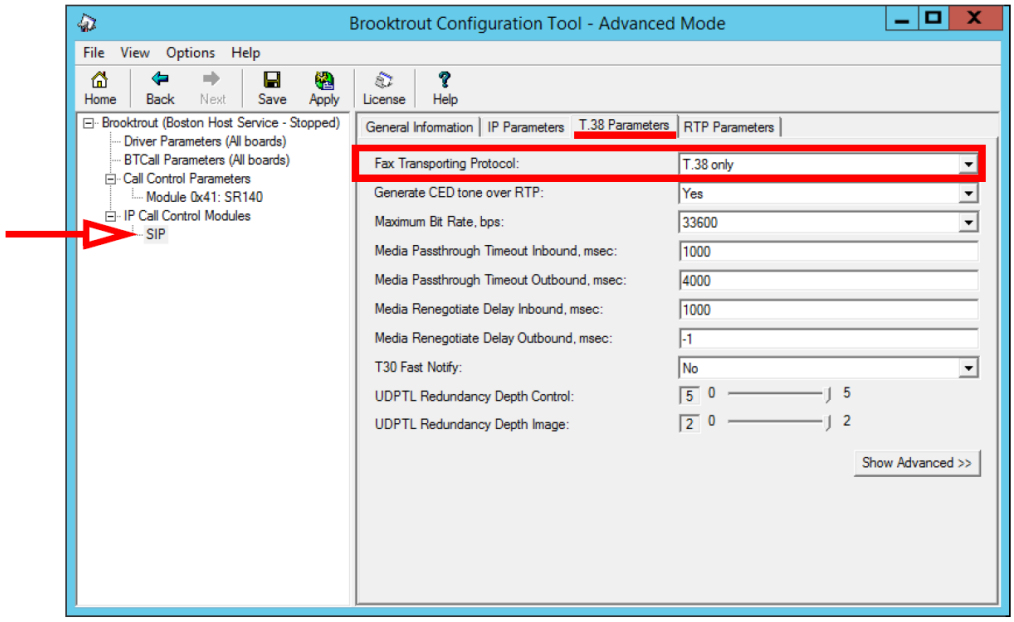
   Enter the path to the appropriate file in the space beside Country Telephony Parameter File. By default, this will be: **C:\Program Files\Brooktrout\config\BT_CPARM.cfg**

   Modify the path according to the location where your administrator has installed the program.

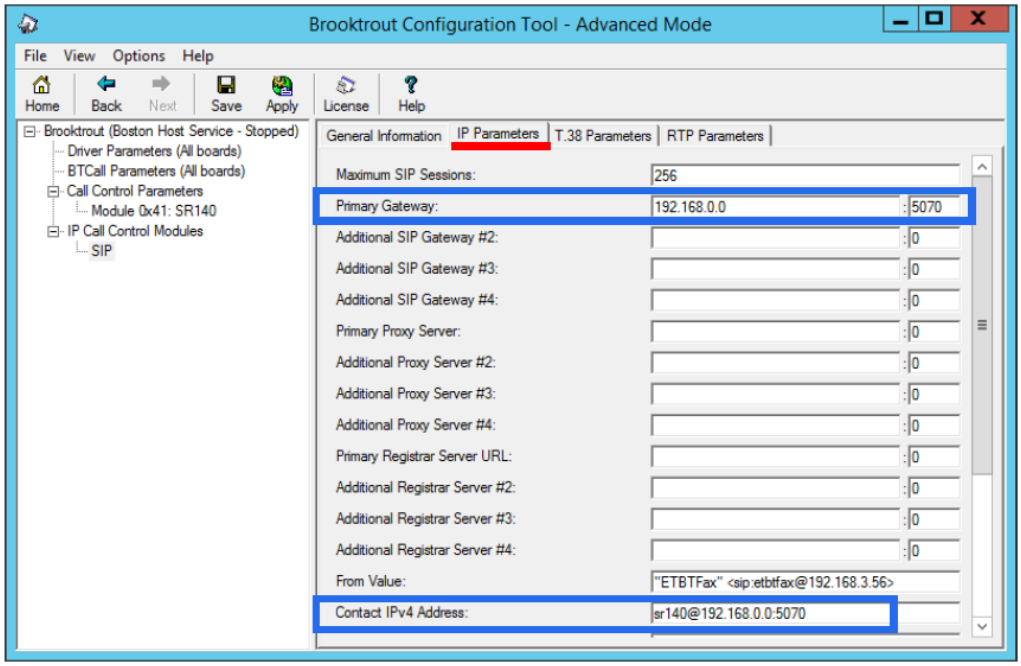
   Select your **Country** from the dropdown list.



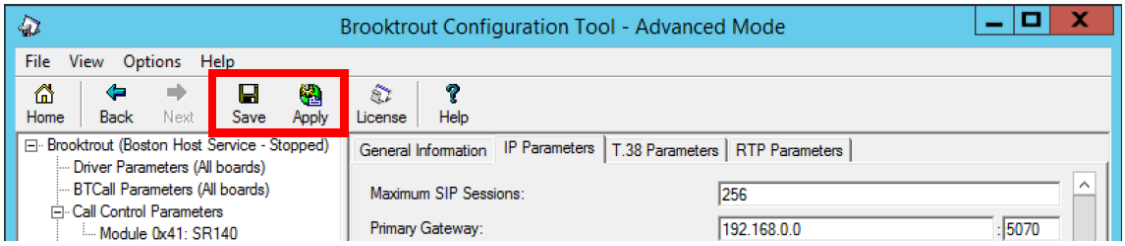
4. In the left-hand window, select **SIP** under **IP Call Control Modules**. Go to the T.38 Parameters tab. For Fax Transporting Protocol, the recommended value is T.38 only.



5. Move to the **IP Parameters** tab.
For Primary Gateway, enter the **IP address** and **port number** to be used for all outbound fax traffic.



6. For **Contact IPv4 Address**, enter **sr140@** followed by the **IP address** and **port** used for inbound faxing. This must be a different port than the one used for the Avaya Messaging voice server (5060).
7. Click **Save** to confirm the changes.
8. Click **Apply** to restart all affected services.

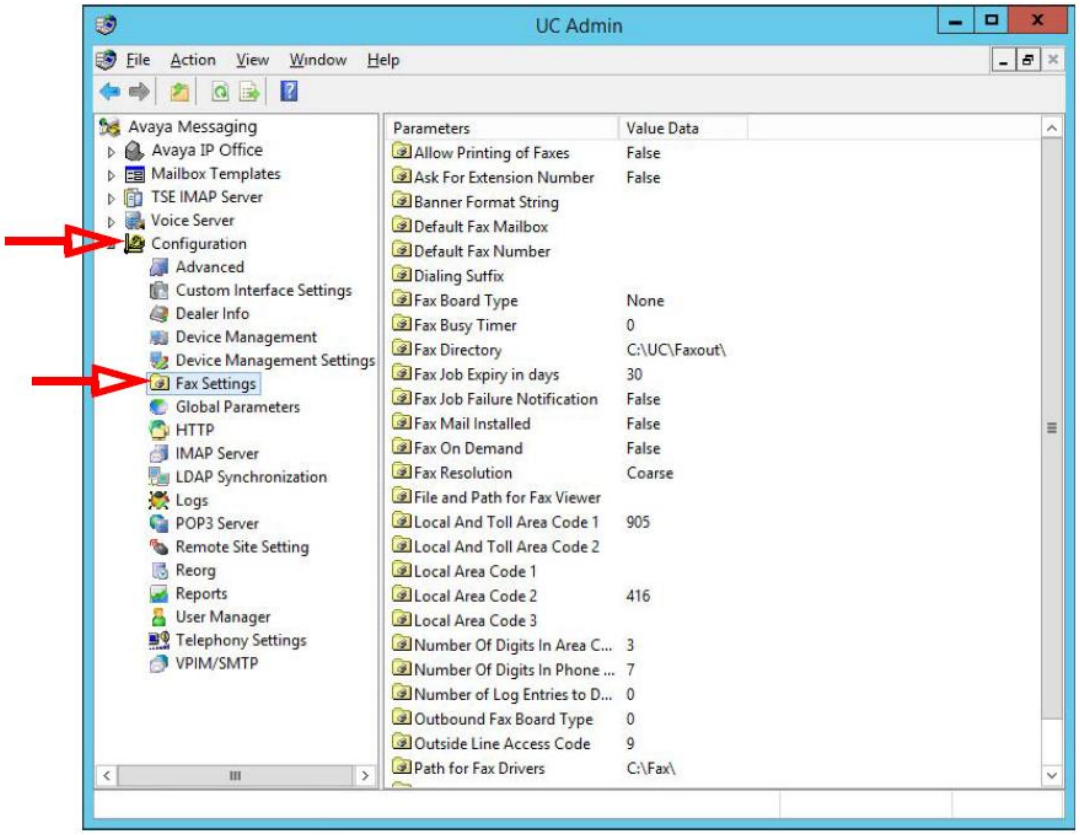


The configuration of the SR140 software is complete.

Avaya Messaging Configuration

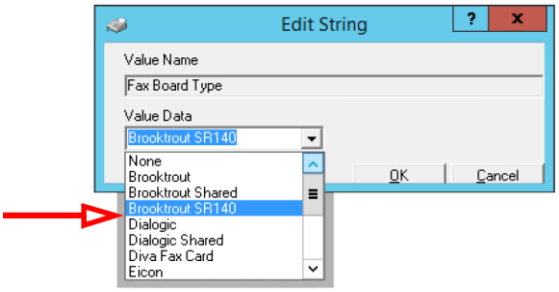
The voice server must be configured to send faxes to the SR140, and to prepare to receive them across the same channel. A setting for incoming, and another for outgoing faxes must be configured on the server using Avaya Messaging Admin.

1. Go to **Start > All Programs > Avaya Messaging > Avaya Messaging Admin** or click the Avaya Messaging Admin icon on the server desktop. Enter the username and password at the prompt.
2. Open **Configuration** and click on **Fax Settings**.

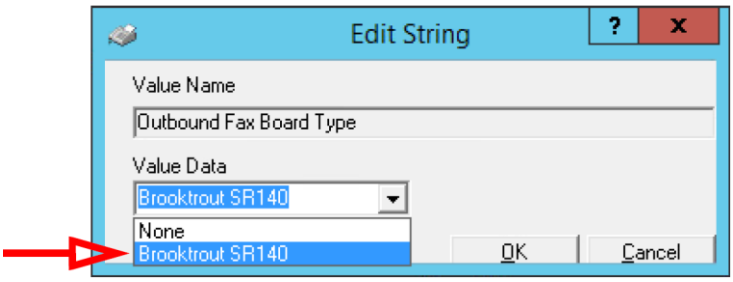


3. In the right-hand pane, locate the entry for **Fax Board Type**. Double-click to open its settings. From the dropdown menu, choose **Brooktrout SR140**.

   Click **OK**.

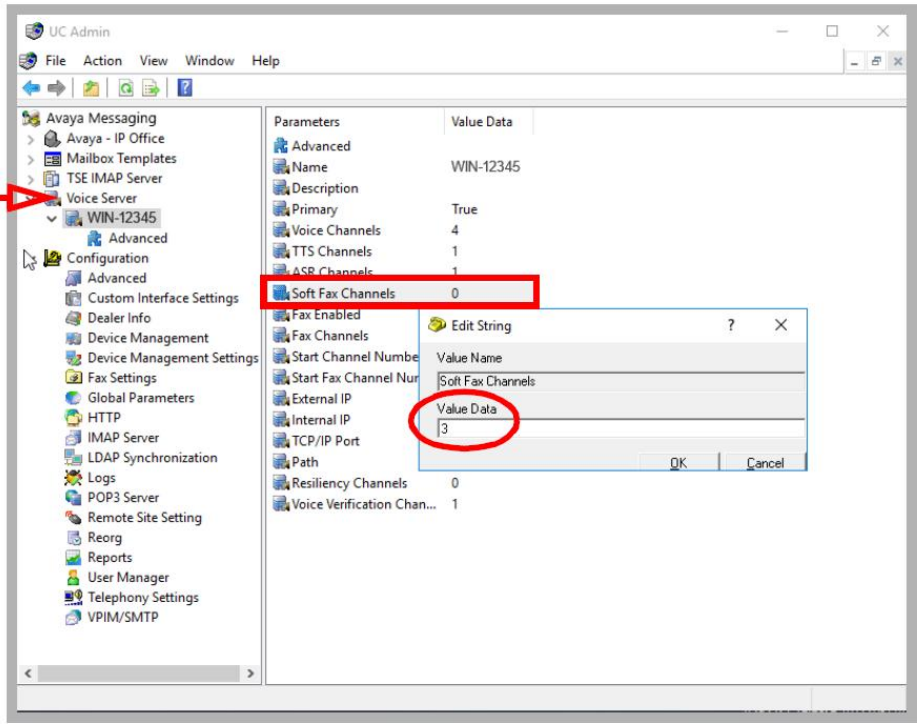


4. Double-click on **Outbound Fax Board Type**. Choose **Brooktrout SR140** from the dropdown menu. Click **OK**.

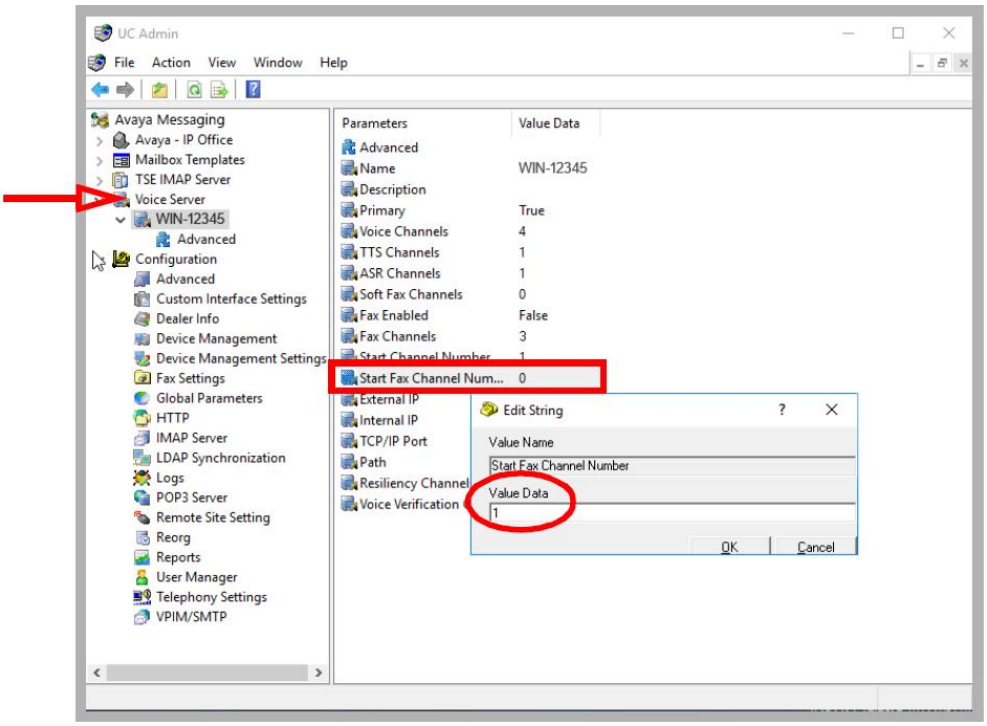


   Hint: If faxes are only **received** through the SR140 software, the Outbound Fax Board Type can be set to another value if required.

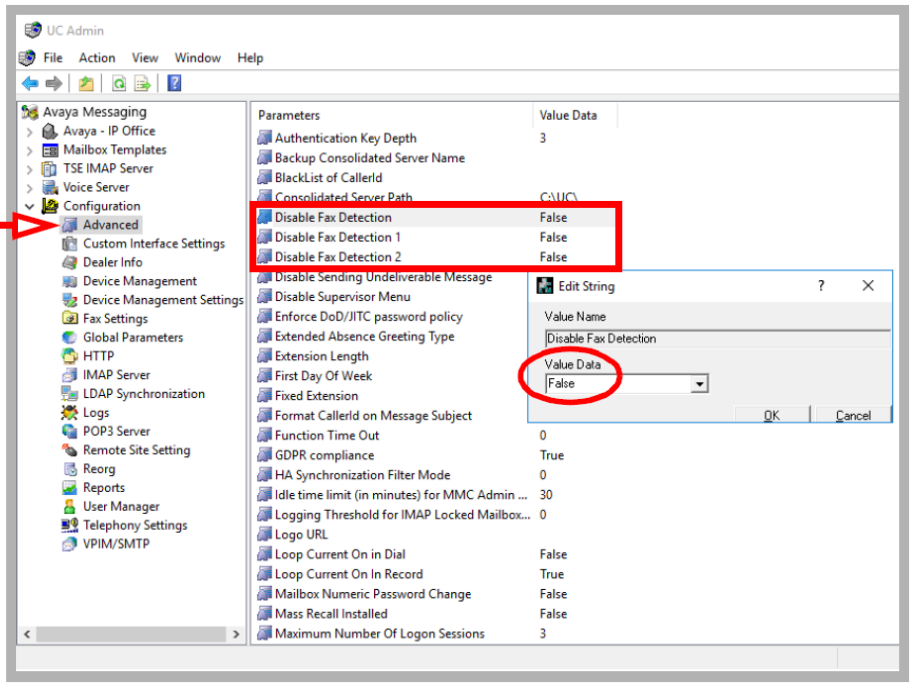
5. Under **Voice Server**, select your voice server. Double-click **Soft Fax Channels** and change its value data from **0** to the number of channels you have. Click **OK** when finished.



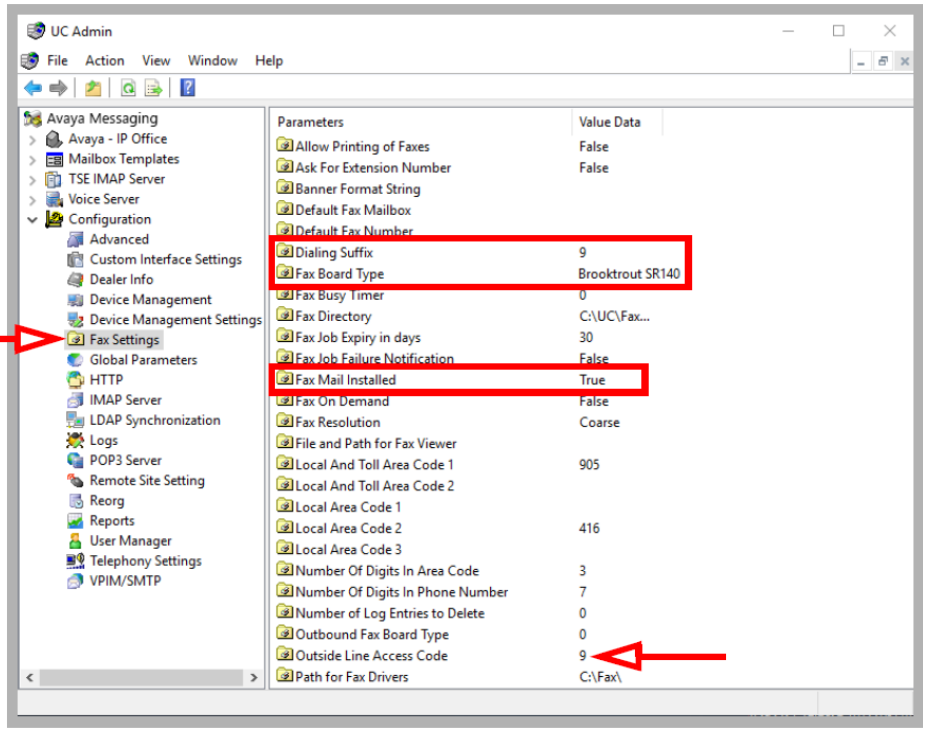
6. Double-click **Start Fax Channel Number** and change its value data to 1. Click **OK** when finished.



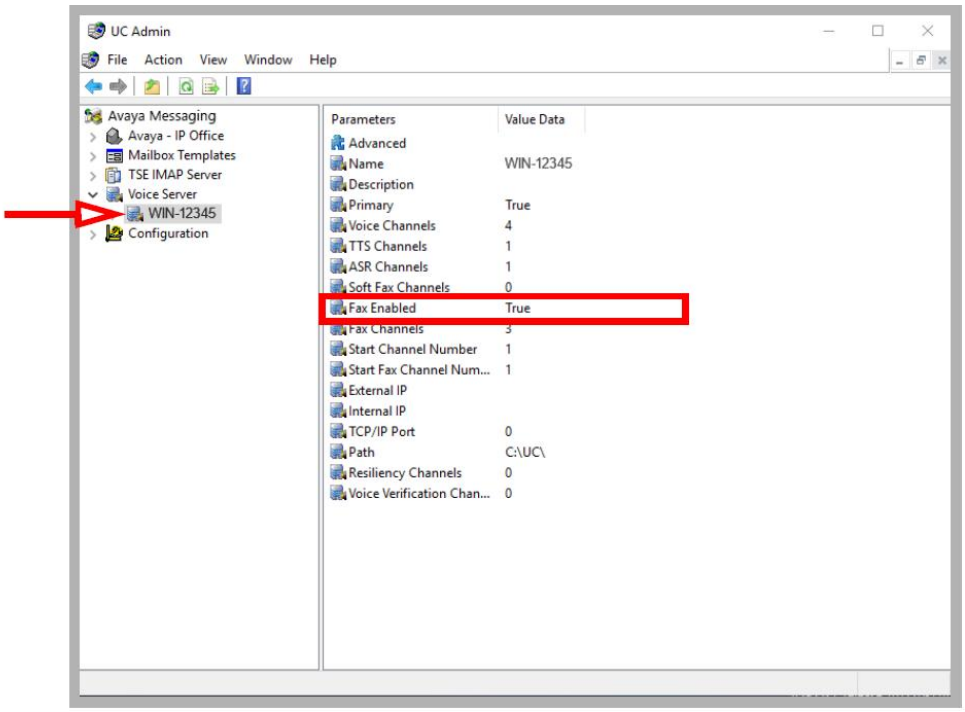
7. Open **Configuration > Advanced**. Set **Disable Fax Detection** to **False** for all entries shown.



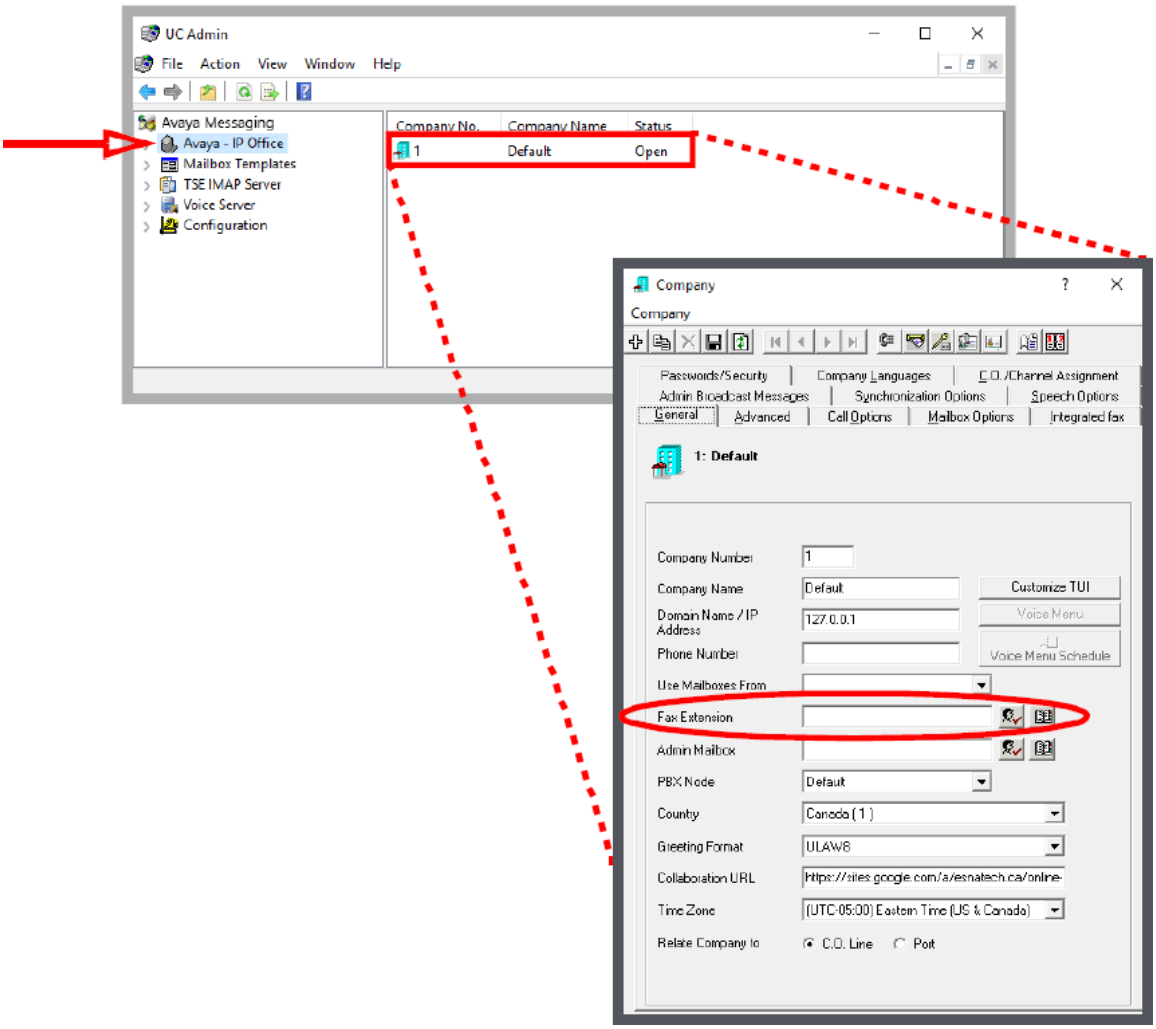
8. Go to **Configuration > Fax Settings**.
   Double-click **Dialing Suffix** and set the **Value Data** field match your **Outside Line Access Code**. Click **OK**. Double-click **Fax Board Type** and set the **Value Data** field to **Brooktrout SR140**. Click **OK**. Double-click **Fax Mail Installed** and set the **Value Data** field to **True**. Click **OK**.



9. Restart the voice server.
10. Once the server is online, open UC Admin and under **Voice Server**, verify that the **Fax Enabled** field is set to **True**.

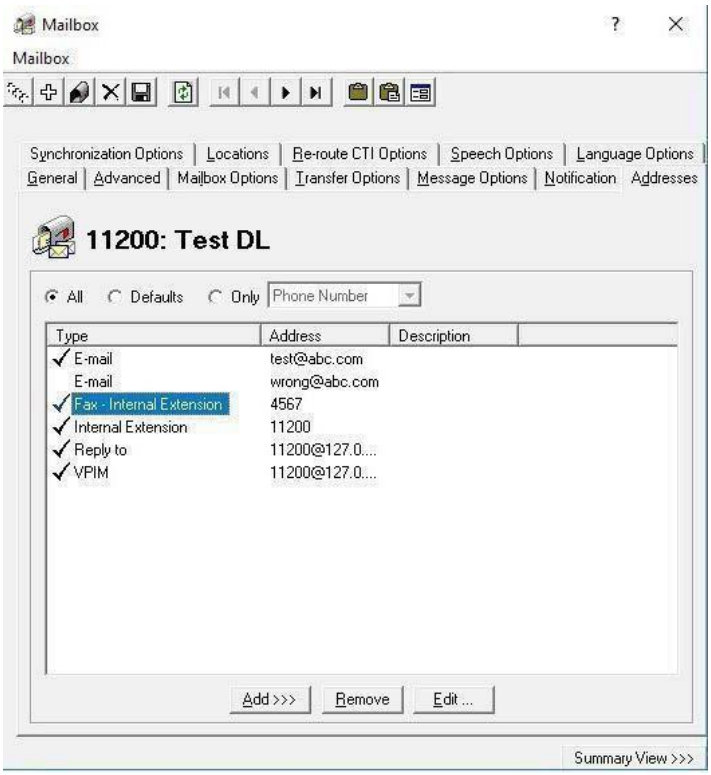

UC Admin
File Action View Window Help
Avaya Messaging
Avaya - IP Office
Mailbox Templates
TSE IMAP Server
Voice Server
WIN-12345
Configuration
Parameters
Value Data
Advanced
Name
WIN-12345
Description
Primary
True
Voice Channels
4
TTS Channels
1
ASR Channels
1
Soft Fax Channels
0
Fax Enabled
True
Fax Channels
3
Start Channel Number
1
Start Fax Channel Num...
1
External IP
Internal IP
TCP/IP Port
0
Path
C:\UC\
Resiliency Channels
0
Voice Verification Chan...
0

11. Set up one mailbox to be used as the default destination for incoming fax traffic. In UC Admin, double-click your company to open the properties window.
On the **General** tab, locate **Fax Extension** and specify which mailbox to send faxes into.
When ready, click **Save**.



12. Inbound faxes require routing calls through port 5070 to Avaya Messaging since Brooktrout listens on that port. This requires a DID for each mailbox configured for fax. Add the fax DID number in the **Addresses** tab of the mailbox. This can be an internal number for the fax DID.

    For example, for DID 705 213 4567, add the fax extension 4567 which can be dialed from outside and will be routed through port 5070 and will be received into that mailbox. If not properly configured, the fax will be sent to the default system mailbox.



Monitoring Channel Activity

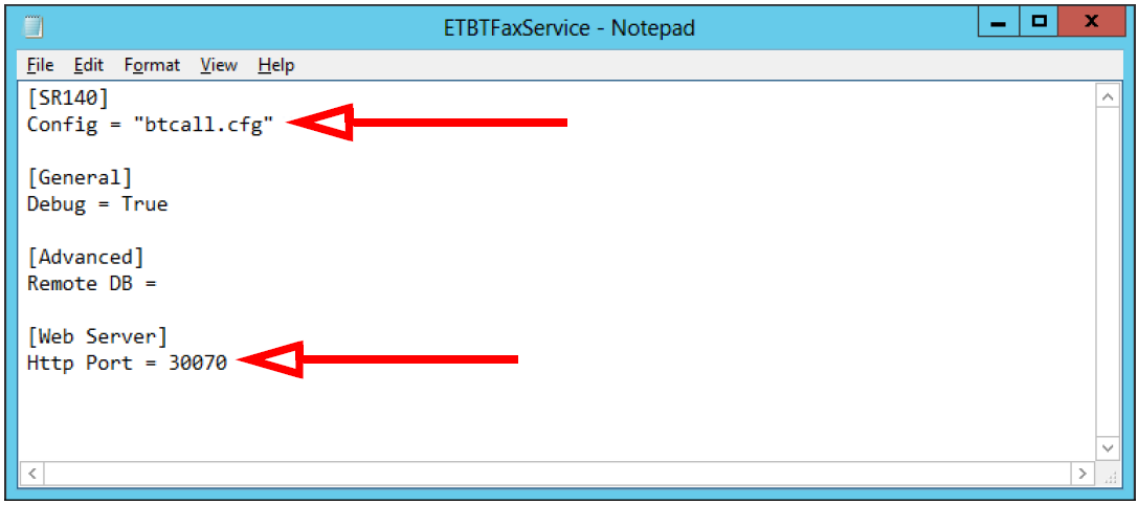
Setup

To monitor the traffic through the fax software, the configuration file on the Avaya Messaging Voice Server must be setup to point to the correct file locations.

1. On the computer where Avaya Messaging is installed, use a text editor (i.e., Windows Notepad) to open the configuration file. By default, this will be:

   C:\UC\ETBTFax\Config\ETBTFaxService.ini

   Modify the path according to the location where your administrator has installed the program.



2. Modify the Config entry to include the full path to the btcall.cfg file. By default, this will be:

   "C:\Program Files\Brooktrout\config\btcall.cfg".

   Be sure to enclose the path within double quotation marks " ".
   Modify the path according to the location where your administrator has installed the program.
   Enter the **HTTP Port** number that will be used to monitor fax channel activity.

3. When all changes have been made, click **File > Save**

Monitoring via Browser

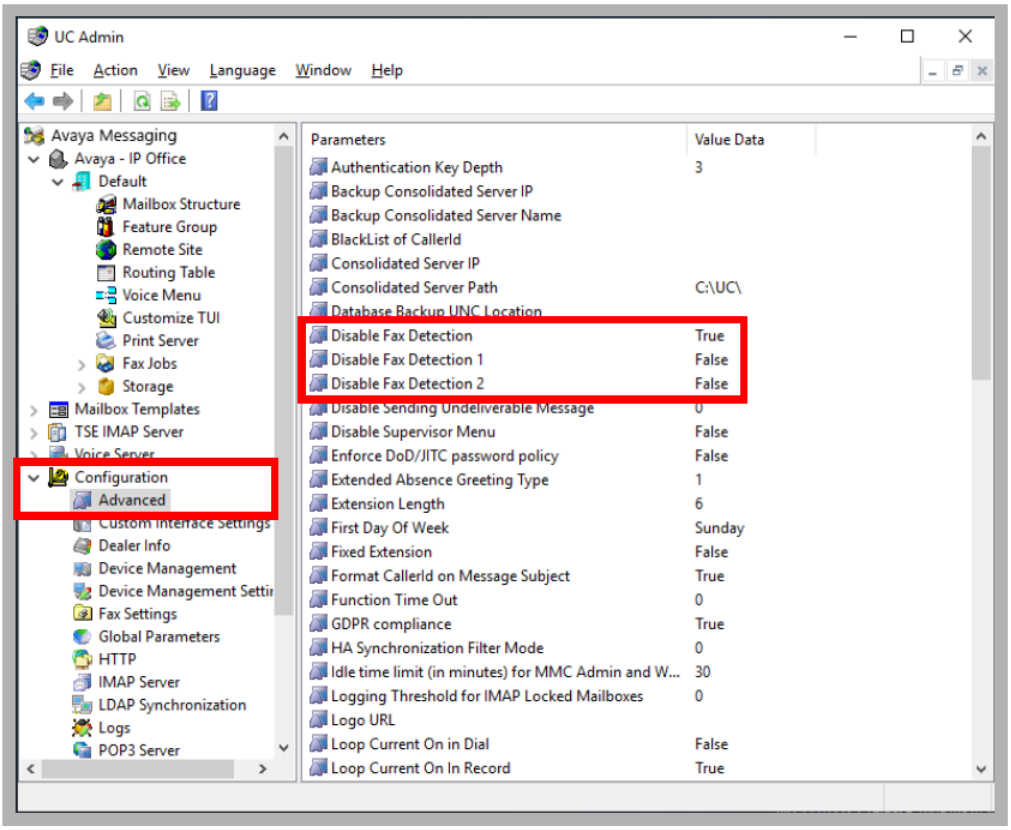
To monitor activity on a fax server, open a browser and navigate to: **http:\\localhost:30070**
Change **localhost** to the IP address of the fax server if you want to monitor from a different computer.
Change the **port number** (30070 in this example) to the value entered in step 2 above.

Fax Detect and Deflect

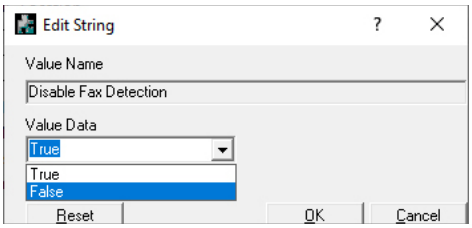
If an SR 140 is installed and configured on your system, a single telephone number can be setup to receive both voice and fax telephone calls.
During the auto attendant playback, and during the personal message playback, the system monitors the call for the presence of a fax signal.
If no signal is detected, it is handled as a standard voice call.
If a fax carrier signal is detected, the call is routed to the fax number configured in the recipient's mailbox.

Configuring Avaya Messaging

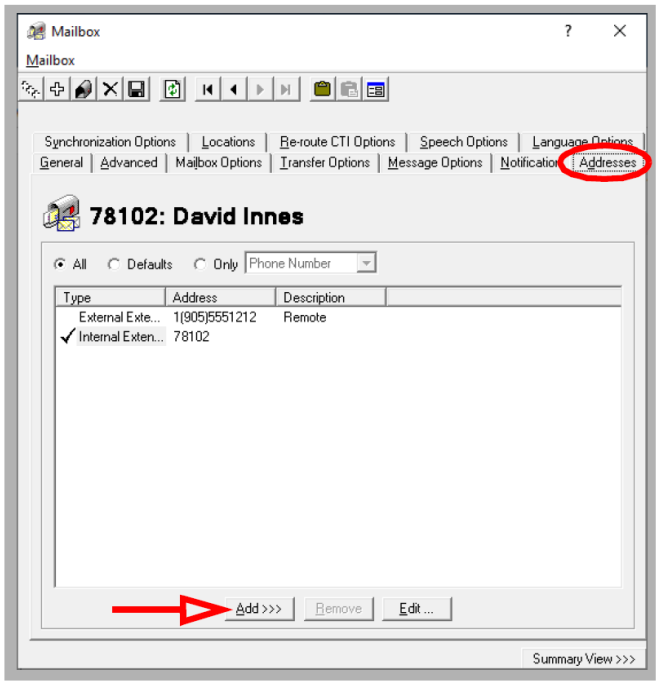
1. Open UC Admin and login.
2. Go to **Configuration > Advanced**.



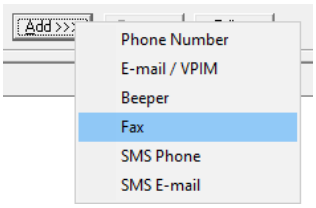
3. In the right-hand panel, double-click **Disable Fax Detection** and set the value to **False**. Click **OK**.
4. Repeat for **Disable Fax Detection 1** and **Disable Fax Detection 2**.



5. Open a user mailbox and go to the **Addresses** tab.

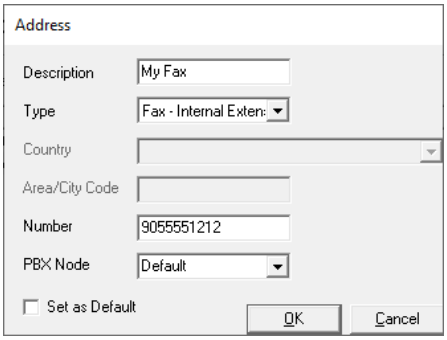


6. Click **Add** and select **Fax** from the list of options.

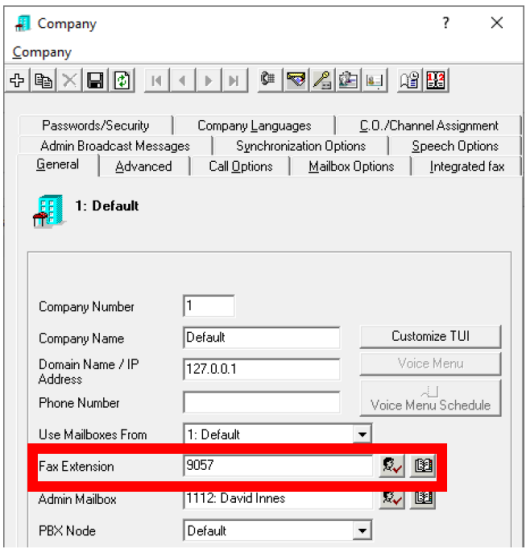


7. Provide a human readable description for the fax connection.
   Type: Select one of the following options from the dropdown list.
   Fax - External Extension: Enter the Country, the Area/City Code, and the fax number that will receive fax calls.
   Fax - Internal Extension: Enter the internal company extension (6 digit maximum) that will receive fax calls.
   Select the **Node** if more than one are present. When ready, click **OK**.

8. Click **Save** to complete the configuration.



Note: If no fax number is configured for the mailbox, the fax is routed to the extension specified under **Company > General > Fax Extension**.



Single DID for Fax and Voice

It is possible to use a single DID number for both voice and inbound fax traffic. While the voice mailbox greeting is being played, the system continues to listen for a fax signal. If one is detected, the system stops playing the greeting and begins the handshaking procedure necessary to receive the fax.

A greeting must be a minimum of 6 seconds long to allow enough time for the detection of the fax tone. This section covers the process to setup a single DID number to handle both voice and inbound fax traffic. Avaya Aura Session Manager is required for this installation. ASM must be setup and running before proceeding further.

Overview

To use a single DID number for voice and fax, add to your existing voice messaging integration via the Avaya Aura Session Manager. Refer to the existing *Aura Session Manager – Avaya Messaging configuration guide* for complete details.
In this example, the voice messaging service number has been configured as 78000. Aura extensions are already configured to use 78000 for voice messaging.

This configuration shows one Aura extension / mailbox user (71802) with voice messaging coverage to 78000. With voice messaging working, enables single number faxing for this user. Refer to the previous sections for the installing and configuring the SR140 fax service on Avaya Messaging.

We will configure the unique prefix 52 for the SR140 service on the Avaya Messaging server and then assign a unique fax internal extension number (52002) to the mailbox user. The Communication Manager must be configured to use prefix 52 to take the SIP route to Session Manager. Fax internal extensions are configured through Avaya Messaging Admin only so that the fax service can deliver the message to the correct mailbox. These extensions do not need to be configured on CM.

Session Manager Configuration

This section covers configuring the Avaya Messaging server SR140 as a SIP entity of Session Manager. We will assign port **5070** as a SIP route prefix for the SR140 SIP entity. In this example, prefix **52** (length = 5) is used.

Avaya Messaging Configuration

Here we use the Avaya Messaging Admin to give each user a unique fax internal extension starting with **52**. In this example, the user's primary extension is **78102**, and their fax internal extension is **52002**.

Communication Manager Configuration

Using Communication Manager, configure prefix **52** to take the SIP route to Session Manager. The same SIP route can be employed for both voice and fax messaging.
Additional user mailboxes, such as 78103 and 78104, will have fax internal extensions configured as 52003, 52004, etc.

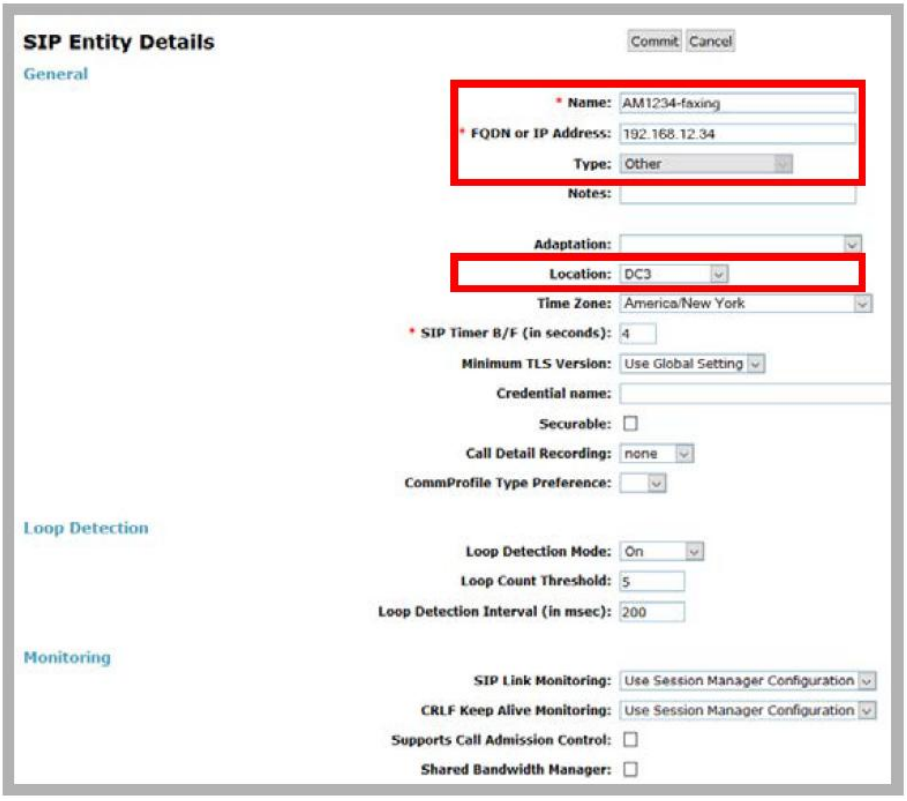
A Sample Use Case

An incoming fax is routed to extension 78102 and the user doesn't answer the call and it goes to voicemail. The Caller hits the Send button on the fax machine as soon as call is answered. The Avaya Messaging server detects the fax tone and initiates a call transfer (SIP REFER) to user 78102's internal fax extension (52002) via Session Manager.
Session Manager routes the call to CM, and CM routes it back to SM based on prefix 52 and then onto the Avaya Messaging SR140 service. The SIP call transfer is completed. The SR140 connects to the call, processes the fax job and deposits the fax image into mailbox 78102 (based on fax internal extension 52002).

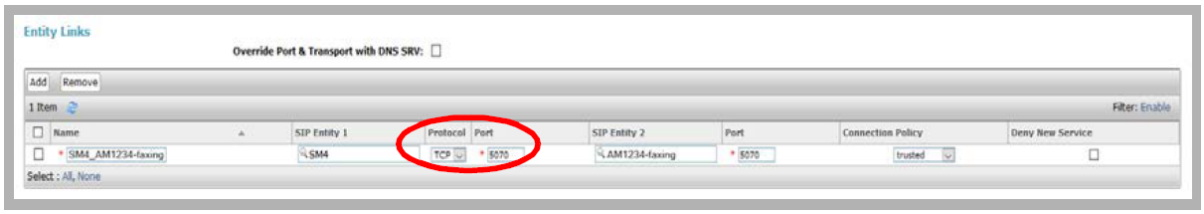
Configuring Session Manager

1. **Add SR140 as SIP Entity**

Login to the Session Manager Web UI and open **Element > Routing > SIP Entities > Add new SIP entity**. Configure the following items.



Name: Enter the Messaging server name.
FQDN or IP Address: Type the **IP Address** or the **Fully Qualified Domain Name** of the Messaging server. When using FQDN, make sure that Session Manager resolves to the correct IP address.
Type: Choose **Other** from the list.
Location: Select your location from the dropdown list.
Entity Links: Use port **5070** and the **TCP** protocol to route to the Avaya Messaging server SR140 faxboard.



Note: This entity must be different from the entity used for Avaya Messaging's voice calling.

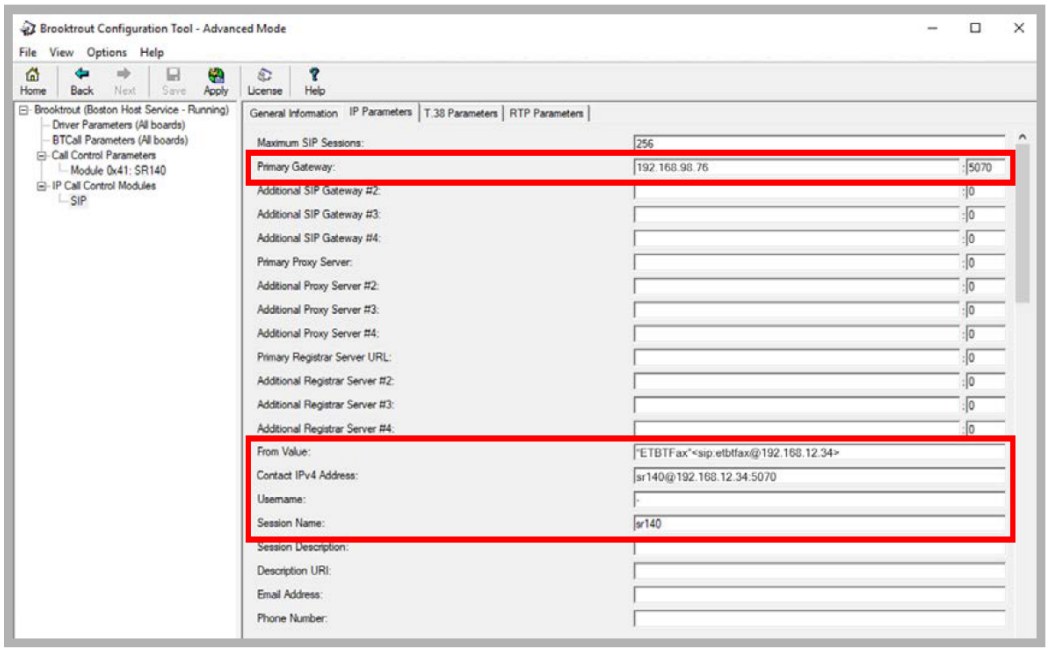
2. Check Connection between SM and AM SR140

The Dialogic / Brooktrout SR140 configuration on the Avaya Messaging server must be configured before proceeding. Refer to the previous sections of this chapter for details.
Open the Session Manager UI and go to **Element > Session manager > System status > SIP Entity** monitoring. Verify that the connection is **UP**.



Hint: If the connection fails, check that the **Dialogic / Brooktrout** configuration is correct, then restart the **Dialogic Corporation Boston Host service** on the Avaya Messaging server.

This is the Brooktrout configuration tool for Session Manager (SIP Asset IP address 192.168.98.76) and the Avaya Messaging server (192.168.12.34) connection.

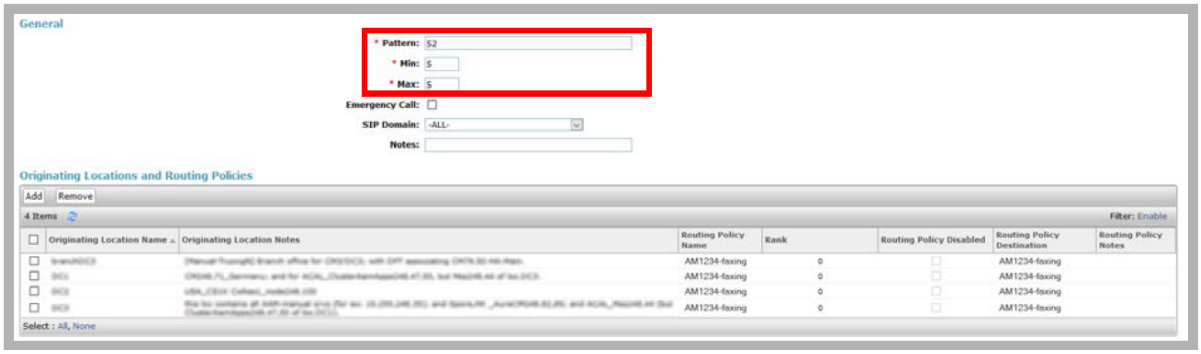


Primary Gateway: Enter the IP address of the **Session Manager** server. Use Port 5070. From Value: Input the string “ETBTFax”<sip:etbtfax@192.168.12.34>.
Contact IPv4 Address: Enter **sr140@** followed by the IP address and port (5070) used for inbound faxing. For example: sr140@192.168.12.34:5070.
Username: Place a dash - in this field.
Session Name: Type sr140 here.

Click **Save** to confirm the changes. Click **Apply** and restart the **Dialogic Corporation Boston Host service**. The configuration of the SR140 software is complete.

3. **Dial Pattern**

Add a new dial pattern for fax calling.



Add a value for **Pattern** ID that has not been previously used by SMGR. In this example, **52** is used. Enter the minimum and maximum lengths.
Originating Location and Routing Policies: Add the SR 140 fax messaging server entity for routing Policies.

Avaya Messaging Server Configuration

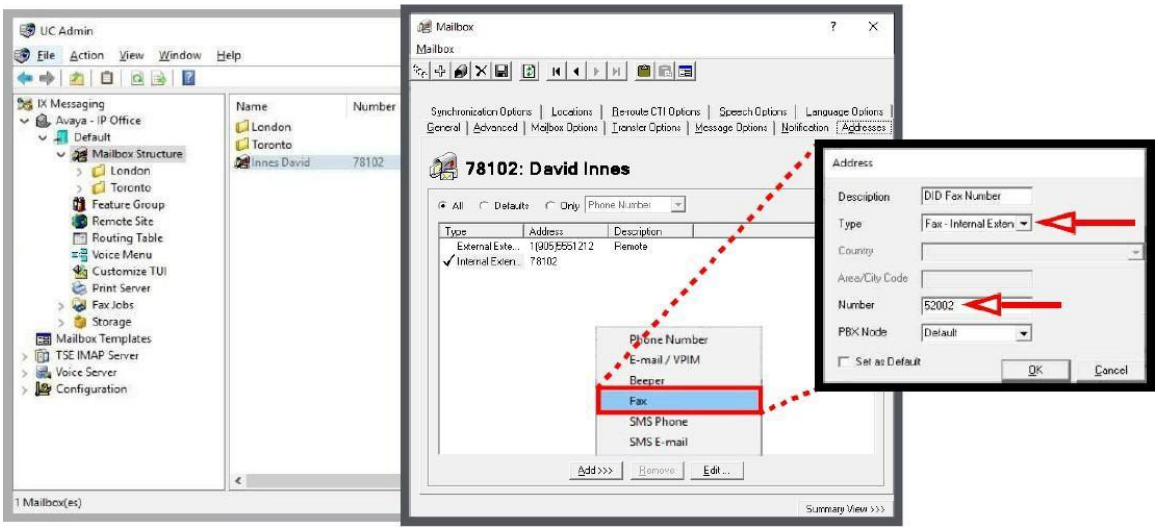
Create a Mailbox for the Fax Extension

Launch Avaya Messaging Admin and open the user's mailbox at the **Addresses** tab.

Click **Add** and select **Fax**.
Enter a Description to identify this address.

For **Type**, choose Fax-Internal extension and enter the fax extension Number. This number must be different than the mailbox extension and must begin with the prefix associated with the SR140 SIP entity.

In this example, prefix 52 was configured, the mailbox user's primary extension is 78102, and the fax internal extension is 52002.

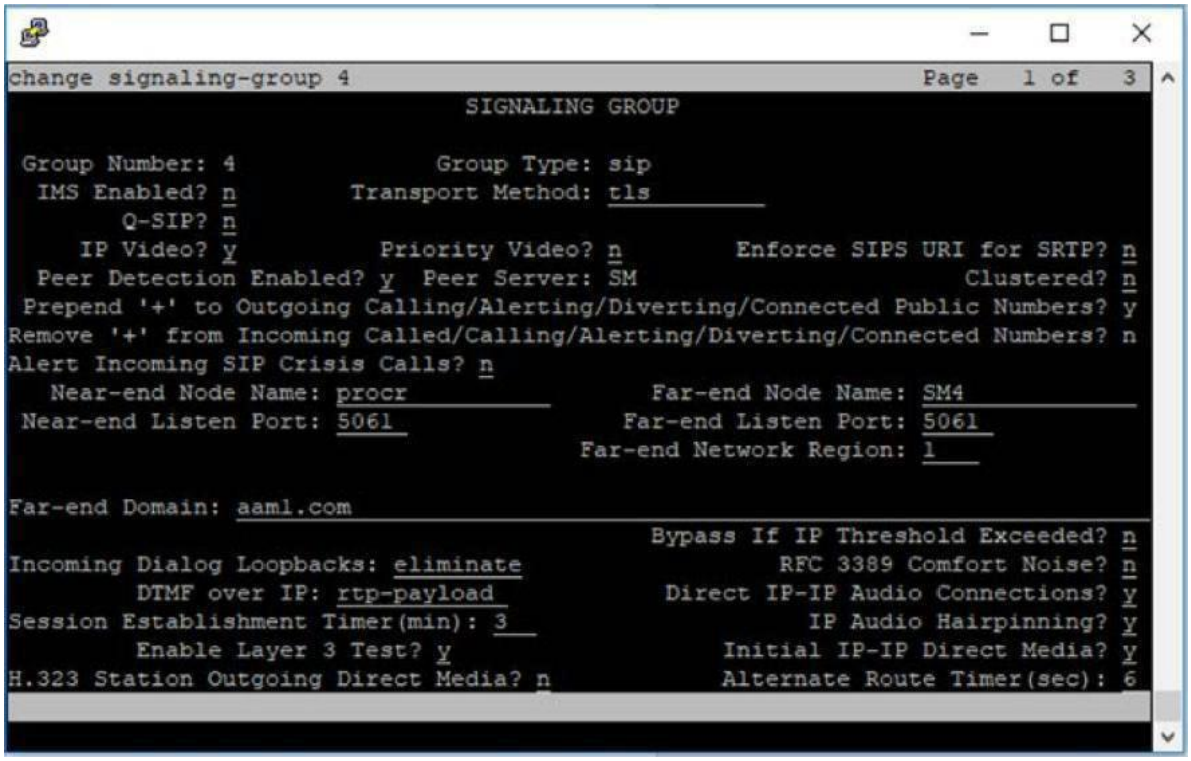


Note: The Fax number must begin with the prefix created in the **Dial Pattern**.
Note: Each mailbox must have a unique fax extension. In this example, mailboxes 78103 and 78104 have the fax internal extension numbers 52003 and 52004, respectively.

Communication Manager Configuration

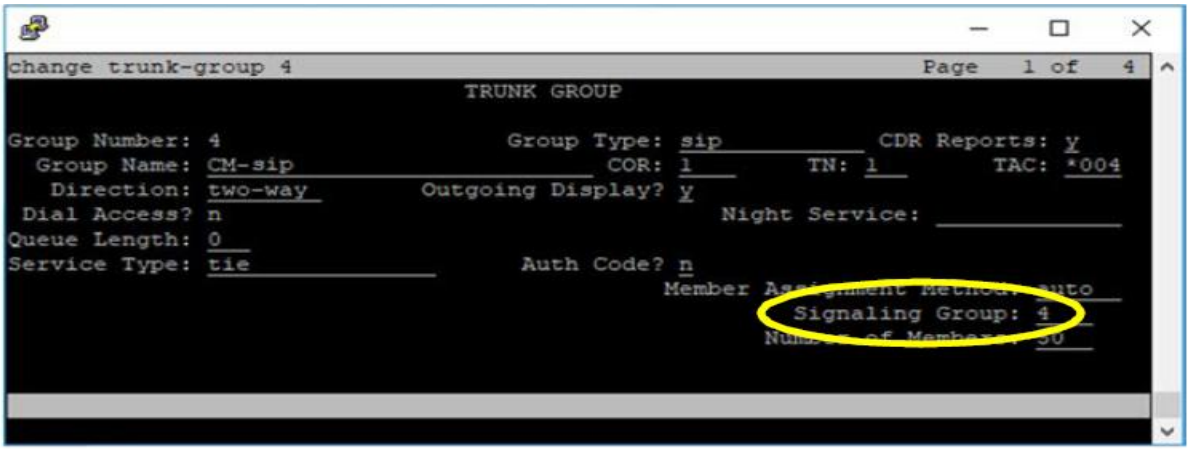
1. Create Signaling Group

Using CM administrator, enter the command: **add signaling-group <number>.**
Replace **<number>** with the value that will identify this group. It must be a unique number not used by any other group.
For example, **add signaling-group 4**.



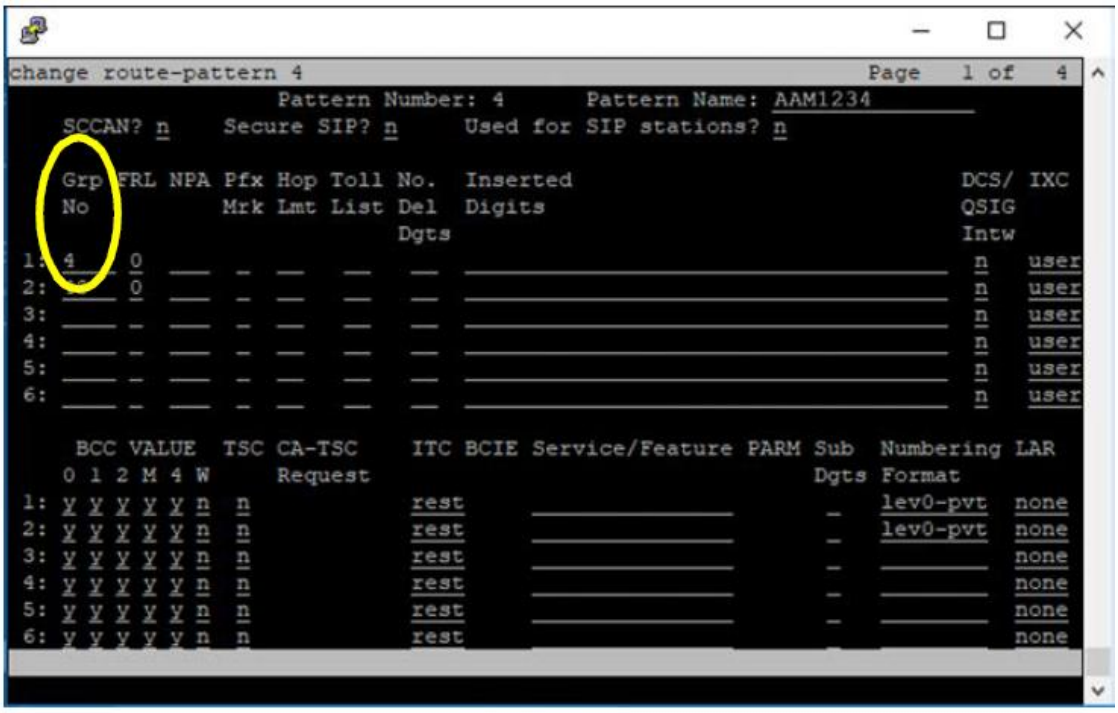
2. Configure Trunk Group

Using CM administrator, enter the command: add trunk-group **<number>**. Replace <number> with the value that will identify this group.
Signaling Group: Enter the value for signaling group created above.



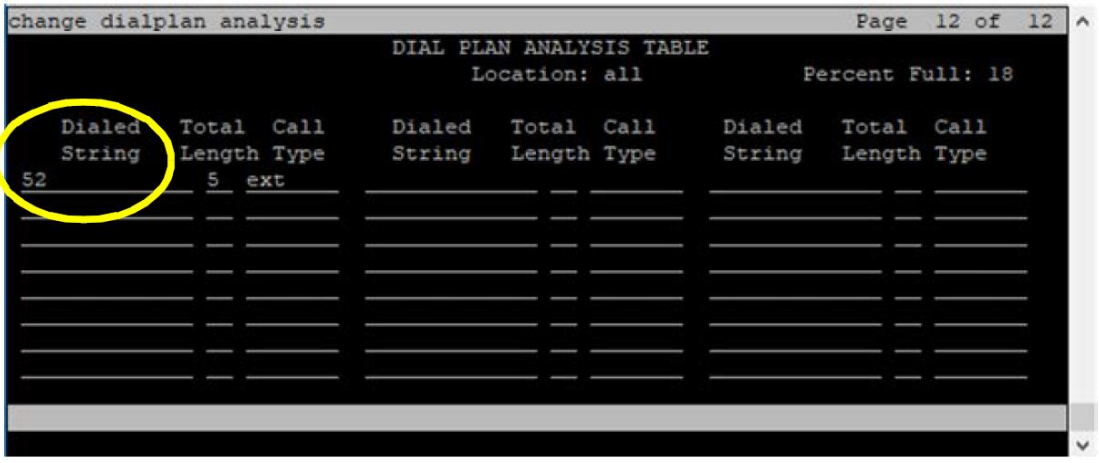
3. Define Route Pattern

Using CM administrator, enter the command: **change route-pattern <number>**. Replace **<number>** with the value that will identify this pattern.
Grp No: Enter the trunk-group number created above.



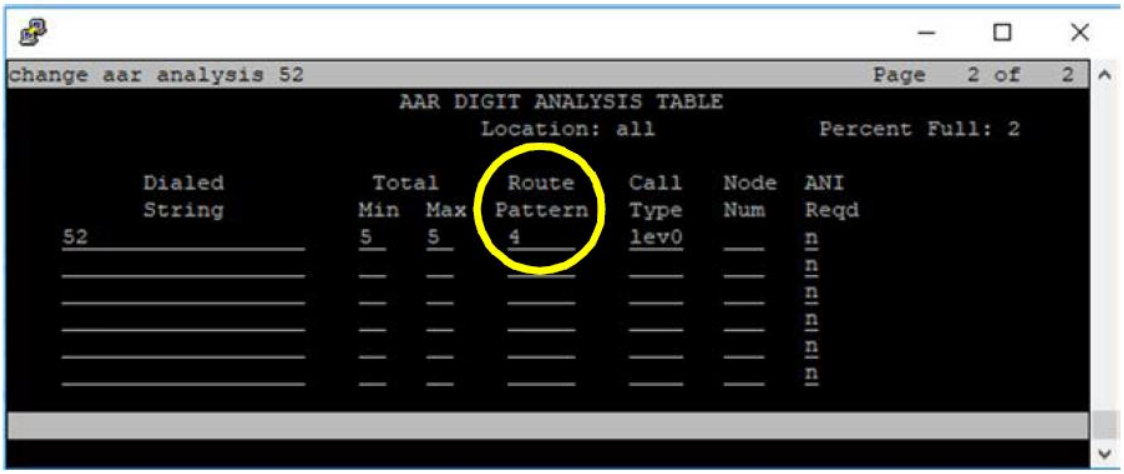
4. Add the Fax Prefix to the Dial Plan

Using CM administrator, enter the command: **change dialplan analysis**.
Dialed String: Add the prefix configured in SMGR for fax extensions.



5. Change aar Analysis

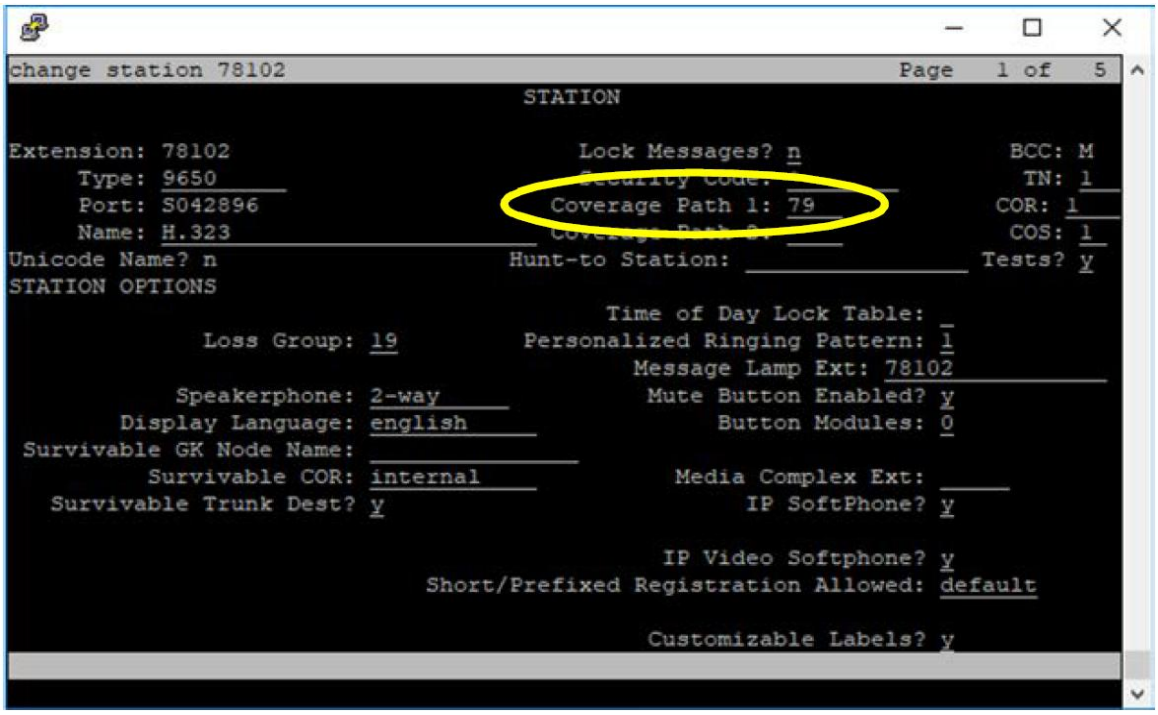
Using CM administrator, enter the command: **change aar analysis**.
Route Pattern: Use the same route pattern number configured for the Avaya Messaging server voice call that routes to SM. In this example, route pattern **4** is used for both the fax number and the call pilot number.



6. Extension for Mailbox Number

Using CM administrator, enter the command: **change station <mailbox number on messaging server>**. Replace **<mailbox number on messaging server>** with the user's voice extension (78102).

Coverage Path 1: Set the coverage path that uses the hunt group configured for the voice mail number.



The configuration is complete.

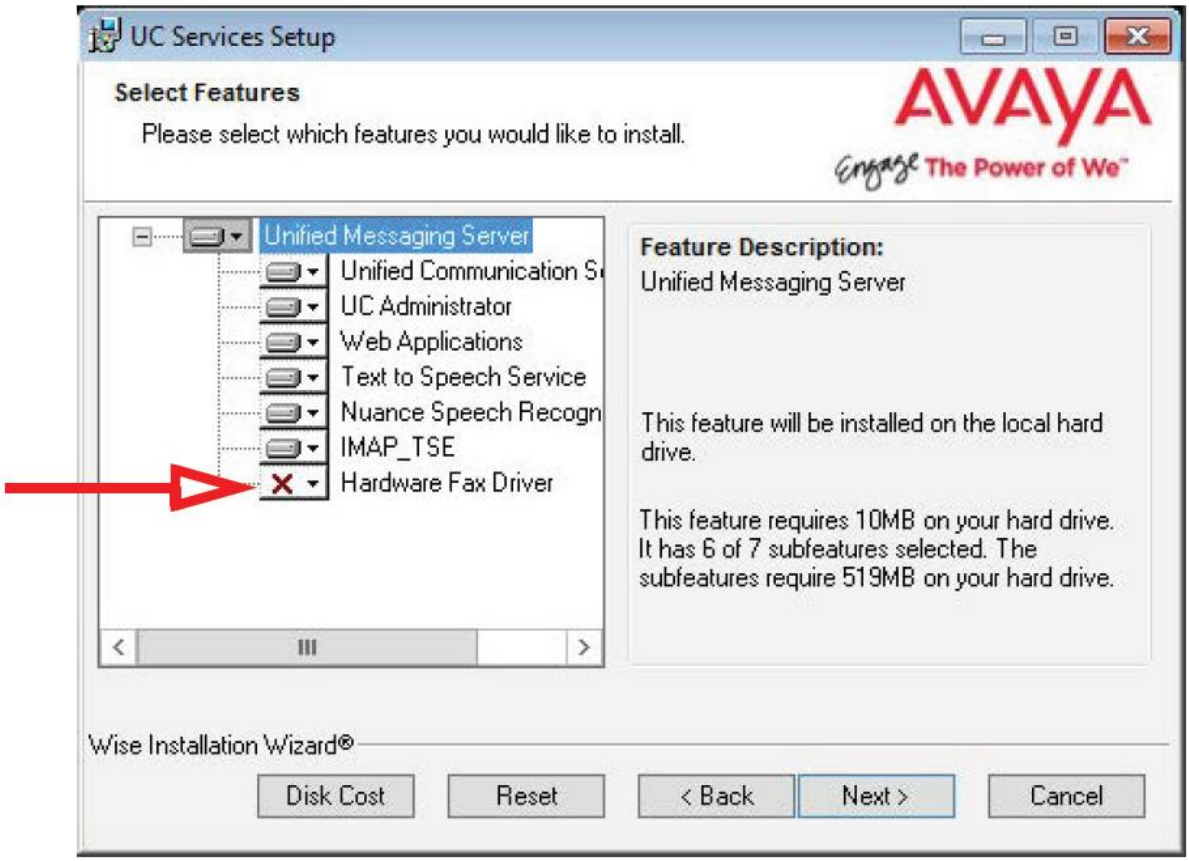
Chapter 18: DIALOGIC SR140 SECURE FAX

Introduction

Avaya Messaging can be set up to securely send and receive faxes through the Dialogic SR140 fax software. The transmissions use Transport Layer Security (TLS) to encode the data. This method complies with JITC requirements for secure communications.
Sites receiving secure faxes must also be set up to use the TLS protocol. Incoming faxes must also be secured using TLS protocols.

Pre-requisites

Install the Avaya Messaging program onto the computer that will act as the **Voice Server**. Ensure that the **Hardware Fax Driver** option is enabled at the **Features Selection** screen during program installation. This will ensure that the necessary program elements are included with Avaya Messaging.



For High Availability (HA) installations, the SR140 can be installed on the Primary or any of the Secondary servers.

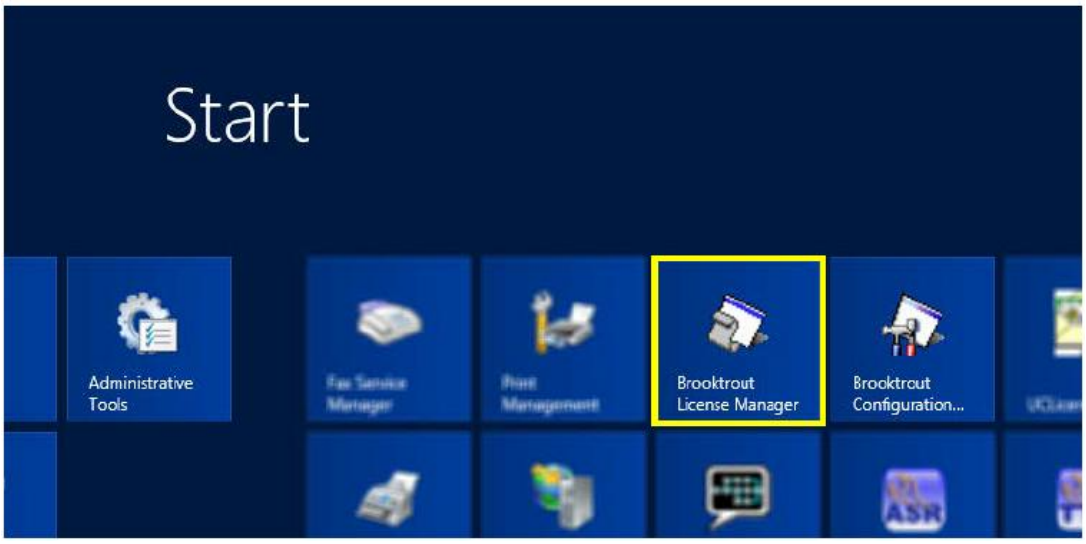
Important: Secure Fax using the SR140 fax software requires 2 licenses from Dialogic; the standard fax license, and a secure fax license.

Configuration

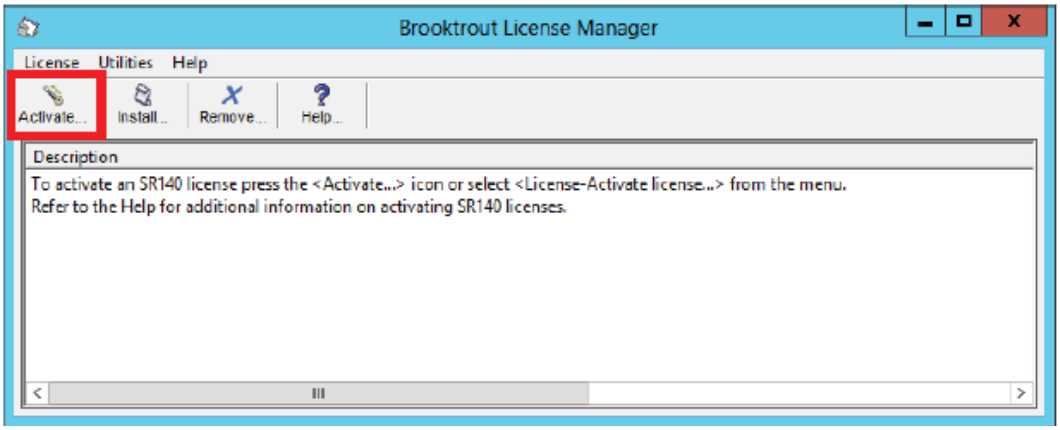
Once the Dialogic SR140 and the Avaya Messaging voice server are both operating, the fax software must be configured to communicate with the UC platform.

License Manager

1. Open the **Brooktrout License Manager** program.

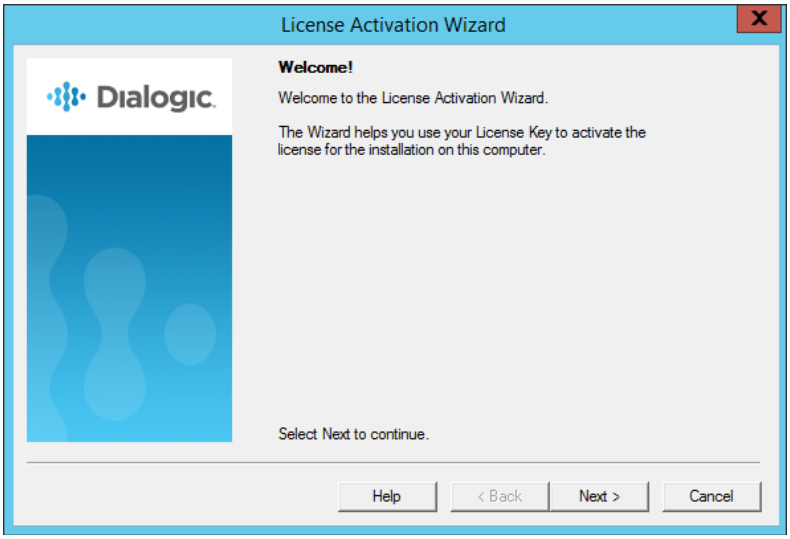


2. Enable the SR140 license by clicking the **Activate** button.

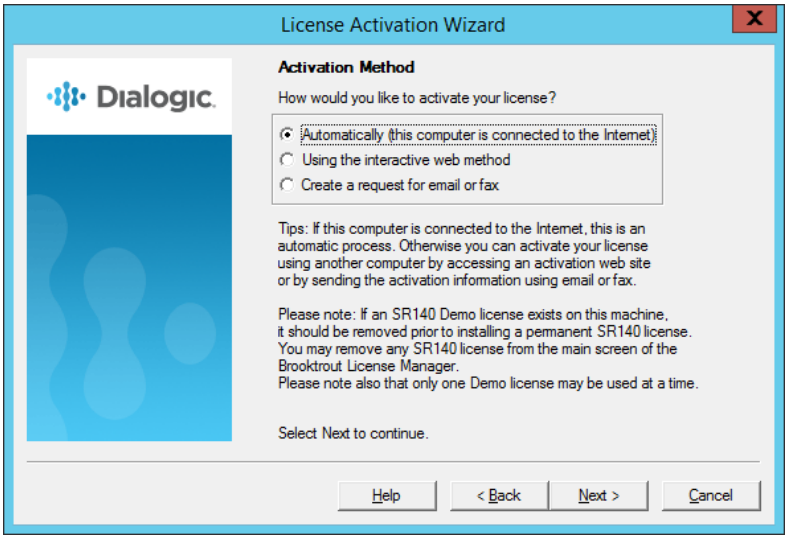


Note: The procedure shown here uses the **Activation Wizard** and an Internet connection.
If you have a license file, select **Install** and point the program to the file provided by your vendor.

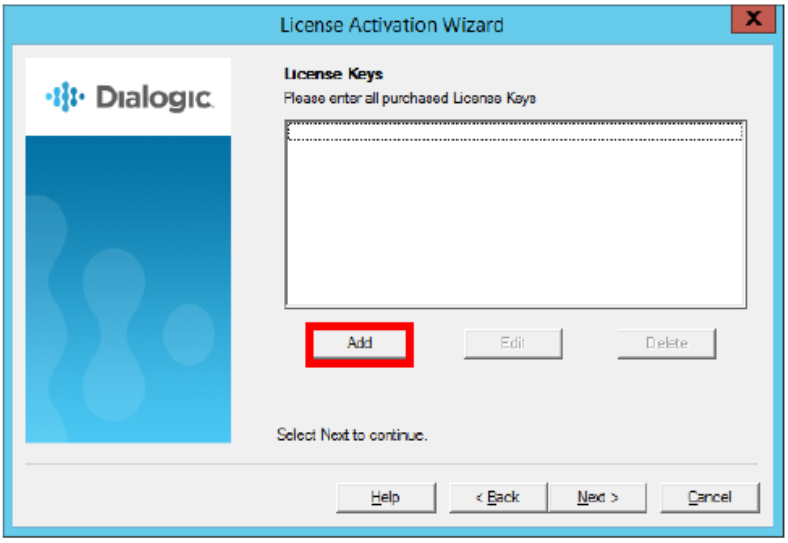
3. Click **Next**.



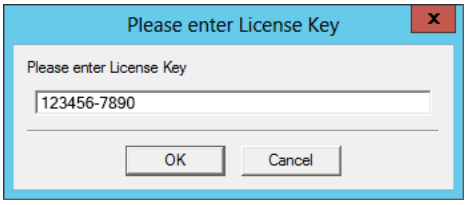
4. Enable **Automatically**... as the **Activation Method**, then click **Next**.



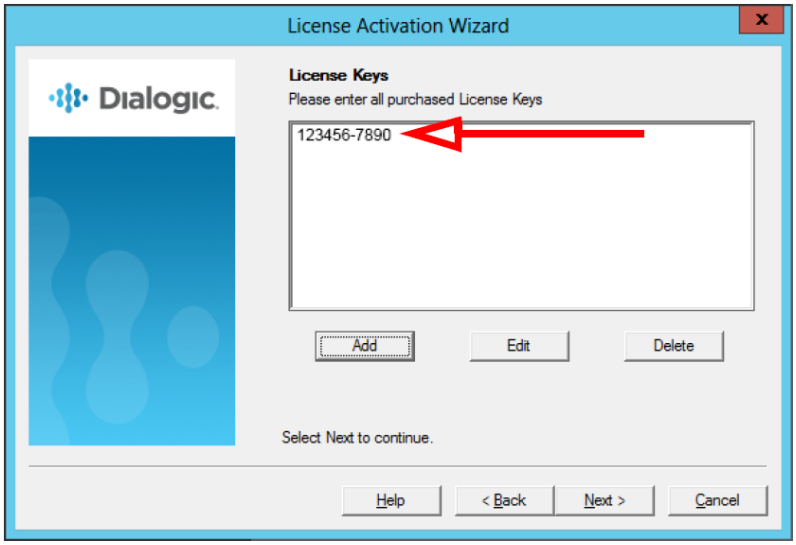
5. Currently, no **License Keys** are installed. Click **Add**.



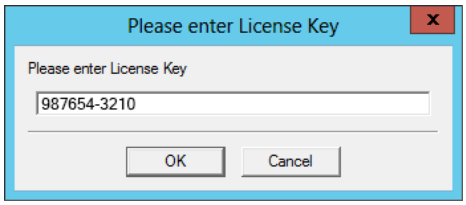
6. Enter the SR140 **standard** license key number that came with the fax software package. Click **OK** when ready.



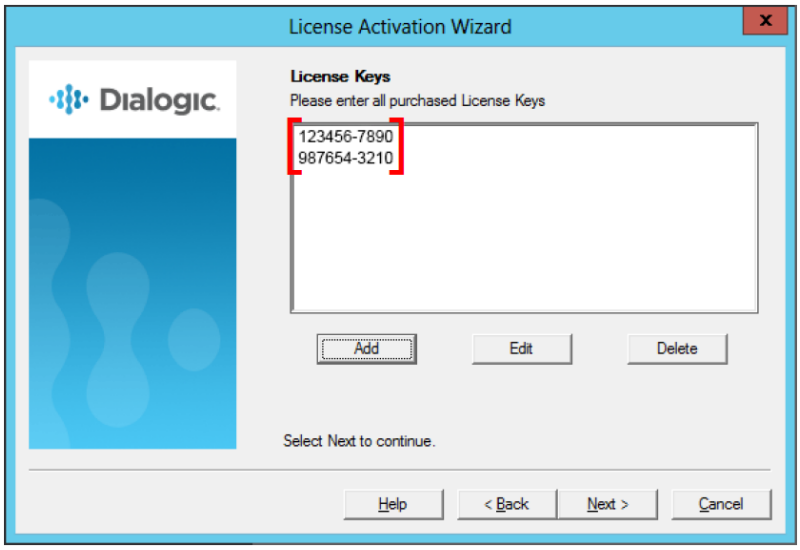
7. The new license key has been successfully added to the system. Click **Add**.



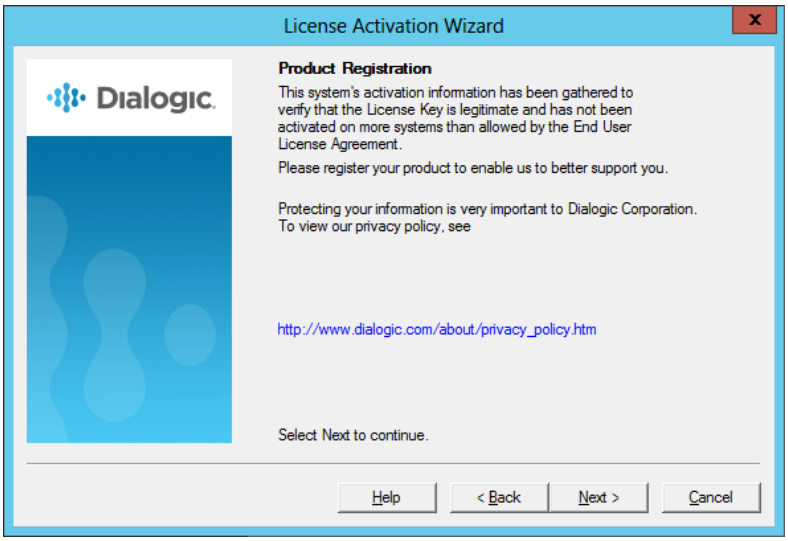
8. Enter the SR140 **secure** fax license key number. Click **OK**.



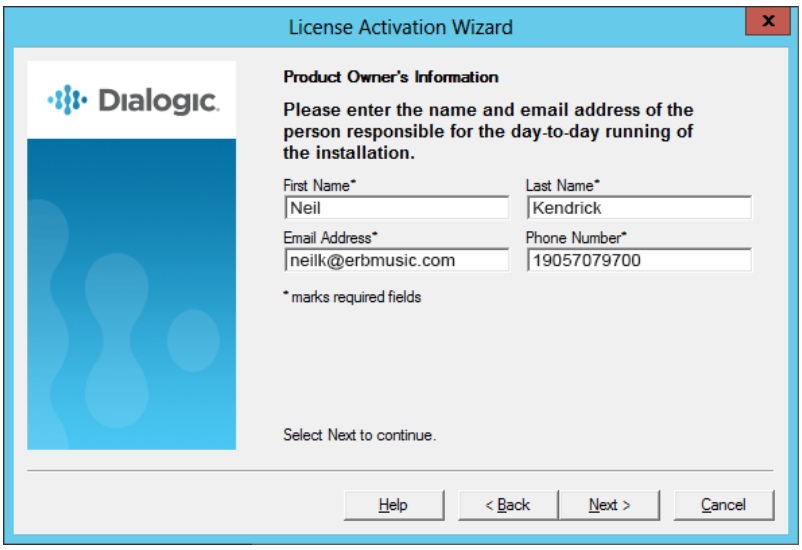
9. Both license keys have been successfully added to the system. Click **Next**.



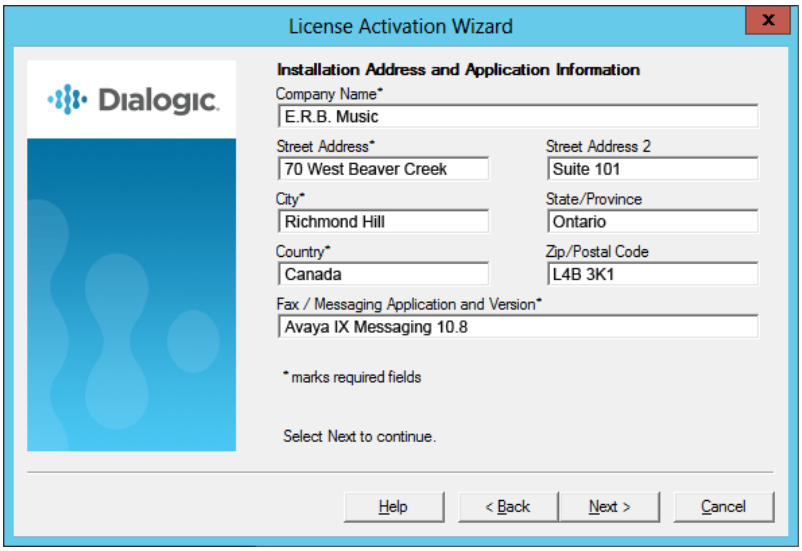
10. Click **Next** to continue to the **Product Registration** pages.



11. Enter the details of the site administrator. All fields are required for registration. Click **Next**.



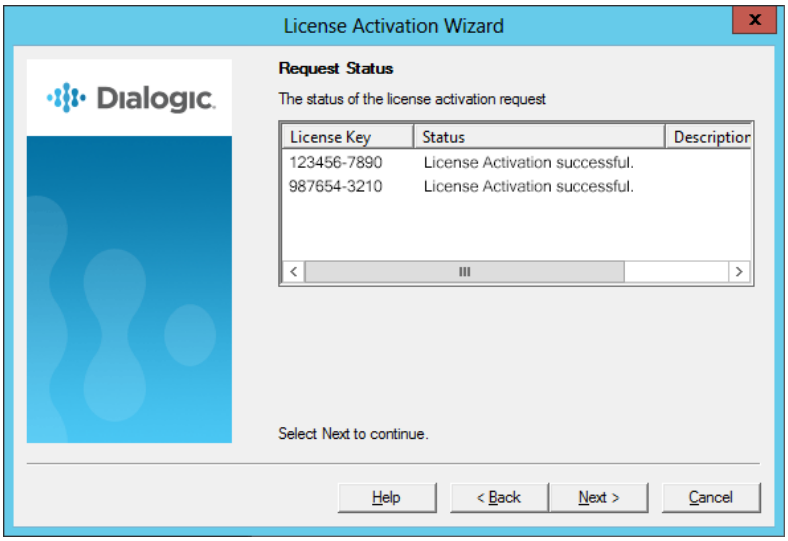
12. Enter the details for the location where the software is installed. Click **Next** to continue.



13. The program will connect to the Dialogic servers to upload the registration details. This requires a working Internet connection and must be completed before the license is activated. When it has finished, click **Next** to continue.



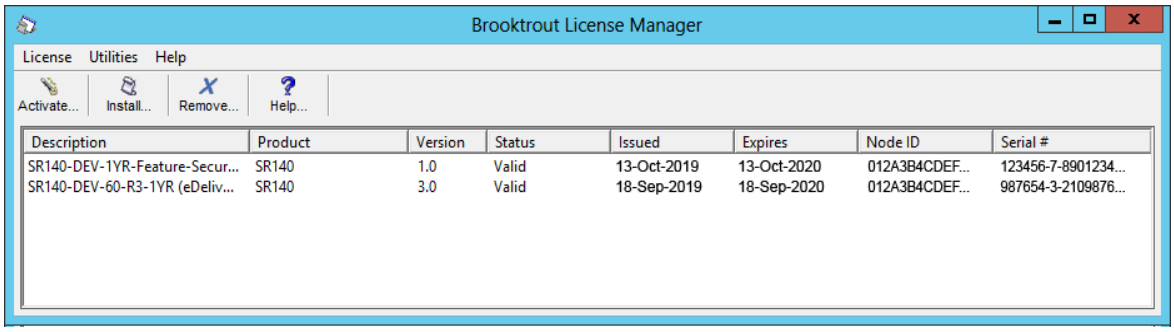
14. The new licenses have been activated on the system. Click **Next**.



15. Click **Finish** to complete the Wizard.

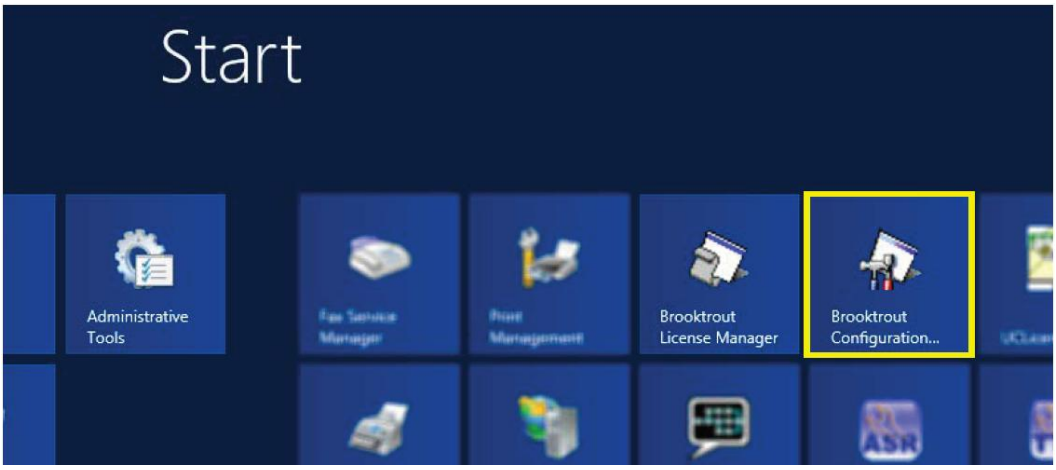


16. The added licenses appear in the **Brooktrout License Manager**.

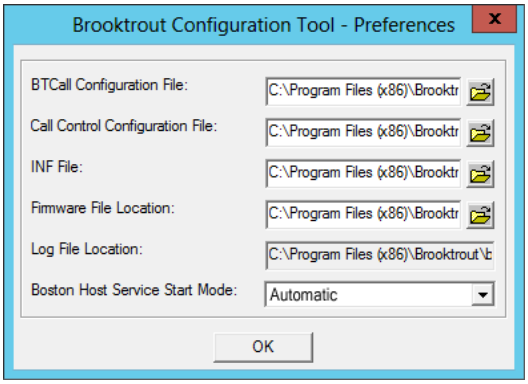


Configuration Manager

1. Open the **Brooktrout Configuration Manager** program.

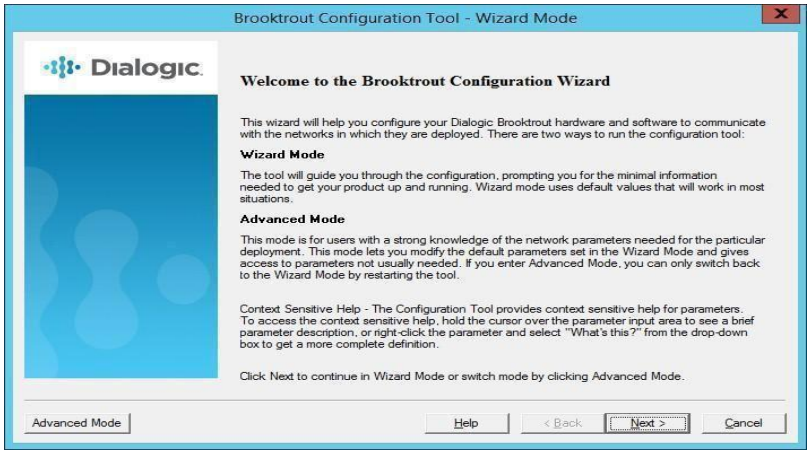


2. At **Configuration Tool - Preferences**, change **Boston Host Service Start Mode** to **Automatic** and click **OK**.

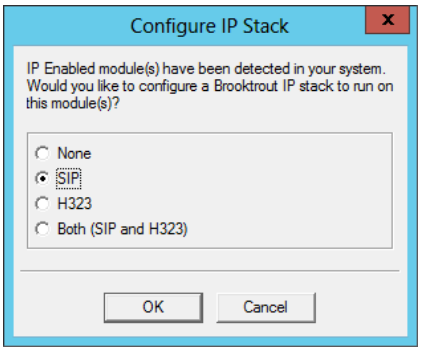


Hint: This screen will only appear the first time you run the program. Thereafter, this screen will be skipped.

3. When the Configuration Wizard starts, choose Advanced Mode.

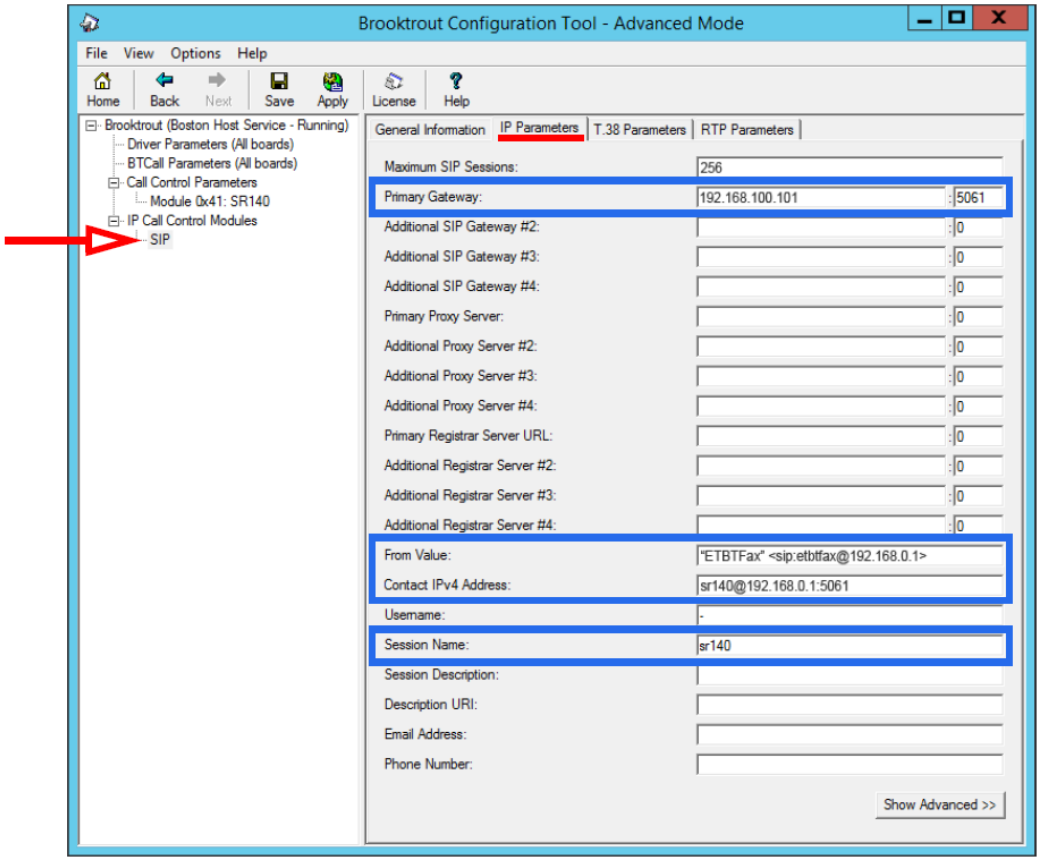


4. Enable the stack option for SIP, then click **OK** to continue.



Hint: This screen will only appear the first time you run the program. Thereafter, this screen will be skipped.

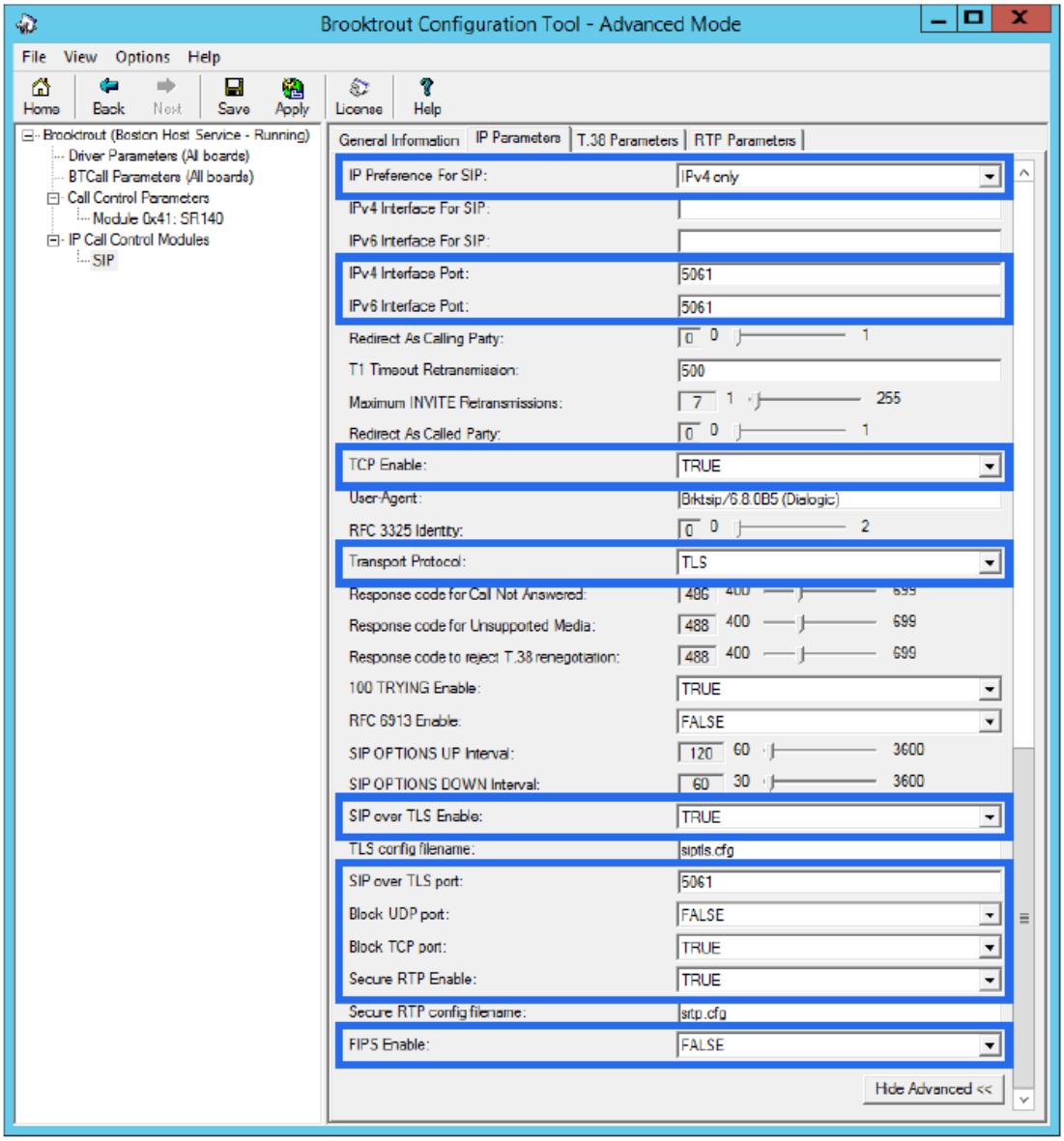
5. In the left-hand panel, click **SIP** beneath **IP Call Control Modules**. Go to the **IP Parameters** tab and specify the following for your site.



Primary Gateway: Enter the IP address of the Avaya Aura Communication Manager server. This was initially configured on the device. Add the port value that the CM uses for faxing in the second field.
From Value: In this field, (including the quotes) type "**ETBTFax" <sip:etbtfax@** followed by the IP address of the Avaya Messaging voice server. For example: "**ETBTFax" <sip:etbtfax@192.168.0.1>** .

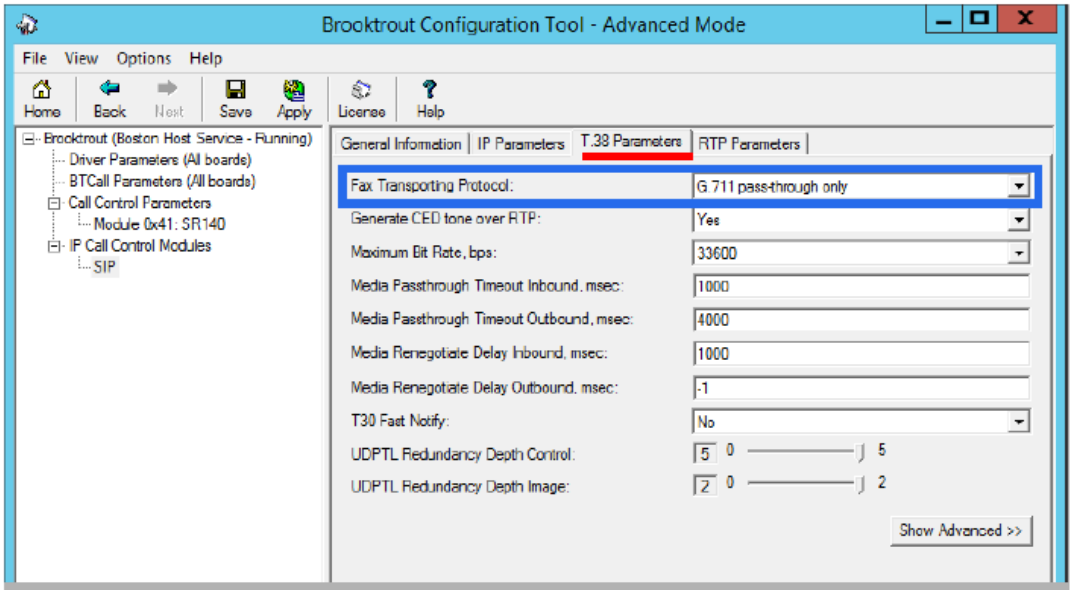
Contact IPv4 Address: Add **sr140@** followed by the IP address and the port used by the Avaya Messaging voice server. For example: **sr140@192.168.0.1:5061** .
Session Name: Enter **sr140** in this field. When ready, click **Show Advanced>>.**

6. Specify the following for your site.

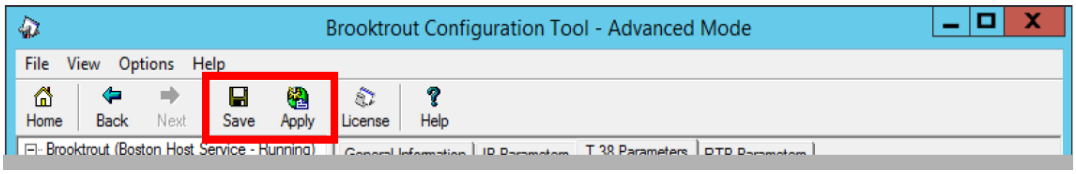


IP Preference for SIP: Select **IPv4 only** from the dropdown list.
IPv4 Interface Port: Enter the port used for faxing. IPv6 Interface Port: Enter the port used for faxing.
TCP Enable: Set this to **TRUE**.
Transport Protocol: Choose **TLS** from the dropdown list.
SIP over TLS Enable: Set this to **TRUE**.
SIP over TLS Port: Enter the port used for faxing.
Block UDP port: Set this to **FALSE**.
Block TCP port: Set this to **TRUE**.
Secure RTP Enable: Set this to **TRUE**.
FIPS Enable: Set this to **FALSE**.

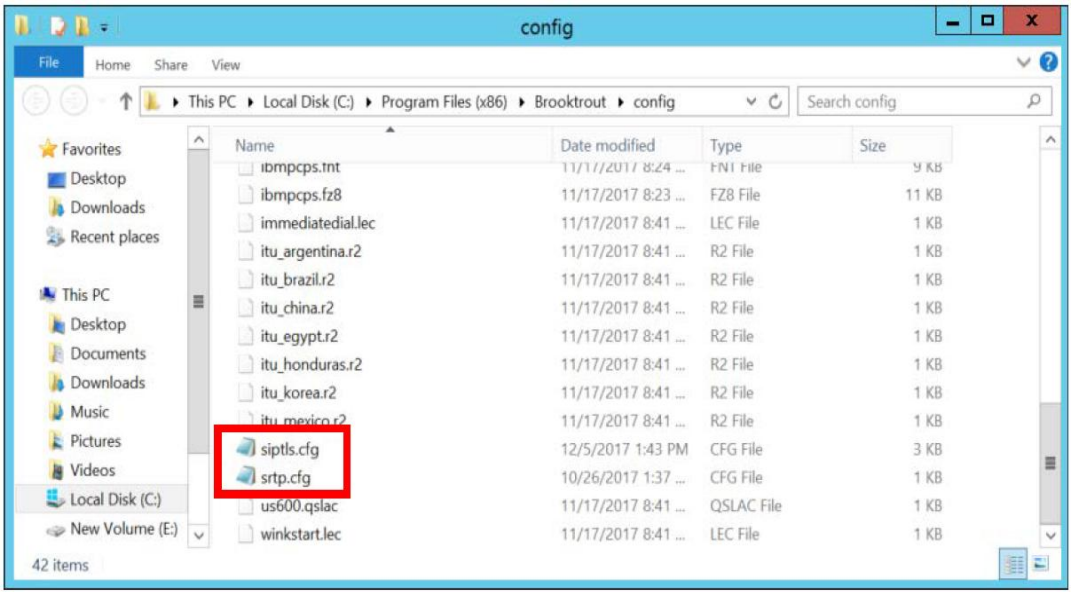
7. Go to the **T.38 Parameters** tab and specify the following for your site. **Fax Transport Protocol**: Select **G.711 pass-through only** from the dropdown list.



8. Click **Save**, then **Apply**.

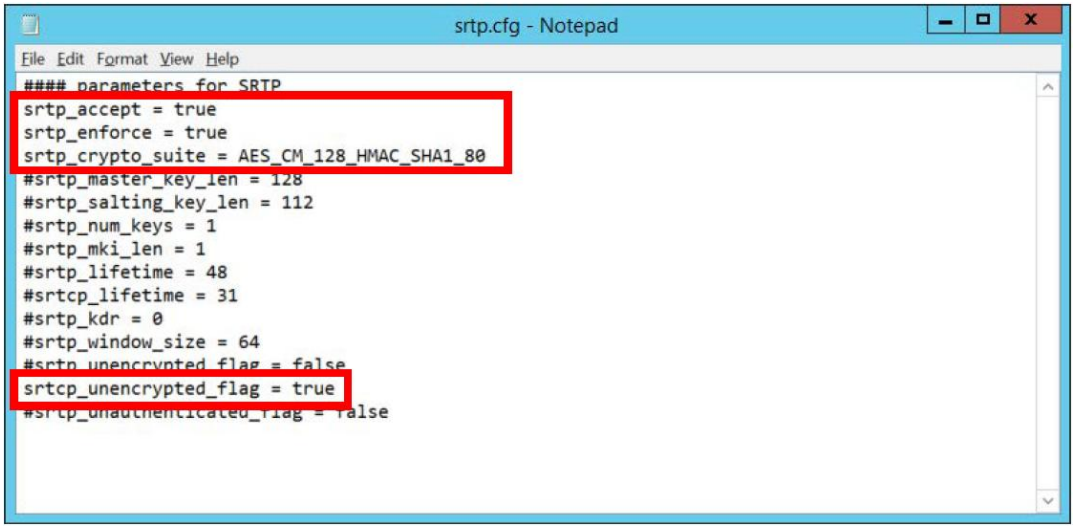


9. On the Avaya Messaging voice server, go to the installation drive and locate the folder **\Program Files (x86)\Brooktrout\config**



10. In the folder, open the **SRTP.cfg file** using a text editor such as Notepad.

Remove the **#** (uncomment) at the start of the following lines, and verify their values are as Shown.

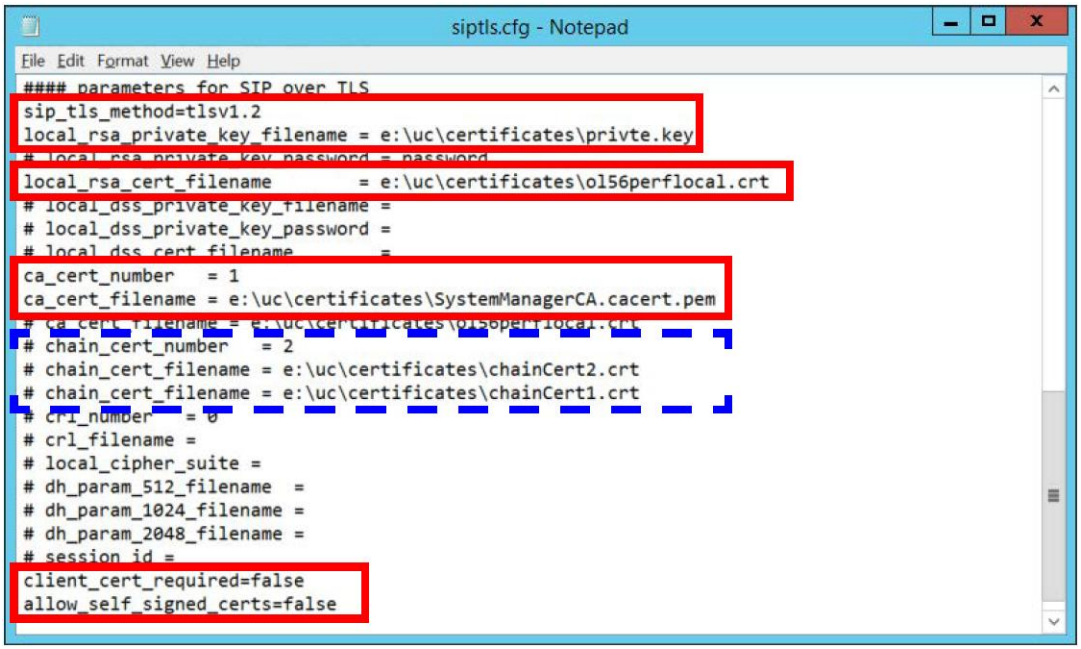


srtp_accept= true

srtp_enforce = true
srtp_crypto_suite = AES_CM_128_HMAC_SHA1_80
srtcp_unencrypted_flag = true

Save the file when finished.

11. Open the SIPTLS.cfg file.
    Remove the **#** (uncomment) at the start of the following lines, and verify their values are as shown.



sip_tls_method = : Leave this field at its default value.
local_rsa_private_key_filename = : Enter the path to the location of your private key file.
local_rsa_cert_filename = : Enter the path to the location of your server certificate file.
ca_cert_number = : Put the number of the cert you are using here. Add as many as are required**.**
ca_cert_filename = : Put the name of the certificate file you are using here. Add as many as are required. (optional)

chain_cert_number = : Put the number of the cert you are using here. Add as many as are required.This is only required if you are using Intermediate certificates.

(optional) **chain_cert_filname =** : Put the name of the certificate file you are using here. Add as many as are required. This is only required if you are using Intermediate certificates.
client_cert_required = false

allow_self_signed_certs = false

12. When finished, restart the **UC BTFaxServer** and the **Dialogic Corporation Boston Host Service** services on the computer, or reboot the server.

Avaya Aura Communication Manager Configuration

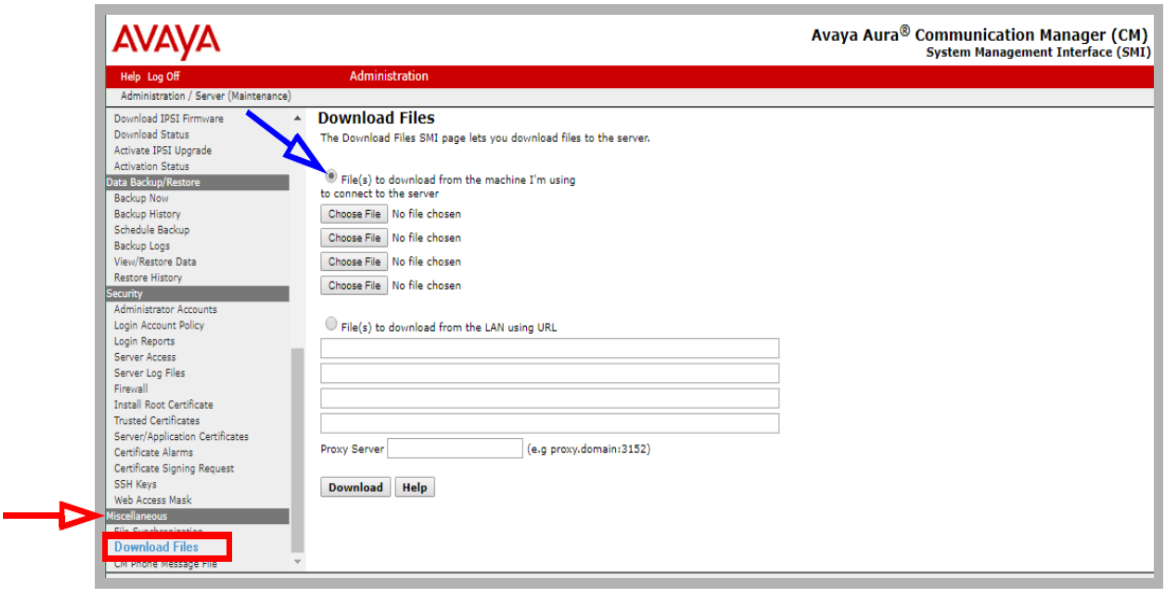
The certificate files must be copied to the AACM server.

1. Login to the AACM server using administrator credentials. Go to **Administration > Server (Maintenance)**.

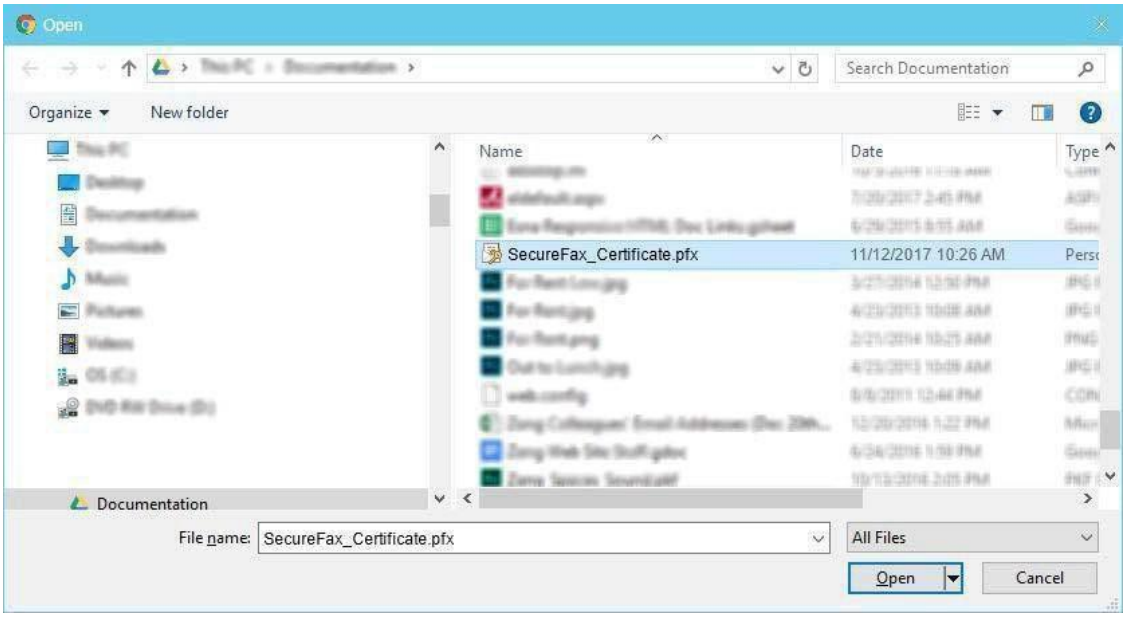


2. Go to **Miscellaneous > Download Files**.

   Enable the **File(s) to download from the machine I'm using to connect to the server** radio button.

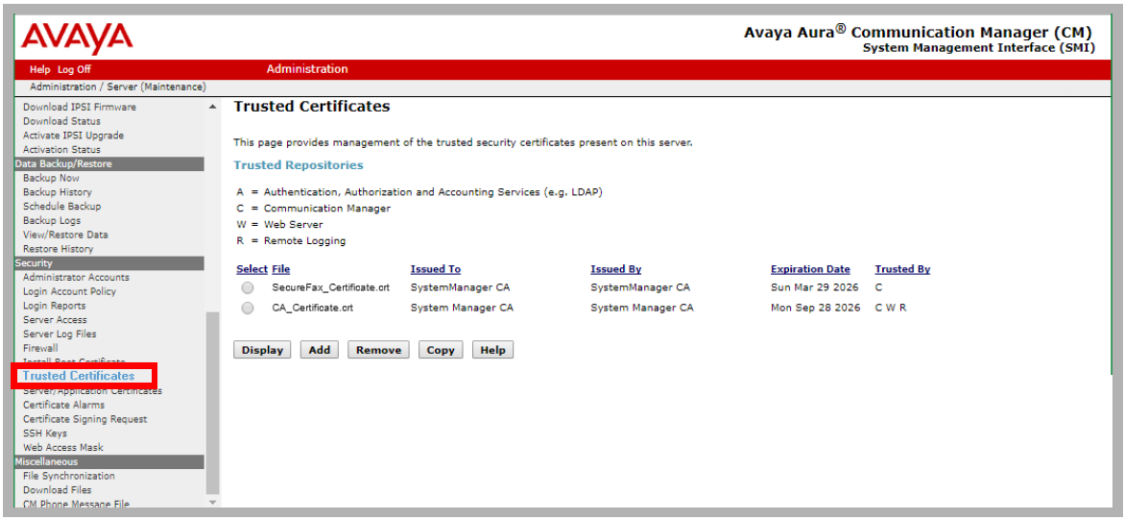


3. Click **Choose File** and find the certificate file. Select the file and click **Open** to add it to the list. Repeat for each certificate file (CA, Intermediate, Server, etc.).

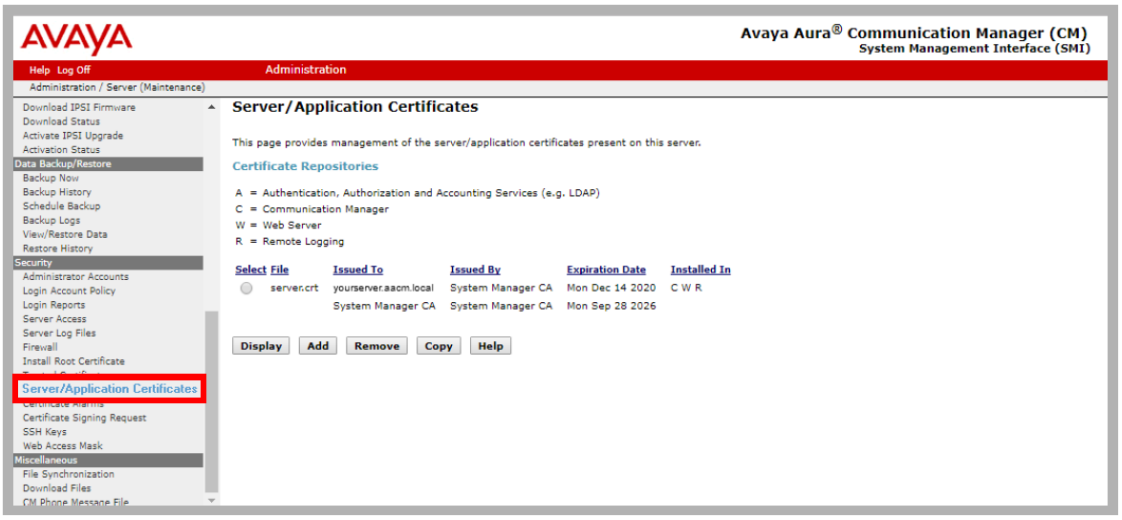


When finished, click the **Download** button to copy the files to the server.

4. In the left-hand column, select **Security > Trusted Certificates**.
Click **Add** and attach each of the CA and Intermediate certificates downloaded in step 3.



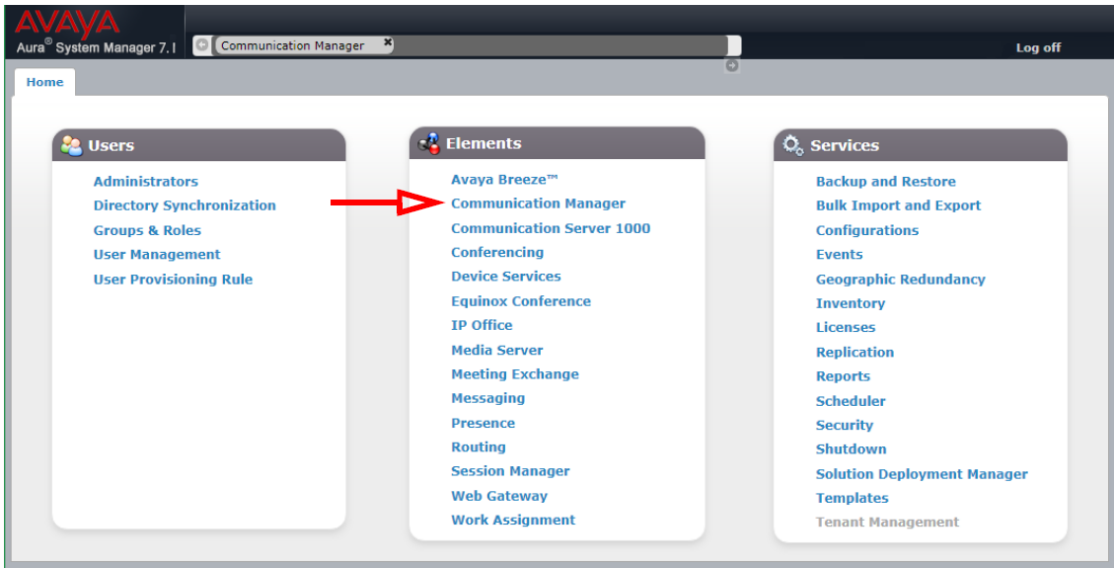
5. In the left-hand column, click **Server/Application Certificates**. Click **Add** and attach the server certificate downloaded in step 3.



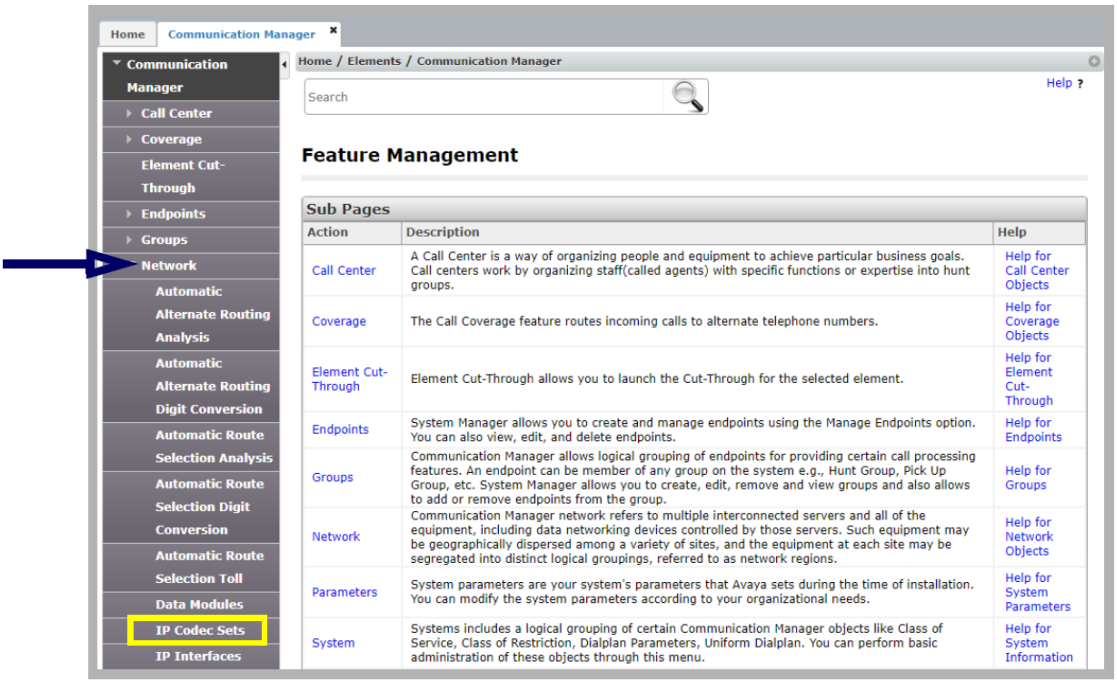
6. Close the **Communication Manager** console.

Avaya Aura System Manager Setup

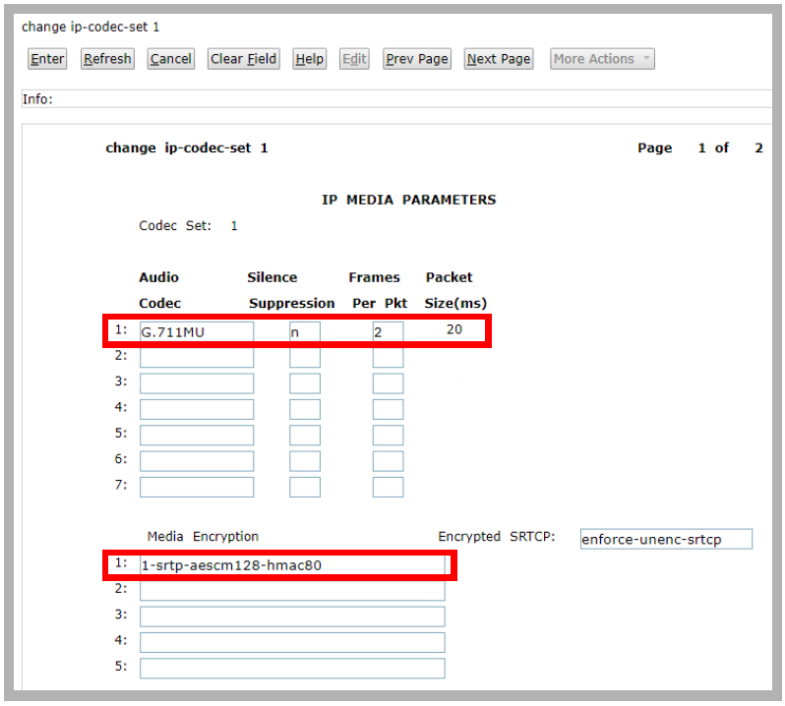
1. Login to the System Manager using an administrator account. Under **Elements**, select **Communication Manager**.



2. Go to **Network > IP Codec Sets**.



3. **Add / Edit** an audio codec set.



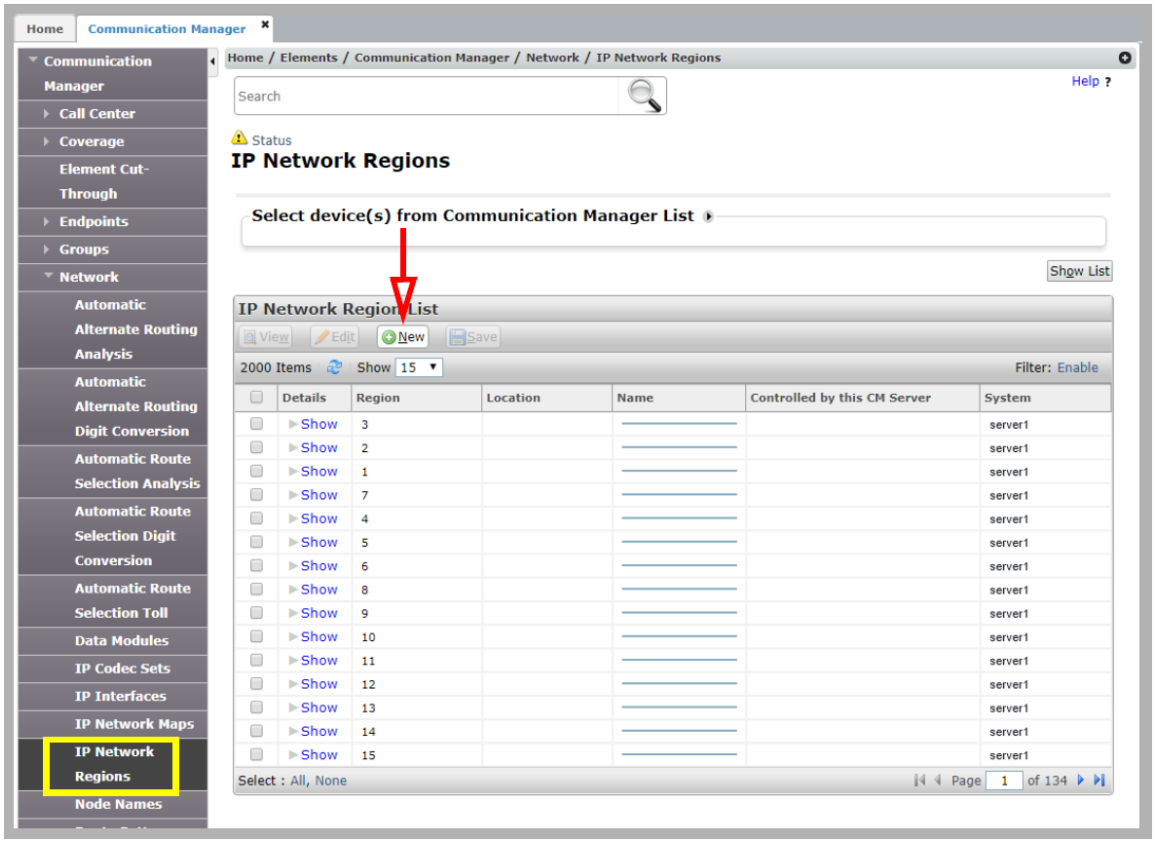
Audio Codec: Set this to **G.711MU**.

Silence Suppression: Choose **n**.

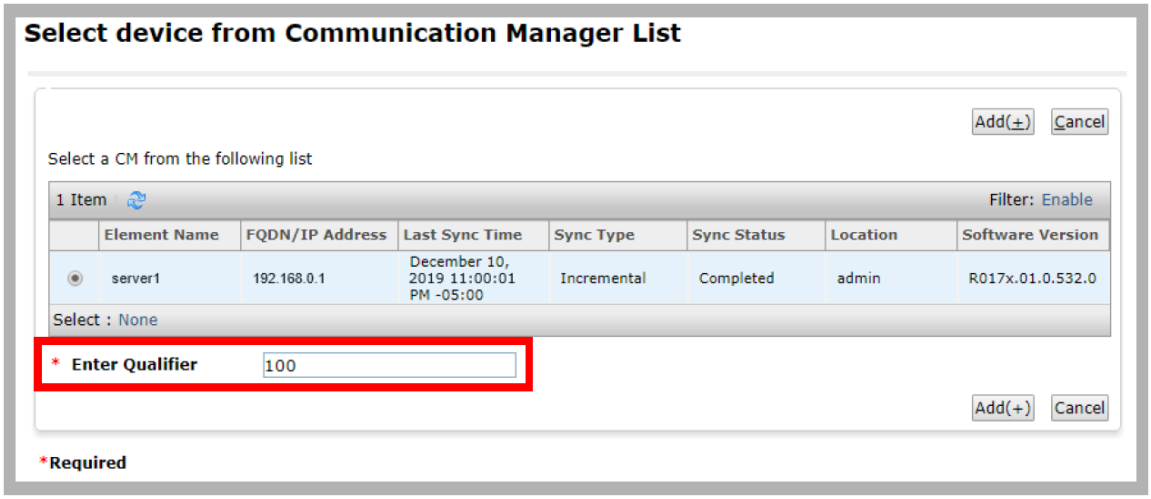
Frames Per Pkt: Enter a value of **2**.

Media Encryption: Select **1-srtp-aescm128-hmac80** from the dropdown list.

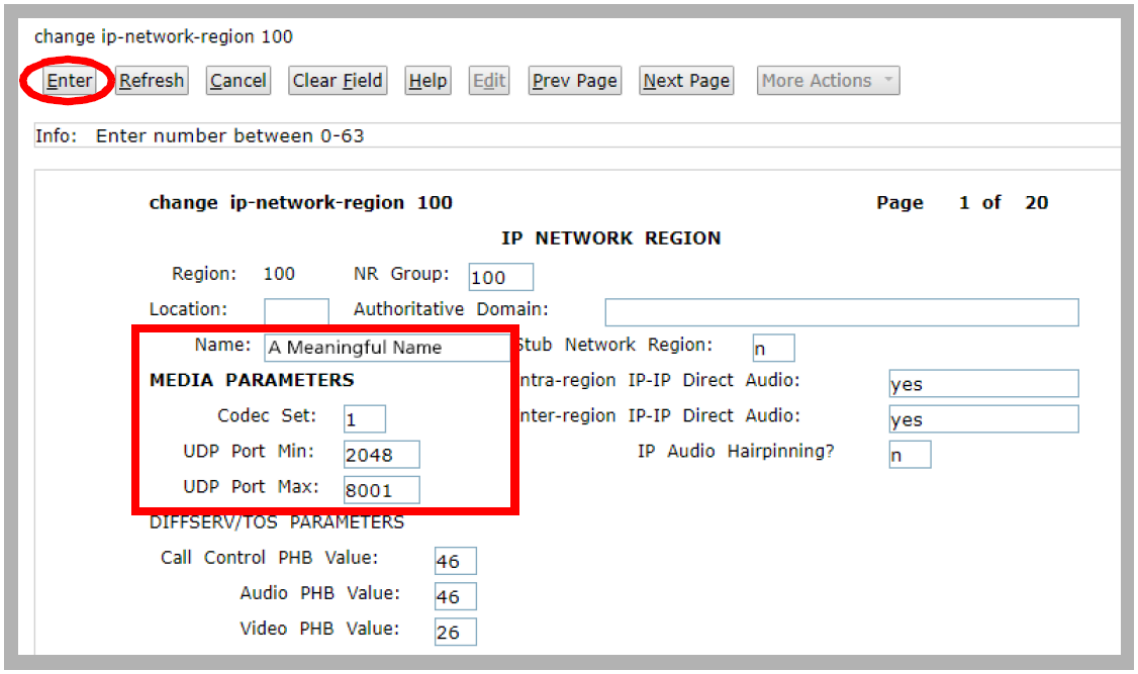
4. Go to **IP Network Regions** in the left-hand column. Click **New** to create an entry.



5. Enter an available **Network Region** qualifier (a number between 1-250), then click **Add**.

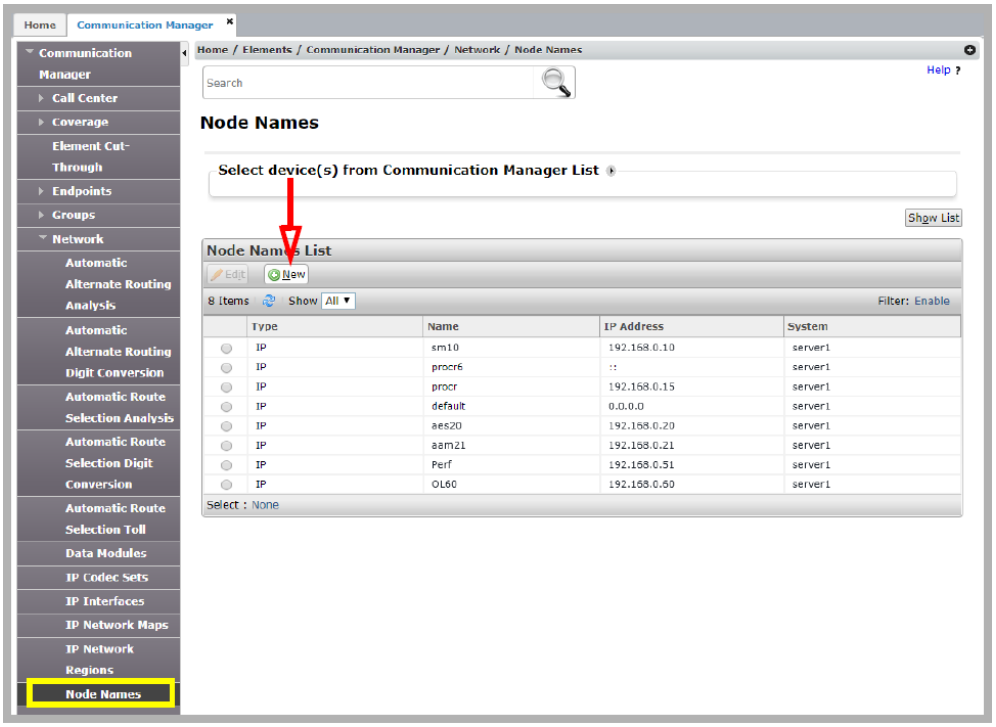


6. Enter the following parameters.

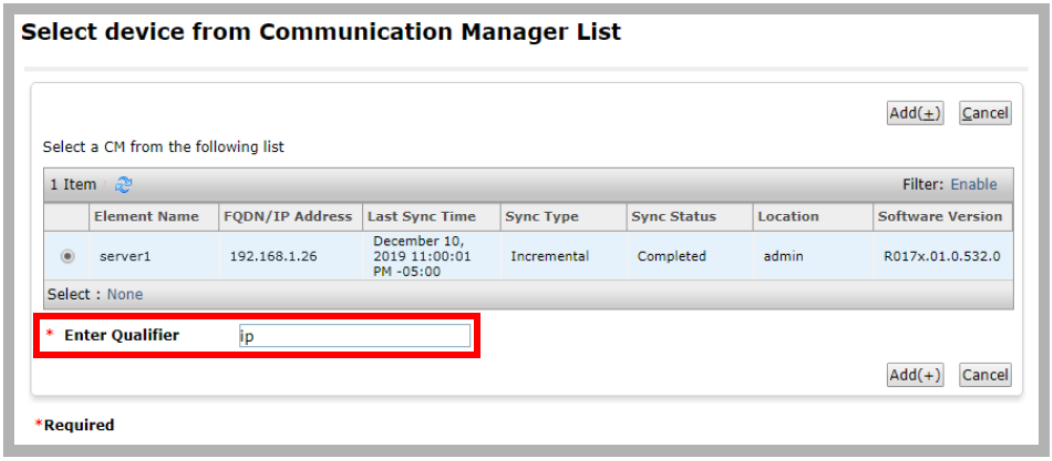


Name: Enter a meaningful, human readable name.
Codec Set: Set this to the codec set number configured in step 3.
UDP Port Min: Enter **2048** here.
UDP Port Max: Enter **8001** here.
Click the **ENTER** button when finished.

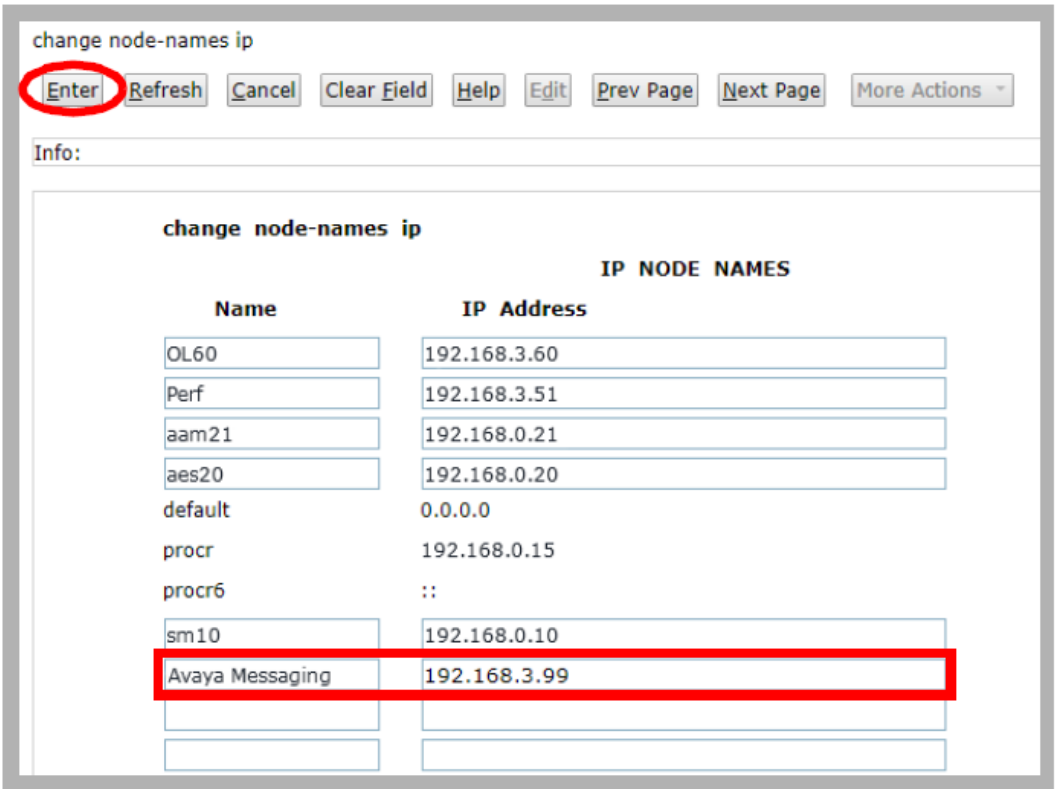
7. Open **Node Names** in the left-hand column. Click **New**.



8. Select **IP** from the qualifier dropdown list, then click **Add**.

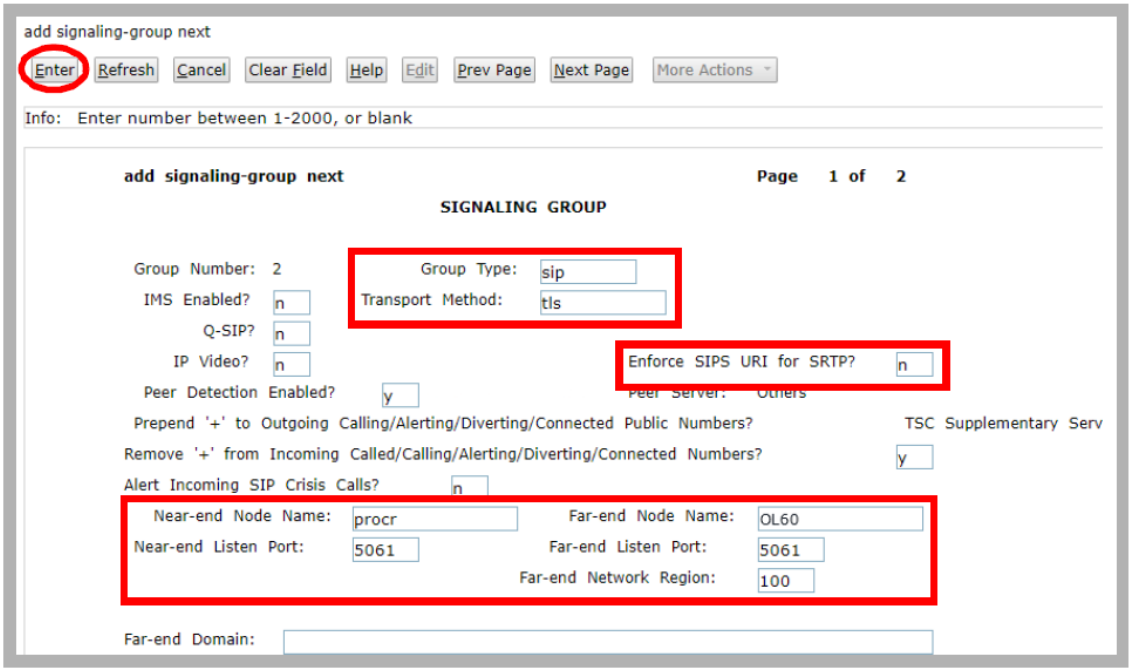


9. In a blank space on the page, name the node, then enter the **IP address** of the Avaya Messaging voice server. When ready, click the **ENTER** button.



10. Open **Signaling Groups** in the left-hand column. Select an existing group (typically group 1) to edit or create a new group. If creating a new group, when prompted by a Qualifier, enter **NEXT**.

    Enter the required values.

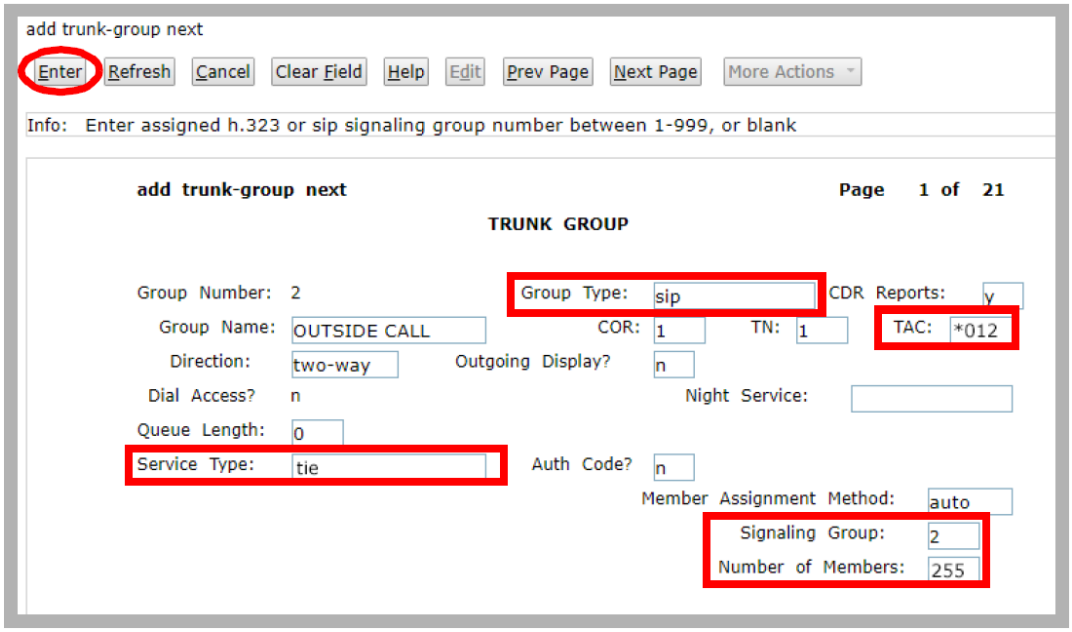


Group Type: Choose SIP from the dropdown list.

Transport Method: Select tls from the dropdown list.

Enforce SIPS URI for SRTP: Set this value to n.
Near-end Node Name: Enter the value procr in this field.
Far-end Node Name: Enter the Node Name from in step 9.
Near-end Listen Port: Enter the port number used for faxing.
Far-end Listen Port: Enter the port number used for faxing.
Far-end Network Region: Enter the network region used as the qualifier in step 5.
When ready, click the **ENTER** button.

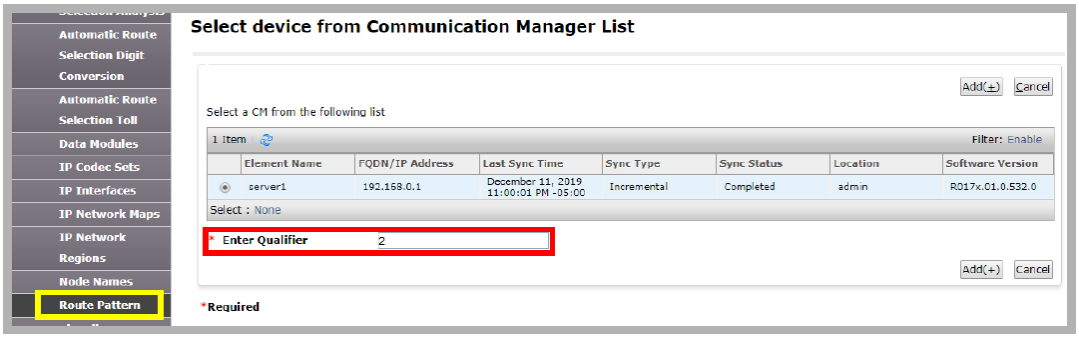
11. Open **Trunk Groups** in the left-hand column. Select an existing group (typically group 1) to edit, or create a new group. If creating a new group, when prompted for a Qualifier, enter **NEXT**.



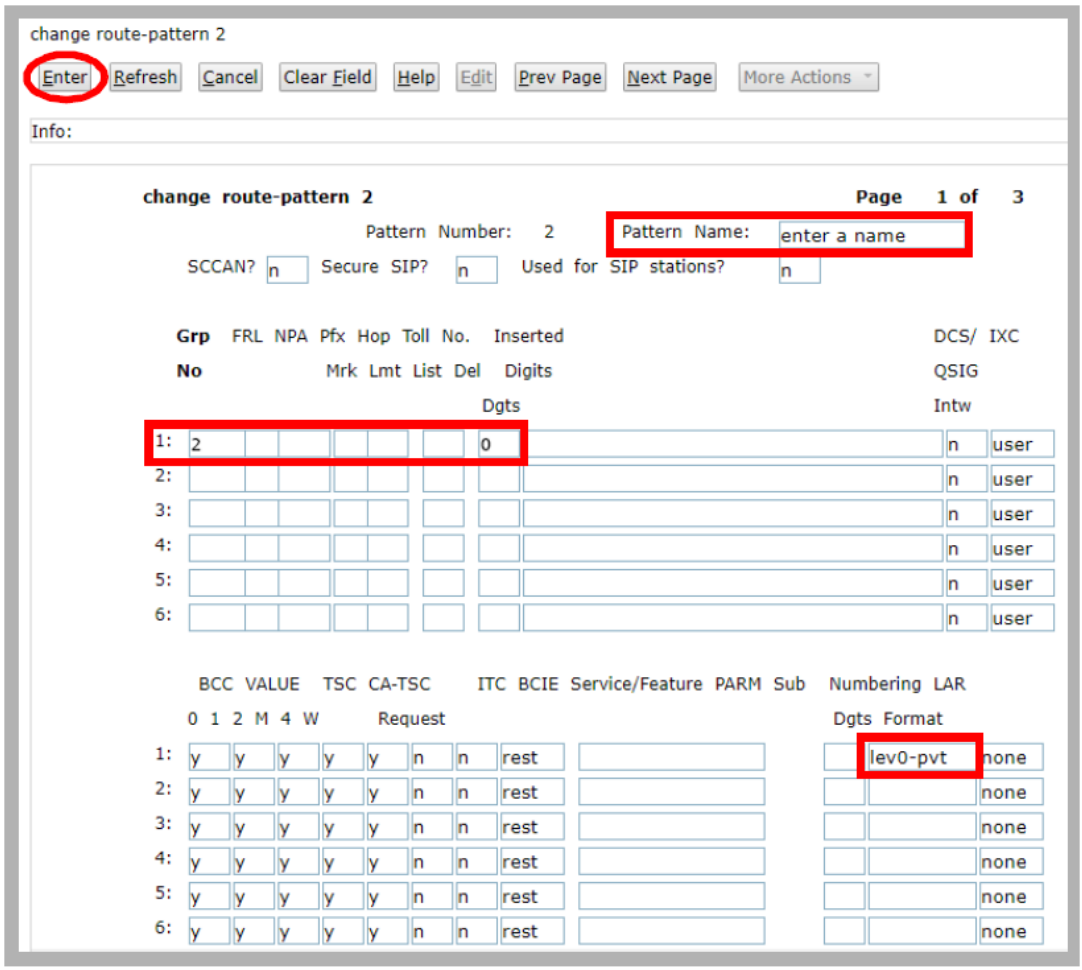
TAC (Trunk Access Code): Enter any unique number. Any four digits, or # and *
Group Type: Select **SIP** from the dropdown list.
Signaling Group: Enter the number of the signaling group from step 10.
Service Type: Select **tie** from the dropdown list.
Number of Members: Type in **255** for this value.

When ready, click the **ENTER** button.

12. Open **Route Pattern** in the left-hand column. Click **New** to create a group. Give it the number of the Trunk Group specified above (step 11), then click **Add**.



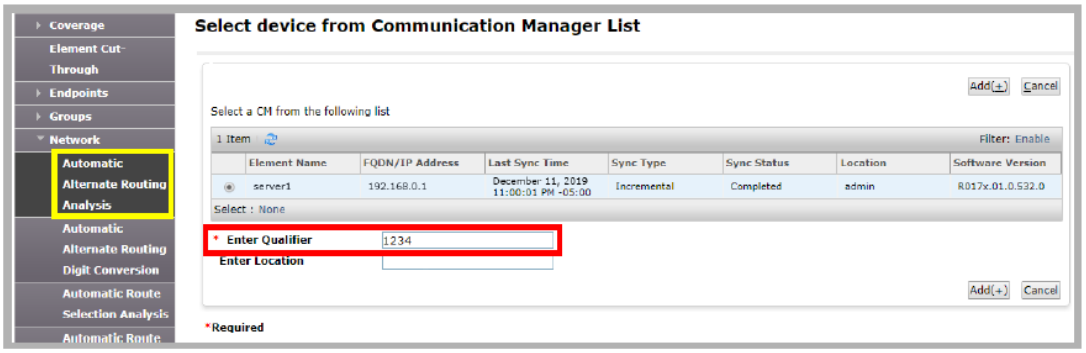
13. Enter the values required.



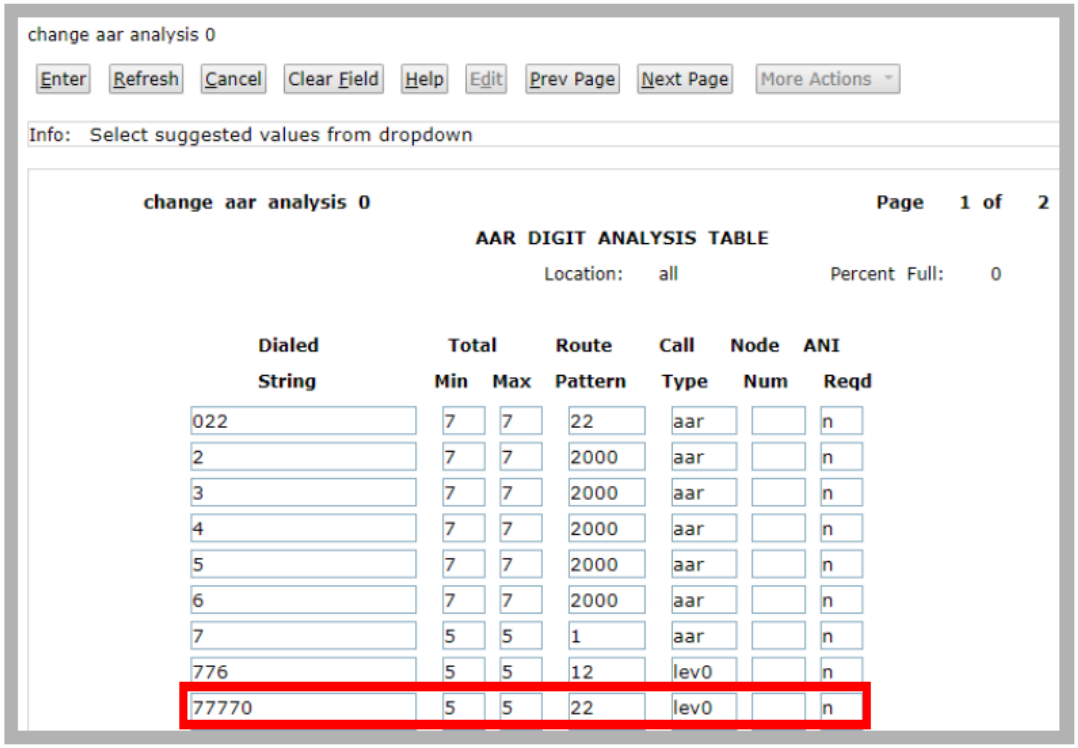
Grp No : Enter the trunk group number configured in step 10.
No. Del Dgts: Usually, set this value to **0**.
Pattern Name: Give the route pattern a human readable name.
Numbering Format: Select **lev0-pvt** from the dropdown list.

When ready, click the **ENTER** button.

14. Open **Automatic Alternate Routing Analysis** in the left-hand column. Click **New** and enter the hunt group number for your system. Or select an existing extension and choose **Edit**. Click **Add**.



15. Modify a Dialed String entry.



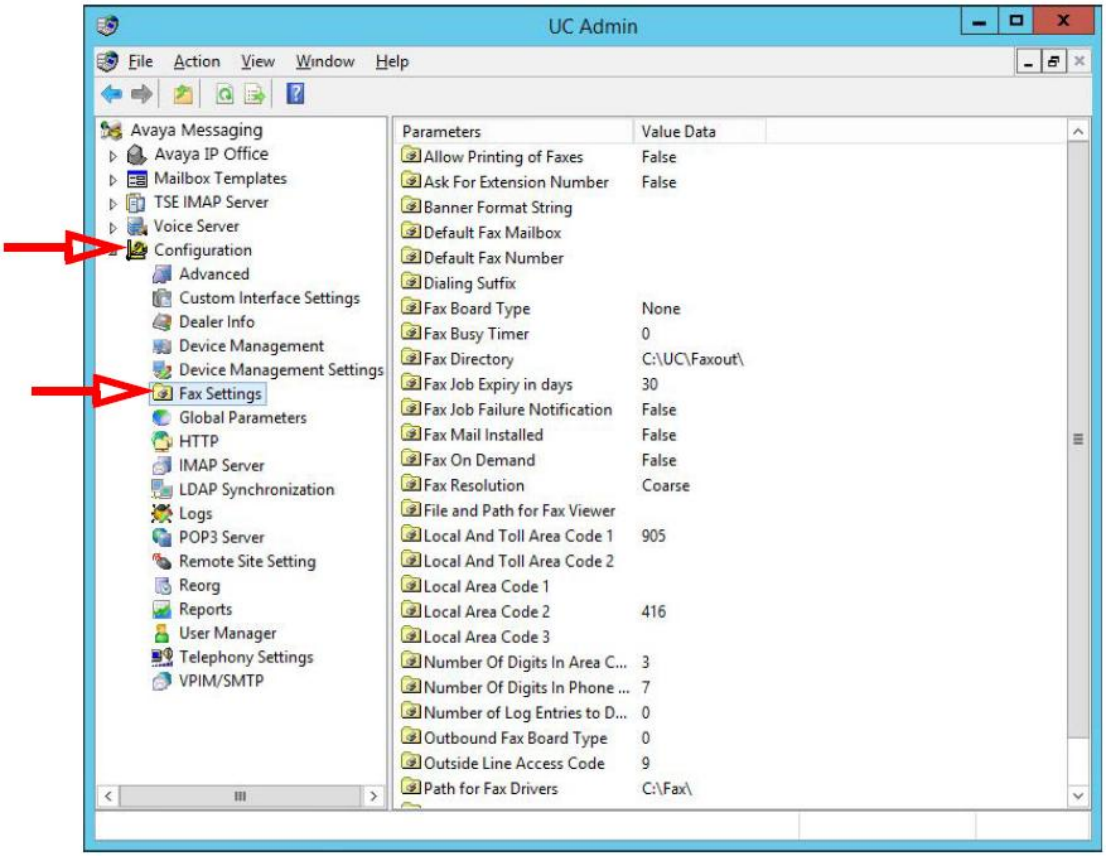
Min / Max: Set these values to the longest or shortest number that can be entered.
Route Pattern: Enter the number of the Route Pattern created in step 12.
Call Type: Select **lev0** from the dropdown list.
When ready, click the **ENTER** button.

Avaya Messaging Configuration

The voice server must be configured to send faxes to the SR140, and to prepare to receive them across the same channel. A setting for incoming, and another for outgoing faxes must be configured on the server using Avaya Messaging Admin.

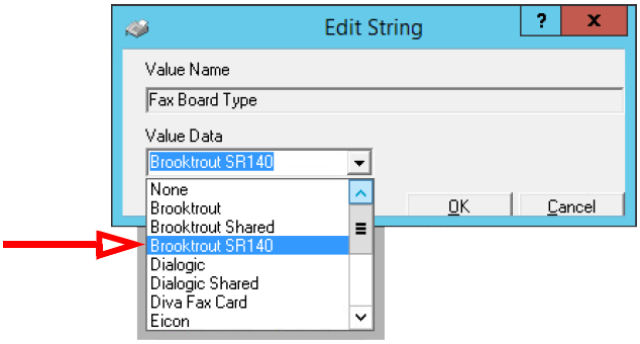
1. Go to **Start > All Programs > Avaya Messaging > Avaya Messaging Admin**, or click the Avaya Messaging Admin icon on the server desktop. Enter the username and password at the prompt.

2. Open **Configuration** and click on **Fax Settings**.

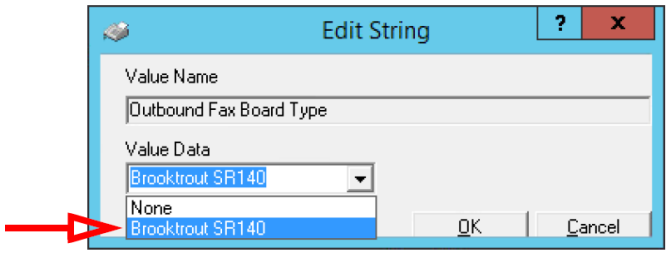


3. In the right-hand pane, locate the entry for **Fax Board Type**. Double-click to open its settings. From the dropdown menu, choose **Brooktrout SR140**.

   Click **OK**.



4. Double-click on **Outbound Fax Board Type**. Choose **Brooktrout SR140** from the dropdown menu. Click **OK**.



Hint: If faxes are only **received** through the SR140 software, the Outbound Fax Board Type can be set to another value if required.

Chapter 19: WEB ACCESS

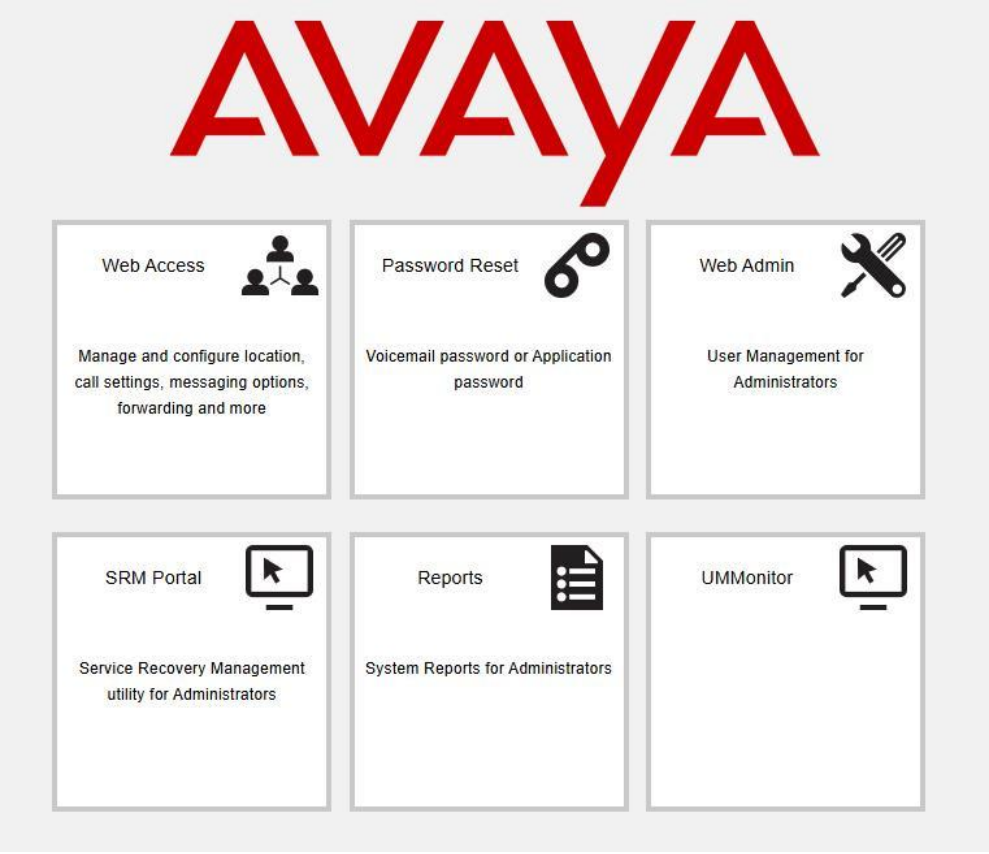
Introduction

Business today requires flexibility and mobility. Company personnel find it increasingly necessary to go where the customers are. Advances in technology allow people to work from home or other locations away from the office. The Avaya Messaging Web Access is an Internet browser-based application that gives users on a UC system the ability to manage all aspects of their communication and schedule from any Internet enabled computer. The Mobile Web Access works with mobile devices as well.
Email, fax and voice messages can be accessed and dealt with. Users can also update their current location. Personal calendars are also available for viewing and modification. Wherever you may need to travel, Web Access will be there to help keep you in touch.

Getting Started

Note: Use Google Chrome for best results. Other web browsers may not be fully supported or provide access to all features.

To launch Web Access, open a web browser and navigate to the corporate UC server site. Click the Web Access icon to start the program.



These links provide multiple authentication methods to access Web Access, some of which may be disabled by your administrator. Select the credentials to use and login.



Note: This screen does not appear if you login without having logged out from a previous session.

Navigation

Web Access consists of five major sections: **Messaging**, **Location**, **People**, **Notification** and Settings.

Through these menus, you have access to all of your messages (voice, fax, and email), and can respond to, delete and manage them. You also have complete access to manage your UC presence, location, schedule, and contacts.



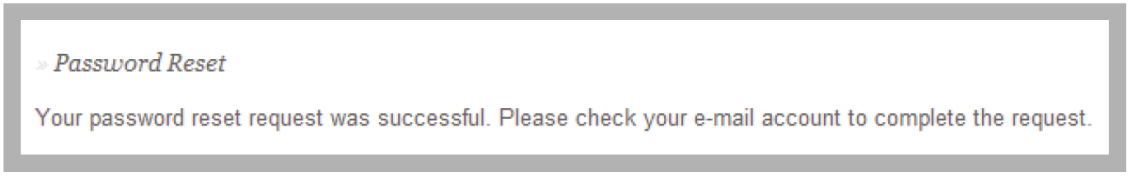
Chapter 20: PASSWORD RESET

Accessing an account requires a password. The voicemail and application passwords can be reset through any web browser from the UC Server web page.

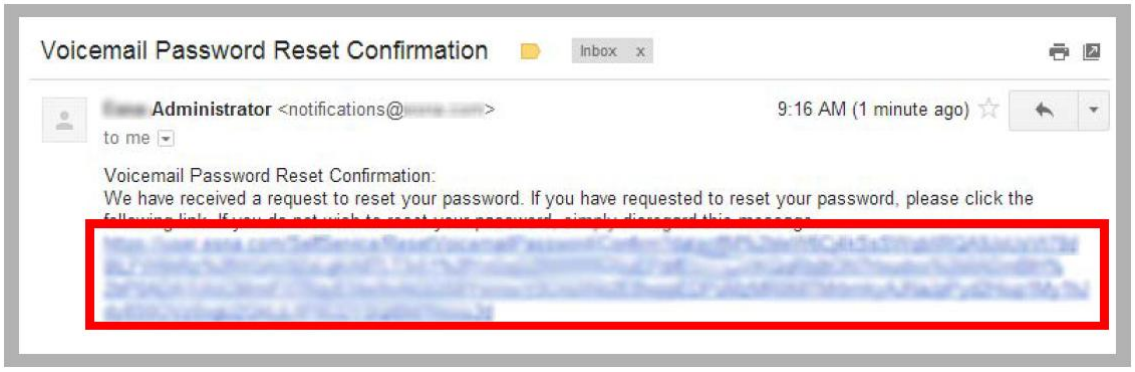
1. Using any web browser, enter the URL for the voice server (i.e., user.yourcompany.com). Select **Password Reset**.
2. Enter an **email address** and select the password to reset: reset Voicemail Password or Application Password.



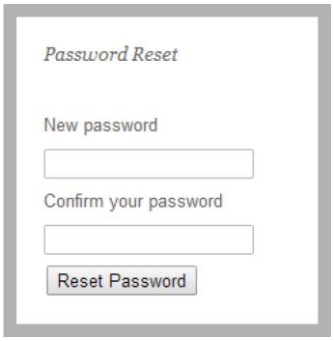
3. Enter the security code in the space provided, Click **Send a Request** when ready.



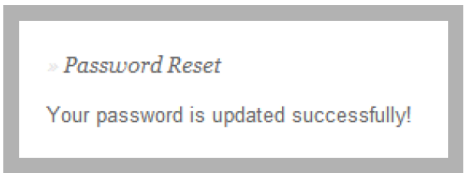
4. The specified email address will receive a message with a link. Click on the link to enter the details of the new password.



5. Enter a new password in the spaces provided, then click **Reset Password**.



6. The account password will be changed to the new value.



Chapter 21: WEB UM MONITOR

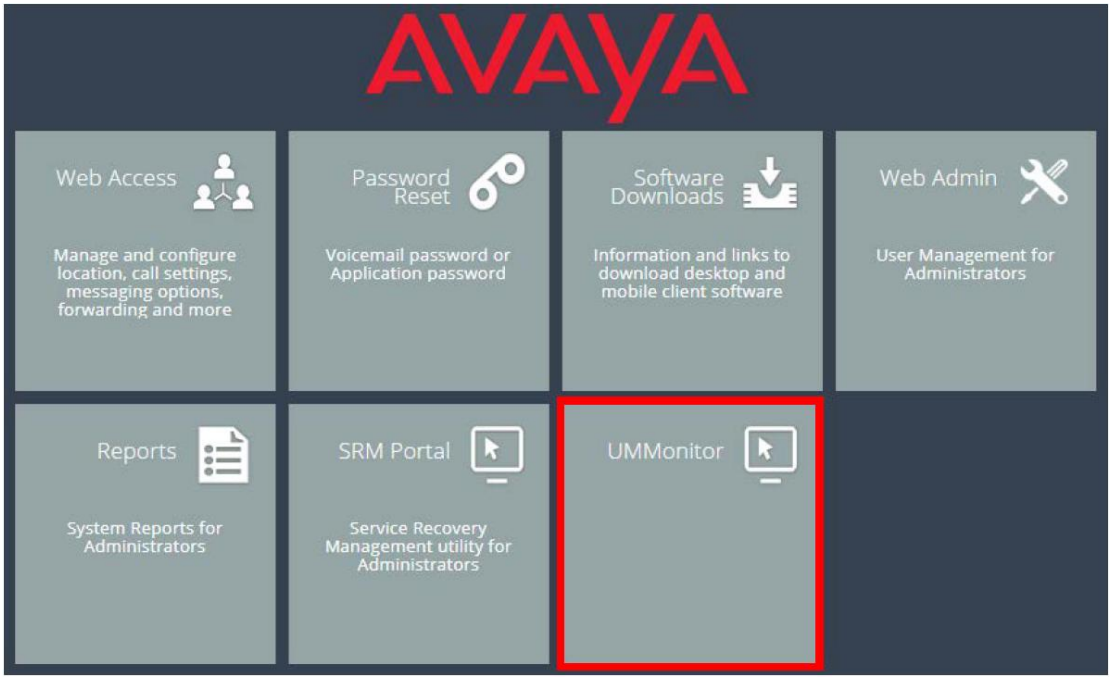
Introduction

The Web UM Monitor is a suite of tools to watch the performance of the system for the purposes of troubleshooting.

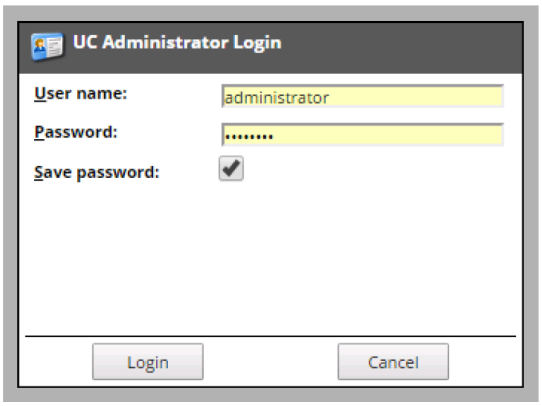
Getting Started

Note: Use Google Chrome for best results. Other web browsers may not be fully supported or provide access to all features.

1. To launch Web UM Monitor, open a web browser and navigate to the corporate UC server site. Click the **UM Monitor** icon to start the utility.



2. Enter the administrator username and password for the voice server.



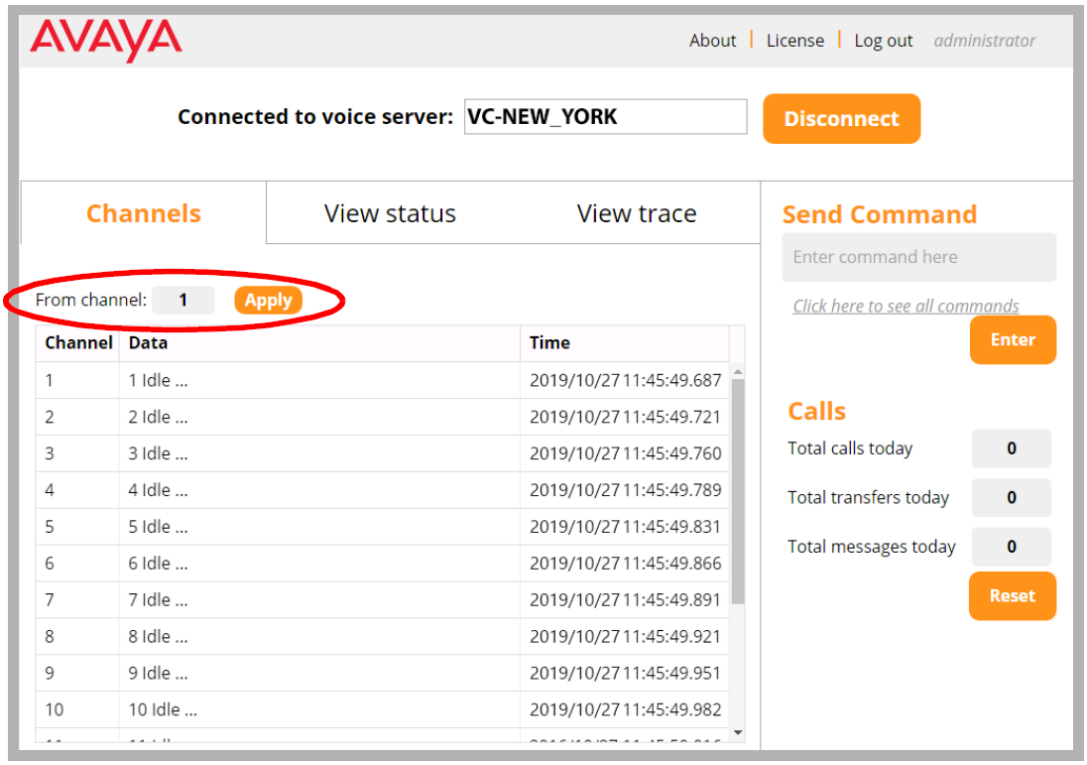
3. From the dropdown menu, select the voice server you want to monitor.



4. Click **Connect** to begin monitoring the voice server.
   Hint: When finished, click **Disconnect** to stop monitoring that voice server.

The Channels Tab

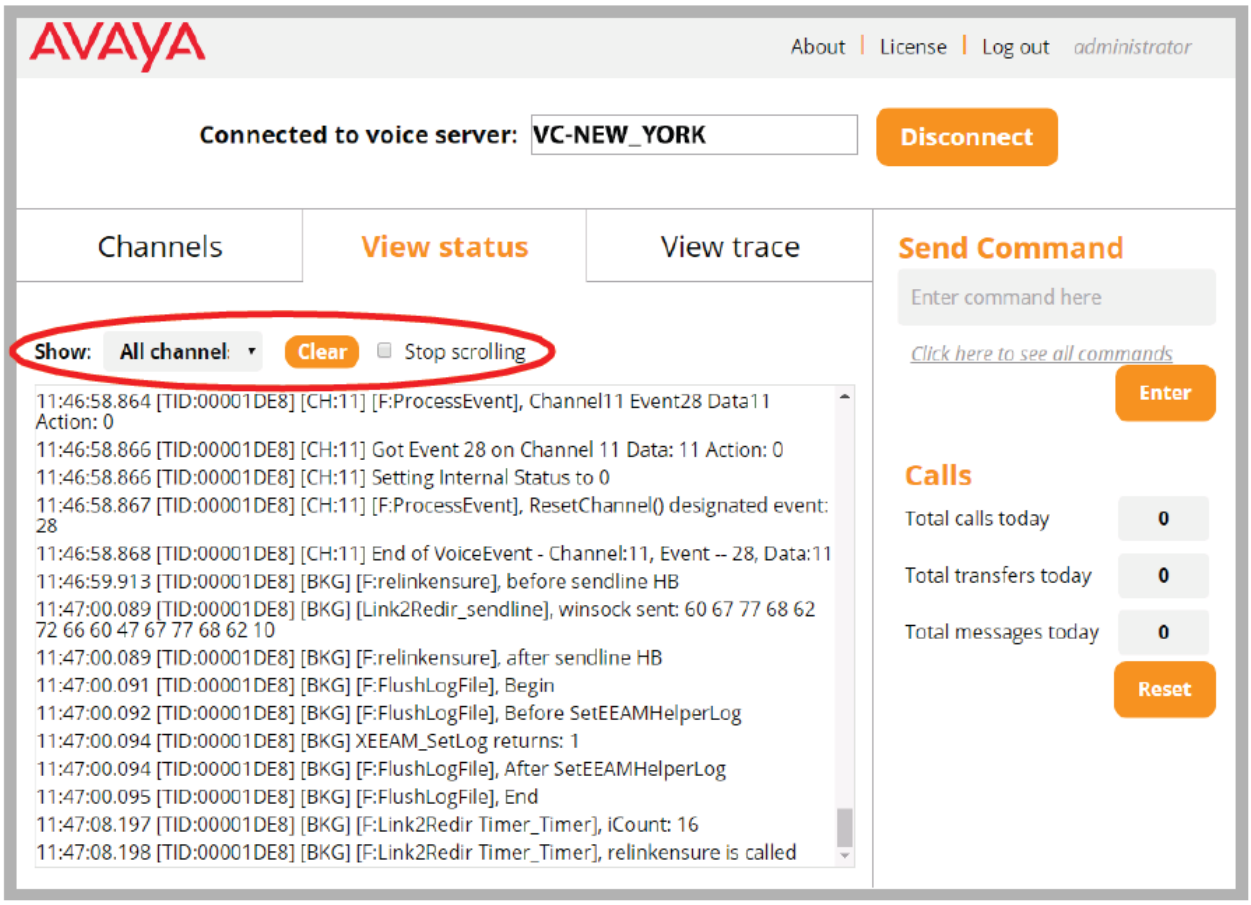
The Channels Tab is the starting point for the program. In this panel the status of each channel is displayed working on the voice server.



Hint: To view only a range of channels, enter the starting channel number in the box and click **Apply**. Only the channels from there up to the last will be shown.

The View Status Tab

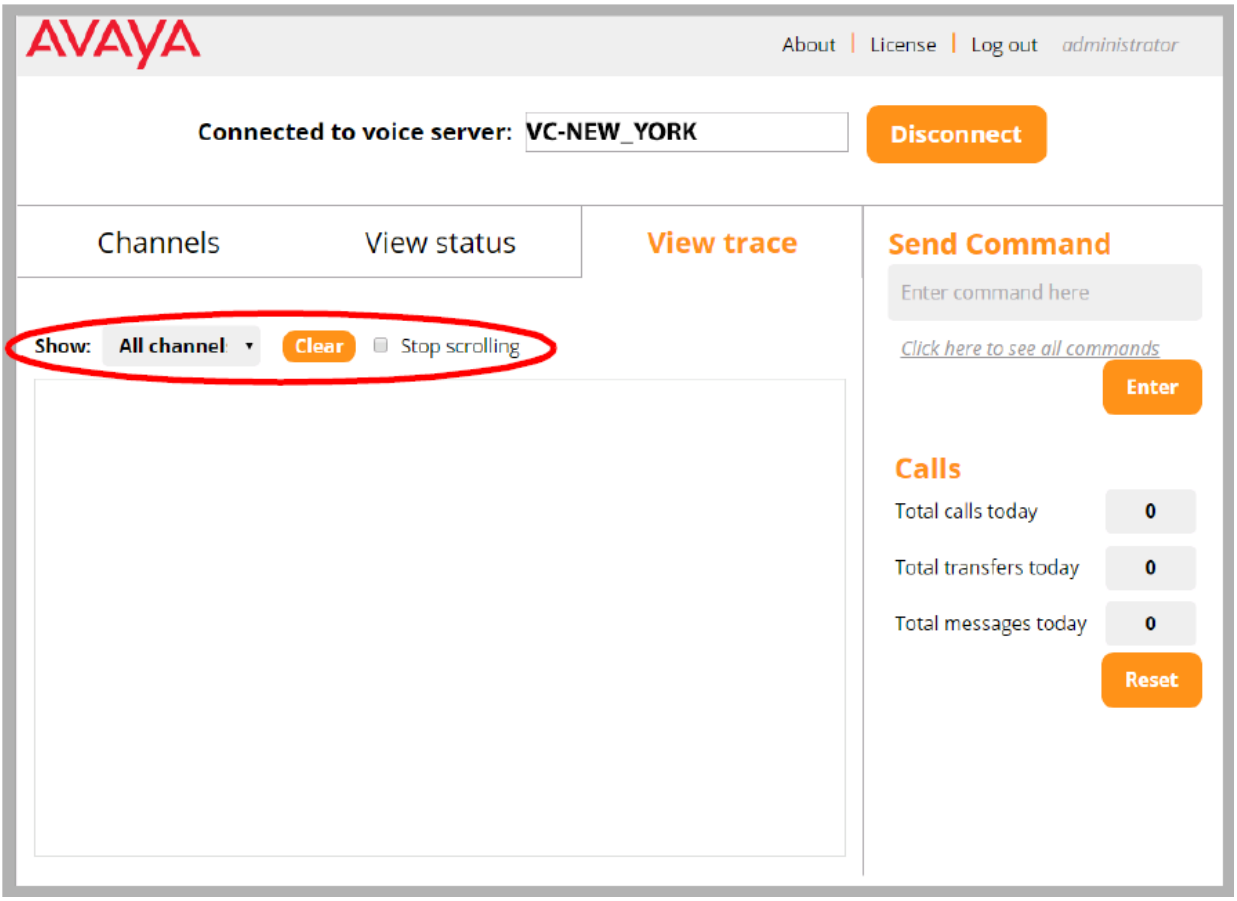
This pane shows the commands that are being sent and received through all of the voice server channels.



Select either **All channels** or a specific channel to monitor from the dropdown list.
Use **Clear** to remove all status entries from the display. New status entries will begin to fill the screen.
Enable **Stop scrolling** to freeze the window. New entries will continue to be added to the bottom of the list, but the pane will not move until you manually begin scrolling.

The View Trace Tab

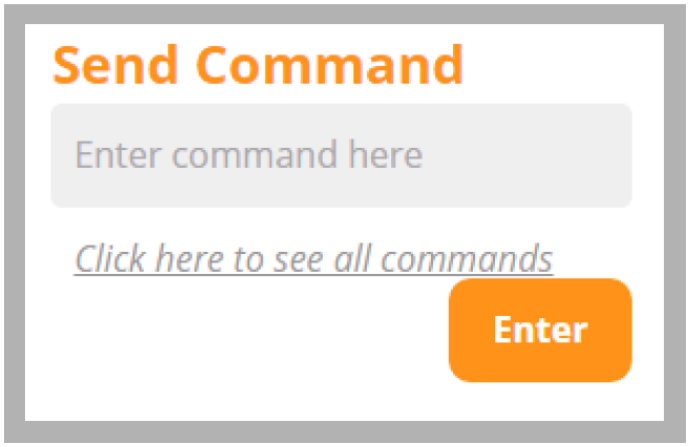
The View Trace tab allows you to get a clearer idea of what each channel is doing.



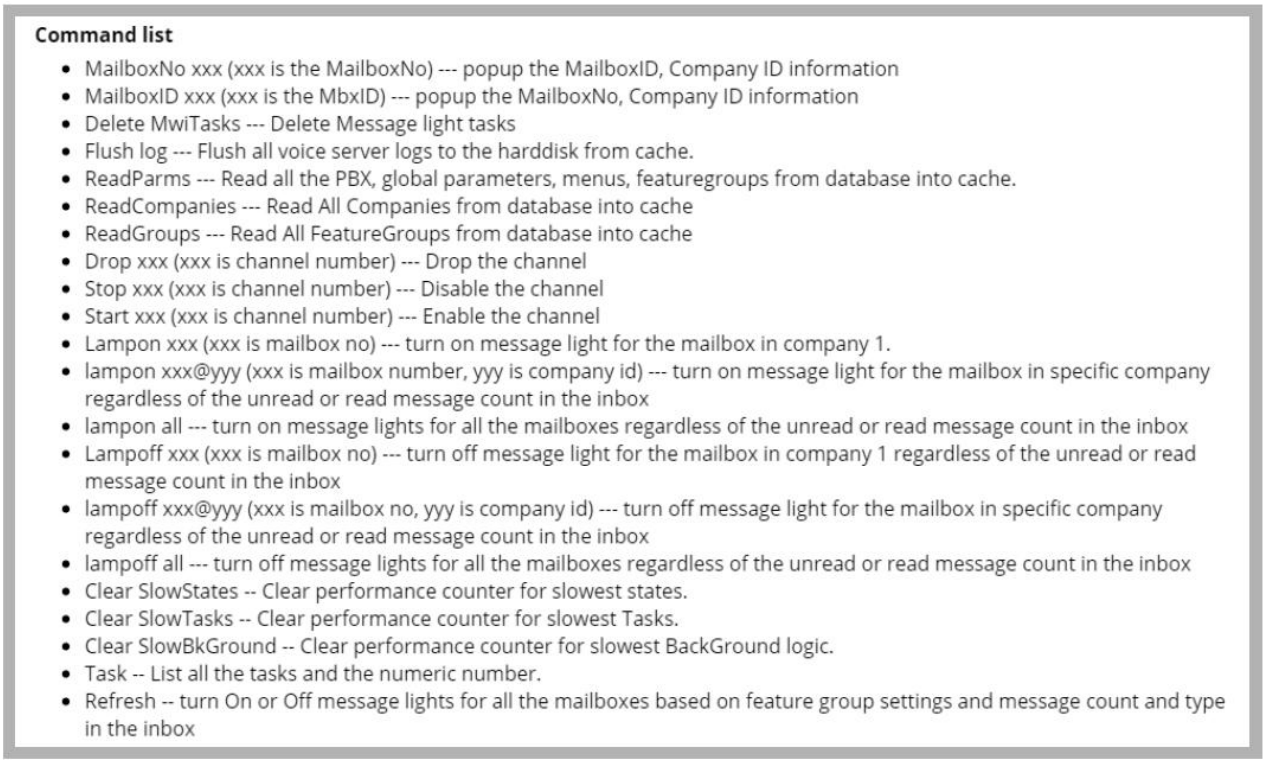
Select either **All channels** or a specific channel to monitor from the dropdown list.
Use **Clear** to remove all status entries from the display. New status entries will begin to fill the screen.
Enable **Stop scrolling** to freeze the window. New entries will continue to be added to the bottom of the list, but the pane will not move until you manually begin scrolling.

Sending Commands

Use Send Commands to issue commands directly to the voice server. Enter the command into the space provided and click the **Enter** button.



You can also view all available commands and their format by clicking the link.

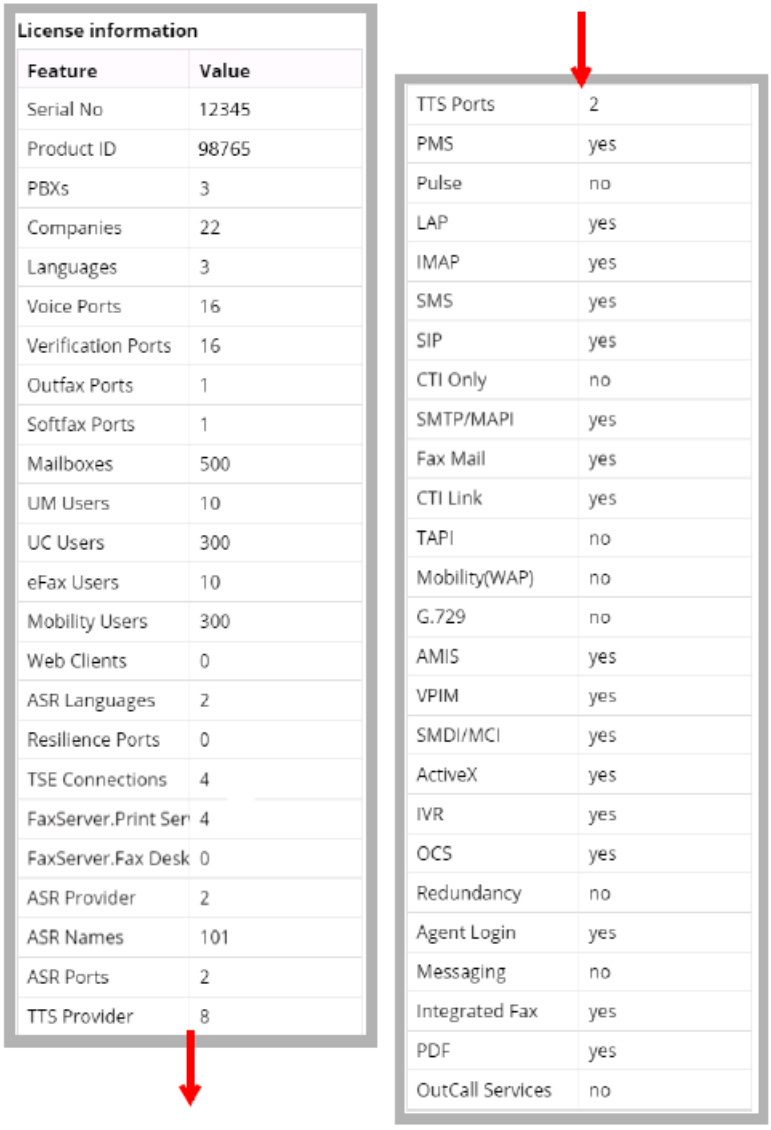


Command list

- MailboxNo xxx (xxx is the MailboxNo) --- popup the MailboxID, Company ID information
- MailboxID xxx (xxx is the MbxID) --- popup the MailboxNo, Company ID information
- Delete MwiTasks --- Delete Message light tasks
- Flush log --- Flush all voice server logs to the harddisk from cache.
- ReadParms --- Read all the PBX, global parameters, menus, featuregroups from database into cache.
- ReadCompanies --- Read All Companies from database into cache
- ReadGroups --- Read All FeatureGroups from database into cache
- Drop xxx (xxx is channel number) --- Drop the channel
- Stop xxx (xxx is channel number) --- Disable the channel
- Start xxx (xxx is channel number) --- Enable the channel
- Lampon xxx (xxx is mailbox no) --- turn on message light for the mailbox in company 1.
- lampon xxx@yyy (xxx is mailbox number, yyy is company id) --- turn on message light for the mailbox in specific company regardless of the unread or read message count in the inbox
- lampon all --- turn on message lights for all the mailboxes regardless of the unread or read message count in the inbox
- Lampoff xxx (xxx is mailbox no) --- turn off message light for the mailbox in company 1 regardless of the unread or read message count in the inbox
- lampoff xxx@yyy (xxx is mailbox no, yyy is company id) --- turn off message light for the mailbox in specific company regardless of the unread or read message count in the inbox
- lampoff all --- turn off message lights for all the mailboxes regardless of the unread or read message count in the inbox
- Clear SlowStates -- Clear performance counter for slowest states.
- Clear SlowTasks -- Clear performance counter for slowest Tasks.
- Clear SlowBkGround -- Clear performance counter for slowest BackGround logic.
- Task -- List all the tasks and the numeric number.
- Refresh -- turn On or Off message lights for all the mailboxes based on feature group settings and message count and type in the inbox

Display License Details

This menu displays the details of the license for the selected voice server.



License information

Feature	Value
Serial No	12345
Product ID	98765
PBXs	3
Companies	22
Languages	3
Voice Ports	16
Verification Ports	16
Outfax Ports	1
Softfax Ports	1
Mailboxes	500
UM Users	10
UC Users	300
eFax Users	10
Mobility Users	300
Web Clients	0
ASR Languages	2
Resilience Ports	0
TSE Connections	4
FaxServer.Print Ser	4
FaxServer.Fax Desk	0
ASR Provider	2
ASR Names	101
ASR Ports	2
TTS Provider	8
TTS Ports	2
PMS	yes
Pulse	no
LAP	yes
IMAP	yes
SMS	yes
SIP	yes
CTI Only	no
SMTP/MAPI	yes
Fax Mail	yes
CTI Link	yes
TAPI	no
Mobility(WAP)	no
G.729	no
AMIS	yes
VPIM	yes
SMDI/MCI	yes
ActiveX	yes
IVR	yes
OCS	yes
Redundancy	no
Agent Login	yes
Messaging	no
Integrated Fax	yes
PDF	yes
OutCall Services	no

Chapter 22: INTEGRATION WITH AVAYA CPaaS

Introduction

Avaya CPaaS is a robust development platform — create what you need and integrate it seamlessly with Avaya Messaging and go!

Integrating with an Avaya Messaging system, either on a single server or high availability installation, gives you the ability to receive SMS messages through a number purchased on Avaya CPaaS, anywhere in the world. Messages are delivered directly to your Avaya Messaging mailbox.

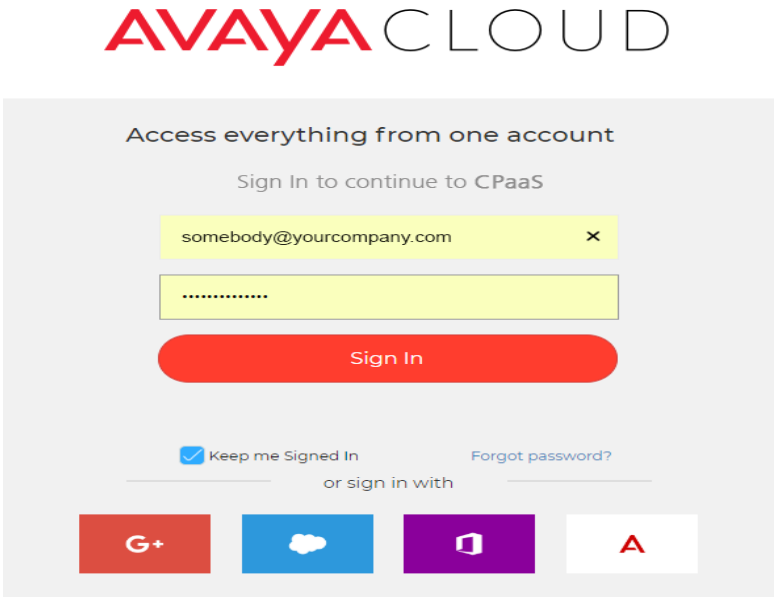
Pre-requisites

- Officelinx/IX Messaging/Messaging 10.5 or later.
- An Internet connection.
- An Avaya CPaaS account and telephone number.

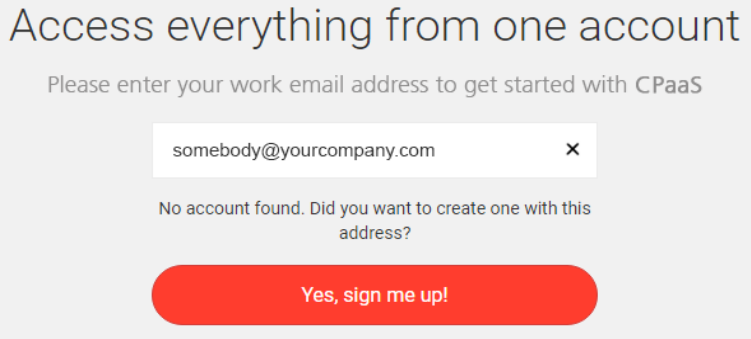
Avaya CPaaS Configuration

An account with Avaya must be setup, and a number with support for SMS messaging must be purchased from Avaya CPaaS.

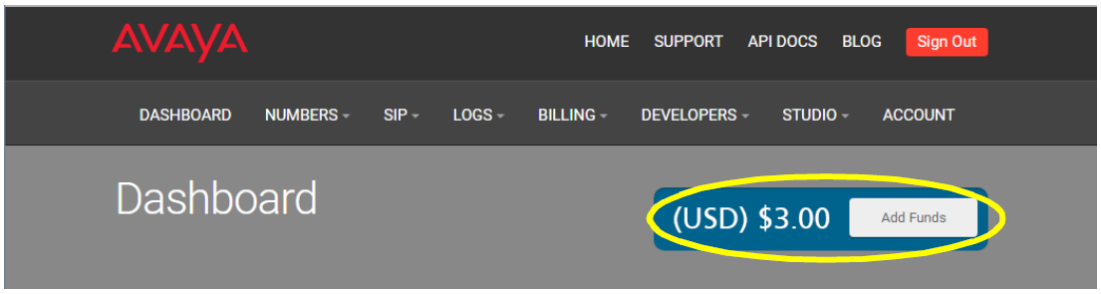
1. Open an Internet browser and go to https://cloud.zang.io/ (accounts.avayacloud.com). Enter your Avaya account credentials and click **Log In**.



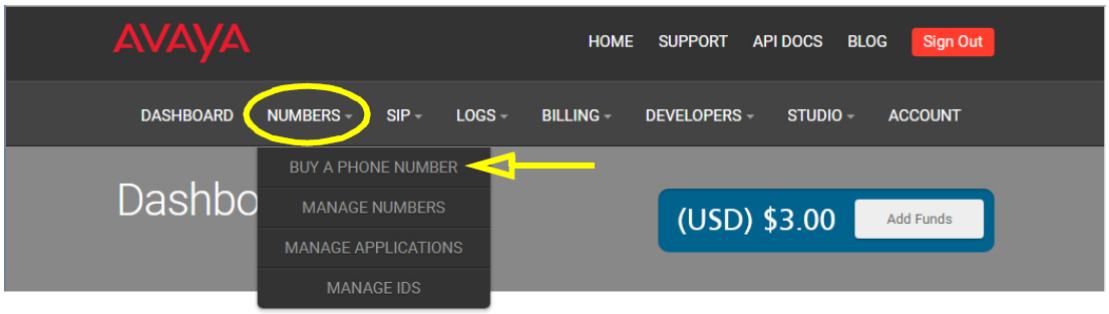
If you do not already have one, you can create a new account now. Enter your email address in the space provided, click **Yes, sign me up!** and follow the prompts to create a new account.



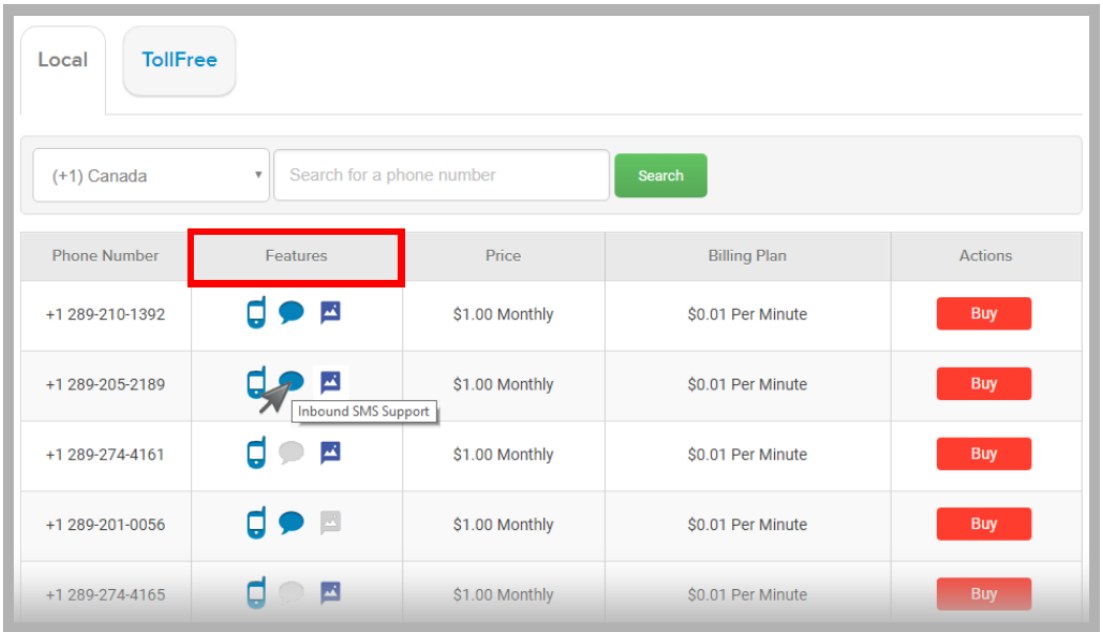
2. New accounts are given a few dollars to get started. If necessary, click **Add Funds** and add cash to your account balance. Numbers typically cost from $1 to $3 / month, depending upon the country and if it is local or toll free.



3. With your account properly funded, select **Numbers** and click **Buy a Phone Number**.

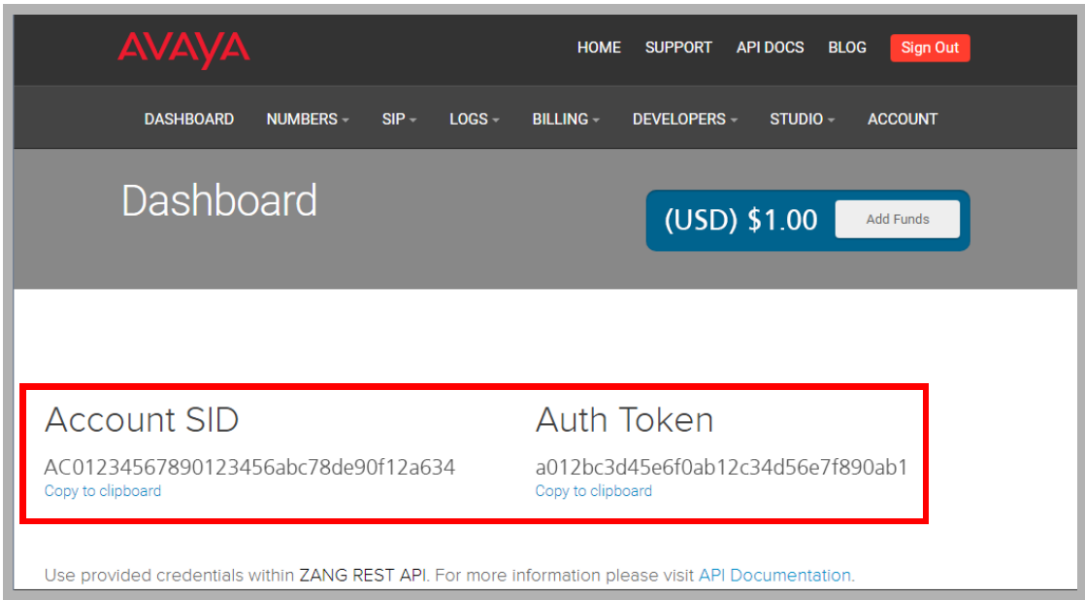


4. Choose between **Local** or **Toll-Free** numbers.
Select the **country** that will host the number. You can also enter the area / city code to narrow the search. Leave the search field empty to view all numbers available in the selected country.
When ready, click **Search** and the list of available numbers will appear.



5. Locate the number you want. For the number to work with Avaya Messaging, the number must support SMS Messaging. In the **Features** column, look for numbers that have a blue icon indicating that the number can be used with incoming SMS messages. Number with gray icons do NOT have that feature available.
   When you have located a suitable number, click **Buy** to add the number to your account.

6. From the Avaya CPaaS Dashboard, record the **Account SID** and the **Auth Token** values.

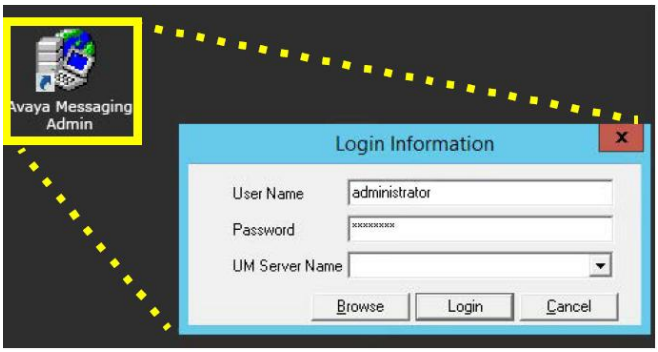


Continue with the configuration of Avaya Messaging.

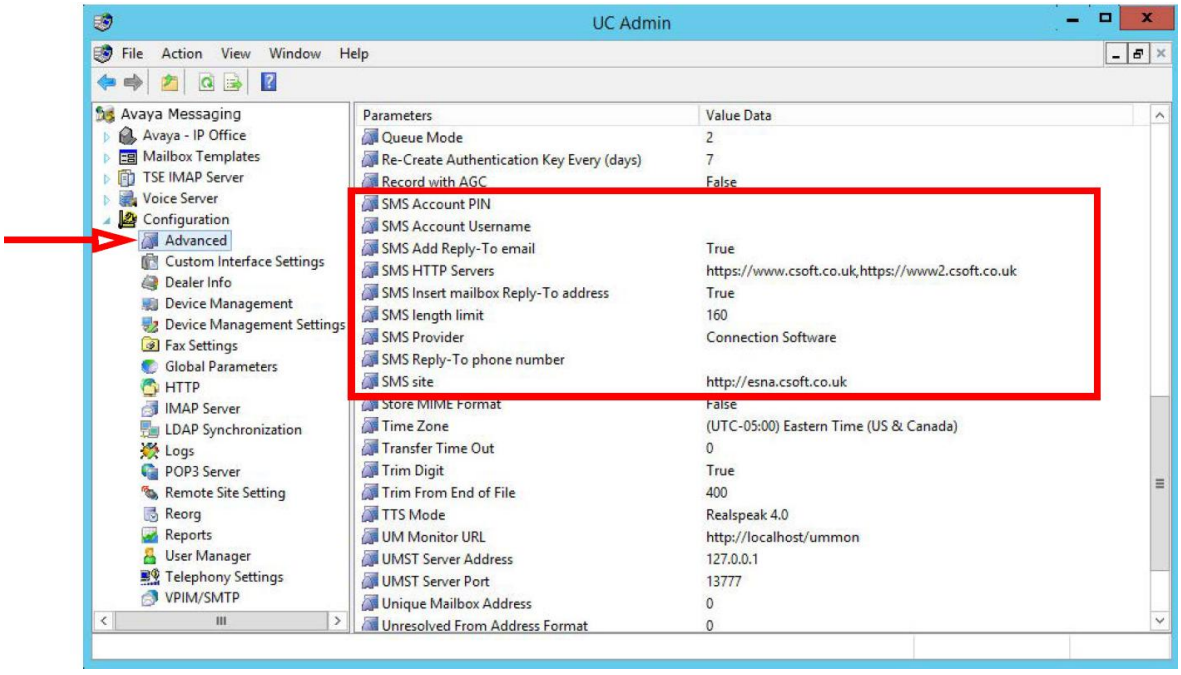
Avaya Messaging Voice Server Configuration

The configuration of Avaya Messaging is done using the Avaya Messaging Admin program on the Voice Server. In a High Availability environment, the configuration is done on the Consolidated Server only.

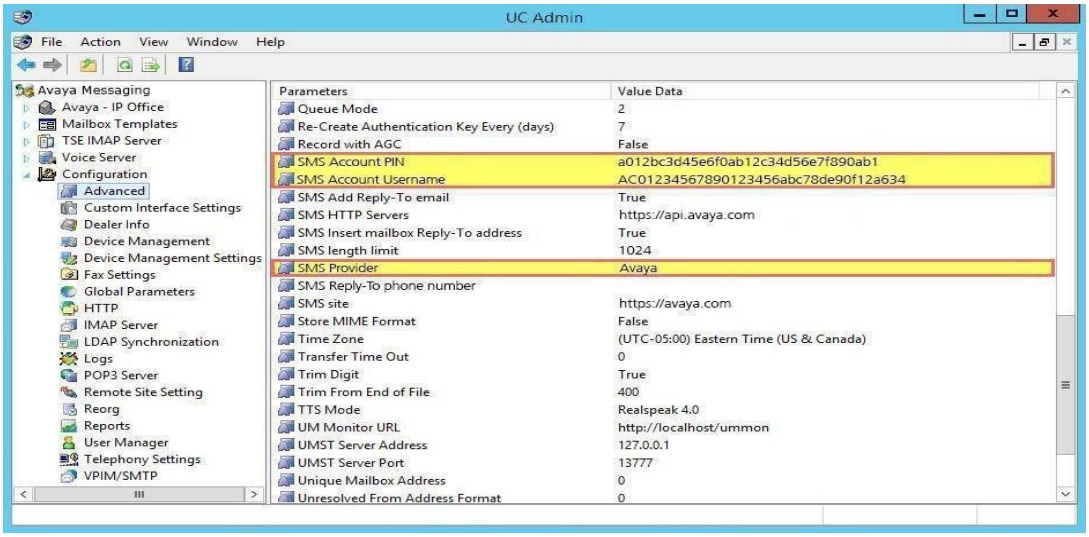
1. On the Avaya Messaging Voice Server, or the HA Consolidated Server, open **Avaya Messaging Admin,** and login.



2. Go to **Configuration > Advanced** and scroll down to the SMS options.



3. Make the following configuration changes. For each entry, double-click the item and modify the details where necessary.



- **SMS Provider**: From the dropdown menu, select **Avaya**. Most of the other fields should be filled in automatically.
- **SMS Account Username**: Enter the **Account SID** of your Avaya CPaaS account.
- **SMS Account PIN**: Enter the **Auth Token** of your Avaya CPaaS account.

Avaya Messaging User Configuration

The Avaya CPaaS telephone number must be associated with a user's mailbox to ensure that the SMS messages are delivered correctly. There are four methods that you can use. Some require changing the user mailbox through Avaya Messaging Admin, others need an INI file to route incoming messages, and two require the sender to include additional addressing details in the body of the message.

Pick the one that best matches your needs.

One-to-one:

Personal number / **Direct number**: Each user has their own dedicated Avaya CPaaS telephone number.

Any-to-many

Mailbox / **Keyword**: Your company has one or more Avaya CPaaS telephone numbers, each supporting many users.

METHOD	MODIFY MAILBOX	INI FILE ENTRY	SENDER ADDRESSING
Personal number	✓		
Direct number		✓	
Mailbox			✓
Keyword		✓	✓

One-to-one

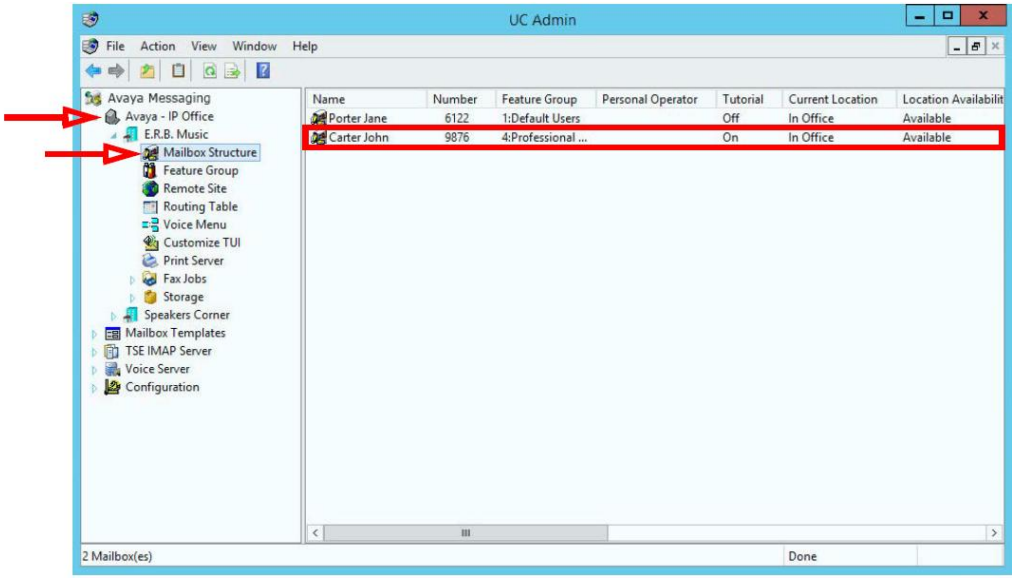
Use one of these methods if each user has exclusive use of a Avaya CPaaS telephone number.



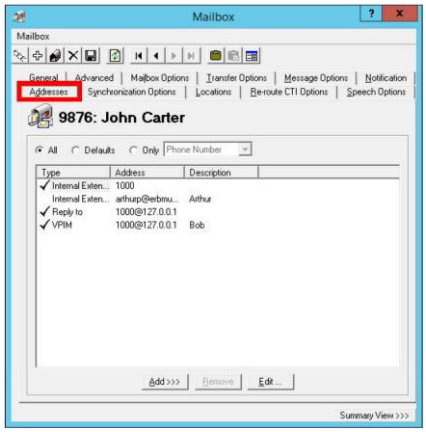
Personal number

Associating the number with the mailbox is done by modifying the user profile in Avaya Messaging Admin. No INI file entry or additional Sender Addressing is required.

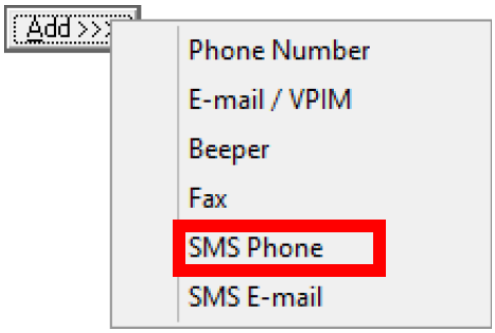
1. In Avaya Messaging Admin, open the **PBX** and go to the **Company** menu. Select **Mailbox Structure**.



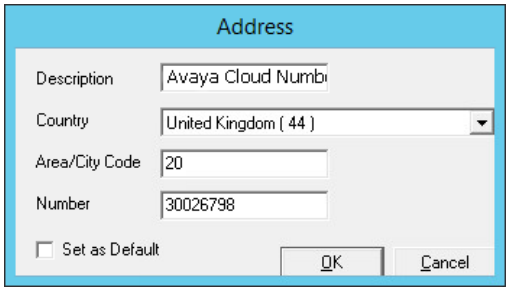
2. Double-click a user and open the **Addresses** tab.



3. Click **Add** and choose **SMS Phone**.

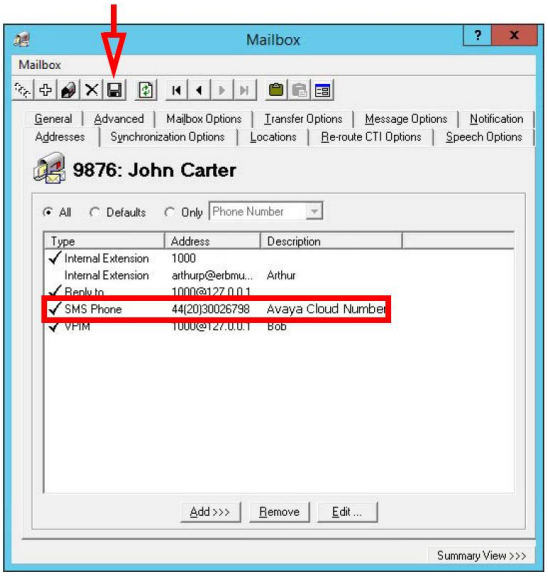


4. Enter the required information and click **OK** when ready.



- **Description**: Give this address a label.
- **Country**: From the dropdown menu, select the country that this number applies to.
- **Area/City Code**: Enter the city or area code for this number.
- **Number**: Enter the Avaya CPaaS telephone number here.
- **Set as Default**: This field should be disabled.

5. The new address has been added to the user. Click **Save**.



All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to this user's mailbox.

Direct number

Associating the number with the mailbox is done through the INI file.
No additional Sender Addressing or changes to the user profile are required.

1. Open a text editing software program such as Windows Notepad and create/modify the INI file.
2. Each person using **Direct number** must have an entry in the INI file, and each entry contains four elements.

```
[Application1]
Number= 1(905)707-9700
Mailbox= 9876
Company= 1

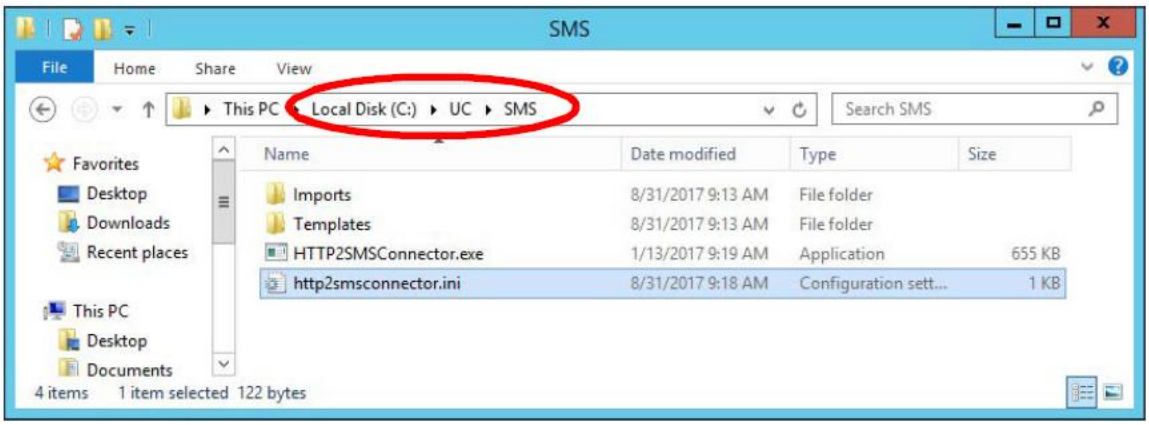
[Application2]
Number= 1(905)707-9170
Mailbox= 9877
Company= 1
```

• **[ApplicationX]**: This is an incrementing label, ApplicationX, where X is a unique identifier for each user (i.e., [Application1] , [Application2] , etc.). There are no spaces in this title, and it must be enclosed in square brackets.
• **Number=** : Specify the Avaya CPaaS telephone number for the recipient. This is where the sender addresses the message.

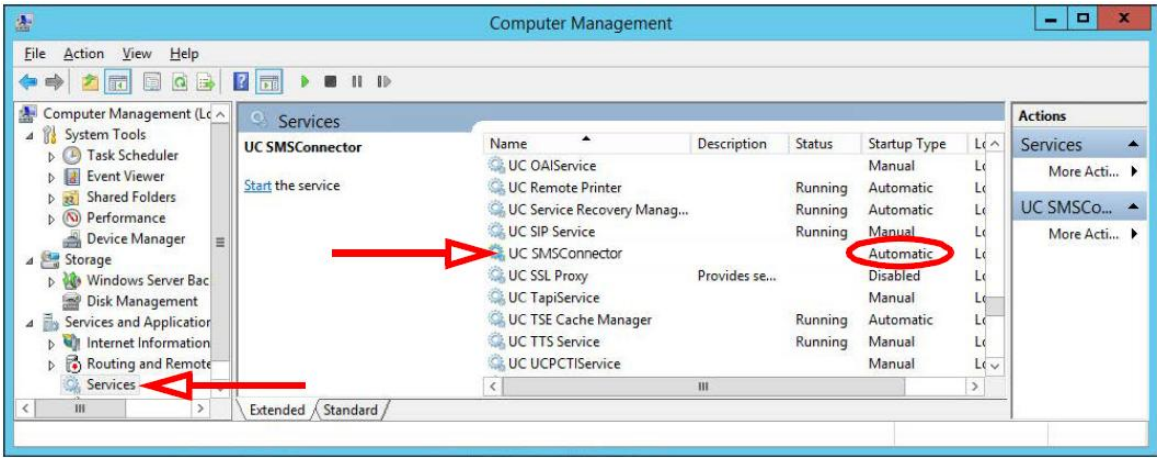
Caution: The number in an incoming message must match this value exactly or the message cannot be delivered.

• **Mailbox=** : Enter the mailbox for the recipient. The incoming SMS message will be delivered here.
• **Company=** : For sites that have multiple tenants / companies, enter the company number for this user here. This value must match the company numbers defined on the Avaya Messaging voice server. In most cases, where there is only a single company using the server, set this value to 1.

3. Once all users have been added, save the file with the name: http2smsconnector.ini. Save it on the Avaya Messaging Voice Server installation drive in the UC/SMS folder.



4. Stop and re-start the **UC SMSConnector** service on the Voice Server, or reboot the server. This service should also be configured to start automatically.



Note: You can combine both **Direct number** and **Keyword** entries in the same INI file. Only the information in each entry will change.

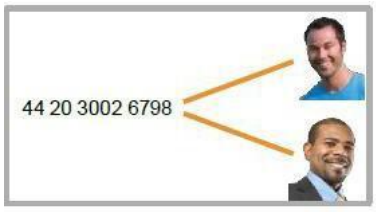
```
[Keyword1]
Value= ASKJohnC,JohnC
Mailbox= 9876
Company= 1

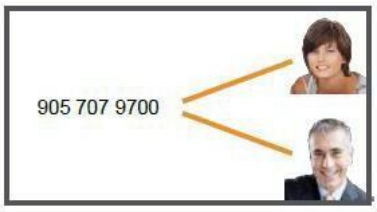
[Application1]
Number= 1(905)707-9700
Mailbox= 9876
Company= 1
```

All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to the user's mailbox defined in the INI file.

Any-to-many

Use one of these methods if your company has one or more Avaya CPaaS telephone numbers with many people using each one.





Mailbox

The sender must begin the message with ## followed by the mailbox number of the recipient. This mailbox must be followed by Space or Enter.
Associating the number with the mailbox is done explicitly by the sender within the body of the message. No INI file entry or changes to the user profile are required.



All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to the user's mailbox is based upon the value that the sender includes within the body of message.

Keyword

A unique Keyword is used to identify the recipient of the message.
Associating the number with the mailbox requires both addressing within the body of the message and an entry in the INI file.
No changes to the user profile are required.

1. Open a text editing software program such as Windows Notepad and create/modify the INI file.
2. Each person using **Keyword** must have an entry in the INI file, and each entry contains four elements.

```
[Keyword1]
Value= ASKJOHNC,JOHNC
Mailbox= 9876
Company= 1

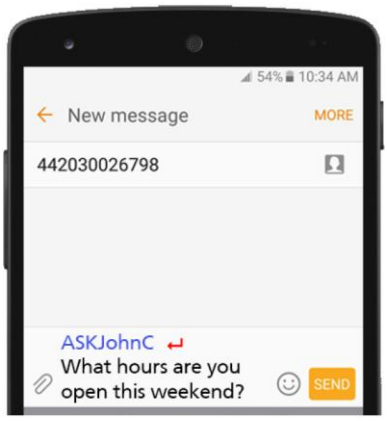
[Keyword2]
Value= ASKALF,ALANF
Mailbox= 9877
Company= 1
```

[KeywordX]: This is an incrementing label, KeywordX, where X is a unique identifier for each user (i.e., [Keyword1], [Keyword2] , etc.). There are no spaces in this title, and it must be enclosed in square brackets.
• **Value=** : Specify the unique keyword that identifies the recipient. Multiple keywords can be included if they are separated by a comma. This keyword must be included in the body of the

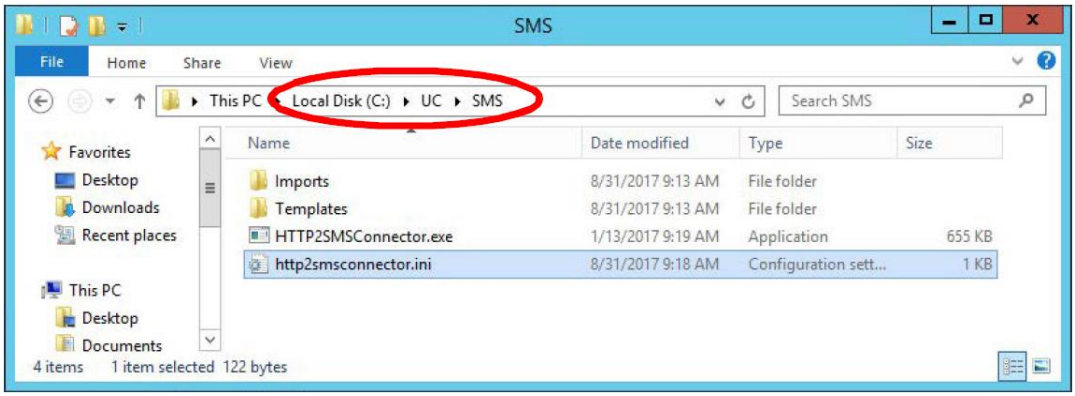
message as the first item, followed by Space or Enter.
Caution: Keyword values are case sensitive. The keyword in an incoming message must match this value exactly or the message cannot be delivered.

• **Mailbox=** : Enter the mailbox for the recipient. The incoming SMS message will be delivered here.

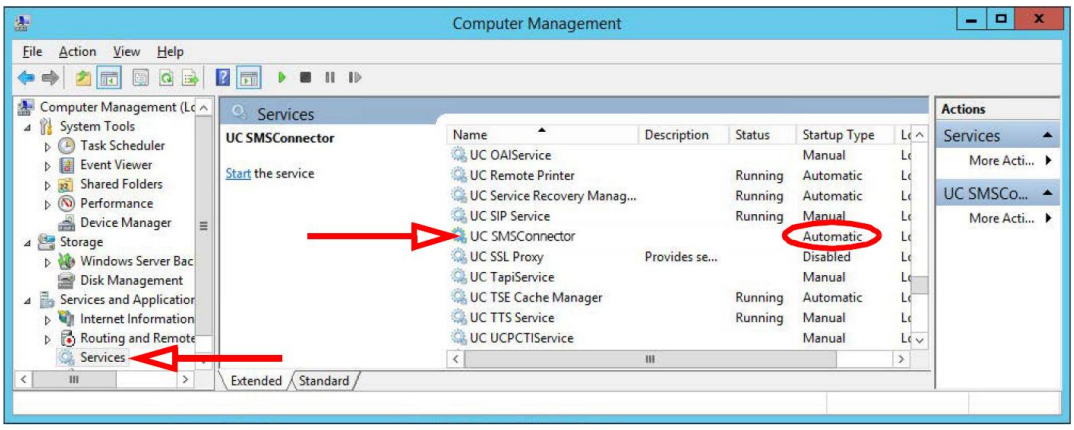
• **Company=** : For sites that have multiple tenants / companies, enter the company number for this user here. This value must match the company numbers defined on the Avaya Messaging Voice Server. In most cases, where there is only a single company configured, set this value to **1**.



3. Once all users have been added, save the file with the name: http2smsconnector.ini
Save it on the Avaya Messaging Voice Server installation drive in the UC/SMS folder.



4. Stop and restart the **UC SMSConnector** service on the Voice Server or reboot the server.
This service should also be configured to start automatically.



All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to the user's mailbox using both the addressing within the body of the message and the entry within the INI file.

Note: You can combine both **Keyword** and **Direct number** entries in the same INI file. Only the information in each entry will change.

```
[Keyword1]
Value= ASKJohnC,JohnC
Mailbox= 9876
Company= 1

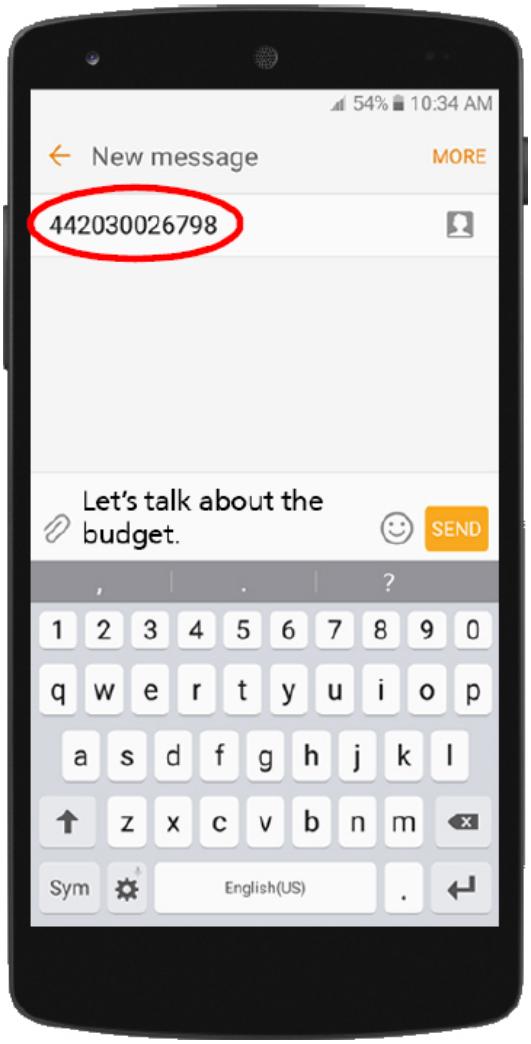
[Application1]
Number= 1(905)707-9700
Mailbox= 9876
Company= 1
```

Addressing SMS Messages

Once the Avaya CPaaS telephone number has been purchased and Avaya Messaging configured to use it, messages sent to that number will be received in the recipient's inbox.
Contacts wishing to send a message to the user address it to the Avaya CPaaS telephone number. Additional addressing by the sender may be required.

Personal number

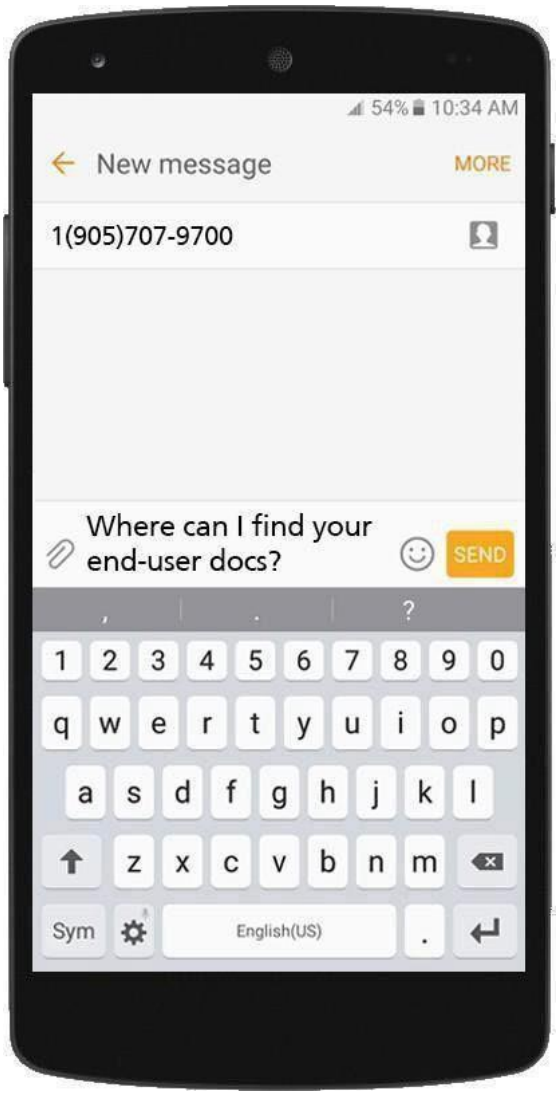
The sender only needs to provide the number (e.g., **442030026798**) to address the message.



The Voice Server spots the telephone number and uses the Avaya Messaging Admin Addresses tab to direct the message to the correct mailbox.

Direct number

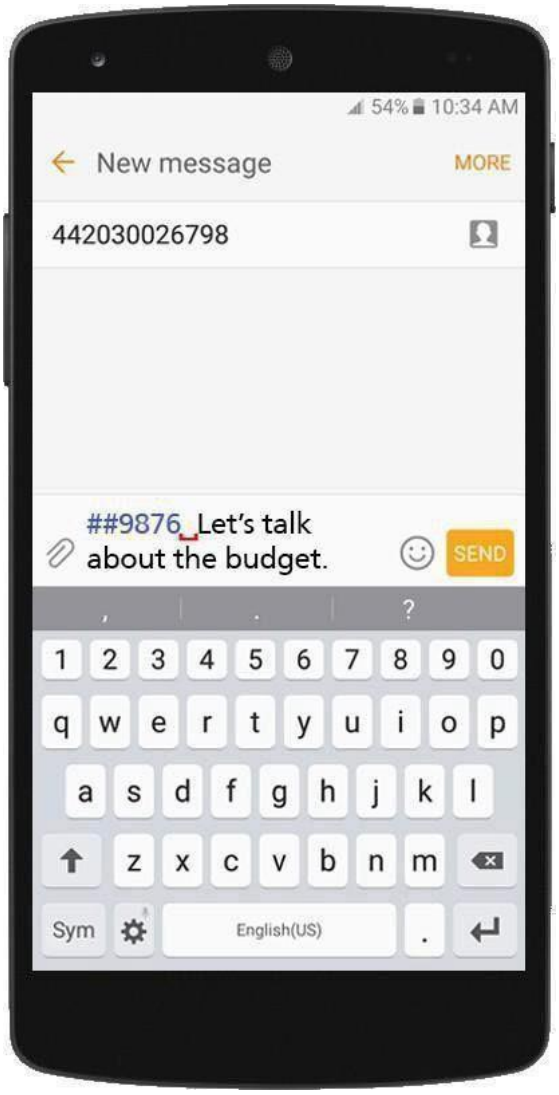
Enter the recipient's Avaya CPaaS telephone number (e.g., 1(905)707-9700) exactly as it is configured in the INI file.



The Voice Server spots the telephone number and uses the INI file to direct the message to the correct mailbox.

Mailbox

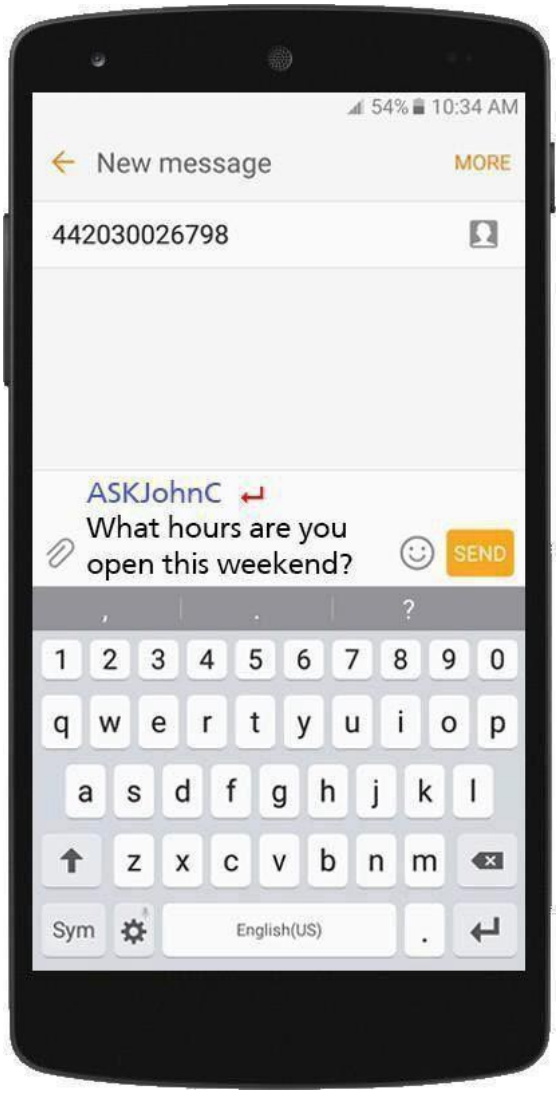
The sender must include the recipient's mailbox number in the body of the message. The number must be preceded by ## (e.g., **##9876**).



The **##** marker tells the server that the number that follows is the extension of the recipient and the message is delivered accordingly.

Keyword

The sender must include the keyword exactly as it is configured for that user in the INI file (e.g., ASKJohnC). The keyword is case sensitive.



The Voice Server spots the keyword and uses the INI file to direct the message to the correct mailbox.

Chapter 23: ACCESSIBILITY

Introduction

Avaya Messaging provides greater accessibility to people with special needs. Avaya Messaging offers 508 compliance and TTY integration.

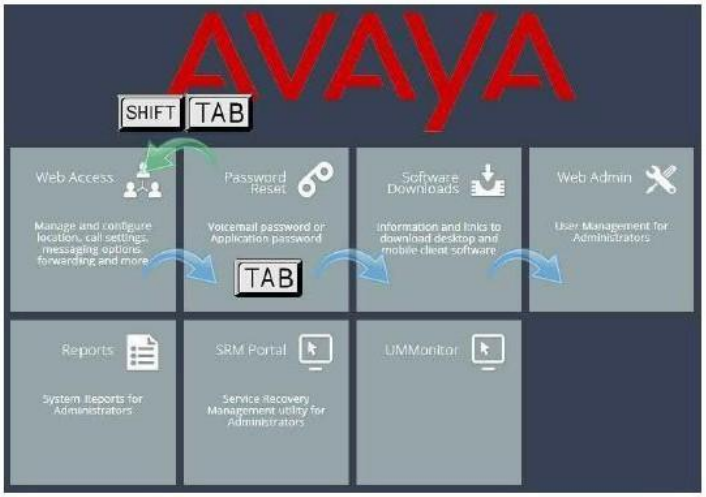
508 Compliance

Complying with the 508 standards in Avaya Messaging means that the user interface for a program must be usable to clients without the use of a mouse. The user interface for launching and navigating through the Web Access program provides access to all areas using the keyboard alone.

The keyboard commands are shown here:

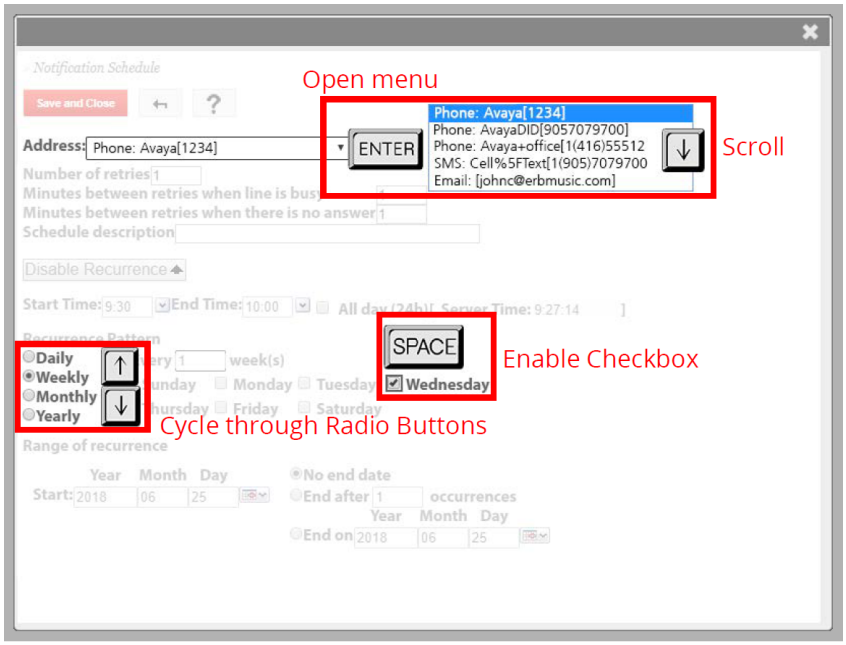
KEYSTROKE	FUNCTION
TAB	Skip to next item.
SHIFT + TAB	Return to the previous item.
ENTER or SPACE	Enable or Select the current item.
→ ←	Expand / Collapse menus.
↑ ↓	Scroll Up and Down within a menu. Toggle the current radio button.

The login, splash screen and Web Access interface are all 508 compliant.


AVAYA
SHIFT
TAB
Web Access
Manage and configure location, call settings, messaging options, forwarding and more
Password Reset
Voicemail password or Application password
TAB
Software Downloads
Information and links to download desktop and mobile client software
Web Admin
User Management for Administrators
Reports
System Reports for Administrators
SRM Portal
Service Recovery Management utility for Administrators
UMMonitor


UC Sign In
Select authentication provider
SHIFT
TAB
TAB
Google
Office 365
Windows
UC



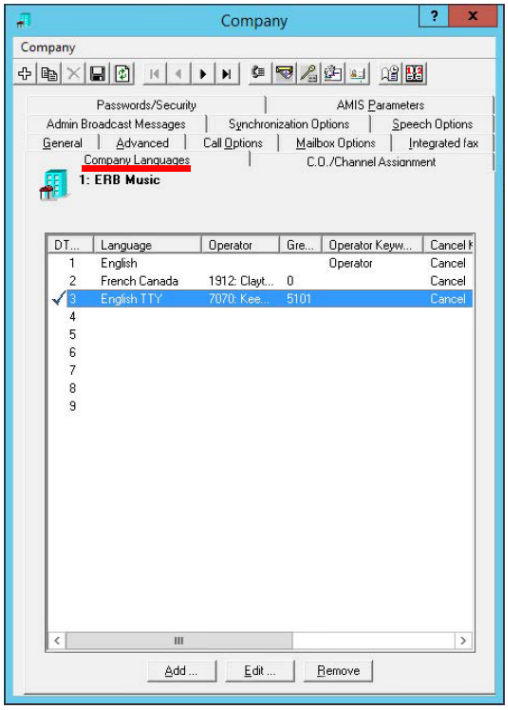


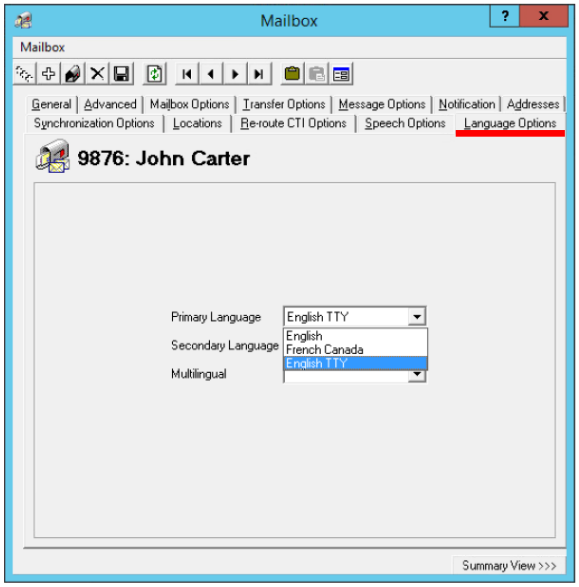
TTY Integration

Avaya Messaging includes support for TTY devices on your corporate voicemail system. TTY compatibility is provided through a language pack which can be downloaded from **PLDS**.

Install the language pack according to the instructions found in chapter *Language Pack Installation* of the *Server Installation Guide*.

Once the language pack for **TTY English** has been installed, it can be chosen as the default language for your company and for each user's mailbox.





Hint: It is recommended that a separate telephone number be used for the company for TTY language prompts. This prevents TTY callers from getting no response on their device from a voice-enabled system, and hearing callers receiving unintelligible signals on their handset from the TTY service.

Voice Recordings and TTY

The TTY system automatically converts system prompts into signals compatible with TTY devices. However, voice recordings made on-site cannot be converted.

To build greetings that appear on TTY devices, the greeting must be typed into a software program that converts the text into a TTY compatible audio format, which is then saved as a WAV file. These audio files can then be uploaded into Avaya Messaging to replace the voice recordings for that company with TTY prompts.

Note: It is recommended that the TTY feature be used only with shorter messages and prompts, such as for managing your mailbox and for internal transfers. For use with longer texts, such as with the Telephone User Interface (TUI), using Avaya Messaging Web Access is preferred.