AVAYA MESSAGING™

Feature Description Guide

Release 11.0
Issue 11
29 June, 2022

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 feature 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.

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 mediums which may include product information, 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 User agrees 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You 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 SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON

BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named
User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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, and 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. Note, unless otherwise stated, that 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https:// support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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.

Trademarks

AVAYA MESSAGING FEATURE DESCRIPTION GUIDE

Table of Contents

1 AUTOMATIC SPEECH RECOGNITION (ASR)

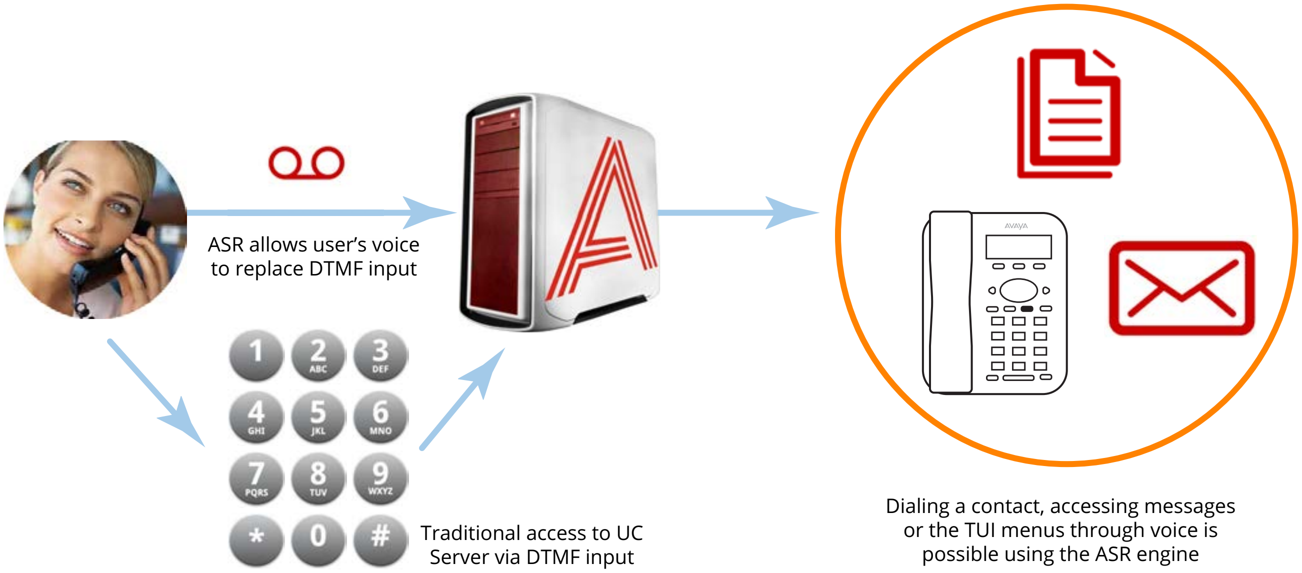
In This Chapter:

Introduction

Automatic Speech Recognition (ASR) is a vital component of the UC system. ASR allows the system to recognize human speech, so that users to 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 allows user's voice to replace DTMF input

Traditional access to UC Server via DTMF input

Dialing a contact, accessing messages or the TUI menus through voice is possible using the ASR engine

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 give 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 8.0 - 10.8 Avaya Messaging version 11.0 or higher

Server Configuration

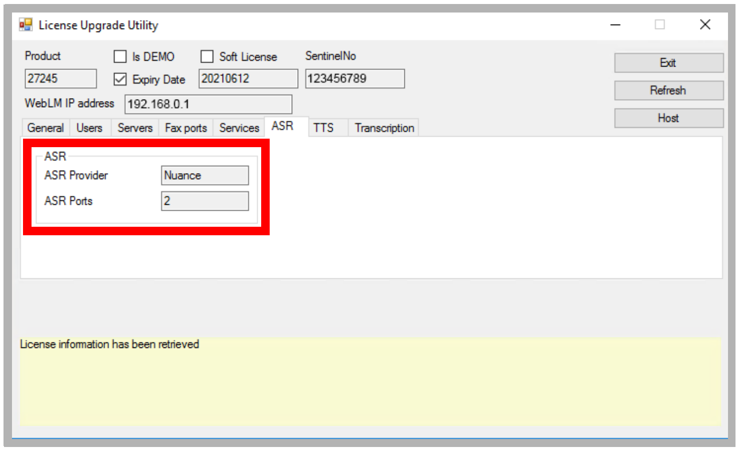
Server configuration for ASR is completed in several steps.

First, verify the Avaya Messaging license that you have. In order 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.

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.



Product: 27245
☐ Is DEMO
☑ Expiry Date: 20210612
☐ Soft License
SentinelNo: 123456789
WebLM IP address: 192.168.0.1

ASR
ASR Provider: Nuance
ASR Ports: 2

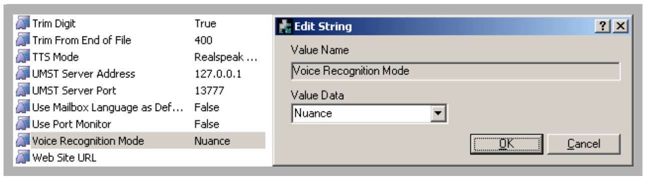
License information has been retrieved

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.

Avaya Messaging Admin Configuration



Trim Digit	True
Trim From End of File	400
TTS Mode	Realspeak ...
UMST Server Address	127.0.0.1
UMST Server Port	13777
Use Mailbox Language as Def...	False
Use Port Monitor	False
Voice Recognition Mode	Nuance
Web Site URL	

Edit String

Value Name: Voice Recognition Mode

Value Data: Nuance

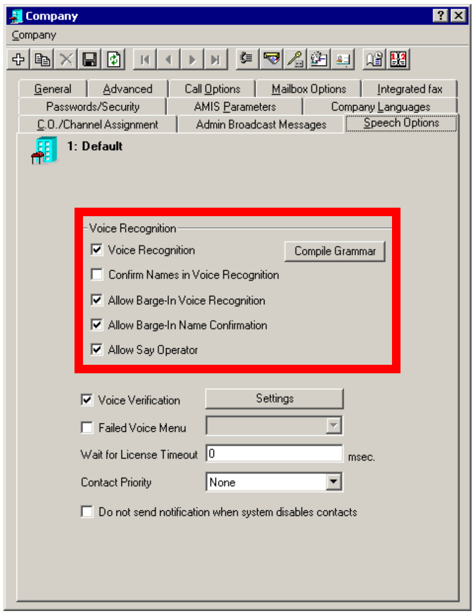
1. Open Avaya Messaging Admin and go to **Configuration > Advanced**. In the right pane, set **Voice recognition mode** to Nuance.
2. Once this option has been set, go to **Company Properties**.
3. Right-click on the company that will use ASR. Choose **Properties**.
4. Go to the **Speech Options** tab 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

1: Default

Voice Recognition

☑ Voice Recognition

☐ Confirm Names in Voice Recognition

☑ Allow Barge-In Voice Recognition

☑ Allow Barge-In Name Confirmation

☑ Allow Say Operator

☑ Voice Verification

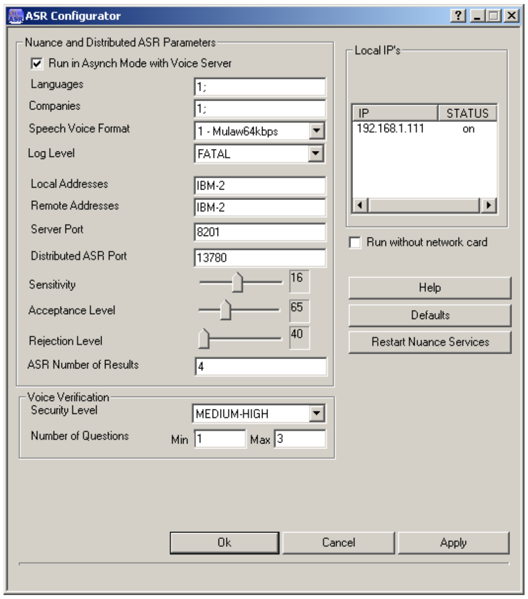
☐ Failed Voice Menu

Wait for License Timeout: 0 msec.

Contact Priority: None

☐ Do not send notification when system disables contacts

ASR Configurator



ASR Configurator

Nuance and Distributed ASR Parameters

☑ Run in Asynch Mode with Voice Server

Languages	1;
Companies	1;
Speech Voice Format	1 - Mulaw64kbps
Log Level	FATAL
Local Addresses	IBM-2
Remote Addresses	IBM-2
Server Port	8201
Distributed ASR Port	13780
Sensitivity	16
Acceptance Level	65
Rejection Level	40
ASR Number of Results	4

Voice Verification

Security Level	MEDIUM-HIGH
Number of Questions	Min 1 Max 3

Local IP's

IP	STATUS
192.168.1.111	on

□ Run without network card

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 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:

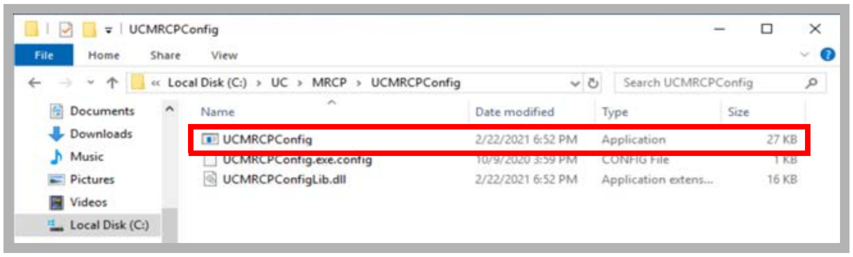
Security Level	Typical Usage Recommendation	FA Rate
Very-High	Access to mailbox accounts with critical information	0.1Internet to 0.2Internet
High	Access to mailbox accounts with high privilege	0.2Internet to 1.5Internet
Medium-High	Access to typical mailbox accounts	1.5Internet to 3Internet
Medium	Access 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

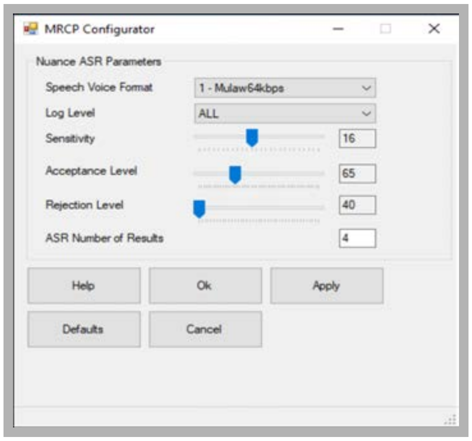
The ASR feature should work well immediately after installation. However, if there are issues with the feature, such as excessive requests to “Please repeat that”, the administrator can adjust the program settings.

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



Name	Date modified	Type	Size
UCMRCPConfig	2/22/2021 6:52 PM	Application	27 KB
UCMRCPConfig.exe.config	10/9/2020 3:59 PM	CONFIG File	1 KB
UCMRCPConfigLib.dll	2/22/2021 6:52 PM	Application extens...	16 KB

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



Nuance ASR Parameters

Speech Voice Format: 1 - Mulaw64kbps
Log Level: ALL
Sensitivity: 16
Acceptance Level: 65
Rejection Level: 40
ASR Number of Results: 4

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 recevies 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 unuseable and stop the process.

ASR Number of Results: Specify the number of results to return (minimum **1**) when more than one directory entry is found. For example, if there are 10 John Smiths at the company, this value will limit the number of results offerred to the caller (4 by default) instead of listing all of them.

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

When ready, click **Apply**.

2 ENHANCED CALL CONTROL

In This Chapter:

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 have the ability to 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 work station or a specific telephone system. Any telephone that is capable of DTMF input will be able to send commands to the Avaya Messaging server as long as 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.

Visual Guide

Business is always on the move, so it is not always ideal to stay idle. This is true even when you're on the phone. The important call you're answering from your workstation phone may be preventing you from other tasks or being elsewhere. You could ask the caller to call you back on your cell phone or ask if it would be okay for you to call them back on the other line but this would usually break the flow of conversation and is not ideal for majority of situations.

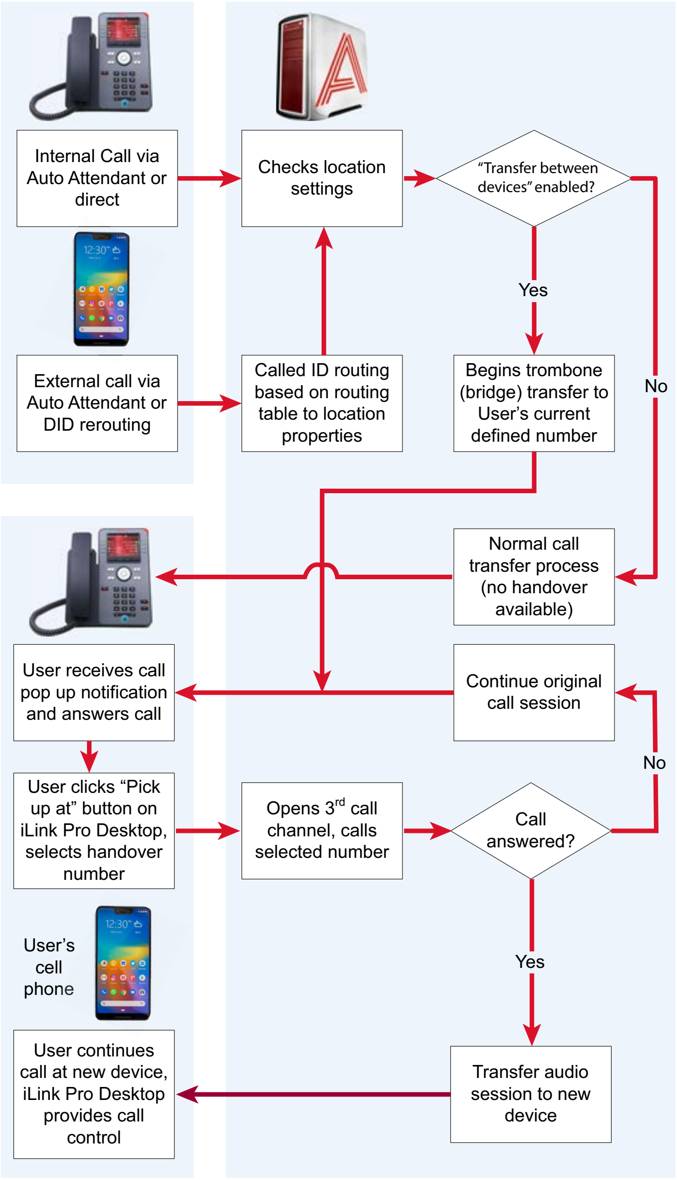
The hand off feature was added to the Avaya Messaging system to remedy such an issue. You can now seamlessly transfer your current ongoing phone call at your desk to another device (e.g. cell phone, another station, etc) without any interruption. The person you are talking to will most likely not even notice the transfer since the call is instantly connected to your second line the moment you confirm.

A call may be managed through Handoff no matter what device is being used as long as the call is managed through the Avaya Messaging system (i.e. calls are made through auto attendant). As long as such a condition is met, and the user has the permission to transfer between devices, the user may initiate a Handoff through the iLink Pro Desktop.

As you can see from the flowchart, the calls are not interrupted in any way. While traditional call transfers put the second party on hold during the transfer, there is no "buffer" required during a Handoff. The call is seamlessly transferred between the devices, and the audio stream moves from one device to another without any pauses in between. The second party is unlikely to notice that the Handoff has occurred at all.

The server is able to establish a connection by recognizing the answered status on the second device, which means that the Handoff feature automatically moves the audio stream from first device to the second automatically right after the second device answers.

Since the call is still being monitored by the system, the user is free to perform a Handoff repeatedly as long as he/she has access to the iLink Pro Desktop call control or ECC.


Internal Call via Auto Attendant or direct
Checks location settings
"Transfer between devices" enabled?
Yes
No
External call via Auto Attendant or DID rerouting
Called ID routing based on routing table to location properties
Begins trombone (bridge) transfer to User's current defined number
Normal call transfer process (no handover available)
User receives call pop up notification and answers call
Continue original call session
No
User clicks "Pick up at" button on iLink Pro Desktop, selects handover number
Opens 3rd call channel, calls selected number
Call answered?
Yes
User's cell phone
User continues call at new device, iLink Pro Desktop provides call control
Transfer audio session to new device

Requirements

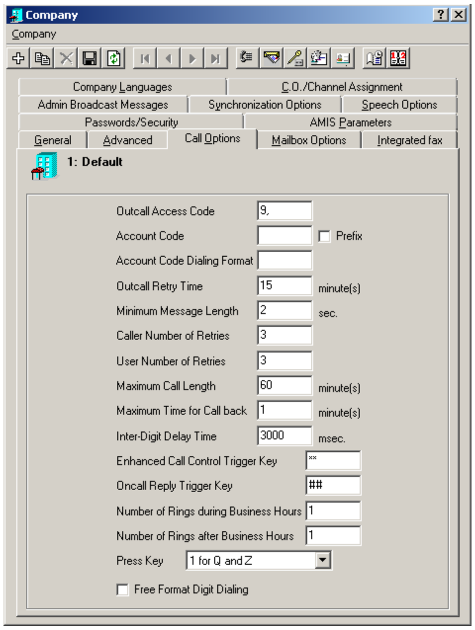
Requirements	Details
License	---
Software	Officelinx/IX Messaging version 9.0 - 10.8 Avaya Messaging version 11.0 or higher

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.

Note: Users must log out and log back into iLink Pro Desktop to access Call Handoff from the client application after you have enabled the feature.

Company



1: Default

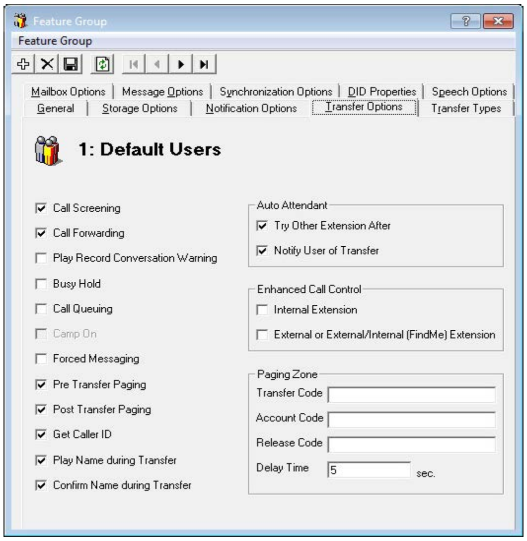
Outcall Access Code	9,	
Account Code		□ Prefix
Account Code Dialing Format		
Outcall Retry Time	15	minute(s)
Minimum Message Length	2	sec.
Caller Number of Retries	3	
User Number of Retries	3	
Maximum Call Length	60	minute(s)
Maximum Time for Call back	1	minute(s)
Inter-Digit Delay Time	3000	msec.
Enhanced Call Control Trigger Key	**	
Oncall Reply Trigger Key	##	
Number of Rings during Business Hours	1	
Number of Rings after Business Hours	1	
Press Key	1 for Q and Z	

□ Free Format Digit Dialing

From **Company> Call Options** tab, modify the **Enhanced Call CAontrol 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



1: Default Users

☑ Call Screening
☑ Call Forwarding
□ Play Record Conversation Warning
□ Busy Hold
□ Call Queuing
□ Camp On
□ Forced Messaging
☑ Pre Transfer Paging
☑ Post Transfer Paging
☑ Get Caller ID
☑ Play Name during Transfer
☑ Confirm Name during Transfer

Auto Attendant
☑ Try Other Extension After
☑ Notify User of Transfer

Enhanced Call Control
□ Internal Extension
□ External or External/Internal (FindMe) Extension

Paging Zone
Transfer Code
Account Code
Release Code
Delay Time 5 sec.

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 as long as the call is made to the user through auto attendant.

User Guide

Enhanced Call Control is meant for use on an external number. If you are at your typical location (i.e. your work station), using the telephone’s own call control or iLink Pro Desktop’s call control will be more efficient and easier. However, you will have access to this feature even on your desktop phone if the administrator has enabled it for you.

Keep in mind that pushing the right command keys is vital for Enhanced Call Control since there is no simple means to monitor the call’s status without iLink Pro Desktop. 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 by iLink Pro Desktop's Call Manager feature. Please 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

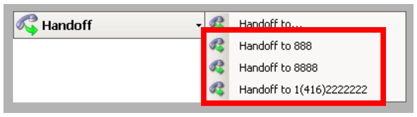
3 - Hand off the current call to another device

4 - Disconnect the other person on hold and return you to the Auto Attendant

- Disconnect the current call for both parties

Initiating a Handoff to Predefined Numbers

By default, iLink Pro Desktop will allow you to hand off the calls to numbers assigned to your current location. Select the number you wish to hand off the call to by clicking on the appropriate entry.

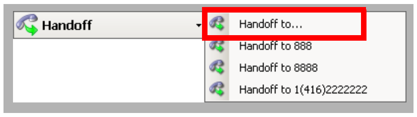


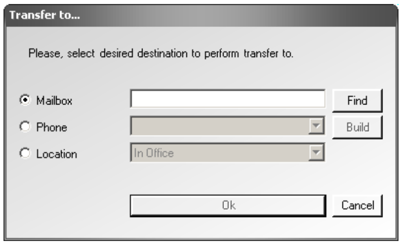
Once you initiate the handoff, the selected number will ring. When the new extension is answered, the old connection will be terminated and the conversation will continue on the new device only. You will still retain the ability to control the call from iLink Pro Desktop, which means that you can freely handoff the phone call to any destination as many times as you wish.

Initiating a Handoff to Custom Numbers

Note: You cannot handoff a call to a custom number through ECC. You may only perform this action from iLink Pro Desktop.

When you wish to handoff to a number that isn't defined under your current locations, you can choose the **Handoff to...** option then manually define the destination.





Please, select desired destination to perform transfer to.

● Mailbox
○ Phone
○ Location: In Office

Select one of the following radio buttons, then either enter or select the destination.

- **Mailbox**: Use this option to handoff the call to another mailbox. You can use the **Find** button to search for a mailbox if you do not know the number.
- **Phone**: Use this option to handoff the call to an external phone number. Clicking on build will allow you to separately define country & area codes.
- **Location**: Use this option to handoff the call to a chosen location's default number.

3 SPEECH COMMANDS

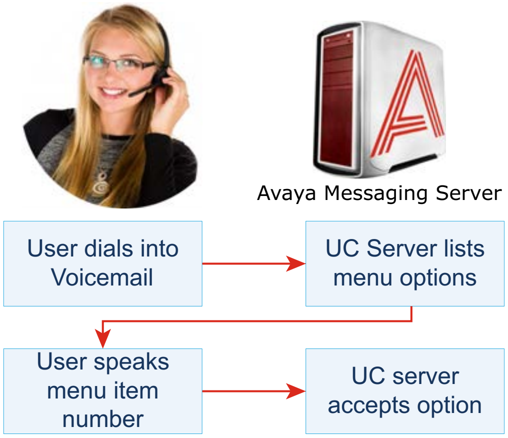
In This Chapter:

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 the Speech Command as a valid entry and performs the action associated with the number.


Avaya Messaging Server
User dials into Voicemail
UC Server lists menu options
User speaks menu item number
UC server accepts option

Requirements

Requirements	Details
License	---
Software	Officelinx/IX Messaging version 9.0 - 10.8 Avaya Messaging version 11.0 or higher

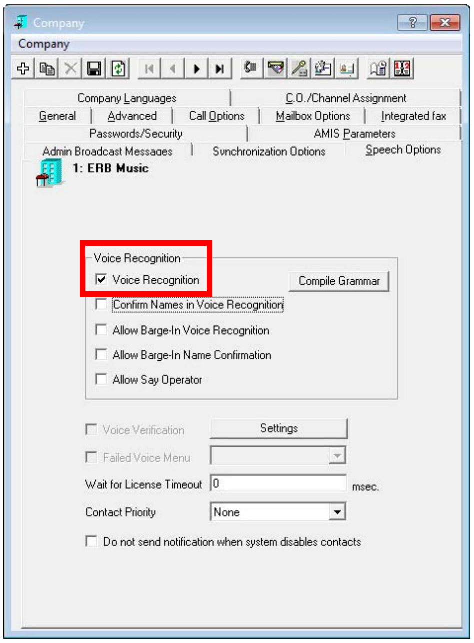
Server Configuration

In order 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.



1: ERB Music

Voice Recognition
- ☑ Voice Recognition
- □ Confirm Names in Voice Recognition
- □ Allow Barge-In Voice Recognition
- □ Allow Barge-In Name Confirmation
- □ Allow Say Operator

□ Voice Verification

□ Failed Voice Menu

Wait for License Timeout 0 msec.

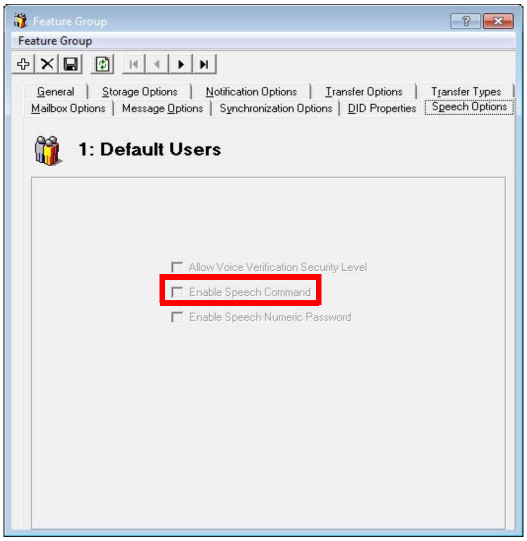
Contact Priority None

□ Do not send notification when system disables contacts

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.

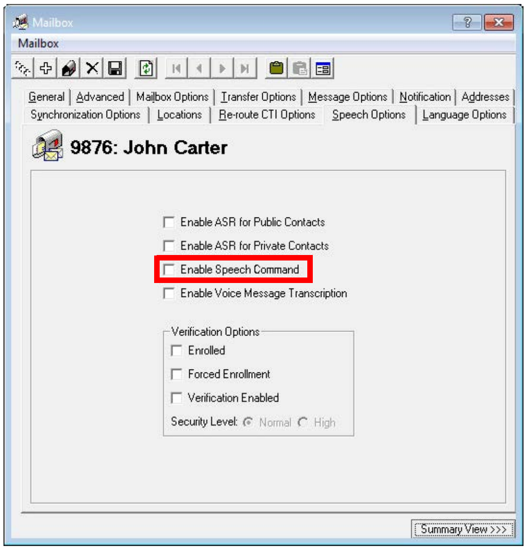


1: Default Users

- □ Allow Voice Verification Security Level
- □ Enable Speech Command
- □ Enable Speech Numeric Password

Mailbox Properties

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



9876: John Carter

□ Enable ASR for Public Contacts
□ Enable ASR for Private Contacts
□ Enable Speech Command
□ Enable Voice Message Transcription

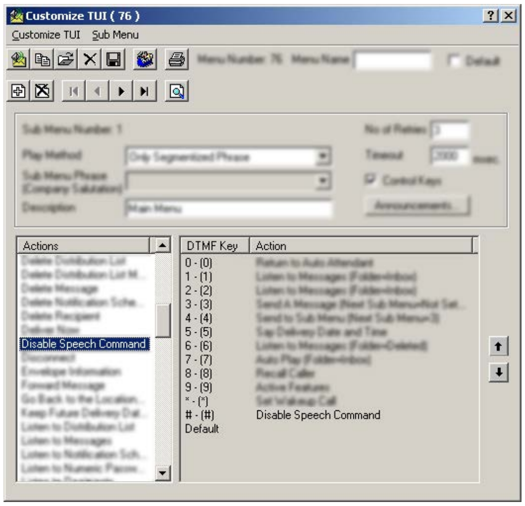
Verification Options
□ Enrolled
□ Forced Enrollment
□ Verification Enabled
Security Level: ● Normal ○ High

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 **Disable 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.



Sub Menu Number: 1
Play Method: Only Segmentized Phrase
Sub Menu Phrase (Company Salutation):
Description: Main Menu
No of Retries: 3
Timeout: 2000 msec
☑ Control Keys

Actions: Delete Distribution List, Delete Distribution List M..., Delete Message, Delete Notification Sche..., Delete Recipient, Deliver Now, Disable Speech Command, Disconnect, Envelope Information, Forward Message, Go Back to the Location..., Keep Future Delivery Dat..., Listen to Distribution List, Listen to Messages, Listen to Notification Sch..., Listen to Numeric Pacon...

DTMF Key	Action
0 - (0)	Return to Auto Attendant
1 - (1)	Listen to Messages (Folder=Inbox)
2 - (2)	Listen to Messages (Folder=Inbox)
3 - (3)	Send A Message (Next Sub Menu=Not Set...
4 - (4)	Send to Sub Menu (Next Sub Menu=3)
5 - (5)	Say Delivery Date and Time
6 - (6)	Listen to Messages (Folder=Deleted)
7 - (7)	Auto Play (Folder=Inbox)
8 - (8)	Recall Caller
9 - (9)	Active Features
* - (*)	Set Wakeup Call
# - (#)	Disable Speech Command
Default	

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 of 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 in order 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 Speech Command from time to time due to high amount of background noise. If you have the **Disable 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 disable action will vary depending on the TUI associated with your mailbox.

4 SPEECH CONTACTS

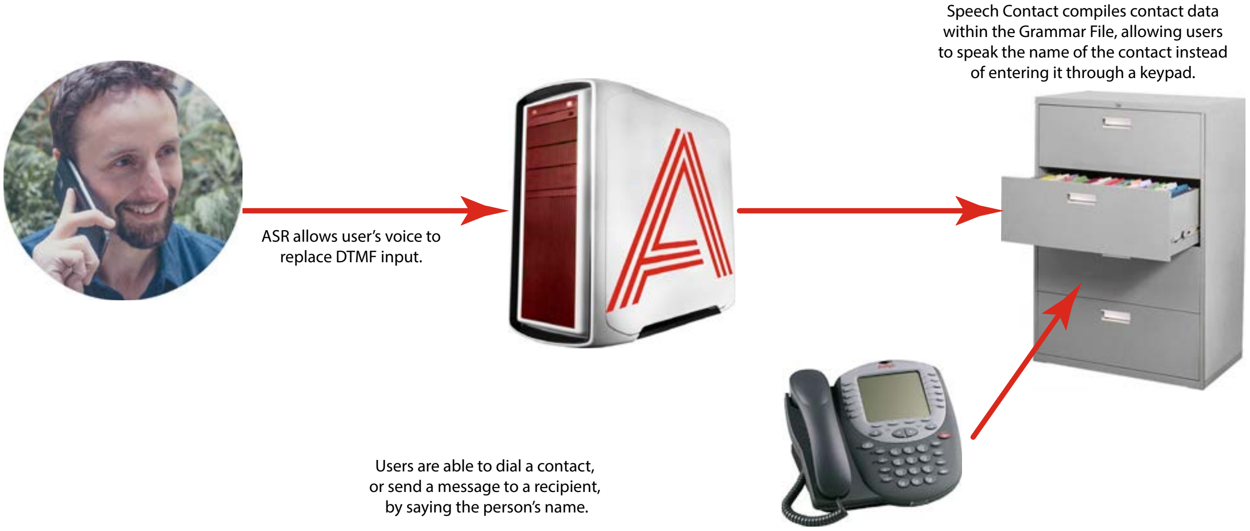
In This Chapter:

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.

In order 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


Speech Contact compiles contact data within the Grammar File, allowing users to speak the name of the contact instead of entering it through a keypad.
ASR allows user's voice to replace DTMF input.
Users are able to dial a contact, or send a message to a recipient, by saying the person's name.

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.

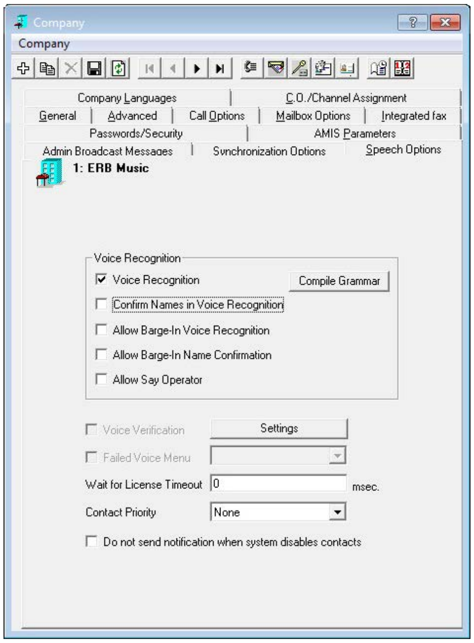
Requirements

Requirements	Details
License	ASR
Software	Officelinx/IX Messaging version 8.1 - 10.8 Avaya Messaging version 11.0 or higher

Server Configuration

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

Procedure



1: ERB Music

Voice Recognition

☑ Voice Recognition

□ Confirm Names in Voice Recognition

□ Allow Barge-In Voice Recognition

□ Allow Barge-In Name Confirmation

□ Allow Say Operator

□ Voice Verification

□ Failed Voice Menu

Wait for License Timeout 0 msec.

Contact Priority None

□ Do not send notification when system disables contacts

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 speech 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 the **Enable ASR for Public Contacts** or **Enable ASR for Private Contacts** according to the selection you have made in this dropdown list.

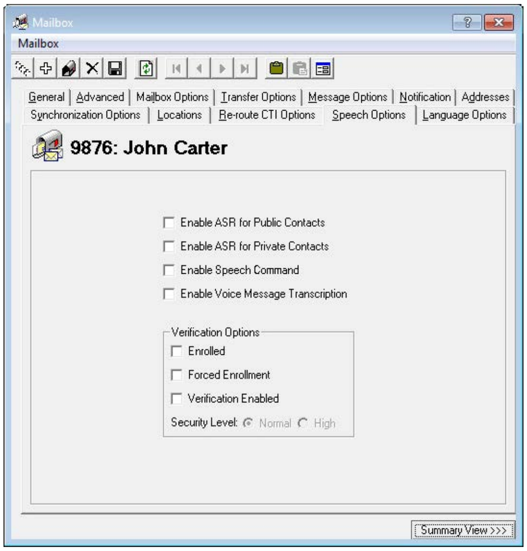
   For example, selecting **Private** in this dropdown list, and disabling **Enable ASR for Private Contacts** on the **Mailbox > Mailbox Options** screen will give priority to Public contacts.

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.



9876: John Carter

□ Enable ASR for Public Contacts

□ Enable ASR for Private Contacts

□ Enable Speech Command

□ Enable Voice Message Transcription

Verification Options

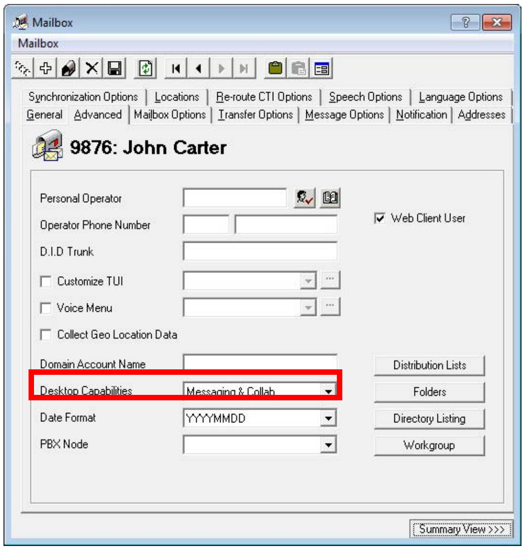
□ Enrolled

□ Forced Enrollment

□ Verification Enabled

Security Level: ● Normal ○ High

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



9876: John Carter

☑ Web Client User

Desktop Capabilities: Messaging & Collab

Date Format: YYYYMMDD

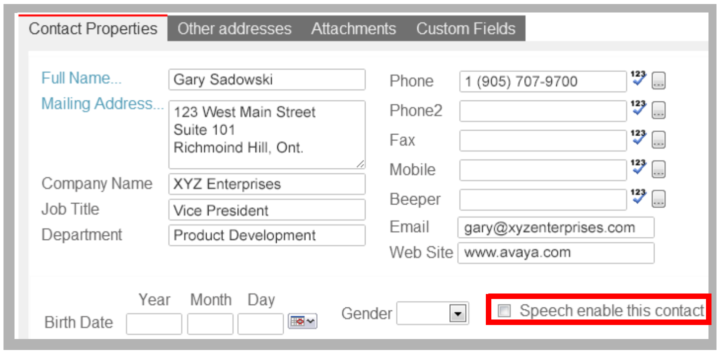
User Guide

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

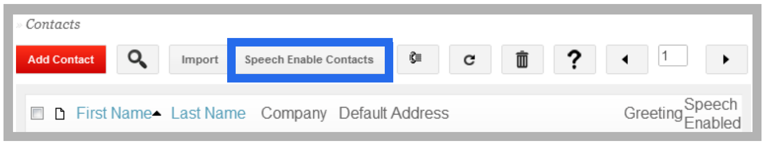
You can enable speech for your contacts individually from each contact's properties.



Full Name... Gary Sadowski
Mailing Address... 123 West Main Street
Suite 101
Richmoind Hill, Ont.
Company Name XYZ Enterprises
Job Title Vice President
Department Product Development
Phone 1 (905) 707-9700
Phone2
Fax
Mobile
Beeper
Email gary@xyzenterprises.com
Web Site www.avaya.com
Birth Date Year Month Day
Gender
□ Speech enable this contact

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.

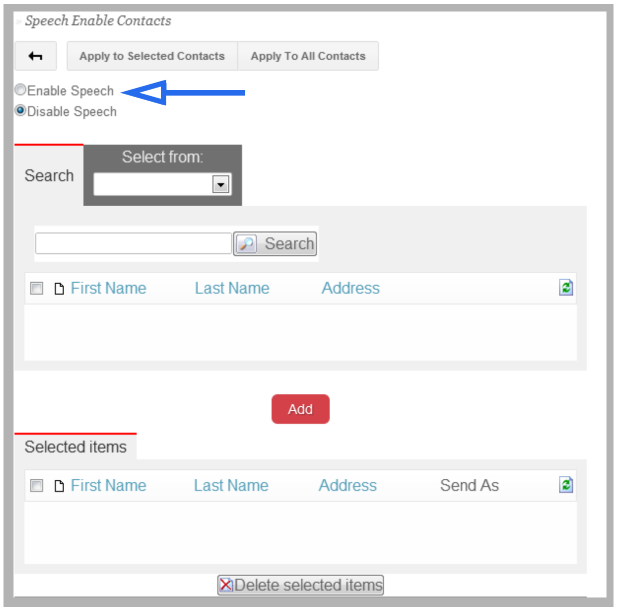


2. Select the **Enable Speech** radio button.

If you wish to enable speech for **all** of your contacts, click on the
Apply To All Contacts button.

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

1. Populate the uppermost listbox 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.
2. Add contacts from the upper listbox to the bottom by enabling the checkbox beside the contact, then clicking the **Add** button.
3. When all desired contacts have been added, click on the **Apply to Selected Contacts** button to apply the changes.



○ Enable Speech
● Disable Speech

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 enable this contact** is checked. You may freely modify individual entries by enabling or disabling this checkbox.

5 WEBLINKS

In This Chapter:

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 below process 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 networking knowledge who understands the process would be able to configure the settings necessary for your own system setup.

Also, please keep in mind that 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, which changes the interface you must configure the feature from.

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 setup 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 on **page 45**.

If the server has **IIS 6** installed, begin the process on **page 46**.

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 on **page 47**.

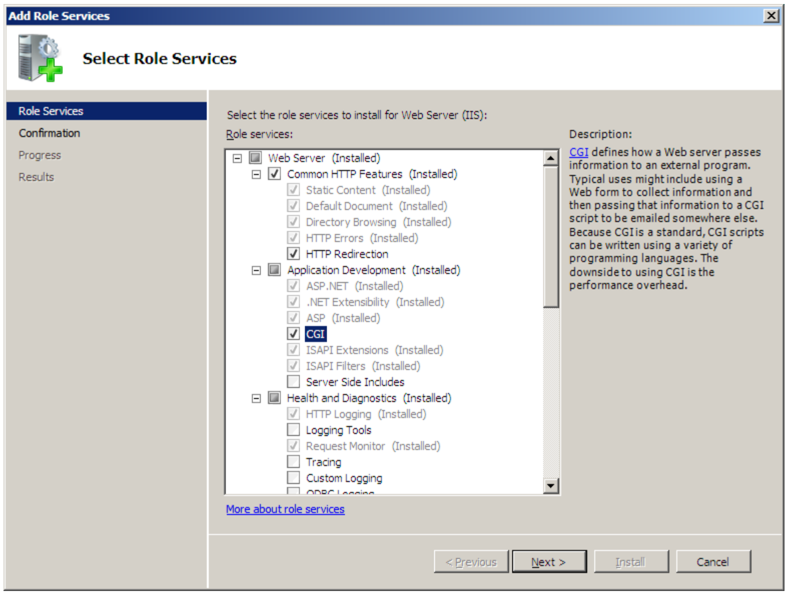
Configuration with IIS 7

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 on page 46**.

1. In order 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**.



Select the role services to install for Web Server (IIS):

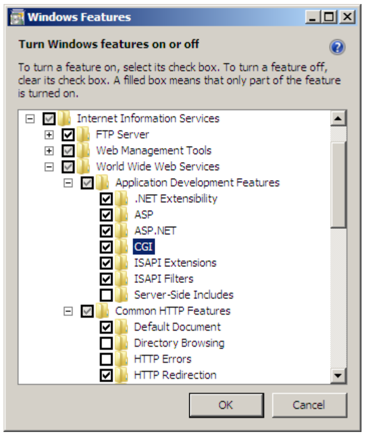
Role services:

- ▣ Web Server (Installed)
  - ☑ Common HTTP Features (Installed)
    - ☑ Static Content (Installed)
    - ☑ Default Document (Installed)
    - ☑ Directory Browsing (Installed)
    - ☑ HTTP Errors (Installed)
    - ☑ HTTP Redirection
  - ▣ Application Development (Installed)
    - ☑ ASP.NET (Installed)
    - ☑ .NET Extensibility (Installed)
    - ☑ ASP (Installed)
    - ☑ CGI
    - ☑ ISAPI Extensions (Installed)
    - ☑ ISAPI Filters (Installed)
    - ☐ Server Side Includes
  - ▣ Health and Diagnostics (Installed)
    - ☑ HTTP Logging (Installed)
    - ☐ Logging Tools
    - ☑ Request Monitor (Installed)
    - ☐ Tracing
    - ☐ Custom Logging
    - ☐ ODBC Logging

Description:

CGI defines how a Web server passes information to an external program. Typical uses might include using a Web form to collect information and then passing that information to a CGI script to be emailed somewhere else. Because CGI is a standard, CGI scripts can be written using a variety of programming languages. The downside to using CGI is the performance overhead.

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



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ▣ Internet Information Services
  - ☑ FTP Server
  - ▣ Web Management Tools
  - ▣ World Wide Web Services
    - ▣ Application Development Features
      - ☑ .NET Extensibility
      - ☑ ASP
      - ☑ ASP.NET
      - ☑ CGI
      - ☑ ISAPI Extensions
      - ☑ ISAPI Filters
      - ☐ Server-Side Includes
    - ▣ Common HTTP Features
      - ☑ Default Document
      - ☐ Directory Browsing
      - ☐ HTTP Errors
      - ☑ HTTP Redirection

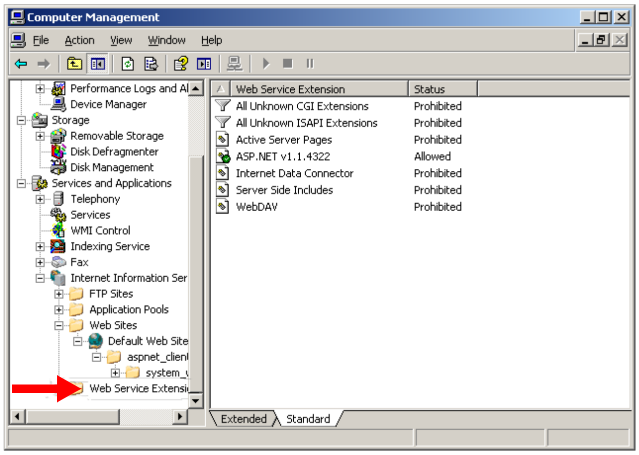
Important: Continue with the section **Avaya Messaging Configuration on page 47**.

Configuration with IIS 6

Warning: Use these instructions if have IIS 6 on your system. If you have IIS7, then use the section **Configuration with IIS 7 on page 45**.

1. Open the **Start** menu.

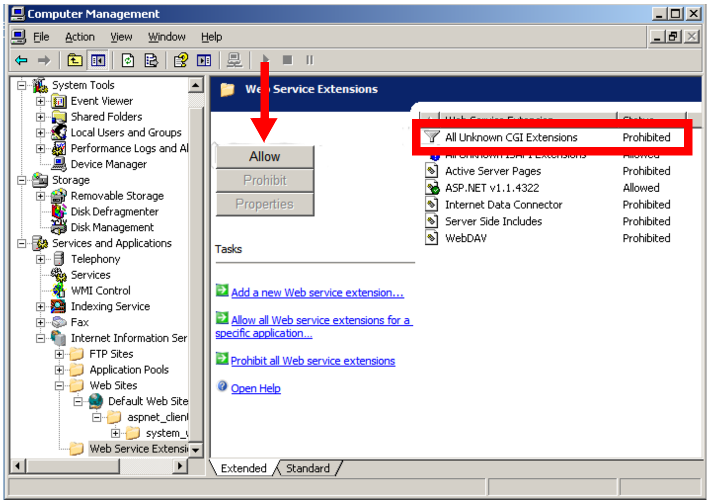
   Right-click **My Computer** then choose **Manage**.
2. On the left-hand side, select **Web Service Extensions**.



Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Prohibited
ASP.NET v1.1.4322	Allowed
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

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

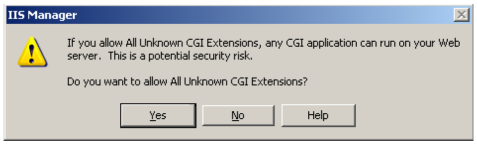
   Click on **Allow**.



All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Allowed
Active Server Pages	Prohibited
ASP.NET v1.1.4322	Allowed
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

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**.



If you allow All Unknown CGI Extensions, any CGI application can run on your Web server. This is a potential security risk.

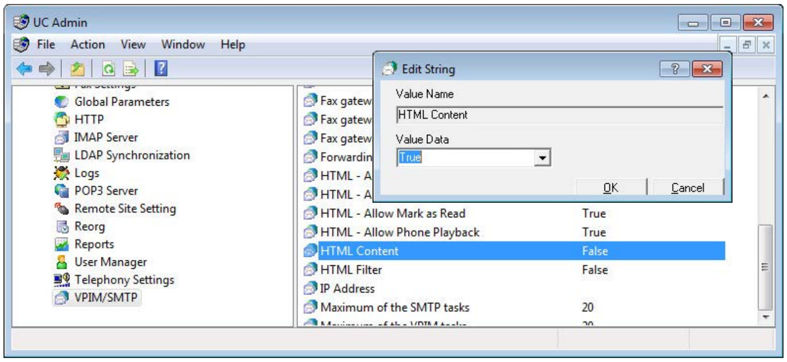
Do you want to allow All Unknown CGI Extensions?

Important: Continue with the section **Avaya Messaging Configuration on page 47**.

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**.



HTML - Allow Mark as Read	True
HTML - Allow Phone Playback	True
HTML Content	False
HTML Filter	False
IP Address	
Maximum of the SMTP tasks	20

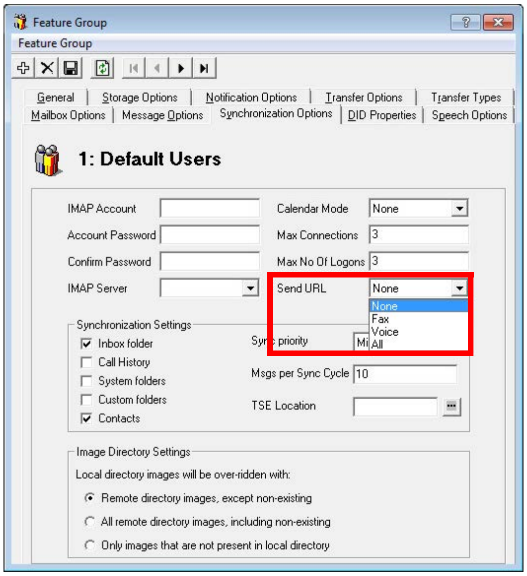
Edit String

Value Name: HTML Content

Value Data: 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.



1: Default Users

IMAP Account:

Account Password:

Confirm Password:

IMAP Server:

Calendar Mode: None

Max Connections: 3

Max No Of Logons: 3

Send URL: None

Synchronization Settings

☑ Inbox folder

□ Call History

□ System folders

□ Custom folders

☑ Contacts

Sync priority: Mi

Msgs per Sync Cycle: 10

TSE Location:

Image Directory Settings

Local directory images will be over-ridden with:

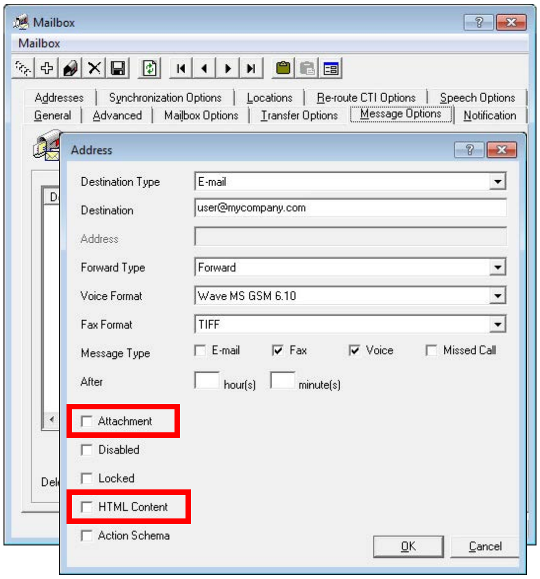
● Remote directory images, except non-existing

○ All remote directory images, including non-existing

○ Only images that are not present in local directory

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 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.



Destination Type: E-mail

Destination: user@mycompany.com

Address:

Forward Type: Forward

Voice Format: Wave MS GSM 6.10

Fax Format: TIFF

Message Type: □ E-mail ☑ Fax ☑ Voice □ Missed Call

After: hour(s) minute(s)

□ Attachment

□ Disabled

□ Locked

□ HTML Content

□ Action Schema

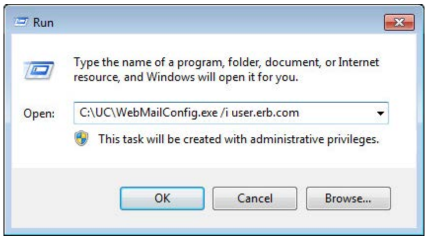
Warning: Please keep in mind that this step is **only for users who will be using email forwarding instead of IMAP CSE Synchronization**. If you configure forwarding for users who are using IMAP CSE Synchronization, there will be an infinite loop of messages. You should either use IMAP sync or forwarding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

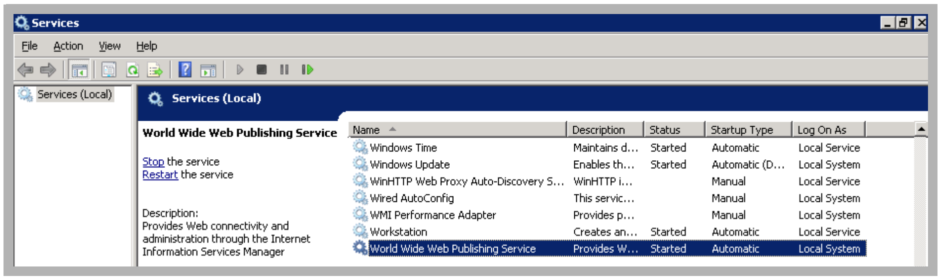


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: C:\UC\WebMailConfig.exe /i user.erb.com

This task will be created with administrative privileges.

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



World Wide Web Publishing Service

Stop the service
Restart the service

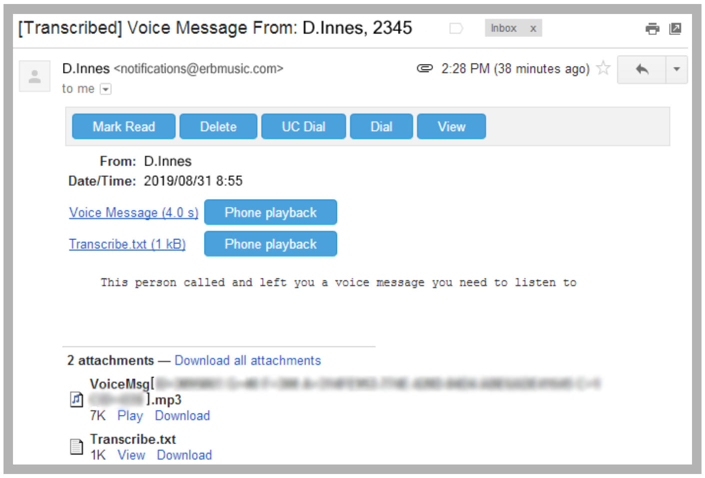
Description:
Provides Web connectivity and administration through the Internet Information Services Manager

Name	Description	Status	Startup Type	Log On As
Windows Time	Maintains d...	Started	Automatic	Local Service
Windows Update	Enables th...	Started	Automatic (D...	Local System
WinHTTP Web Proxy Auto-Discovery S...	WinHTTP i...		Manual	Local Service
Wired AutoConfig	This servic...		Manual	Local System
WMI Performance Adapter	Provides p...		Manual	Local System
Workstation	Creates an...	Started	Automatic	Local Service
World Wide Web Publishing Service	Provides W...	Started	Automatic	Local System

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.



[Transcribed] Voice Message From: D.Innes, 2345

D.Innes <notifications@erbmusic.com>
to me

2:28 PM (38 minutes ago)

From: D.Innes
Date/Time: 2019/08/31 8:55

Voice Message (4.0 s)
Transcribe.txt (1 kB)

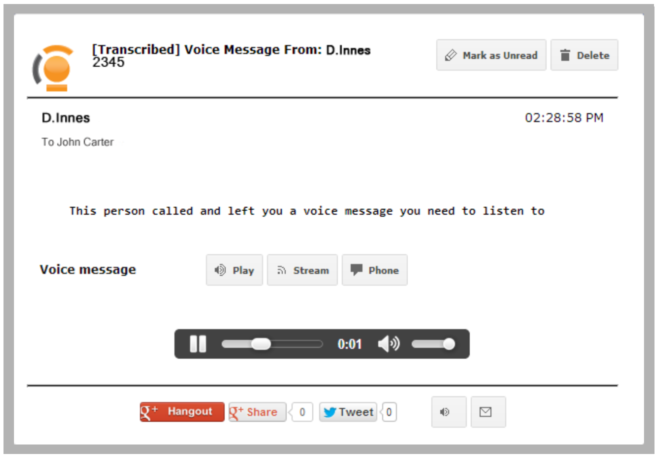
```
This person called and left you a voice message you need to listen to
```

2 attachments — Download all attachments

VoiceMsg[[redacted]].mp3
7K Play Download

Transcribe.txt
1K View Download

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



[Transcribed] Voice Message From: D.Innes 2345

D.Innes
To John Carter

02:28:58 PM

```
This person called and left you a voice message you need to listen to
```

Voice 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.

Forwarded messages will contain links which are only viewable by authorized users.

6 EMAIL ACTION SCHEMA

In This Chapter:

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.

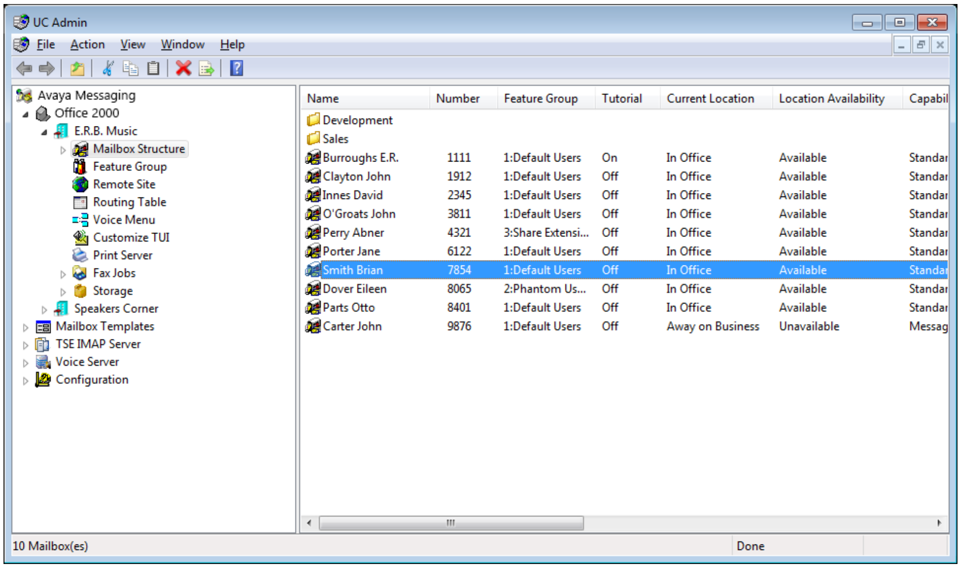
Warning: This feature is only compatible with email programs that support **DKIM verification**.

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.

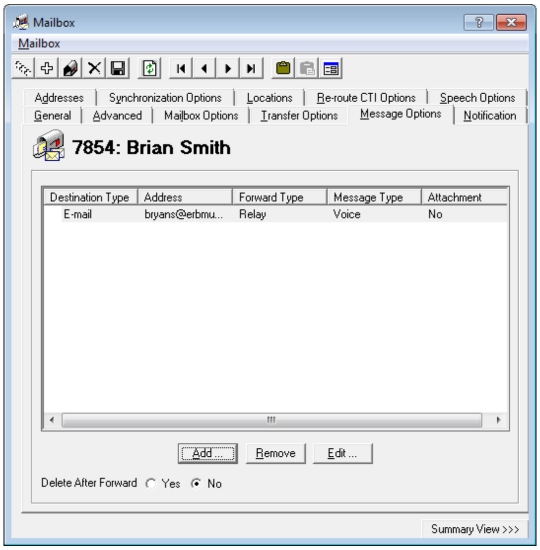
1. Start Avaya Messaging Admin and open the **Mailbox** folder.



Name	Number	Feature Group	Tutorial	Current Location	Location Availability	Capabil
Development						
Sales						
Burroughs E.R.	1111	1:Default Users	On	In Office	Available	Standar
Clayton John	1912	1:Default Users	Off	In Office	Available	Standar
Innes David	2345	1:Default Users	Off	In Office	Available	Standar
O'Groats John	3811	1:Default Users	Off	In Office	Available	Standar
Perry Abner	4321	3:Share Extensi...	Off	In Office	Available	Standar
Porter Jane	6122	1:Default Users	Off	In Office	Available	Standar
Smith Brian	7854	1:Default Users	Off	In Office	Available	Standar
Dover Eileen	8065	2:Phantom Us...	Off	In Office	Available	Standar
Parts Otto	8401	1:Default Users	Off	In Office	Available	Standar
Carter John	9876	1:Default Users	Off	Away on Business	Unavailable	Messag

10 Mailbox(es) Done

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

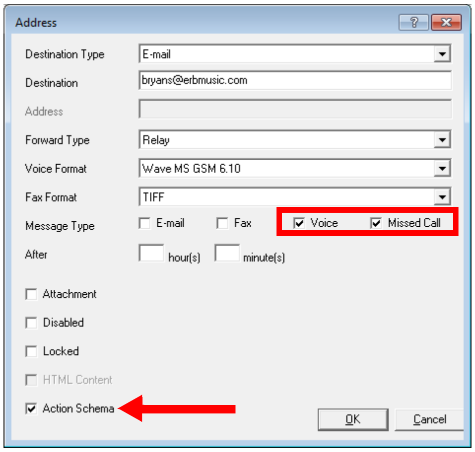


7854: Brian Smith

Destination Type	Address	Forward Type	Message Type	Attachment
E-mail	bryans@erbmu...	Relay	Voice	No

Delete After Forward ○ Yes ● No

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.



Address

Destination Type	E-mail
Destination	bryans@erbmusic.com
Address	
Forward Type	Relay
Voice Format	Wave MS GSM 6.10
Fax Format	TIFF
Message Type	□ E-mail □ Fax ☑ Voice ☑ Missed Call
After	hour(s) minute(s)

□ Attachment

□ Disabled

□ Locked

□ HTML Content

☑ Action Schema

Click **OK** when finished.

Hint: For a complete details for all of the items in the Addresses window, refer to the **Add / Edit Message Options**, page 161 in the Server Configuration Guide.

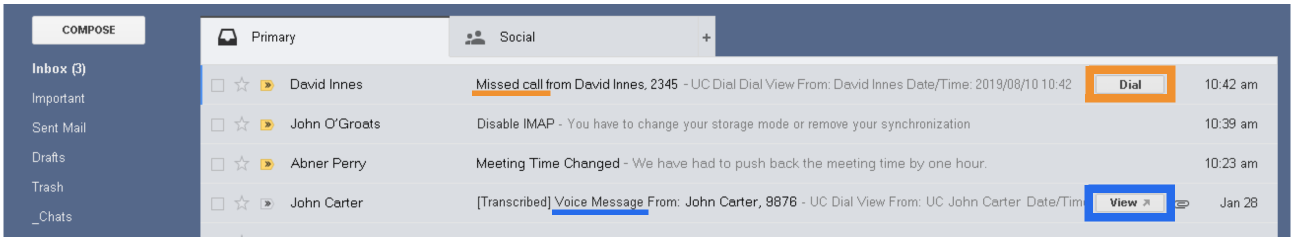
5. Save the changes to the mailbox.

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 leave a message, then the **Dial** button will appear.



David Innes	Missed call from David Innes, 2345 - UC Dial Dial View From: David Innes Date/Time: 2019/08/10 10:42	Dial	10:42 am
John O'Groats	Disable IMAP - You have to change your storage mode or remove your synchronization		10:39 am
Abner Perry	Meeting Time Changed - We have had to push back the meeting time by one hour.		10:23 am
John Carter	[Transcribed] Voice Message From: John Carter, 9876 - UC Dial View From: UC John Carter Date/Tim	View	Jan 28

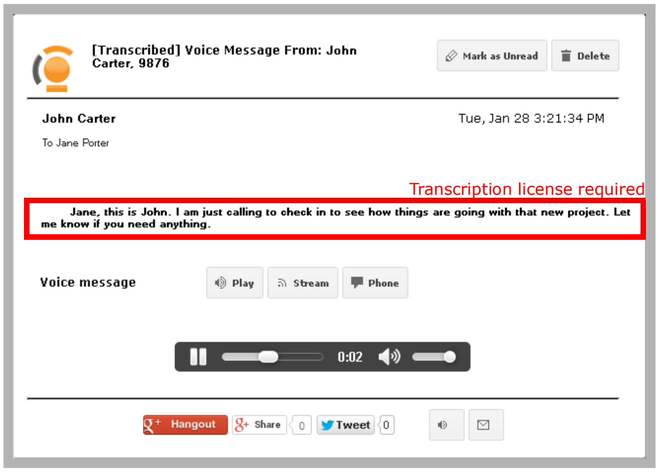
Note: In the examples that follow, when initiating a telephone call to the contact, the device currently selected is used. The current device is defined within your location setup. For example, if your current location is **Mobile**, the call will ring on the device configured for that location (i.e.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

Dial

The Dial button will start the iLink 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.



[Transcribed] Voice Message From: John Carter, 9876

John Carter

Tue, Jan 28 3:21:34 PM

To Jane Porter

Transcription license required

Jane, this is John. I am just calling to check in to see how things are going with that new project. Let me know if you need anything.

Voice message

Play Play

<Back to View>

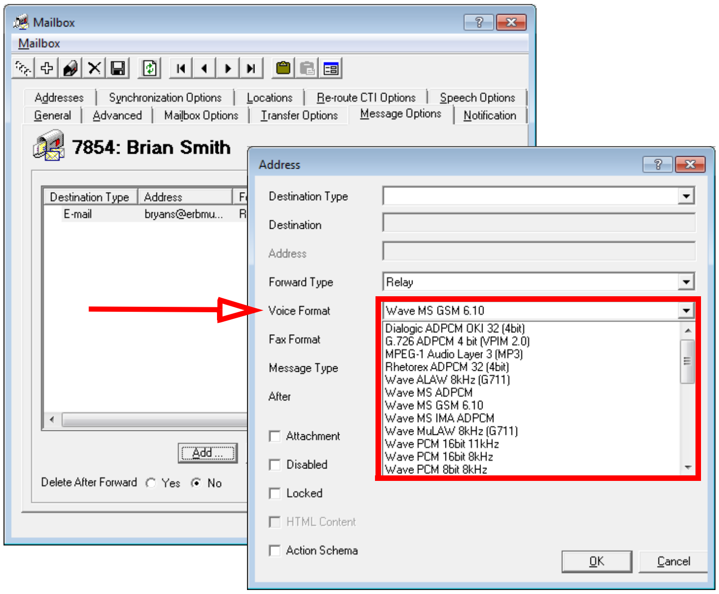
Choose **Play** to have the voice message converted to MP3 format and played through the browser.

Stream Stream

<Back to View>

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**.



7854: Brian Smith

Destination Type	Address	F
E-mail	bryans@erbmu...	R

Delete After Forward ○ Yes ● No

Address

Destination Type:
Destination:
Address:
Forward Type: Relay
Voice Format: Wave MS GSM 6.10
- Dialogic ADPCM OKI 32 (4bit)
- G.726 ADPCM 4 bit (VPIM 2.0)
- MPEG-1 Audio Layer 3 (MP3)
- Rhetorex ADPCM 32 (4bit)
- Wave ALAW 8kHz (G711)
- Wave MS ADPCM
- Wave MS GSM 6.10
- Wave MS IMA ADPCM
- Wave MuLAW 8kHz (G711)
- Wave PCM 16bit 11kHz
- Wave PCM 16bit 8kHz
- Wave PCM 8bit 8kHz

Fax Format
Message Type
After

□ Attachment
□ Disabled
□ Locked
□ HTML Content
□ Action Schema

Phone Phone

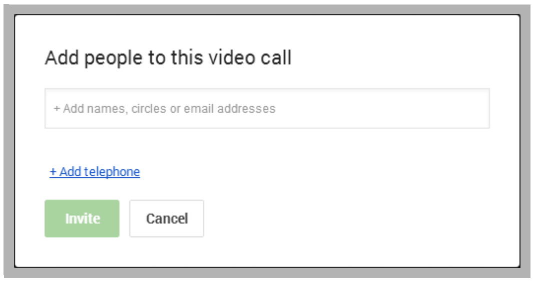
<Back to View>

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 g+ Hangout

<Back to View>

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 in to their account to receive the invitation.

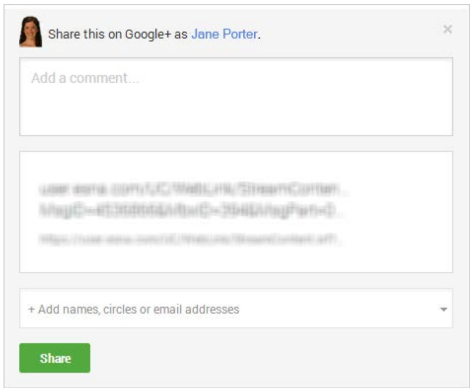


Add people to this video call

Google+ Share Share

<Back to View>

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



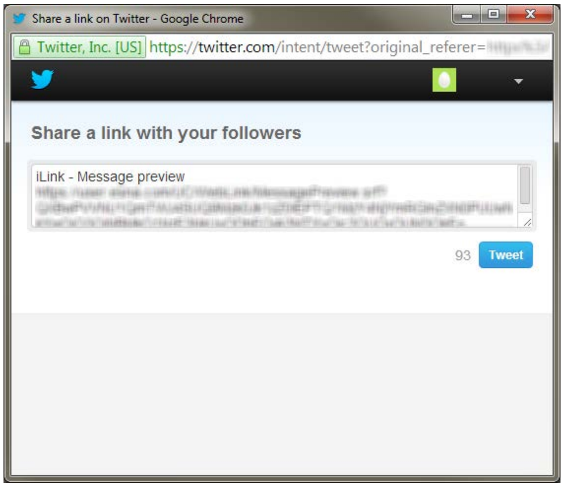
Share this on Google+ as Jane Porter.

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

Twitter Tweet

<Back to View>

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



Share a link on Twitter - Google Chrome
Twitter, Inc. [US]
https://twitter.com/intent/tweet?original_referer=

Share a link with your followers

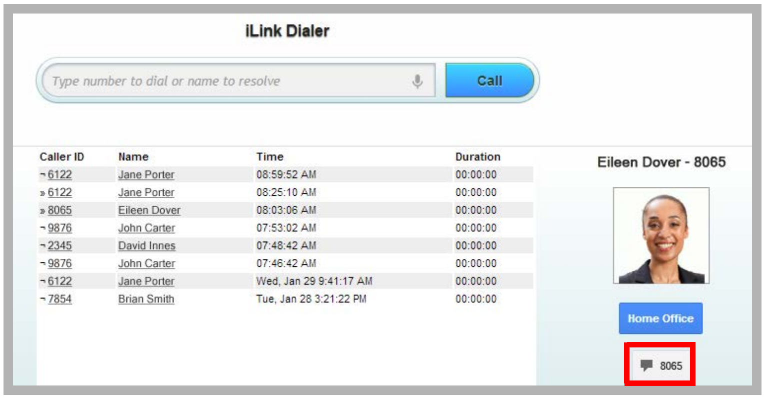
iLink - Message preview

iLink Dialer

<Back to View>

iLink 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.



iLink Dialer

Caller ID	Name	Time	Duration
¬ 6122	Jane Porter	08:59:52 AM	00:00:00
» 6122	Jane Porter	08:25:10 AM	00:00:00
» 8065	Eileen Dover	08:03:06 AM	00:00:00
¬ 9876	John Carter	07:53:02 AM	00:00:00
¬ 2345	David Innes	07:48:42 AM	00:00:00
¬ 9876	John Carter	07:46:42 AM	00:00:00
¬ 6122	Jane Porter	Wed, Jan 29 9:41:17 AM	00:00:00
¬ 7854	Brian Smith	Tue, Jan 28 3:21:22 PM	00:00:00

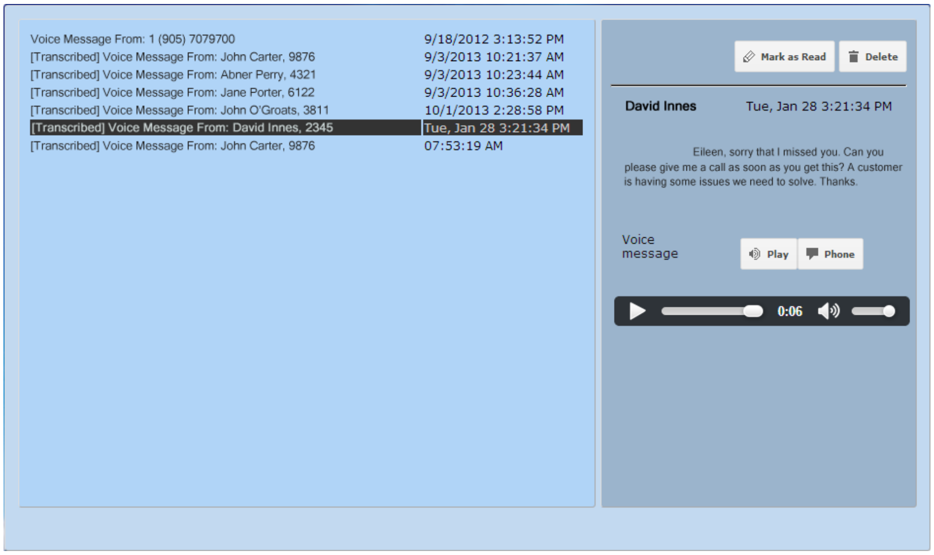
Eileen Dover - 8065

iLink Messages

<Back to View>

iLink 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.



Voice Message From: 1 (905) 7079700	9/18/2012 3:13:52 PM
[Transcribed] Voice Message From: John Carter, 9876	9/3/2013 10:21:37 AM
[Transcribed] Voice Message From: Abner Perry, 4321	9/3/2013 10:23:44 AM
[Transcribed] Voice Message From: Jane Porter, 6122	9/3/2013 10:36:28 AM
[Transcribed] Voice Message From: John O'Groats, 3811	10/1/2013 2:28:58 PM
[Transcribed] Voice Message From: David Innes, 2345	Tue, Jan 28 3:21:34 PM
[Transcribed] Voice Message From: John Carter, 9876	07:53:19 AM

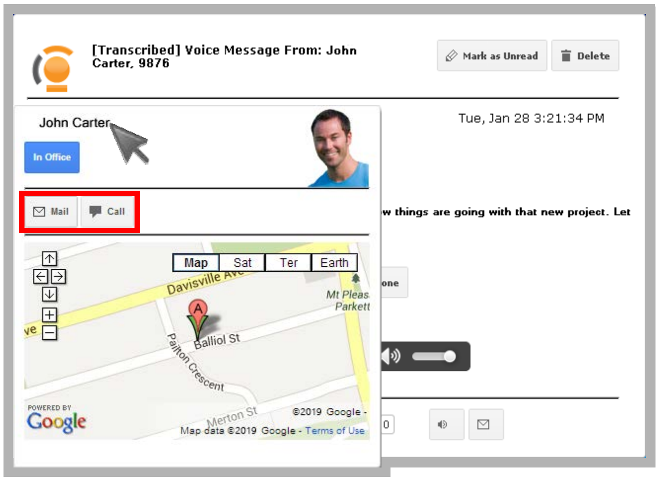
David Innes Tue, Jan 28 3:21:34 PM

Eileen, sorry that I missed you. Can you please give me a call as soon as you get this? A customer is having some issues we need to solve. Thanks.

Contact Location

<Back to View>

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.



[Transcribed] Voice Message From: John Carter, 9876

John Carter

Tue, Jan 28 3:21:34 PM

w things are going with that new project. Let

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.

7 NUANCE TRANSCRIPTION SERVICE

In This Chapter:

Introduction

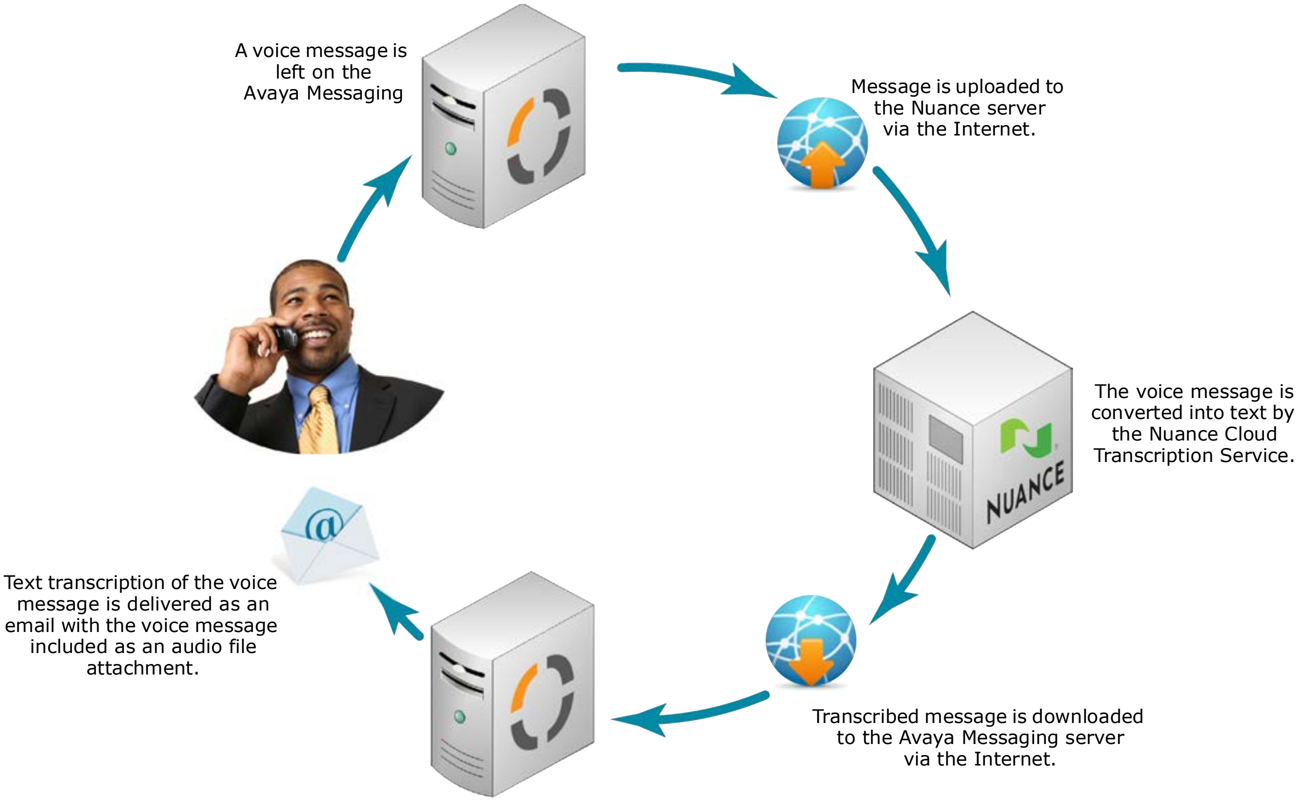
Note: Transcription provides text output from voice messages left in a user's mailbox. The user will receive an email with the transcribed text of the message.

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 for the Nuance (cloud based) or Mutare (on-premise) Transcription Services are available through Avaya.

This chapter describes the configuration for the Nuance cloud-based transcription service.

Visual Guide


A voice message is left on the Avaya Messaging
Message is uploaded to the Nuance server via the Internet.
The voice message is converted into text by the Nuance Cloud Transcription Service.
NUANCE
Transcribed message is downloaded to the Avaya Messaging server via the Internet.
Text transcription of the voice message is delivered as an email with the voice message included as an audio file attachment.
@

When a voice message arrives on the voice server, the message is sent to the Nuance transcription server. 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	Nuance Subscription available from Avaya
Software	Avaya Messaging version 8.1 or higher

- A Nuance transcription service subscription.
- Must have **Enabled SSL** on the **IIS** using a **Secure Certificate** Key. Please refer to the **IIS/SSL** document located in Avaya Messaging Server Configuration Guide Security chapter.
- Internet access for Avaya Messaging server. This can be an external IP address, or a Domain Name providing access directly or through proxy to the Avaya Messaging server.

Licensing

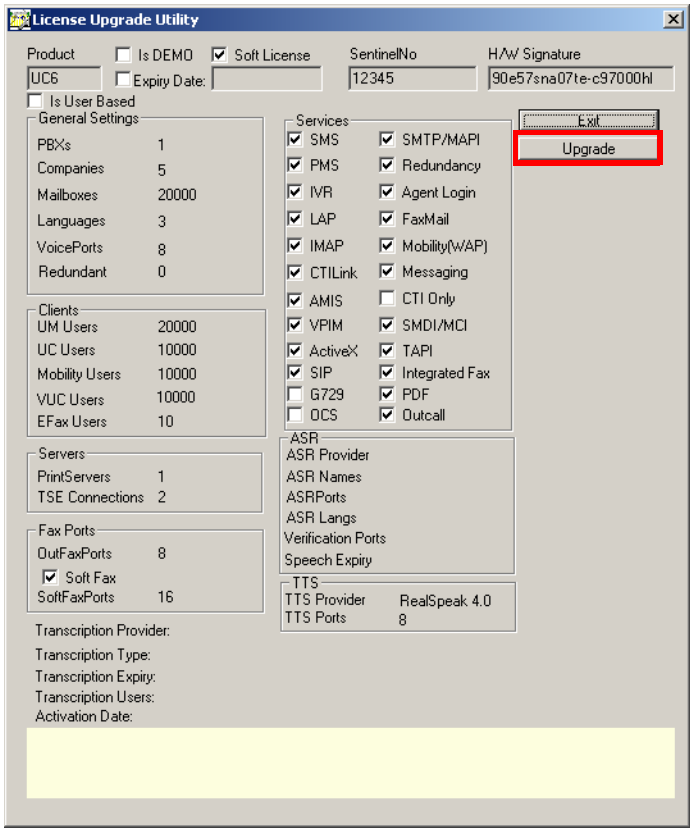
The transcription feature is not included with the standard Avaya Messaging license but is available as an option from Avaya. These instructions are only required if a Nuance transcription license is purchased after Avaya Messaging is installed and configured.

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.

Upgrading the License

If Avaya Messaging has already been installed and setup on a server, add a transcription license by following these steps.

1. On the Avaya Messaging server, go to **Start > All Programs > Avaya Messaging > UCLicenseUpgrade**.
2. The **License Upgrade Utility** screen appears. Click **Upgrade**.



Product: UC6
□ Is DEMO ☑ Soft License
□ Expiry Date:
SentinelNo: 12345
H/W Signature: 90e57sna07te-c97000hl
□ Is User Based

General Settings

PBXs	1
Companies	5
Mailboxes	20000
Languages	3
VoicePorts	8
Redundant	0

Clients

UM Users	20000
UC Users	10000
Mobility Users	10000
VUC Users	10000
EFax Users	10

Servers

PrintServers	1
TSE Connections	2

Fax Ports

OutFaxPorts	8
☑ Soft Fax	
SoftFaxPorts	16

Transcription Provider:
Transcription Type:
Transcription Expiry:
Transcription Users:
Activation Date:

Services

☑ SMS	☑ SMTP/MAPI
☑ PMS	☑ Redundancy
☑ IVR	☑ Agent Login
☑ LAP	☑ FaxMail
☑ IMAP	☑ Mobility(WAP)
☑ CTILink	☑ Messaging
☑ AMIS	□ CTI Only
☑ VPIM	☑ SMDI/MCI
☑ ActiveX	☑ TAPI
☑ SIP	☑ Integrated Fax
□ G729	☑ PDF
□ OCS	☑ Outcall

ASR
ASR Provider
ASR Names
ASRPorts
ASR Langs
Verification Ports
Speech Expiry

TTS

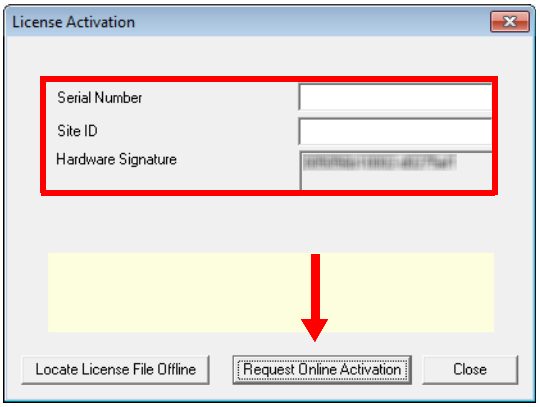
TTS Provider	RealSpeak 4.0
TTS Ports	8

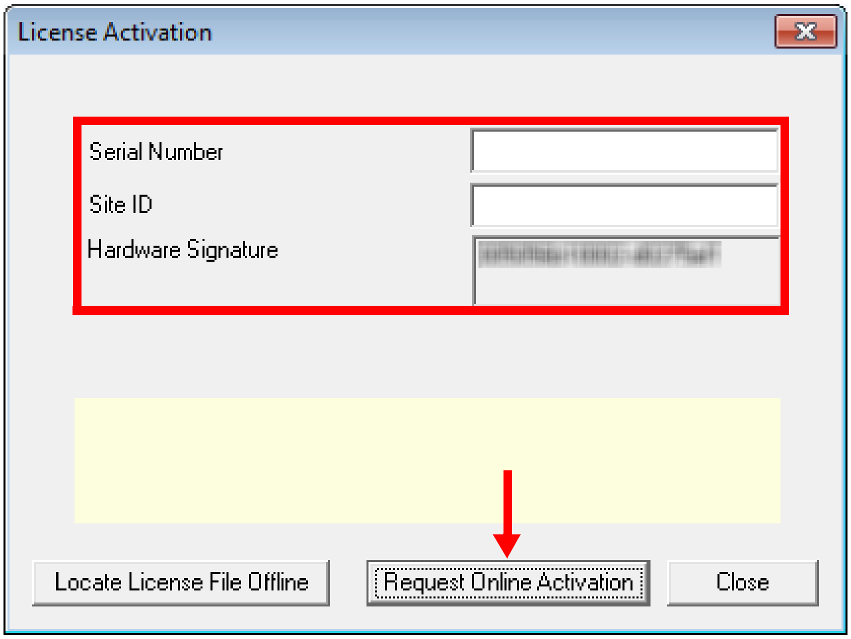
3. The Serial Number and Site ID will already be entered. If not, enter the data manually:

   Serial Number: Enter the serial number for your Avaya Messaging license.

   Site ID: Enter the site ID for your location.

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

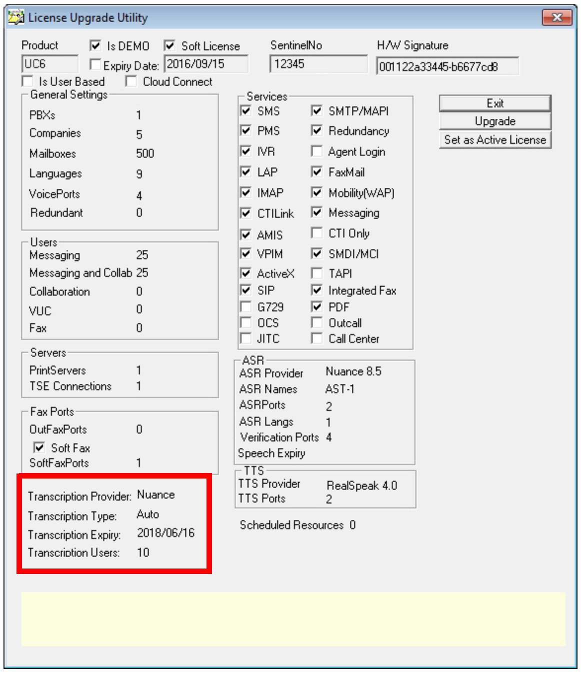




4. Click **Request Online Activation**.

5. The license will be updated from Avaya's online license server to include the latest features.

   Click **Set as Active License**.



Product: UC6 ☑ Is DEMO ☑ Soft License SentinelNo: 12345 H/W Signature: 001122a33445-b6677cd8

☐ Expiry Date: 2016/09/15

☐ Is User Based ☐ Cloud Connect

General Settings

PBXs	1
Companies	5
Mailboxes	500
Languages	9
VoicePorts	4
Redundant	0

Users

Messaging	25
Messaging and Collab	25
Collaboration	0
VUC	0
Fax	0

Servers

PrintServers	1
TSE Connections	1

Fax Ports

OutFaxPorts	0
☑ Soft Fax	
SoftFaxPorts	1

Transcription Provider:	Nuance
Transcription Type:	Auto
Transcription Expiry:	2018/06/16
Transcription Users:	10

Services

☑ SMS	☑ SMTP/MAPI
☑ PMS	☑ Redundancy
☑ IVR	☐ Agent Login
☑ LAP	☑ FaxMail
☑ IMAP	☑ Mobility(WAP)
☑ CTILink	☑ Messaging
☑ AMIS	☐ CTI Only
☑ VPIM	☑ SMDI/MCI
☑ ActiveX	☐ TAPI
☑ SIP	☑ Integrated Fax
☐ G729	☑ PDF
☐ OCS	☐ Outcall
☐ JITC	☐ Call Center

ASR

ASR Provider	Nuance 8.5
ASR Names	AST-1
ASRPorts	2
ASR Langs	1
Verification Ports	4
Speech Expiry	

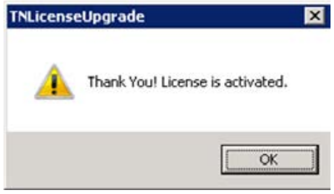
TTS

TTS Provider	RealSpeak 4.0
TTS Ports	2

Scheduled Resources 0

6. Your Nuance transcription license is activated.

   Click **OK** to continue and configure of the service.



Thank You! License is activated.

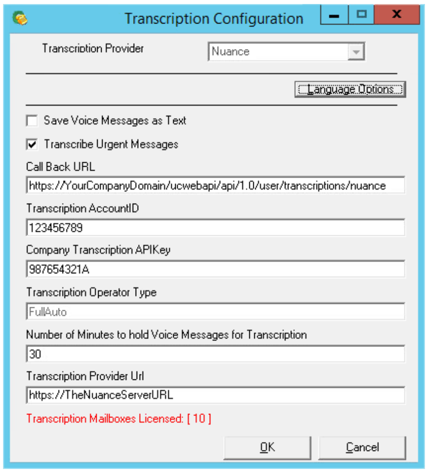
Avaya Messaging Server Configuration

Once you have added the transcription license, you must configure Avaya Messaging to communicate with the Nuance servers over the Internet.

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

Transcription Configuration Tool

1. On the Avaya Messaging server, go to **Start > All Programs > Avaya Messaging > UCTranscriptionConfig**.
2. Enter all required information.



Transcription Configuration

Transcription Provider: Nuance

□ Save Voice Messages as Text

☑ Transcribe Urgent Messages

Call Back URL: https://YourCompanyDomain/ucwebapi/api/1.0/user/transcriptions/nuance

Transcription AccountID: 123456789

Company Transcription APIKey: 987654321A

Transcription Operator Type: FullAuto

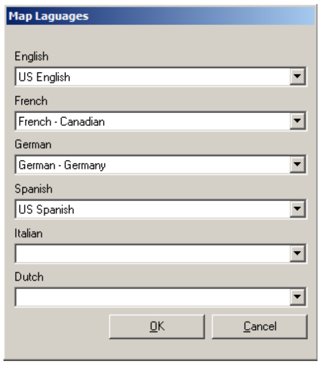
Number of Minutes to hold Voice Messages for Transcription: 30

Transcription Provider Url: https://TheNuanceServerURL

Transcription Mailboxes Licensed: [10]

Note: Step 3 applies only to installations using the **Nuance Multilingual Transcription Service**.

3. Click **Language Options**. Specify the regional variation for each required language.
4. Click **OK** when finished.



Map Laguages

English: US English

French: French - Canadian

German: German - Germany

Spanish: US Spanish

Italian:

Dutch:

Save Voice Messages as Text

Enable this checkbox to have the system 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 accessible URL of your Avaya Messaging Voicemail server to which Nuance will send completed transcriptions. You can configure your DNS and change “YourCompanyUrl” only (i.e. from “https://YourCompanyUrl/uc/webtranscribe/WebTranscribeclass.asp” you only need to change “YourCompnayUrl”) since the virtual folders and the transcription receiver applications are automatically setup.

Number of Minutes to Hold Voice Messages for Transcription

Voice messages for selected mailboxes are put on hold until the transcription is returned from Nuance. 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.

Language Options / Map Languages

Nuance supports many regional variations within a language. Differences due to accent, pacing and word selection can be compensated for by choosing the appropriate variation from the dropdown lists.

Maximum Transcribed Message Length

Nuance will transcribe up to the first 60 seconds of any message. The portion of the message beyond 60 seconds will not be transcribed, although the voice recording will be unaffected.

Nuance Server Configuration Requirements

In order for the Nuance servers to properly receive and reply to transcription requests, the customer must provide certain information regarding the setup of their computer network. This information must be provided before the transcription service can be used. Your sales associate will collect this information when the license is purchased.

The information required is listed in the following table.

Item	Details	Description
Customer request source IP address	(e.g. 11.22.33.44)	This is the IP address **from** which (source) the customer will send transcription requests to Nuance.
Nuance request target IP address:Port	(e.g. 98.765.432.100:8621)	This is the IP address and port **to** which (target) the customer will send transcription requests to Nuance.
Customer Result URL (Call Back URL):Port (default Nuance port is 80 or 443)	(e.g. http://12.34.56.789:80/ NuanceResult)	This is the customer URL (Call Back URL) and port **to** which Nuance will send the completed transcription requests. If the customer wants to use ports other than 80 and 443, Avaya must be informed so that the corresponding changes can be applied to the transcription server.
Nuance Result IP address:Port (not required for Nuance Multi-Lingual install)	(e.g. 99.888.777.100:80)	This is the URL and port **from** which Nuance will send the completed transcription requests back to the customer.
Special requests	(e.g. https using self-signed certificates from IP:port)	Include any special requests from the customer such as the use of https, self-signed certificates, ssl, etc. Otherwise, Nuance will use default port 8X21 to create inbound URL into Nuance .
Type of Service	(e.g. Fully Automated)	Specify the type of transcription service desired: fully automated (computer based), semi-automated (with some human assistance), other.
Nuance Operator ID	(e.g. CUST-VM2T)	Customer ID to be used for the new tenant or type of service.
Customer prefix for session ID's	(e.g. CUST-xxxxx-yyyyy-zzzz)	Customer should use a unique string like “Customer-XXXX” for session ID’s.

The customer’s network administrator must ensure that all of the necessary changes have been made to network security systems (i.e. firewall, antivirus) to permit this communication. The stated ports and addresses must be opened for both outbound and inbound traffic.

Verification

Once all of the information has been collected and the network adjustments made, the connection between the customer's network and the Nuance 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 Nuance 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 in that time, the process will time out and a regular 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 Nuance 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.

8 MUTARE TRANSCRIPTION SERVICE

In This Chapter:

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.

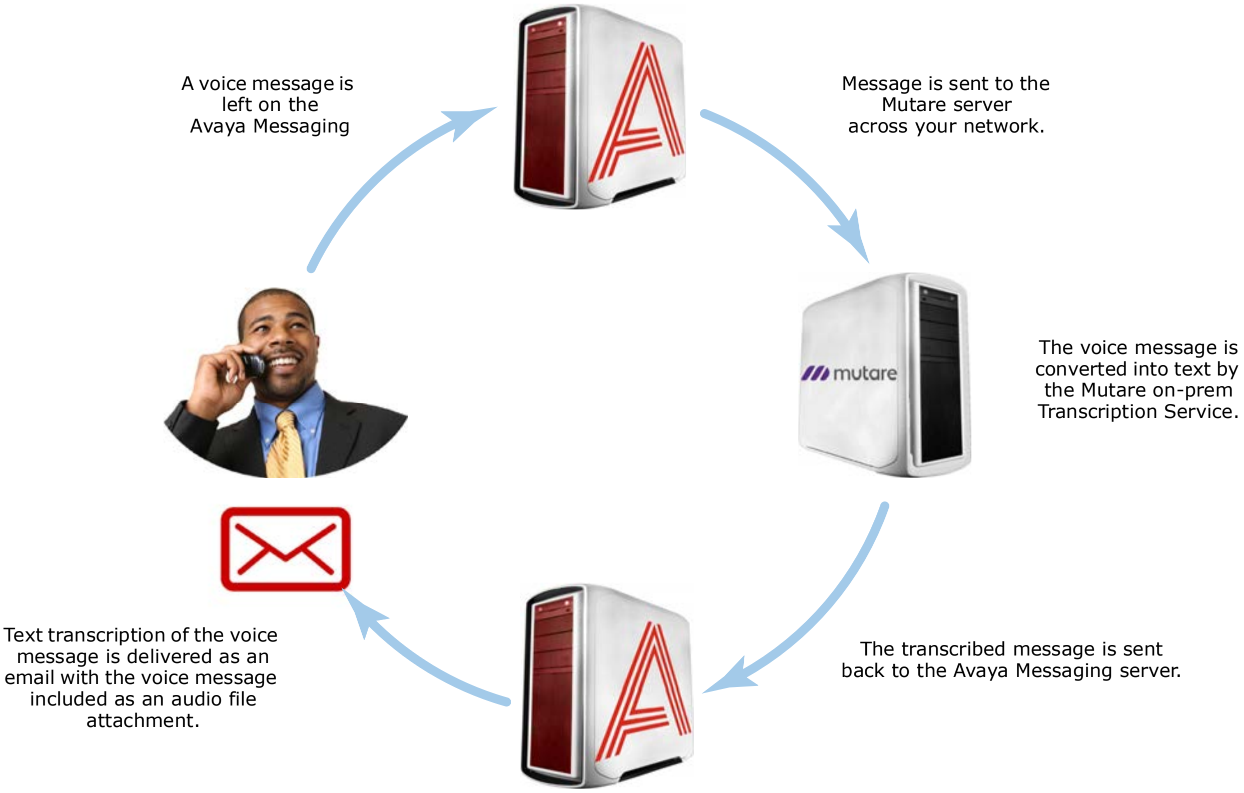
The Transcription feature allows users to receive text output from voice messages. The transcribed voice message is delivered to the user in the body of an email.

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


A voice message is left on the Avaya Messaging
Message is sent to the Mutare server across your network.
mutare
The voice message is converted into text by the Mutare on-prem Transcription Service.
The transcribed message is sent back to the Avaya Messaging server.
Text transcription of the voice message is delivered as an email with the voice message included as an audio file attachment.

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 10.6 - 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.

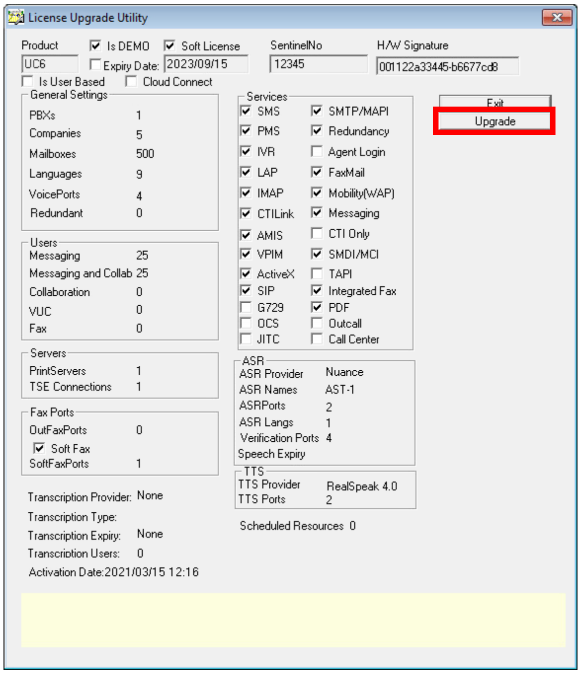
Once you have purchased a license, it must be activated through the UC License Upgrade Utility. The service must then be configured through the Transcription Configuration Tool.

> **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**.



Product: UC6

☑ Is DEMO ☑ Soft License

☐ Expiry Date: 2023/09/15

SentinelNo: 12345

H/W Signature: 001122a33445-b6677cd8

☐ Is User Based ☐ Cloud Connect

General Settings

PBXs	1
Companies	5
Mailboxes	500
Languages	9
VoicePorts	4
Redundant	0

Users

Messaging	25
Messaging and Collab	25
Collaboration	0
VUC	0
Fax	0

Servers

PrintServers	1
TSE Connections	1

Fax Ports

OutFaxPorts 0

☑ Soft Fax

SoftFaxPorts 1

Services

☑ SMS	☑ SMTP/MAPI
☑ PMS	☑ Redundancy
☑ IVR	☐ Agent Login
☑ LAP	☑ FaxMail
☑ IMAP	☑ Mobility(WAP)
☑ CTILink	☑ Messaging
☑ AMIS	☐ CTI Only
☑ VPIM	☑ SMDI/MCI
☑ ActiveX	☐ TAPI
☑ SIP	☑ Integrated Fax
☐ G729	☑ PDF
☐ OCS	☐ Outcall
☐ JITC	☐ Call Center

ASR

ASR Provider	Nuance
ASR Names	AST-1
ASRPorts	2
ASR Langs	1
Verification Ports	4
Speech Expiry	

TTS

TTS Provider	RealSpeak 4.0
TTS Ports	2

Scheduled Resources 0

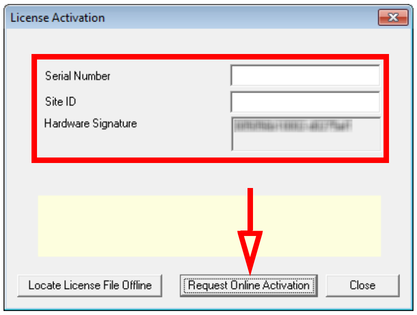
Transcription Provider: None
Transcription Type:
Transcription Expiry: None
Transcription Users: 0
Activation Date:2021/03/15 12:16

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.

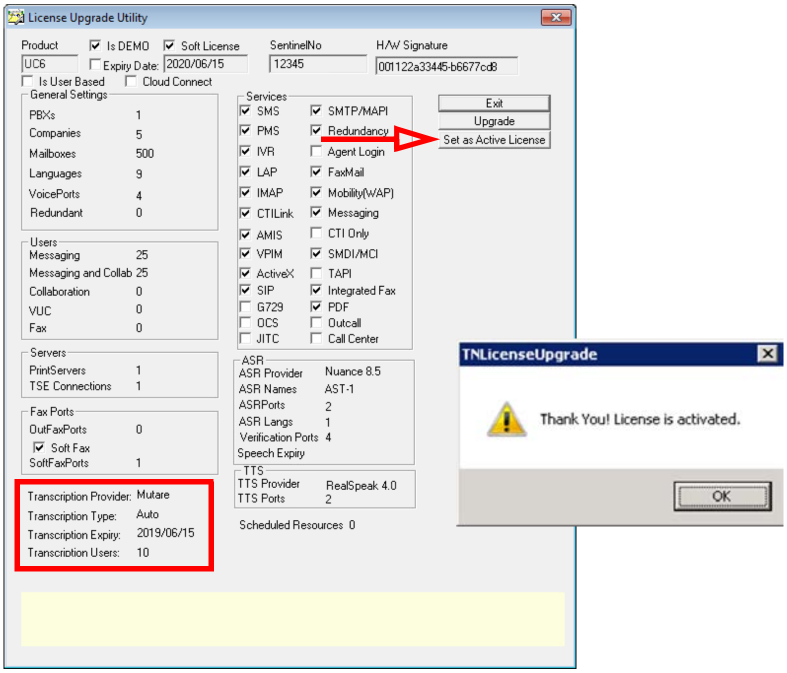
   Both of these items are provided by Avaya as part of the initial Avaya Messaging license package.


License Activation

Serial Number
Site ID
Hardware Signature

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**.


License Upgrade Utility

Product: UC6 ☑ Is DEMO ☑ Soft License
□ Expiry Date: 2020/06/15
SentinelNo: 12345
H/W Signature: 001122a33445-b6677cd8
□ Is User Based □ Cloud Connect

General Settings
PBXs 1
Companies 5
Mailboxes 500
Languages 9
VoicePorts 4
Redundant 0

Users
Messaging 25
Messaging and Collab 25
Collaboration 0
VUC 0
Fax 0

Servers
PrintServers 1
TSE Connections 1

Fax Ports
OutFaxPorts 0
☑ Soft Fax
SoftFaxPorts 1

Transcription Provider: Mutare
Transcription Type: Auto
Transcription Expiry: 2019/06/15
Transcription Users: 10

Services
☑ SMS ☑ SMTP/MAPI
☑ PMS ☑ Redundancy
☑ IVR □ Agent Login
☑ LAP ☑ FaxMail
☑ IMAP ☑ Mobility(WAP)
☑ CTILink ☑ Messaging
☑ AMIS □ CTI Only
☑ VPIM ☑ SMDI/MCI
☑ ActiveX □ TAPI
☑ SIP ☑ Integrated Fax
□ G729 ☑ PDF
□ OCS □ Outcall
□ JITC □ Call Center

ASR
ASR Provider Nuance 8.5
ASR Names AST-1
ASRPorts 2
ASR Langs 1
Verification Ports 4
Speech Expiry

TTS
TTS Provider RealSpeak 4.0
TTS Ports 2

Scheduled Resources 0

TNLicenseUpgrade

Thank You! License is activated.

6. Restart the server to complete the update.

Your transcription license is activated.

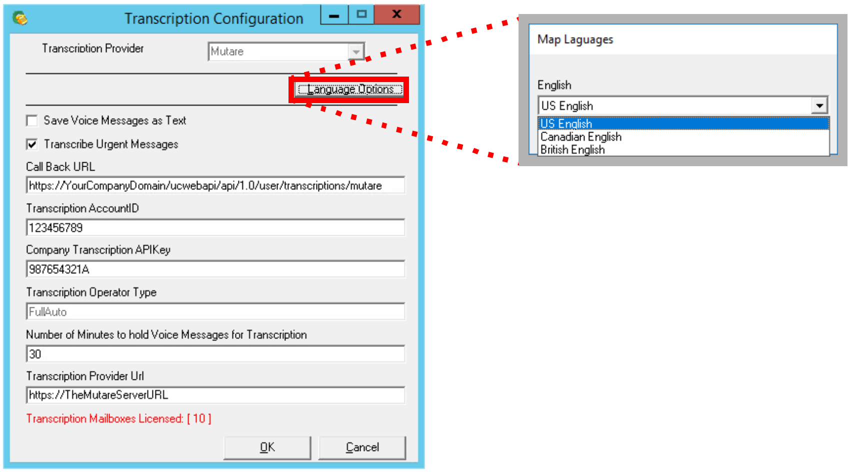
Avaya Messaging Server Configuration

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.



Transcription Configuration

Transcription Provider: Mutare

Language Options

□ Save Voice Messages as Text

☑ Transcribe Urgent Messages

Call Back URL: https://YourCompanyDomain/ucwebapi/api/1.0/user/transcriptions/mutare

Transcription AccountID: 123456789

Company Transcription APIKey: 987654321A

Transcription Operator Type: FullAuto

Number of Minutes to hold Voice Messages for Transcription: 30

Transcription Provider Url: https://TheMutareServerURL

Transcription Mailboxes Licensed: [10]

OK Cancel

Map Laguages

English: US English

US English
Canadian English
British English

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 an language selected here.

4. Click **OK** when finished.

Verification

Once all of the information has been collected and the network adjustments made, the connection between the customer's network and the Mutare on-premise 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 in that time, the process will time out and the untranscribed 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.

9 GOOGLE INTEGRATION

In This Chapter:

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 suites your requirements.

CHAPTER	INTEGRATION	WHY YOU WANT IT
9	Google	Creates a secure connection through OAuth2 to your Gmail and Google Apps accounts.
10	Exchange using EWS	The simplest connection between your Exchange server and Avaya Messaging.
11	Exchange without EWS	A connection between Exchange and Avaya Messaging for legacy systems.
12	Exchange 2010	A connection between Exchange 2010 and Avaya Messaging.
13	Office 365 using Graph	Setup the latest high security integration procedures for maximum data integrity.
14	Office 365 using EWS	Quick connection between your O365 server and Avaya Messaging.

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 of their messages. All of 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.

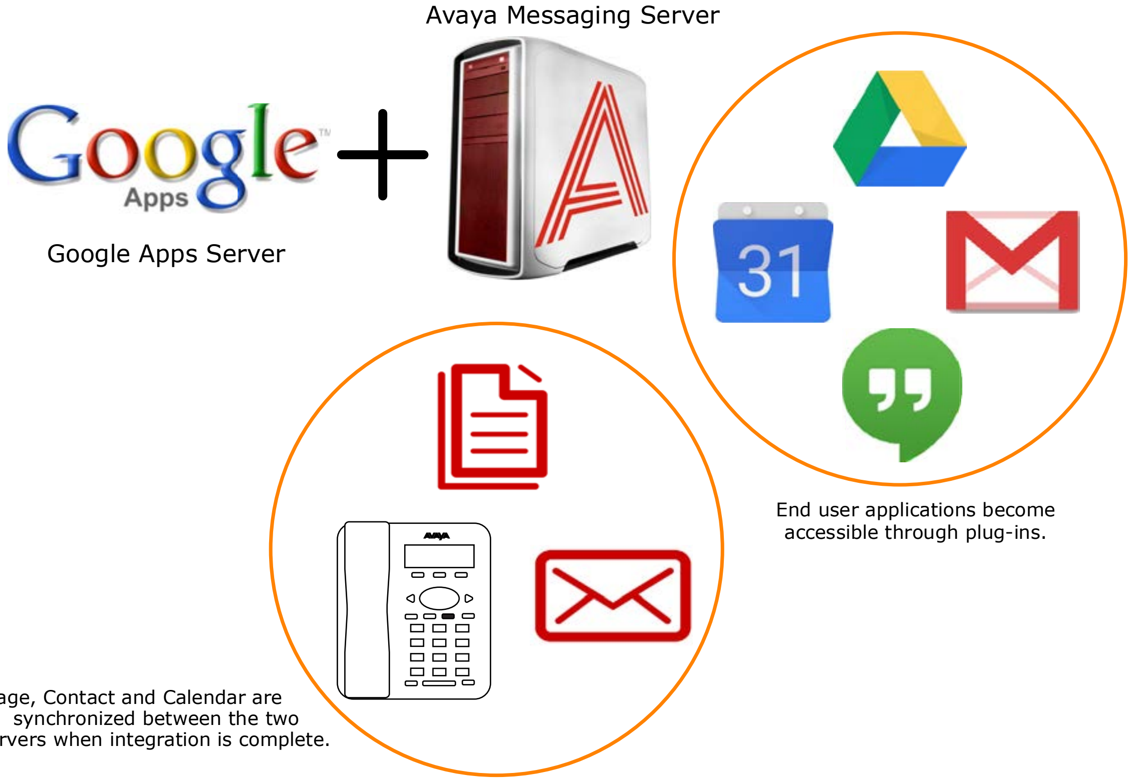
Note: Integration with Google apps and other 3rd party applications and plug-ins may require additional licensing.

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



End user applications become accessible through plug-ins.

Message, Contact and Calendar are synchronized between the two servers when integration is complete.

Requirements

Requirements	Details
License	---
Software	Officelinx/IX Messaging version 9.1 - 10.8 Avaya Messaging version 11.0 and higher

Server Configuration

Server configuration of Google Integration makes extensive use of CSE and CSE.PIM for message, contact and calendar synchronization. As long as the web server is able communicate properly with the worldwide web, users will be able to configure all of their gadgets and plug-ins on their own through the **User Guide on page 98**.

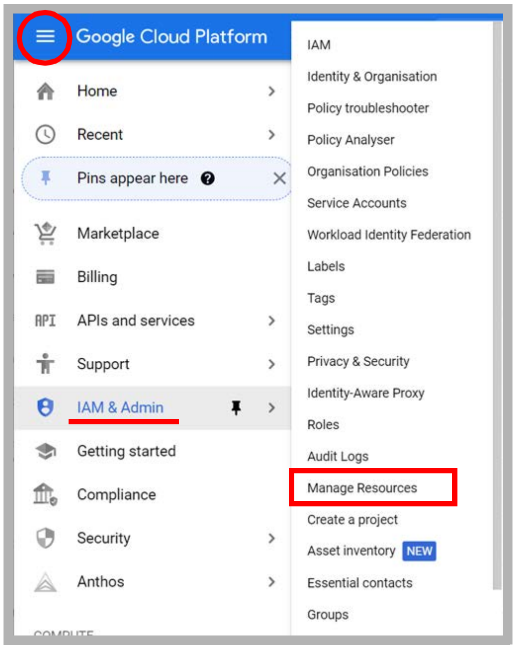
Client authentication and synchronization is handled using OAuth 2.0 and the Google API.

Install and configure OAuth2.0

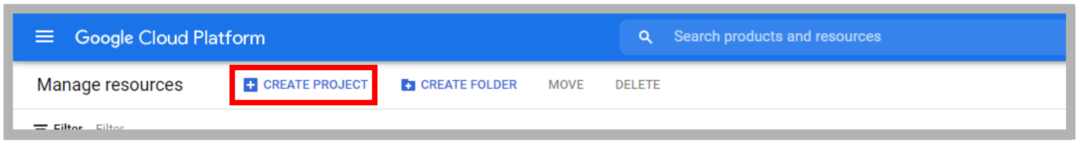
OAuth 2.0 provides secure user authentication and is required for Gmail to access the messaging servers.

OAuth 2.0 Setup

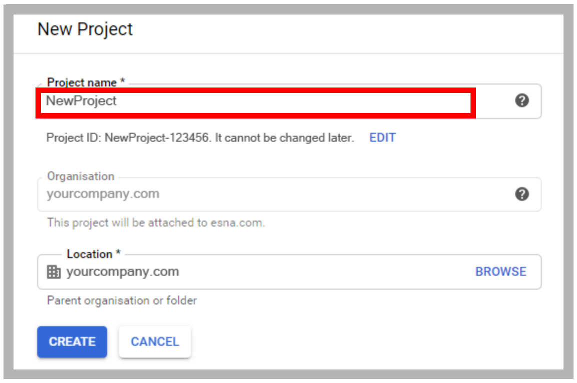
1. Open a web browser and go to https://console.developers.google.com. Login using your Google credentials.
2. Click the **Navigation** menu ☰. Select **IAM & Admin > Manage Resources**.



3. Click **CREATE PROJECT**.



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



New Project

Project name *: NewProject

Project ID: NewProject-123456. It cannot be changed later. EDIT

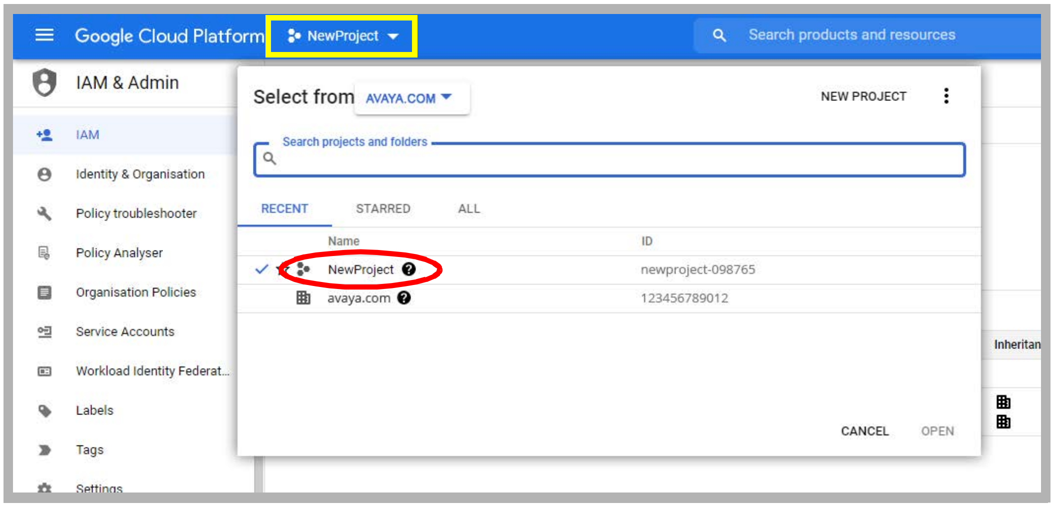
Organisation: yourcompany.com

This project will be attached to esna.com.

Location *: yourcompany.com

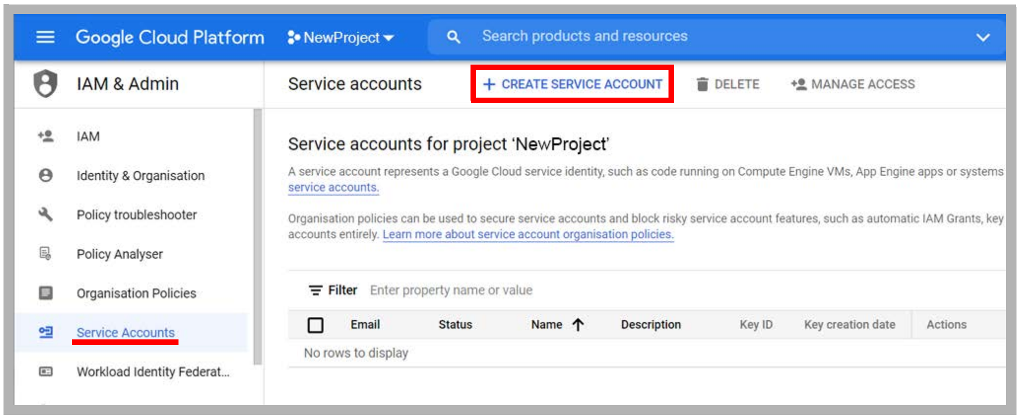
Parent organisation or folder

5. Open the navigation menu and select **IAM & Admin > IAM**. Ensure that the project you just created is chosen in the **Select Project** dropdown menu.



Name	ID
NewProject	newproject-098765
avaya.com	123456789012

6. In the left-hand panel, select **Service accounts**. Click **CREATE SERVICE ACCOUNT**.



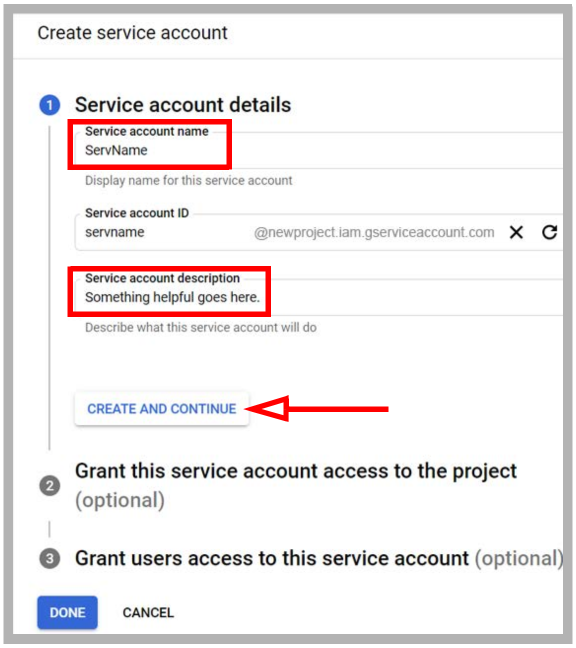
Service accounts for project 'NewProject'

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems service accounts.

Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key accounts entirely. Learn more about service account organisation policies.

☐	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
No rows to display							

7. Give the account a name and a description, then click **CREATE AND CONTINUE**.

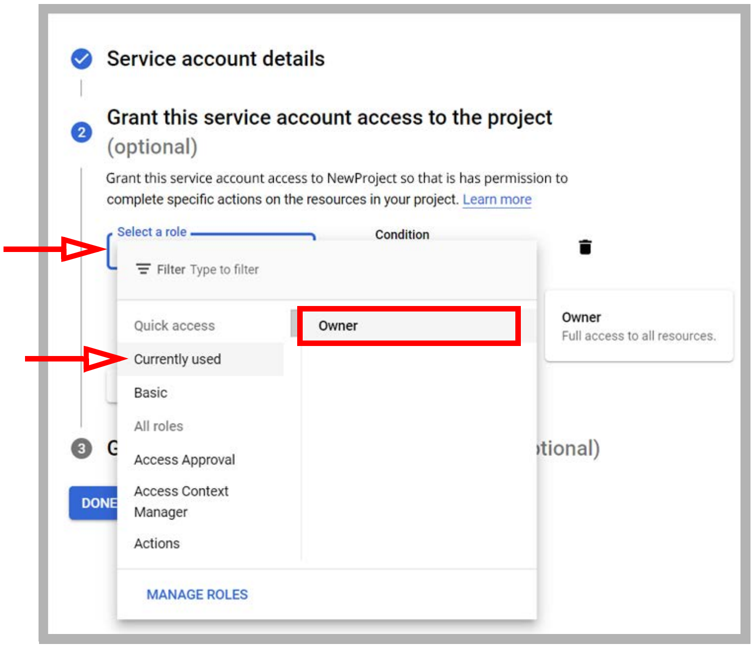

Create service account
1
Service account details
Display name for this service account
Describe what this service account will do
CREATE AND CONTINUE
2
Grant this service account access to the project (optional)
3
Grant users access to this service account (optional)
DONE
CANCEL

Service account name: ServName

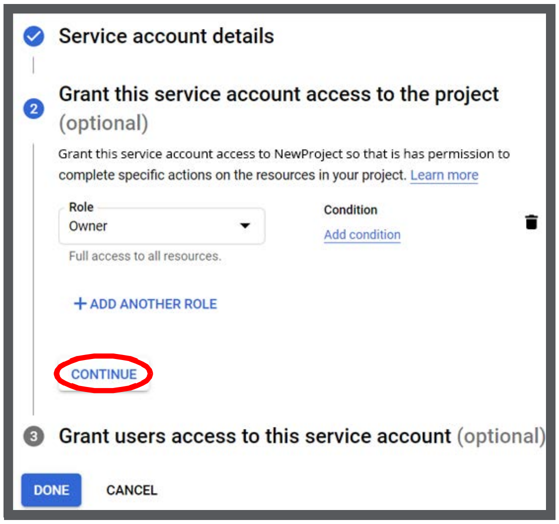
Service account ID: servname @newproject.iam.gserviceaccount.com

Service account description: Something helpful goes here.

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



Grant this service account access to NewProject so that is has permission to complete specific actions on the resources in your project. Learn more

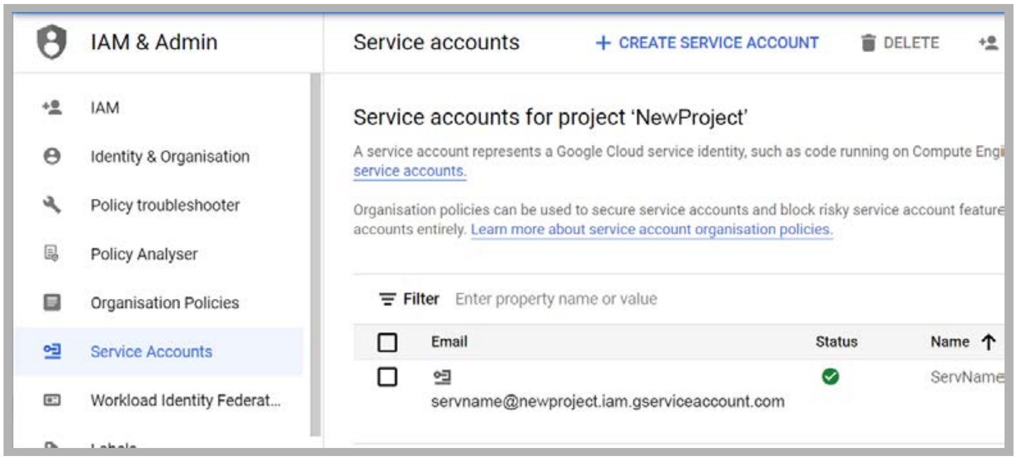

Service account details
2
Grant this service account access to the project (optional)
Condition
Add condition
+ ADD ANOTHER ROLE
CONTINUE
3
Grant users access to this service account (optional)
DONE
CANCEL

Grant this service account access to NewProject so that is has permission to complete specific actions on the resources in your project. Learn more

Role: Owner

Full access to all resources.

9. Click the name of the service account you just created.



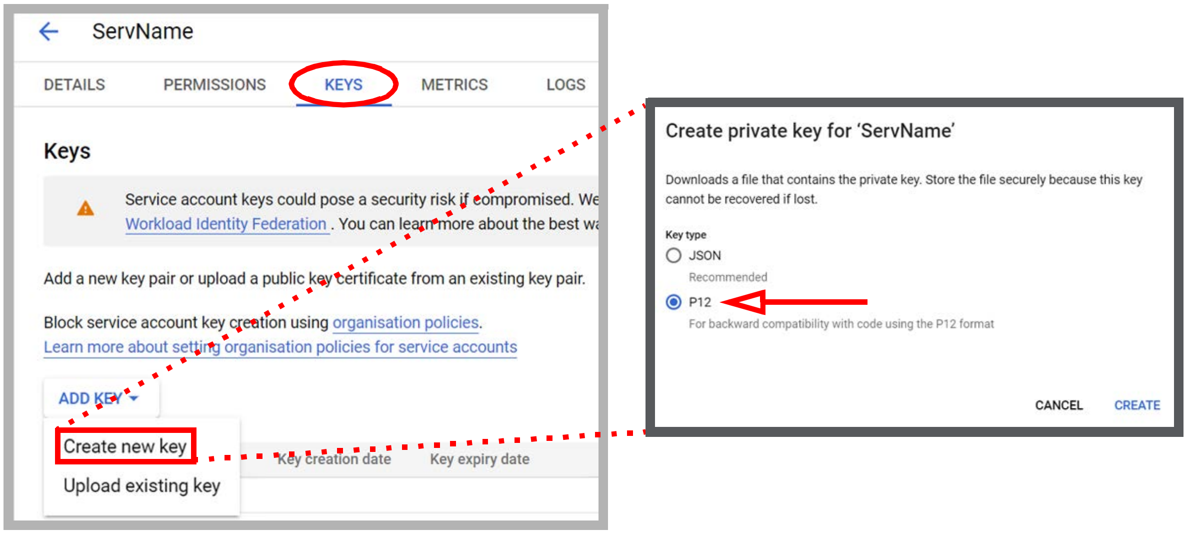
Service accounts for project 'NewProject'

A service account represents a Google Cloud service identity, such as code running on Compute Engi service accounts.

Organisation policies can be used to secure service accounts and block risky service account feature accounts entirely. Learn more about service account organisation policies.

□	Email	Status	Name ↑
□	servname@newproject.iam.gserviceaccount.com	✓	ServName

10. Open the **KEYS** tab and click **ADD KEY > Create new key**. Enable the **P12** option, and click **CREATE**.



Keys

Service account keys could pose a security risk if compromised. We Workload Identity Federation . You can learn more about the best wa

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts

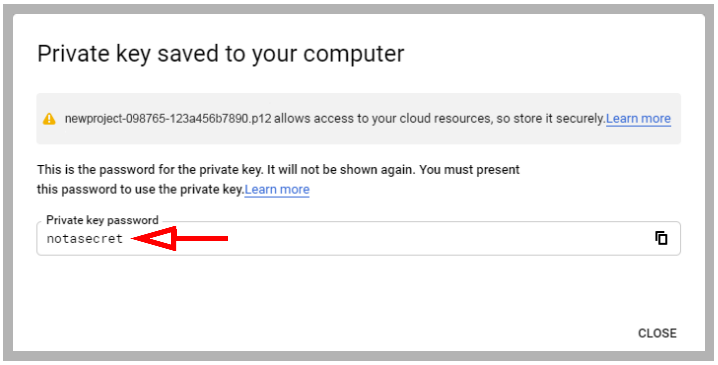
Create private key for 'ServName'

Downloads a file that contains the private key. Store the file securely because this key cannot be recovered if lost.

Key type
○ JSON
Recommended
● P12
For backward compatibility with code using the P12 format

11. 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.)

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



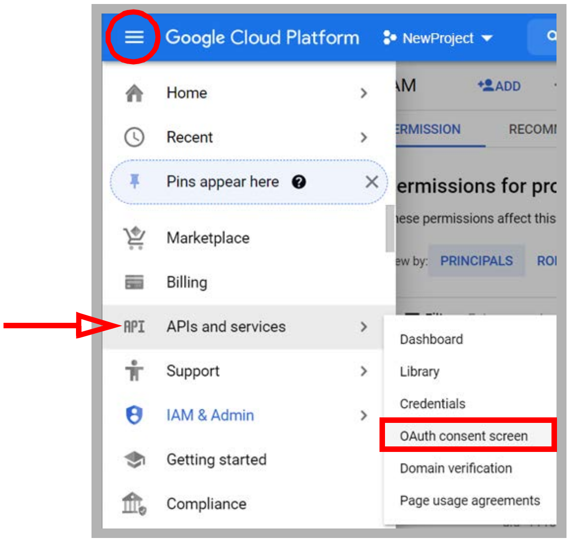
Private key saved to your computer

newproject-098765-123a456b7890.p12 allows access to your cloud resources, so store it securely.Learn more

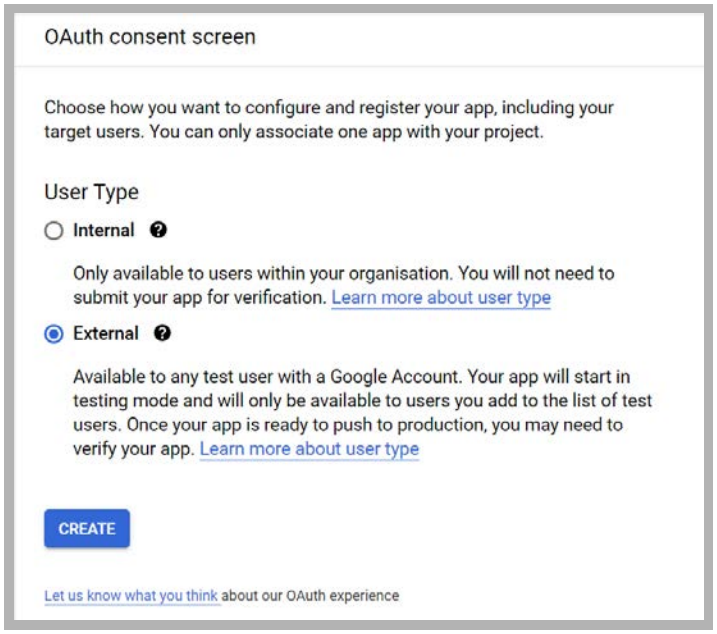
This is the password for the private key. It will not be shown again. You must present this password to use the private key.Learn more

Private key password
notasecret

13. Open the Navigation Menu and select **APIs and services**. Click **OAuth consent screen**.



14. Enable **External**, then click **CREATE**.



OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

○ Internal

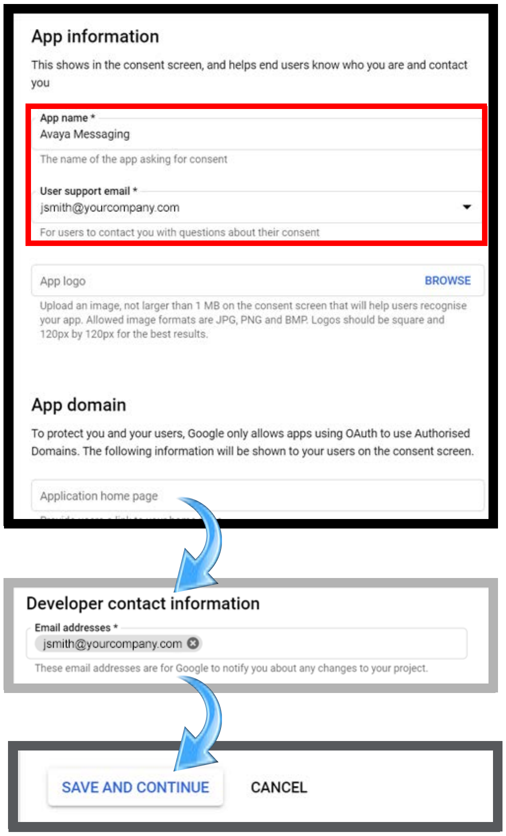
Only available to users within your organisation. You will not need to submit your app for verification. Learn more about user type

● External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. Learn more about user type

Let us know what you think about our OAuth experience

15. Enter an **App name** for this configuration.
Provide a **User support email** address where users can find out more about their consent.
When ready, click **SAVE AND CONTINUE**.



App information

This shows in the consent screen, and helps end users know who you are and contact you

App name * Avaya Messaging

The name of the app asking for consent

User support email * jsmith@yourcompany.com

For users to contact you with questions about their consent

App logo

Upload an image, not larger than 1 MB on the consent screen that will help users recognise your app. Allowed image formats are JPG, PNG and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorised Domains. The following information will be shown to your users on the consent screen.

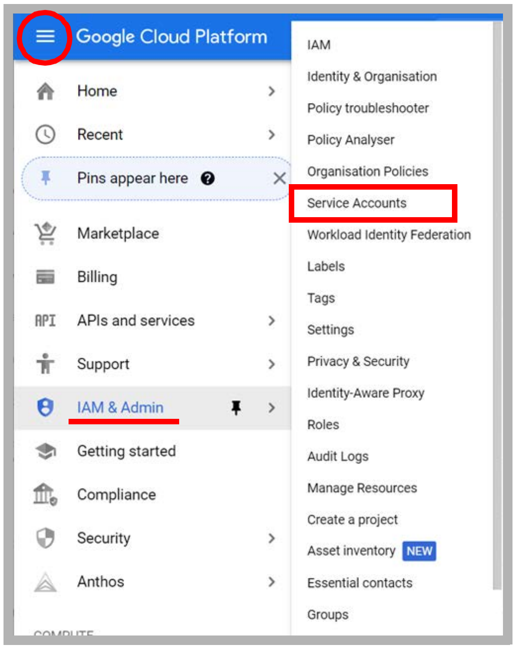
Application home page

Developer contact information

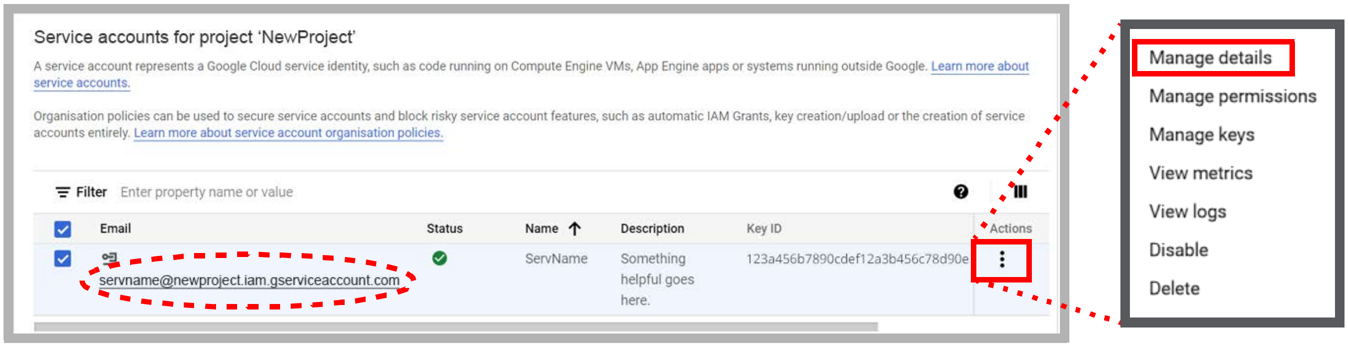
Email addresses * jsmith@yourcompany.com

These email addresses are for Google to notify you about any changes to your project.

16. From the Navigation menu, go to **IAM & admin > Service accounts**.



17. For the account you just created, click the **Actions** icon and choose **Manage Details**.



Service accounts for project 'NewProject'

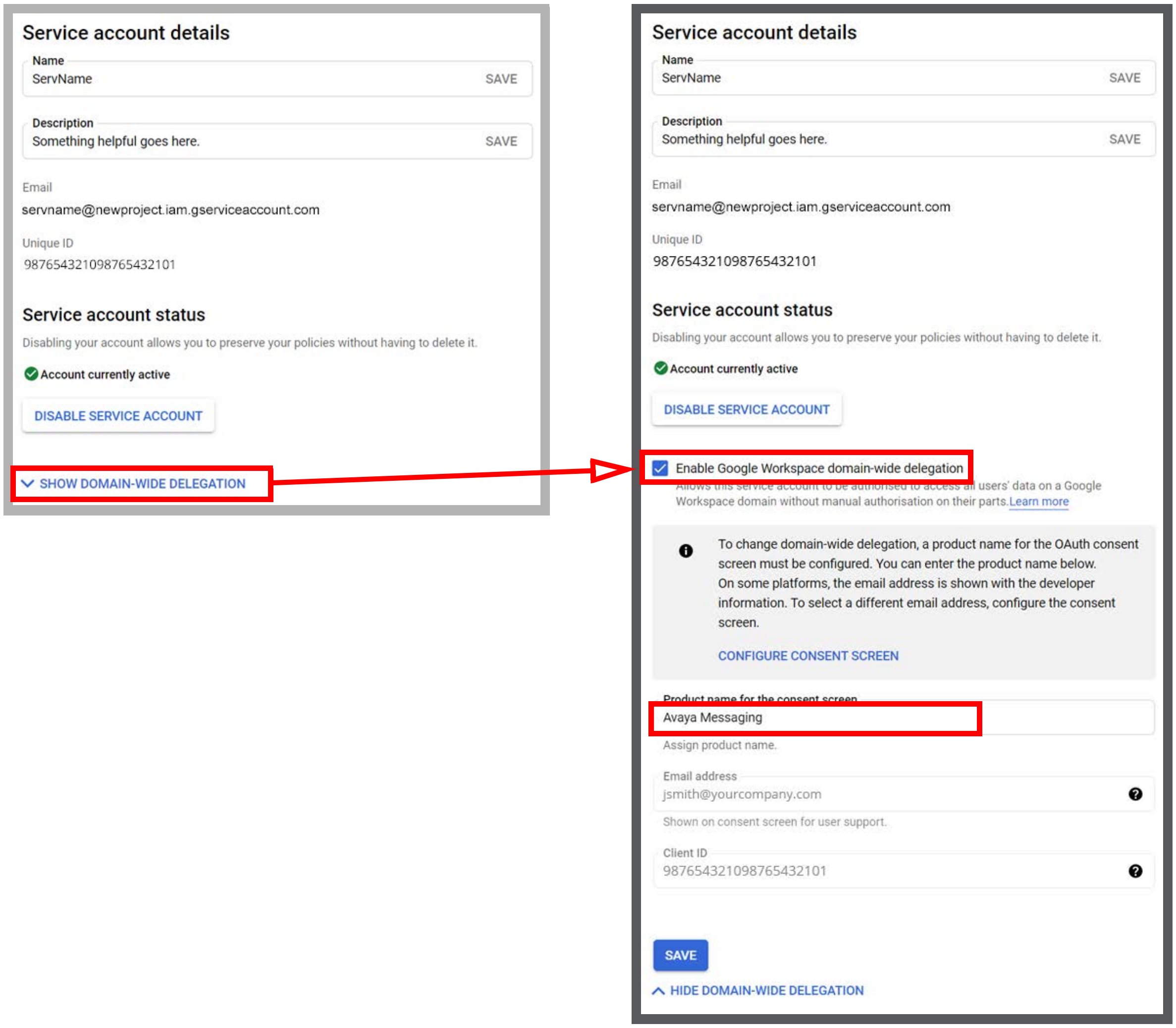
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems running outside Google. Learn more about service accounts.

Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload or the creation of service accounts entirely. Learn more about service account organisation policies.

Filter Enter property name or value

☑	Email	Status	Name ↑	Description	Key ID	Actions
☑	servname@newproject.iam.gserviceaccount.com	✓	ServName	Something helpful goes here.	123a456b7890cdef12a3b456c78d90e	⋮

18. Expand **SHOW DOMAIN-WIDE DELEGATION** and turn on **Enable Google Workspace domain-wide delegation**.
Enter a product name that will appear on the consent screen.
When ready, click **Save**.



Service account details

Name: ServName SAVE

Description: Something helpful goes here. SAVE

Email
servname@newproject.iam.gserviceaccount.com

Unique ID
987654321098765432101

Service account status

Disabling your account allows you to preserve your policies without having to delete it.

✓ Account currently active

DISABLE SERVICE ACCOUNT

SHOW DOMAIN-WIDE DELEGATION

Service account details

Name: ServName SAVE

Description: Something helpful goes here. SAVE

Email
servname@newproject.iam.gserviceaccount.com

Unique ID
987654321098765432101

Service account status

Disabling your account allows you to preserve your policies without having to delete it.

✓ Account currently active

DISABLE SERVICE ACCOUNT

☑ Enable Google Workspace domain-wide delegation
Allows this service account to be authorised to access all users' data on a Google Workspace domain without manual authorisation on their parts. Learn more

To change domain-wide delegation, a product name for the OAuth consent screen must be configured. You can enter the product name below. On some platforms, the email address is shown with the developer information. To select a different email address, configure the consent screen.

CONFIGURE CONSENT SCREEN

Product name for the consent screen: Avaya Messaging
Assign product name.

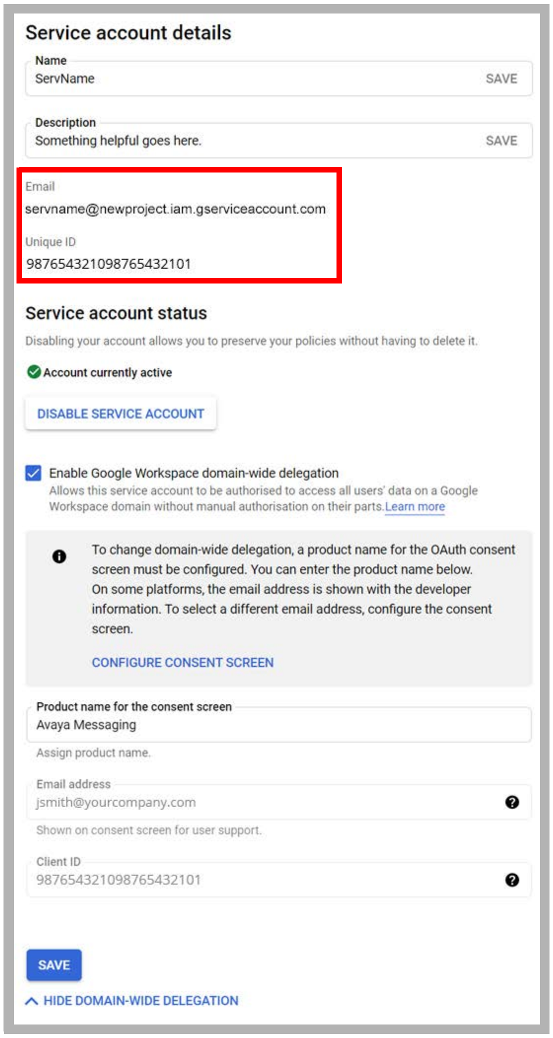
Email address: jsmith@yourcompany.com
Shown on consent screen for user support.

Client ID: 987654321098765432101

SAVE

HIDE DOMAIN-WIDE DELEGATION

19. On this screen, record the **Email address** (for step 24) and the **Unique ID** (for step 28).



Service account details

Name
ServName SAVE

Description
Something helpful goes here. SAVE

Email
servname@newproject.iam.gserviceaccount.com

Unique ID
987654321098765432101

Service account status

Disabling your account allows you to preserve your policies without having to delete it.

Account currently active

DISABLE SERVICE ACCOUNT

☑ Enable Google Workspace domain-wide delegation
Allows this service account to be authorised to access all users' data on a Google Workspace domain without manual authorisation on their parts. Learn more

To change domain-wide delegation, a product name for the OAuth consent screen must be configured. You can enter the product name below.
On some platforms, the email address is shown with the developer information. To select a different email address, configure the consent screen.

CONFIGURE CONSENT SCREEN

Product name for the consent screen
Avaya Messaging
Assign product name.

Email address
jsmith@yourcompany.com
Shown on consent screen for user support.

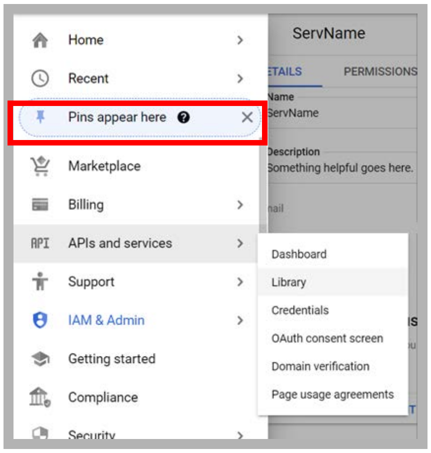
Client ID
987654321098765432101

SAVE

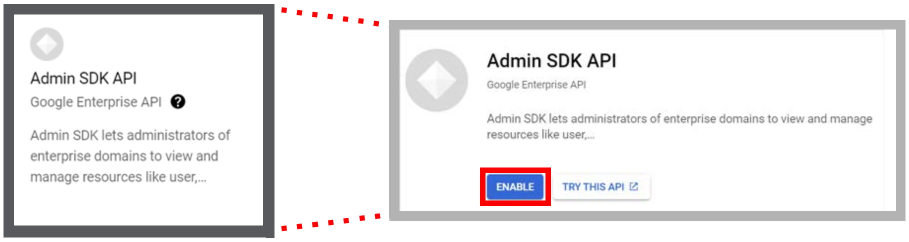
HIDE DOMAIN-WIDE DELEGATION

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.

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



21. Under the **Google Workspace** category, select **Admin SDK API**. You may need to click **View all** to see this item. Click **Enable**.



Admin SDK API

Google Enterprise API

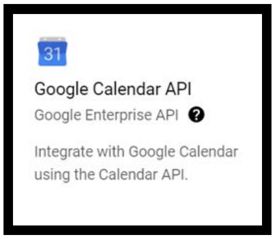
Admin SDK lets administrators of enterprise domains to view and manage resources like user,...

Admin SDK API

Google Enterprise API

Admin SDK lets administrators of enterprise domains to view and manage resources like user,...

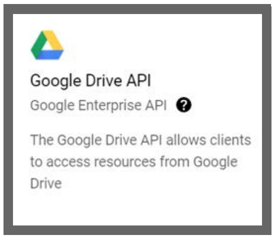
22. Once enabled, return to the Google Workspace page (**APIs & Services > Library**). Repeat to enable all of the following APIs:
    - **Google Calendar API**
    - **Google Drive API**
    - **Gmail API**



Google Calendar API

Google Enterprise API

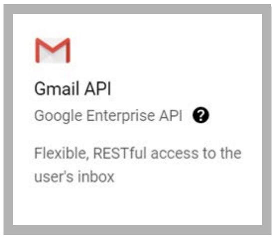
Integrate with Google Calendar using the Calendar API.



Google Drive API

Google Enterprise API

The Google Drive API allows clients to access resources from Google Drive

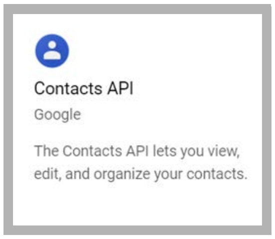


Gmail API

Google Enterprise API

Flexible, RESTful access to the user's inbox

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



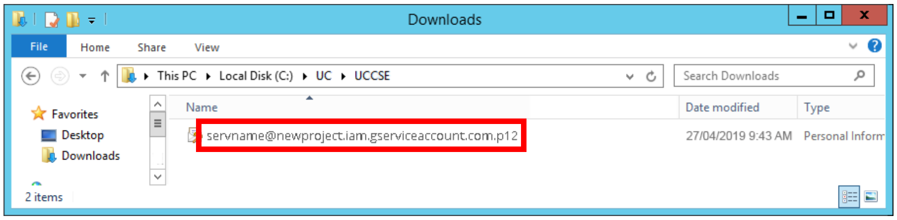
Contacts API

Google

The Contacts API lets you view, edit, and organize your contacts.

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. See **Minimum Required Scopes and APIs by Product** for details.

24. 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.



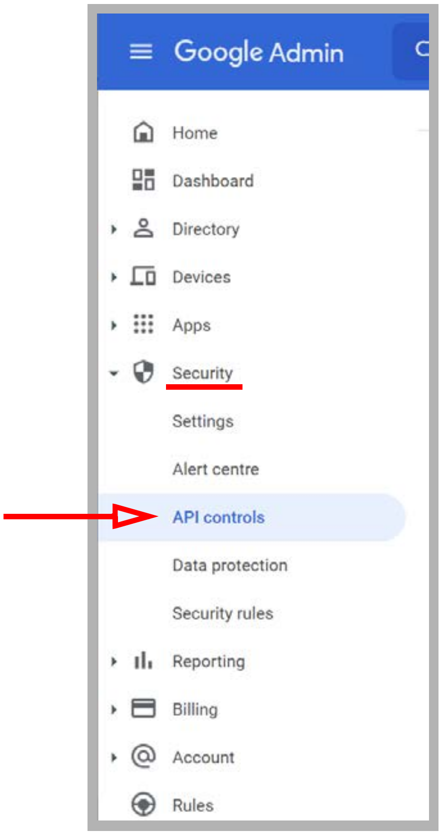
Downloads

Name	Date modified	Type
servname@newproject.iam.gserviceaccount.com.p12	27/04/2019 9:43 AM	Personal Inform

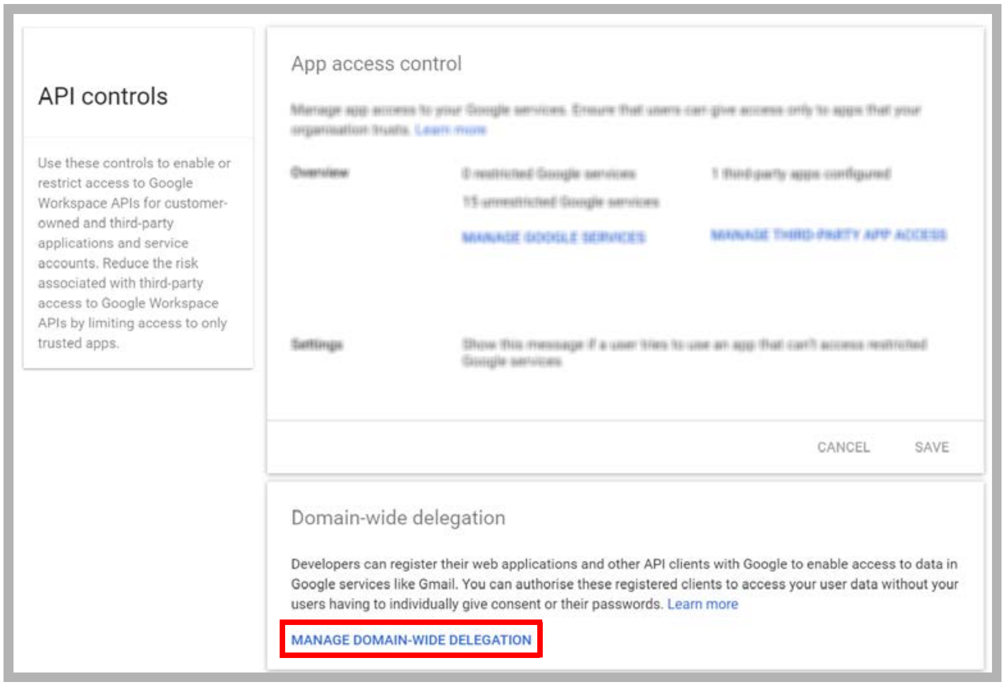
Caution: **Do Not change** the extension of the file. Always ensure it retains the P12 extension.

Domain Setup

25. Go to admin.google.com and login to Google as an administrator. In the left-hand panel, open **Security > API controls**.



26. Click **MANAGE DOMAIN-WIDE DELEGATION**.



API controls

Use these controls to enable or restrict access to Google Workspace APIs for customer-owned and third-party applications and service accounts. Reduce the risk associated with third-party access to Google Workspace APIs by limiting access to only trusted apps.

App access control

Manage app access to your Google services. Ensure that users can give access only to apps that your organisation trusts. Learn more

Overview

0 restricted Google services

15 unrestricted Google services

MANAGE GOOGLE SERVICES

1 third-party apps configured

MANAGE THIRD-PARTY APP ACCESS

Settings

Show this message if a user tries to use an app that can't access restricted Google services

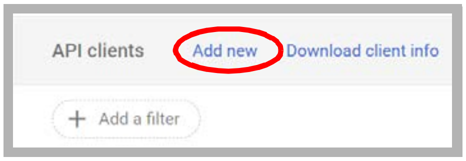
CANCEL SAVE

Domain-wide delegation

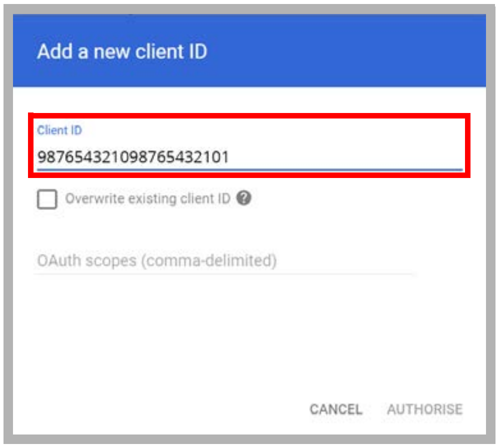
Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorise these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

MANAGE DOMAIN-WIDE DELEGATION

27. Click **Add new**.



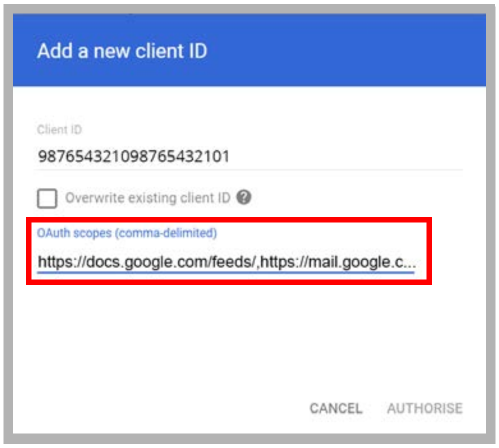
28. In the space provided, enter the **Unique ID** from step 19.



Client ID
98765432109876543210 1

29. In the space for **OAuth scopes**, enter the following string:

```
https://docs.google.com/feeds/,https://mail.google.com/,https://
www.google.com/m8/feeds/,https://www.googleapis.com/auth/calendar
```



Client ID
98765432109876543210 1

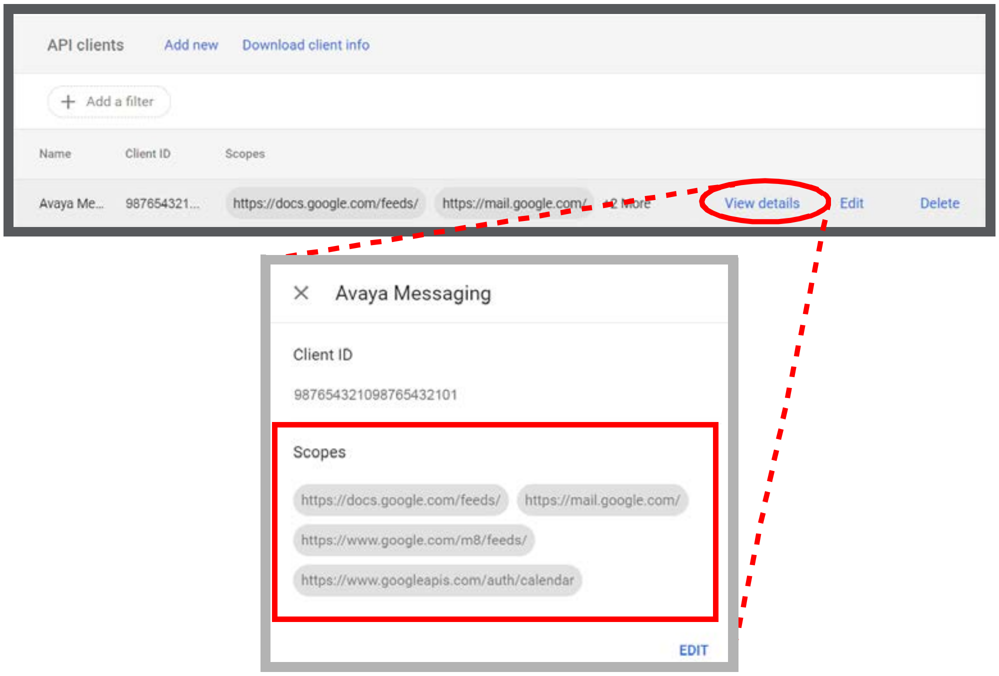
OAuth scopes (comma-delimited)
https://docs.google.com/feeds/,https://mail.google.c...

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. See **Minimum Required Scopes and APIs by Product** for details.

30. When ready, click **Authorize**.

31. Verify that the selected scopes were successfully installed.



Name	Client ID	Scopes
Avaya Me...	987654321...	https://docs.google.com/feeds/ https://mail.google.com/ +2 More

Avaya Messaging

Client ID

987654321098765432101

Scopes

https://docs.google.com/feeds/ https://mail.google.com/ https://www.google.com/m8/feeds/ https://www.googleapis.com/auth/calendar

The scopes are:

docs.google.com/feeds
mail.google.com
www.google.com/m8/feeds
www.googleapis.com/auth/calendar

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**).

Minimum Required Scopes and APIs by Product

Enabling all of the listed scopes and APIs will work for most situations. However, not all administrators will want to open all of these channels if it is not necessary. This table shows the minimum required scopes and APIs for each product.

		AVAYA CLOUD APPLICATION LINK	**AVAYA WORKSPACES** (CHROME EXTENSION)	**AVAYA COMMUNICATOR FOR WEB**
SCOPES * (see below)	auth/admin	•	•	•
	auth/calendar			
	auth/drive	•		
	auth/drive.file	•		
	calendar/feeds	•	•	•
	calendar/resource			
	m8/feeds	•	•	•
	mail.google.com	•		
APIs	Admin SDK	•	•	•
	Contacts API	•	•	•
	Google Calendar API	•	•	•
	Google Drive API	•		
	GMail API	•		

* The full paths for all listed scopes are displayed here.

auth/admin - https://www.googleapis.com/auth/admin.directory.user.readonly
auth/calendar - https://www.googleapis.com/auth/calendar
auth/drive - https://www.googleapis.com/auth/drive
auth/drive.file - https://www.googleapis.com/auth/drive.file
calendar/feeds - https://www.google.com/calendar/feeds/
calendar/resource - https://apps-apis.google.com/a/feeds/calendar/resource/
m8/feeds - https://www.google.com/m8/feeds/
mail.google.com - https://mail.google.com/

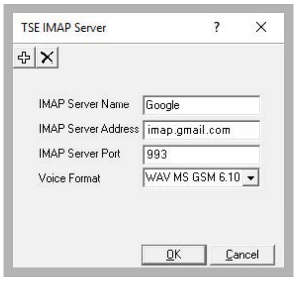
Configuring Avaya Messaging for use with OAuth 2.0

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.

32. Open **Avaya Messaging Admin**.

33. Right-click on **TSE IMAP Server** and select **New > TSE IMAP Server**.

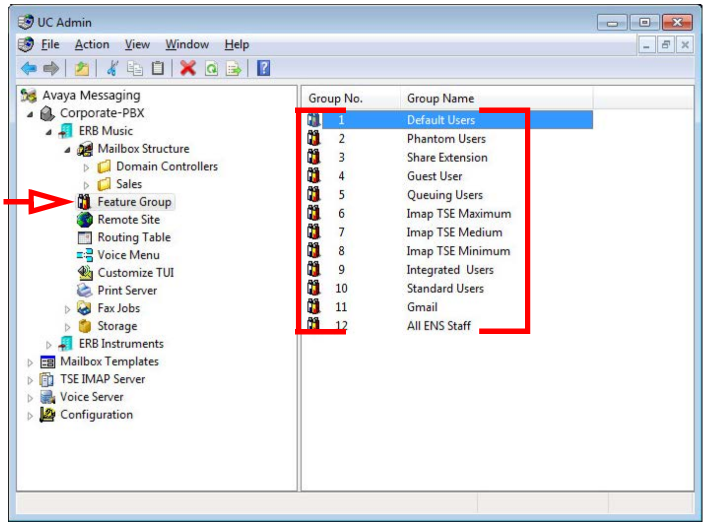


IMAP Server Name	Google
IMAP Server Address	imap.gmail.com
IMAP Server Port	993
Voice Format	WAV MS GSM 6.10

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.

Click **OK** when ready.

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



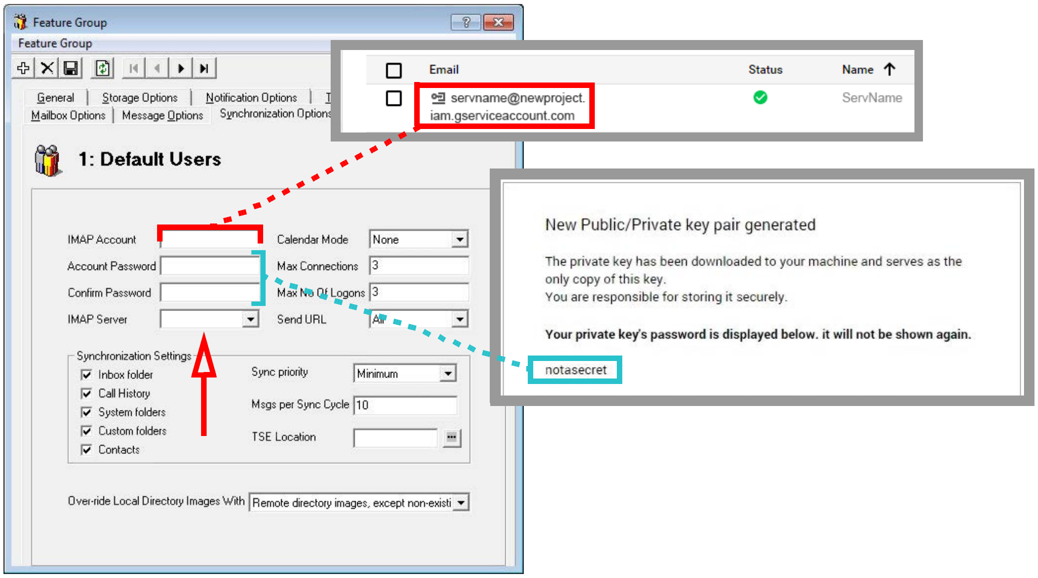
Group No.	Group Name
1	Default Users
2	Phantom Users
3	Share Extension
4	Guest User
5	Queuing Users
6	Imap TSE Maximum
7	Imap TSE Medium
8	Imap TSE Minimum
9	Integrated Users
10	Standard Users
11	Gmail
12	All ENS Staff

35. 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**.



Feature Group

Feature Group

General | Storage Options | Notification Options | T
Mailbox Options | Message Options | Synchronization Options

1: Default Users

IMAP Account:
Account Password:
Confirm Password:
IMAP Server:
Calendar Mode: None
Max Connections: 3
Max No Of Logons: 3
Send URL: All

Synchronization Settings
☑ Inbox folder
☑ Call History
☑ System folders
☑ Custom folders
☑ Contacts

Sync priority: Minimum
Msgs per Sync Cycle: 10
TSE Location:

Over-ride Local Directory Images With: Remote directory images, except non-existi

□	Email	Status	Name ↑
□	servname@newproject.iam.gserviceaccount.com	✓	ServName

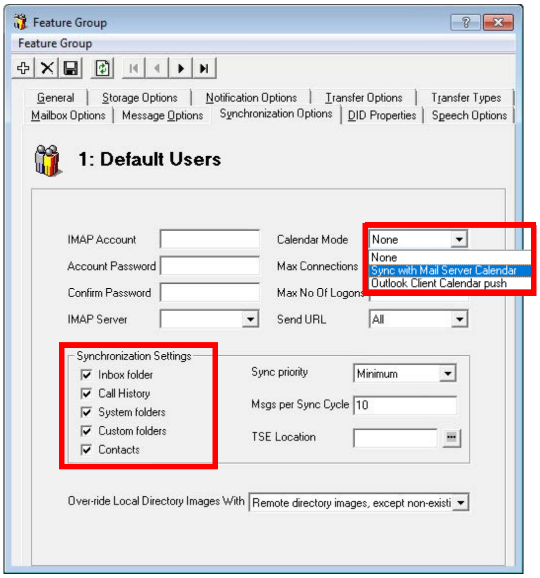
New Public/Private key pair generated

The private key has been downloaded to your machine and serves as the only copy of this key.
You are responsible for storing it securely.

Your private key's password is displayed below. it will not be shown again.

notasecret

36. 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.



Feature Group

Feature Group

General | Storage Options | Notification Options | Transfer Options | Transfer Types
Mailbox Options | Message Options | Synchronization Options | DID Properties | Speech Options

1: Default Users

IMAP Account:
Account Password:
Confirm Password:
IMAP Server:
Calendar Mode: None
None
Sync with Mail Server Calendar
Outlook Client Calendar push
Max Connections
Max No Of Logons
Send URL: All

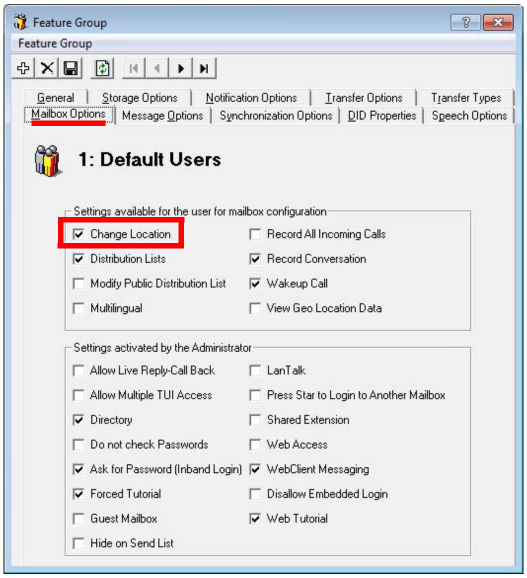
Synchronization Settings
☑ Inbox folder
☑ Call History
☑ System folders
☑ Custom folders
☑ Contacts

Sync priority: Minimum
Msgs per Sync Cycle: 10
TSE Location:

Over-ride Local Directory Images With: Remote directory images, except non-existi

37. Click **Save** 💾 to preserve the changes.

38. 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.



1: Default Users

Settings available for the user for mailbox configuration

- ☑ Change Location
- ☑ Distribution Lists
- ☐ Modify Public Distribution List
- ☐ Multilingual
- ☐ Record All Incoming Calls
- ☑ Record Conversation
- ☑ Wakeup Call
- ☐ View Geo Location Data

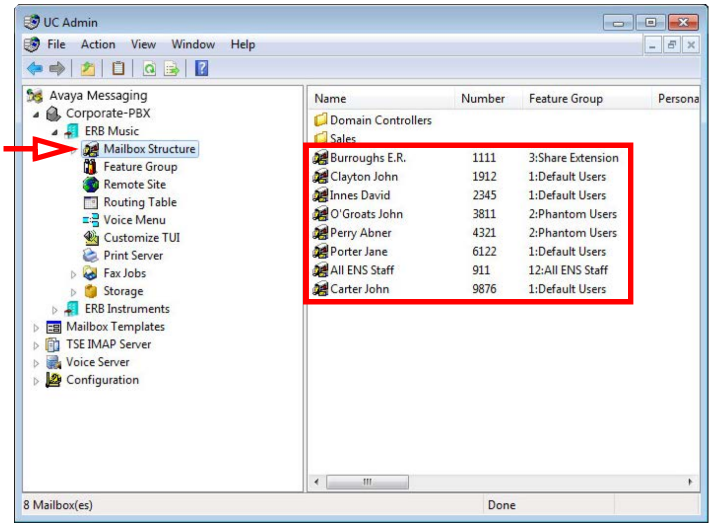
Settings activated by the Administrator

- ☐ Allow Live Reply-Call Back
- ☐ Allow Multiple TUI Access
- ☑ Directory
- ☐ Do not check Passwords
- ☑ Ask for Password (Inband Login)
- ☑ Forced Tutorial
- ☐ Guest Mailbox
- ☐ Hide on Send List
- ☐ LanTalk
- ☐ Press Star to Login to Another Mailbox
- ☐ Shared Extension
- ☐ Web Access
- ☑ WebClient Messaging
- ☐ Disallow Embedded Login
- ☑ Web Tutorial

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.

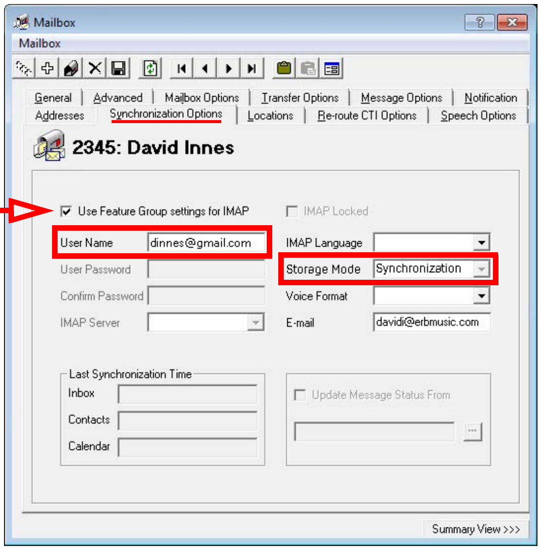
39. Click **Save** 💾 to preserve the changes.

40. In AM Admin, open **Mailbox Structure** and double-click a client to modify.



Name	Number	Feature Group	Persona
Domain Controllers			
Sales			
Burroughs E.R.	1111	3:Share Extension	
Clayton John	1912	1:Default Users	
Innes David	2345	1:Default Users	
O'Groats John	3811	2:Phantom Users	
Perry Abner	4321	2:Phantom Users	
Porter Jane	6122	1:Default Users	
All ENS Staff	911	12:All ENS Staff	
Carter John	9876	1:Default Users	

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


Mailbox
Mailbox
General | Advanced | Mailbox Options | Transfer Options | Message Options | Notification
Addresses | Synchronization Options | Locations | Re-route CTI Options | Speech Options
Summary View >>>

2345: David Innes

☑ Use Feature Group settings for IMAP

□ IMAP Locked

User Name	dinnes@gmail.com	IMAP Language	
User Password		Storage Mode	Synchronization
Confirm Password		Voice Format	
IMAP Server		E-mail	davidi@erbmusic.com

Last Synchronization Time

Inbox

Contacts

Calendar

□ Update Message Status From

42. 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.

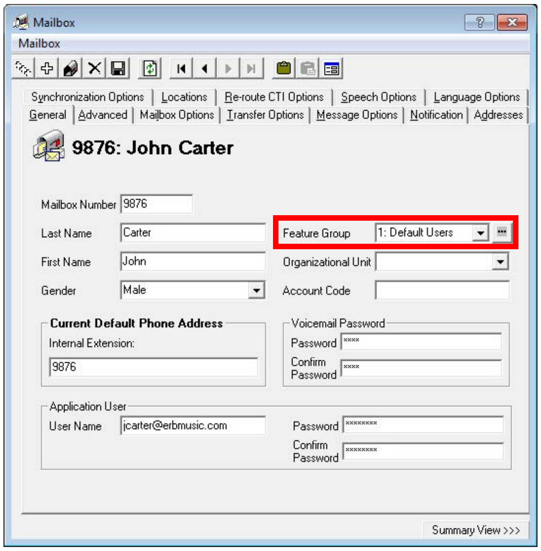
43. Click **Save** to preserve the changes.

44. 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.

45. Repeat steps 40 through 43 for each client that requires OAuth 2.0 synchronization.

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


Mailbox
Mailbox
Synchronization Options | Locations | Re-route CTI Options | Speech Options | Language Options
General | Advanced | Mailbox Options | Transfer Options | Message Options | Notification | Addresses
Summary View >>>

9876: John Carter

Mailbox Number	9876		
Last Name	Carter	Feature Group	1: Default Users
First Name	John	Organizational Unit	
Gender	Male	Account Code	

Current Default Phone Address

Internal Extension: 9876

Voicemail Password

Password ****

Confirm Password ****

Application User

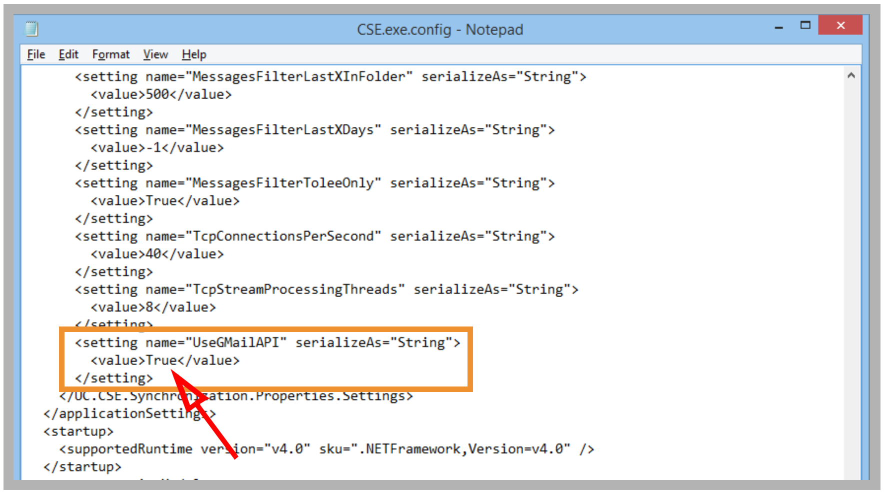
User Name jcarter@erbmusic.com

Password ********

Confirm Password ********

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

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



```
      <setting name="MessagesFilterLastXInFolder" serializeAs="String">
        <value>500</value>
      </setting>
      <setting name="MessagesFilterLastXDays" serializeAs="String">
        <value>-1</value>
      </setting>
      <setting name="MessagesFilterToleeOnly" serializeAs="String">
        <value>True</value>
      </setting>
      <setting name="TcpConnectionsPerSecond" serializeAs="String">
        <value>40</value>
      </setting>
      <setting name="TcpStreamProcessingThreads" serializeAs="String">
        <value>8</value>
      </setting>
      <setting name="UseGMailAPI" serializeAs="String">
        <value>True</value>
      </setting>
    </UC.CSE.Synchronization.Properties.Settings>
  </applicationSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0" />
  </startup>
```

    Go to **File > Save** to complete the change.

48. 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 this 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

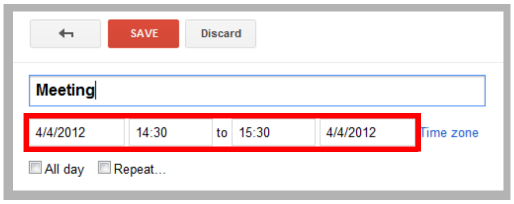
In order to consolidate all messages (e.g. voice, text, fax, etc.) in a single email account, synchronize your Gmail or Google Apps email with the UC server's Web Access mailbox. If your organization is using OAuth2 authorization, you will not have to enter any details beyond the email address.

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 filters 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.



Meeting

4/4/2012 14:30 to 15:30 4/4/2012

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

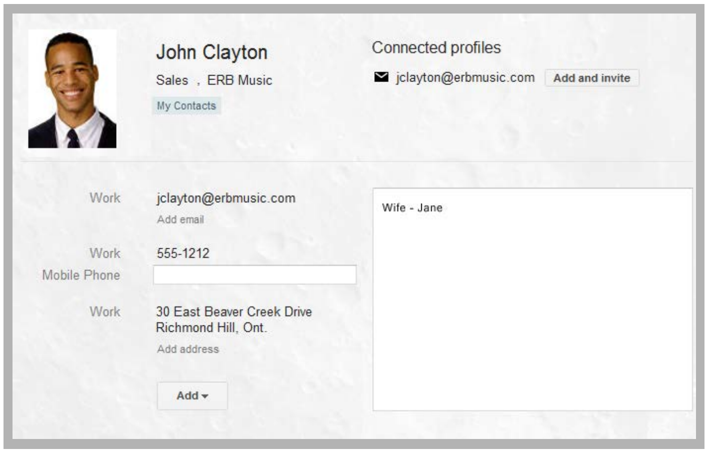
Note: All your calendar events and contacts from your current mail server will be populated into your Avaya Messaging mailbox right after your administrator finishes the configuration.

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.



John Clayton

Sales , ERB Music

My Contacts

Connected profiles

jclayton@erbmusic.com

Work jclayton@erbmusic.com

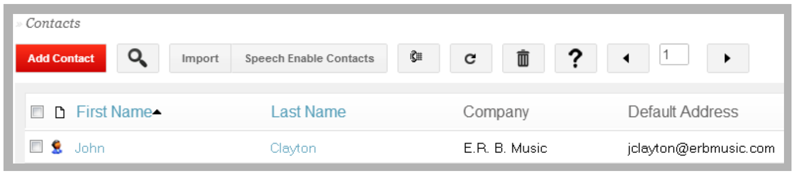
Work 555-1212

Mobile Phone

Work 30 East Beaver Creek Drive
Richmond Hill, Ont.

Wife - Jane

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



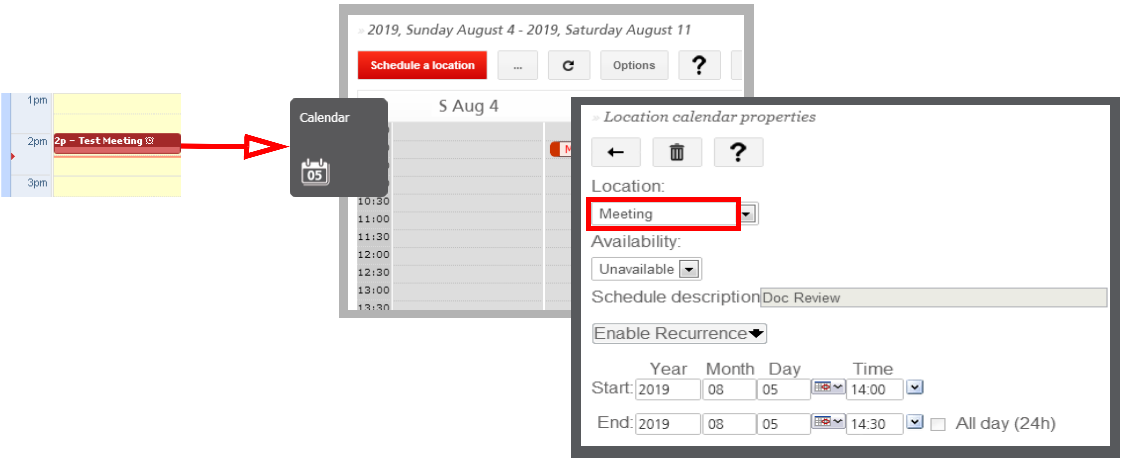
Contacts

□	First Name▲	Last Name	Company	Default Address
□	John	Clayton	E.R. B. Music	jclayton@erbmusic.com

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.



Location: Meeting
Availability: Unavailable
Schedule description Doc Review
Enable Recurrence

	Year	Month	Day	Time
Start:	2019	08	05	14:00
End:	2019	08	05	14:30

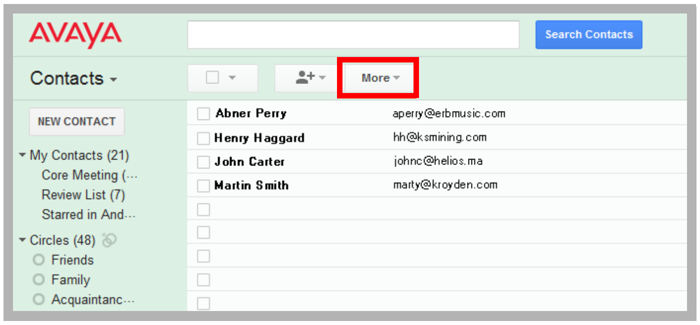
□ All day (24h)

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 contacts window.

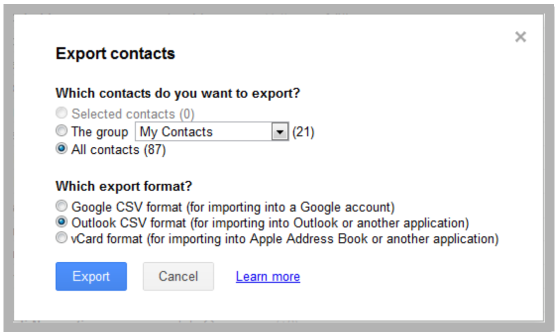


Abner Perry	aperry@erbmusic.com
Henry Haggard	hh@ksmining.com
John Carter	johnc@helios.ma
Martin Smith	marty@kroyden.com

3. You can choose to export selected contact, 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.



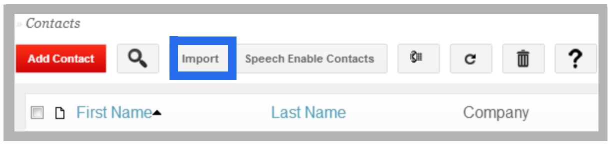
Export contacts

Which contacts do you want to export?
○ Selected contacts (0)
○ The group My Contacts (21)
● All contacts (87)

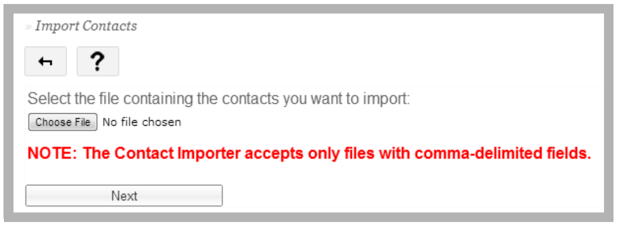
Which export format?
○ Google CSV format (for importing into a Google account)
● Outlook CSV format (for importing into Outlook or another application)
○ vCard format (for importing into Apple Address Book or another application)

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.



Import Contacts

Select the file containing the contacts you want to import:

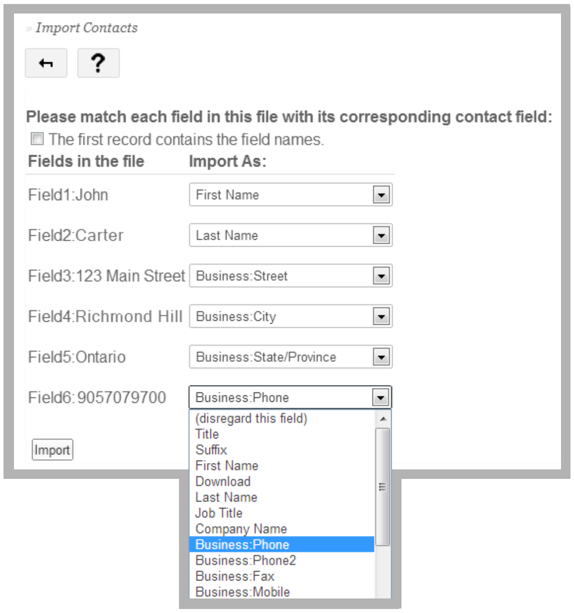
Choose File No file chosen

NOTE: The Contact Importer accepts only files with comma-delimited fields.

Next

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.



Import Contacts

Please match each field in this file with its corresponding contact field:

□ The first record contains the field names.

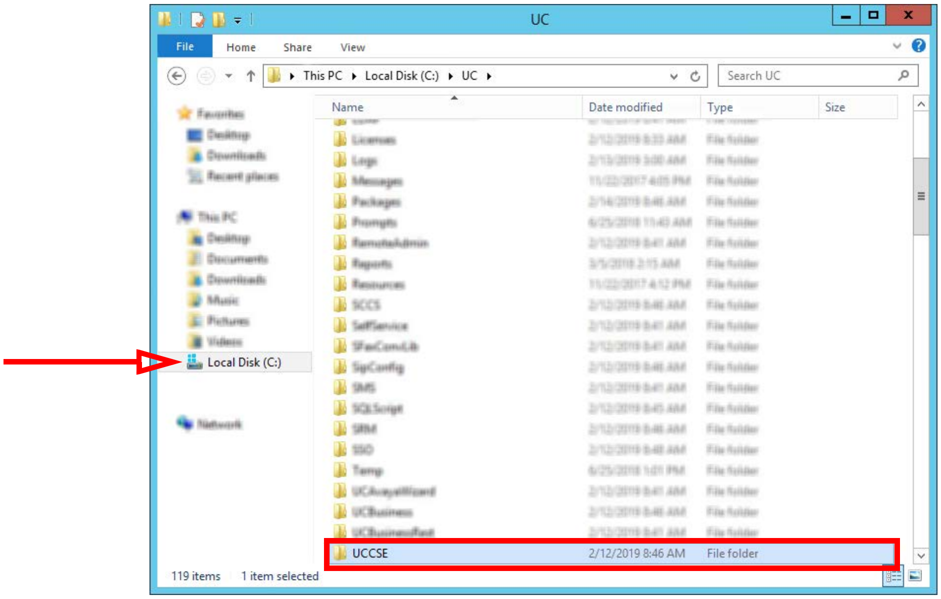
Fields in the file	Import As:
Field1:John	First Name
Field2:Carter	Last Name
Field3:123 Main Street	Business:Street
Field4:Richmond Hill	Business:City
Field5:Ontario	Business:State/Province
Field6:9057079700	Business:Phone

Reconfiguring Synchronization Components for Gmail

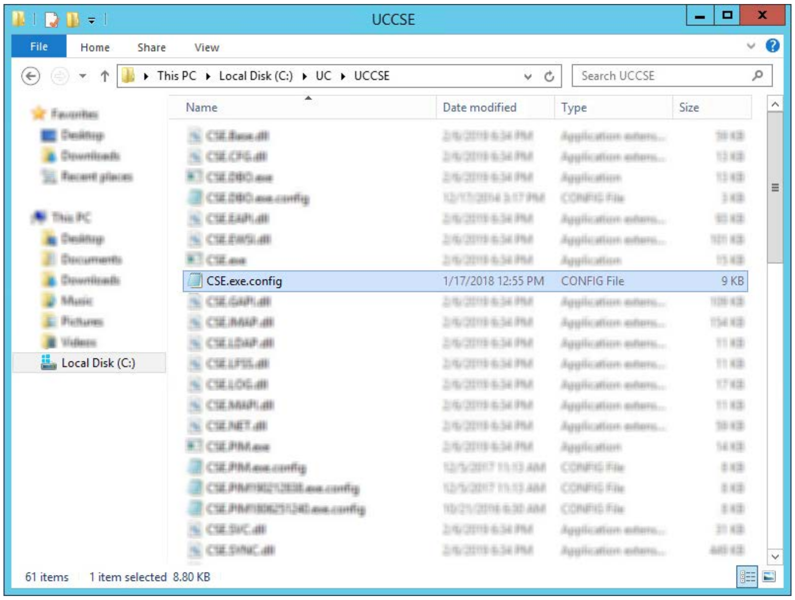
Once the installation has been completed, verify that the system configuration files are set to use GMAIL. This should be done on all servers running CSE: The voice server in a single server environment, the Consolidated server under HA, and all remote CSE servers operating.

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.

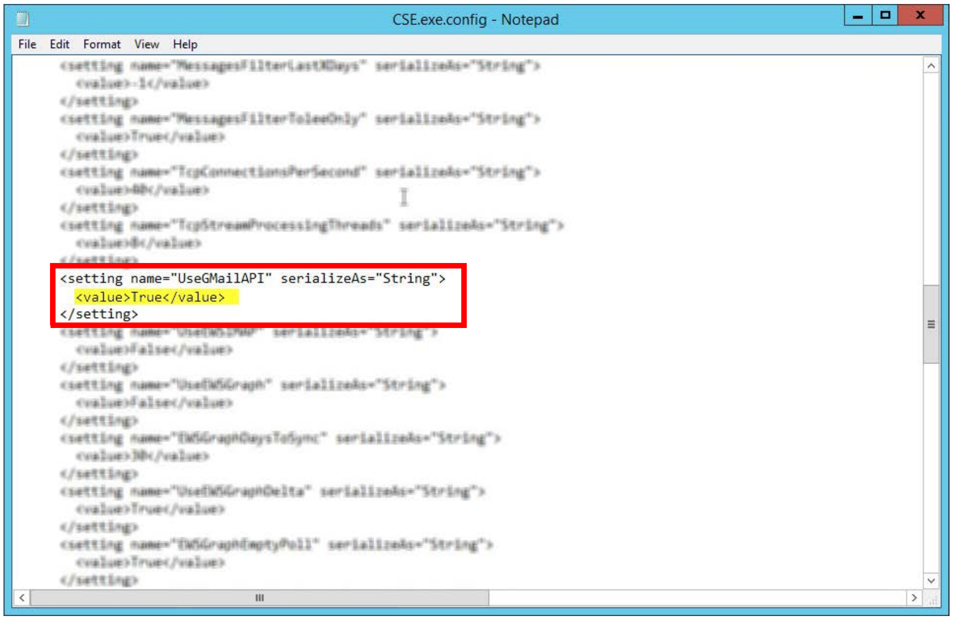


2. Within the folder, open the **CSE.exe.config** file in a text editor such as NotePad.



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

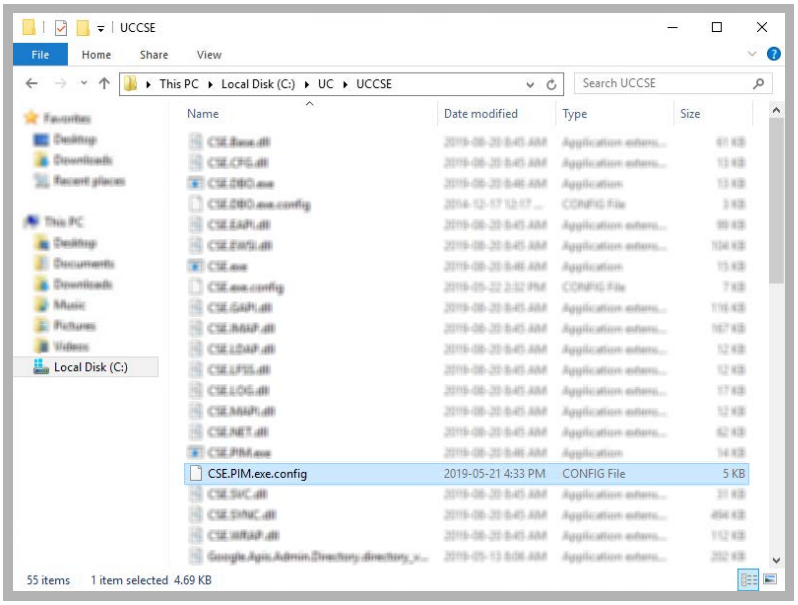
```
<setting name=”UseGMailAPI” serializeAs=“String”>
    <value>True</value>
</setting>
```



```
<setting name="MessagesFilterLastXDays" serializeAs="String">
  <value>-1</value>
</setting>
<setting name="MessagesFilterToleeOnly" serializeAs="String">
  <value>True</value>
</setting>
<setting name="TcpConnectionsPerSecond" serializeAs="String">
  <value>80</value>
</setting>
<setting name="TcpStreamProcessingThreads" serializeAs="String">
  <value>8</value>
</setting>
<setting name="UseGMailAPI" serializeAs="String">
  <value>True</value>
</setting>
<setting name="UseEWSIMAP" serializeAs="String">
  <value>False</value>
</setting>
<setting name="UseEWSGraph" serializeAs="String">
  <value>False</value>
</setting>
<setting name="EWSGraphDaysToSync" serializeAs="String">
  <value>30</value>
</setting>
<setting name="UseEWSGraphDelta" serializeAs="String">
  <value>True</value>
</setting>
<setting name="EWSGraphEmptyPoll" 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.

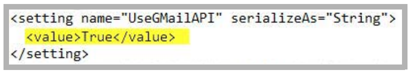


Name	Date modified	Type	Size
CSE.Base.dll	2019-08-20 8:45 AM	Application extens...	61 KB
CSE.CFG.dll	2019-08-20 8:45 AM	Application extens...	13 KB
CSE.DBO.exe	2019-08-20 8:46 AM	Application	13 KB
CSE.DBO.exe.config	2014-12-17 12:17 ...	CONFIG File	3 KB
CSE.EAPI.dll	2019-08-20 8:45 AM	Application extens...	99 KB
CSE.EWSI.dll	2019-08-20 8:45 AM	Application extens...	104 KB
CSE.exe	2019-08-20 8:46 AM	Application	15 KB
CSE.exe.config	2019-05-22 2:32 PM	CONFIG File	7 KB
CSE.GAPI.dll	2019-08-20 8:45 AM	Application extens...	116 KB
CSE.IMAP.dll	2019-08-20 8:45 AM	Application extens...	167 KB
CSE.LDAP.dll	2019-08-20 8:45 AM	Application extens...	12 KB
CSE.LFSS.dll	2019-08-20 8:45 AM	Application extens...	12 KB
CSE.LOG.dll	2019-08-20 8:45 AM	Application extens...	17 KB
CSE.MAPI.dll	2019-08-20 8:45 AM	Application extens...	12 KB
CSE.NET.dll	2019-08-20 8:45 AM	Application extens...	62 KB
CSE.PIM.exe	2019-08-20 8:46 AM	Application	14 KB
CSE.PIM.exe.config	2019-05-21 4:33 PM	CONFIG File	5 KB
CSE.SVC.dll	2019-08-20 8:45 AM	Application extens...	31 KB
CSE.SYNC.dll	2019-08-20 8:45 AM	Application extens...	494 KB
CSE.WRAP.dll	2019-08-20 8:45 AM	Application extens...	112 KB
Google.Apis.Admin.Directory.directory_v...	2019-05-13 8:06 AM	Application extens...	202 KB

55 items   1 item selected 4.69 KB

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

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



```
<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.

10 EXCHANGE 2019/2016/2013 INTEGRATION: USING EWS

In This Chapter:

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 suites your requirements.

CHAPTER	INTEGRATION	WHY YOU WANT IT
9	Google	Creates a secure connection through OAuth2 to your Gmail and Google Apps accounts.
10	Exchange using EWS	The simplest connection between your Exchange server and Avaya Messaging.
11	Exchange without EWS	A connection between Exchange and Avaya Messaging for legacy systems.
12	Exchange 2010	A connection between Exchange 2010 and Avaya Messaging.
13	Office 365 using Graph	Setup the latest high security integration procedures for maximum data integrity.
14	Office 365 using EWS	Quick connection between your O365 server and Avaya Messaging.

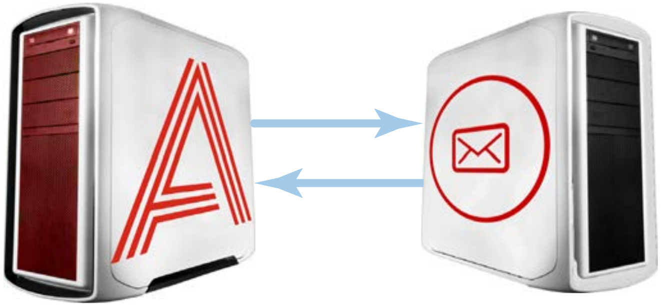
Introduction

Avaya Messaging and an Exchange server are able to 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.

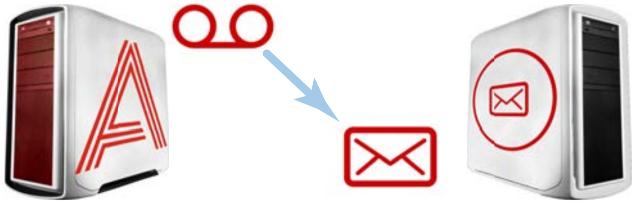
The use of EWS for Exchange 2019 and 2016 is required since IMAP is no longer supported. When using Exchange 2013, the use of EWS is optional and follows the same procedures. This chapter may be applied to both versions.

Visual Guide

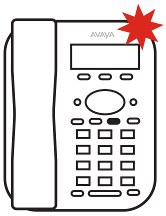


Data is synchronized between the Voice and Mail servers. Message status and deletions are synchronized almost instantly between the two, allowing a single message store for easier management for both administrators and end users.

You may also choose to synchronize Contact and Calendar data between the two servers along with messages.



In a typical situation, voice messages will be synchronized from the Voice Server to the Mail Server.



Since status is synchronized, message lights on integrated telephone systems will also be accurate no matter where the message is read or received.

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 will be 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 in order for Avaya Messaging to communicate properly.

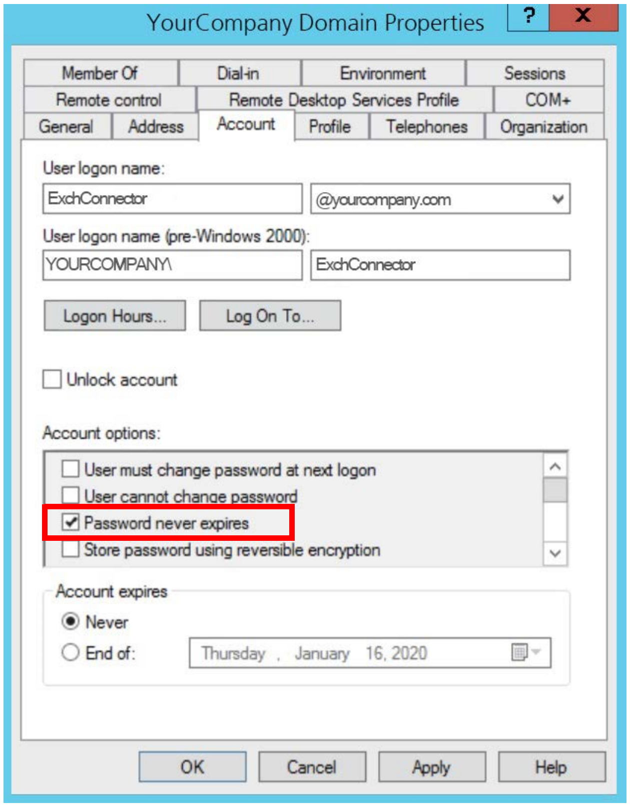
You must have a corporate Exchange server, either locally on virtually, configured and operating before proceeding.

Caution: Exchange 2019 and 2016 do not support non-EWS connections. Only EWS can be used. Exchange 2013 supports both EWS and IMAP.

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.



User logon name:

ExchConnector @yourcompany.com

User logon name (pre-Windows 2000):

YOURCOMPANY\ ExchConnector

☐ Unlock account

Account options:

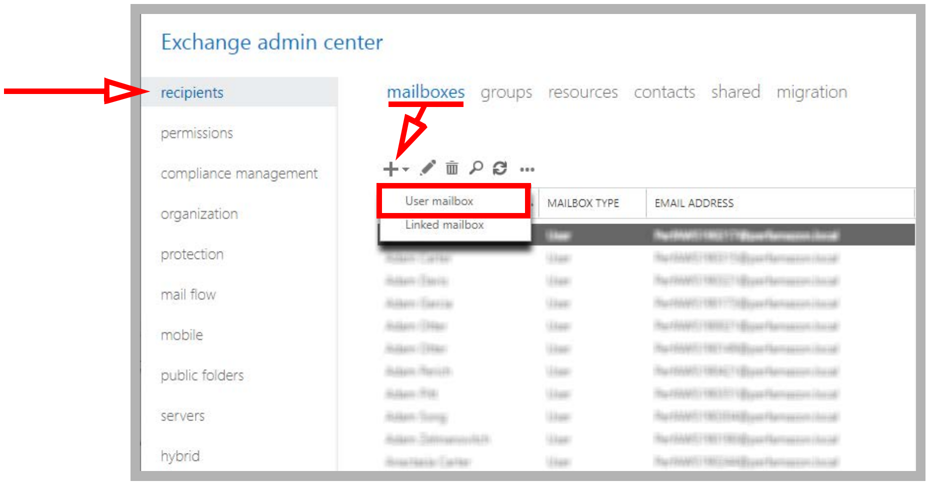
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☑ Password never expires
- ☐ Store password using reversible encryption

Account expires

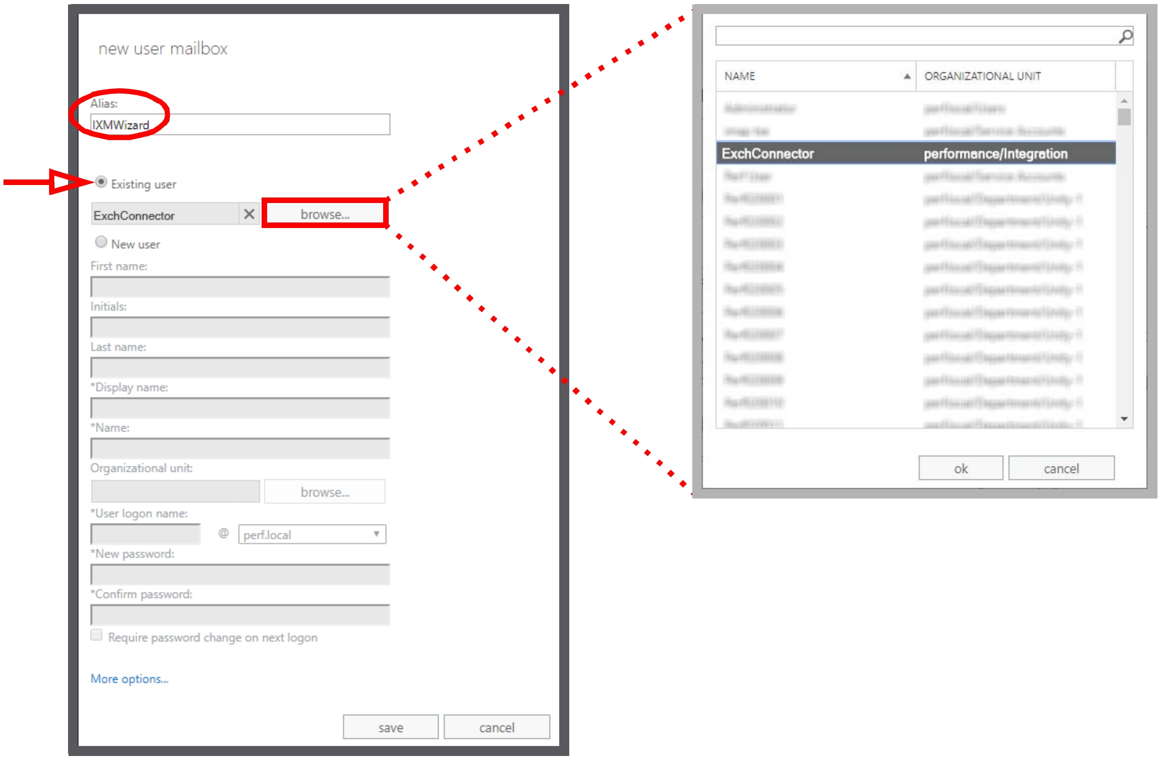
● Never

○ End of: Thursday , January 16, 2020

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.



Alias: IXMWizard

● Existing user

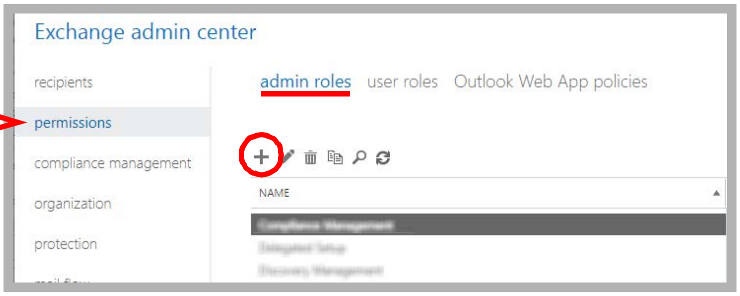
ExchConnector ✕ browse...

@ perf.local

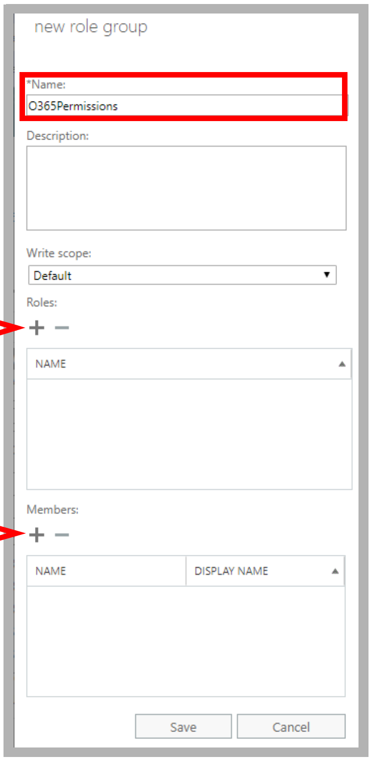
ExchConnector performance/Integration

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). Beside **Roles**, click **Add** ➕.

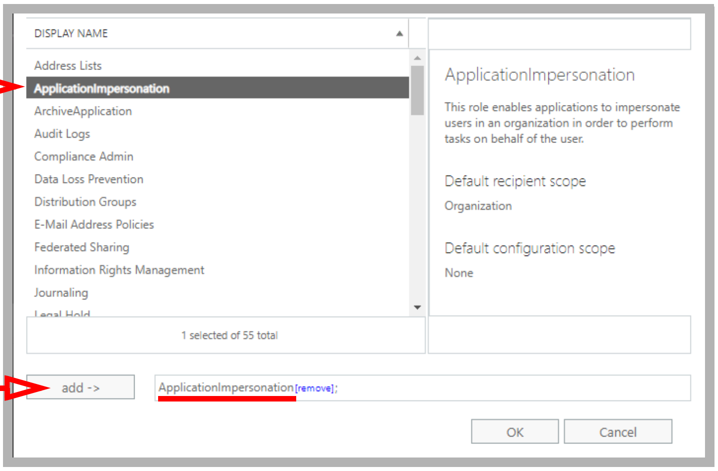

new role group

*Name: O365Permissions

Description:

Write scope: Default

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


DISPLAY NAME
Address Lists
ApplicationImpersonation
ArchiveApplication
Audit Logs
Compliance Admin
Data Loss Prevention
Distribution Groups
E-Mail Address Policies
Federated Sharing
Information Rights Management
Journaling
Legal Hold

1 selected of 55 total

ApplicationImpersonation

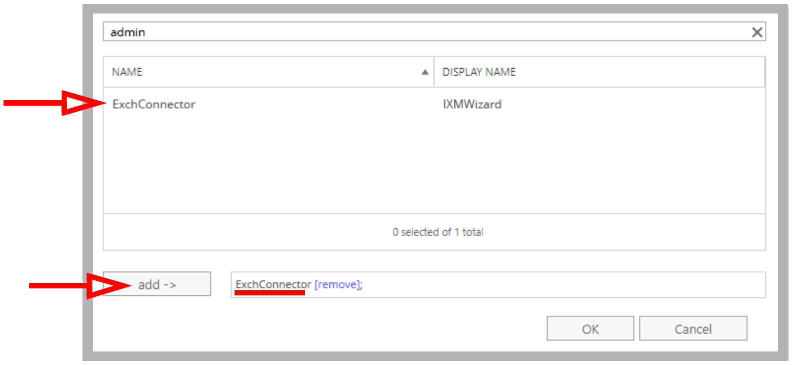
This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.

Default recipient scope
Organization

Default configuration scope
None

add -> ApplicationImpersonation[remove];

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



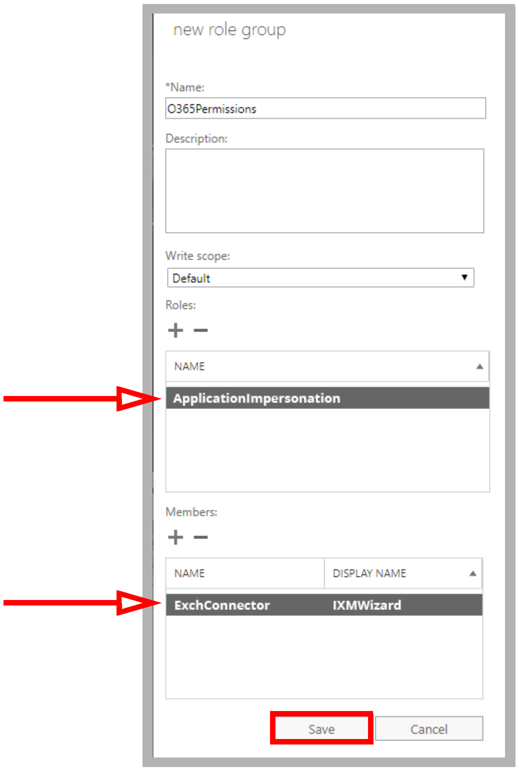
admin

NAME	DISPLAY NAME
ExchConnector	IXMWizard

0 selected of 1 total

ExchConnector [remove];

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



new role group

*Name: O365Permissions

Description:

Write scope: Default

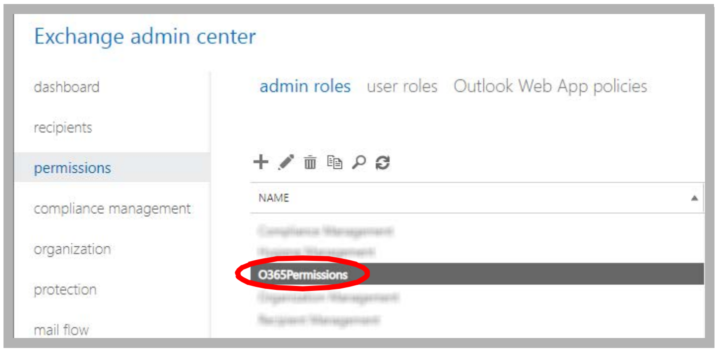
Roles:

NAME
ApplicationImpersonation

Members:

NAME	DISPLAY NAME
ExchConnector	IXMWizard

Confirm that the new role appears in the list.



Exchange admin center

NAME
[redacted]
O365Permissions
[redacted]

The new account has been created.

AM Admin Configuration

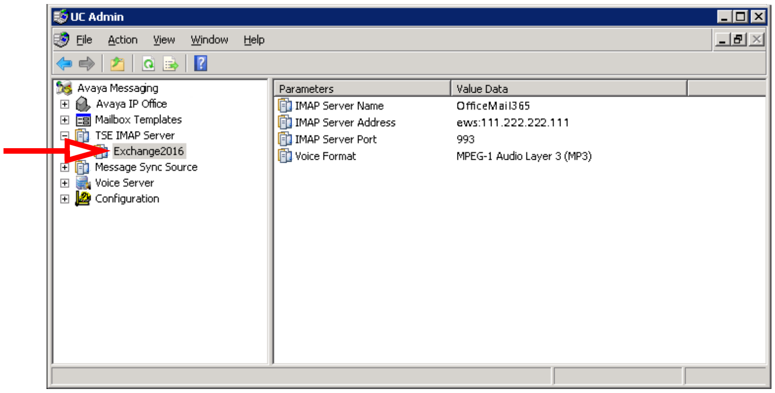
For Avaya Messaging and Exchange to be able to synchronize data, Avaya Messaging must be able to communicate with the Exchange server using the correct credentials. The superuser account streamlines this process while still enforcing individual password security protocols on each mailbox.

Adding the CSE Endpoint for EWS

In order 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. A 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.



Parameters	Value Data
IMAP Server Name	OfficeMail365
IMAP Server Address	ews:111.222.222.111
IMAP Server Port	993
Voice Format	MPEG-1 Audio Layer 3 (MP3)

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:

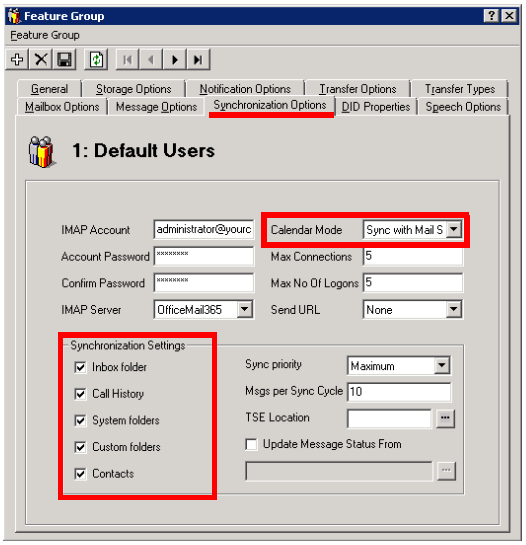
IMAP Account: Enter the user/service account created in step 3 above. Include the complete user@domain.com (e.g. **administrator@yourcompany.onmicrosoft.com**).

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.



1: Default Users

IMAP Account: administrator@yourc
Account Password: ********
Confirm Password: ********
IMAP Server: OfficeMail365
Calendar Mode: Sync with Mail S
Max Connections: 5
Max No Of Logons: 5
Send URL: None

Synchronization Settings
☑ Inbox folder
☑ Call History
☑ System folders
☑ Custom folders
☑ Contacts

Sync priority: Maximum
Msgs per Sync Cycle: 10
TSE Location:
☐ Update Message Status From

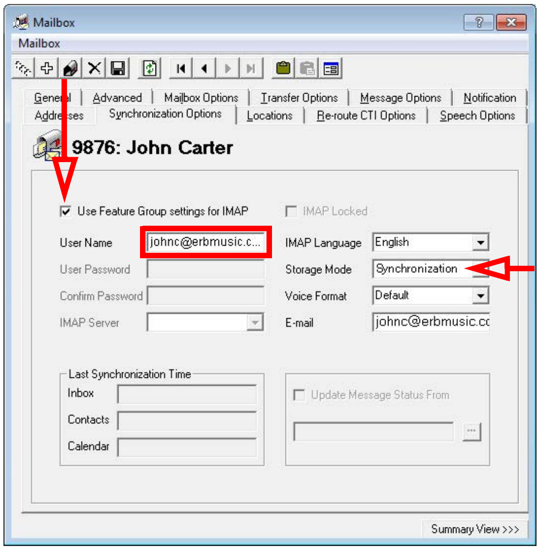
Save all changes.

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.


Mailbox
Mailbox
General | Advanced | Mailbox Options | Transfer Options | Message Options | Notification
Addresses | Synchronization Options | Locations | Re-route CTI Options | Speech Options
Summary View >>>

9876: John Carter

☑ Use Feature Group settings for IMAP

□ IMAP Locked

User Name: johnc@erbmusic.c...

User Password:

Confirm Password:

IMAP Server:

IMAP Language: English

Storage Mode: Synchronization

Voice Format: Default

E-mail: johnc@erbmusic.cc

Last Synchronization Time

Inbox:

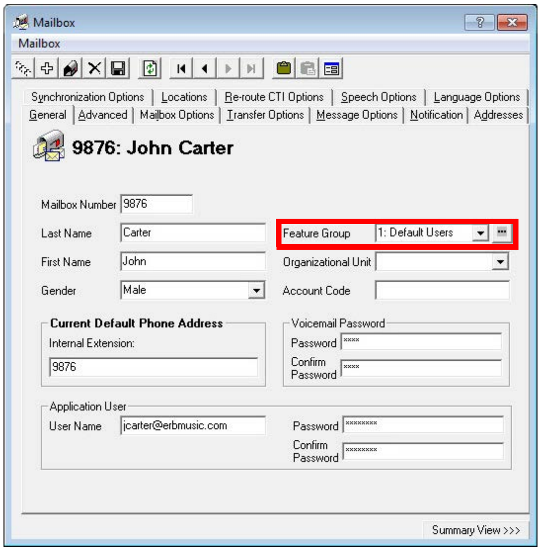
Contacts:

Calendar:

□ Update Message Status From

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.


Mailbox
Mailbox
Synchronization Options | Locations | Re-route CTI Options | Speech Options | Language Options
General | Advanced | Mailbox Options | Transfer Options | Message Options | Notification | Addresses
Summary View >>>

9876: John Carter

Mailbox Number: 9876

Last Name: Carter

First Name: John

Gender: Male

Feature Group: 1: Default Users

Organizational Unit:

Account Code:

Current Default Phone Address

Internal Extension: 9876

Voicemail Password

Password: ****

Confirm Password: ****

Application User

User Name: jcarter@erbmusic.com

Password: *********

Confirm Password: *********

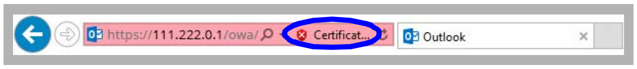
Certificate Configuration

In order 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.

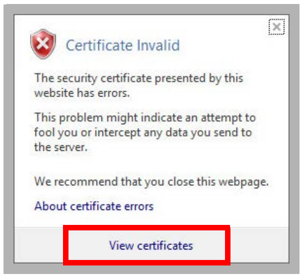
The simplest way to achieve this is to access the OWA (Outlook Web App) web page for Exchange on the voice server.

> **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**.


Certificate Invalid

The security certificate presented by this website has errors.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

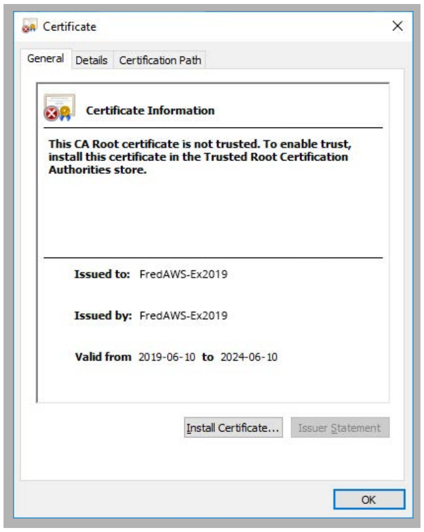
We recommend that you close this webpage.

About certificate errors

View certificates

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


Certificate

General | Details | Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: FredAWS-Ex2019

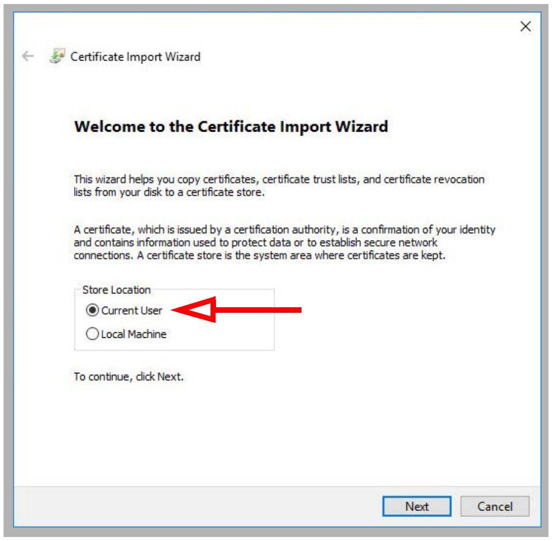
Issued by: FredAWS-Ex2019

Valid from 2019-06-10 to 2024-06-10

Install Certificate... | Issuer Statement

OK

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



Welcome to the Certificate Import Wizard

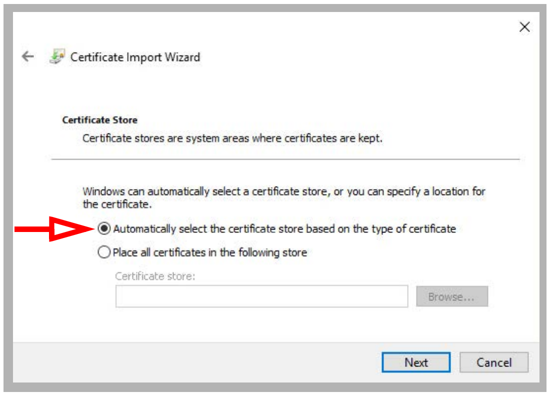
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

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



Certificate Store

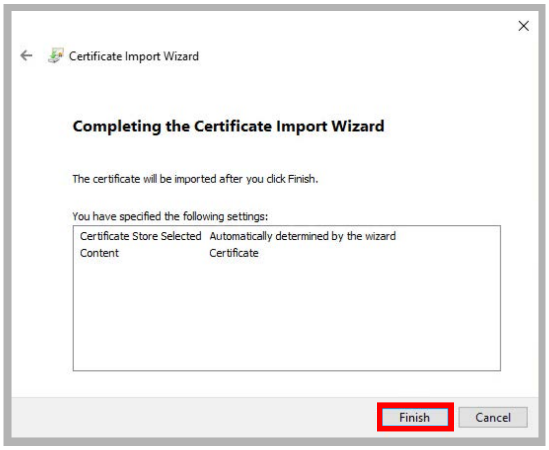
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate
○ Place all certificates in the following store

Certificate store:

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



Completing the Certificate Import Wizard

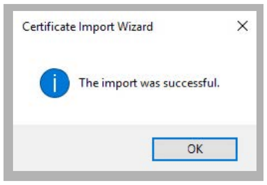
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

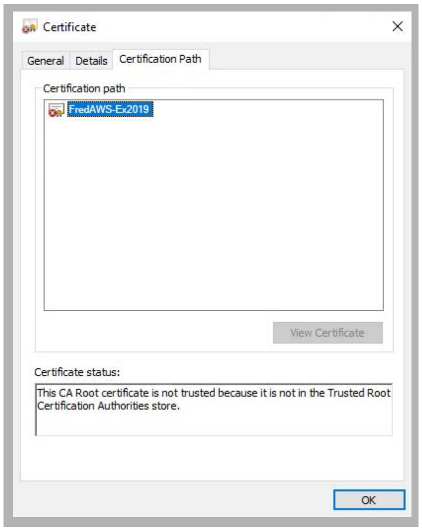
8. The following popup confirms the import was successful.

Click **OK**.



The import was successful.

9. You will be able to confirm the status of the certificate through this window.



Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

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

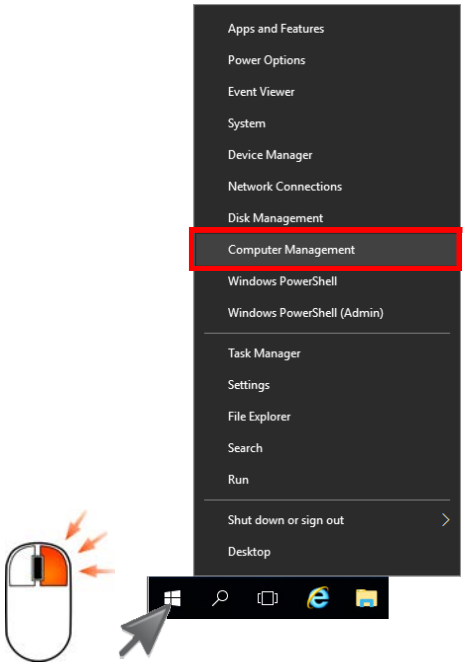
Once you have configured the IMAP CSE server with your mail server, you will be able to select the degree of synchronization from the Feature Group. Ensure that you verify all of the information so that users do not lose any calendar, contact or message data during synchronization.

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

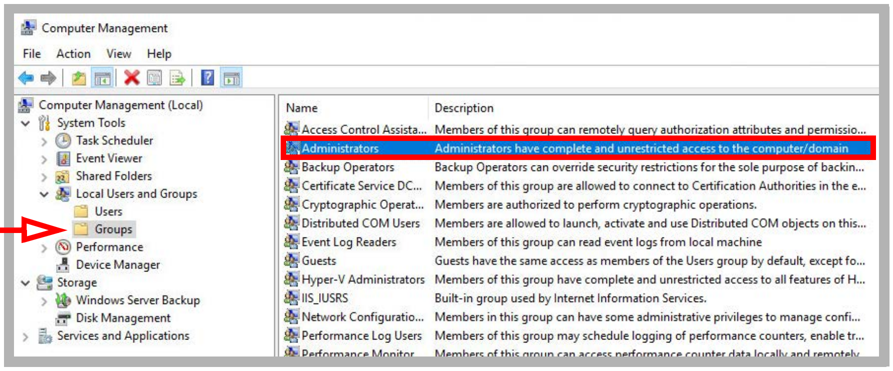
Windows Configuration

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**.

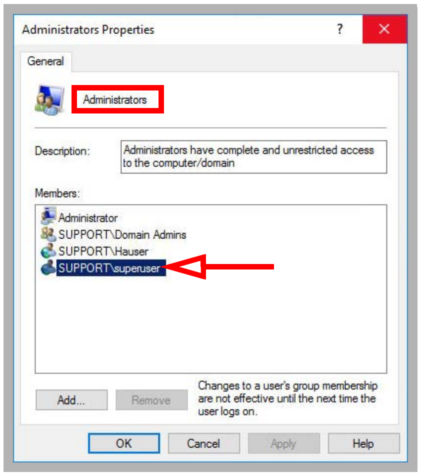


2. Go to **System Tools > Local Users and Groups > Groups**. Double-click **Administrators**.



Name	Description
Access Control Assista...	Members of this group can remotely query authorization attributes and permissio...
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backin...
Certificate Service DC...	Members of this group are allowed to connect to Certification Authorities in the e...
Cryptographic Operat...	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this...
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except fo...
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of H...
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuratio...	Members in this group can have some administrative privileges to manage confi...
Performance Log Users	Members of this group may schedule logging of performance counters, enable tr...
Performance Monitor...	Members of this group can access performance counter data locally and remotely

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



Administrators Properties

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

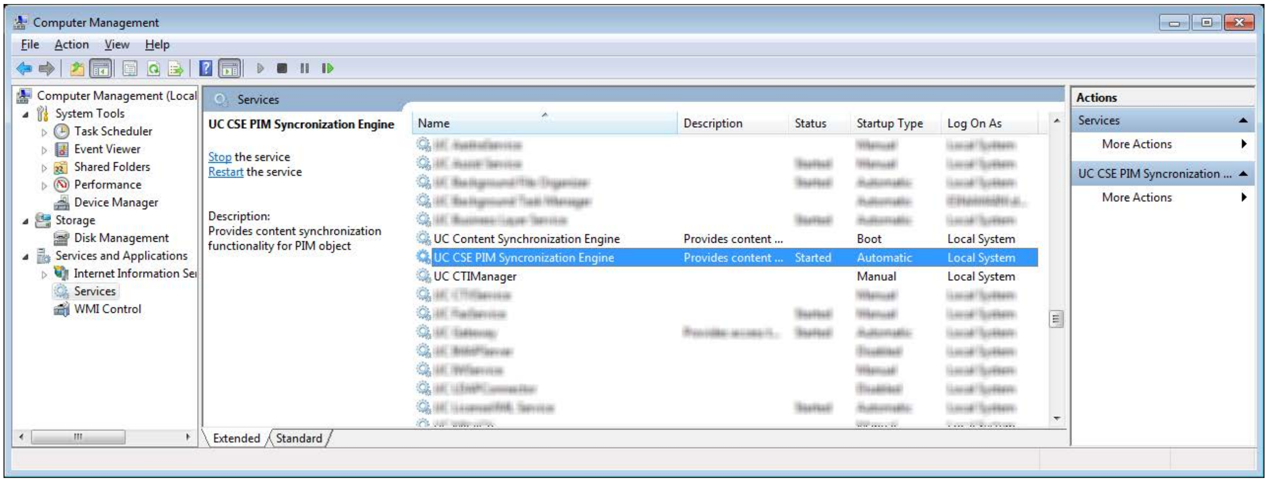
Members:

- Administrator
- SUPPORT\Domain Admins
- SUPPORT\Hauser
- SUPPORT\superuser

Changes to a user's group membership are not effective until the next time the user logs on.

4. The **UC CSE PIM Synchronization Engine** service must login and run with the Superuser credentials.

Open the **Computer Management** console and select **Services**.



Computer Management

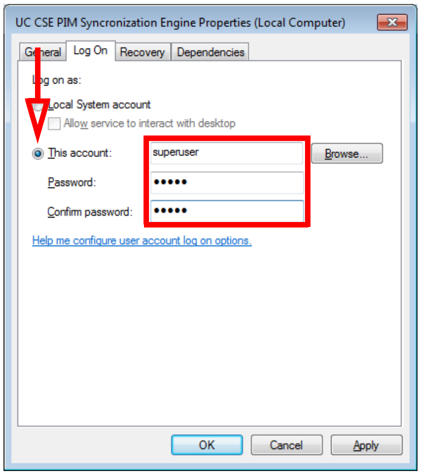
UC CSE PIM Syncronization Engine

Stop the service
Restart the service

Description:
Provides content synchronization functionality for PIM object

Name	Description	Status	Startup Type	Log On As
UC Content Synchronization Engine	Provides content ...		Boot	Local System
UC CSE PIM Syncronization Engine	Provides content ...	Started	Automatic	Local System
UC CTIManager			Manual	Local System

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.



UC CSE PIM Syncronization Engine Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: superuser

Password: •••••

Confirm password: •••••

Help me configure user account log on options.

Click **Apply** and **OK** when finished.

6. Restart the service.

Avaya Messaging Configuration - Feature Group

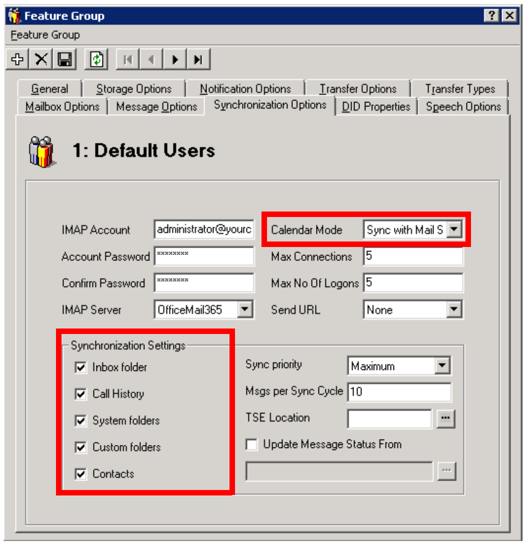
Feature Group configuration requires changes on two tabs; **Synchronization Options** and **Mailbox Options**. You can define exactly what is going to be synchronized for the users from these two sections.

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.



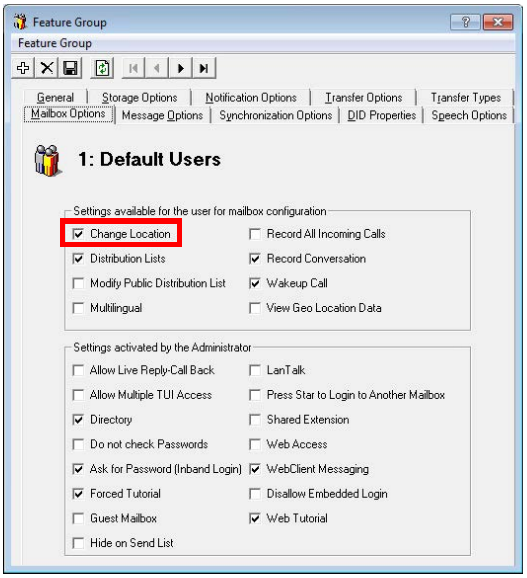
1: Default Users

IMAP Account: administrator@yourc
Account Password: ********
Confirm Password: ********
IMAP Server: OfficeMail365
Calendar Mode: Sync with Mail S
Max Connections: 5
Max No Of Logons: 5
Send URL: None

Synchronization Settings
- ☑ Inbox folder
- ☑ Call History
- ☑ System folders
- ☑ Custom folders
- ☑ Contacts

Sync priority: Maximum
Msgs per Sync Cycle: 10
TSE Location:
☐ Update Message Status From

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



1: Default Users

Settings available for the user for mailbox configuration
- ☑ Change Location
- ☑ Distribution Lists
- ☐ Modify Public Distribution List
- ☐ Multilingual
- ☐ Record All Incoming Calls
- ☑ Record Conversation
- ☑ Wakeup Call
- ☐ View Geo Location Data

Settings activated by the Administrator
- ☐ Allow Live Reply-Call Back
- ☐ Allow Multiple TUI Access
- ☑ Directory
- ☐ Do not check Passwords
- ☑ Ask for Password (Inband Login)
- ☑ Forced Tutorial
- ☐ Guest Mailbox
- ☐ Hide on Send List
- ☐ LanTalk
- ☐ Press Star to Login to Another Mailbox
- ☐ Shared Extension
- ☐ Web Access
- ☑ WebClient Messaging
- ☐ Disallow Embedded Login
- ☑ Web Tutorial

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.

User Guide

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.

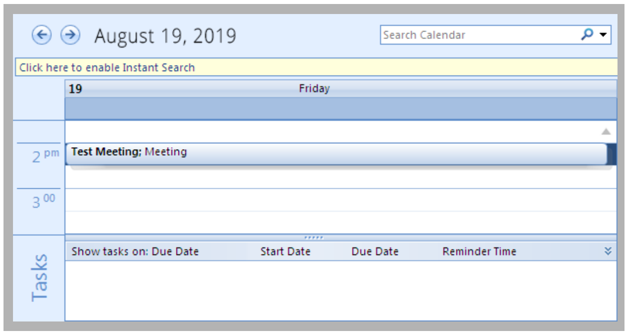
Note: All of the calendar events and contacts from your mail server will be copied into your Avaya Messaging mailbox as soon as the administrator finishes configuring the systems.

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.

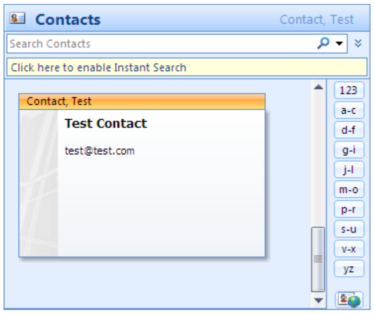
The time and date of the meeting is automatically sent to the Avaya Messaging mailbox. By default, the location for these events will be marked as **Meeting**. You may change this manually through Web Access, or in the case of Outlook, you may utilize the iLink Pro Desktop tool bar to assign a specific location to the event.



Test Meeting; Meeting

Contact Synchronization

When you create a contact entry from Outlook, the entry will be copied into your Avaya Messaging mailbox.

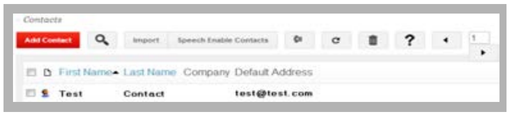


Contact, Test

Test Contact

test@test.com

Contact information is automatically sent to the Avaya Messaging mailbox.



First Name	Last Name	Company	Default Address
Test	Contact		test@test.com

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 be 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 2007	Exchange 2013	Exchange 2016
Messages	<20000	<100000	<100000
Contact and Calendar Entries	<5000	<10000	<10000

11 EXCHANGE 2013 INTEGRATION NON-EWS

In This Chapter:

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 suites your requirements.

CHAPTER	INTEGRATION	WHY YOU WANT IT
9	Google	Creates a secure connection through OAuth2 to your Gmail and Google Apps accounts.
10	Exchange using EWS	The simplest connection between your Exchange server and Avaya Messaging.
11	Exchange without EWS	A connection between Exchange and Avaya Messaging for legacy systems.
12	Exchange 2010	A connection between Exchange 2010 and Avaya Messaging.
13	Office 365 using Graph	Setup the latest high security integration procedures for maximum data integrity.
14	Office 365 using EWS	Quick connection between your O365 server and Avaya Messaging.

Introduction

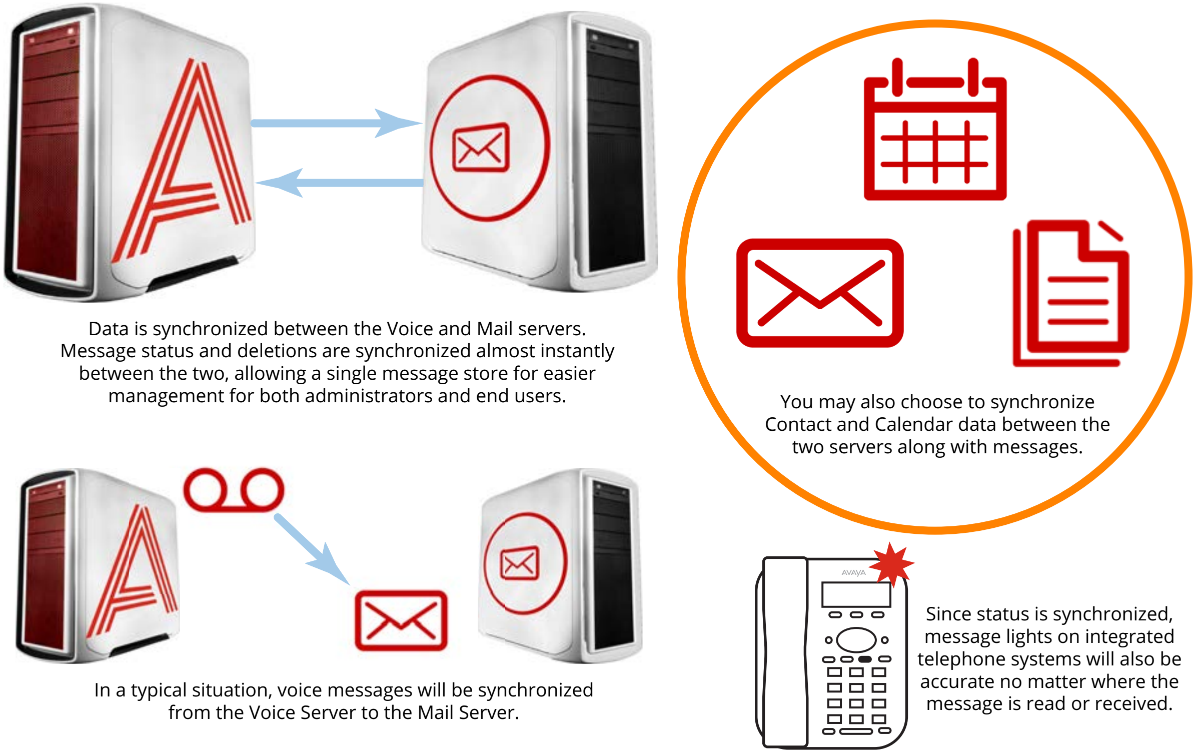
Avaya Messaging and an Exchange server are able to integrate through the IMAPCSE services, providing a truly unified messaging experience. Once the configuration is complete the servers communicate and synchronize all data among themselves, eliminating the need for you to constantly manage multiple locations.

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.

Exchange 2013 can be configured for either IMAP or EWS integration. This chapter covers the setup required to use IMAP.

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

Visual Guide



Data is synchronized between the Voice and Mail servers. Message status and deletions are synchronized almost instantly between the two, allowing a single message store for easier management for both administrators and end users.

You may also choose to synchronize Contact and Calendar data between the two servers along with messages.

In a typical situation, voice messages will be synchronized from the Voice Server to the Mail Server.

Since status is synchronized, message lights on integrated telephone systems will also be accurate no matter where the message is read or received.

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 will be 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	Officelinx/IX Messaging version 9.0 - 10.8 Avaya Messaging version 11.0 or higher

Server Configuration

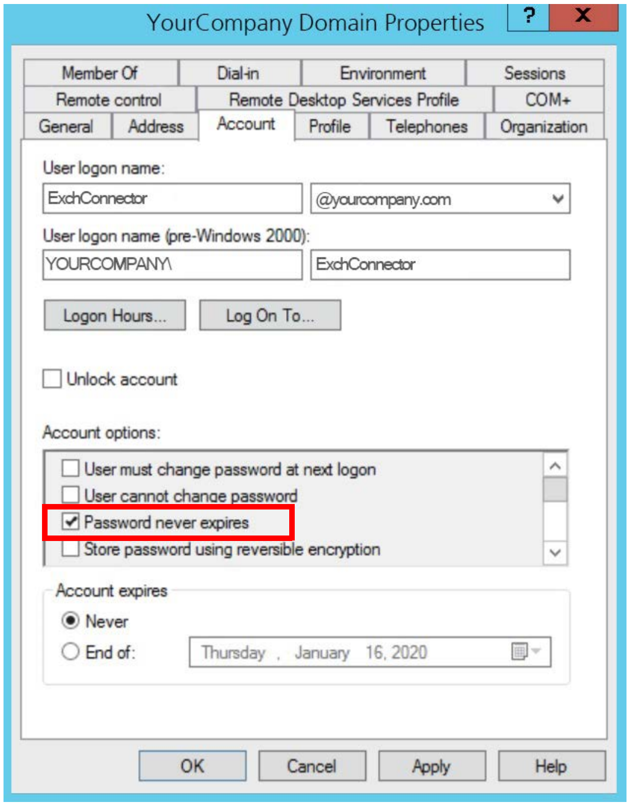
Server configuration requires the creation of a superuser account from the active directory that has the necessary permissions within the Exchange console. Once the account has been made, it must be added to the voice server configuration, and the channel of communication between the two servers must be established.

Exchange server must also have IMAP enabled in order for Avaya Messaging to communicate properly. Once the superuser account is ready, enable IMAP for your Exchange server through the command shell.

Exchange 2013 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.



User logon name:

ExchConnector @yourcompany.com

User logon name (pre-Windows 2000):

YOURCOMPANY\ ExchConnector

☐ Unlock account

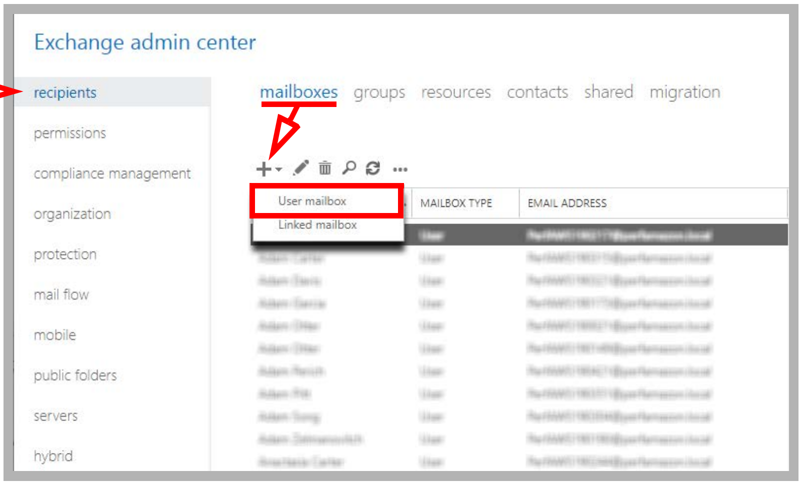
Account options:

☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Store password using reversible encryption

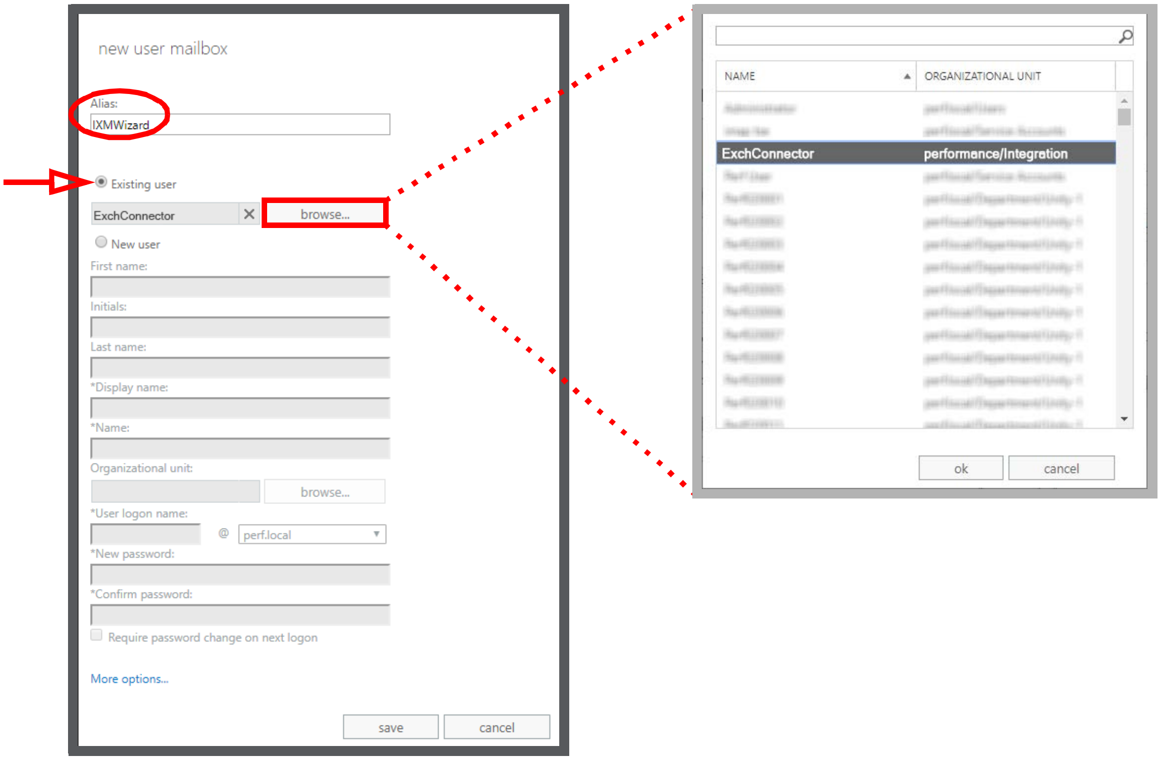
Account expires

● Never
○ End of: Thursday , January 16, 2020

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 above. Provide a human friendly **Alias** to refer to this user.


new user mailbox

Alias: IXMWizard

● Existing user

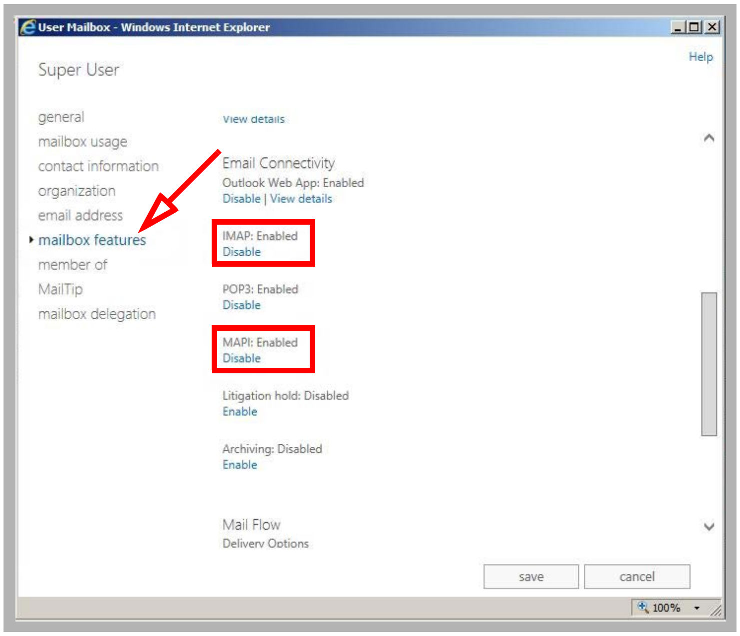
ExchConnector

○ New user

NAME	ORGANIZATIONAL UNIT
ExchConnector	performance/Integration

When ready, click **Save**.

4. On the **mailbox features** tab, ensure that **IMAP** and **MAPI** are both **Enabled**.



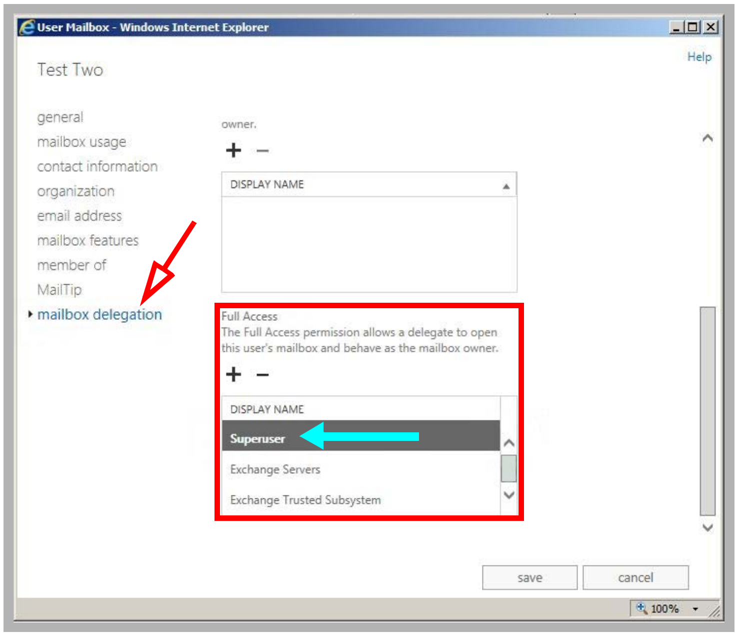
5. At the Command Prompt, run the following command lines to attach the necessary permissions to the Superuser account. Include the **alias** recorded earlier as a part of the command:

   Get-Mailbox -OrganizationalUnit UnitName -ResultSize Unlimited | Add-MailboxPermission -User ExchConnector -AccessRights FullAccess -InheritanceType All

   Get-Mailbox -OrganizationalUnit UnitName -ResultSize Unlimited | Add-ADPermission -User ExchConnector -ExtendedRights “Send As” -InheritanceType All

6. To verify the correct setup for the Superuser account, open any other account and go to the **mailbox delegation** tab.

   Ensure that the alias for the Superuser account is included beneath the listing for Full Access.



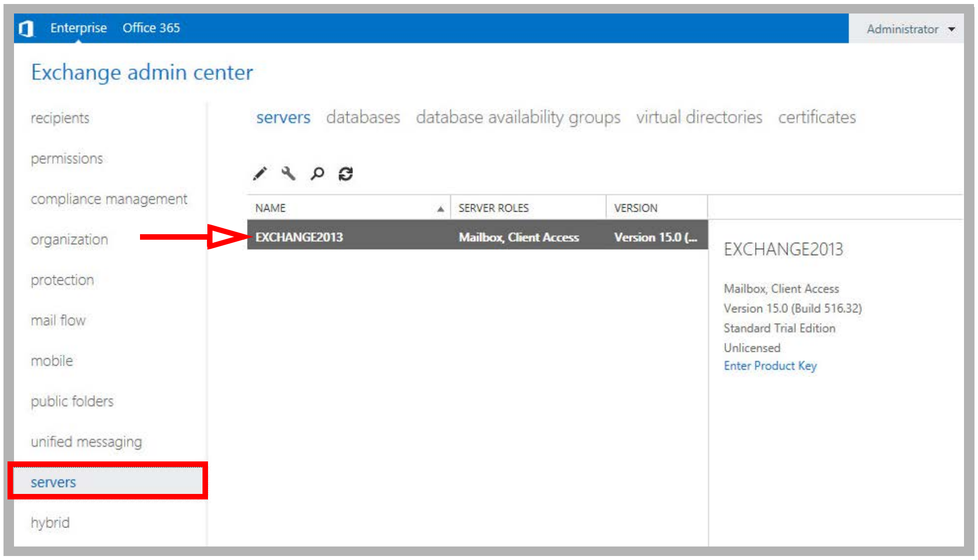
User Mailbox - Windows Internet Explorer

Test Two

Full Access
The Full Access permission allows a delegate to open this user's mailbox and behave as the mailbox owner.

DISPLAY NAME
Superuser
Exchange Servers
Exchange Trusted Subsystem

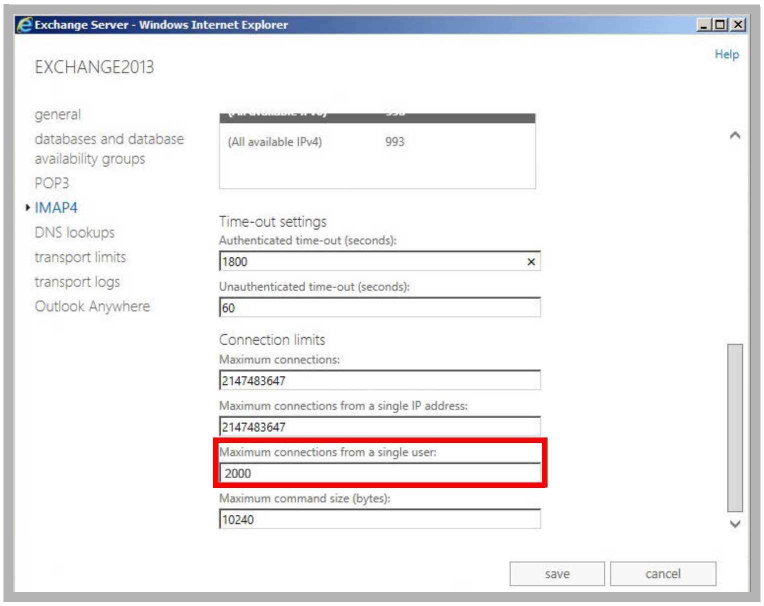
7. From the **Exchange 2013 Admin Center**, go to **Servers** and open **Exchange 2013**.



NAME	SERVER ROLES	VERSION
EXCHANGE2013	Mailbox, Client Access	Version 15.0 (...

EXCHANGE2013
Mailbox, Client Access
Version 15.0 (Build 516.32)
Standard Trial Edition
Unlicensed
Enter Product Key

8. Choose **IMAP4**. Click **More Options**, and scroll down to find **Maximum connections from a single user**. Set this value to **2000**.



(All available IPv4) 993

Time-out settings

Authenticated time-out (seconds): 1800

Unauthenticated time-out (seconds): 60

Connection limits

Maximum connections: 2147483647

Maximum connections from a single IP address: 2147483647

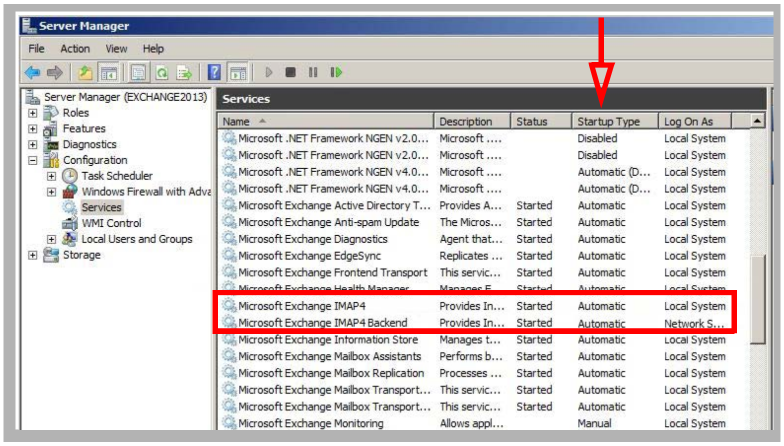
Maximum connections from a single user: 2000

Maximum command size (bytes): 10240

9. Open the **Windows Server Manager MMC** to view the system **Services**.

   Set both of the IMAP4 services to use **Automatic Startup**.

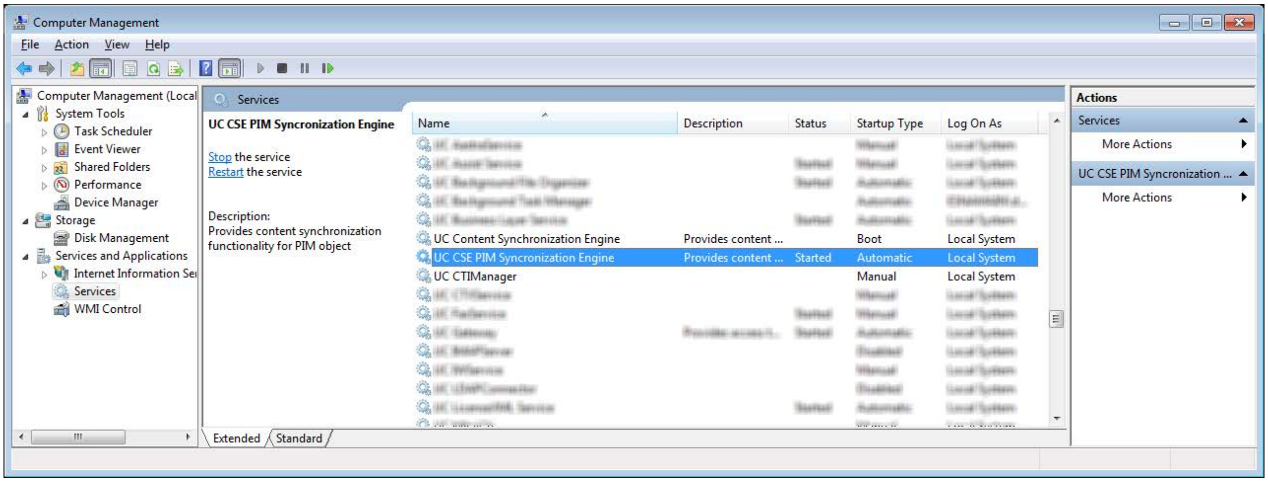
   If these services are still running, shut them down and restart them for the changes to take affect. Otherwise, Restart both services.



Name	Description	Status	Startup Type	Log On As
Microsoft .NET Framework NGEN v2.0...	Microsoft		Disabled	Local System
Microsoft .NET Framework NGEN v2.0...	Microsoft		Disabled	Local System
Microsoft .NET Framework NGEN v4.0...	Microsoft		Automatic (D...	Local System
Microsoft .NET Framework NGEN v4.0...	Microsoft		Automatic (D...	Local System
Microsoft Exchange Active Directory T...	Provides A...	Started	Automatic	Local System
Microsoft Exchange Anti-spam Update	The Micros...	Started	Automatic	Local System
Microsoft Exchange Diagnostics	Agent that...	Started	Automatic	Local System
Microsoft Exchange EdgeSync	Replicates ...	Started	Automatic	Local System
Microsoft Exchange Frontend Transport	This servic...	Started	Automatic	Local System
Microsoft Exchange Health Manager	Manages E...	Started	Automatic	Local System
Microsoft Exchange IMAP4	Provides In...	Started	Automatic	Local System
Microsoft Exchange IMAP4 Backend	Provides In...	Started	Automatic	Network S...
Microsoft Exchange Information Store	Manages t...	Started	Automatic	Local System
Microsoft Exchange Mailbox Assistants	Performs b...	Started	Automatic	Local System
Microsoft Exchange Mailbox Replication	Processes ...	Started	Automatic	Local System
Microsoft Exchange Mailbox Transport...	This servic...	Started	Automatic	Local System
Microsoft Exchange Mailbox Transport...	This servic...	Started	Automatic	Local System
Microsoft Exchange Monitoring	Allows appl...		Manual	Local System

10. The **UC CSE PIM Synchronization Engine** service must login and run with the Superuser credentials.

    Open the **Computer Management** console and select **Services**.



UC CSE PIM Syncronization Engine

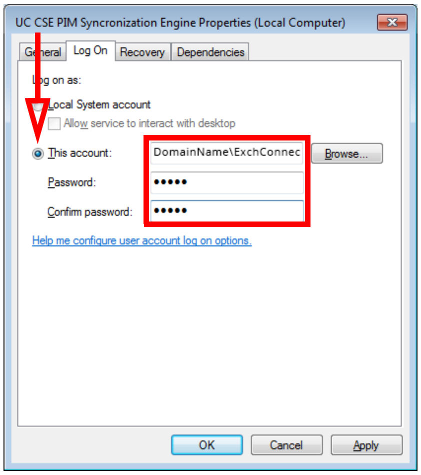
Stop the service
Restart the service

Description:
Provides content synchronization functionality for PIM object

Name	Description	Status	Startup Type	Log On As
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
UC Content Synchronization Engine	Provides content ...		Boot	Local System
UC CSE PIM Syncronization Engine	Provides content ...	Started	Automatic	Local System
UC CTIManager			Manual	Local System
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

11. Stop the **UC CSE PIM Synchronization Engine** service.

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



UC CSE PIM Syncronization Engine Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: DomainName\ExchConnec

Password: •••••

Confirm password: •••••

Click **Apply** and **OK** when finished.

13. Restart the service.

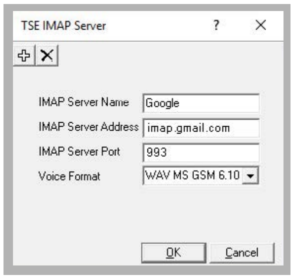
The new account has been created.

Avaya Messaging 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

In order for the Avaya Messaging server to recognize the Exchange server, you must add a new CSE Endpoint entry in the **Avaya Messaging Admin > TSE IMAP Server** section.



TSE IMAP Server

IMAP Server Name: Google

IMAP Server Address: imap.gmail.com

IMAP Server Port: 993

Voice Format: WAV MS GSM 6.10

> **Note**: **CSE** was formerly known as **TSE**.

IMAP Server Name: This name is for your reference and does impact system performance.

IMAP Server Address: Enter the server address of the Exchange server.

IMAP Server Port: The port number of the Exchange server. By default, IMAP uses port **993**.

Voice Format: From the dropdown menu, select the voice format used when sending voice messages to external voice servers.

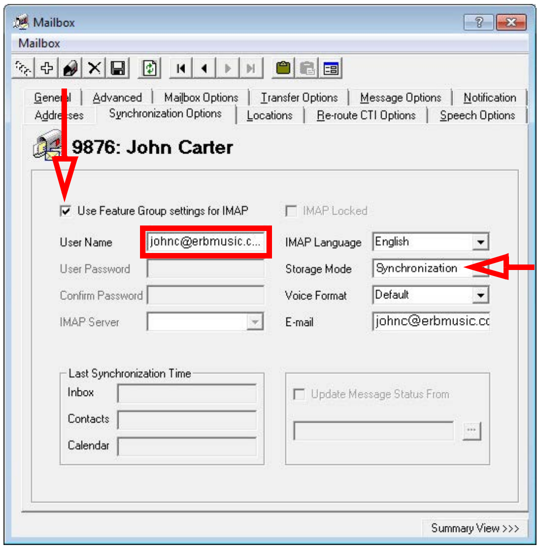
Individual Mailbox Configuration

With the superuser account, you do not have to fully enter the individual mailbox credentials for IMAPCSE synchronization.

Enable **Use Feature Group settings for IMAP** then enter the **User Name** (this will be the alias for the Exchange account that the current mailbox will be synchronized with).

Under **Storage Mode**, select **Synchronization**.

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



Mailbox

9876: John Carter

☑ Use Feature Group settings for IMAP   □ IMAP Locked

User Name: johnc@erbmusic.c...

User Password:

Confirm Password:

IMAP Server:

IMAP Language: English

Storage Mode: Synchronization

Voice Format: Default

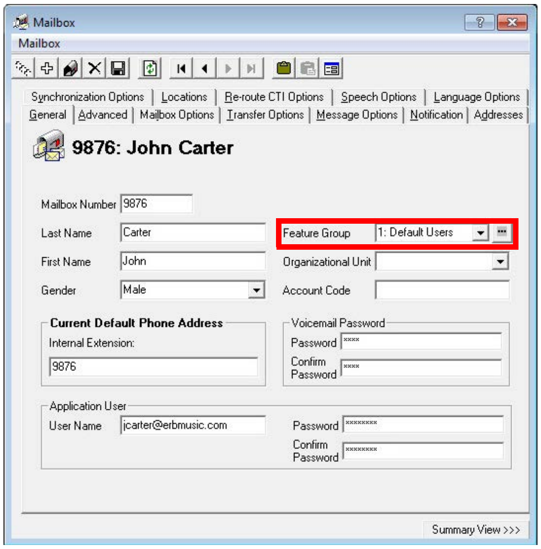
E-mail: johnc@erbmusic.cc

Last Synchronization Time: Inbox, Contacts, Calendar

□ Update Message Status From

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.



Mailbox

9876: John Carter

Mailbox Number: 9876

Last Name: Carter

First Name: John

Gender: Male

Feature Group: 1: Default Users

Organizational Unit:

Account Code:

Current Default Phone Address

Internal Extension: 9876

Voicemail Password

Password: ****

Confirm Password: ****

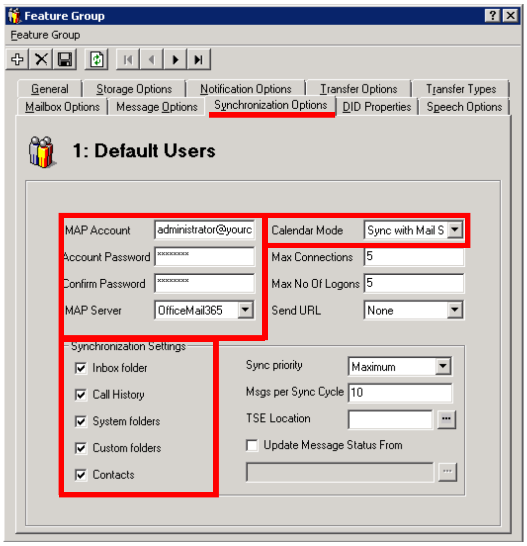
Application User

User Name: jcarter@erbmusic.com

Password: ********

Confirm Password: ********

Feature Group Configuration



Feature Group

Feature Group

1: Default Users

MAP Account	administrator@yourc	Calendar Mode	Sync with Mail S
Account Password	********	Max Connections	5
Confirm Password	********	Max No Of Logons	5
MAP Server	OfficeMail365	Send URL	None

Synchronization Settings

- ☑ Inbox folder
- ☑ Call History
- ☑ System folders
- ☑ Custom folders
- ☑ Contacts

Sync priority: Maximum

Msgs per Sync Cycle: 10

TSE Location:

☐ Update Message Status From

The Feature Group plays a key role in IMAPCSE synchronization by providing the necessary credentials. From the **Synchronization Options** tab, configure the settings 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.

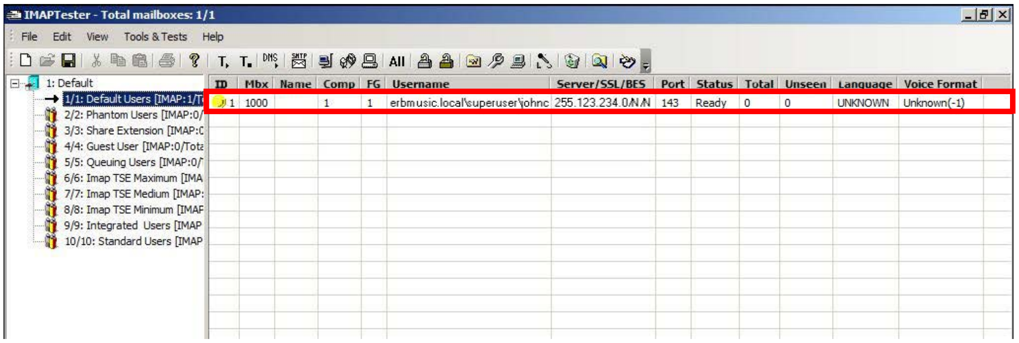
IMAP Server: Type in the name of the **IMAP TSE Server** created in the previous step (e.g. **OfficeMail365**).

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 and proceed to Registry Settings.

1. Test the connection to verify the work this far. Launch the **IMAP Tester** utility from **Start > Avaya Messaging**. Double-click on the Superuser account to open the **IMAP Settings** window.

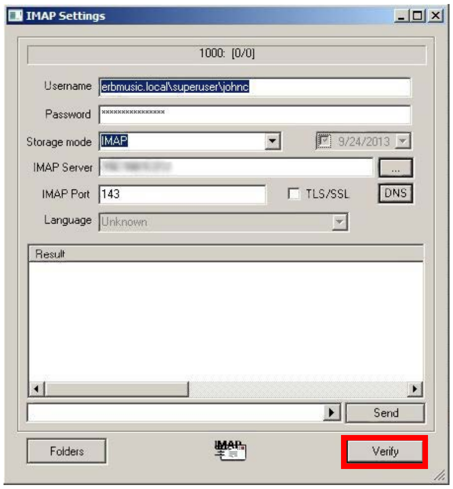


IMAPTester - Total mailboxes: 1/1

- 1: Default
  - 1/1: Default Users [IMAP:1/T
  - 2/2: Phantom Users [IMAP:0/
  - 3/3: Share Extension [IMAP:0
  - 4/4: Guest User [IMAP:0/Tota
  - 5/5: Queuing Users [IMAP:0/
  - 6/6: Imap TSE Maximum [IMA
  - 7/7: Imap TSE Medium [IMAP:
  - 8/8: Imap TSE Minimum [IMAF
  - 9/9: Integrated Users [IMAP
  - 10/10: Standard Users [IMAP

ID	Mbx	Name	Comp	FG	Username	Server/SSL/BES	Port	Status	Total	Unseen	Language	Voice Format
1	1000		1	1	erbmusic.local\superuser\johnc	255.123.234.0/N/N	143	Ready	0	0	UNKNOWN	Unknown(-1)

2. Click **Verify** to run the test.



IMAP Settings

1000: [0/0]

Username: erbmusic.local\superuser\johnc

Password: ****************

Storage mode: IMAP　　9/24/2013

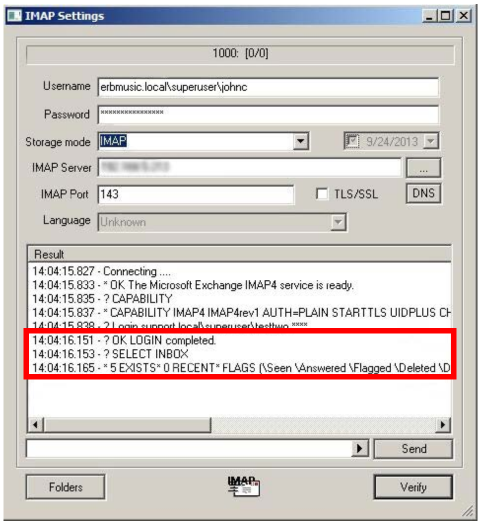
IMAP Server: [redacted]

IMAP Port: 143　　☐ TLS/SSL

Language: Unknown

Result

3. If successful, the result will include the entry for **OK LOGIN completed**.



IMAP Settings

1000: [0/0]

Username: erbmusic.local\superuser\johnc

Password: ****************

Storage mode: IMAP

☑ 9/24/2013

IMAP Server: [redacted]

IMAP Port: 143

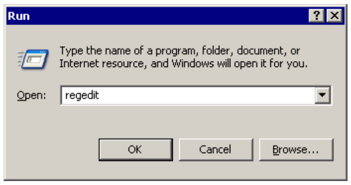
☐ TLS/SSL

Language: Unknown

```
Result
14:04:15.827 - Connecting ....
14:04:15.833 - * OK The Microsoft Exchange IMAP4 service is ready.
14:04:15.835 - ? CAPABILITY
14:04:15.837 - * CAPABILITY IMAP4 IMAP4rev1 AUTH=PLAIN STARTTLS UIDPLUS CH
14:04:15.838 - ? Login support.local\superuser\testtwo ****
14:04:16.151 - ? OK LOGIN completed.
14:04:16.153 - ? SELECT INBOX
14:04:16.165 - * 5 EXISTS* 0 RECENT* FLAGS (\Seen \Answered \Flagged \Deleted \D
```

Registry Settings

In order for Avaya Messaging to manage communications with the Exchange server, you must manually add a registry value on the Avaya Messaging server. Run the registry editor by typing **regedit** from the Run command.

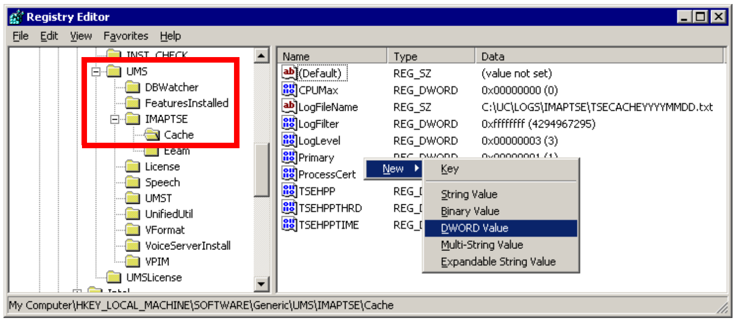


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache**. Create a new **DWORD Value** entry in this location.

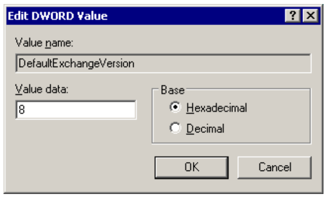


Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)
CPUMax	REG_DWORD	0x00000000 (0)
LogFileName	REG_SZ	C:\UC\LOGS\IMAPTSE\TSECACHEYYYYMMDD.txt
LogFilter	REG_DWORD	0xffffffff (4294967295)
LogLevel	REG_DWORD	0x00000003 (3)
Primary	REG_DWORD	0x00000001 (1)
ProcessCert		
TSEHPP	REG_[	
TSEHPPTHRD	REG_[	
TSEHPPTIME	REG_[	

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache

Name the entry **DefaultExchangeVersion** and assign it a value of **8**.



Edit DWORD Value

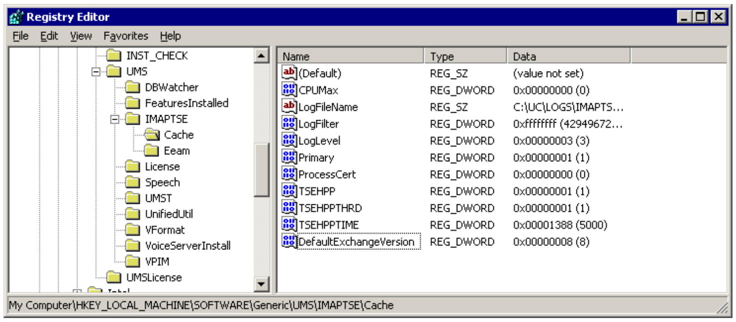
Value name: DefaultExchangeVersion

Value data: 8

Base: ● Hexadecimal ○ Decimal

The new registry entry will appear in the Registry.

Proceed with Certificate Configuration.



Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)
CPUMax	REG_DWORD	0x00000000 (0)
LogFileName	REG_SZ	C:\UC\LOGS\IMAPTS...
LogFilter	REG_DWORD	0xffffffff (42949672...
LogLevel	REG_DWORD	0x00000003 (3)
Primary	REG_DWORD	0x00000001 (1)
ProcessCert	REG_DWORD	0x00000000 (0)
TSEHPP	REG_DWORD	0x00000001 (1)
TSEHPPTHRD	REG_DWORD	0x00000001 (1)
TSEHPPTIME	REG_DWORD	0x00001388 (5000)
DefaultExchangeVersion	REG_DWORD	0x00000008 (8)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache

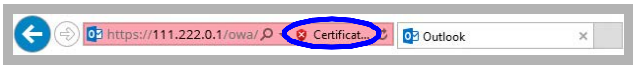
Certificate Configuration

In order 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.

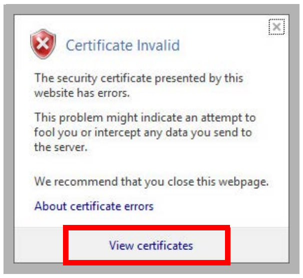
The simplest way to achieve this is to access the OWA (Outlook Web App) web page for Exchange on the voice server.

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**.



Certificate Invalid

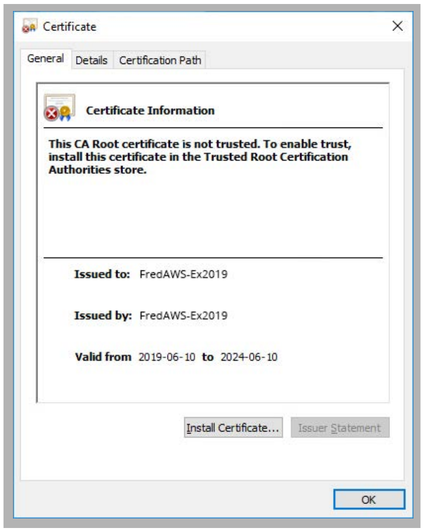
The security certificate presented by this website has errors.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

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



Certificate Information

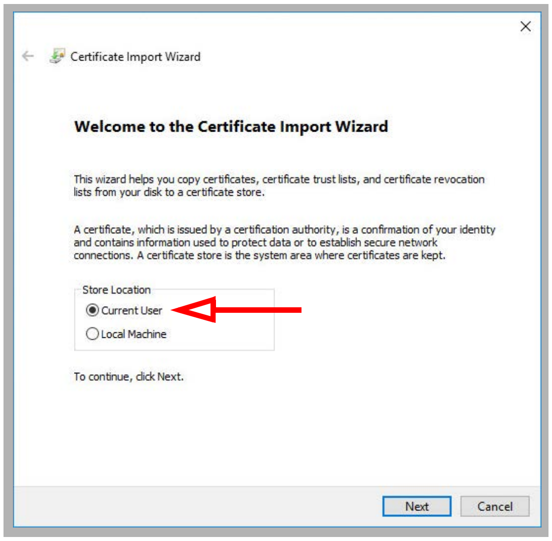
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: FredAWS-Ex2019

Issued by: FredAWS-Ex2019

Valid from 2019-06-10 to 2024-06-10

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


Certificate Import Wizard

Welcome to the Certificate Import Wizard

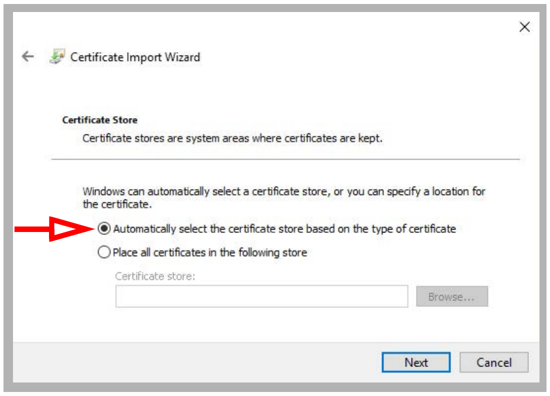
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

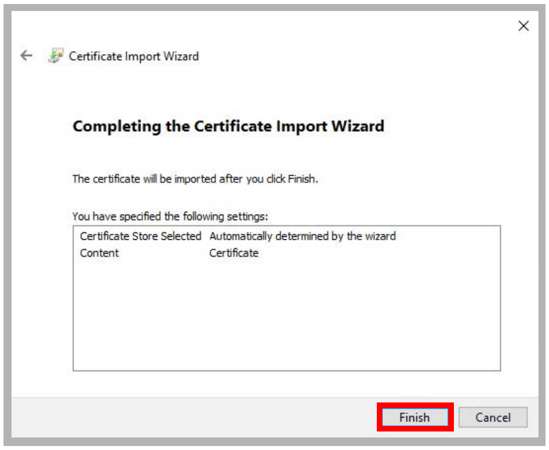
6. Enable **Automatically select the certificate store based on the type of certificate** then click **Next**.


Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.
● Automatically select the certificate store based on the type of certificate
○ Place all certificates in the following store
Certificate store:

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


Certificate Import Wizard

Completing the Certificate Import Wizard

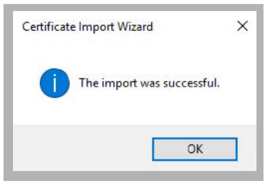
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

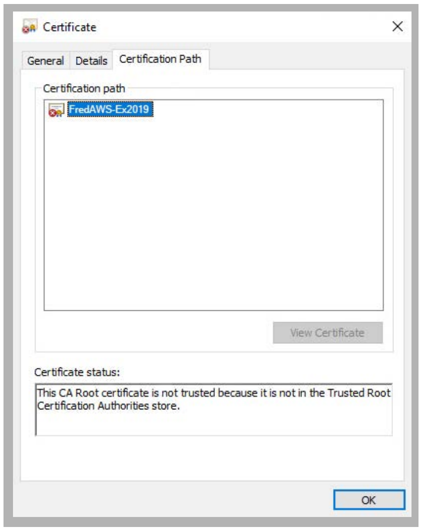
8. The following popup confirms the import was successful.

Click **OK**.


Certificate Import Wizard

The import was successful.

9. You will be able to confirm the status of the certificate through this window.



Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

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 of the information so that users do not lose any calendar, contact or message data during synchronization.

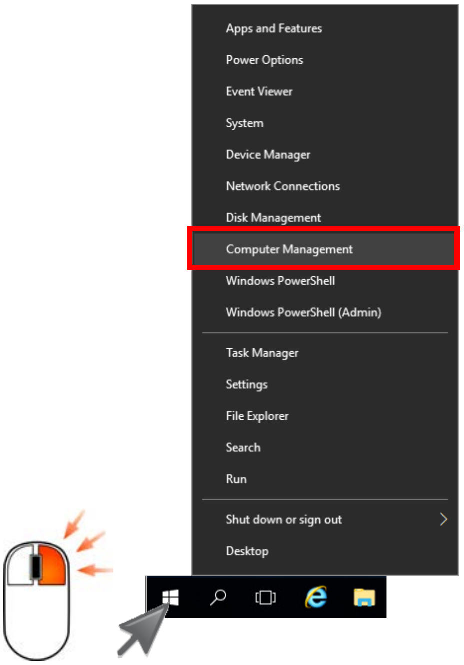
Warning: As a precaution, **backup the calendar and/or contact events** of your users before proceeding with the contact and calendar synchronization.

Note: If you did not install the Exchange MAPI component during the initial Avaya Messaging installation, you must do so manually now by running the **ExchangeMapiCdo.msi** file from **MSExchange** folder on Avaya Messaging installation DVD. This is a required component for contact and calendar synchronization.

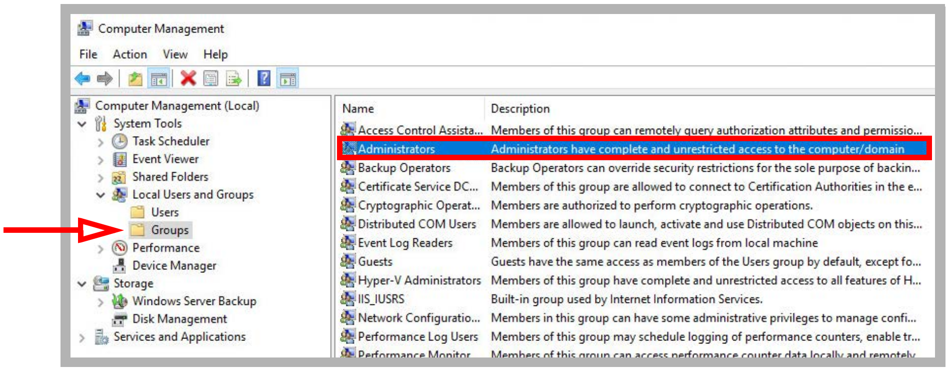
Windows Configuration

The Superuser account must be configured as a local administrator on the voice server computer. It must also be set to run the **UC TSE Cache Manager** service.

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

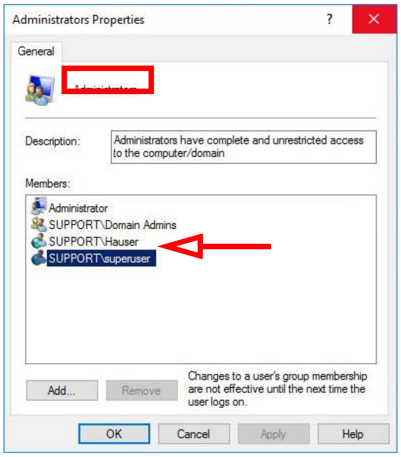


2. Go to **System Tools > Local Users and Groups > Groups**. Double-click **Administrators**.



Name	Description
Access Control Assista...	Members of this group can remotely query authorization attributes and permissio...
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backin...
Certificate Service DC...	Members of this group are allowed to connect to Certification Authorities in the e...
Cryptographic Operat...	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this...
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except fo...
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of H...
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuratio...	Members in this group can have some administrative privileges to manage confi...
Performance Log Users	Members of this group may schedule logging of performance counters, enable tr...
Performance Monitor ...	Members of this group can access performance counter data locally and remotely

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



Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

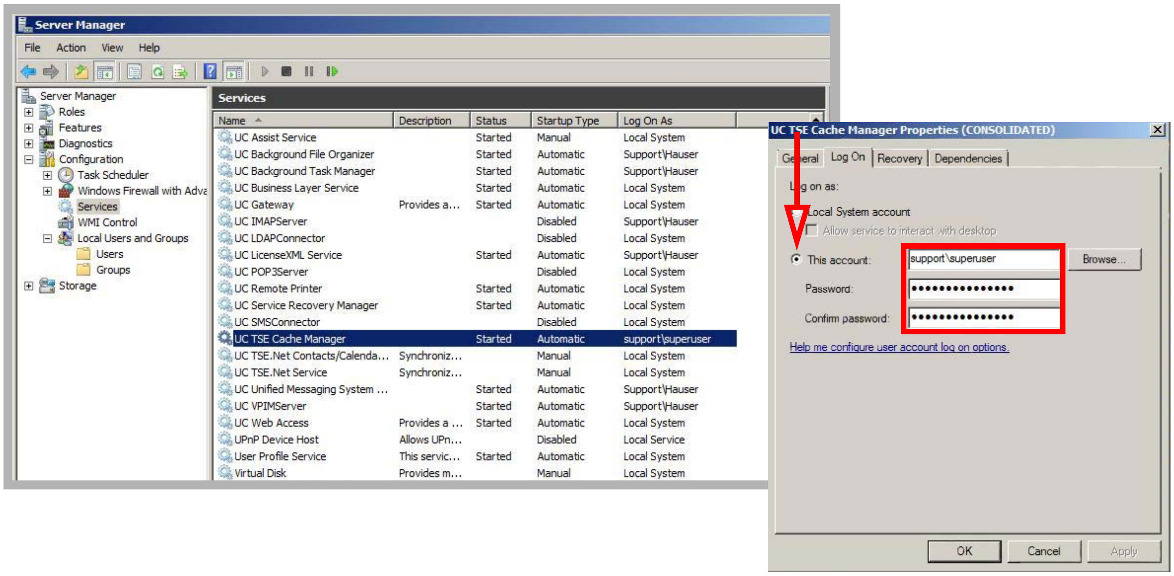
- Administrator
- SUPPORT\Domain Admins
- SUPPORT\Hauser
- SUPPORT\superuser

Changes to a user's group membership are not effective until the next time the user logs on.

4. From Windows **Server Manager > Services**, double-click on the **UC TSE Cache Manager** service in the right-hand pane.

   On the **Log On** tab, enable the **This account** button and enter the credentials for the superuser account in the spaces provided.

   The typical format will be **domain\super_user_name**.



Server Manager

Services

Name	Description	Status	Startup Type	Log On As
UC Assist Service		Started	Manual	Local System
UC Background File Organizer		Started	Automatic	Support\Hauser
UC Background Task Manager		Started	Automatic	Support\Hauser
UC Business Layer Service		Started	Automatic	Local System
UC Gateway	Provides a…	Started	Automatic	Local System
UC IMAPServer			Disabled	Support\Hauser
UC LDAPConnector			Disabled	Local System
UC LicenseXML Service		Started	Automatic	Support\Hauser
UC POP3Server			Disabled	Local System
UC Remote Printer		Started	Automatic	Local System
UC Service Recovery Manager		Started	Automatic	Local System
UC SMSConnector			Disabled	Local System
UC TSE Cache Manager		Started	Automatic	support\superuser
UC TSE.Net Contacts/Calenda…	Synchroniz…		Manual	Local System
UC TSE.Net Service	Synchroniz…		Manual	Local System
UC Unified Messaging System …		Started	Automatic	Support\Hauser
UC VPIMServer		Started	Automatic	Support\Hauser
UC Web Access	Provides a …	Started	Automatic	Local System
UPnP Device Host	Allows UPn…		Disabled	Local Service
User Profile Service	This servic…	Started	Automatic	Local System
Virtual Disk	Provides m…		Manual	Local System

UC TSE Cache Manager Properties (CONSOLIDATED)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: support\superuser

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

Avaya Messaging Configuration - Feature Group

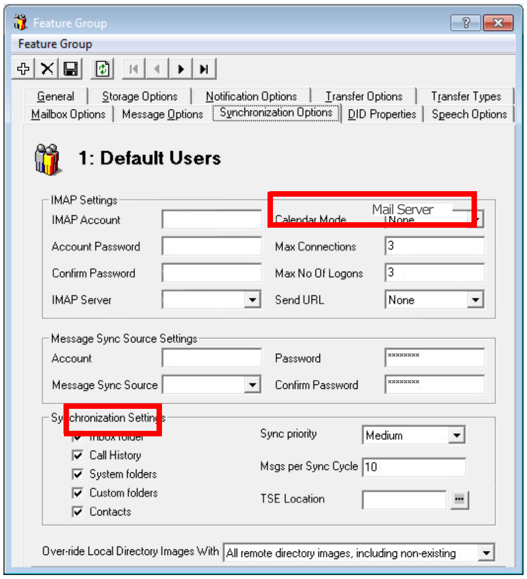
Feature Group configuration requires changes on two tabs; **Synchronization Options** and **Mailbox Option**. You can define exactly what is going to be synchronized for the users from these two sections.

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 **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.



1: Default Users

IMAP Settings

IMAP Account		Calendar Mode	Mail Server None
Account Password		Max Connections	3
Confirm Password		Max No Of Logons	3
IMAP Server		Send URL	None

Message Sync Source Settings

Account		Password	********
Message Sync Source		Confirm Password	********

Synchronization Settings

- ☑ Inbox folder
- ☑ Call History
- ☑ System folders
- ☑ Custom folders
- ☑ Contacts

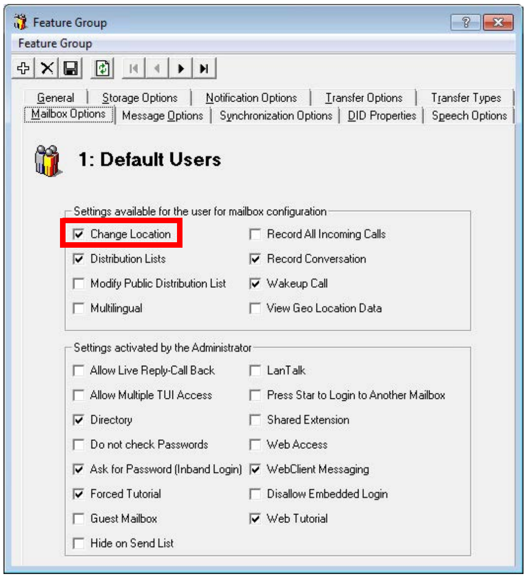
Sync priority: Medium

Msgs per Sync Cycle: 10

TSE Location:

Over-ride Local Directory Images With: All remote directory images, including non-existing

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



1: Default Users

Settings available for the user for mailbox configuration

- ☑ Change Location
- ☑ Distribution Lists
- ☐ Modify Public Distribution List
- ☐ Multilingual
- ☐ Record All Incoming Calls
- ☑ Record Conversation
- ☑ Wakeup Call
- ☐ View Geo Location Data

Settings activated by the Administrator

- ☐ Allow Live Reply-Call Back
- ☐ Allow Multiple TUI Access
- ☑ Directory
- ☐ Do not check Passwords
- ☑ Ask for Password (Inband Login)
- ☑ Forced Tutorial
- ☐ Guest Mailbox
- ☐ Hide on Send List
- ☐ LanTalk
- ☐ Press Star to Login to Another Mailbox
- ☐ Shared Extension
- ☐ Web Access
- ☑ WebClient Messaging
- ☐ Disallow Embedded Login
- ☑ Web Tutorial

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.

User Guide

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.

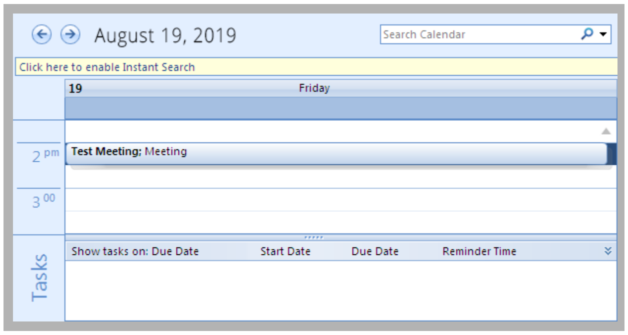
Note: All of the calendar events and contacts from your mail server will be copied into your Avaya Messaging mailbox as soon as the administrator finishes configuring the systems.

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.

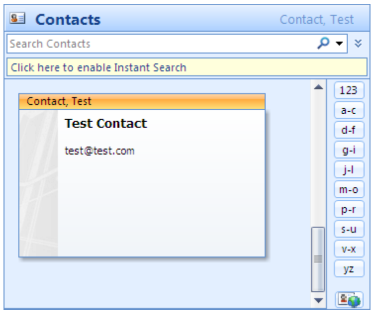
The time and date of the meeting is automatically sent to the Avaya Messaging mailbox. By default, the location for these events will be marked as **Meeting**. You may change this manually through Web Access, or in the case of Outlook, you may utilize the iLink Pro Desktop tool bar to assign a specific location to the event.



Test Meeting; Meeting

Contact Synchronization

When you create a contact entry from Outlook, the entry will be copied into your Avaya Messaging mailbox.

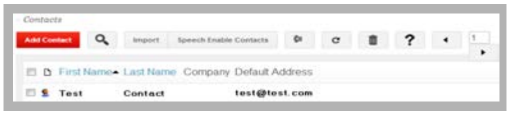


Contact, Test

Test Contact

test@test.com

Contact information is automatically sent to the Avaya Messaging mailbox.



First Name	Last Name	Company	Default Address
Test	Contact		test@test.com

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

MS Exchange Performance Considerations

Microsoft (**http://support.microsoft.com/kb/905803**) advises that a 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.

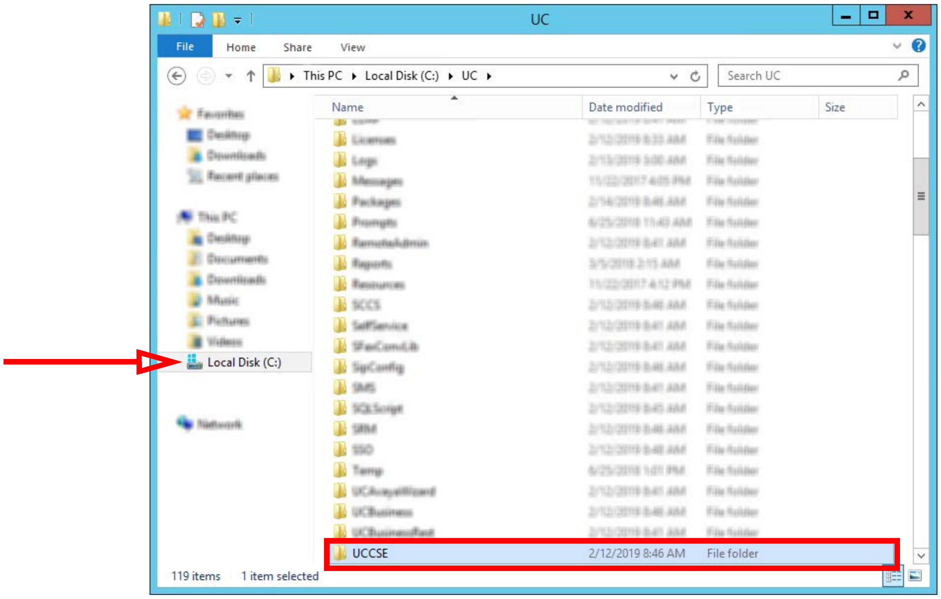
Items in Folder	Exchange 2003	Exchange 2007	Exchange 2003
Messages	<5000 combined	<20000	<100000
Contact and Calendar Entries		<5000	<10000

Reconfiguring Synchronization Components for IMAP

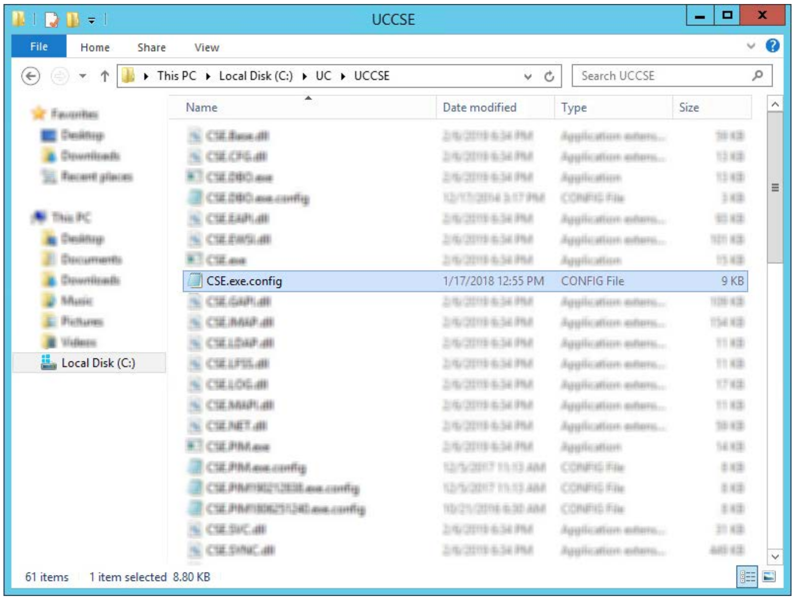
Once the installation has been completed, verify that the system configuration files are set to use IMAP. This should be done on all servers running CSE: The voice server in a single server environment, the Consolidated server under HA, and all remote CSE servers operating.

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.

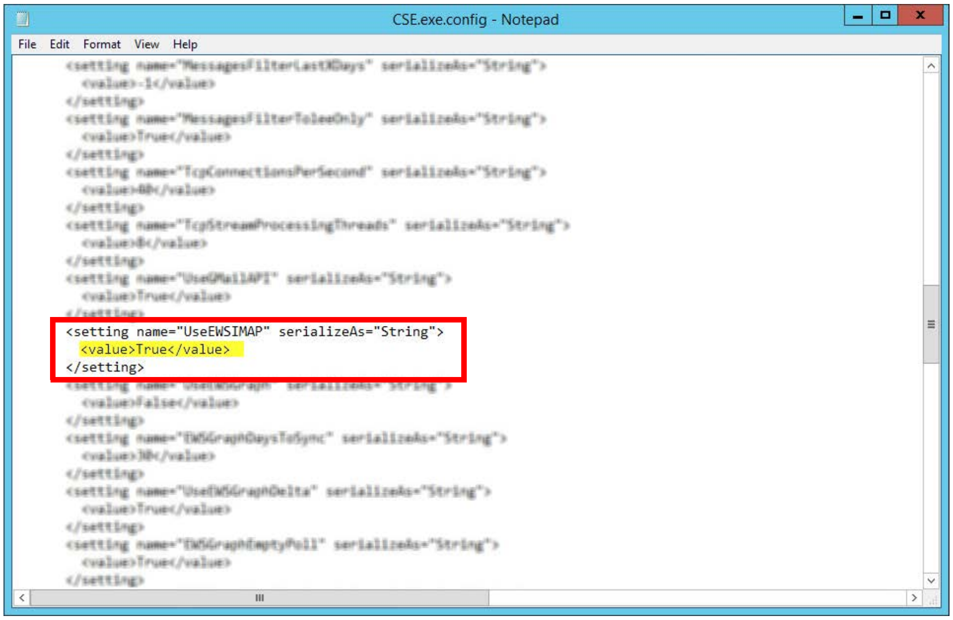


2. Within the folder, open the **CSE.exe.config** file in a text editor such as NotePad.



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

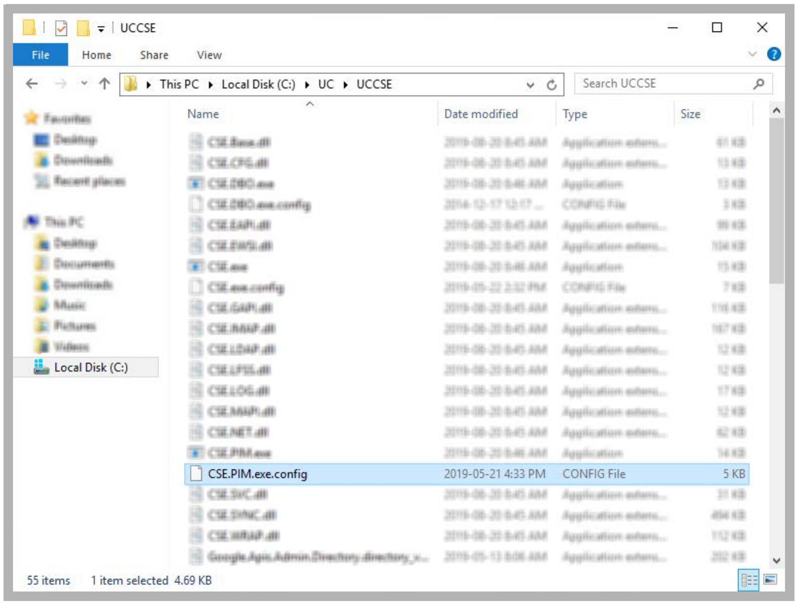
```
<setting name="UseEWSIMAP" serializeAs="String">
    <value>True</value>
</setting>
```



```
<setting name="MessagesFilterLastXDays" serializeAs="String">
  <value>-1</value>
</setting>
<setting name="MessagesFilterToleeOnly" serializeAs="String">
  <value>True</value>
</setting>
<setting name="TcpConnectionsPerSecond" serializeAs="String">
  <value>80</value>
</setting>
<setting name="TcpStreamProcessingThreads" serializeAs="String">
  <value>8</value>
</setting>
<setting name="UseGMailAPI" serializeAs="String">
  <value>True</value>
</setting>
<setting name="UseEWSIMAP" serializeAs="String">
  <value>True</value>
</setting>
<setting name="UseEWSGraph" serializeAs="String">
  <value>False</value>
</setting>
<setting name="EWSGraphDaysToSync" serializeAs="String">
  <value>30</value>
</setting>
<setting name="UseEWSGraphDelta" serializeAs="String">
  <value>True</value>
</setting>
<setting name="EWSGraphEmptyPoll" 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.

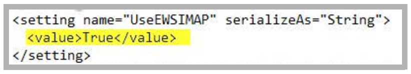


Name	Date modified	Type	Size
CSE.Base.dll	2019-08-20 8:45 AM	Application extens...	61 KB
CSE.CFG.dll	2019-08-20 8:45 AM	Application extens...	13 KB
CSE.DBO.exe	2019-08-20 8:46 AM	Application	13 KB
CSE.DBO.exe.config	2014-12-17 12:17 ...	CONFIG File	3 KB
CSE.EAPI.dll	2019-08-20 8:45 AM	Application extens...	99 KB
CSE.EWSI.dll	2019-08-20 8:45 AM	Application extens...	104 KB
CSE.exe	2019-08-20 8:46 AM	Application	15 KB
CSE.exe.config	2019-05-22 2:32 PM	CONFIG File	7 KB
CSE.GAPI.dll	2019-08-20 8:45 AM	Application extens...	116 KB
CSE.IMAP.dll	2019-08-20 8:45 AM	Application extens...	167 KB
CSE.LDAP.dll	2019-08-20 8:45 AM	Application extens...	12 KB
CSE.LFSS.dll	2019-08-20 8:45 AM	Application extens...	12 KB
CSE.LOG.dll	2019-08-20 8:45 AM	Application extens...	17 KB
CSE.MAPI.dll	2019-08-20 8:45 AM	Application extens...	12 KB
CSE.NET.dll	2019-08-20 8:45 AM	Application extens...	62 KB
CSE.PIM.exe	2019-08-20 8:46 AM	Application	14 KB
CSE.PIM.exe.config	2019-05-21 4:33 PM	CONFIG File	5 KB
CSE.SVC.dll	2019-08-20 8:45 AM	Application extens...	31 KB
CSE.SYNC.dll	2019-08-20 8:45 AM	Application extens...	494 KB
CSE.WRAP.dll	2019-08-20 8:45 AM	Application extens...	112 KB
Google.Apis.Admin.Directory.directory_v...	2019-05-13 8:08 AM	Application extens...	202 KB

55 items 1 item selected 4.69 KB

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

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



```
<setting name="UseEWSIMAP" 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.

12 EXCHANGE 2010 INTEGRATION

In This Chapter:

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 suites your requirements.

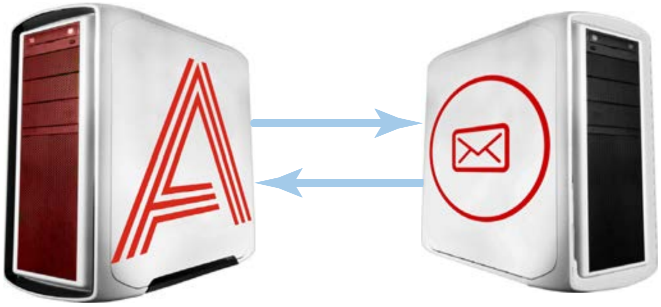
CHAPTER	INTEGRATION	WHY YOU WANT IT
9	Google	Creates a secure connection through OAuth2 to your Gmail and Google Apps accounts.
10	Exchange using EWS	The simplest connection between your Exchange server and Avaya Messaging.
11	Exchange without EWS	A connection between Exchange and Avaya Messaging for legacy systems.
12	Exchange 2010	A connection between Exchange 2010 and Avaya Messaging.
13	Office 365 using Graph	Setup the latest high security integration procedures for maximum data integrity.
14	Office 365 using EWS	Quick connection between your O365 server and Avaya Messaging.

Introduction

Avaya Messaging and an Exchange server are able to integrate through the IMAPCSE services, 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.

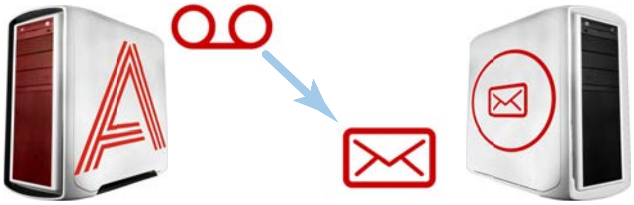
Each user's Exchange credentials are stored within the Avaya Messaging mailbox, allowing the server to synchronize messages to and from the Exchange server. End users can manage their credentials through Web Access. Administrators may also manage credentials from the admin console.

Visual Guide

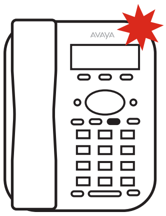


Data is synchronized between the Voice and Mail servers. Message status and deletions are synchronized almost instantly between the two, allowing a single message store for easier management for both administrators and end users.

You may also choose to synchronize Contact and Calendar data between the two servers along with messages.



In a typical situation, voice messages will be synchronized from the Voice Server to the Mail Server.



Since status is synchronized, message lights on integrated telephone systems will also be accurate no matter where the message is read or received.

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 will be 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	Officelinx/IX Messaging version 8.5 - 10.8 Avaya Messaging version 11.0 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.

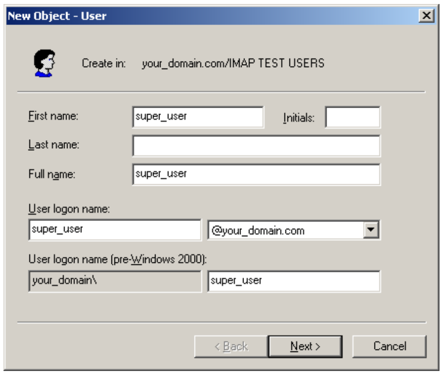
Exchange server must also have IMAP enabled in order for Avaya Messaging to communicate properly. Once the superuser account is ready, enable IMAP for your Exchange server through the command shell.

Creating a superuser from Active Directory

A new user account must be created before it can be setup as a superuser with the necessary access privileges.

1. From the active directory, create a new user.
   The user name can be anything.
   For this guide, we will be using “super_user” as the user name and “perf.local” as the domain within which Exchange 2010 is installed.

Note: Change the domain and user name to match your network’s requirements.


New Object - User

Create in: your_domain.com/IMAP TEST USERS

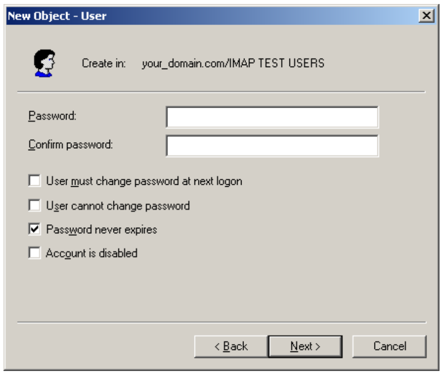
First name: super_user
Initials:
Last name:
Full name: super_user

User logon name: super_user @your_domain.com

User logon name (pre-Windows 2000): your_domain\ super_user

2. Ensure that **Password never expires** is enabled.

   Since this password is applied to the **Feature Group**, an expired password means that all mailbox accounts associated with that Feature Group will not be synchronized until the password is reset.

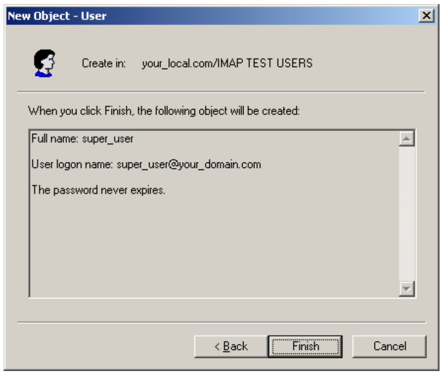

New Object - User

Create in: your_domain.com/IMAP TEST USERS

Password:
Confirm password:

☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Account is disabled

3. Confirm the information then click **Finish** to add the user.


New Object - User

Create in: your_local.com/IMAP TEST USERS

When you click Finish, the following object will be created:

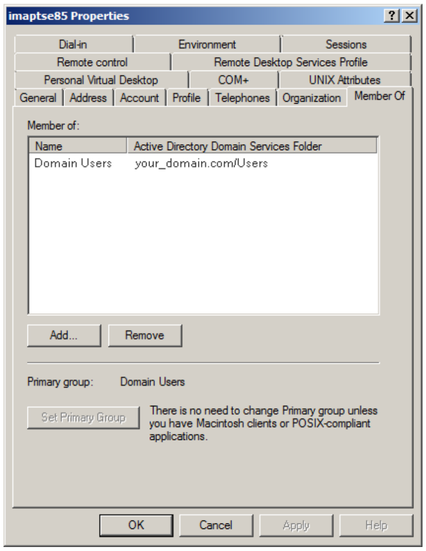
Full name: super_user

User logon name: super_user@your_domain.com

The password never expires.

4. After the user is created, ensure that it is a member of a group with the necessary access.

   The correct group to join may vary from system to system, but the key is to ensure that this user has full administrative access to the Exchange server.



Member of:

Name	Active Directory Domain Services Folder
Domain Users	your_domain.com/Users

Primary group: Domain Users

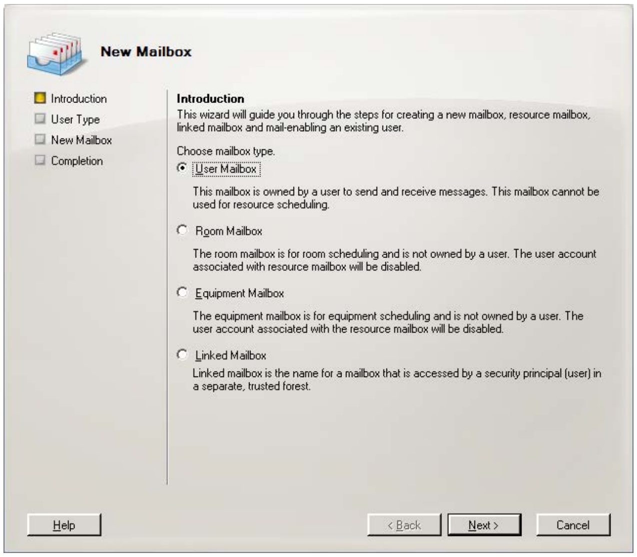
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Proceed to the Exchange 2010 configuration after the superuser account is ready.

Exchange 2010 superuser Creation/Configuration

Once the superuser account is ready on Active Directory, create a mailbox for that user in the Exchange 2010 environment.

1. Create a new **User Mailbox** mailbox from the Exchange 2010 Management Console.



New Mailbox

Introduction

This wizard will guide you through the steps for creating a new mailbox, resource mailbox, linked mailbox and mail-enabling an existing user.

Choose mailbox type.

● User Mailbox

This mailbox is owned by a user to send and receive messages. This mailbox cannot be used for resource scheduling.

○ Room Mailbox

The room mailbox is for room scheduling and is not owned by a user. The user account associated with resource mailbox will be disabled.

○ Equipment Mailbox

The equipment mailbox is for equipment scheduling and is not owned by a user. The user account associated with the resource mailbox will be disabled.

○ Linked Mailbox

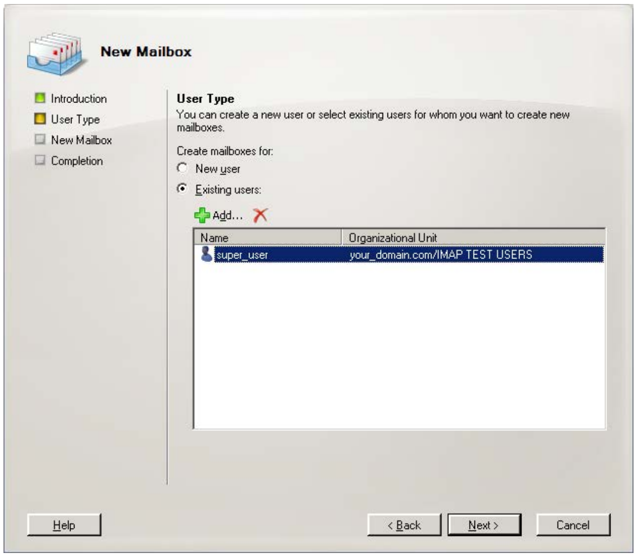
Linked mailbox is the name for a mailbox that is accessed by a security principal (user) in a separate, trusted forest.

2. When prompted, choose **Existing User**.
3. Click on the **Add** button.

   In the popup window, select the superuser account that was previously in the Active Directory.

   Click **OK** to add that account to the list of new mailboxes.

4. Click **Next** to continue.



New Mailbox

User Type

You can create a new user or select existing users for whom you want to create new mailboxes.

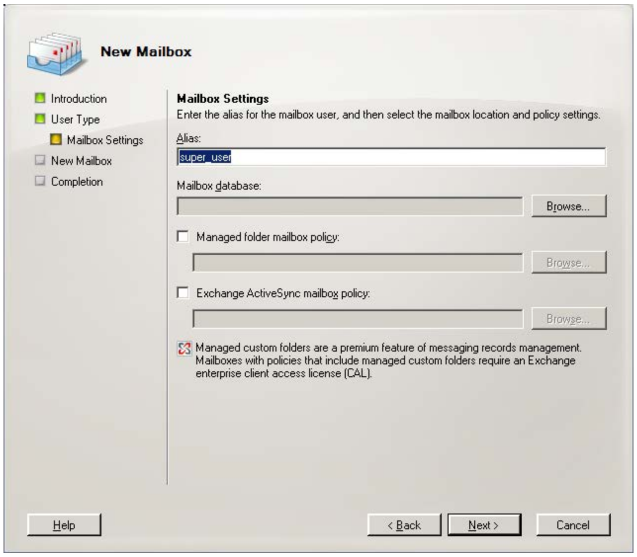
Create mailboxes for:

○ New user

● Existing users:

Name	Organizational Unit
super_user	your_domain.com/IMAP TEST USERS

5. Select the correct database and change any other settings that are required by your system configuration.



Mailbox Settings

Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias: super_user

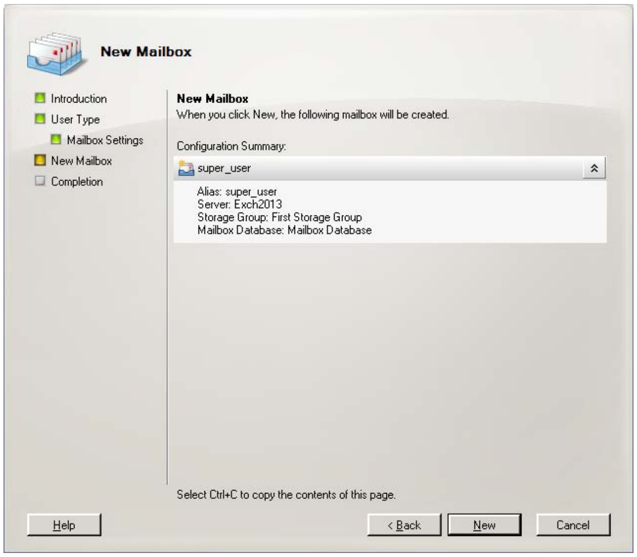
Mailbox database:

☐ Managed folder mailbox policy:

☐ Exchange ActiveSync mailbox policy:

Managed custom folders are a premium feature of messaging records management. Mailboxes with policies that include managed custom folders require an Exchange enterprise client access license (CAL).

6. Confirm the information then click **New** to create the mailbox.



New Mailbox

When you click New, the following mailbox will be created.

Configuration Summary:

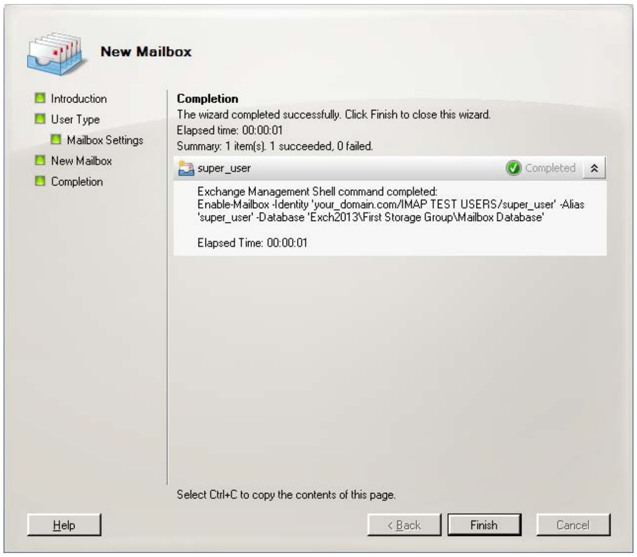
super_user

Alias: super_user
Server: Exch2013
Storage Group: First Storage Group
Mailbox Database: Mailbox Database

Select Ctrl+C to copy the contents of this page.

7. The superuser account has been created.

   Click **Finish** to exit the wizard.



Completion

The wizard completed successfully. Click Finish to close this wizard.
Elapsed time: 00:00:01
Summary: 1 item(s). 1 succeeded, 0 failed.

super_user ✓ Completed

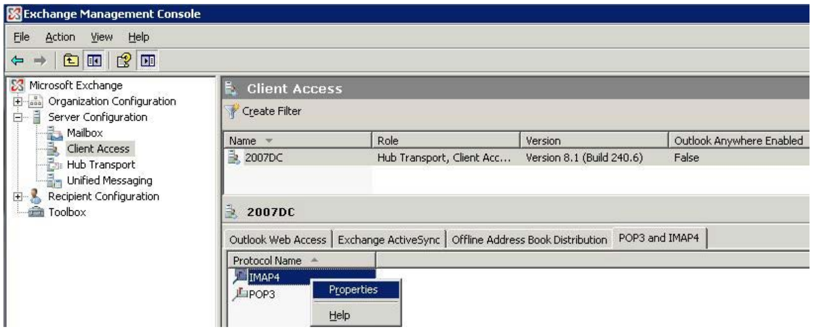
Exchange Management Shell command completed:
Enable-Mailbox -Identity 'your_domain.com/IMAP TEST USERS/super_user' -Alias 'super_user' -Database 'Exch2013\First Storage Group\Mailbox Database'

Elapsed Time: 00:00:01

Select Ctrl+C to copy the contents of this page.

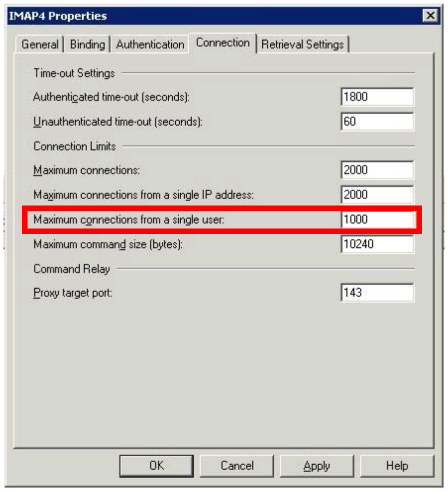
8. In order for a superuser account to properly manage all messages, you must allow a higher number of connections than there are by default.

   Open the **IMAP4 Properties** from the Client Access section.



Name	Role	Version	Outlook Anywhere Enabled
2007DC	Hub Transport, Client Acc…	Version 8.1 (Build 240.6)	False

9. From the **Connection** tab, set **Maximum connections from a single user** to **1000**.



Time-out Settings

Authenticated time-out (seconds): 1800

Unauthenticated time-out (seconds): 60

Connection Limits

Maximum connections: 2000

Maximum connections from a single IP address: 2000

Maximum connections from a single user: 1000

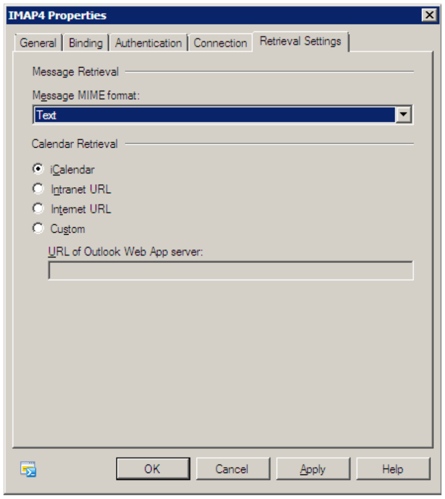
Maximum command size (bytes): 10240

Command Relay

Proxy target port: 143

10. From the Retrieval Settings tab, set **Message MIME format** to **Text**.

    Click **OK** to save your changes.



Message Retrieval

Message MIME format: Text

Calendar Retrieval

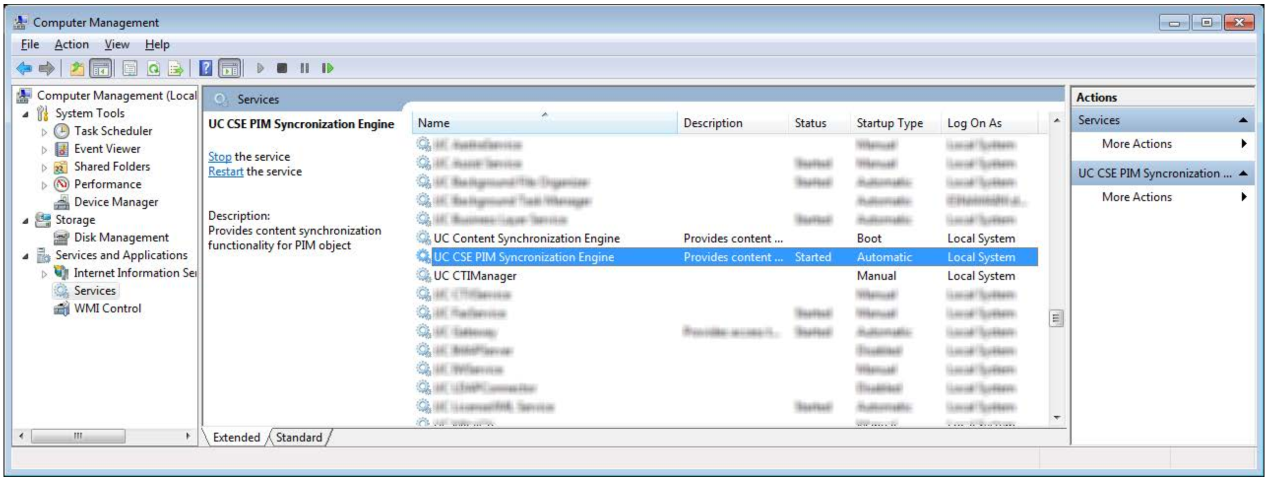
● iCalendar
○ Intranet URL
○ Internet URL
○ Custom

URL of Outlook Web App server:

Now that the superuser account is ready, prepare the Exchange 2010 server for integration and apply the correct administrative rights to the superuser account.

11. The **UC CSE PIM Synchronization Engine** service must login and run with the Superuser credentials.

    Open the **Computer Management** console and select **Services**.



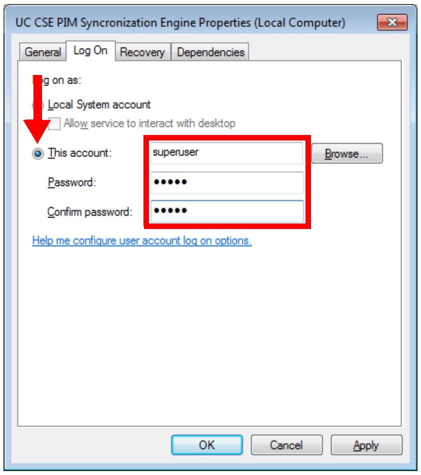
UC CSE PIM Syncronization Engine

Stop the service
Restart the service

Description:
Provides content synchronization functionality for PIM object

Name	Description	Status	Startup Type	Log On As
UC Content Synchronization Engine	Provides content ...		Boot	Local System
UC CSE PIM Syncronization Engine	Provides content ...	Started	Automatic	Local System
UC CTIManager			Manual	Local System

12. Stop the **UC CSE PIM Synchronization Engine** service.
13. 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.


UC CSE PIM Syncronization Engine Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.
OK
Cancel
Apply

g on as:

○ Local System account

□ Allow service to interact with desktop

● This account: superuser

Password: •••••

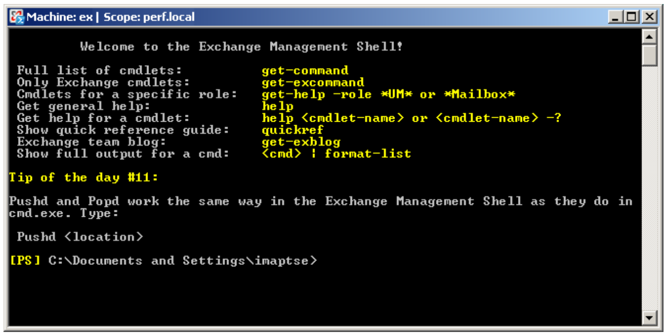
Confirm password: •••••

Click **Apply** and **OK** when finished.

14. Restart the service.

Exchange 2010 Shell Configuration

Since only simple actions are available through the GUI, continue the configuration through the Exchange Management Shell.



Machine: ex | Scope: perf.local

```
         Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #11:

Pushd and Popd work the same way in the Exchange Management Shell as they do in
cmd.exe. Type:

 Pushd <location>

[PS] C:\Documents and Settings\imaptse>
```

Note: <> represents a single space in the command.

Configuring the IMAP server

All IMAP server settings may be viewed by typing the command:

Get-imapsettings

For integration with the IMAPCSE, you must execute this command to change the way in which logins are handled by IMAP.

Set-imapsettings<>–logintype<>PlaintextLogin

By default, the IMAP server daemon is disabled in Exchange 2010, so you must turn it on manually. You must configure the server so that the IMAP services are always started automatically for server restarts.

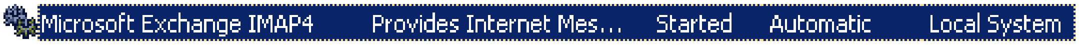
Set-service<>msExchangeIMAP4<>–startuptype<>automatic

Start the IMAP Service

Start–service<>msExchangeIMAP4

At this stage, the IMAP service will be running, and it will start each time the computer restarts.

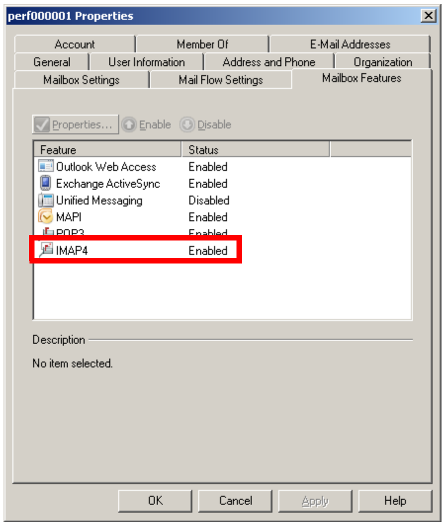
To test this, open a command prompt (Windows prompt not Exchange Shell) and enter **telnet<>serverIP<>143**. You should see the banner reply. You may also verify the procedure by checking the status of the service.



Microsoft Exchange IMAP4   Provides Internet Mes...   Started   Automatic   Local System

IMAP Enabling All Existing Mailboxes in a Store

If the mailboxes within your Exchange server do not have IMAP enabled, you can use the following commands to enable the feature for the mailboxes. You may confirm the status of the feature by opening the mailbox properties, then going to the **Mailbox Features** tab as shown here.



Feature	Status
Outlook Web Access	Enabled
Exchange ActiveSync	Enabled
Unified Messaging	Disabled
MAPI	Enabled
POP3	Enabled
IMAP4	Enabled

Description

No item selected.

Note: All mailbox accounts that require IMAPCSE synchronization must have IMAP enabled under Exchange.

IMAP Enabling All Users

```
Get-mailbox<>|<>Set-CASMailbox<>–ImapEnabled:$true
```

This command gets each mailbox and pipes it into the **Set-CASMailbox** command sequentially.

IMAP Enabling a Single User

Use this command to individually enable IMAP on each user.

```
Set-CASMailbox<>%mailbox%<>–ImapEnabled:$true
```

The **%mailbox%** variable represents the mailbox account name for which you want to enable IMAP.

Configuring Permissions for the superuser Account

The following commands will give the superuser account permission to logon to all user's mailboxes. There are two separate commands needed; type the first, hit enter, and then type the second.

In both cases, the **%superuser%** variable represents the domain and superuser account you have created in the previous steps. For example, if the superuser's user name is **SUPER_USER**, and the domain is **COMAPNY.COM**, enter **COMPANY\SUPER_USER** in place of **%superuser%.**

Command 1

```
Get-Mailbox<>|<>Add-ADPermission<>-User<>'%superuser%'<>-ExtendedRights<>'Send-as'<>-InheritanceType<>All
```

Command 2

```
Get-Mailbox<>|<>Add-MailboxPermission<>-User '%superuser%'<>-AccessRights<>'FullAccess'<>-InheritanceType<>All
```

This is the last configuration step required on the Exchange 2010 server and you are ready to move on to the Avaya Messaging configuration.

Note: If you add new mailbox accounts to the Exchange server after this point, you must enable those accounts for IMAP manually as well. To do this, use the following commands.

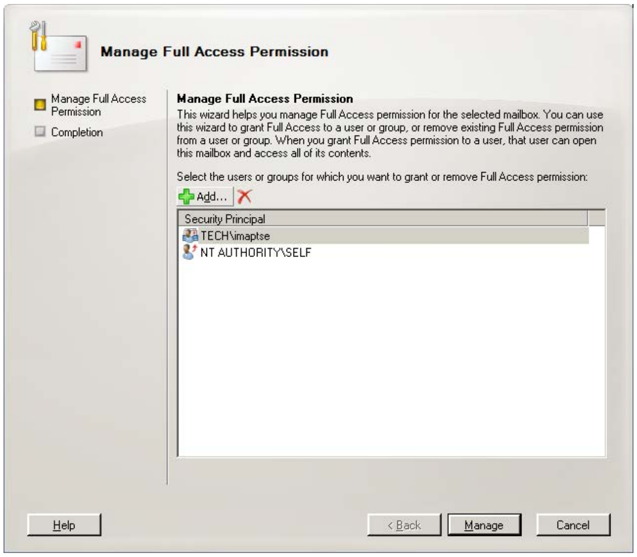
IMAP Enable a New Mailbox

```
Set-CASMailbox<>%mailbox%<>–ImapEnabled:$true
```

Run a Modified Version of Command 2 Without the Pipeswitch

```
add-mailboxpermission<>-identity%mailbox%<>-User '%superuser%'<>-AccessRights<>'FullAccess'<>-
  InheritanceType<>All
```

You can confirm the access rights for the superuser account by opening the **Manage Full Access Permission** panel. The superuser account name should be listed.


Manage Full Access Permission

Manage Full Access Permission

This wizard helps you manage Full Access permission for the selected mailbox. You can use this wizard to grant Full Access to a user or group, or remove existing Full Access permission from a user or group. When you grant Full Access permission to a user, that user can open this mailbox and access all of its contents.

Select the users or groups for which you want to grant or remove Full Access permission:

Security Principal
TECH\imaptse
NT AUTHORITY\SELF

A More Secure Solution

Command 1 and 2 (above) provide full access for the superuser to the entire store drive. Instead, you can use these commands to limit access to just the MSExchange stores:

```
Get-MailboxDatabase | Add-ADPermission -User '%superuser%' -AccessRights ExtendedRight -
ExtendedRights Receive-As, ms-Exch-Store-Admin
```

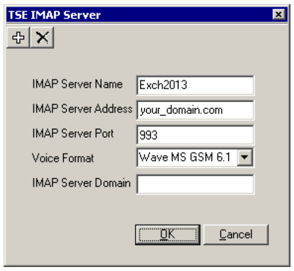
> **Note:** If a new mailbox database is created for Microsoft Exchange, you must re-enter this command so that the new file is given the correct user access rights.

Avaya Messaging 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

In order for the Avaya Messaging server to recognize the Exchange server, you must add a new CSE Endpoint entry in the **Avaya Messaging Admin > TSE IMAP Server** section.



IMAP Server Name: Exch2013
IMAP Server Address: your_domain.com
IMAP Server Port: 993
Voice Format: Wave MS GSM 6.1
IMAP Server Domain:

Note: **CSE** was formerly known as **TSE**.

IMAP Server Name: This name is for your reference and does impact system performance.

IMAP Server Address: Enter the server address of the Exchange server.

IMAP Server Port: The port number of the Exchange server. By default, IMAP uses port 993.

Voice Format: From the dropdown menu, select the voice format used when sending voice messages to external voice servers.

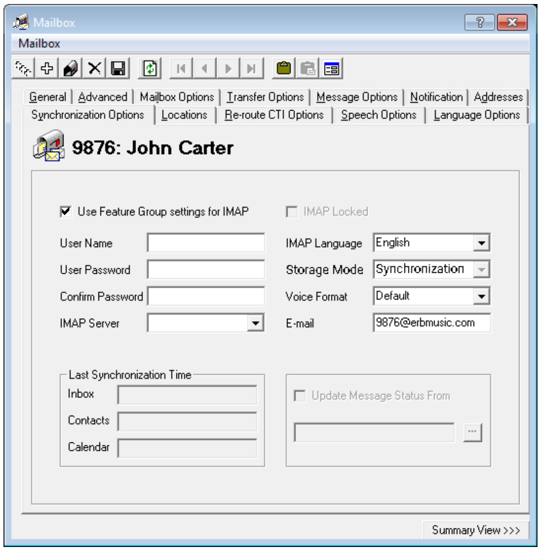
IMAP Server Domain: Enter the Domain address of the IMAP server. Since it is possible to define the IMAP Server Address using an IP address, the Domain address entered here is used to verify the Reply to address of a mailbox using IMAP CSE synchronization, preventing typical message looping scenarios.

Individual Mailbox Configuration

With the superuser account, you do not have to fully enter the individual mailbox credentials for IMAPCSE synchronization.

Enable **Use Feature Group settings for IMAP** then enter the **User Name** (this will be the alias for the Exchange account that the current mailbox will be synchronized with) and leave the **User Password** and **IMAP Server** fields empty.

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


Mailbox
Mailbox
General | Advanced | Mailbox Options | Transfer Options | Message Options | Notification | Addresses
Synchronization Options | Locations | Re-route CTI Options | Speech Options | Language Options
Last Synchronization Time
Inbox
Contacts
Calendar
Summary View >>>

9876: John Carter

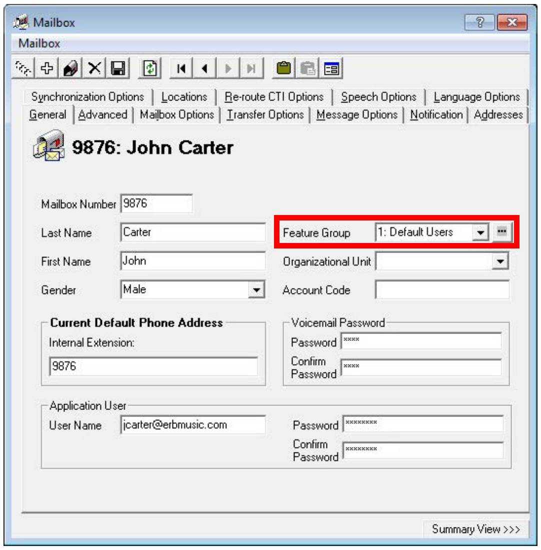
☑ Use Feature Group settings for IMAP
□ IMAP Locked

User Name:
User Password:
Confirm Password:
IMAP Server:
IMAP Language: English
Storage Mode: Synchronization
Voice Format: Default
E-mail: 9876@erbmusic.com

□ Update Message Status From

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.



9876: John Carter

Mailbox Number 9876

Last Name Carter

First Name John

Gender Male

Feature Group 1: Default Users

Organizational Unit

Account Code

Current Default Phone Address

Internal Extension: 9876

Voicemail Password

Password ****

Confirm Password ****

Application User

User Name jcarter@erbmusic.com

Password ********

Confirm Password ********

Feature Group Configuration

The Feature Group plays a key role in IMAPCSE synchronization by providing the necessary credentials. From the **Synchronization Options** tab, configure the settings as follows:

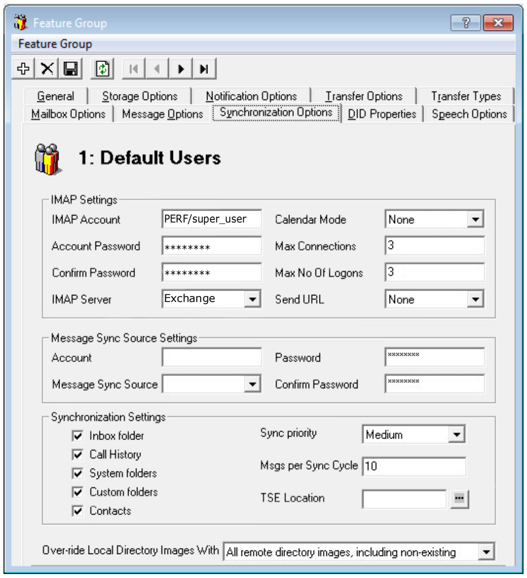
IMAP Account: Enter the account name for the superuser. The typical format will be **domain/super_user_name**.

Account Password: Enter the password of the superuser account.

Confirm Password: Re-enter the password.

IMAP Server: Select the CSE Endpoint created in the previous steps.

Save all changes and proceed to Registry Settings.



1: Default Users

IMAP Settings

IMAP Account PERF/super_user

Account Password ********

Confirm Password ********

IMAP Server Exchange

Calendar Mode None

Max Connections 3

Max No Of Logons 3

Send URL None

Message Sync Source Settings

Account

Message Sync Source

Password ********

Confirm Password ********

Synchronization Settings

☑ Inbox folder

☑ Call History

☑ System folders

☑ Custom folders

☑ Contacts

Sync priority Medium

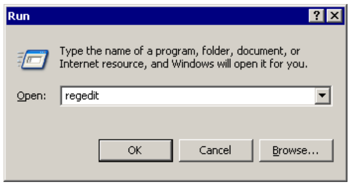
Msgs per Sync Cycle 10

TSE Location

Over-ride Local Directory Images With All remote directory images, including non-existing

Registry Settings

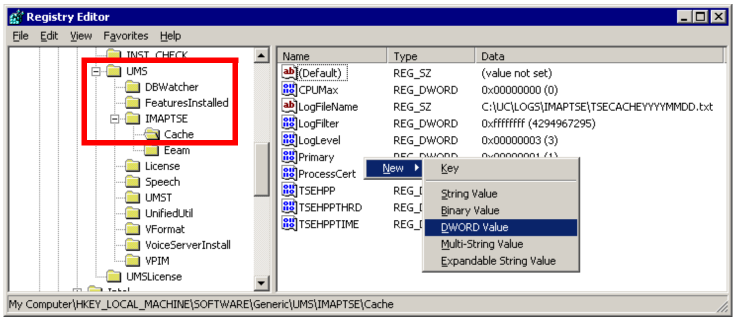
In order for Avaya Messaging to manage communications with the Exchange server, you must manually add a registry value on the Avaya Messaging server. Run the registry editor by typing **regedit** from the Run command.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

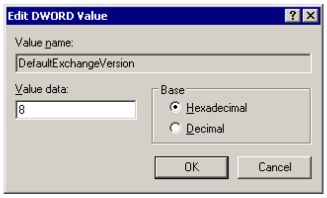
Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache**. Create a new **DWORD Value** entry in this location.



Name	Type	Data
(Default)	REG_SZ	(value not set)
CPUMax	REG_DWORD	0x00000000 (0)
LogFileName	REG_SZ	C:\UC\LOGS\IMAPTSE\TSECACHEYYYYMMDD.txt
LogFilter	REG_DWORD	0xffffffff (4294967295)
LogLevel	REG_DWORD	0x00000003 (3)
Primary	REG_DWORD	0x00000001 (1)
ProcessCert		
TSEHPP	REG_	
TSEHPPTHRD	REG_	
TSEHPPTIME	REG_	

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache

Name the entry **DefaultExchangeVersion** and assign it a value of **8**.



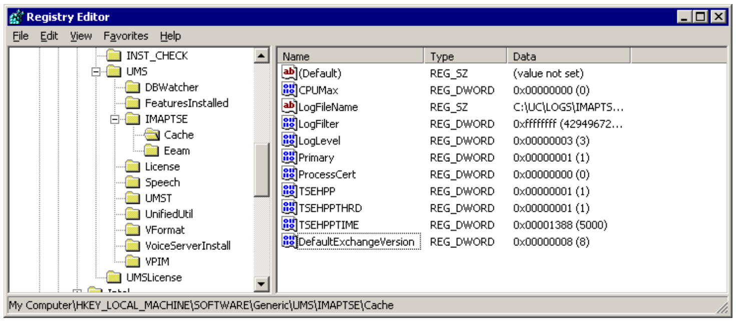
Value name: DefaultExchangeVersion

Value data: 8

● Hexadecimal
○ Decimal

The new registry entry will appear in the Registry.

Proceed with Certificate Configuration.



Name	Type	Data
(Default)	REG_SZ	(value not set)
CPUMax	REG_DWORD	0x00000000 (0)
LogFileName	REG_SZ	C:\UC\LOGS\IMAPTS...
LogFilter	REG_DWORD	0xffffffff (42949672...
LogLevel	REG_DWORD	0x00000003 (3)
Primary	REG_DWORD	0x00000001 (1)
ProcessCert	REG_DWORD	0x00000000 (0)
TSEHPP	REG_DWORD	0x00000001 (1)
TSEHPPTHRD	REG_DWORD	0x00000001 (1)
TSEHPPTIME	REG_DWORD	0x00001388 (5000)
DefaultExchangeVersion	REG_DWORD	0x00000008 (8)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache

Certificate Configuration

In order 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 server.

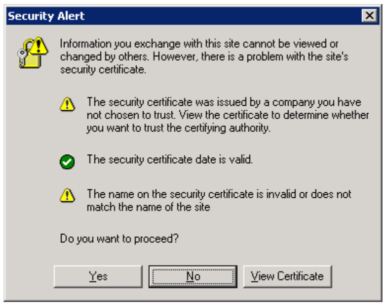
The simplest way to achieve this is to access the OWA (Outlook Web Access) web page of the Exchange server.

> **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 the OWA page (e.g. https://exchange_2010/owa).

   You will see the following security warning popup.

   Click on **View Certificate**.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

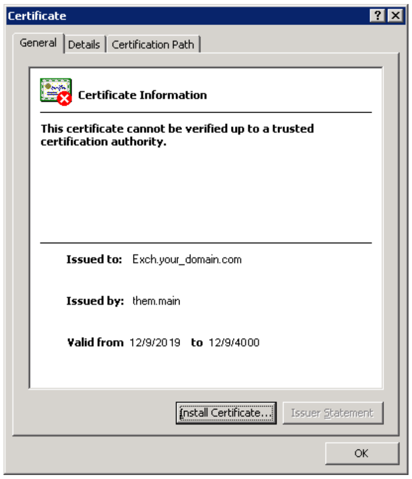
The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

2. Click on **Install Certificate** to launch to 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.



Certificate Information

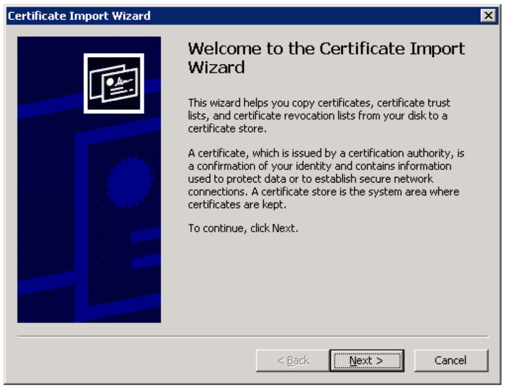
This certificate cannot be verified up to a trusted certification authority.

Issued to: Exch.your_domain.com

Issued by: them.main

Valid from 12/9/2019 to 12/9/4000

3. Click **Next**.



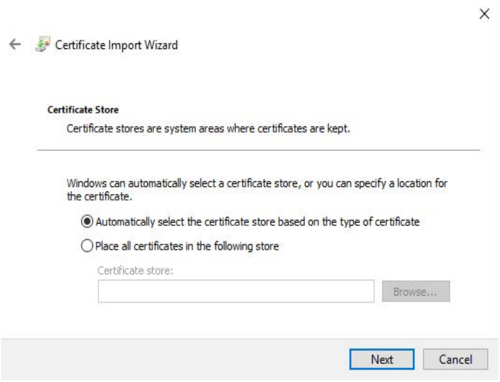
Welcome to the Certificate Import Wizard

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.

To continue, click Next.

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



Certificate Store

Certificate stores are system areas where certificates are kept.

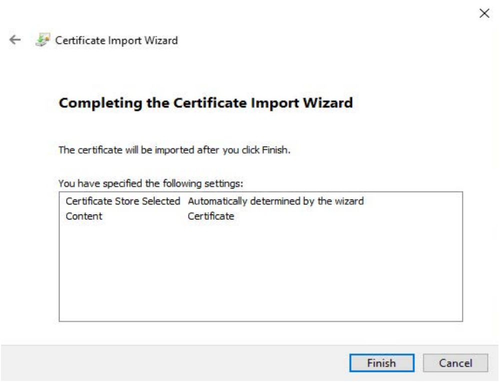
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

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



Completing the Certificate Import Wizard

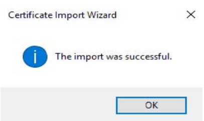
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

6. The following popup confirms the import was successful.

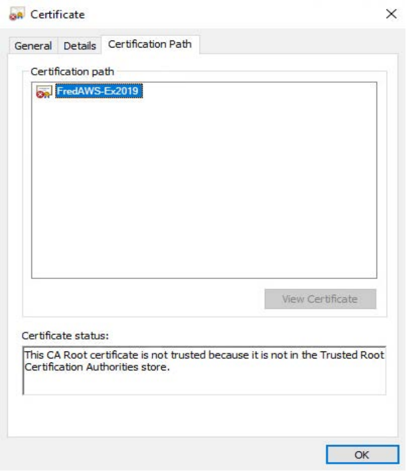
   Click **OK**.



The import was successful.

7. 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.

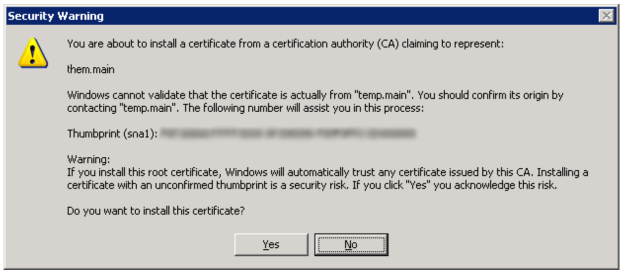


Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

8. Depending on the security settings on the system, you may also see the following warning popup.

   Click **Yes** to accept the certificate in this case.



You are about to install a certificate from a certification authority (CA) claiming to represent:

them.main

Windows cannot validate that the certificate is actually from "temp.main". You should confirm its origin by contacting "temp.main". The following number will assist you in this process:

Thumbprint (sha1): [redacted]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

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 of 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.

Note: If you did not install the Exchange MAPI component during the initial Avaya Messaging installation, you must do so manually now by running the **ExchangeMapiCdo.msi** file from **MSExchange** folder on Avaya Messaging installation DVD. This is a required component for contact and calendar synchronization.

Feature Group

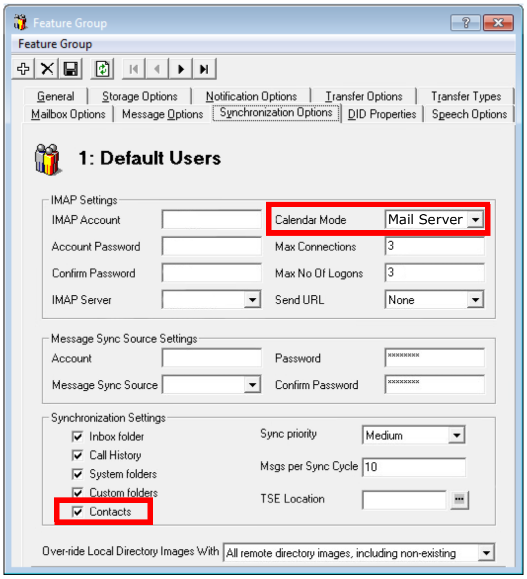
Feature Group configuration requires changes on two tabs; **Synchronization Options** and **Mailbox Option**. You can define exactly what is going to be synchronized for the users from these two sections.

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 **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.



1: Default Users

IMAP Settings

IMAP Account:
Account Password:
Confirm Password:
IMAP Server:
Calendar Mode: Mail Server
Max Connections: 3
Max No Of Logons: 3
Send URL: None

Message Sync Source Settings

Account:
Message Sync Source:
Password: ********
Confirm Password: ********

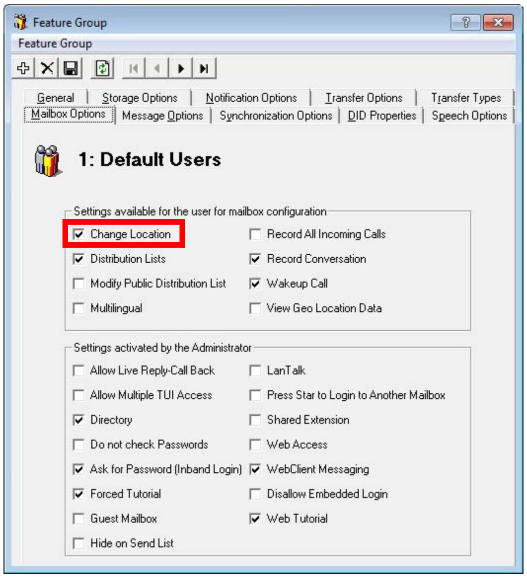
Synchronization Settings

☑ Inbox folder
☑ Call History
☑ System folders
☑ Custom folders
☑ Contacts

Sync priority: Medium
Msgs per Sync Cycle: 10
TSE Location:

Over-ride Local Directory Images With: All remote directory images, including non-existing

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



1: Default Users

Settings available for the user for mailbox configuration

☑ Change Location
☑ Distribution Lists
☐ Modify Public Distribution List
☐ Multilingual
☐ Record All Incoming Calls
☑ Record Conversation
☑ Wakeup Call
☐ View Geo Location Data

Settings activated by the Administrator

☐ Allow Live Reply-Call Back
☐ Allow Multiple TUI Access
☑ Directory
☐ Do not check Passwords
☑ Ask for Password (Inband Login)
☑ Forced Tutorial
☐ Guest Mailbox
☐ Hide on Send List
☐ LanTalk
☐ Press Star to Login to Another Mailbox
☐ Shared Extension
☐ Web Access
☑ WebClient Messaging
☐ Disallow Embedded Login
☑ Web Tutorial

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.

User Guide

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.

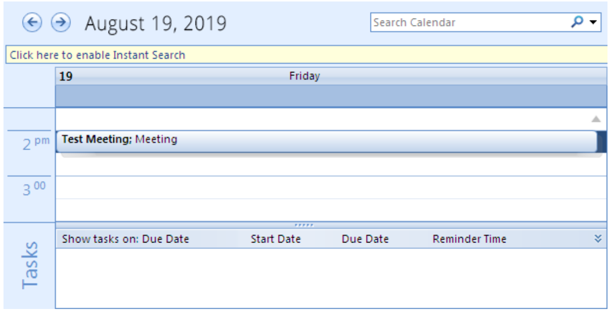
Note: All of the calendar events and contacts from your mail server will be copied into your Avaya Messaging mailbox as soon as the administrator finishes configuring the systems.

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.

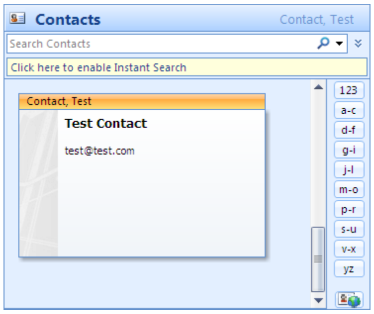
The time and date of the meeting is automatically sent to the Avaya Messaging mailbox. By default, the location for these events will be marked as **Meeting**. You may change this manually through Web Access, or in the case of Outlook, you may utilize the iLink Pro Desktop tool bar to assign a specific location to the event.



Test Meeting: Meeting

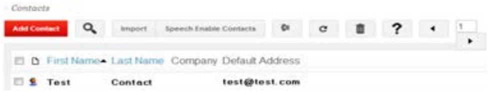
Contact Synchronization

When you create a contact entry from Outlook, the entry will be copied into your Avaya Messaging mailbox.



Contact, Test
Test Contact
test@test.com

Contact information is automatically sent to the Avaya Messaging mailbox.



First Name	Last Name	Company	Default Address
Test	Contact		test@test.com

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

MS Exchange Performance Considerations

Microsoft (**http://support.microsoft.com/kb/905803**) advises that a 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 2003	Exchange 2007	Exchange 2003
Messages	<5000 combined	<20000	<100000
Contact and Calendar Entries		<5000	<10000

13 OFFICE 365 INTEGRATION WITH MICROSOFT GRAPH

In This Chapter:

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 suites your requirements.

CHAPTER	INTEGRATION	WHY YOU WANT IT
9	Google	Creates a secure connection through OAuth2 to your Gmail and Google Apps accounts.
10	Exchange using EWS	The simplest connection between your Exchange server and Avaya Messaging.
11	Exchange without EWS	A connection between Exchange and Avaya Messaging for legacy systems.
12	Exchange 2010	A connection between Exchange 2010 and Avaya Messaging.
13	Office 365 using Graph	Setup the latest high security integration procedures for maximum data integrity.
14	Office 365 using EWS	Quick connection between your O365 server and Avaya Messaging.

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:

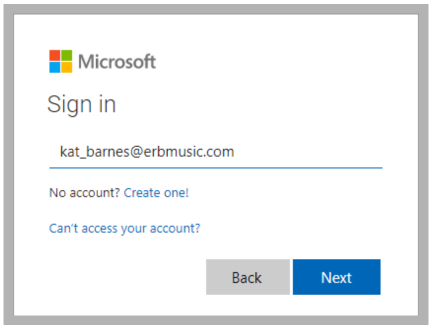
- The Office 365 domain has been setup and deployed (requires Mid-size Business and Enterprise plan minimum, E1 or E3).
- You must have administrative access to the Office 365 domain.
- Avaya Messaging Server installed and running (refer to Avaya's documentation web site).

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 communication traffic flows.

Warning: This section contains advanced concepts and programming steps that could adversely affect operations if handled incorrectly. Read through these 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 the Office 365 site at https://www.office.com.
   Click **Sign in** and login using your Office 365 administrator account credentials.
   Click **Next** when ready.



Microsoft

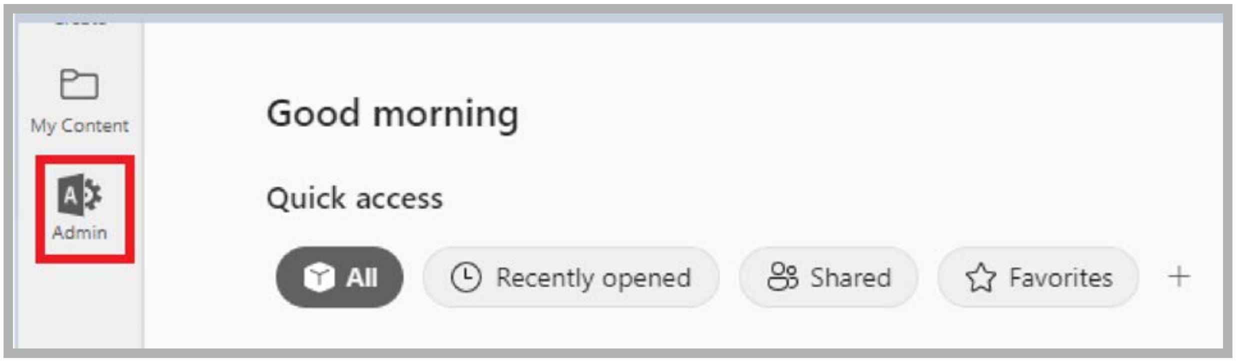
Sign in

kat_barnes@erbmusic.com

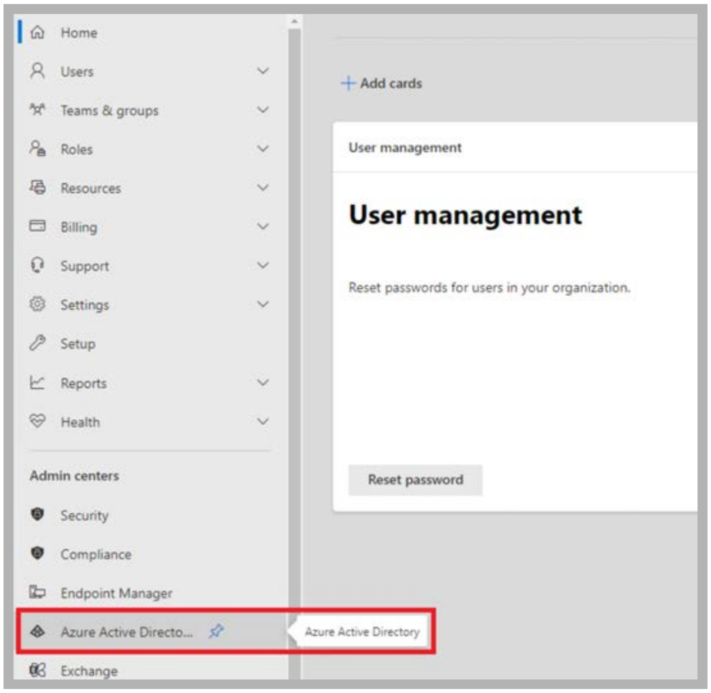
No account? Create one!

Can't access your account?

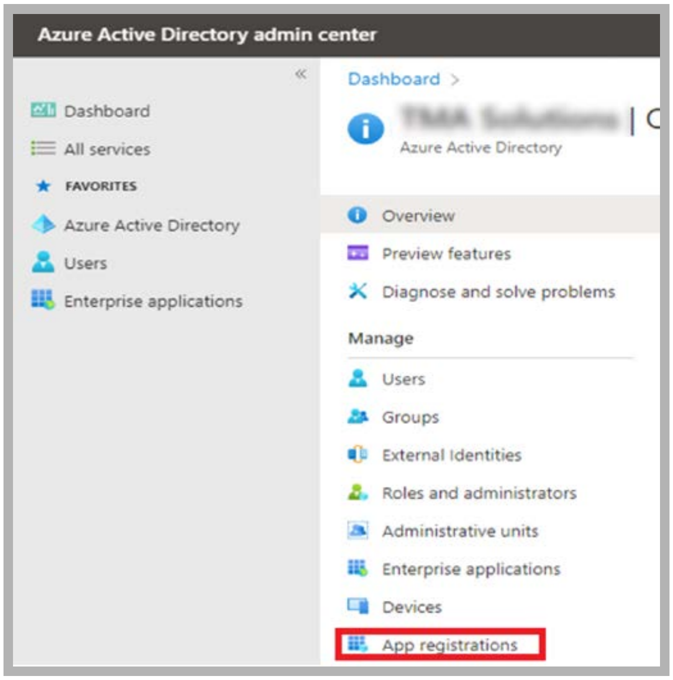
2. On the Office365 home page, click **Admin**.



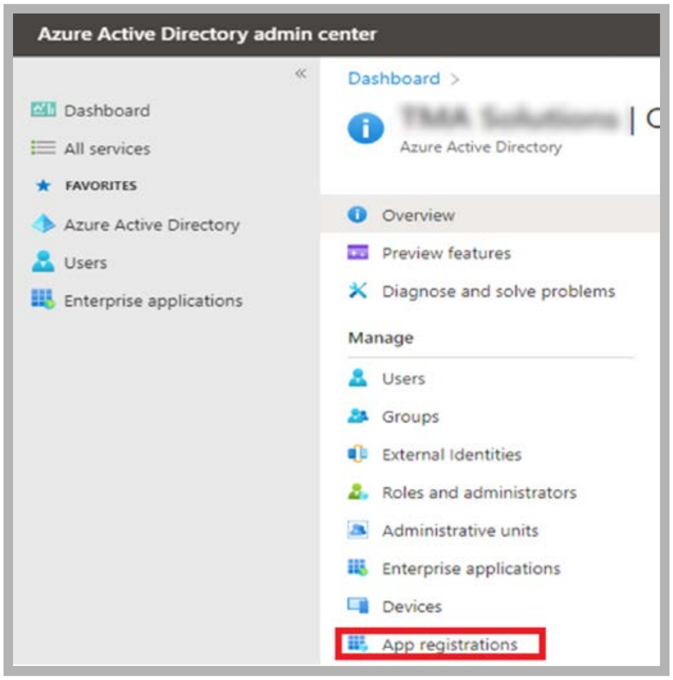
3. In the left-hand panel (**Show All**), under **Admin centers**, select **Azure Active Directory**. The Azure dashboard will appear.



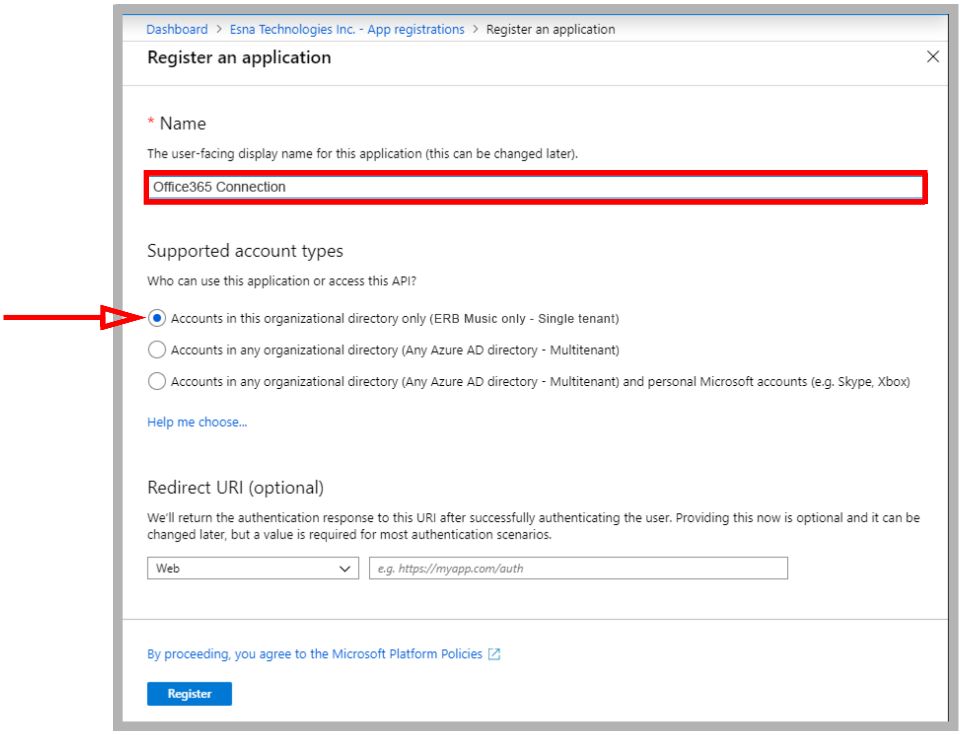
4. Open **Azure Active Directory** and select **App registrations**.



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**.



Dashboard > Esna Technologies Inc. - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Office365 Connection

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (ERB Music only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

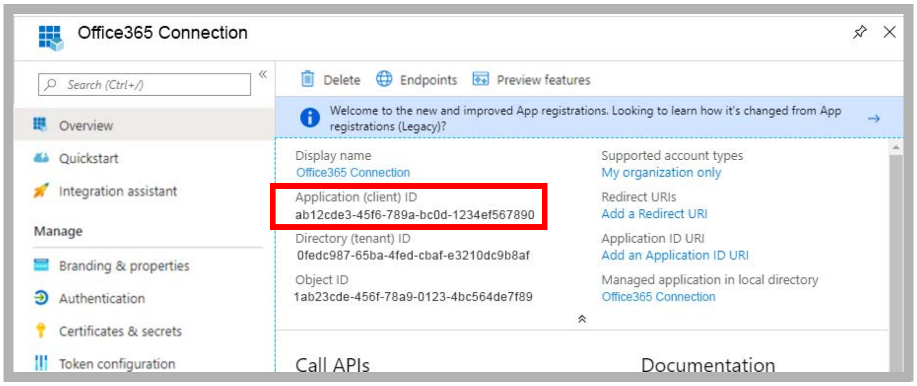
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Register

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



Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)?

Display name: Office365 Connection

Application (client) ID: ab12cde3-45f6-789a-bc0d-1234ef567890

Directory (tenant) ID: 0fedc987-65ba-4fed-cbaf-e3210dc9b8af

Object ID: 1ab23cde-456f-78a9-0123-4bc564de7f89

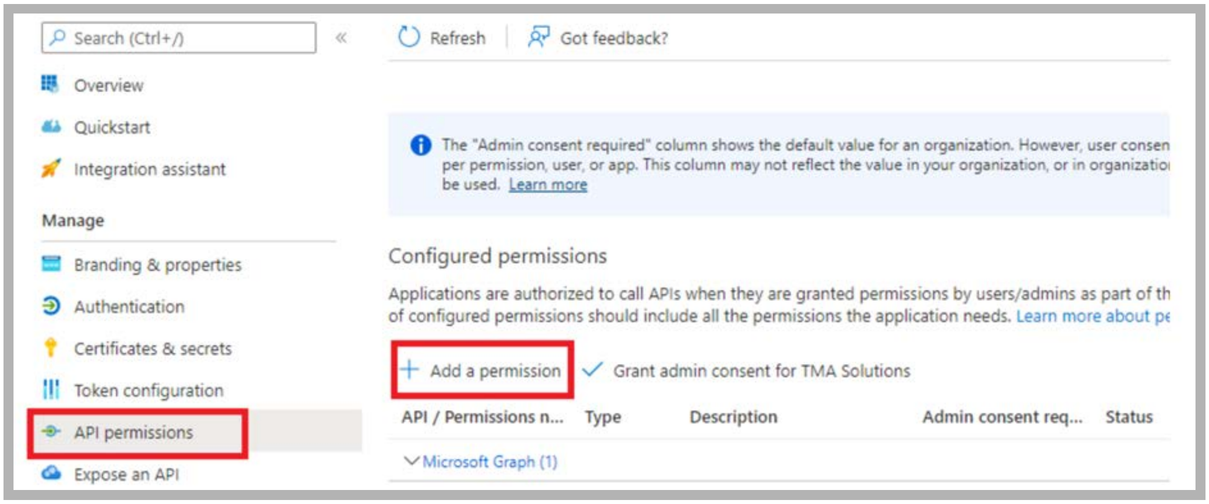
Supported account types: My organization only

Redirect URIs: Add a Redirect URI

Application ID URI: Add an Application ID URI

Managed application in local directory: Office365 Connection

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

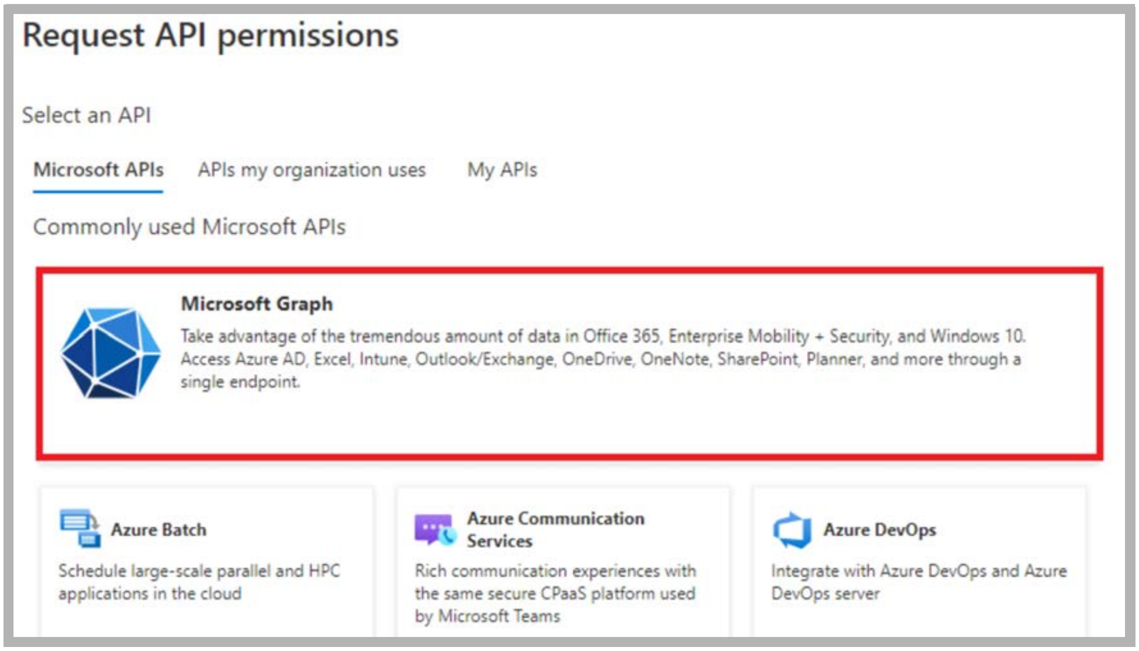


The "Admin consent required" column shows the default value for an organization. However, user consen per permission, user, or app. This column may not reflect the value in your organization, or in organizatio be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of th of configured permissions should include all the permissions the application needs. Learn more about pe

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



Request API permissions

Select an API

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

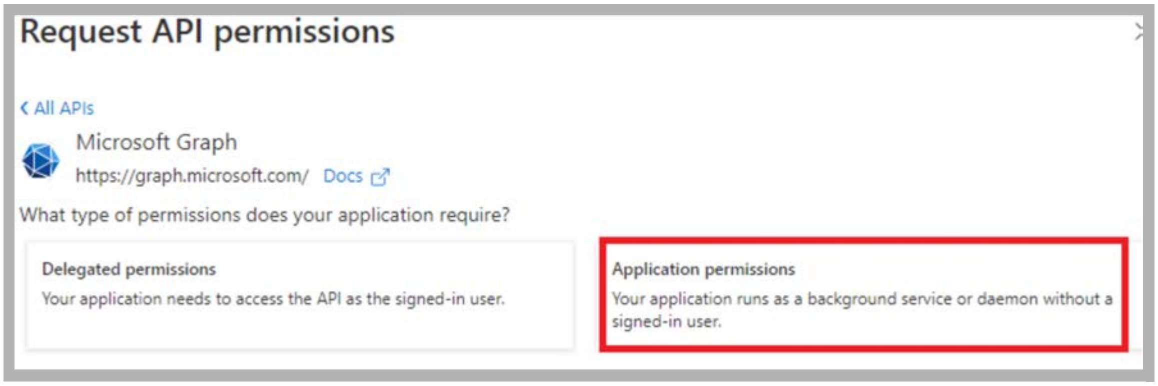
Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

10. Choose **Application permissions**.



Request API permissions

< All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

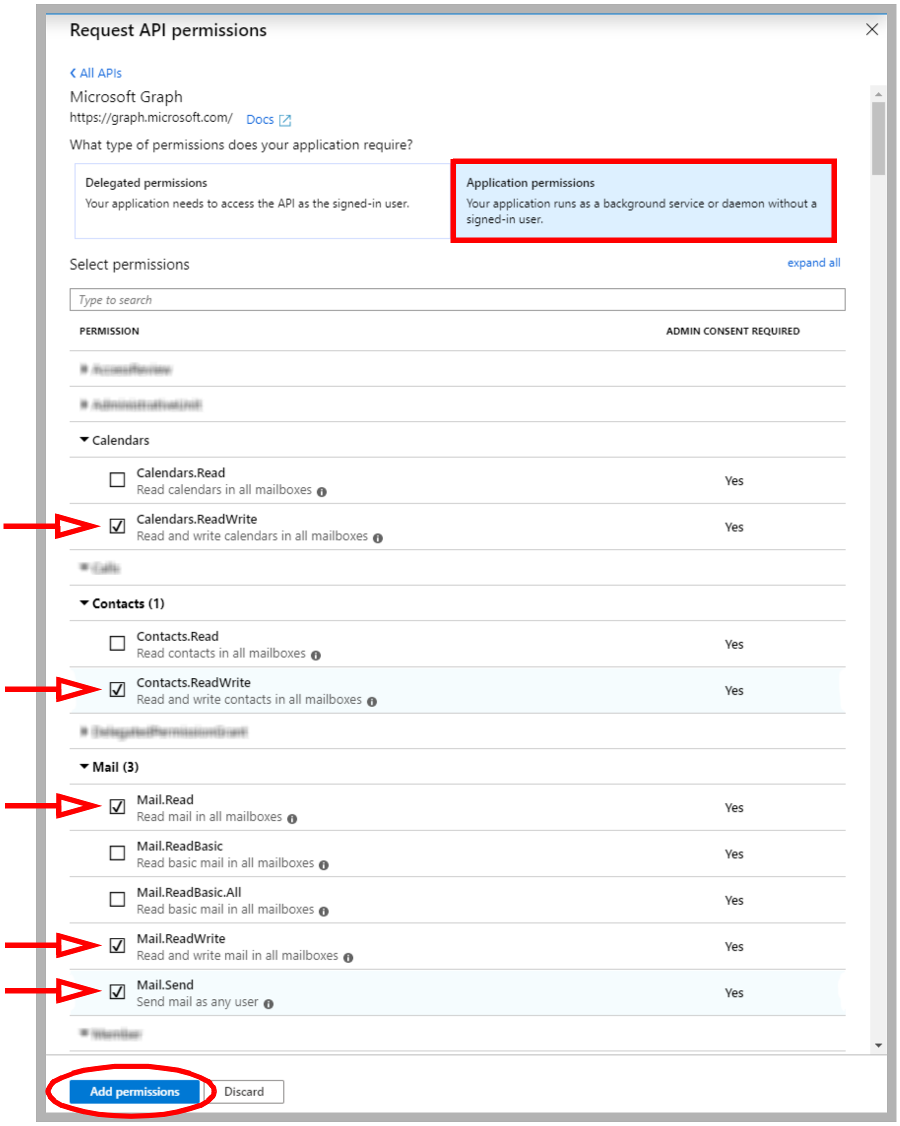
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

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

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

Click **Add permissions**.



Request API permissions

< All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

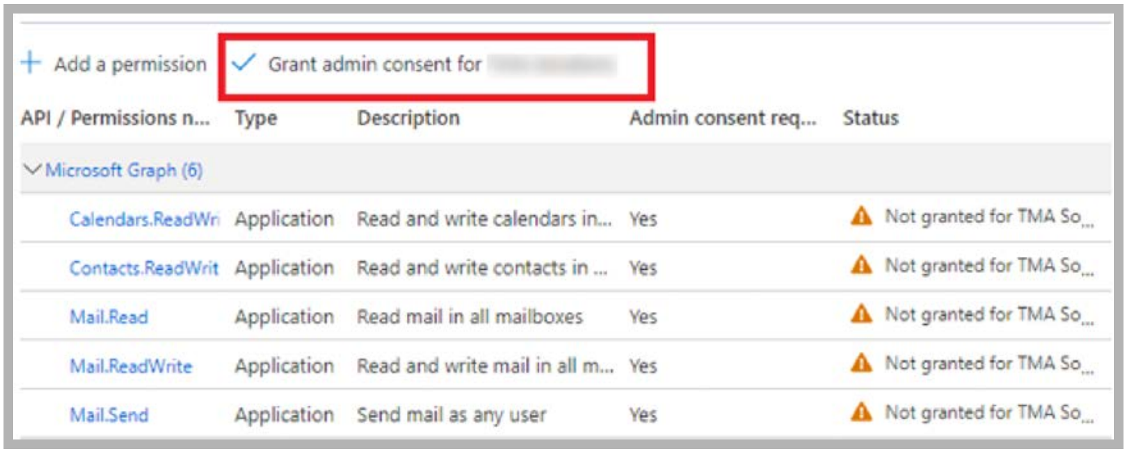
expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▾ Calendars	
□ Calendars.Read Read calendars in all mailboxes	Yes
☑ Calendars.ReadWrite Read and write calendars in all mailboxes	Yes
▾ Contacts (1)	
□ Contacts.Read Read contacts in all mailboxes	Yes
☑ Contacts.ReadWrite Read and write contacts in all mailboxes	Yes
▾ Mail (3)	
☑ Mail.Read Read mail in all mailboxes	Yes
□ Mail.ReadBasic Read basic mail in all mailboxes	Yes
□ Mail.ReadBasic.All Read basic mail in all mailboxes	Yes
☑ Mail.ReadWrite Read and write mail in all mailboxes	Yes
☑ Mail.Send Send mail as any user	Yes

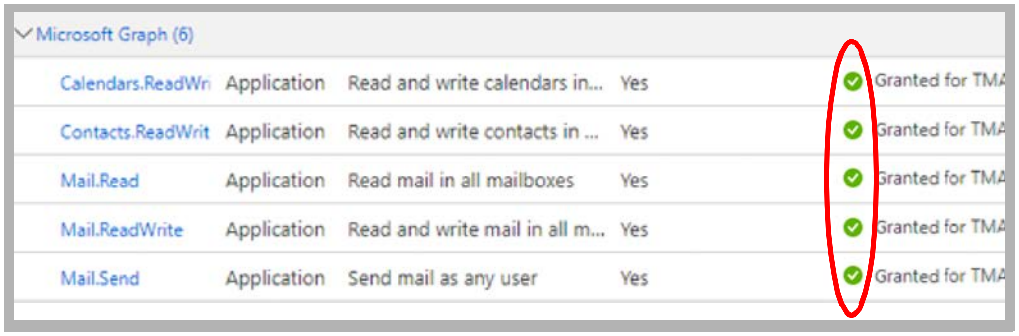
Note: The permissions that are required are based upon each site's requirements. For example, if Calendar or Contact synchronization is not necessary, then those permissions can be left out.

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



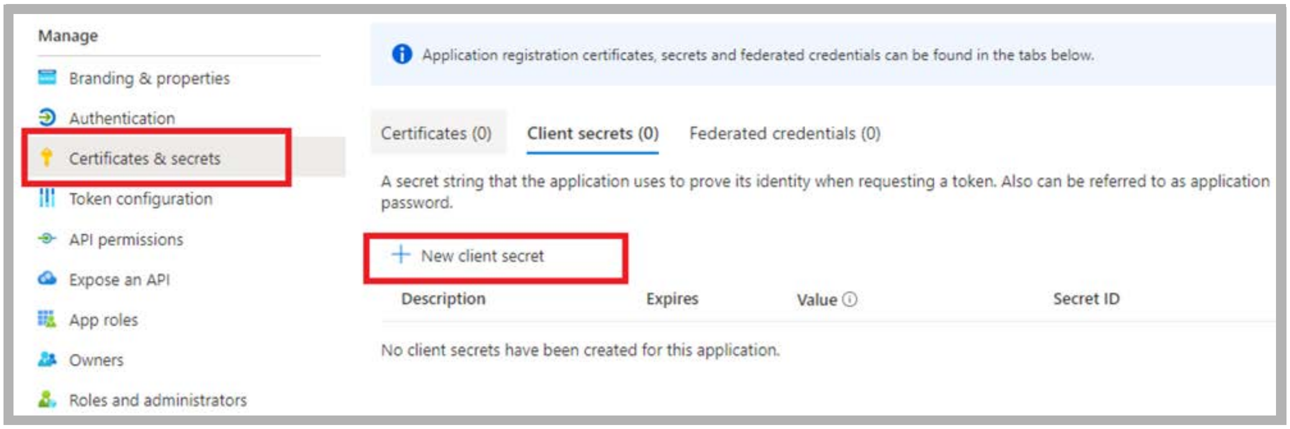
API / Permissions n...	Type	Description	Admin consent req...	Status
Calendars.ReadWr	Application	Read and write calendars in...	Yes	⚠ Not granted for TMA So...
Contacts.ReadWrit	Application	Read and write contacts in ...	Yes	⚠ Not granted for TMA So...
Mail.Read	Application	Read mail in all mailboxes	Yes	⚠ Not granted for TMA So...
Mail.ReadWrite	Application	Read and write mail in all m...	Yes	⚠ Not granted for TMA So...
Mail.Send	Application	Send mail as any user	Yes	⚠ Not granted for TMA So...

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



Calendars.ReadWr	Application	Read and write calendars in...	Yes	✓ Granted for TMA
Contacts.ReadWrit	Application	Read and write contacts in ...	Yes	✓ Granted for TMA
Mail.Read	Application	Read mail in all mailboxes	Yes	✓ Granted for TMA
Mail.ReadWrite	Application	Read and write mail in all m...	Yes	✓ Granted for TMA
Mail.Send	Application	Send mail as any user	Yes	✓ Granted for TMA

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



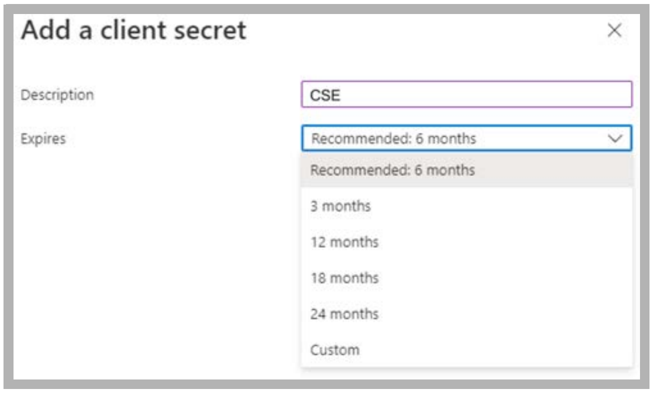
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID

No client secrets have been created for this application.

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



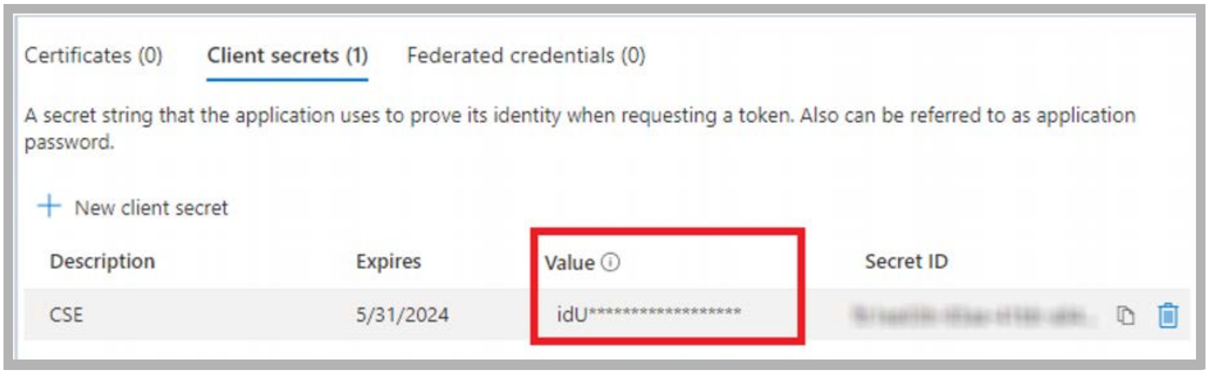
Add a client secret

Description: CSE

Expires: Recommended: 6 months

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.



A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
CSE	5/31/2024	idU******************	[redacted]

17. In Avaya Messaging Admin, add a new TSE IMAP server, and include the Office 365 server information.

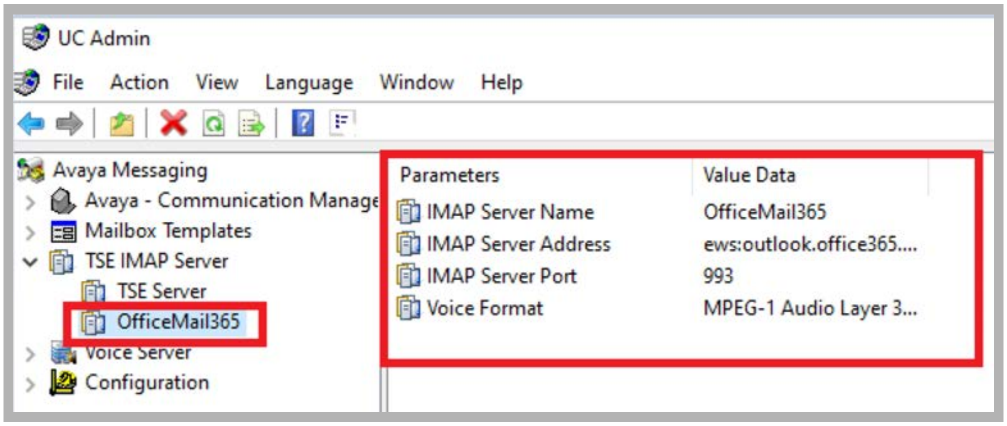
    IMAP Server Name: Enter a name for this connection (e.g. **OfficeMail365**).

    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.



Parameters	Value Data
IMAP Server Name	OfficeMail365
IMAP Server Address	ews:outlook.office365....
IMAP Server Port	993
Voice Format	MPEG-1 Audio Layer 3...

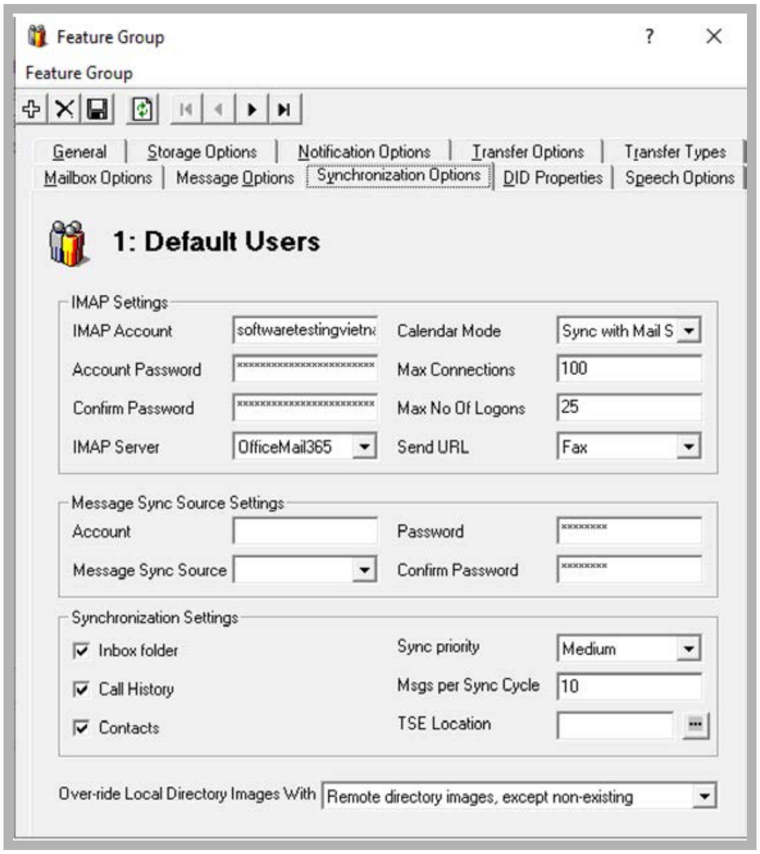
18. Go to the **Feature Group > Synchronization Options** tab.
Under **IMAP Settings**, configure:

- **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**.


Feature Group
? ×
Feature Group
General | Storage Options | Notification Options | Transfer Options | Transfer Types
Mailbox Options | Message Options | Synchronization Options | DID Properties | Speech Options

1: Default Users

IMAP Settings

IMAP Account	softwaretestingvietn:	Calendar Mode	Sync with Mail S
Account Password	************************	Max Connections	100
Confirm Password	************************	Max No Of Logons	25
IMAP Server	OfficeMail365	Send URL	Fax

Message Sync Source Settings

Account		Password	********
Message Sync Source		Confirm Password	********

Synchronization Settings

☑ Inbox folder	Sync priority	Medium
☑ Call History	Msgs per Sync Cycle	10
☑ Contacts	TSE Location	

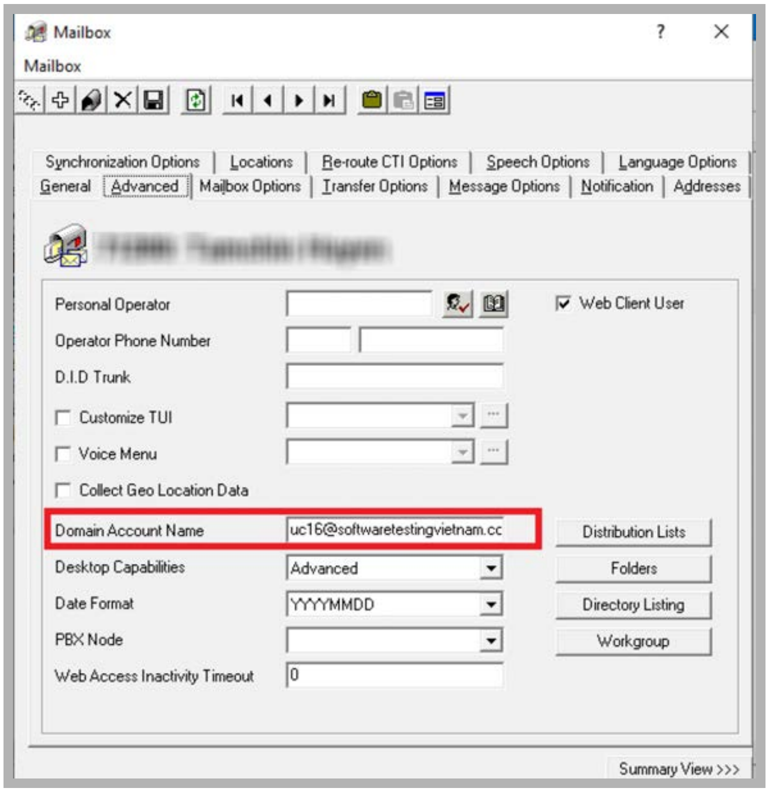
Over-ride Local Directory Images With: Remote directory images, except non-existing

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**.

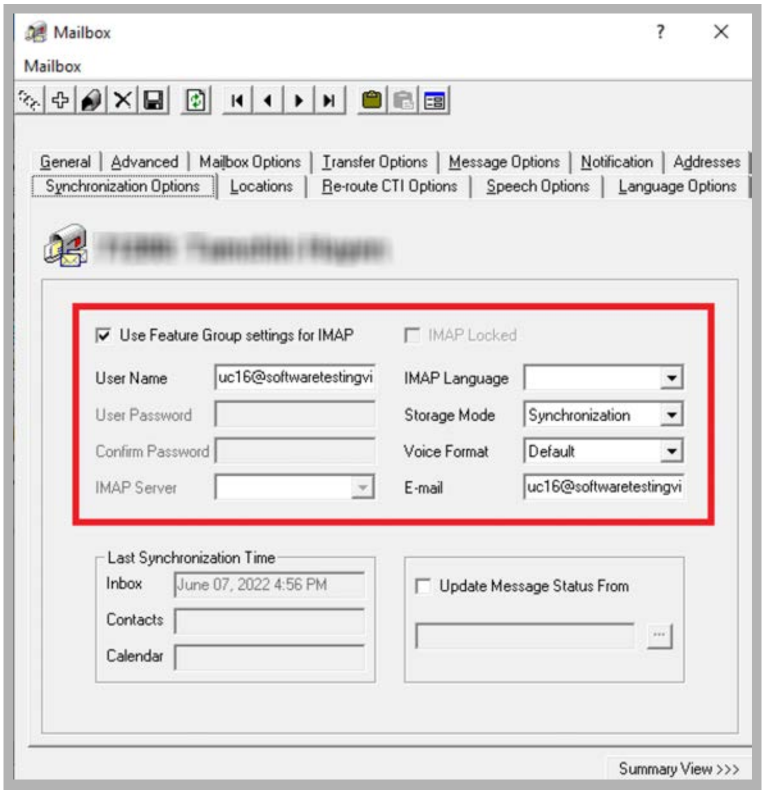


[redacted]

Personal Operator	
Operator Phone Number	
D.I.D Trunk	
□ Customize TUI	
□ Voice Menu	
□ Collect Geo Location Data	
Domain Account Name	uc16@softwaretestingvietnam.cc
Desktop Capabilities	Advanced
Date Format	YYYYMMDD
PBX Node	
Web Access Inactivity Timeout	0

☑ Web Client User

2. On the Synchronization Options tab:
   - Enable Use Feature Group settings for IMAP
   - **User Name**: Enter you Office365 account.
   - **Storage Mode**: Set this to **Synchronization**.
   - **Voice Format**: Choose **Default**.
   - **E-mail**: Enter you Office365 email address.



[redacted]

☑ Use Feature Group settings for IMAP

□ IMAP Locked

User Name: uc16@softwaretestingvi

User Password:

Confirm Password:

IMAP Server:

IMAP Language:

Storage Mode: Synchronization

Voice Format: Default

E-mail: uc16@softwaretestingvi

Last Synchronization Time

Inbox: June 07, 2022 4:56 PM

Contacts:

Calendar:

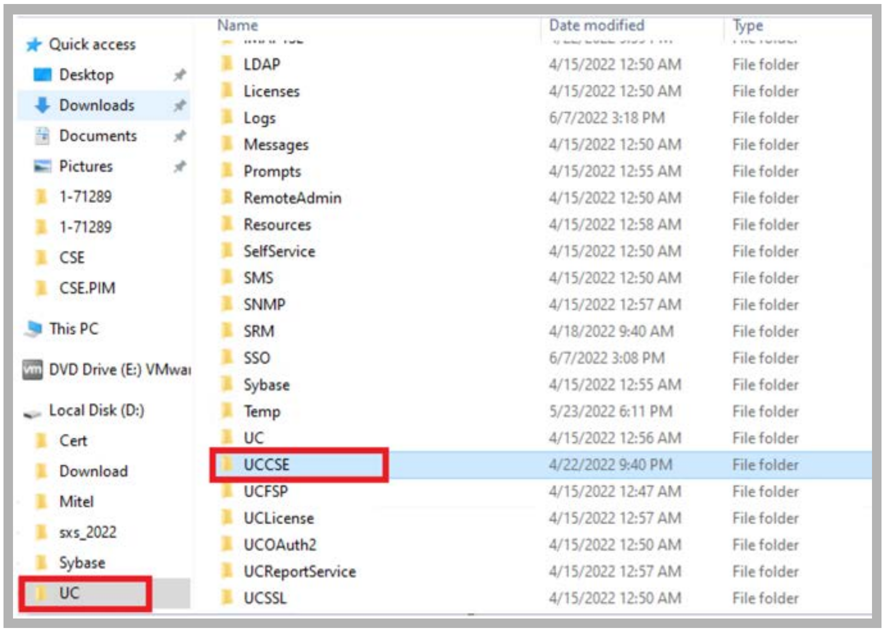
□ Update Message Status From

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.

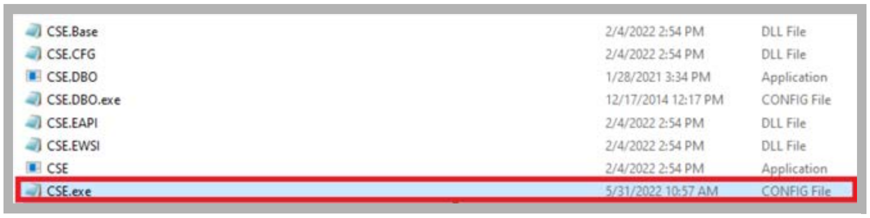
1. Open the **UC/UCCSE** folder on the program installation drive.



Quick access
Desktop
Downloads
Documents
Pictures
1-71289
1-71289
CSE
CSE.PIM
This PC
DVD Drive (E:) VMwa
Local Disk (D:)
Cert
Download
Mitel
sxs_2022
Sybase
UC

Name	Date modified	Type
LDAP	4/15/2022 12:50 AM	File folder
Licenses	4/15/2022 12:50 AM	File folder
Logs	6/7/2022 3:18 PM	File folder
Messages	4/15/2022 12:50 AM	File folder
Prompts	4/15/2022 12:55 AM	File folder
RemoteAdmin	4/15/2022 12:50 AM	File folder
Resources	4/15/2022 12:58 AM	File folder
SelfService	4/15/2022 12:50 AM	File folder
SMS	4/15/2022 12:50 AM	File folder
SNMP	4/15/2022 12:57 AM	File folder
SRM	4/18/2022 9:40 AM	File folder
SSO	6/7/2022 3:08 PM	File folder
Sybase	4/15/2022 12:55 AM	File folder
Temp	5/23/2022 6:11 PM	File folder
UC	4/15/2022 12:56 AM	File folder
UCCSE	4/22/2022 9:40 PM	File folder
UCFSP	4/15/2022 12:47 AM	File folder
UCLicense	4/15/2022 12:57 AM	File folder
UCOAuth2	4/15/2022 12:50 AM	File folder
UCReportService	4/15/2022 12:57 AM	File folder
UCSSL	4/15/2022 12:50 AM	File folder

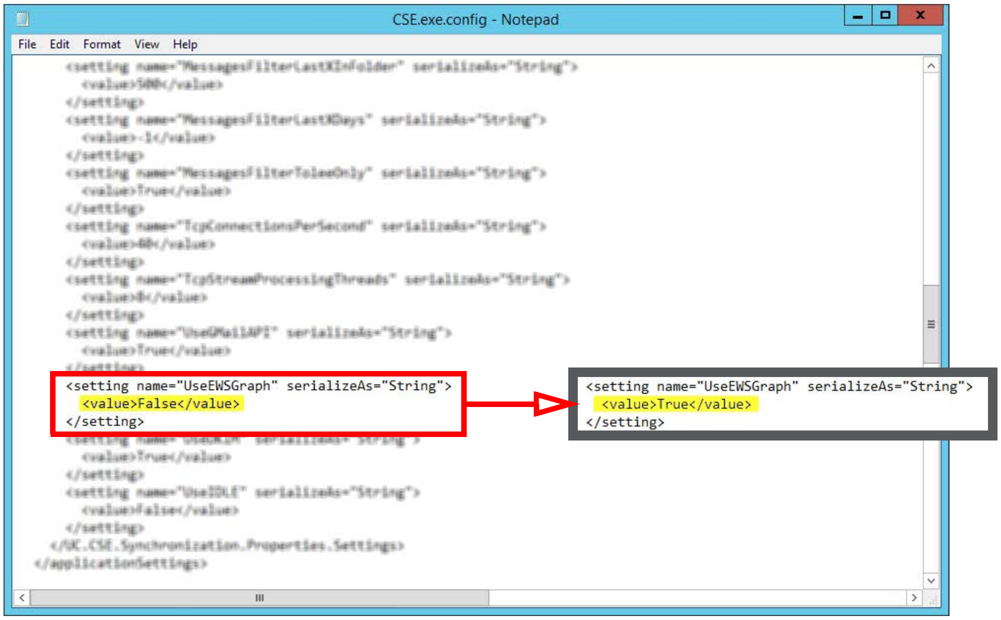
2. Within the folder, open the **CSE.exe.config** file in a text editor such as NotePad.



CSE.Base	2/4/2022 2:54 PM	DLL File
CSE.CFG	2/4/2022 2:54 PM	DLL File
CSE.DBO	1/28/2021 3:34 PM	Application
CSE.DBO.exe	12/17/2014 12:17 PM	CONFIG File
CSE.EAPI	2/4/2022 2:54 PM	DLL File
CSE.EWSI	2/4/2022 2:54 PM	DLL File
CSE	2/4/2022 2:54 PM	Application
CSE.exe	5/31/2022 10:57 AM	CONFIG File

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

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



CSE.exe.config - Notepad

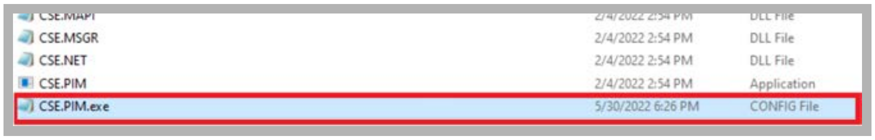
```
    <setting name="MessagesFilterLastXInFolder" serializeAs="String">
      <value>500</value>
    </setting>
    <setting name="MessagesFilterLastXDays" serializeAs="String">
      <value>-1</value>
    </setting>
    <setting name="MessagesFilterToleeOnly" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="TcpConnectionsPerSecond" serializeAs="String">
      <value>60</value>
    </setting>
    <setting name="TcpStreamProcessingThreads" serializeAs="String">
      <value>8</value>
    </setting>
    <setting name="UseGMailAPI" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="UseEWSGraph" serializeAs="String">
      <value>False</value>
    </setting>
    <setting name="UseOAuth" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="UseIDLE" serializeAs="String">
      <value>False</value>
    </setting>
  </UC.CSE.Synchronization.Properties.Settings>
</applicationSettings>
```

```
<setting name="UseEWSGraph" 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.

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

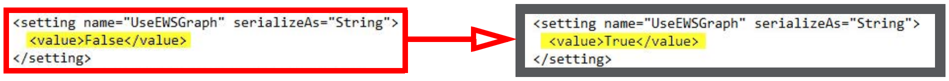
4. Within the UCCSE folder, open the **CSE.PIM.exe.config** file in a text editor such as NotePad.



CSE.MAPI	2/4/2022 2:54 PM	DLL File
CSE.MSGR	2/4/2022 2:54 PM	DLL File
CSE.NET	2/4/2022 2:54 PM	DLL File
CSE.PIM	2/4/2022 2:54 PM	Application
CSE.PIM.exe	5/30/2022 6:26 PM	CONFIG File

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

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



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

```
<setting name="UseEWSGraph" 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.

```
<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.

14 AVAYA MESSAGING TO OFFICE 365 INTEGRATION WITH EWS

In This Chapter:

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 suites your requirements.

CHAPTER	INTEGRATION	WHY YOU WANT IT
9	Google	Creates a secure connection through OAuth2 to your Gmail and Google Apps accounts.
10	Exchange using EWS	The simplest connection between your Exchange server and Avaya Messaging.
11	Exchange without EWS	A connection between Exchange and Avaya Messaging for legacy systems.
12	Exchange 2010	A connection between Exchange 2010 and Avaya Messaging.
13	Office 365 using Graph	Setup the latest high security integration procedures for maximum data integrity.
14	Office 365 using EWS	Quick connection between your O365 server and Avaya Messaging.

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:

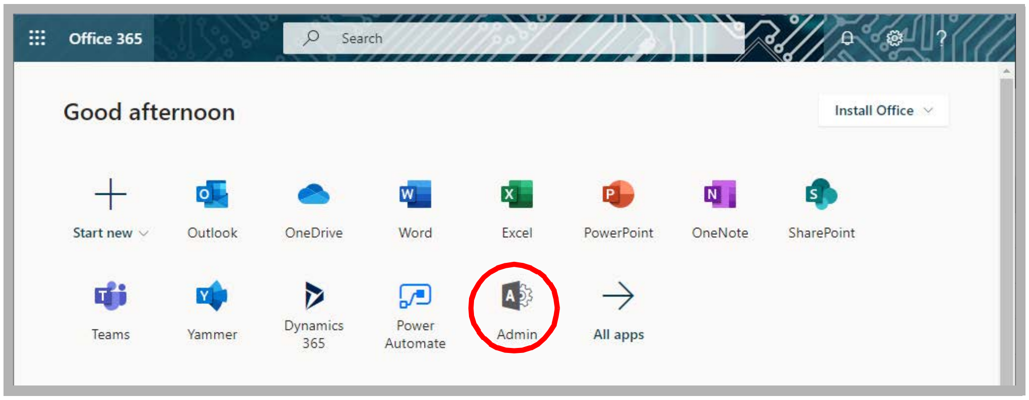
- The Office 365 domain has been setup and deployed (requires Midsize Business and Enterprise plan minimum, E1 or E3).
- Avaya Messaging Server installed and running (refer to Avaya’s documentation web site), either in a single server configuration, or in a High Availability environment (1 Consolidated server, 1 Primary server, 1+ Secondary servers).

Office 365 Configuration

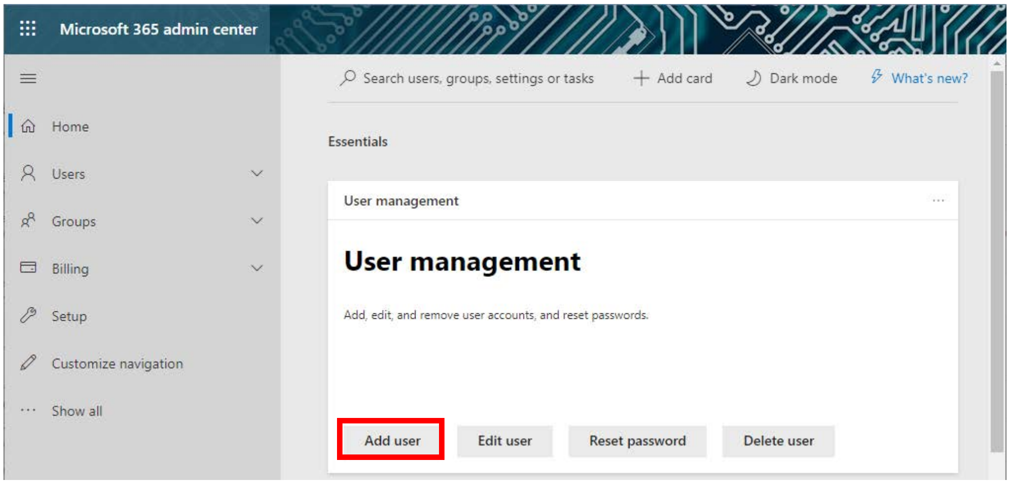
Web Interface Configuration

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**.

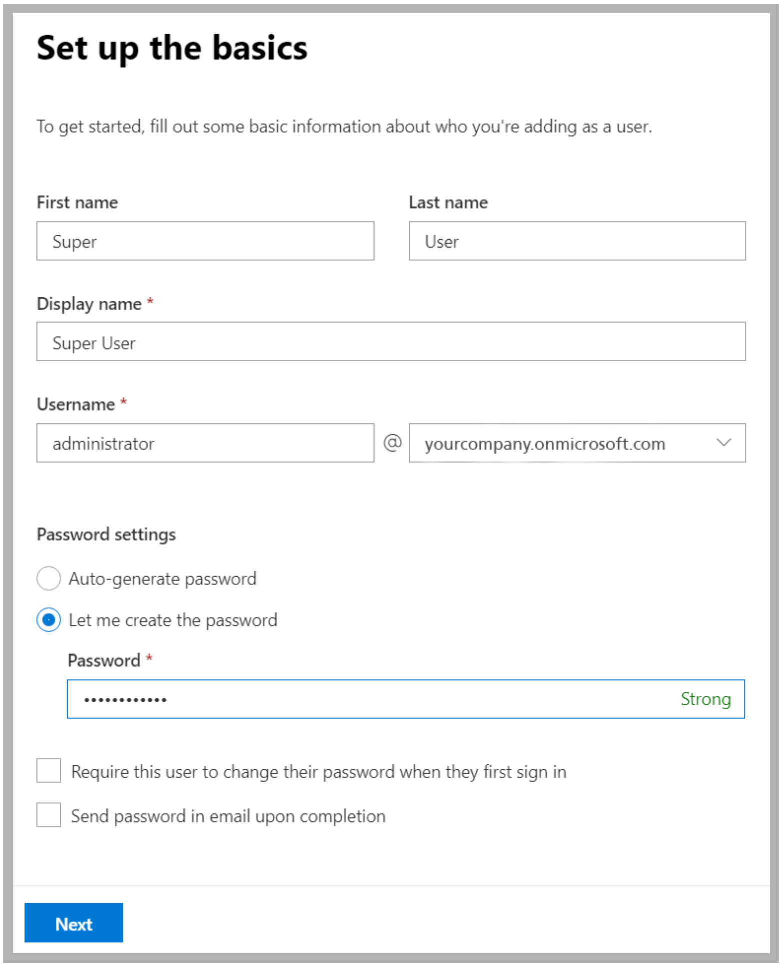


2. Under **User Management**, select **Add User**.



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

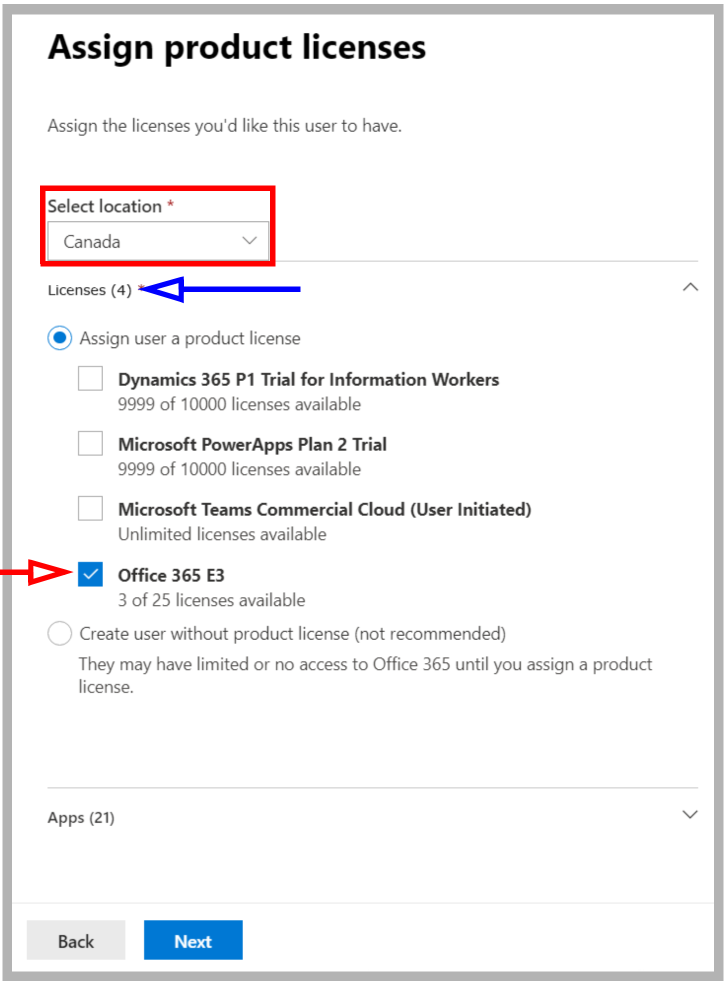
Password *: •••••••••••• Strong

□ Require this user to change their password when they first sign in

□ Send password in email upon completion

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

   When ready, click **Next**.



Assign product licenses

Assign the licenses you'd like this user to have.

Select location *
Canada

Licenses (4) *

● Assign user a product license

□ **Dynamics 365 P1 Trial for Information Workers**
9999 of 10000 licenses available

□ **Microsoft PowerApps Plan 2 Trial**
9999 of 10000 licenses available

□ **Microsoft Teams Commercial Cloud (User Initiated)**
Unlimited licenses available

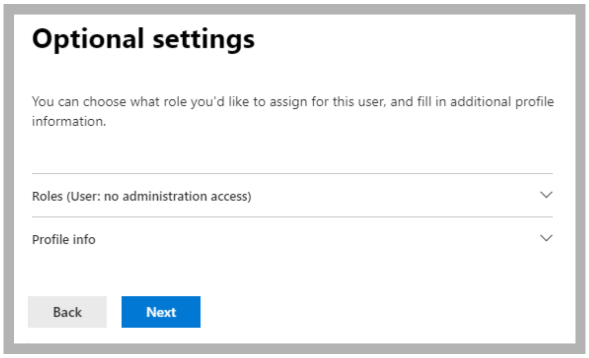
☑ **Office 365 E3**
3 of 25 licenses available

○ Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

Apps (21)

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**.



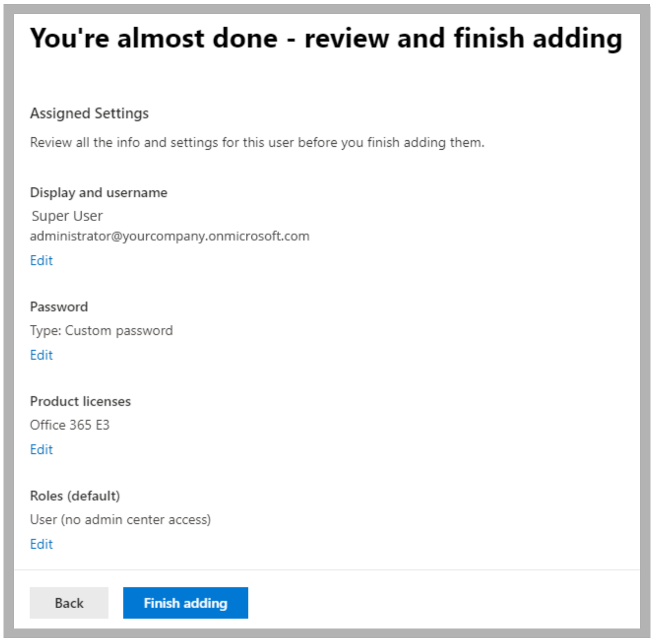
Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles (User: no administration access)

Profile info

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.



You're almost done - review and finish adding

Assigned Settings

Review all the info and settings for this user before you finish adding them.

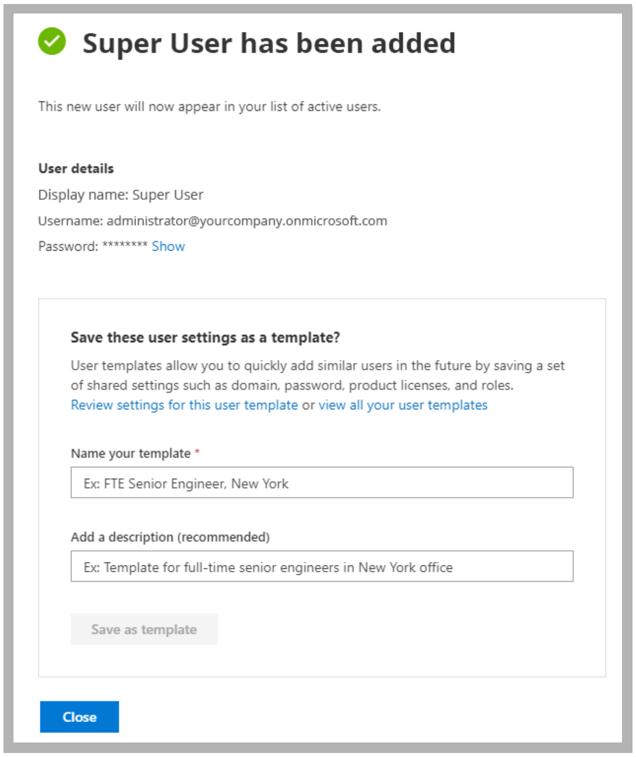
Display and username
Super User
administrator@yourcompany.onmicrosoft.com
Edit

Password
Type: Custom password
Edit

Product licenses
Office 365 E3
Edit

Roles (default)
User (no admin center access)
Edit

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



Super User has been added

This new user will now appear in your list of active users.

User details
Display name: Super User
Username: administrator@yourcompany.onmicrosoft.com
Password: ******** Show

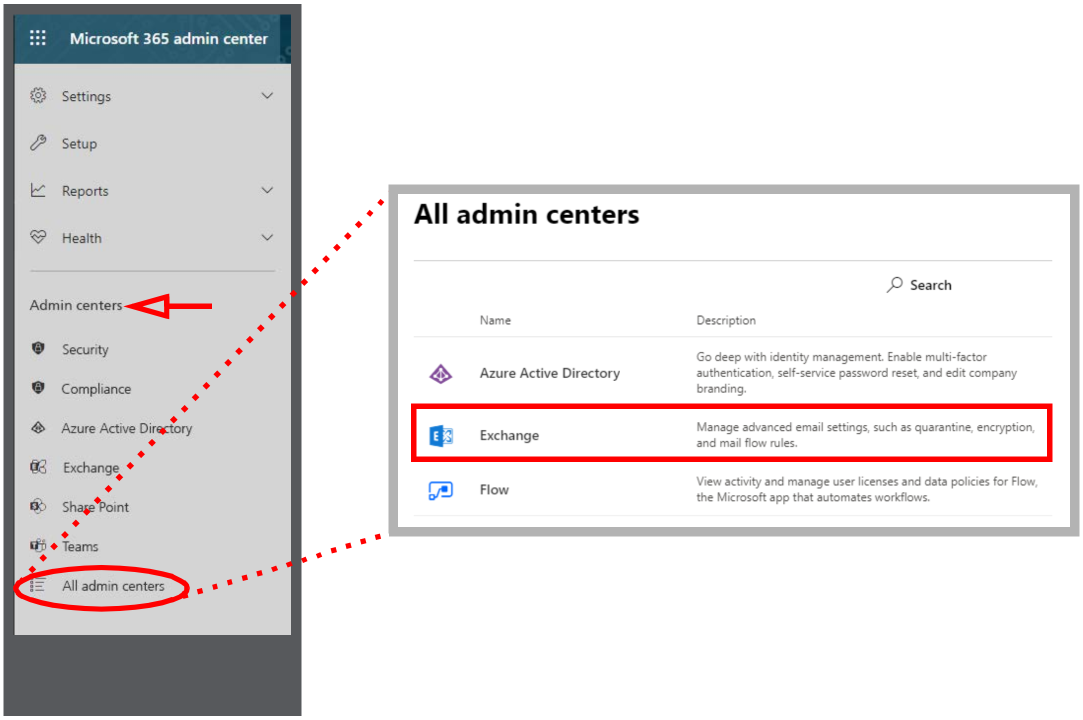
Save these user settings as a template?

User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.
Review settings for this user template or view all your user templates

Name your template *
Ex: FTE Senior Engineer, New York

Add a description (recommended)
Ex: Template for full-time senior engineers in New York office

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

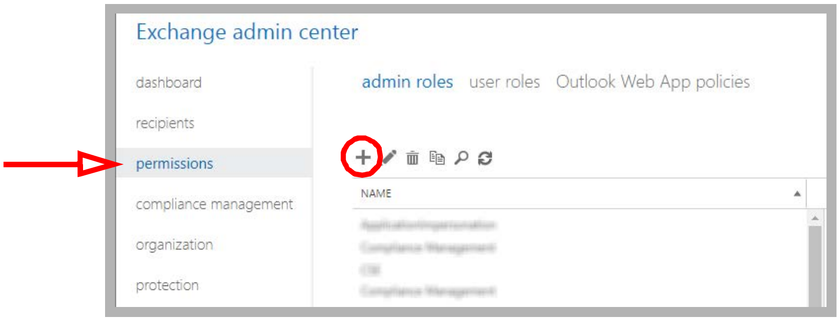


All admin centers

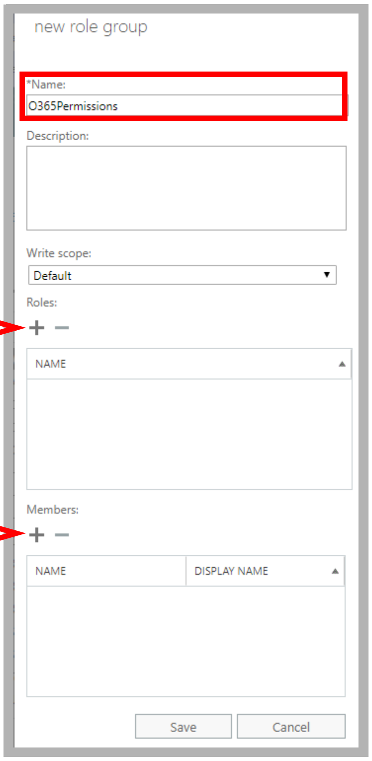
Search

Name	Description
Azure Active Directory	Go deep with identity management. Enable multi-factor authentication, self-service password reset, and edit company branding.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Flow	View activity and manage user licenses and data policies for Flow, the Microsoft app that automates workflows.

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



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



new role group

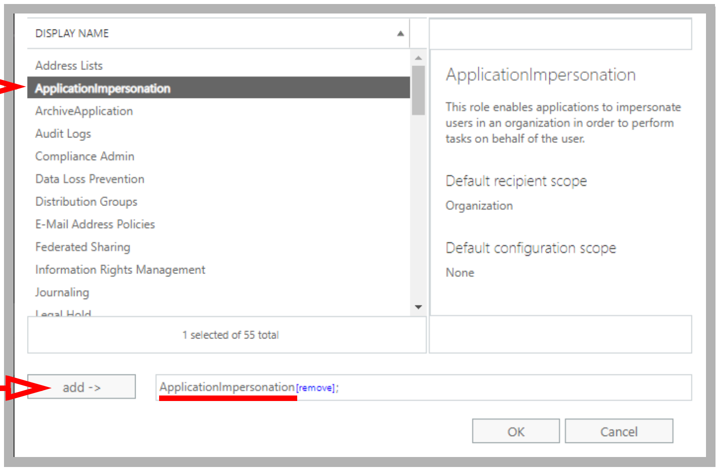
*Name: O365Permissions

Description:

Write scope: Default

Roles:

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



DISPLAY NAME

Address Lists
ApplicationImpersonation
ArchiveApplication
Audit Logs
Compliance Admin
Data Loss Prevention
Distribution Groups
E-Mail Address Policies
Federated Sharing
Information Rights Management
Journaling
Legal Hold

1 selected of 55 total

ApplicationImpersonation

This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.

Default recipient scope

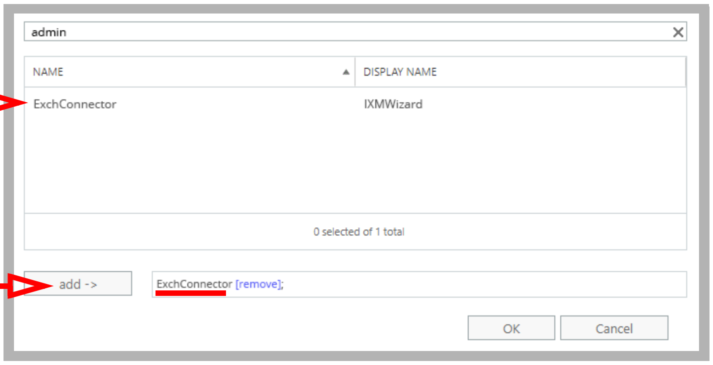
Organization

Default configuration scope

None

ApplicationImpersonation [remove];

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



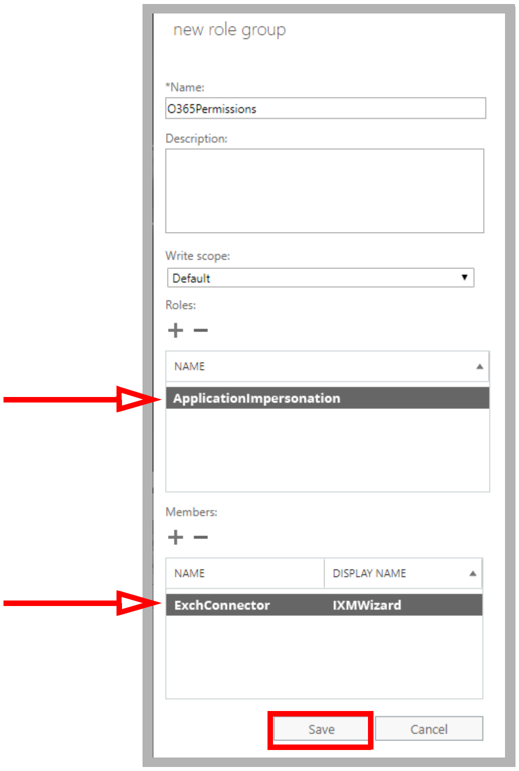
admin

NAME	DISPLAY NAME
ExchConnector	IXMWizard

0 selected of 1 total

ExchConnector [remove];

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



new role group

*Name: O365Permissions

Description:

Write scope: Default

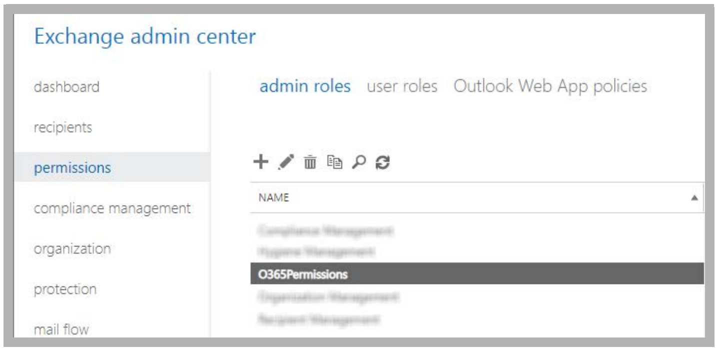
Roles:

NAME
ApplicationImpersonation

Members:

NAME	DISPLAY NAME
ExchConnector	IXMWizard

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



Exchange admin center

NAME
Compliance Management
Hygiene Management
O365Permissions
Organization Management
Recipient Management

The new account has been created.

Avaya Avaya Messaging Server

Server Configuration

1. In Avaya Messaging Admin, add a new TSE IMAP server, and include the Office 365 server information.

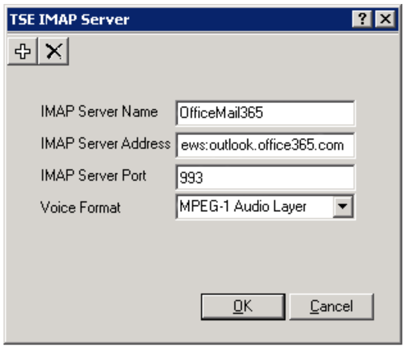
   IMAP Server Name: Enter a name for this connection (e.g. **OfficeMail365**).

   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.



IMAP Server Name: OfficeMail365
IMAP Server Address: ews:outlook.office365.com
IMAP Server Port: 993
Voice Format: MPEG-1 Audio Layer

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:

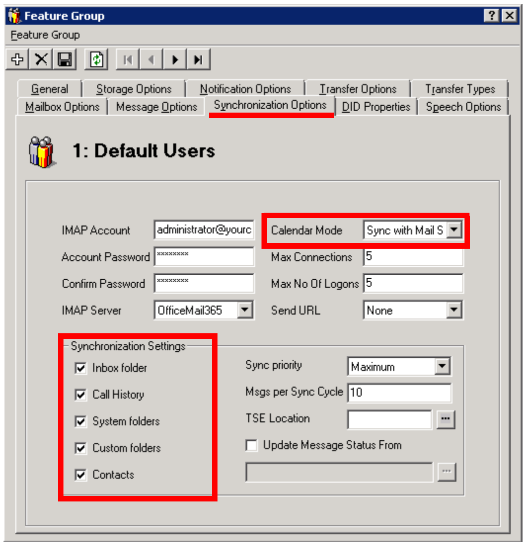
   IMAP Account: Enter the user/service account created in step 3 above. Include the complete user@domain.com (e.g. **administrator@yourcompany.onmicrosoft.com**).

   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.



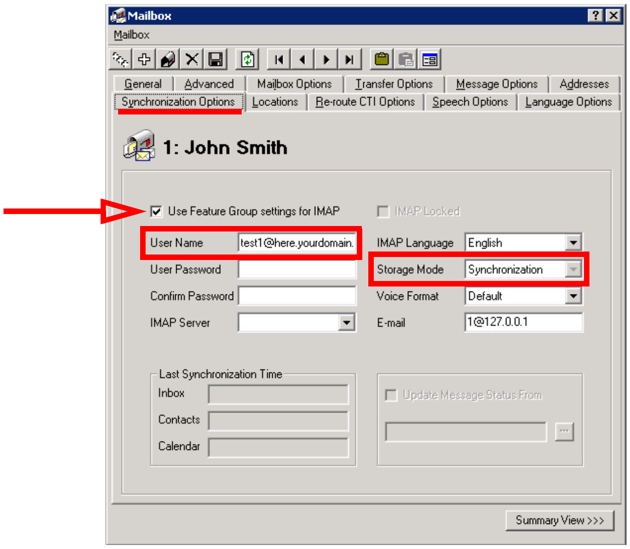
1: Default Users

IMAP Account: administrator@yourc
Account Password: ********
Confirm Password: ********
IMAP Server: OfficeMail365
Calendar Mode: Sync with Mail S
Max Connections: 5
Max No Of Logons: 5
Send URL: None

Synchronization Settings
☑ Inbox folder
☑ Call History
☑ System folders
☑ Custom folders
☑ Contacts

Sync priority: Maximum
Msgs per Sync Cycle: 10
TSE Location:
☐ Update Message Status From

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**.



1: John Smith

☑ Use Feature Group settings for IMAP

□ IMAP Locked

User Name: test1@here.yourdomain.

User Password:

Confirm Password:

IMAP Server:

IMAP Language: English

Storage Mode: Synchronization

Voice Format: Default

E-mail: 1@127.0.0.1

Last Synchronization Time

Inbox:

Contacts:

Calendar:

□ Update Message Status From

Connecting Through EWS Using OAuth 2.0

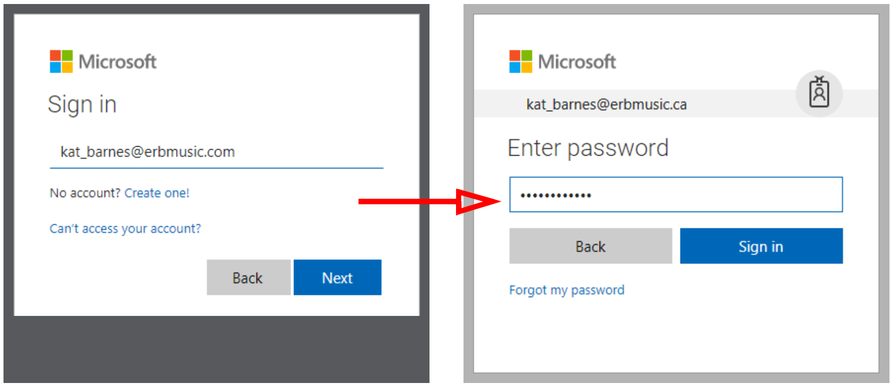
As an option, Avaya Messaging can be connected to Office 365 using Exchange Web Services. This can add an additional layer of security to your communication traffic flows. This section is not required.

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

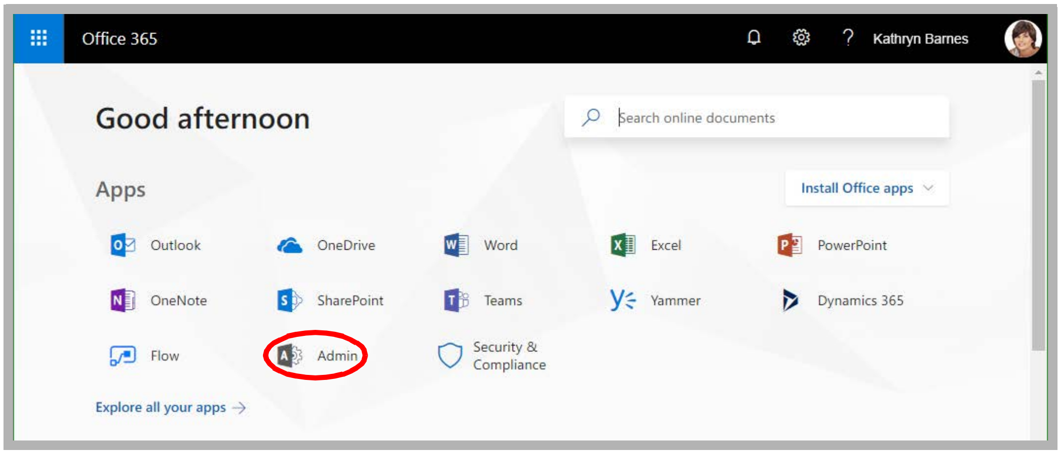
Note: You must have corporate Office 365 and EWS accounts for this configuration.

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

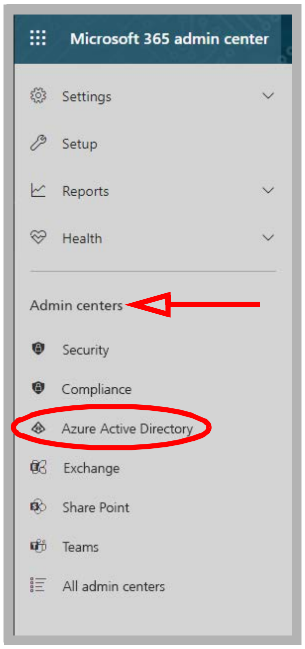
1. Open a web browser and go to the Office 365 site at https://www.office.com.
   Click **Sign in** and login using your Office 365 administrator account credentials.



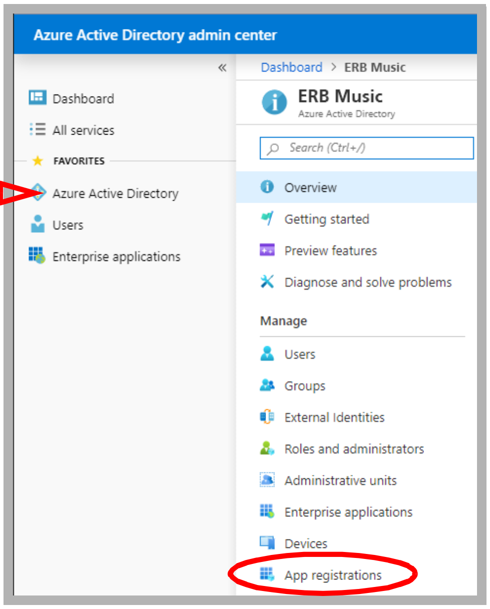
2. Click **Admin**.



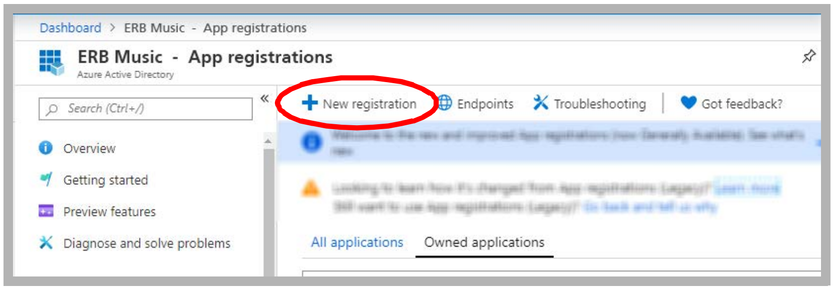
3. In the left-hand panel, open **Admin centers** (Show all) and select **Azure Active Directory**. The Azure dashboard will appear.



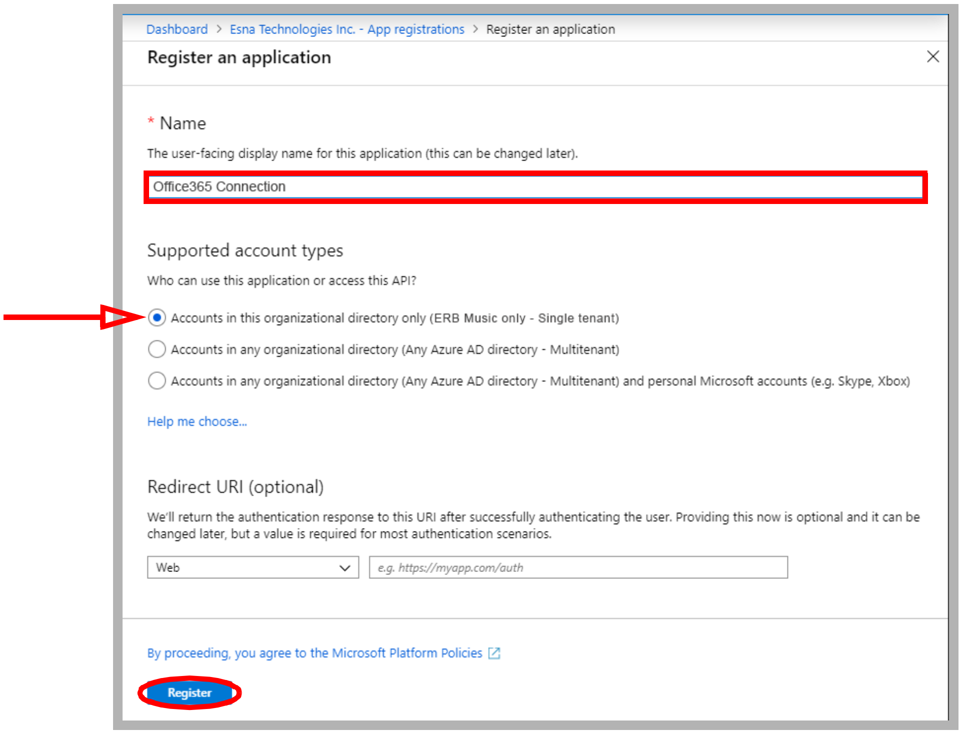
4. Click **Azure Active Directory > App registrations**.



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**.



Dashboard > Esna Technologies Inc. - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Office365 Connection

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (ERB Music only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

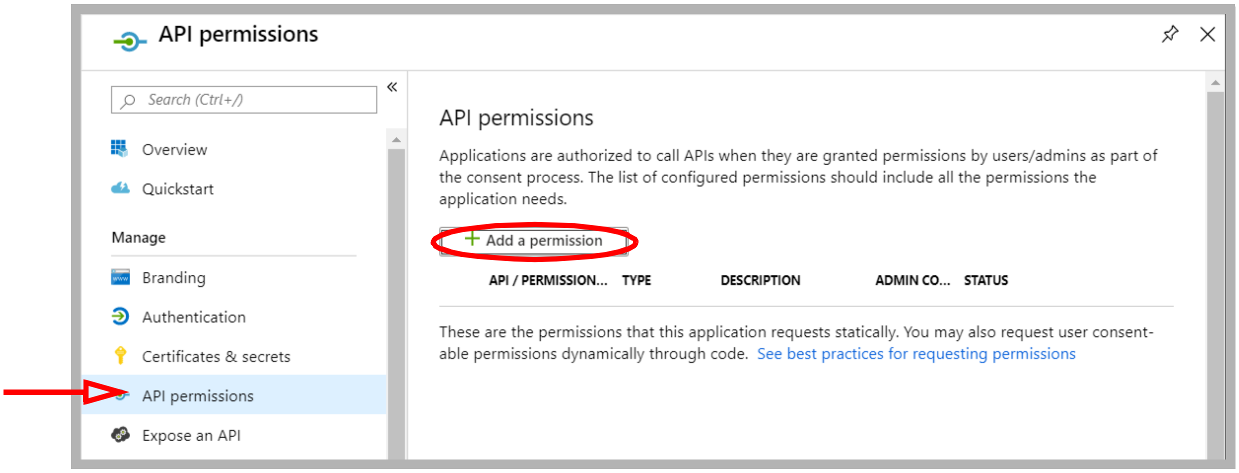
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

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



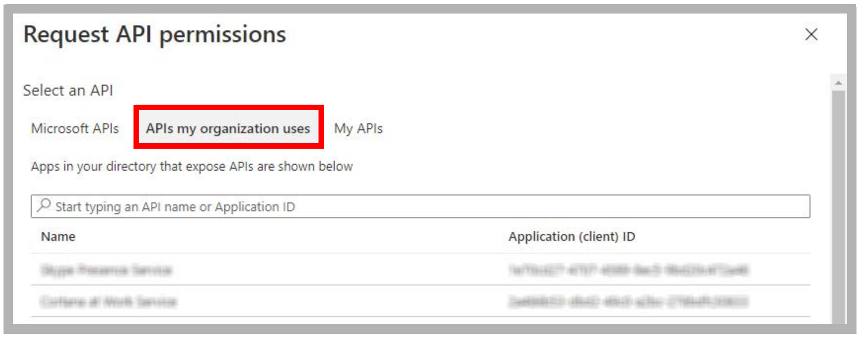
API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

API / PERMISSION...	TYPE	DESCRIPTION	ADMIN CO...	STATUS

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

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



Request API permissions

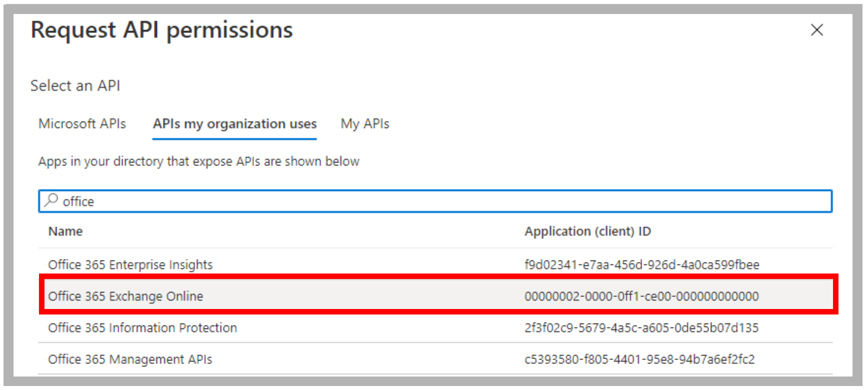
Select an API

Apps in your directory that expose APIs are shown below

Start typing an API name or Application ID

Name	Application (client) ID
[redacted]	[redacted]
[redacted]	[redacted]

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



Request API permissions

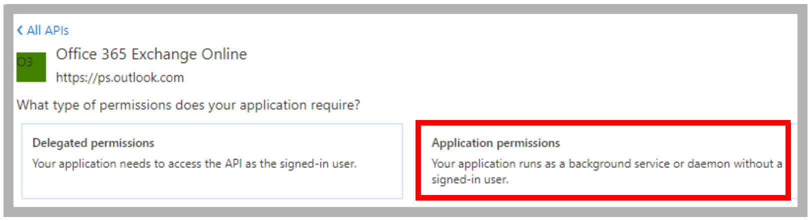
Select an API

Apps in your directory that expose APIs are shown below

office

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2

10. Click **Application permissions**.



< All APIs

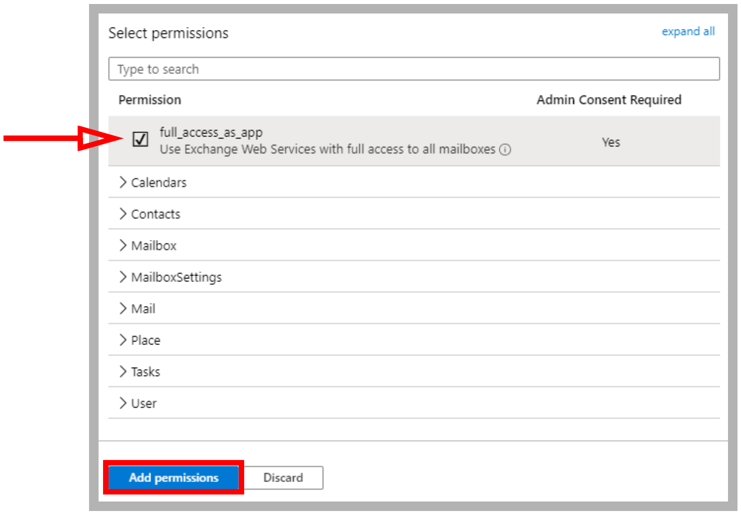
Office 365 Exchange Online
https://ps.outlook.com

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

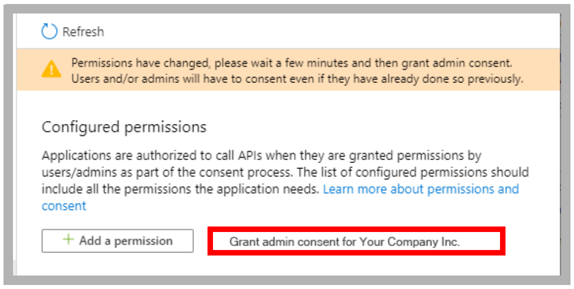
11. Enable **full_access_as_app**. Click **Add permissions**.



Select permissions

Permission	Admin Consent Required
☑ full_access_as_app Use Exchange Web Services with full access to all mailboxes ⓘ	Yes
> Calendars	
> Contacts	
> Mailbox	
> MailboxSettings	
> Mail	
> Place	
> Tasks	
> User	

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

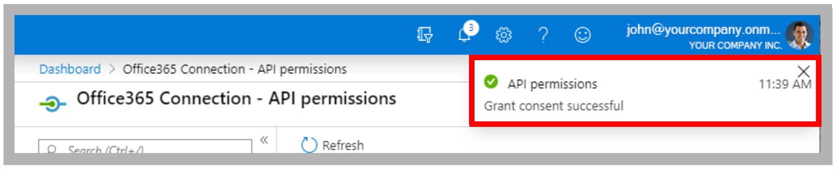


Permissions have changed, please wait a few minutes and then grant admin consent. Users and/or admins will have to consent even if they have already done so previously.

Configured permissions

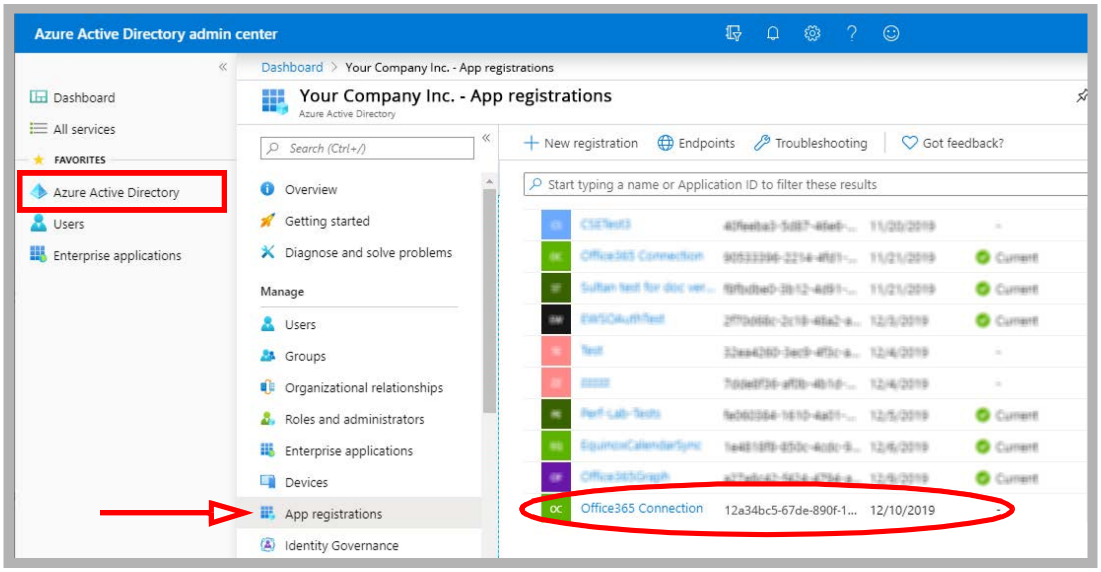
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

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

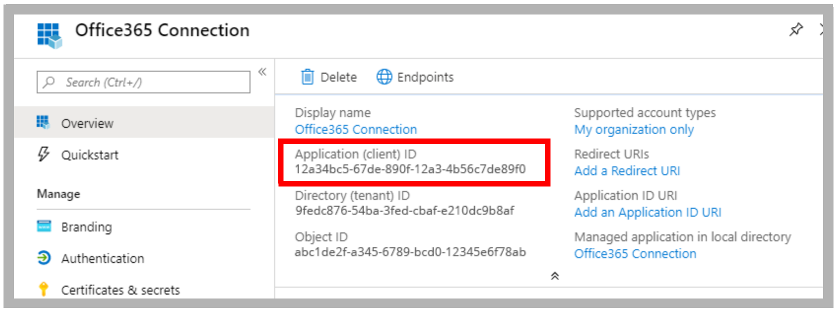

john@yourcompany.onm...
YOUR COMPANY INC.
Dashboard > Office365 Connection - API permissions
Office365 Connection - API permissions
Search (Ctrl+/)
Refresh

API permissions 11:39 AM
Grant consent successful

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



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



Display name
Office365 Connection

Application (client) ID
12a34bc5-67de-890f-12a3-4b56c7de89f0

Directory (tenant) ID
9fedc876-54ba-3fed-cbaf-e210dc9b8af

Object ID
abc1de2f-a345-6789-bcd0-12345e6f78ab

Supported account types
My organization only

Redirect URIs
Add a Redirect URI

Application ID URI
Add an Application ID URI

Managed application in local directory
Office365 Connection

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.

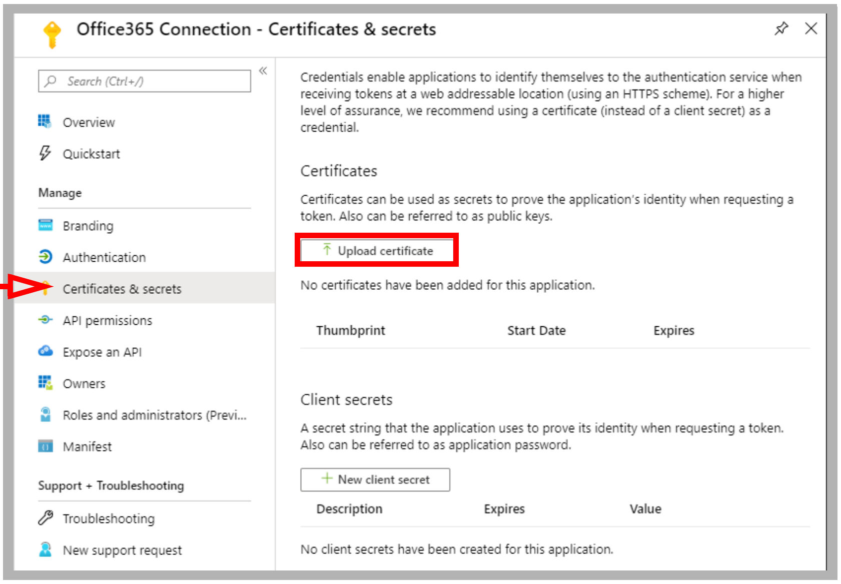
For example: **0a987b654cd32.pfx ----> 12a34bc5-67de-890f-12a3-4b56c7de89f0.p12**

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**.



Office365 Connection - Certificates & secrets

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

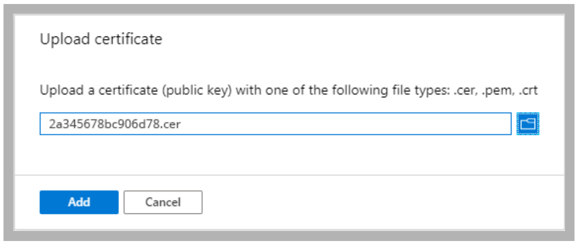
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

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



Upload certificate

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt

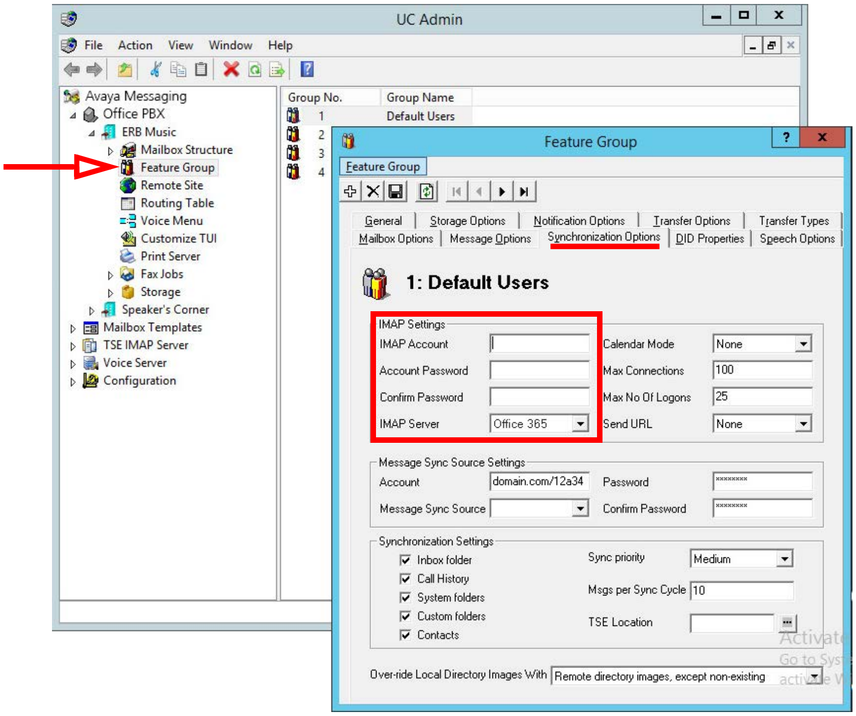
2a345678bc906d78.cer

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.



Group No.	Group Name
1	Default Users
2	
3	
4	

1: Default Users

IMAP Settings

IMAP Account		Calendar Mode	None
Account Password		Max Connections	100
Confirm Password		Max No Of Logons	25
IMAP Server	Office 365	Send URL	None

Message Sync Source Settings

Account	domain.com/12a34	Password	********
Message Sync Source		Confirm Password	********

Synchronization Settings

☑ Inbox folder
☑ Call History
☑ System folders
☑ Custom folders
☑ Contacts

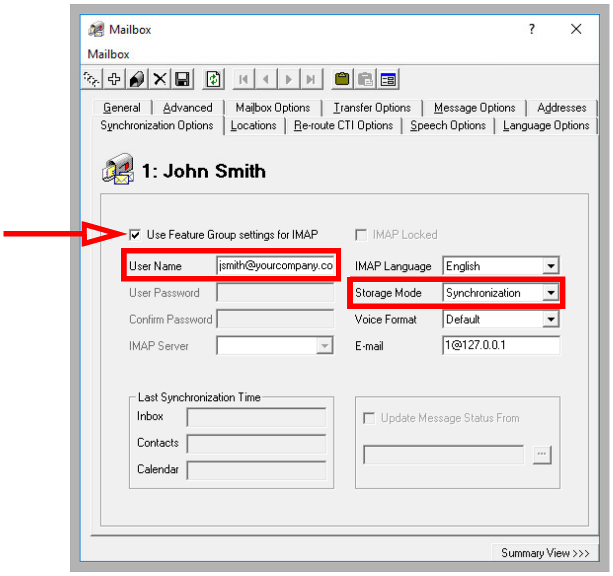
Sync priority	Medium
Msgs per Sync Cycle	10
TSE Location	

Over-ride Local Directory Images With: Remote directory images, except non-existing

When ready, 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.

    Enable **Use Feature Group settings for IMAP**.
    Type in the **User Name** for this account.
    For **Storage Mode**, select **Synchronization**.



1: John Smith

☑ Use Feature Group settings for IMAP
□ IMAP Locked

User Name	jsmith@yourcompany.co	IMAP Language	English
User Password		Storage Mode	Synchronization
Confirm Password		Voice Format	Default
IMAP Server		E-mail	1@127.0.0.1

Last Synchronization Time
Inbox
Contacts
Calendar

□ Update Message Status From

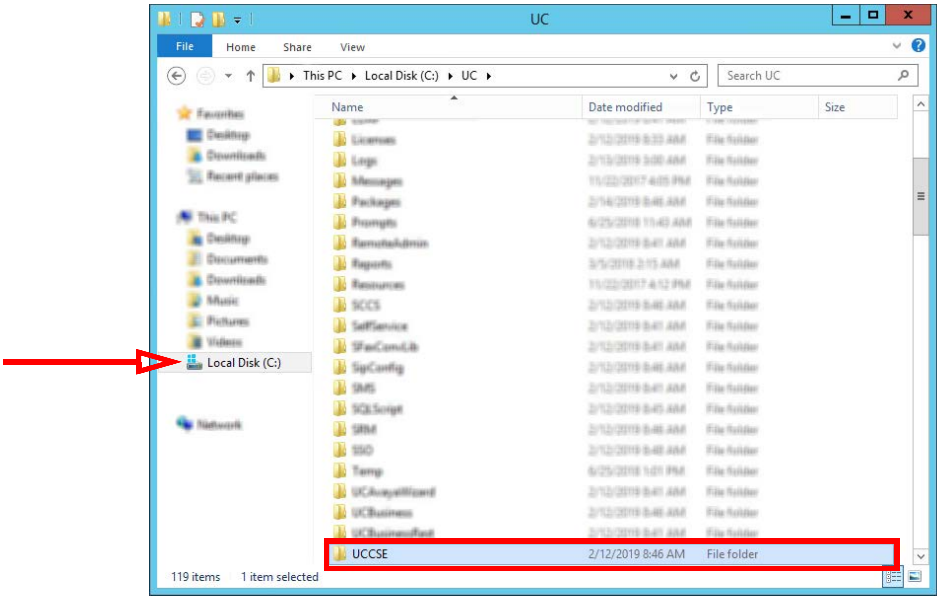
When ready, click **Save**.

The configuration is complete.

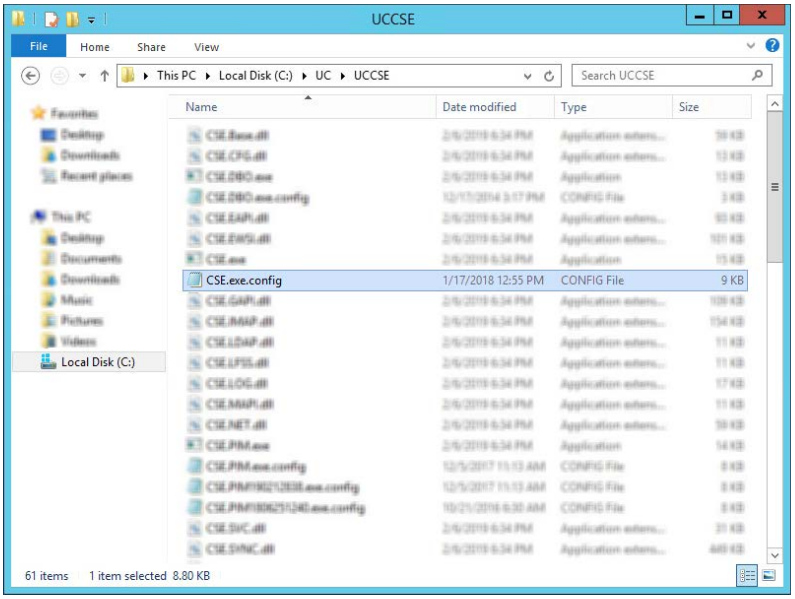
Verify Configuration Setting

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.

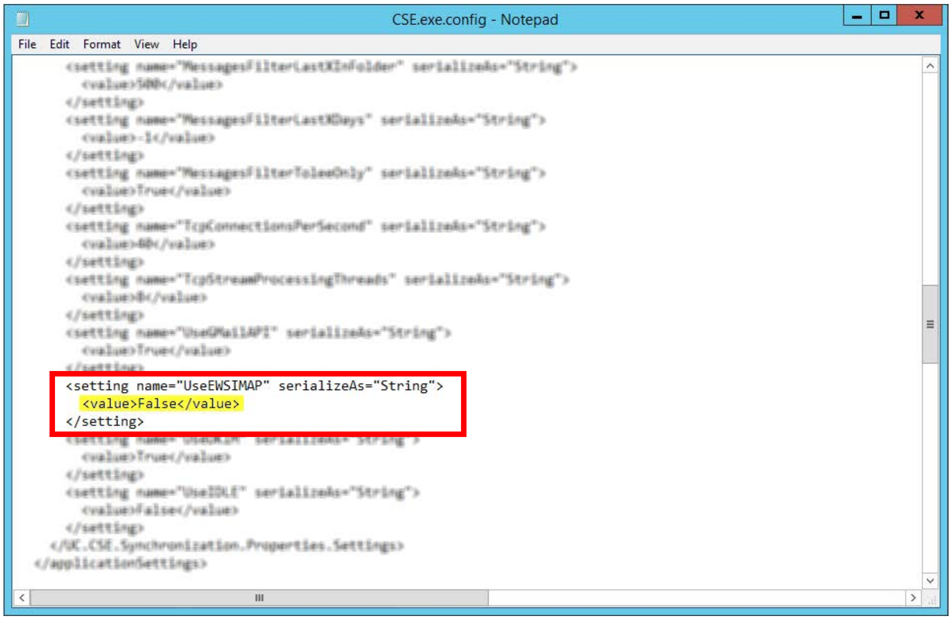


2. Within the folder, open the CSE.exe.config file in a text editor such as NotePad.



3. Scroll down to find the following lines:

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



```
    <setting name="MessagesFilterLastXInFolder" serializeAs="String">
      <value>500</value>
    </setting>
    <setting name="MessagesFilterLastXDays" serializeAs="String">
      <value>-1</value>
    </setting>
    <setting name="MessagesFilterToleeOnly" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="TcpConnectionsPerSecond" serializeAs="String">
      <value>60</value>
    </setting>
    <setting name="TcpStreamProcessingThreads" serializeAs="String">
      <value>8</value>
    </setting>
    <setting name="UseGMailAPI" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="UseEWSIMAP" serializeAs="String">
      <value>False</value>
    </setting>
    <setting name="UseOKIM" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="UseIDLE" serializeAs="String">
      <value>False</value>
    </setting>
  </UC.CSE.Synchronization.Properties.Settings>
</applicationSettings>
```

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.

15 IBM DOMINO INTEGRATION

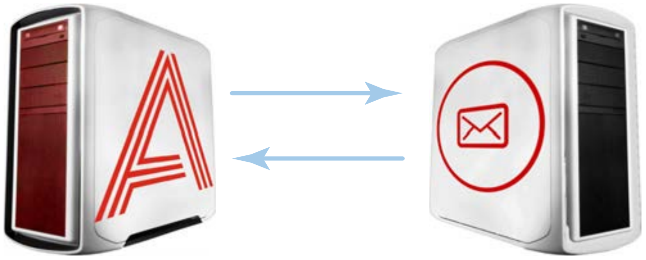
In This Chapter:

Introduction

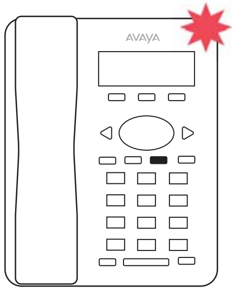
Avaya Messaging and a IBM Domino server are able to integrate through the IMAPCSE services, providing a truly unified messaging experience. Once the configuration is complete the servers communicate and synchronize all data among themselves, eliminating the need for you to constantly manage multiple locations.

The use of the administrator account from IBM Domino allows you to streamline the sign on process while still maintaining individual password security protocols on each mailbox. The Domino administrator account credentials are entered through the Avaya Messaging Admin console.

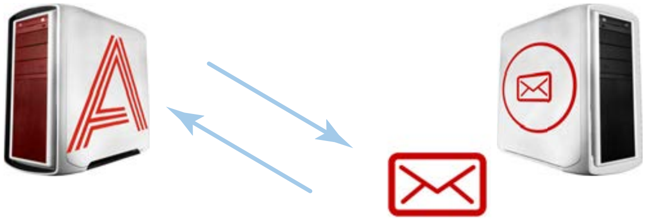
Visual Guide



Data is synchronized between the UC Server and the Mail Server. Message status and deletions are synchronized almost instantly between the two, creating a single message store for easier management by both the administrators and end users.



Since status is synchronized, message lights on integrated telephone systems will also be accurate no matter where the message is read or received.



In a typical situation, voice messages will be synchronized from the Voice Server to the eMail Server, and email messages will be synchronized from the eMail Server to the Voice Server.

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 will be 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	Officelinx/IX Messaging version 8.5 - 10.9 Avaya Messaging version 11.0 or higher

Server Configuration

IBM Domino configuration is largely divided into two parts. First is the configuration of both the Domino server and the Avaya Messaging server to synchronize messages between the mailboxes on both systems. Second is configuring UC forms for IBM Notes so that end users will have the ability to record and playback voice messages from their IBM Notes client. While specific variables regarding settings will differ from site to site, this guide provides a general guideline for integrating IBM Domino with Avaya Messaging.

Setting up IMAP CSE Synchronization

To configure IBM Notes for Avaya Messaging users:

1. Access the IBM Notes Administrator.
2. Under the Domain/People directory, double click **User** and enter a nickname, a user name and an Internet password.
3. On the IBM Domino Console, run the following command:
   Load Convert –m mail\username.nsf * ucmail.ntf.

Note: In the above command, **username** is the IBM mail file, and **ucmail.ntf** is the template into which the forms were installed.

Note: Once the forms have been installed and distributed to the users, their inbox will need to be closed and reopened in order for the templates to be refreshed. This needs to be done every time the Master Template is updated.

The following procedure is optional.

To prevent the IBM Window from scrolling while logging in / out in IMAP:

1. On the IBM Notes Server, open the **notes.ini** file.
2. Set the Log_Session=1 to **0**.
3. Click **Save**, then click **Close**.

Avaya Messaging Configuration: Single User

Note: Configuring Avaya Messaging for use with Superuser credentials is no longer supported.

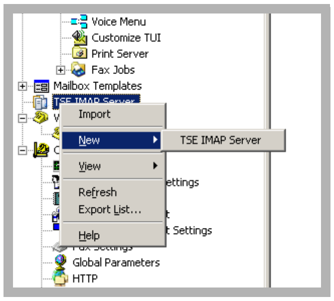
With this option, Avaya Messaging connects to the IBM Domino server on a mailbox-by-mailbox basis, using each individual client's account credentials for each connection.

It is necessary to establish IMAP CSE connections ***before*** setting up Unified Messaging.

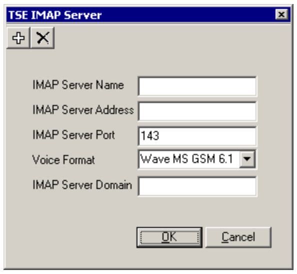
To begin the setup of your unified messaging you need to create a CSE IMAP connection. The purpose of this connection is to tell the voicemail what IP address it is supposed to connect to in order to connect to your IBM Domino server.

To create CSE IMAP connections

1. Login to Avaya Messaging Admin. The following screen appears.



2. Locate **TSE IMAP Server** in the left-hand pane. Right-click and select **New > TSE IMAP Server**. The following screen appears.
3. Complete the following fields:
   - In the **IMAP Server Name** text field, enter a descriptive name of the server.
   - In the **IMAP Server Address** text field, enter the Domino server's IP address.



IMAP Server Name

IMAP Server Address

IMAP Server Port: 143

Voice Format: Wave MS GSM 6.1

IMAP Server Domain

Note: If you are using an **SSL** connection, you should use the **server's domain name (DNS)** instead of the IP address so that the certificate can be authenticated properly. SSL connections should **always use port 993**.

   - Accept the default value in the **IMAP Server Port** field or enter the server port field provided to you by your network Admin.
   - Select the **Voice Format** that your servers will use to handle voice messages.
   - In the **IMAP Server Domain** field, enter the domain name of the mail server to avoid looping messages during synchronization. This server address will be cross referenced with the Reply To address of each mailbox.

Note: **CSE** was formerly known as **TSE**.

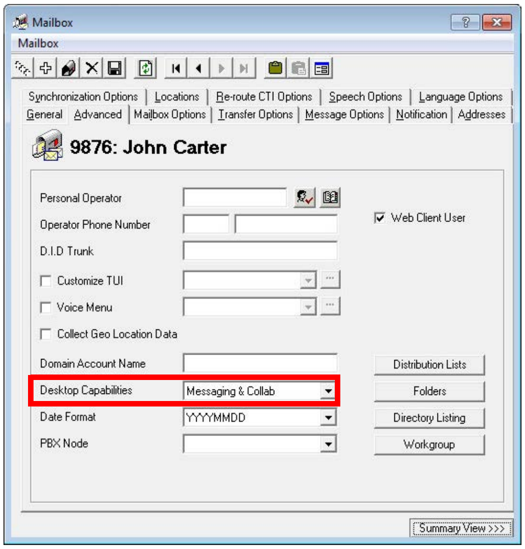
Setting Up Unified Messaging (UM)

Mailbox integration is a configuration where each individual user on your Domino server is given their own mailbox on the Avaya Messaging system.

1. Obtain the list of the users you are going to integrate.

Hint: Contact your system administrator to verify that the usernames and passwords are correct before proceeding.

2. On the voice server machine, open Avaya Messaging Admin.
3. Open the **Mailbox** properties.
4. On the **Addresses** tab, verify that the **Reply To** email address is the address of the user's IBM Domino account. Click **Save**.
5. Click on the **Advanced** tab.
6. From the **Desktop Capabilities** dropdown list, select **Messaging & Collab**.
7. Click the **Save Mailbox** toolbar button.



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

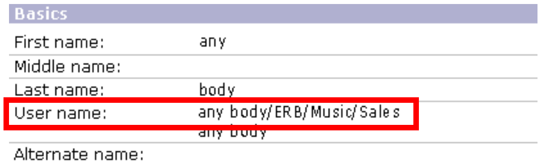
Warning: The following steps must be completed in the specified order.

8. Click on the **Synchronization Options** tab.
9. In the **User Name** field, enter the details of the user's IBM Domino email account. Change all forward slashes / to pipes |, such as:

Firstname Lastname|Organizationname

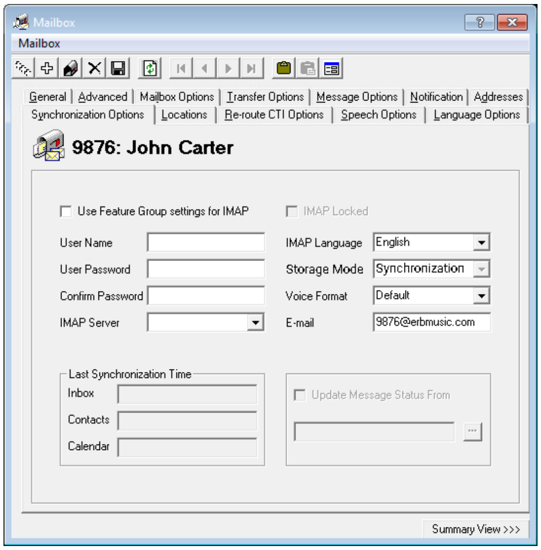
Note: Organizationname may include the domain and other information. Separate all fields by a pipe instead of a slash.

any body|ERB|Music|Sales



Basics

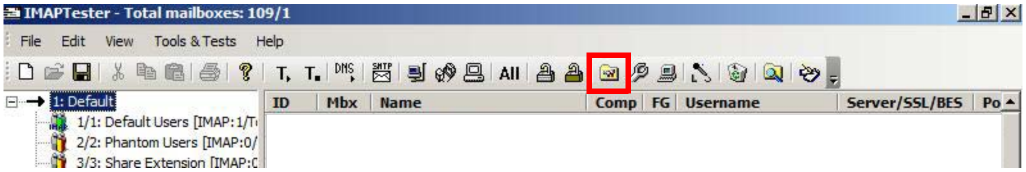
First name: any
Middle name:
Last name: body
User name: any body/ERB/Music/Sales
any body
Alternate name:



9876: John Carter

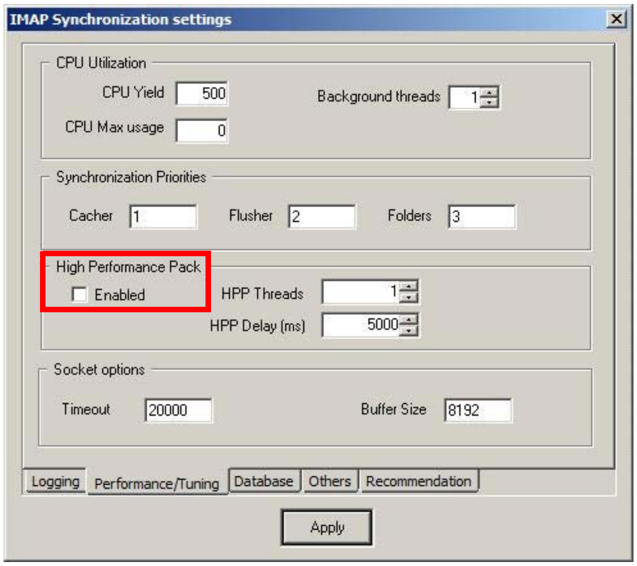
□ Use Feature Group settings for IMAP
□ IMAP Locked
User Name
User Password
Confirm Password
IMAP Server
IMAP Language: English
Storage Mode: Synchronization
Voice Format: Default
E-mail: 9876@erbmusic.com
Last Synchronization Time
Inbox
Contacts
Calendar
□ Update Message Status From

10. From the **Storage Mode** dropdown list, select **IMAP**.
11. Enter the mailbox Internet password in the **User Password** and **Confirm Password** fields.
12. For **IMAP Server**, select the Domino server.
13. Disable the **Use Feature Group setting for IMAP** checkbox.
14. In the **IMAP Language** field, choose the language of the mailbox. You **must** make a choice in this field.
15. Do not use the Message Status feature. Make sure that the **Update Message Status From** checkbox is **not** checked.
16. Click on the **Save Mailbox** toolbar button.
17. On the voice server machine, open IMAP Tester.



1: Default
1/1: Default Users [IMAP:1/T
2/2: Phantom Users [IMAP:0/
3/3: Share Extension [IMAP:C

18. Click on **IMAP Synchronization Settings.**
19. Click on the **Performance/Tuning** tab.
20. Disable the **High Performance Pack** checkbox.
21. Click **Apply** to save the changes. Exit the utility.
22. Restart the UC TSE Cache Manager service.



IMAP Synchronization settings

CPU Utilization
CPU Yield 500
Background threads 1
CPU Max usage 0

Synchronization Priorities
Cacher 1
Flusher 2
Folders 3

High Performance Pack
□ Enabled
HPP Threads 1
HPP Delay (ms) 5000

Socket options
Timeout 20000
Buffer Size 8192

Installing UC Forms for IBM Notes

This section describes the installation and configuration of UC forms for IBM clients. UC forms components are packaged in the **UCMail.ntf** IBM template database, which can be found on the installation DVD. The UCMail template contains the following:

- **UC Player** subform that can be used to extend other forms with an audio player/recorder.
- A subform to indicate the location of iLink Pro Desktop installation file.
- Modified versions of **Memo**, **Reply**, and **Reply with History** forms with UC Player subform added to each.

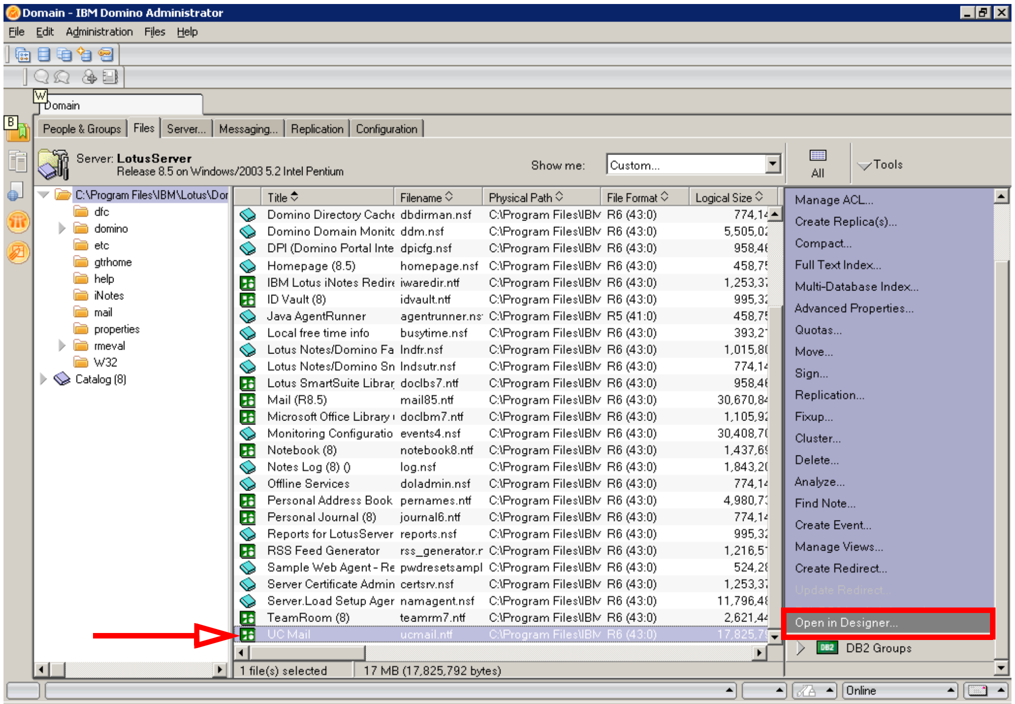
There are two methods for installing UC forms onto the server:

- **A** - Use a provided template as the basis for all UC users.
- **B** - Copy design elements from a provided templates into another, and modify standard forms to include the UC Player subform. This method allows you to add UC player to existing custom templates.

Regardless of which method is used, the design is made available to the IBM Notes client through a manual design refresh initiated by the client, or by running the designer task on the server. Once the design elements are propagated to the target database, each user is provided with an install button within IBM Notes that allows the installation of binary components on the client PC.

Using the Provided Template as Design (Method A)

1. Insert the Avaya Messaging Installation DVD.
2. Copy the **ucmail.ntf** from the DVD (located inside IBM folder) and paste it into the Domino Data folder (e.g. **C:\Program Files\IBM\IBM\Domino\Data**).
3. When you open Domino Administrator, you will notice UC Mail in the list of available templates. Select the template then open it in the **Domino Designer**.

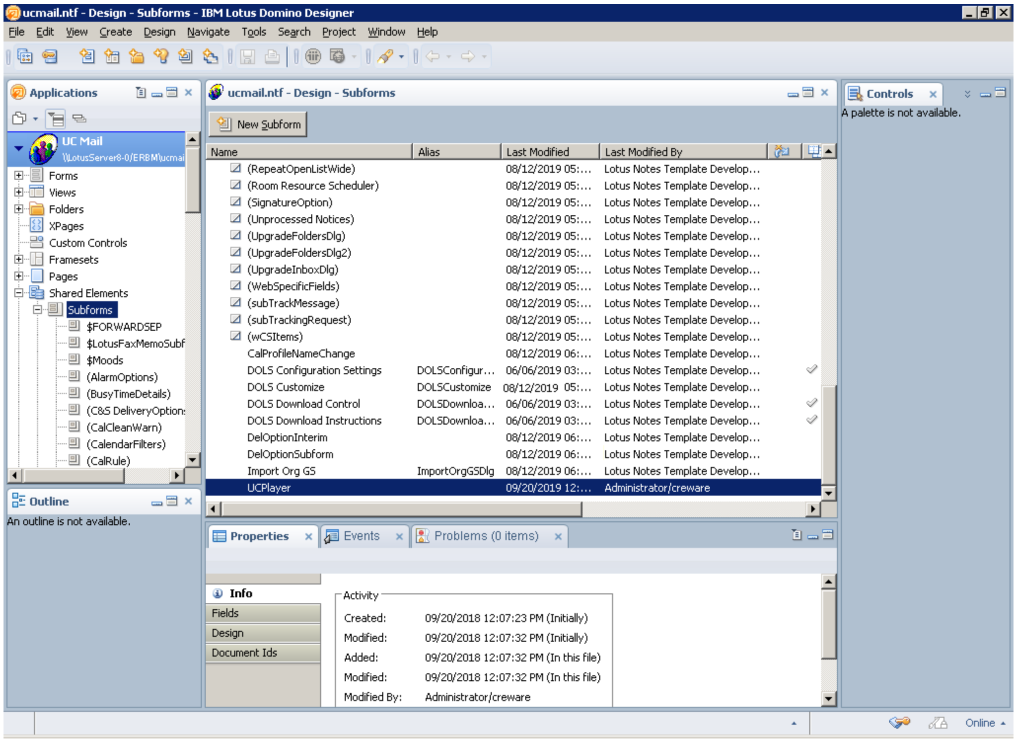


Server: **LotusServer**
Release 8.5 on Windows/2003 5.2 Intel Pentium

Title	Filename	Physical Path	File Format	Logical Size
Domino Directory Cache	dbdirman.nsf	C:\Program Files\IBM	R6 (43:0)	774,14
Domino Domain Monitc	ddm.nsf	C:\Program Files\IBM	R6 (43:0)	5,505,02
DPI (Domino Portal Inte	dpicfg.nsf	C:\Program Files\IBM	R6 (43:0)	958,46
Homepage (8.5)	homepage.nsf	C:\Program Files\IBM	R6 (43:0)	458,75
IBM Lotus iNotes Redire	iwaredir.ntf	C:\Program Files\IBM	R6 (43:0)	1,253,37
ID Vault (8)	idvault.ntf	C:\Program Files\IBM	R6 (43:0)	995,32
Java AgentRunner	agentrunner.ns	C:\Program Files\IBM	R5 (41:0)	458,75
Local free time info	busytime.nsf	C:\Program Files\IBM	R6 (43:0)	393,21
Lotus Notes/Domino Fa	lndfr.nsf	C:\Program Files\IBM	R6 (43:0)	1,015,80
Lotus Notes/Domino Sn	lndsutr.nsf	C:\Program Files\IBM	R6 (43:0)	774,14
Lotus SmartSuite Librar	doclbs7.ntf	C:\Program Files\IBM	R6 (43:0)	958,46
Mail (R8.5)	mail85.ntf	C:\Program Files\IBM	R6 (43:0)	30,670,84
Microsoft Office Library	doclbm7.ntf	C:\Program Files\IBM	R6 (43:0)	1,105,92
Monitoring Configuratio	events4.nsf	C:\Program Files\IBM	R6 (43:0)	30,408,70
Notebook (8)	notebook8.ntf	C:\Program Files\IBM	R6 (43:0)	1,437,69
Notes Log (8) ()	log.nsf	C:\Program Files\IBM	R6 (43:0)	1,843,20
Offline Services	doladmin.nsf	C:\Program Files\IBM	R6 (43:0)	774,14
Personal Address Book	pernames.ntf	C:\Program Files\IBM	R6 (43:0)	4,980,73
Personal Journal (8)	journal6.ntf	C:\Program Files\IBM	R6 (43:0)	774,14
Reports for LotusServer	reports.nsf	C:\Program Files\IBM	R6 (43:0)	995,32
RSS Feed Generator	rss_generator.r	C:\Program Files\IBM	R6 (43:0)	1,216,51
Sample Web Agent - Re	pwdresetsampl	C:\Program Files\IBM	R6 (43:0)	524,28
Server Certificate Admin	certsrv.nsf	C:\Program Files\IBM	R6 (43:0)	1,253,37
Server.Load Setup Ager	namagent.nsf	C:\Program Files\IBM	R6 (43:0)	11,796,48
TeamRoom (8)	teamrm7.ntf	C:\Program Files\IBM	R6 (43:0)	2,621,44
UC Mail	ucmail.ntf	C:\Program Files\IBM	R6 (43:0)	17,825,79

1 file(s) selected 17 MB (17,825,792 bytes)

4. Expand **Shared Elements > Subforms** in the left pane of the Designer window. From the main pane locate **UCPlayer** and double click to open.

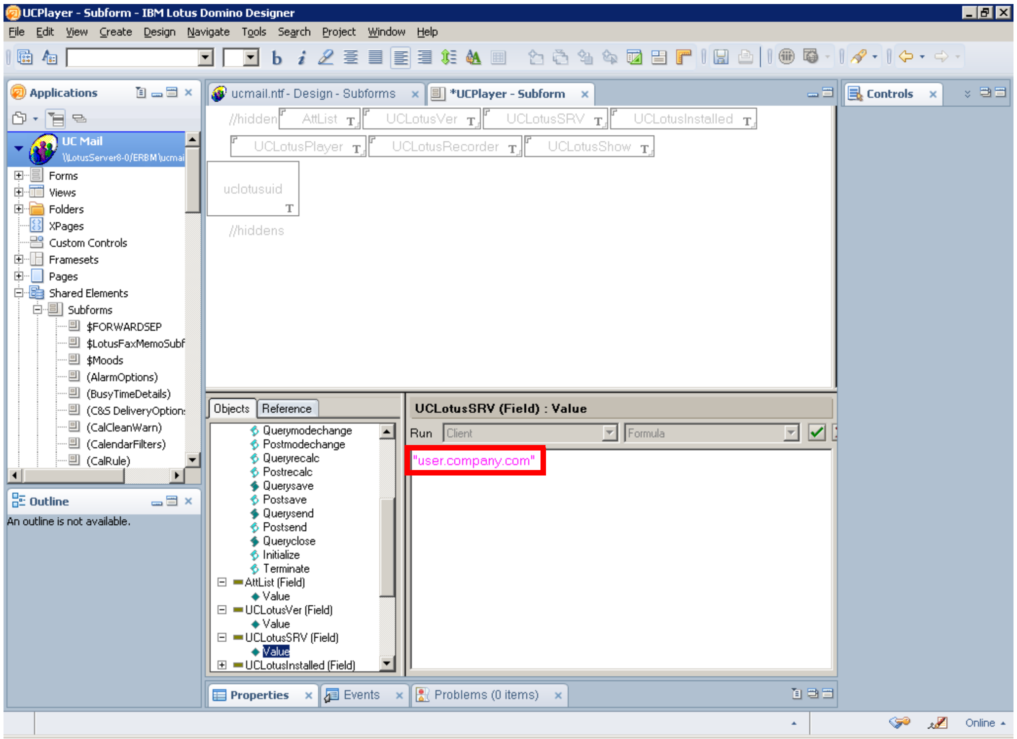


Name	Alias	Last Modified	Last Modified By
(RepeatOpenListWide)		08/12/2019 05:...	Lotus Notes Template Develop...
(Room Resource Scheduler)		08/12/2019 05:...	Lotus Notes Template Develop...
(SignatureOption)		08/12/2019 05:...	Lotus Notes Template Develop...
(Unprocessed Notices)		08/12/2019 05:...	Lotus Notes Template Develop...
(UpgradeFoldersDlg)		08/12/2019 05:...	Lotus Notes Template Develop...
(UpgradeFoldersDlg2)		08/12/2019 05:...	Lotus Notes Template Develop...
(UpgradeInboxDlg)		08/12/2019 05:...	Lotus Notes Template Develop...
(WebSpecificFields)		08/12/2019 05:...	Lotus Notes Template Develop...
(subTrackMessage)		08/12/2019 05:...	Lotus Notes Template Develop...
(subTrackingRequest)		08/12/2019 05:...	Lotus Notes Template Develop...
(wCSItems)		08/12/2019 05:...	Lotus Notes Template Develop...
CalProfileNameChange		08/12/2019 06:...	Lotus Notes Template Develop...
DOLS Configuration Settings	DOLSConfigur...	06/06/2019 03:...	Lotus Notes Template Develop...
DOLS Customize	DOLSCustomize	08/12/2019 05:...	Lotus Notes Template Develop...
DOLS Download Control	DOLSDownloa...	06/06/2019 03:...	Lotus Notes Template Develop...
DOLS Download Instructions	DOLSDownloa...	06/06/2019 03:...	Lotus Notes Template Develop...
DelOptionInterim		08/12/2019 06:...	Lotus Notes Template Develop...
DelOptionSubform		08/12/2019 06:...	Lotus Notes Template Develop...
Import Org GS	ImportOrgGSDlg	08/12/2019 06:...	Lotus Notes Template Develop...
UCPlayer		09/20/2019 12:...	Administrator/creware

Activity

Created: 09/20/2018 12:07:23 PM (Initially)
Modified: 09/20/2018 12:07:32 PM (Initially)
Added: 09/20/2018 12:07:32 PM (In this file)
Modified: 09/20/2018 12:07:32 PM (In this file)
Modified By: Administrator/creware

5. The fields associated with the UC Player subform appear. Open the **UCIBMSRV** variable and enter the Avaya Messaging server's domain name or IP address. This is where end users download the iLink Pro Desktop application. When ready, **Save** and **Close** the subform. This will update the design element signer.



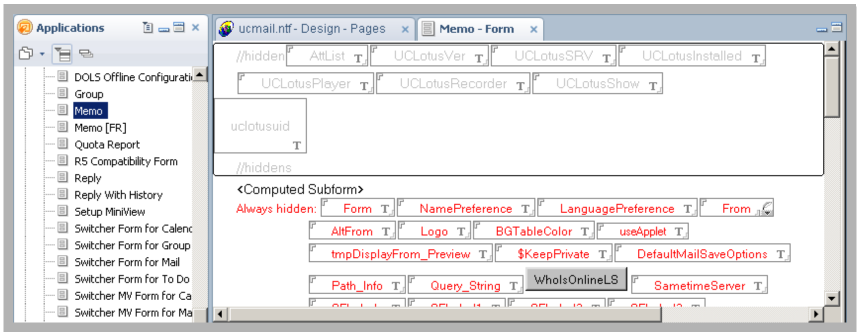
UCLotusSRV (Field) : Value

Run Client Formula

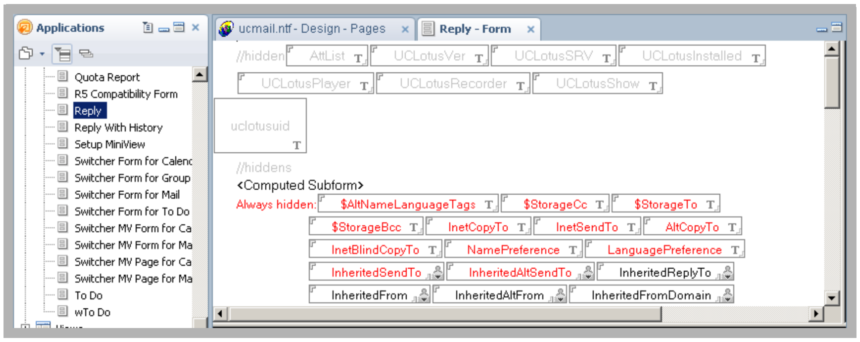
"user.company.com"

Hint: Use the UCIBMVer field to manage version control with UC form.

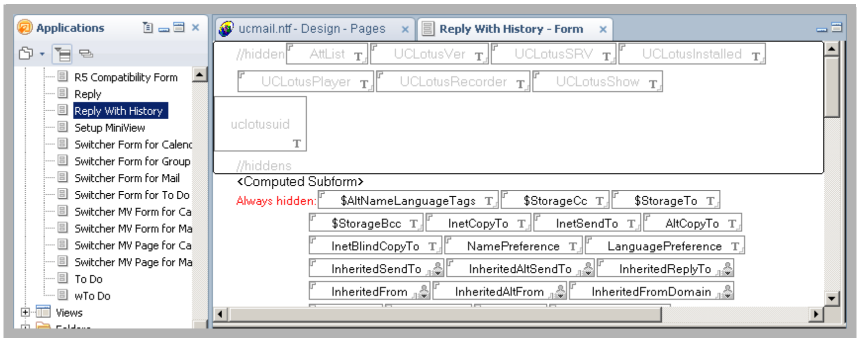
6. From the **Forms** section, double click on **Memo**. Save and close the **Memo** form to update the design element signer.



7. Repeat the process for **Reply** form. Open the form then Save and close to update the design element signer.



8. Repeat the process for **Reply with history** form. Open the form then Save and close to update the design element signer.



9. Repeat the process for any other forms you wish to add the UC Player to, and then exit **Domino Designer**.

ECL Configuration

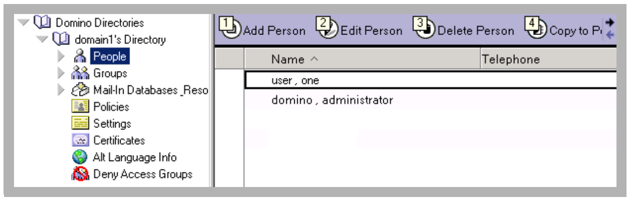
IBM Domino uses an **Execution Control List** (ECL) to set up workstation data security. An ECL limits the actions of formulae, scripts, forms and other objects run on a workstation. For example, an ECL can prevent another person's code from running on a PC and damaging or erasing data.

Domino administrators have the power to allow users to modify their ECLs or to control all changes to their ECLs across an organization. In order to limit workstation access, an ECL will look for a database, template and item signature before opening on the workstation. The ECL will then check this signature against its settings to determine what level of access can be granted.

Groupware forms are subject to an ECL check as well, since they contain scripts and COM objects. Thus, on the first installation of Groupware forms within an organization, you are advised to:

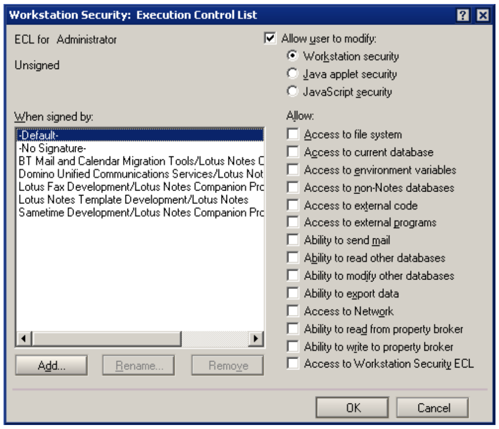
- Modify the Administrative ECL on the Domino Server.
- Propagate the changes to all clients.

1. Open **Domino Administrator**. Locate the **People & Groups** tab.
   From **Actions** menu, select **Edit Administration ECL**.



user , one
domino , administrator

2. From the **Workstation Security: Execution Control List** window, click on the **Add** button.



ECL for Administrator

Unsigned

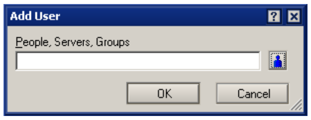
☑ Allow user to modify:
● Workstation security
○ Java applet security
○ JavaScript security

When signed by:
-Default-
-No Signature-
BT Mail and Calendar Migration Tools/Lotus Notes C
Domino Unified Communications Services/Lotus Not
Lotus Fax Development/Lotus Notes Companion Prc
Lotus Notes Template Development/Lotus Notes
Sametime Development/Lotus Notes Companion Prc

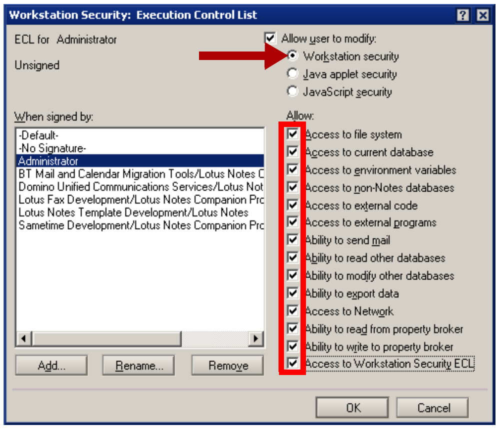
Allow:
☐ Access to file system
☐ Access to current database
☐ Access to environment variables
☐ Access to non-Notes databases
☐ Access to external code
☐ Access to external programs
☐ Ability to send mail
☐ Ability to read other databases
☐ Ability to modify other databases
☐ Ability to export data
☐ Access to Network
☐ Ability to read from property broker
☐ Ability to write to property broker
☐ Access to Workstation Security ECL

3. In the **People, Servers, or Groups** field, enter the name of the person/server/group to be added to the ECL. This should be the person that performed the installation, most likely the Domino Administrator.

   Once you have selected a user, click **OK**.



4. Now select the user or object added in the previous step (Administrator in this example). Enable **Allow user to modify**, then select the **Workstation security** radio button. Enable all checkboxes under **Allow** then click **OK**.



Workstation Security: Execution Control List

ECL for Administrator

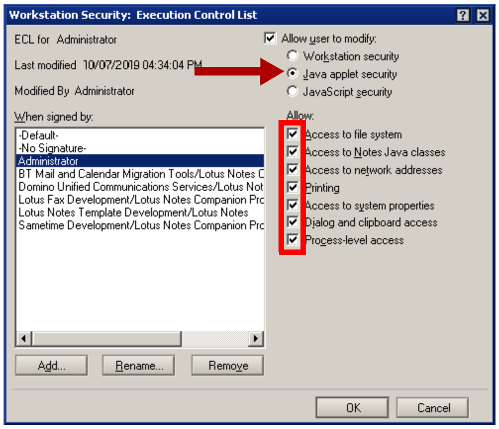
Unsigned

☑ Allow user to modify:
● Workstation security
○ Java applet security
○ JavaScript security

When signed by:
-Default-
-No Signature-
Administrator
BT Mail and Calendar Migration Tools/Lotus Notes C
Domino Unified Communications Services/Lotus Not
Lotus Fax Development/Lotus Notes Companion Prc
Lotus Notes Template Development/Lotus Notes
Sametime Development/Lotus Notes Companion Prc

Allow:
☑ Access to file system
☑ Access to current database
☑ Access to environment variables
☑ Access to non-Notes databases
☑ Access to external code
☑ Access to external programs
☑ Ability to send mail
☑ Ability to read other databases
☑ Ability to modify other databases
☑ Ability to export data
☑ Access to Network
☑ Ability to read from property broker
☑ Ability to write to property broker
☑ Access to Workstation Security ECL

5. Repeat for both the **Java applet security** and **JavaScript security** radio buttons.



Workstation Security: Execution Control List

ECL for Administrator

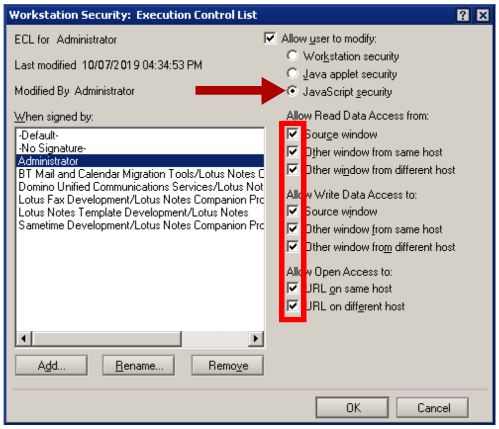
Last modified 10/07/2019 04:34:04 PM

Modified By Administrator

☑ Allow user to modify:
○ Workstation security
● Java applet security
○ JavaScript security

When signed by:
-Default-
-No Signature-
Administrator
BT Mail and Calendar Migration Tools/Lotus Notes C
Domino Unified Communications Services/Lotus Not
Lotus Fax Development/Lotus Notes Companion Prc
Lotus Notes Template Development/Lotus Notes
Sametime Development/Lotus Notes Companion Prc

Allow:
☑ Access to file system
☑ Access to Notes Java classes
☑ Access to network addresses
☑ Printing
☑ Access to system properties
☑ Dialog and clipboard access
☑ Process-level access



Workstation Security: Execution Control List

ECL for Administrator

Last modified 10/07/2019 04:34:53 PM

Modified By Administrator

☑ Allow user to modify:
○ Workstation security
○ Java applet security
● JavaScript security

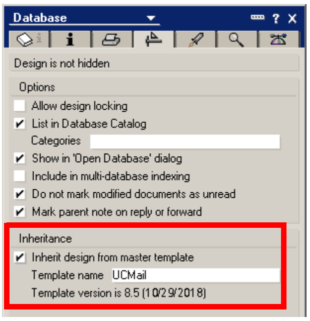
When signed by:
-Default-
-No Signature-
Administrator
BT Mail and Calendar Migration Tools/Lotus Notes C
Domino Unified Communications Services/Lotus Not
Lotus Fax Development/Lotus Notes Companion Prc
Lotus Notes Template Development/Lotus Notes
Sametime Development/Lotus Notes Companion Prc

Allow Read Data Access from:
☑ Source window
☑ Other window from same host
☑ Other window from different host

Allow Write Data Access to:
☑ Source window
☑ Other window from same host
☑ Other window from different host

Allow Open Access to:
☑ URL on same host
☑ URL on different host

6. For each mailbox database that will include UC forms, configure them to inherit the design from the **UCMail** template. This can be done using the load convert command, or manually through mailbox database properties.



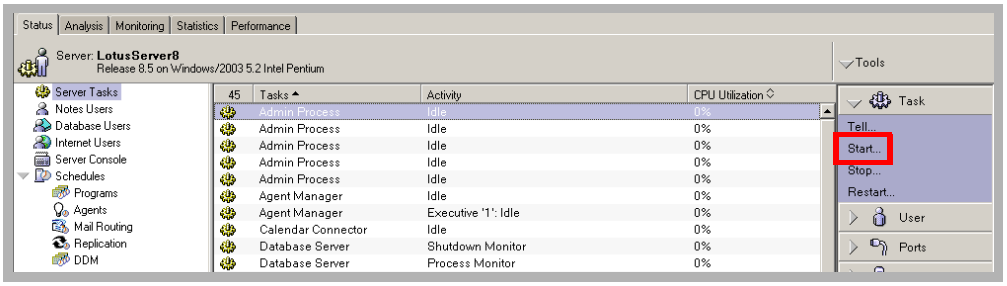
Database

Design is not hidden

Options
□ Allow design locking
☑ List in Database Catalog
Categories
☑ Show in 'Open Database' dialog
□ Include in multi-database indexing
☑ Do not mark modified documents as unread
☑ Mark parent note on reply or forward

Inheritance
☑ Inherit design from master template
Template name UCMail
Template version is 8.5 (10/29/2018)

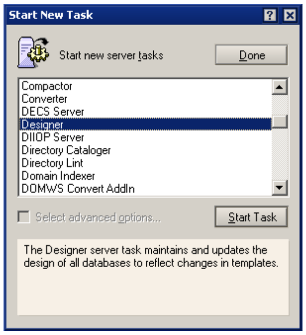
7. Now that the forms are ready, you must append the new design. From **Status > Server Tasks**, click **Start...** in the list of tasks on the right pane.



Server: **LotusServer8**
Release 8.5 on Windows/2003 5.2 Intel Pentium

45	Tasks	Activity	CPU Utilization
	Admin Process	Idle	0%
	Admin Process	Idle	0%
	Admin Process	Idle	0%
	Admin Process	Idle	0%
	Admin Process	Idle	0%
	Agent Manager	Idle	0%
	Agent Manager	Executive '1': Idle	0%
	Calendar Connector	Idle	0%
	Database Server	Shutdown Monitor	0%
	Database Server	Process Monitor	0%

8. Select Designer from the list then click **Start Task**. The design will be updated for all Users. Users can now take advantage of the forms packaged with iLink Pro Desktop in IBM Notes.



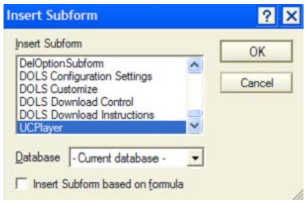
Compactor
Converter
DECS Server
Designer
DIIOP Server
Directory Cataloger
Directory Lint
Domain Indexer
DOMWS Convert AddIn

The Designer server task maintains and updates the design of all databases to reflect changes in templates.

Note: Once the design elements have been propagated to the client database, the forms are almost complete. A few additional components must be installed to fully enable forms on the client.

Adding UC Forms to Existing Design (Method B)

1. This procedure is similar to Method A, but you will be importing the UC form into an existing database template so that you can utilize UC form within an existing custom form design. Please refer to the details within Method A to familiarize with yourself with the procedure before proceeding.
2. Insert the Installation DVD.
3. Copy the **ucmail.ntf** from the DVD and paste into the Domino Data folder (e.g. **C:\Program Files\IBM\IBM\Domino\Data**).
4. Navigate to **File > Database > Open**. Select the **ucmail.ntf** file from Step 3 and open it in Domino Designer.
5. Open the copied template. This template should contain the UC forms. As a rule, all users in an organization will inherit design elements from a single template. Should it be necessary to provide UC functionality to a *select* group of users, it is recommended that a copy of the default template be created and all UC elements placed there. Design elements for UC user databases can then be inherited from the created template.
6. Edit the **UCIBMSRV** variable to point to your Web Access for iLink Pro Desktop download.
7. Copy the **UCPlayer** subform and paste it into the target template. If the **UCPlayer** subform is already present in the target template (upgrade scenario), then remove it prior to upgrading.
8. Open the **Memo** form in the target template and select **Create > Resource > Insert Subform**.



Insert Subform

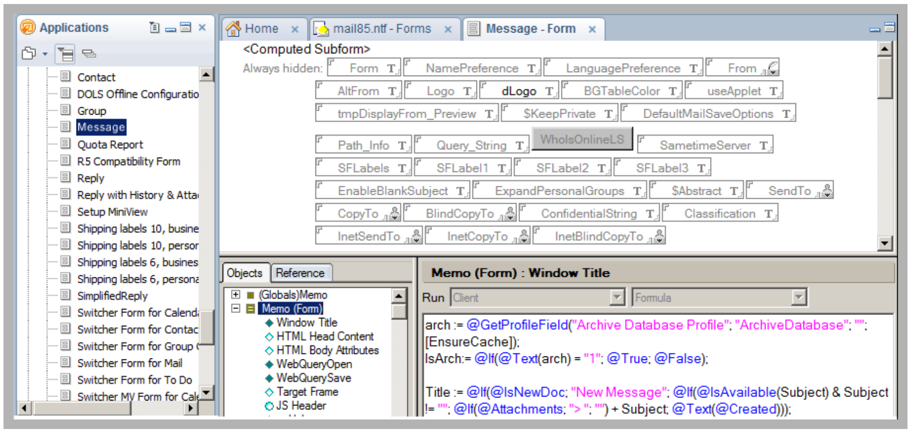
Insert Subform

DelOptionSubform
DOLS Configuration Settings
DOLS Customize
DOLS Download Control
DOLS Download Instructions
UCPlayer

Database - Current database -

□ Insert Subform based on formula

9. Click **OK**. The **UCPlayer** subform will be inserted into the **Message** form.



```
arch := @GetProfileField("Archive Database Profile"; "ArchiveDatabase"; "";
[EnsureCache]);
IsArch:= @If(@Text(arch) = "1"; @True; @False);

Title := @If(@IsNewDoc; "New Message"; @If(@IsAvailable(Subject) & Subject
!= ""; @If(@Attachments; "> "; "") + Subject; @Text(@Created)));
```

10. Click **Save** and close the form.
11. Repeat Steps 7-10 for each form that is to include the **UCPlayer** subform.
12. Create three copies of the modified Memo form and give them the following names: **TelNTVoice**, **TelNTFax**, and **TelNTText**.
13. Follow the procedures on **ECL Configuration on page 216** to complete the process.

User Guide

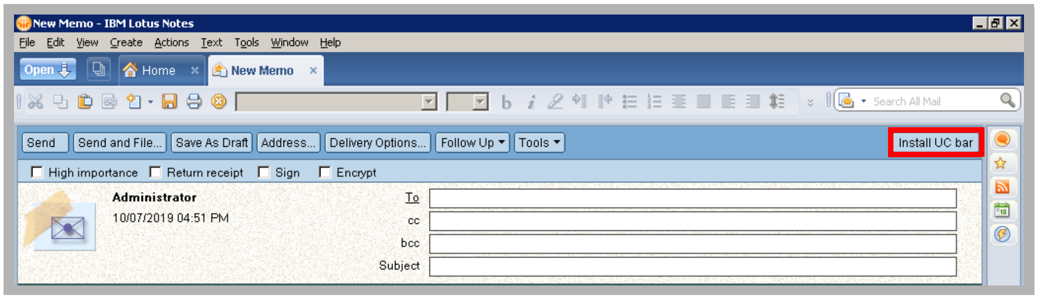
Installing UC Forms in IBM Notes

To use UC forms within IBM Notes, you must install iLink Pro Desktop. Obtain iPD from IBM Notes.

Installing UC Bar and iLink Pro Desktop

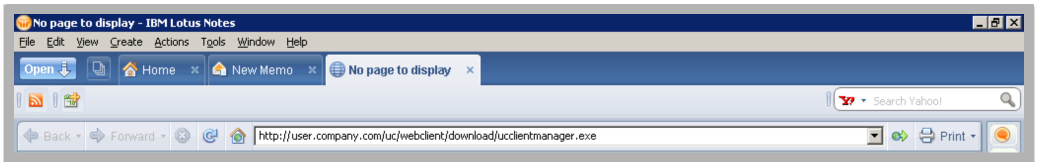
Note: Subforms must be inserted in all areas which require voice message playback function.

1. Run IBM Notes.
2. Open the mail database.
3. Create or open a document that uses a form with the UC Player subform (e.g. **Memo**).
4. In the Actions pane click on the **Install UC bar** button.



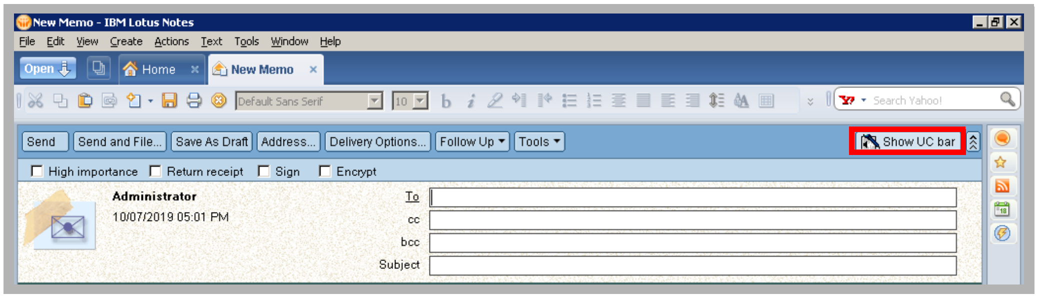
Administrator
10/07/2019 04:51 PM

5. IBM Notes will open a web page to download the iLink Pro Desktop software. iPD must be installed for UC forms to work.


No page to display - IBM Lotus Notes
File Edit View Create Actions Tools Window Help
Open
Home
New Memo
No page to display
Search Yahoo!
Back
Forward
Print

http://user.company.com/uc/webclient/download/ucclientmanager.exe

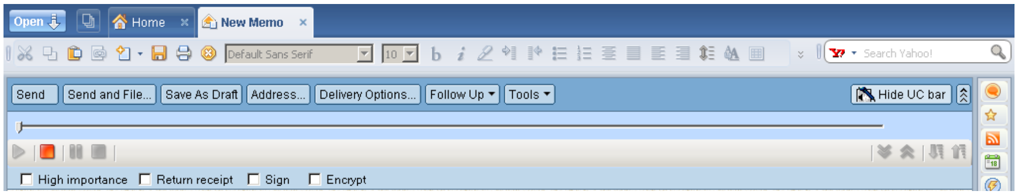
6. Download the installation package then install the application.
7. Once iLink Pro Desktop is installed, the button will change to **Show UC bar**. Click on this button to open the UC form.



Default Sans Serif
10
Administrator
10/07/2019 05:01 PM

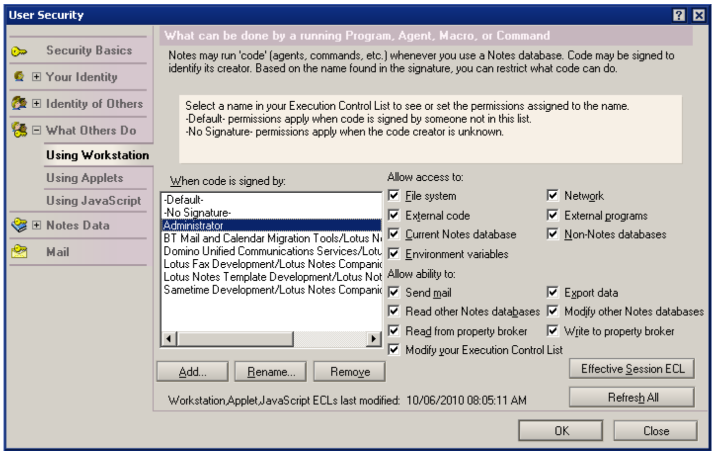
Note: You may have to restart IBM Notes or reopen a form in order to see the new button. You must also be **logged into iLink Pro Desktop** to use the UC forms.

8. You will now have access to Record and Playback actions through the form.



Verifying the IBM Notes client ECL setup

1. Open IBM Notes.
2. Select **File > Security > User Security > What Others Do > Using Workstation**. The User Security dialog box appears.



What can be done by a running Program, Agent, Macro, or Command

Notes may run 'code' (agents, commands, etc.) whenever you use a Notes database. Code may be signed to identify its creator. Based on the name found in the signature, you can restrict what code can do.

Select a name in your Execution Control List to see or set the permissions assigned to the name.
-Default- permissions apply when code is signed by someone not in this list.
-No Signature- permissions apply when the code creator is unknown.

When code is signed by:

-Default-
-No Signature-
Administrator
BT Mail and Calendar Migration Tools/Lotus N
Domino Unified Communications Services/Lotu
Lotus Fax Development/Lotus Notes Companio
Lotus Notes Template Development/Lotus Not
Sametime Development/Lotus Notes Companio

Allow access to:

☑ File system
☑ External code
☑ Current Notes database
☑ Environment variables
☑ Network
☑ External programs
☑ Non-Notes databases

Allow ability to:

☑ Send mail
☑ Read other Notes databases
☑ Read from property broker
☑ Modify your Execution Control List
☑ Export data
☑ Modify other Notes databases
☑ Write to property broker

Add... Rename... Remove Effective Session ECL Refresh All

Workstation,Applet,JavaScript ECLs last modified: 10/06/2010 08:05:11 AM

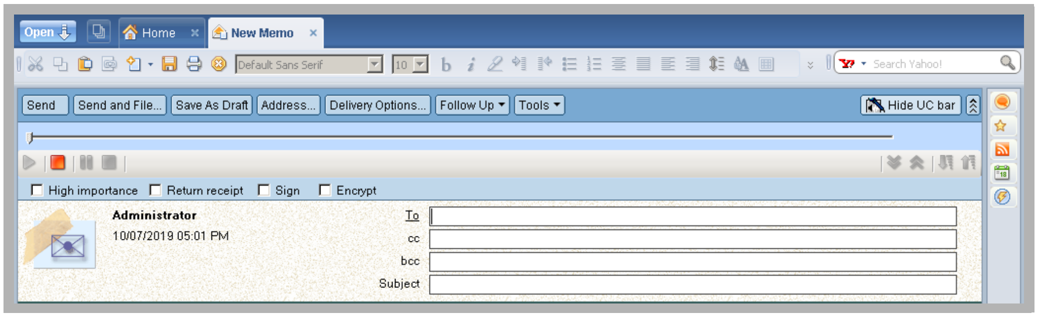
OK Close

3. The ECL should contain all of the entries that were defined in the Administration ECL.

Using UC Forms in IBM Notes

Composing a Voice Message

1. Create a new message.
2. Fill out the **To**, **Subject** and any other fields as you would normally do.
3. Use the UC bar provided to record a message.

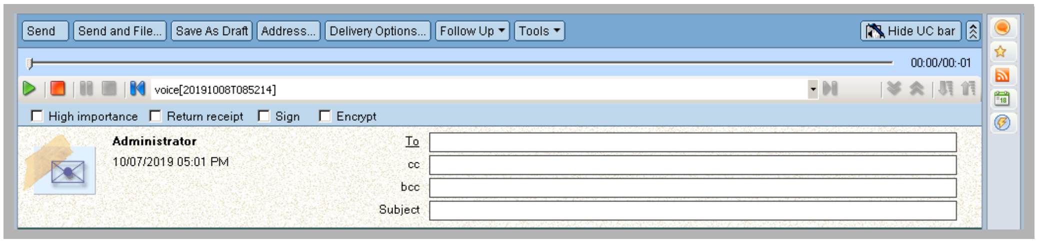


Administrator
10/07/2019 05:01 PM

- Click 🟥 to begin recording the voice message with your microphone.
- Click ☎ to begin recording the voice message with your phone.
- Click ⏸ to pause recording or playback.
- Click ⏹ to stop recording or playback.
- Click ▶ to playback recorded message.

Note: Some actions may not be available depending on site settings.

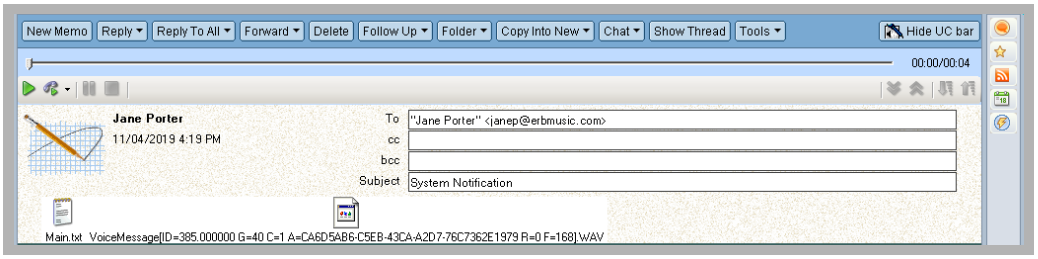
4. When you finish recording a message, you will see an attachment automatically created as shown. Click **Send** to transmit your message.



00:00/00:-01
voice[20191008T085214]
Administrator
10/07/2019 05:01 PM

Listening to a Voice Message

1. Open a voice message from IBM Notes. UC forms will detect voice messages and provide options for message playback.



Jane Porter
11/04/2019 4:19 PM

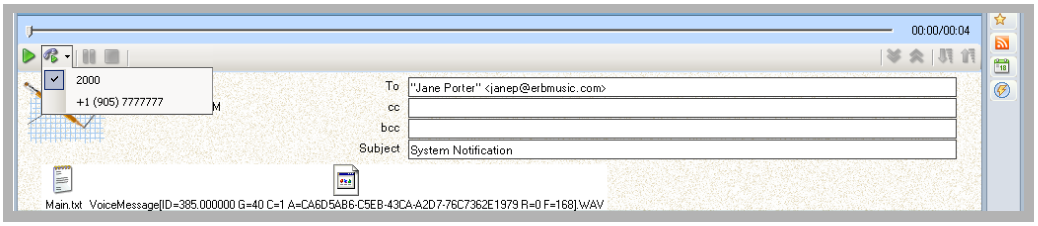
To "Jane Porter" <janep@erbmusic.com>
cc
bcc
Subject System Notification

Main.txt VoiceMessage[ID=385.000000 G=40 C=1 A=CA6D5AB6-C5EB-43CA-A2D7-76C7362E1979 R=0 F=168].WAV

- Click ▶ to begin playing the voice message on your PC speaker.
- Click ☎ to begin playing the voice message on your phone.
- Click ⏸ to pause playback.
- Click ■ to stop playback.

Note: Some actions may not be available depending on site settings.

2. If you choose to play the message on your phone, you will be given an option to choose which number to listen from. The list depends on your current UC location and the extensions defined through iLink Pro Desktop. When you select a number to listen from, UC server will dial that number, then playback the message once the call is answered.

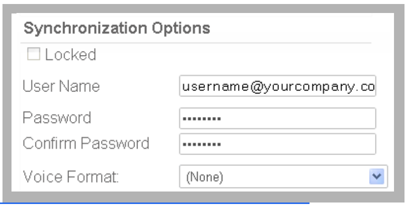


To "Jane Porter" <janep@erbmusic.com>
cc
bcc
Subject System Notification

Main.txt VoiceMessage[ID=385.000000 G=40 C=1 A=CA6D5AB6-C5EB-43CA-A2D7-76C7362E1979 R=0 F=168].WAV

Configuring UC Mailbox to Synchronize with IBM Notes

Note: If you do not have access to Web Access, this configuration can be performed by your administrator.



Synchronization Options

☐ Locked

User Name	username@yourcompany.co
Password	••••••••
Confirm Password	••••••••
Voice Format	(None)

1. Log into Web Access.
2. Click on the **Account** icon.
3. If the **Locked** checkbox is selected, deselect this checkbox.
4. Provide the following information:

    User Name: Enter your mail server user name.

Note: The user name you enter in this field will be the same user name for the email account as it exists on the mail server.

Password: Enter the password for your mail account.

Note: The password you enter in this field will be the same password for the email account as it exists on the mail server.

Confirm Password: Confirm the above password.

Voice Format: From the dropdown menu, select the voice format which will be used for voice messages. You should leave this field as default in most cases.

5. Click on **Save and Close** button at the top.

16

FIND ME FOLLOW ME ON CTI INTEGRATION

In This Chapter:

Introduction

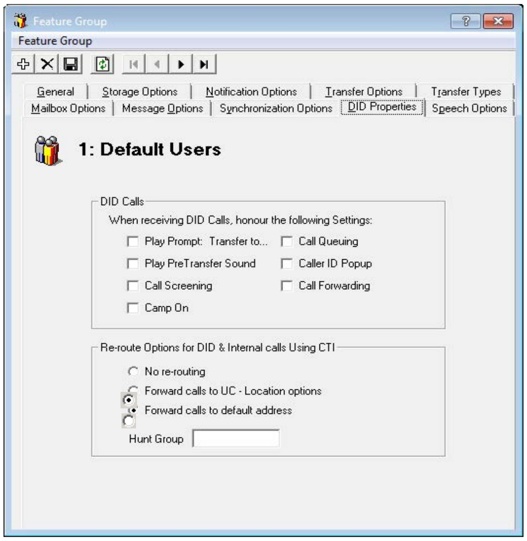
Find me Follow me allows calls to be forwarded to one or more addresses until the user is found. The addresses can be internal or external numbers. They can be dialed sequentially, or simultaneously.

This document is intended for technicians who have some familiarity with the 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 bank.



Feature Group

Feature Group

General | Storage Options | Notification Options | Transfer Options | Transfer Types
Mailbox Options | Message Options | Synchronization Options | DID Properties | Speech Options

1: Default Users

DID Calls

When receiving DID Calls, honour the following Settings:

□ Play Prompt: Transfer to... □ Call Queuing
□ Play PreTransfer Sound □ Caller ID Popup
□ Call Screening □ Call Forwarding
□ Camp On

Re-route Options for DID & Internal calls Using CTI

○ No re-routing
○ Forward calls to UC - Location options
● Forward calls to default address

Hunt Group

Visual Guide

A caller tries to reach a user through UC Server.

UC Server tries to locate the user by trying all devices simultaneously. When the user answers the phone, other devices will stop ringing.

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 8.5 - 10.8 Avaya Messaging version 11.0 or higher

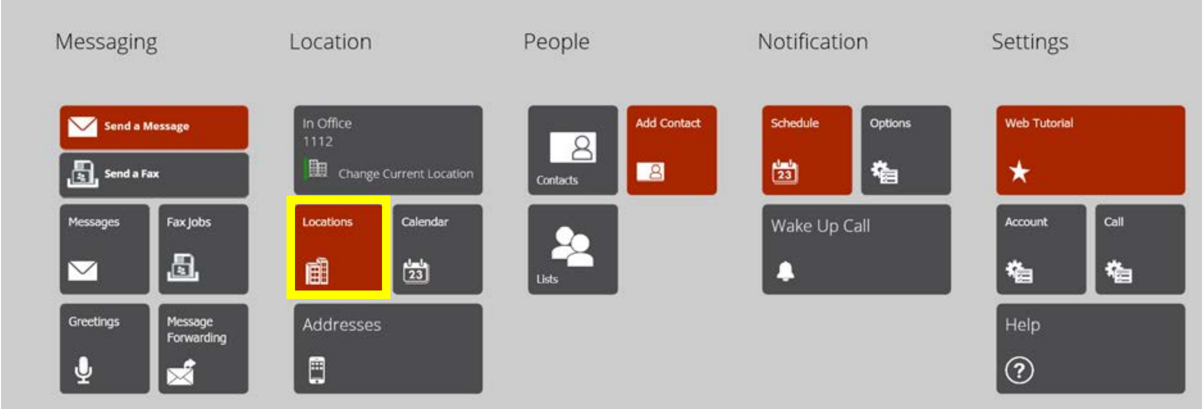
User Guide

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.

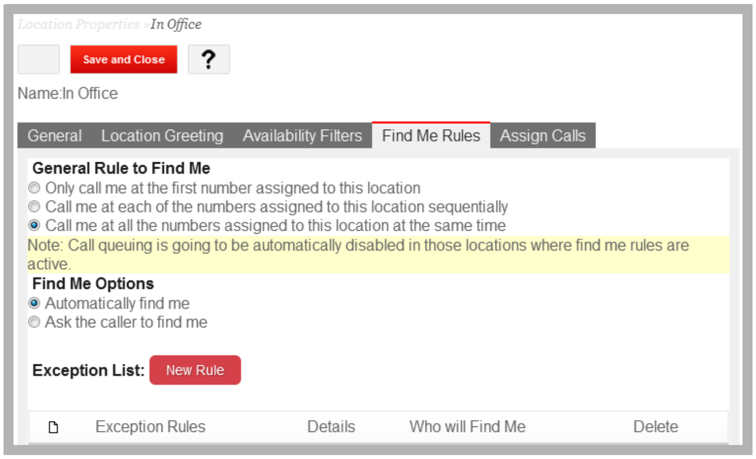
Find me Follow me with CTI Integration

Note: Before users can launch Web Access, two items must be set in Avaya Messaging Admin:
1) Enable **Web Access User** under **Mailbox > Advanced**, and
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.



Name:In Office

General Rule to Find Me

○ Only call me at the first number assigned to this location
○ Call me at each of the numbers assigned to this location sequentially
● Call me at all the numbers assigned to this location at the same time

Note: Call queuing is going to be automatically disabled in those locations where find me rules are active.

Find Me Options

● Automatically find me
○ Ask the caller to find me

Exception List:

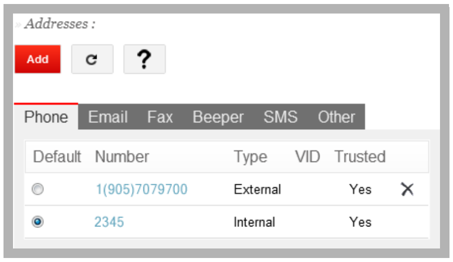
The Find Me Rules page displays all of the options available for that location. It is important to note that this section will configure how the Auto attendant will behave for incoming calls. However, it is necessary to set the current location as well as availability. Refer to page 128 of the Client Applications Guide for further details on these settings.

Addresses

Addresses are an important part of the find 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 in order to configure the find me follow me features.

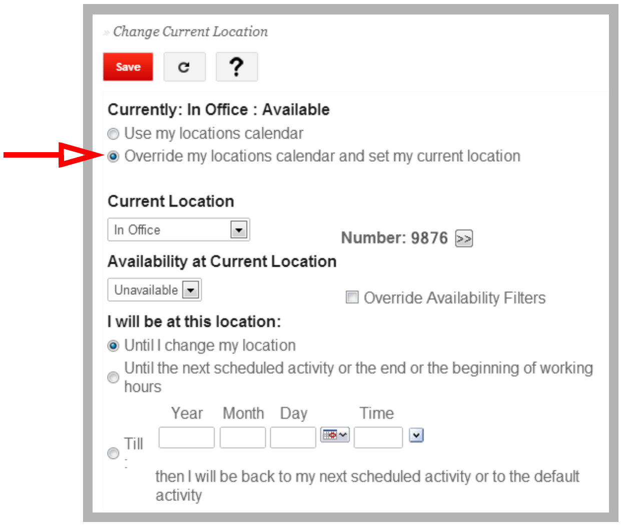
Addresses can be added, edited and deleted on the **Addresses** page of Web Access. Addresses can be internal (such as a desk phone extension) or external (such as a cell phone or phone number off site).



Addresses :

Default	Number	Type	VID	Trusted	
○	1(905)7079700	External		Yes	✕
●	2345	Internal		Yes	

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.



Change Current Location

Currently: In Office : Available

○ Use my locations calendar

● Override my locations calendar and set my current location

Current Location

In Office

Number: 9876 >>

Availability at Current Location

Unavailable

□ Override Availability Filters

I will be at this location:

● Until I change my location

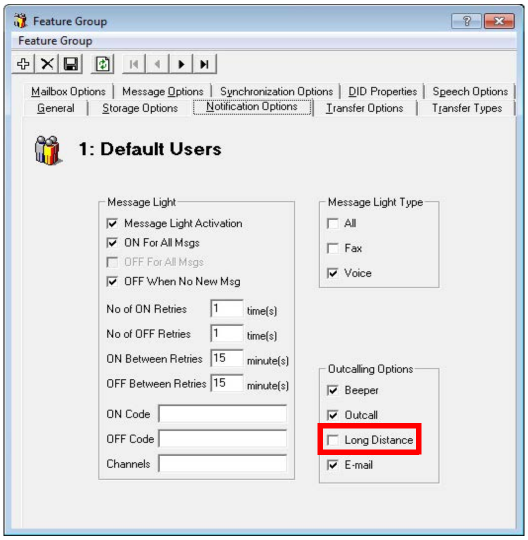
○ Until the next scheduled activity or the end or the beginning of working hours

○ Till : Year Month Day Time

then I will be back to my next scheduled activity or to the default activity

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



1: Default Users

Message Light

☑ Message Light Activation
☑ ON For All Msgs
☐ OFF For All Msgs
☑ OFF When No New Msg

No of ON Retries 1 time(s)
No of OFF Retries 1 time(s)
ON Between Retries 15 minute(s)
OFF Between Retries 15 minute(s)
ON Code
OFF Code
Channels

Message Light Type

☐ All
☐ Fax
☑ Voice

Outcalling Options

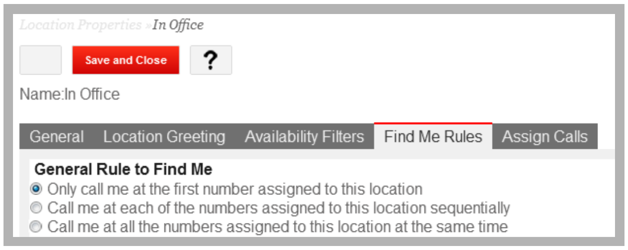
☑ Beeper
☑ Outcall
☐ Long Distance
☑ E-mail

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.



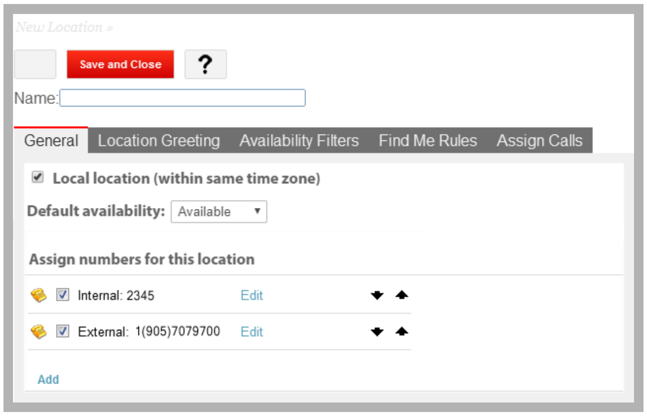
Location Properties » In Office

Name:In Office

General Rule to Find Me

- ● Only call me at the first number assigned to this location
- ○ Call me at each of the numbers assigned to this location sequentially
- ○ Call me at all the numbers assigned to this location at the same time

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.



New Location »

Name:

☑ Local location (within same time zone)

Default availability: Available ▾

Assign numbers for this location

☑	Internal: 2345	Edit	▼ ▲
☑	External: 1(905)7079700	Edit	▼ ▲

Add

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.

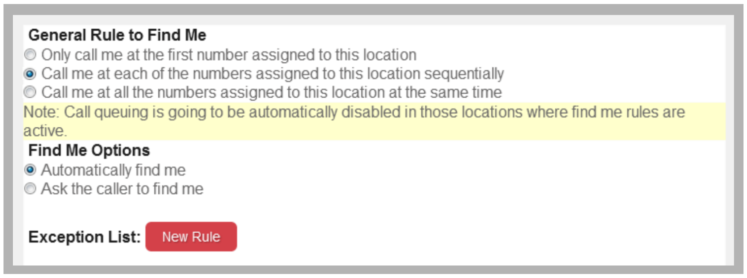
Note: In order for this feature to work, the user must be set up to be in that location and Available. If the user is Unavailable the find me follow me feature will be disabled and the Auto attendant will play the location greeting.

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:

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



General Rule to Find Me

○ Only call me at the first number assigned to this location
● Call me at each of the numbers assigned to this location sequentially
○ Call me at all the numbers assigned to this location at the same time

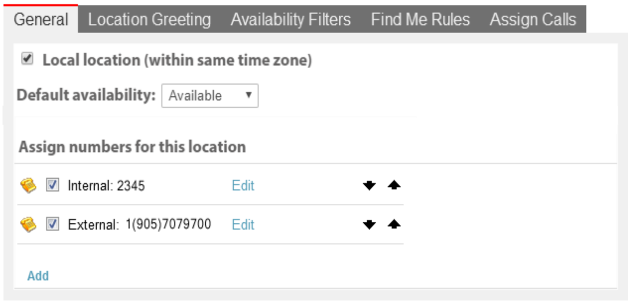
Note: Call queuing is going to be automatically disabled in those locations where find me rules are active.

Find Me Options

● Automatically find me
○ Ask the caller to find me

Exception List: New Rule

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).



☑ Local location (within same time zone)

Default availability: Available ▾

Assign numbers for this location

☑ Internal: 2345 Edit ▼ ▲

☑ External: 1(905)7079700 Edit ▼ ▲

Add

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 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.

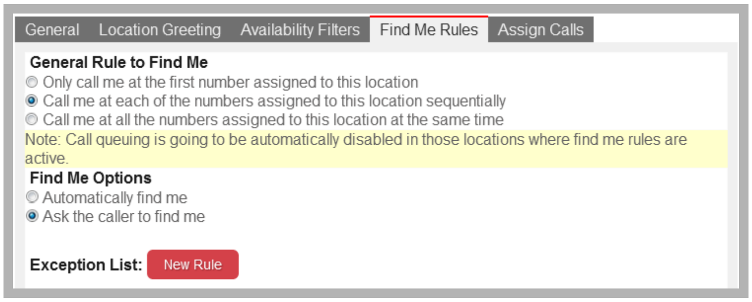
If the default internal address of that mailbox is in the list of numbers assigned to the location, calls made to a DID will always ring that extension first regardless of where it is in the list, and then the Auto attendant will dial the rest of the numbers in sequence from top to bottom (bypassing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

Note: 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. 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:

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:



General Rule to Find Me

○ Only call me at the first number assigned to this location

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

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

Note: Call queuing is going to be automatically disabled in those locations where find me rules are active.

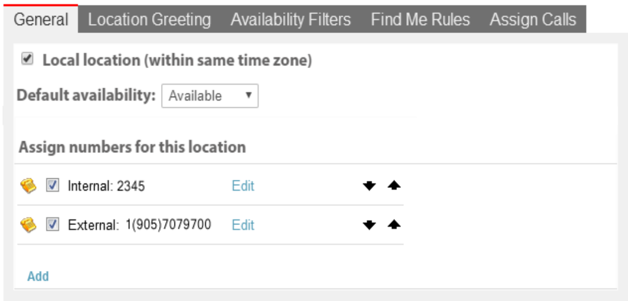
Find Me Options

○ Automatically find me

● Ask the caller to find me

Exception List: New Rule

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).



☑ Local location (within same time zone)

Default availability: Available ▾

Assign numbers for this location

☑ Internal: 2345 Edit

☑ External: 1(905)7079700 Edit

Add

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

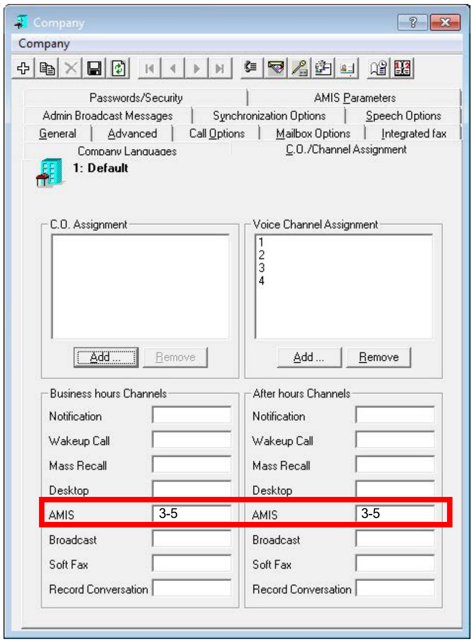
Click on the **Save and Close** button

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: 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. 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



Company

Company

Passwords/Security | AMIS Parameters
Admin Broadcast Messages | Synchronization Options | Speech Options
General | Advanced | Call Options | Mailbox Options | Integrated fax
Company Languages | C.O./Channel Assignment

1: Default

C.O. Assignment

Add ... | Remove

Voice Channel Assignment

1
2
3
4

Add ... | Remove

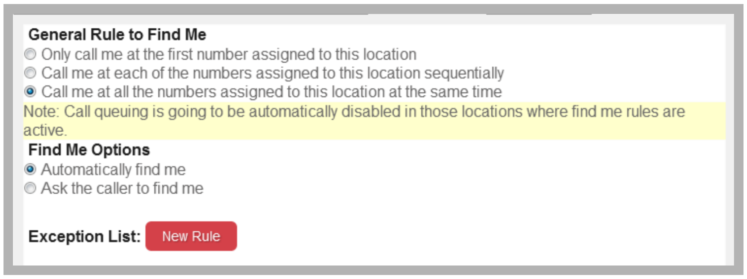
Business hours Channels		After hours Channels	
Notification		Notification	
Wakeup Call		Wakeup Call	
Mass Recall		Mass Recall	
Desktop		Desktop	
AMIS	3-5	AMIS	3-5
Broadcast		Broadcast	
Soft Fax		Soft Fax	
Record Conversation		Record Conversation	

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:



General Rule to Find Me

○ Only call me at the first number assigned to this location
○ Call me at each of the numbers assigned to this location sequentially
● Call me at all the numbers assigned to this location at the same time

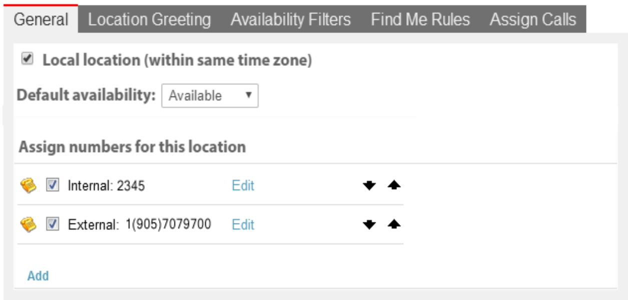
Note: Call queuing is going to be automatically disabled in those locations where find me rules are active.

Find Me Options

● Automatically find me
○ Ask the caller to find me

Exception List: New Rule

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



General | Location Greeting | Availability Filters | Find Me Rules | Assign Calls

☑ **Local location (within same time zone)**

Default availability: Available ▾

Assign numbers for this location

☑ Internal: 2345 Edit

☑ External: 1(905)7079700 Edit

Add

Click on the **Save and Close** button

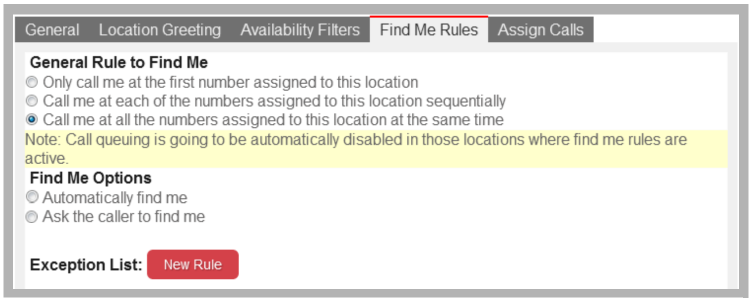
When a call is transferred by the Auto attendant or when a call is made to a DID that rings the extension directly, the Auto attendant will automatically dial all the addresses in the list of numbers assigned to the location simultaneously. If the call is answered and accepted in one of those numbers 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: 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. 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:



General Rule to Find Me

○ Only call me at the first number assigned to this location
○ Call me at each of the numbers assigned to this location sequentially
● Call me at all the numbers assigned to this location at the same time

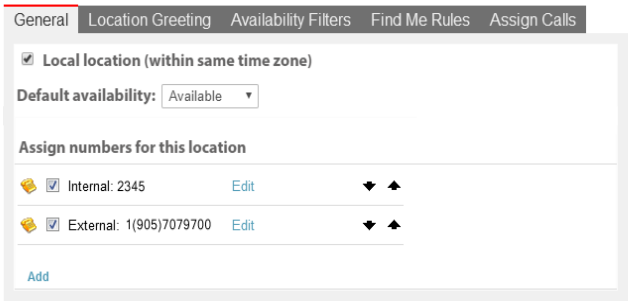
Note: Call queuing is going to be automatically disabled in those locations where find me rules are active.

Find Me Options

○ Automatically find me
○ Ask the caller to find me

Exception List: New Rule

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



☑ Local location (within same time zone)

Default availability: Available

Assign numbers for this location

☑ Internal: 2345

☑ External: 1(905)7079700

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.

17 MULTIPLE TIME ZONE SUPPORT

In This Chapter:

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 the 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

Avaya Messaging Server
User Location
User Location

When the users are location in a different time zone from the Avaya Messaging server, the server is able to honor the time zone of the user and display the date and time of the message dynamically.

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 8.5 - 10.8 Avaya Messaging version 11.0 or higher

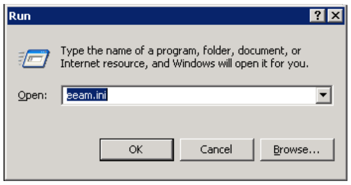
Important: In an HA installation, all servers must have the same time zone set under Windows Date / Time settings. If the servers are configured for different time zones, the timestamps will not play correctly.

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.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

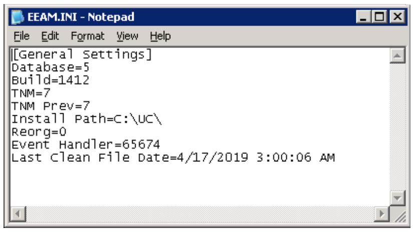
Open: eeam.ini

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.



```
[General Settings]
Database=5
Build=1412
TNM=7
TNM Prev=7
Install Path=C:\UC\
Reorg=0
Event Handler=65674
Last Clean File Date=4/17/2019 3:00:06 AM
```

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 time and date are entered by the user.

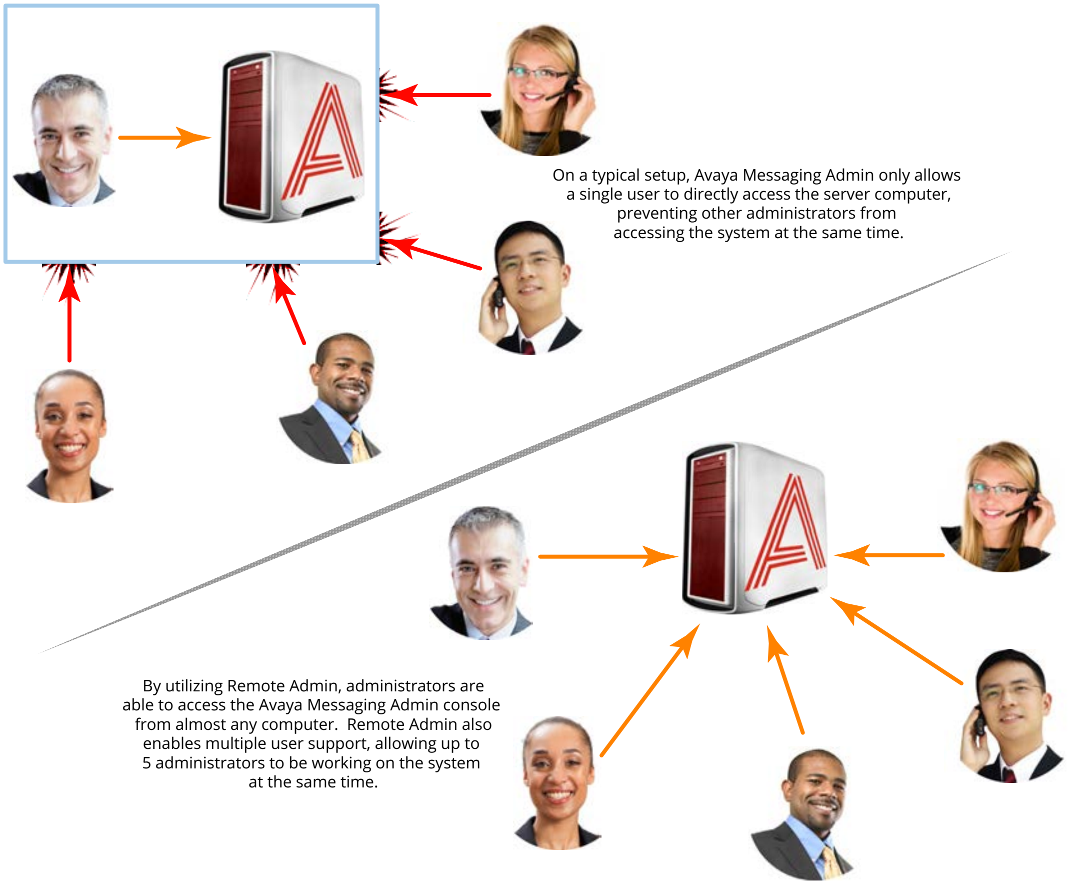
18 REMOTE ADMINISTRATION

In This Chapter:

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 in order to perform administrative functions.

Visual Guide



On a typical setup, Avaya Messaging Admin only allows a single user to directly access the server computer, preventing other administrators from accessing the system at the same time.

By utilizing Remote Admin, administrators are able to access the Avaya Messaging Admin console from almost any computer. Remote Admin also enables multiple user support, allowing up to 5 administrators to be working on the system at the same time.

Requirements

Requirements	Details
Software	Microsoft Windows Server 2012 and 2016 Microsoft Windows 7, 8, and 10.
Network	Workstations where remote admin is installed must be in the same network domain as the Avaya Messaging voice 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

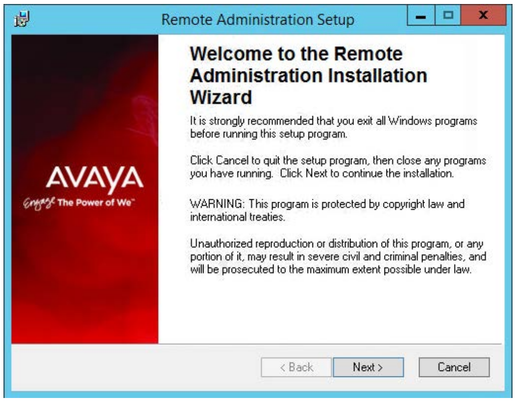
Important: Avaya Messaging must be installed and operating normally on the voice server before proceeding.

Important: 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 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.

   Click **Next** to begin the installation.



Remote Administration Setup

Welcome to the Remote Administration Installation Wizard

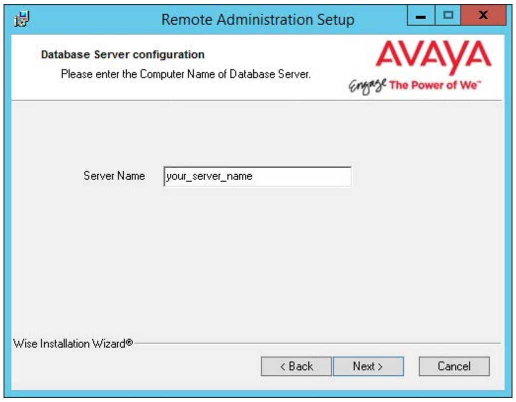
It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

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

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

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



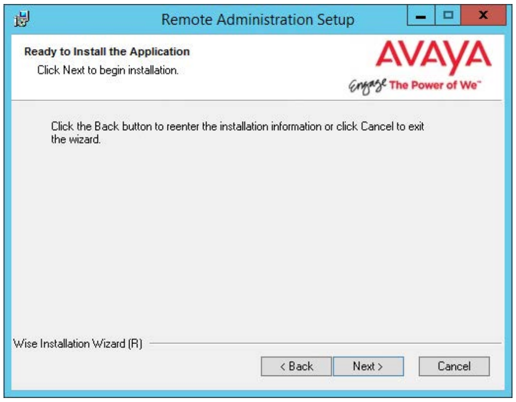
Remote Administration Setup

Database Server configuration

Please enter the Computer Name of Database Server.

Server Name: your_server_name

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



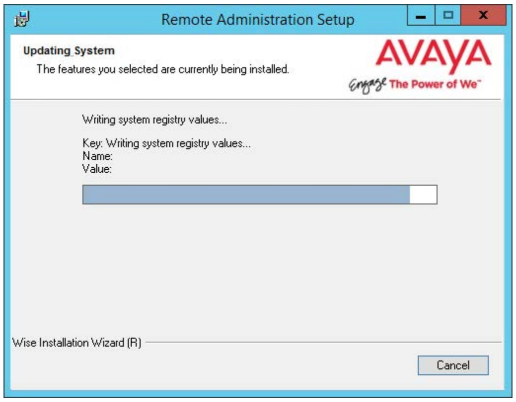
Remote Administration Setup

Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

7. Remote Administrator will be installed on the system.



Updating System

The features you selected are currently being installed.

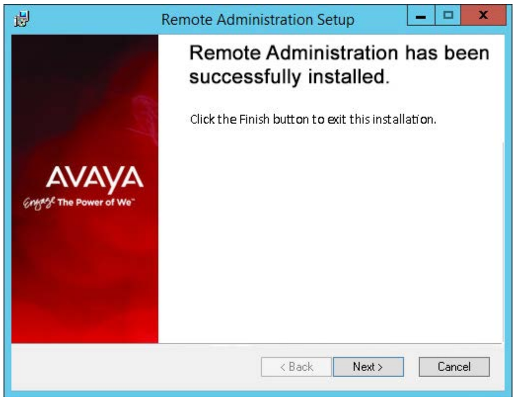
Writing system registry values...

Key: Writing system registry values...
Name:
Value:

Wise Installation Wizard (R)

8. When finished, the wizard will report that the installation was successful.

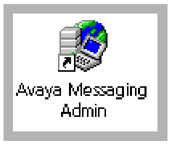
   Click **Finish** to complete the installation.



Remote Administration has been successfully installed.

Click the Finish button to exit this installation.

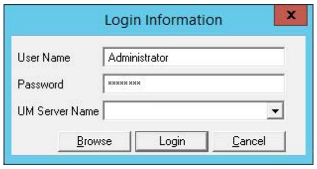
Remote admin is now ready to be used. A shortcut will be placed on your Windows desktop to access the program.



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 **OK.**



User Name: Administrator
Password: *******
UM Server Name:

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

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

19 REMOTE PRINTER

In This Chapter:

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 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.

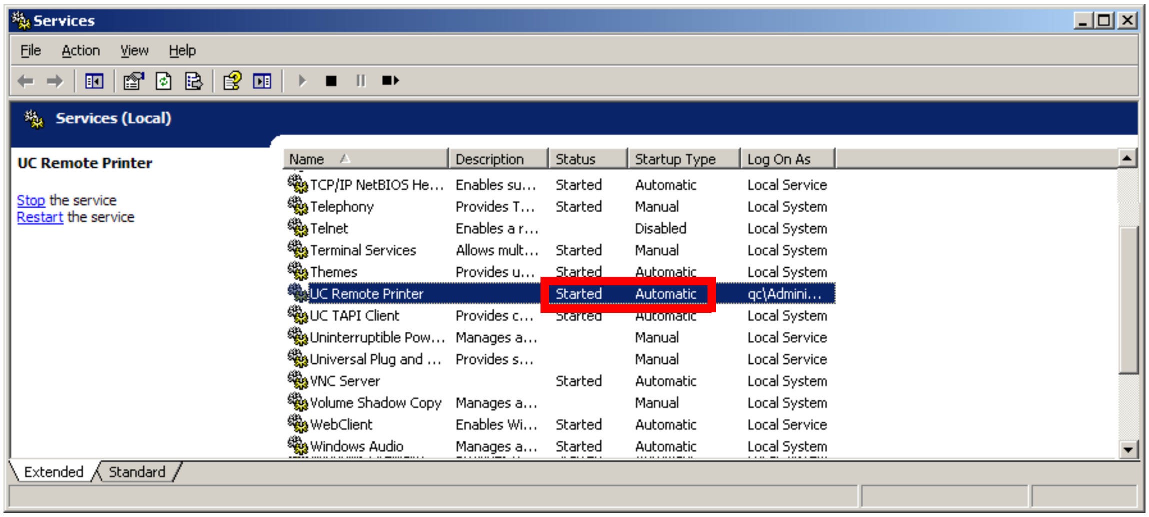
Remote Printer is included on the DVD with the standard release of Avaya Messaging. It is installed by default as part of Avaya Messaging Admin. The Remote Printer program must be installed on the host, and the settings on the voice server must be changed to point to the host machine.

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.



UC Remote Printer

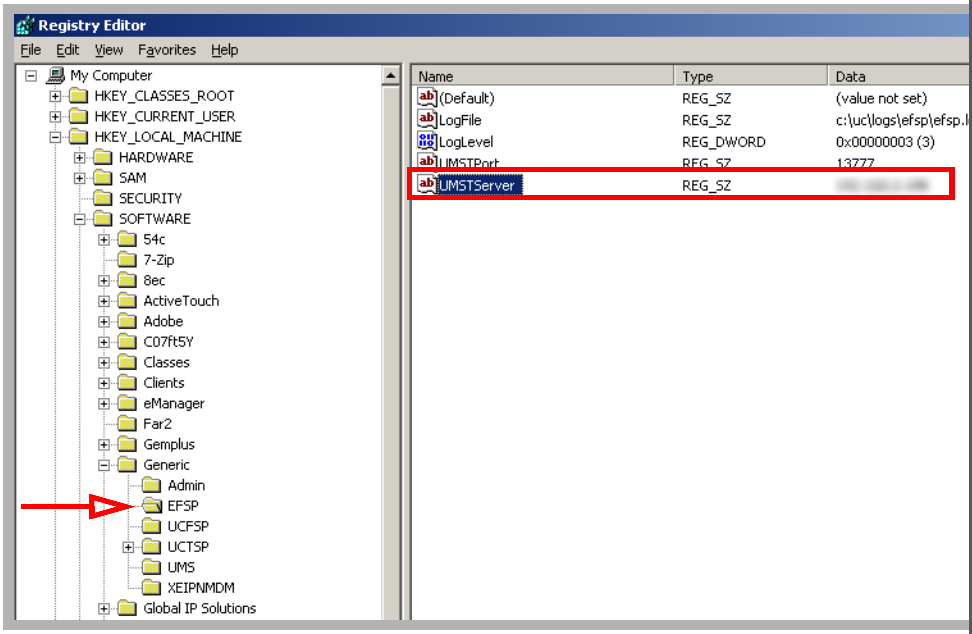
Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
TCP/IP NetBIOS He…	Enables su…	Started	Automatic	Local Service
Telephony	Provides T…	Started	Manual	Local System
Telnet	Enables a r…		Disabled	Local System
Terminal Services	Allows mult…	Started	Manual	Local System
Themes	Provides u…	Started	Automatic	Local System
UC Remote Printer		Started	Automatic	qc\Admini…
UC TAPI Client	Provides c…	Started	Automatic	Local System
Uninterruptible Pow…	Manages a…		Manual	Local Service
Universal Plug and …	Provides s…		Manual	Local Service
VNC Server		Started	Automatic	Local System
Volume Shadow Copy	Manages a…		Manual	Local System
WebClient	Enables Wi…	Started	Automatic	Local Service
Windows Audio	Manages a…	Started	Automatic	Local System

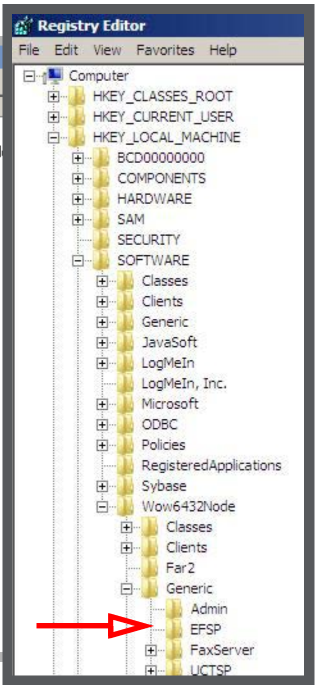
Note: The **Log On As** account should be the same as that used during the installation of MS Office or Adobe Acrobat Reader.

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).



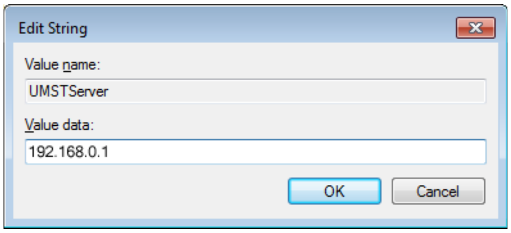
Name	Type	Data
(Default)	REG_SZ	(value not set)
LogFile	REG_SZ	c:\uc\logs\efsp\efsp.l
LogLevel	REG_DWORD	0x00000003 (3)
UMSTPort	REG_SZ	13777
UMSTServer	REG_SZ	[redacted]



32-bit Operating System Path

64-bit Operating System Path

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



Value name: UMSTServer

Value data: 192.168.0.1

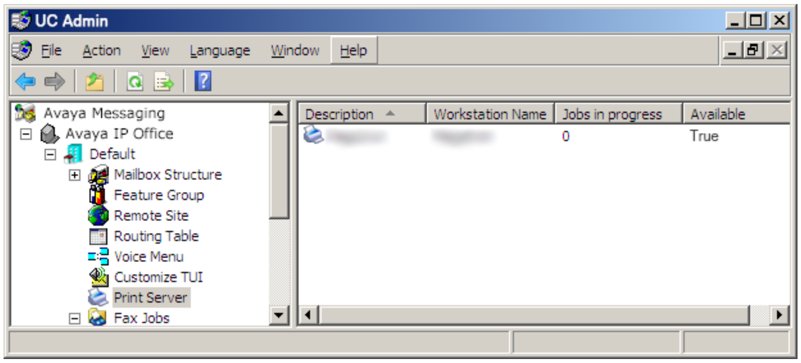
The client side configuration is complete. Proceed with the setup of the Avaya Messaging voice server.

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 setup 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**.



Description	Workstation Name	Jobs in progress	Available
[redacted]	[redacted]	0	True

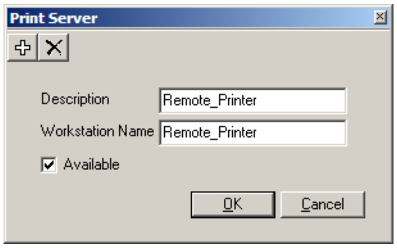
4. Fill in the required fields.

   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.



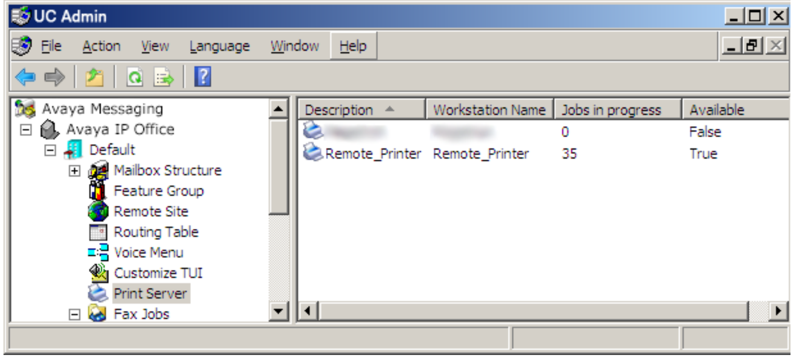
Description: Remote_Printer

Workstation Name: Remote_Printer

☑ Available

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

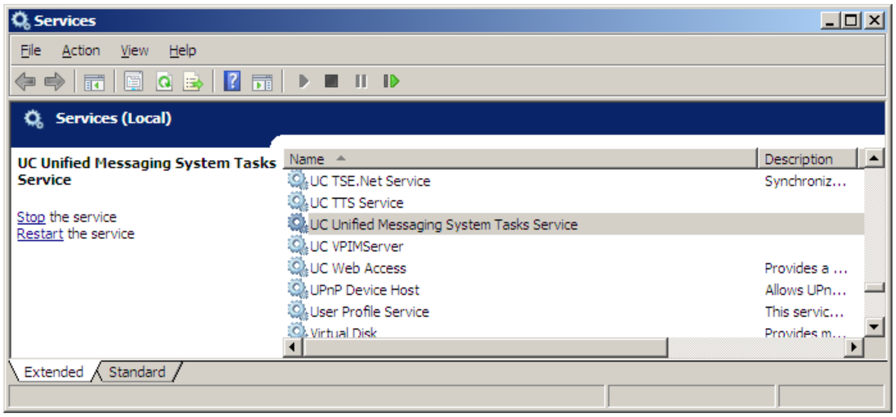
   Click **OK** when finished.



Description	Workstation Name	Jobs in progress	Available
[redacted]	[redacted]	0	False
Remote_Printer	Remote_Printer	35	True

6. Go to **Start>Adnministrative 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**.



UC Unified Messaging System Tasks Service

Stop the service
Restart the service

Name	Description
UC TSE.Net Service	Synchroniz...
UC TTS Service	
UC Unified Messaging System Tasks Service	
UC VPIMServer	
UC Web Access	Provides a ...
UPnP Device Host	Allows UPn...
User Profile Service	This servic...
Virtual Disk	Provides m...

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.

20 AVAYA MESSAGING FAXING

In This Chapter:

Introduction

While most business interactions occur digitally, faxing still remains a required feature for many people. This is especially true when thee 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.

  Refer to **Fax via Windows Fax Services (Windows 7) on page 251** or **Fax via Windows Fax Services (Windows XP) on page 256** for more information.

- **Email Client**: The advantage of this method is being able to send a fax from anywhere 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.

  Refer to **Email to Fax on page 262** for more information.

- **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.

  Refer to **Sending a Fax through Fax Gadget on page 264** for more information.

Fax via Windows Fax Services (Windows 7)

Configuration

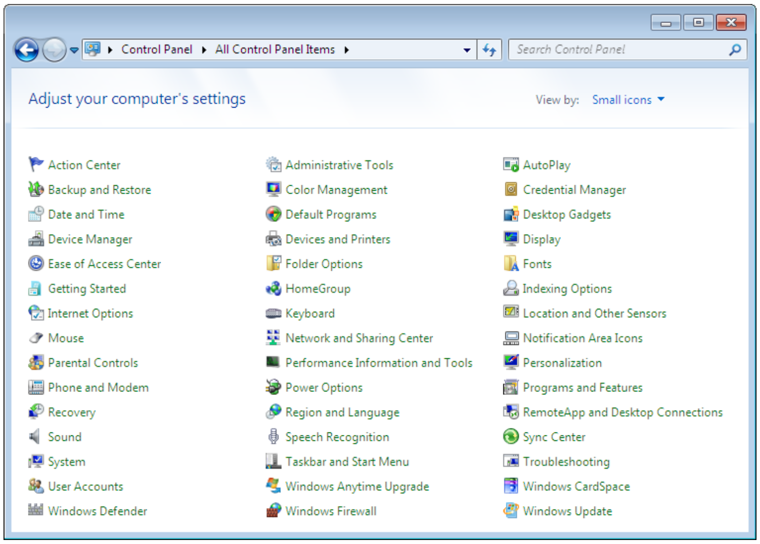
Please follow these steps to configure your client machine with the Windows Fax services.

Warning: This configuration must take place **before** installing iLink Pro Desktop. If iPD has already been installed, remove it, enable fax services, then reinstall the application.

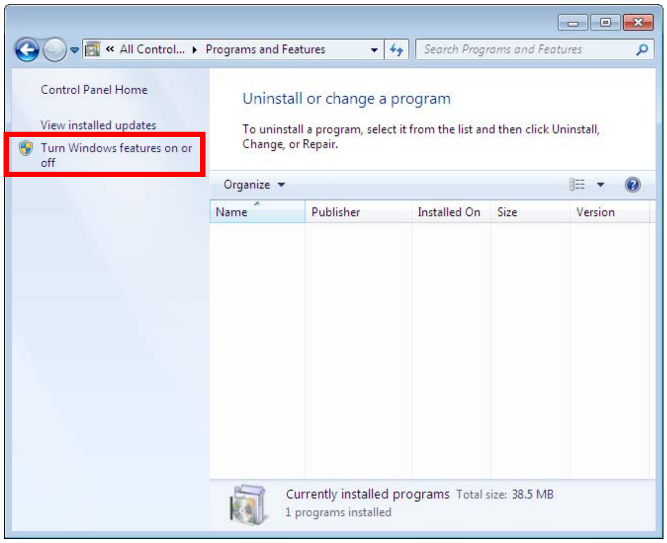
Warning: Only TIFF and TXT formats are supported by default. To send a fax in any other format, the computer must have the necessary program installed to support that file type (i.e. MicroSoft Office for doc and docx files, Acrobat Reader 9 (available on the Avaya Messaging DVD) or earlier for pdf, etc.).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


« All Control... ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize
Name
Publisher
Installed On
Size
Version

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

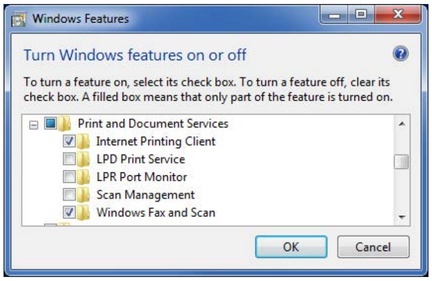
Currently installed programs Total size: 38.5 MB
1 programs installed

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.



Windows Features

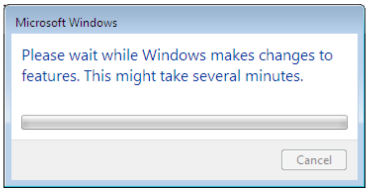
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ▪ Print and Document Services
  - ☑ Internet Printing Client
  - □ LPD Print Service
  - □ LPR Port Monitor
  - □ Scan Management
  - ☑ Windows Fax and Scan

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

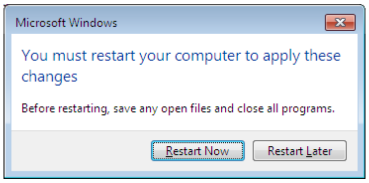
4. Windows will start to add the selected components. This process may take a while.



Microsoft Windows

Please wait while Windows makes changes to features. This might take several minutes.

5. If you are asked to restart your computer, click **Restart Now** to reboot.
6. Once the computer has restarted, install iLink Pro Desktop.
   Refer to the **Client Applications Guide** for more information.



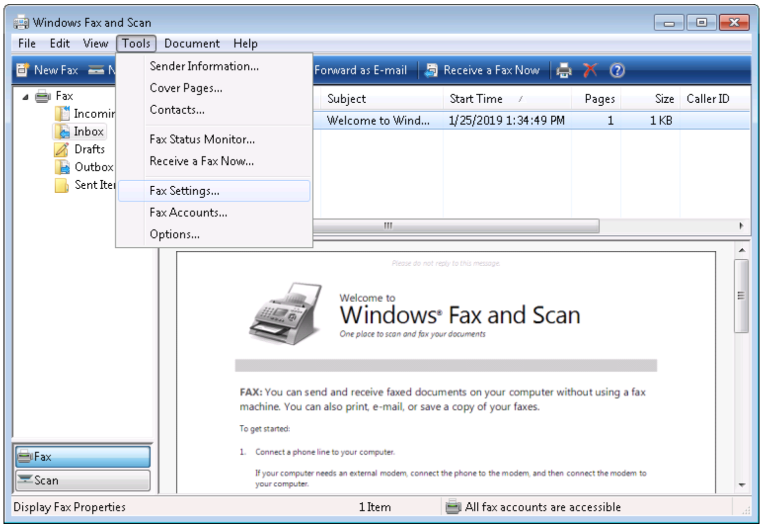
Microsoft Windows

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

7. When iLink Pro Desktop has been installed, go to **Start** > **Programs** and launch **Windows Fax and Scan**.

8. Go to **Tools** > **Fax Settings...**



Windows Fax and Scan

Subject	Start Time	Pages	Size	Caller ID
Welcome to Wind...	1/25/2019 1:34:49 PM	1	1 KB	

Please do not reply to this message.

Welcome to
Windows® Fax and Scan
One place to scan and fax your documents

FAX: You can send and receive faxed documents on your computer without using a fax machine. You can also print, e-mail, or save a copy of your faxes.

To get started:

1. Connect a phone line to your computer.

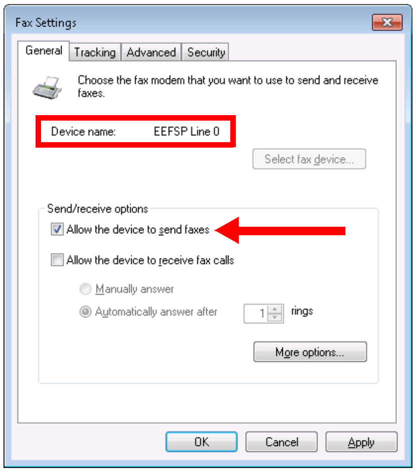
   If your computer needs an external modem, connect the phone to the modem, and then connect the modem to your computer.

Display Fax Properties 1 Item All fax accounts are accessible

9. 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.



Choose the fax modem that you want to use to send and receive faxes.

Device name: EEFSP Line 0

Send/receive options

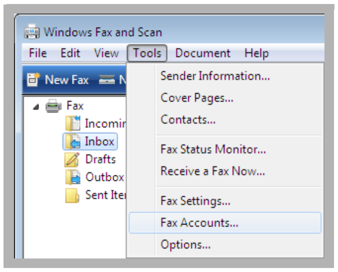
☑ Allow the device to send faxes

□ Allow the device to receive fax calls

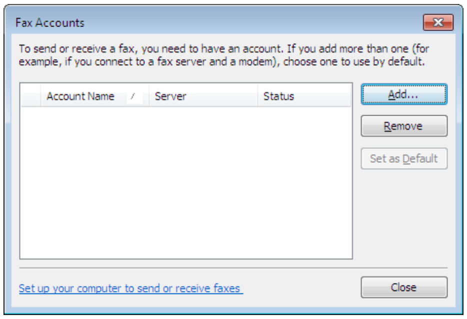
○ Manually answer

● Automatically answer after 1 rings

10. Open **Tools > Fax Accounts...**



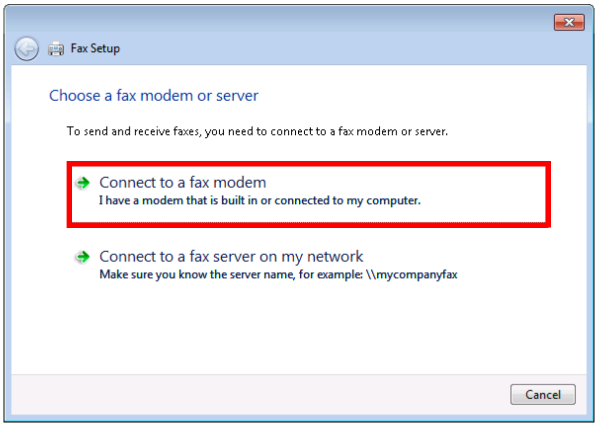
11. Click the **Add...** button.



To send or receive a fax, you need to have an account. If you add more than one (for example, if you connect to a fax server and a modem), choose one to use by default.

Account Name	Server	Status

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



Choose a fax modem or server

To send and receive faxes, you need to connect to a fax modem or server.

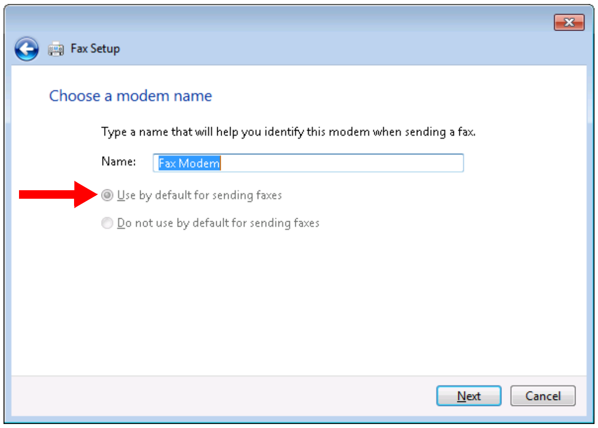
Connect to a fax modem
I have a modem that is built in or connected to my computer.

Connect to a fax server on my network
Make sure you know the server name, for example: \\mycompanyfax

13. 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.



Fax Setup

Choose a modem name

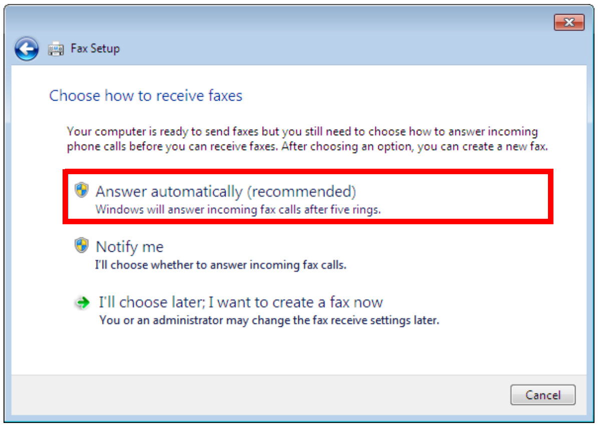
Type a name that will help you identify this modem when sending a fax.

Name: Fax Modem

● Use by default for sending faxes

○ Do not use by default for sending faxes

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



Fax Setup

Choose how to receive faxes

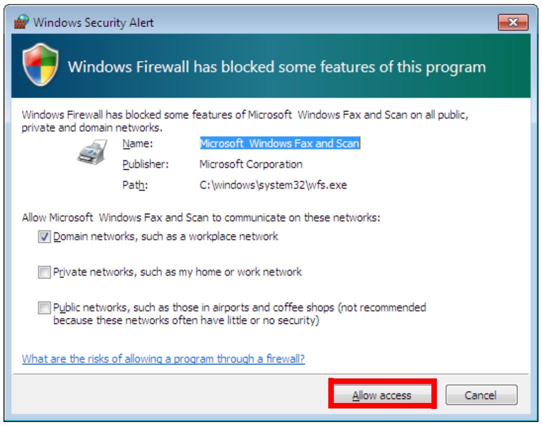
Your computer is ready to send faxes but you still need to choose how to answer incoming phone calls before you can receive faxes. After choosing an option, you can create a new fax.

Answer automatically (recommended)
Windows will answer incoming fax calls after five rings.

Notify me
I'll choose whether to answer incoming fax calls.

I'll choose later; I want to create a fax now
You or an administrator may change the fax receive settings later.

15. If you are prompted regarding your Firewall, click to **Allow access** at the bottom of the window.



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of Microsoft Windows Fax and Scan on all public, private and domain networks.

Name: Microsoft Windows Fax and Scan
Publisher: Microsoft Corporation
Path: C:\windows\system32\wfs.exe

Allow Microsoft Windows Fax and Scan to communicate on these networks:

☑ Domain networks, such as a workplace network

☐ Private networks, such as my home or work network

☐ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

Your computer is now ready to send fax messages.

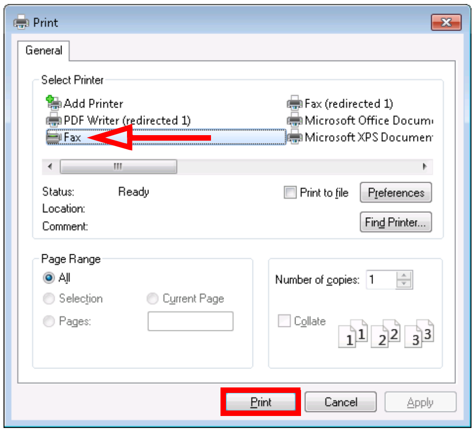
> **Note**: Keep in mind that **you must be logged into iLink Pro Desktop** to send faxes.

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**.

Note: You must be logged into iLink Pro Desktop in order to send a fax.



Status: Ready
Location:
Comment:
Page Range: ● All ○ Selection ○ Current Page ○ Pages:
Number of copies: 1
□ Print to file
□ Collate

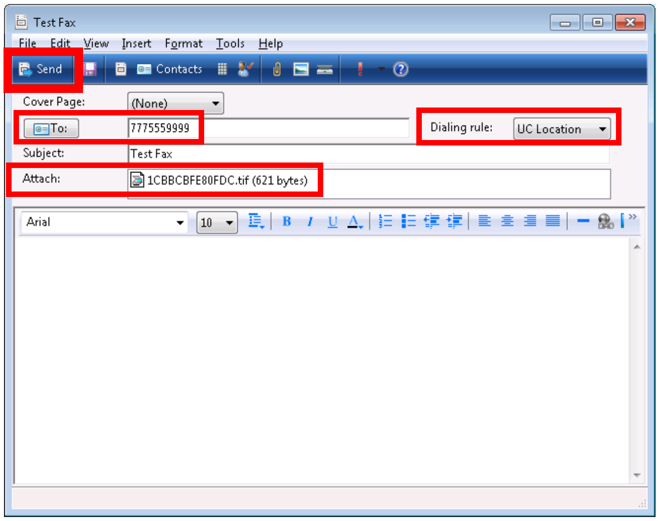
A new window will open to define the destination and any other components required for the fax.

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.

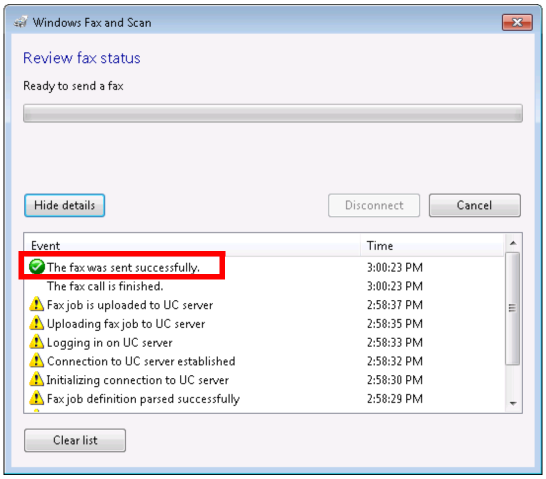


Cover Page: (None)
To: 7775559999
Dialing rule: UC Location
Subject: Test Fax
Attach: 1CBBCBFE80FDC.tif (621 bytes)

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.



Review fax status

Ready to send a fax

Event	Time
The fax was sent successfully.	3:00:23 PM
The fax call is finished.	3:00:23 PM
Fax job is uploaded to UC server	2:58:37 PM
Uploading fax job to UC server	2:58:35 PM
Logging in on UC server	2:58:33 PM
Connection to UC server established	2:58:32 PM
Initializing connection to UC server	2:58:30 PM
Fax job definition parsed successfully	2:58:29 PM

Fax via Windows Fax Services (Windows XP)

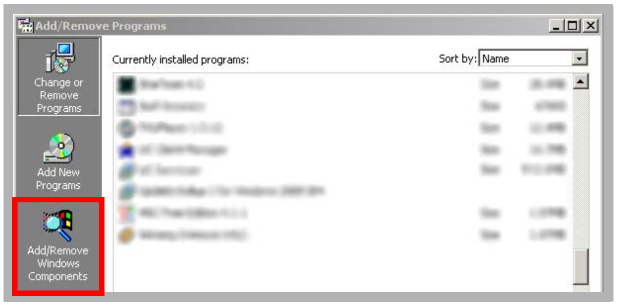
Configuration

Please follow the below steps to configure your client machine for use with Windows Fax services.

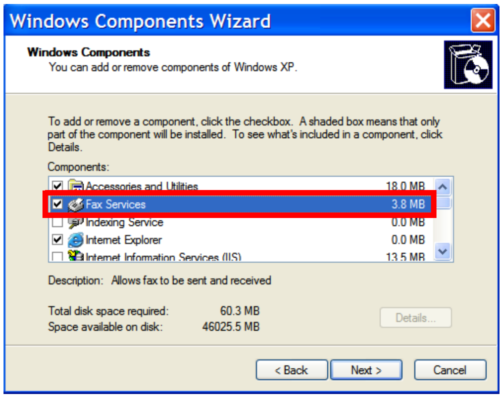
Warning: This configuration must take place **before** installing iLink Pro Desktop. If iPD has already been installed, remove it, enable fax services, then reinstall the application.

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


Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name

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



Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Accessories and Utilities	18.0 MB
☑	Fax Services	3.8 MB
□	Indexing Service	0.0 MB
☑	Internet Explorer	0.0 MB
□	Internet Information Services (IIS)	13.5 MB

Description: Allows fax to be sent and received

Total disk space required: 60.3 MB
Space available on disk: 46025.5 MB

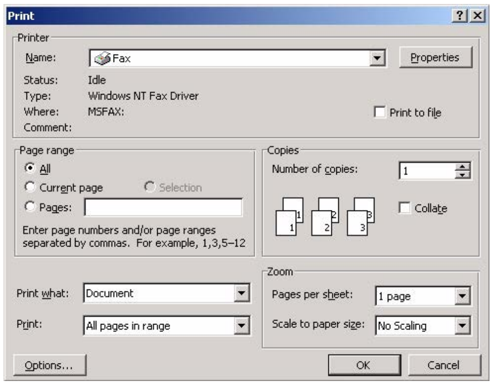
Note: You may be asked to provide a Windows installation disc depending on the computer settings.

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**.


Print

Printer

Name: Fax

Status: Idle

Type: Windows NT Fax Driver

Where: MSFAX:

Comment:

□ Print to file

Page range

● All

○ Current page ○ Selection

○ Pages:

Enter page numbers and/or page ranges separated by commas. For example, 1,3,5–12

Copies

Number of copies: 1

□ Collate

Print what: Document

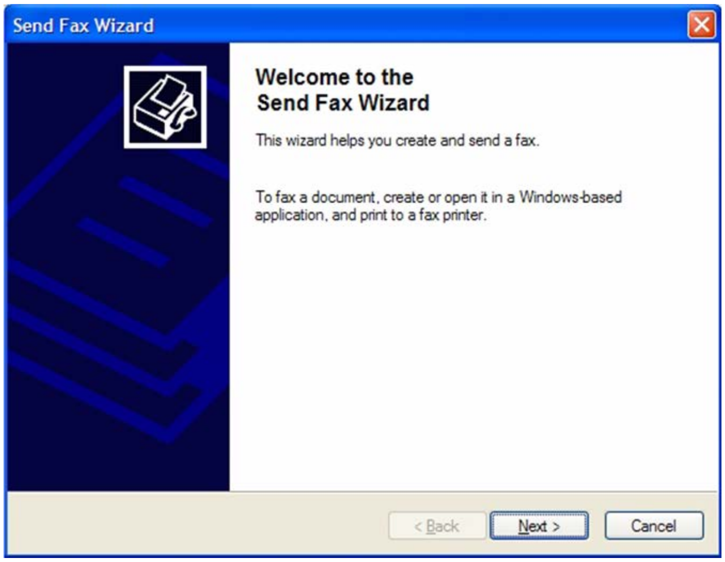
Print: All pages in range

Zoom

Pages per sheet: 1 page

Scale to paper size: No Scaling

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


Send Fax Wizard

Welcome to the Send Fax Wizard

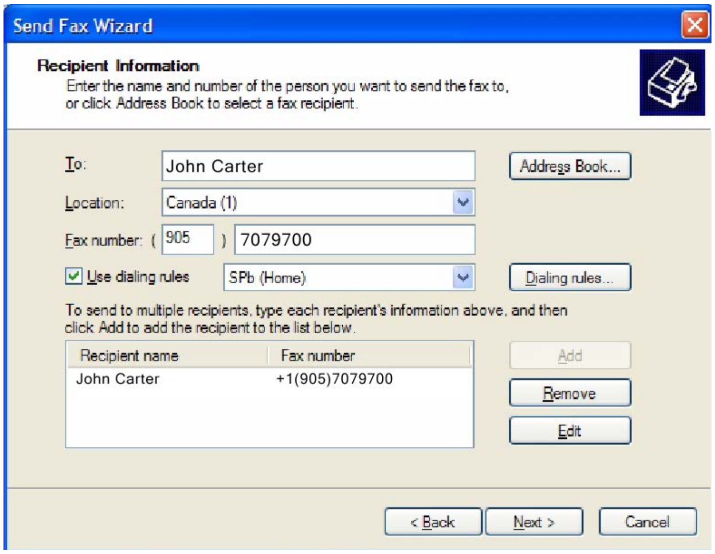
This wizard helps you create and send a fax.

To fax a document, create or open it in a Windows-based application, and print to a fax printer.

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.


Send Fax Wizard

Recipient Information

Enter the name and number of the person you want to send the fax to, or click Address Book to select a fax recipient.

To: John Carter

Location: Canada (1)

Fax number: (905) 7079700

☑ Use dialing rules SPb (Home)

To send to multiple recipients, type each recipient's information above, and then click Add to add the recipient to the list below.

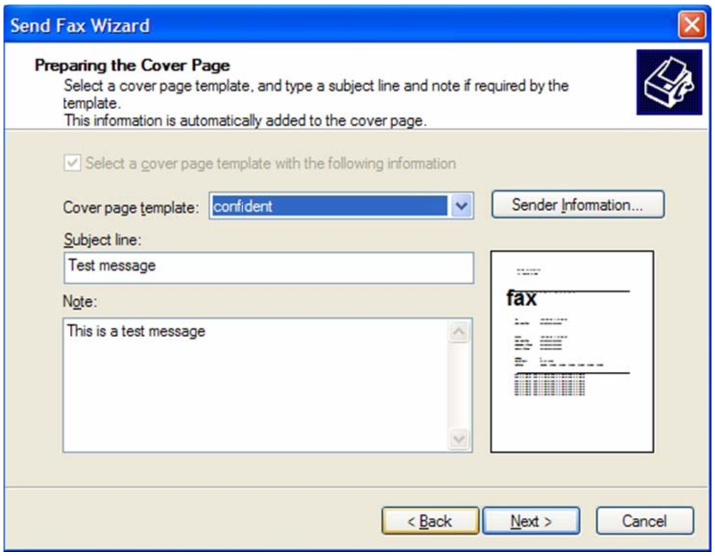
Recipient name	Fax number
John Carter	+1(905)7079700

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.



Send Fax Wizard

Preparing the Cover Page

Select a cover page template, and type a subject line and note if required by the template.
This information is automatically added to the cover page.

☑ Select a cover page template with the following information

Cover page template: confident

Subject line: Test message

Note: This is a test message

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

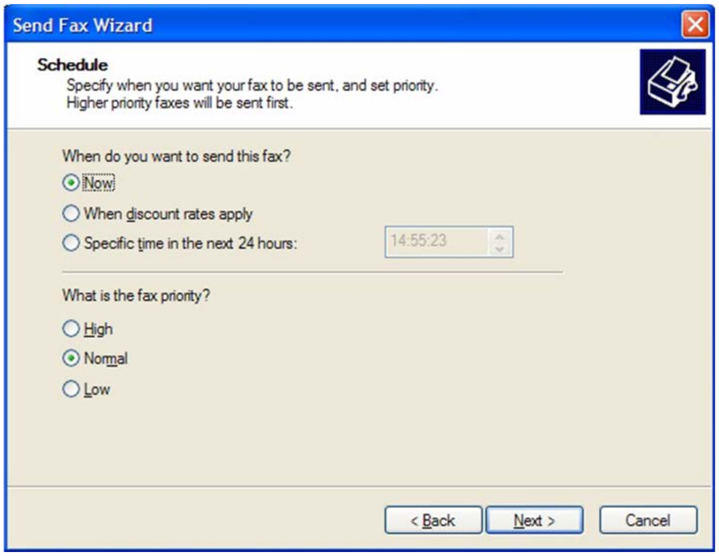
    When discount rates apply - send the fax the next time discount phone rates apply

    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



Send Fax Wizard

Schedule

Specify when you want your fax to be sent, and set priority.
Higher priority faxes will be sent first.

When do you want to send this fax?

● Now

○ When discount rates apply

○ Specific time in the next 24 hours: 14:55:23

What is the fax priority?

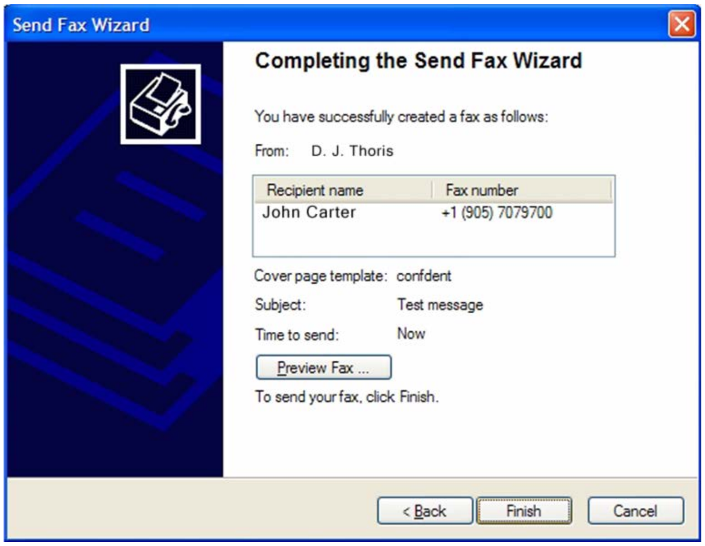
○ High

● Normal

○ Low

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.



Send Fax Wizard

Completing the Send Fax Wizard

You have successfully created a fax as follows:

From: D. J. Thoris

Recipient name	Fax number
John Carter	+1 (905) 7079700

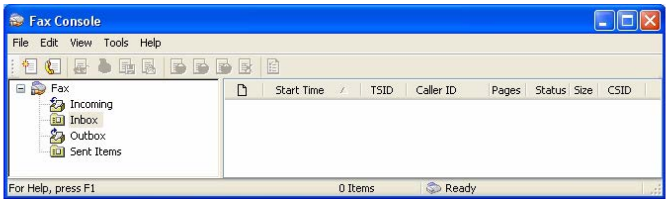
Cover page template: confdent

Subject: Test message

Time to send: Now

To send your fax, click Finish.

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

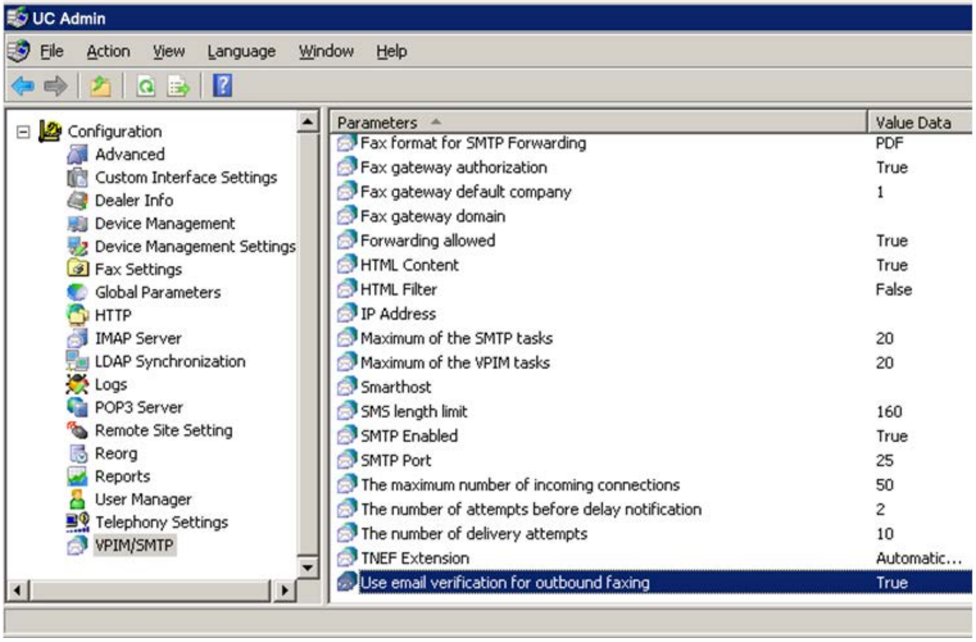
Note: The example shown in this guide uses Gmail. However, this process can be repeated with virtually any email client including web based email, MS Office 365, and MS Exchange.

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's 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**.



Parameters	Value Data
Fax format for SMTP Forwarding	PDF
Fax gateway authorization	True
Fax gateway default company	1
Fax gateway domain	
Forwarding allowed	True
HTML Content	True
HTML Filter	False
IP Address	
Maximum of the SMTP tasks	20
Maximum of the VPIM tasks	20
Smarthost	
SMS length limit	160
SMTP Enabled	True
SMTP Port	25
The maximum number of incoming connections	50
The number of attempts before delay notification	2
The number of delivery attempts	10
TNEF Extension	Automatic...
Use email verification for outbound faxing	True

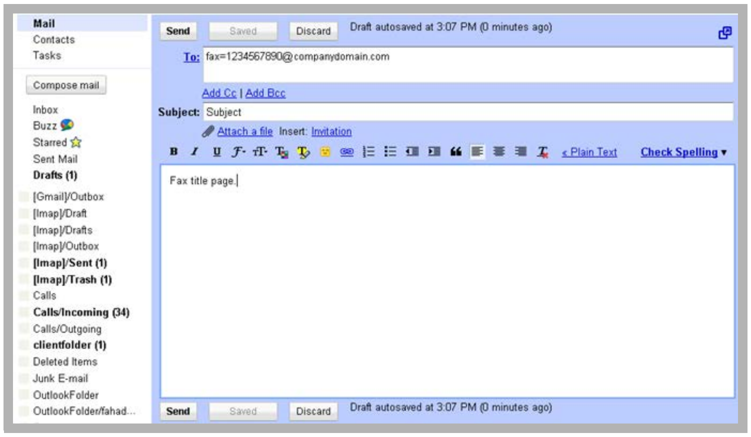
Sending a Fax

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).



Draft autosaved at 3:07 PM (0 minutes ago)

To: fax=1234567890@companydomain.com

Subject: Subject

Fax title page.

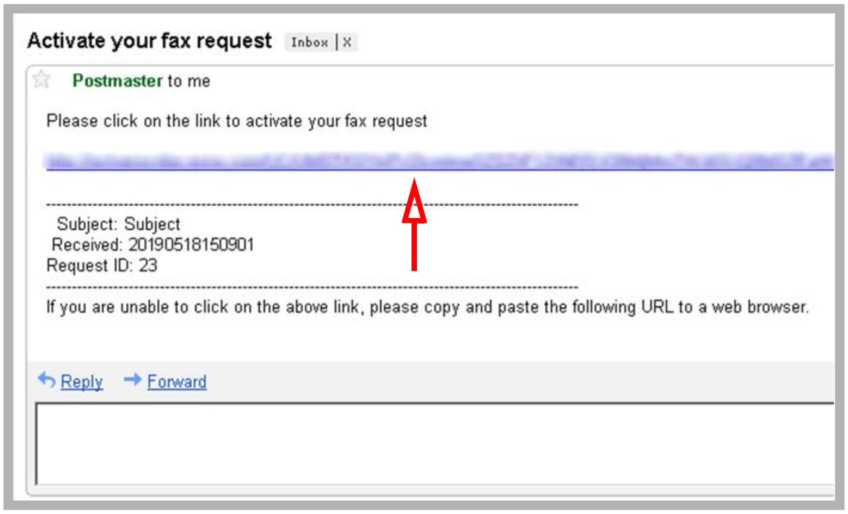
Send the email when you're ready.

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.



Activate your fax request

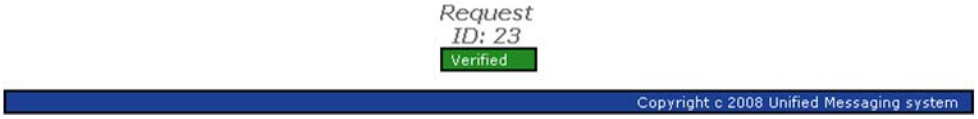
Postmaster to me

Please click on the link to activate your fax request

Subject: Subject
Received: 20190518150901
Request ID: 23

If you are unable to click on the above link, please copy and paste the following URL to a web browser.

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.



Request ID: 23

Verified

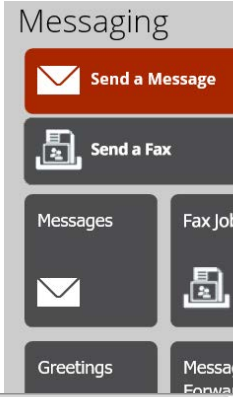
Copyright c 2008 Unified Messaging system

Sending a Fax through Fax Gadget

The Fax Gadget appears. This can be accessed through Web Access directly, or through a link from other web applications such as Avaya iLink Pro.

To send a fax, click **Send a Fax**.

Note: **Send a Fax** will only available if you have a fax board installed on the server to handle fax routing. Otherwise, faxes can be sent by clicking **Send a Message** and setting the outgoing address to **FAX:** followed by the fax number (e.g. fax:9057079700).

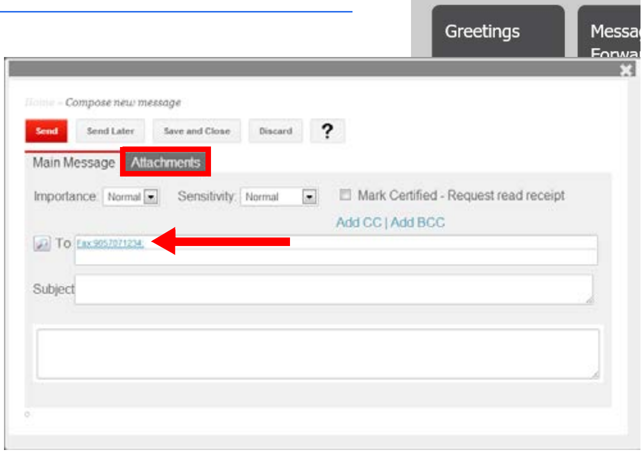


On the **To** field, enter the fax destination number.

It is best to provide all numbers including both country and area code (e.g. 1-123-765-4321).

When you enter the full fax number on this field, the Fax Gadget will automatically add the **Fax:** qualifier to indicate that this is a fax message.

Click on the **Attachments** tab to add content to this fax message. Any attachments to the fax must be in the **PDF** or **TIFF** formats unless the UC server has been specifically setup to support other file types.

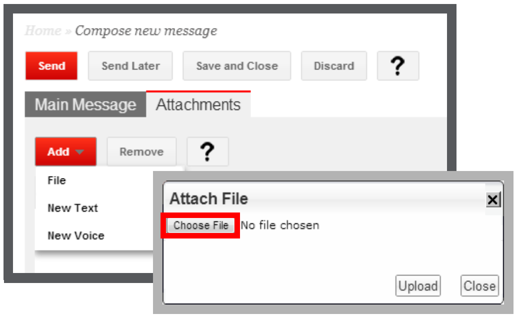


Importance: Normal
Sensitivity: Normal
□ Mark Certified - Request read receipt
To Fax:9057071234;
Subject

Click the **Add** button to open the menu shown here.

Select **File** from the menu and click **Choose File...** to browse for the file to be sent as the fax content.

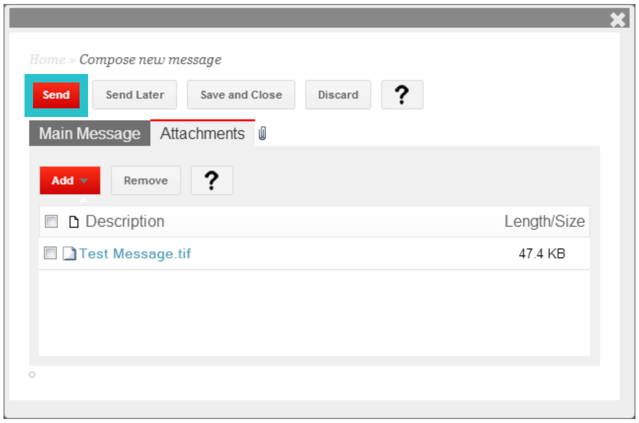
Once the file has been chosen, click **Upload**.



No file chosen

The selected file will now be added as fax content.

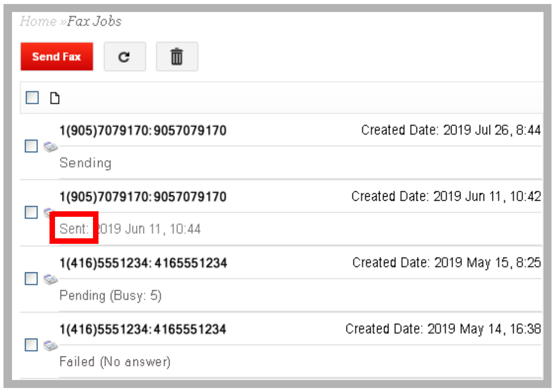
Click **Send** to transmit the fax immediately.



□ Description	Length/Size
□ Test Message.tif	47.4 KB

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.



□ 1(905)7079170: 9057079170 Created Date: 2019 Jul 26, 8:44
Sending

□ 1(905)7079170: 9057079170 Created Date: 2019 Jun 11, 10:42
Sent: 2019 Jun 11, 10:44

□ 1(416)5551234: 4165551234 Created Date: 2019 May 15, 8:25
Pending (Busy: 5)

□ 1(416)5551234: 4165551234 Created Date: 2019 May 14, 16:38
Failed (No answer)

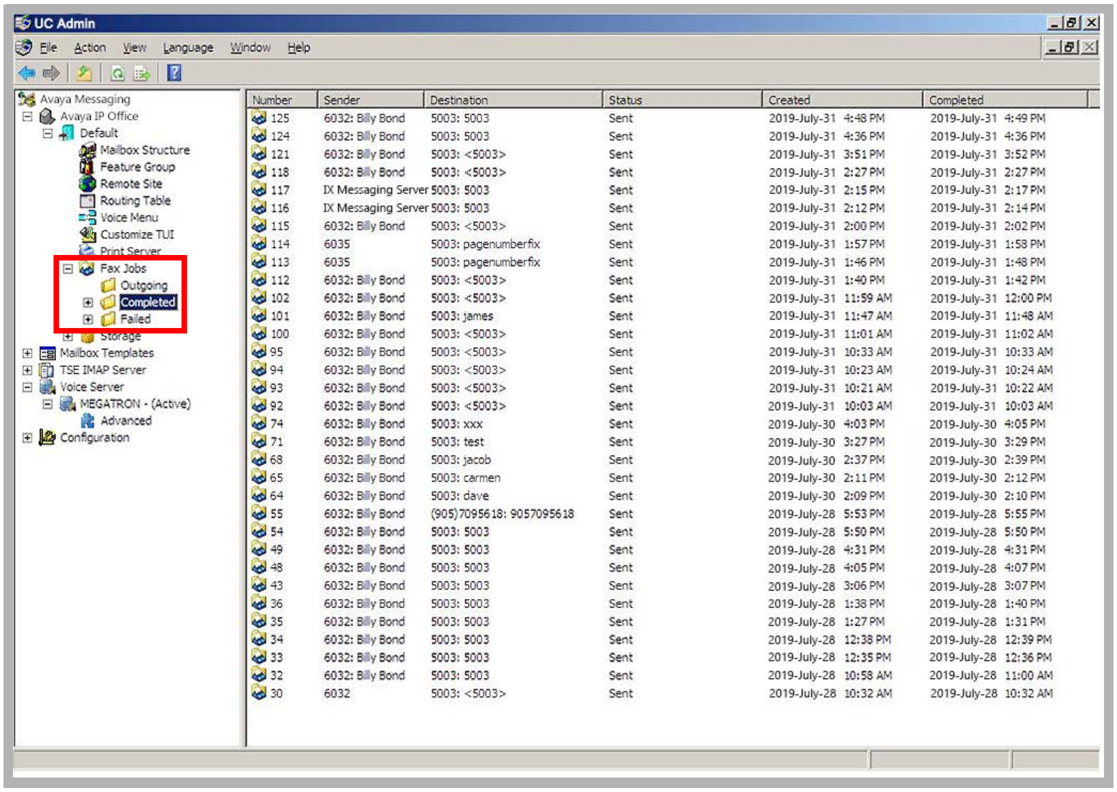
Fax Jobs

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.



Number	Sender	Destination	Status	Created	Completed
125	6032: Billy Bond	5003: 5003	Sent	2019-July-31 4:48 PM	2019-July-31 4:49 PM
124	6032: Billy Bond	5003: 5003	Sent	2019-July-31 4:36 PM	2019-July-31 4:36 PM
121	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 3:51 PM	2019-July-31 3:52 PM
118	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 2:27 PM	2019-July-31 2:27 PM
117	IX Messaging Server	5003: 5003	Sent	2019-July-31 2:15 PM	2019-July-31 2:17 PM
116	IX Messaging Server	5003: 5003	Sent	2019-July-31 2:12 PM	2019-July-31 2:14 PM
115	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 2:00 PM	2019-July-31 2:02 PM
114	6035	5003: pagenumberfix	Sent	2019-July-31 1:57 PM	2019-July-31 1:58 PM
113	6035	5003: pagenumberfix	Sent	2019-July-31 1:46 PM	2019-July-31 1:48 PM
112	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 1:40 PM	2019-July-31 1:42 PM
102	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 11:59 AM	2019-July-31 12:00 PM
101	6032: Billy Bond	5003: james	Sent	2019-July-31 11:47 AM	2019-July-31 11:48 AM
100	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 11:01 AM	2019-July-31 11:02 AM
95	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 10:33 AM	2019-July-31 10:33 AM
94	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 10:23 AM	2019-July-31 10:24 AM
93	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 10:21 AM	2019-July-31 10:22 AM
92	6032: Billy Bond	5003: <5003>	Sent	2019-July-31 10:03 AM	2019-July-31 10:03 AM
74	6032: Billy Bond	5003: xxx	Sent	2019-July-30 4:03 PM	2019-July-30 4:05 PM
71	6032: Billy Bond	5003: test	Sent	2019-July-30 3:27 PM	2019-July-30 3:29 PM
68	6032: Billy Bond	5003: jacob	Sent	2019-July-30 2:37 PM	2019-July-30 2:39 PM
65	6032: Billy Bond	5003: carmen	Sent	2019-July-30 2:11 PM	2019-July-30 2:12 PM
64	6032: Billy Bond	5003: dave	Sent	2019-July-30 2:09 PM	2019-July-30 2:10 PM
55	6032: Billy Bond	(905)7095618: 9057095618	Sent	2019-July-28 5:53 PM	2019-July-28 5:55 PM
54	6032: Billy Bond	5003: 5003	Sent	2019-July-28 5:50 PM	2019-July-28 5:50 PM
49	6032: Billy Bond	5003: 5003	Sent	2019-July-28 4:31 PM	2019-July-28 4:31 PM
48	6032: Billy Bond	5003: 5003	Sent	2019-July-28 4:05 PM	2019-July-28 4:07 PM
43	6032: Billy Bond	5003: 5003	Sent	2019-July-28 3:06 PM	2019-July-28 3:07 PM
36	6032: Billy Bond	5003: 5003	Sent	2019-July-28 1:38 PM	2019-July-28 1:40 PM
35	6032: Billy Bond	5003: 5003	Sent	2019-July-28 1:27 PM	2019-July-28 1:31 PM
34	6032: Billy Bond	5003: 5003	Sent	2019-July-28 12:38 PM	2019-July-28 12:39 PM
33	6032: Billy Bond	5003: 5003	Sent	2019-July-28 12:35 PM	2019-July-28 12:36 PM
32	6032: Billy Bond	5003: 5003	Sent	2019-July-28 10:58 AM	2019-July-28 11:00 AM
30	6032	5003: <5003>	Sent	2019-July-28 10:32 AM	2019-July-28 10:32 AM

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 the transmission of the fax was completed.

21 DIALOGIC SR140 FAX INTEGRATION

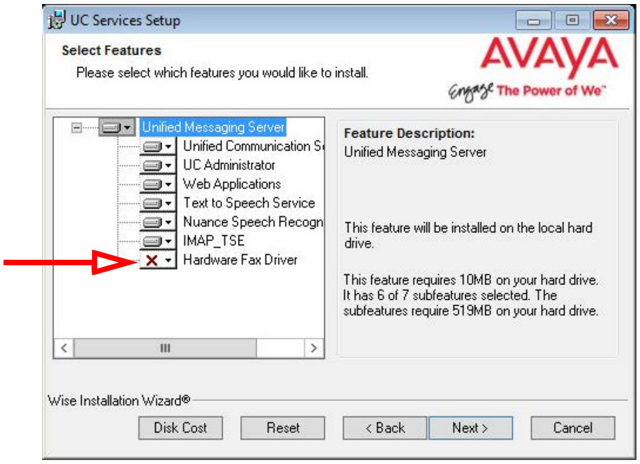
In This Chapter:

Introduction

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

Pre-Requisites

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.


UC Services Setup

Select Features

Please select which features you would like to install.

- Unified Messaging Server
  - Unified Communication S
  - UC Administrator
  - Web Applications
  - Text to Speech Service
  - Nuance Speech Recogn
  - IMAP_TSE
  - ✗ Hardware Fax Driver

Feature Description:
Unified Messaging Server

This feature will be installed on the local hard drive.

This feature requires 10MB on your hard drive. It has 6 of 7 subfeatures selected. The subfeatures require 519MB on your hard drive.

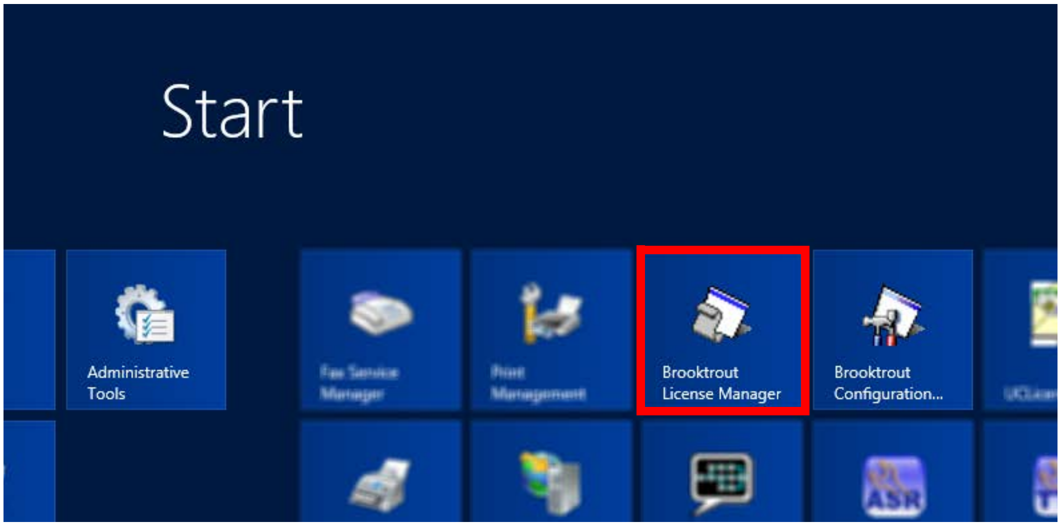
Configuration

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.

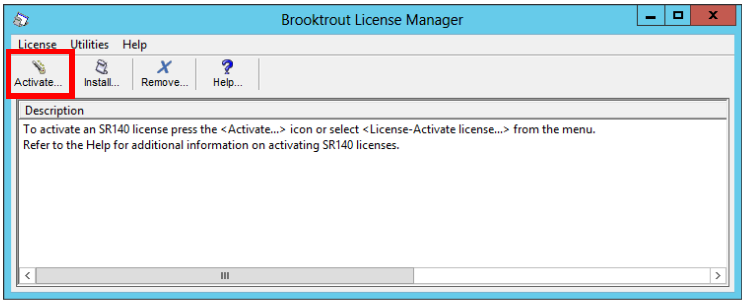
The following procedures must be performed on each computer that is running the SR140 software.

License Manager

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



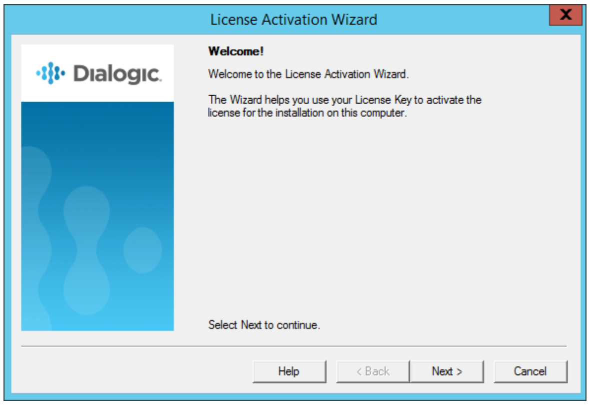
2. Enable the SR140 license by clicking on the **Activate** button.



To activate an SR140 license press the <Activate...> icon or select <License-Activate license...> from the menu.
Refer to the Help for additional information on activating SR140 licenses.

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**.



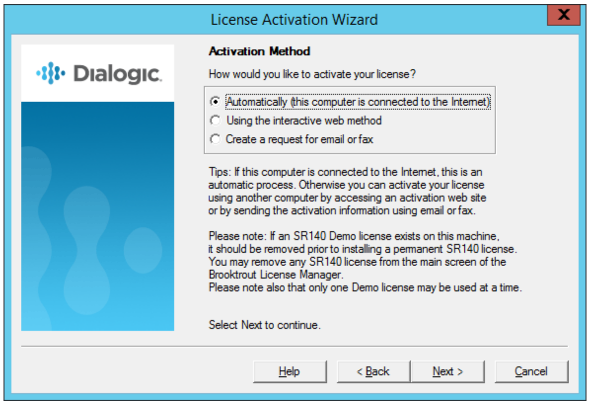
Welcome!

Welcome to the License Activation Wizard.

The Wizard helps you use your License Key to activate the license for the installation on this computer.

Select Next to continue.

4. Make sure that **Automatically** is selected as the **Activation Method**, then click **Next**.



Activation Method

How would you like to activate your license?

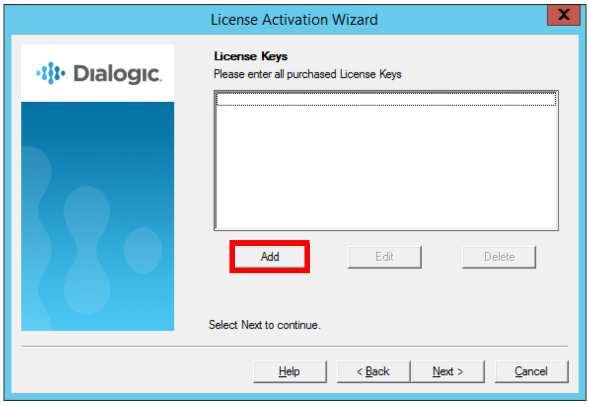
● Automatically (this computer is connected to the Internet)
○ Using the interactive web method
○ Create a request for email or fax

Tips: If this computer is connected to the Internet, this is an automatic process. Otherwise you can activate your license using another computer by accessing an activation web site or by sending the activation information using email or fax.

Please note: If an SR140 Demo license exists on this machine, it should be removed prior to installing a permanent SR140 license. You may remove any SR140 license from the main screen of the Brooktrout License Manager.
Please note also that only one Demo license may be used at a time.

Select Next to continue.

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

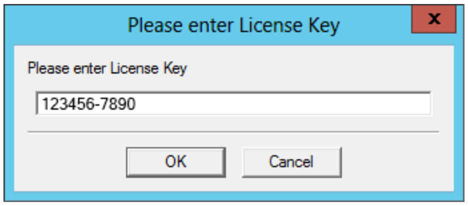


License Keys

Please enter all purchased License Keys

Select Next to continue.

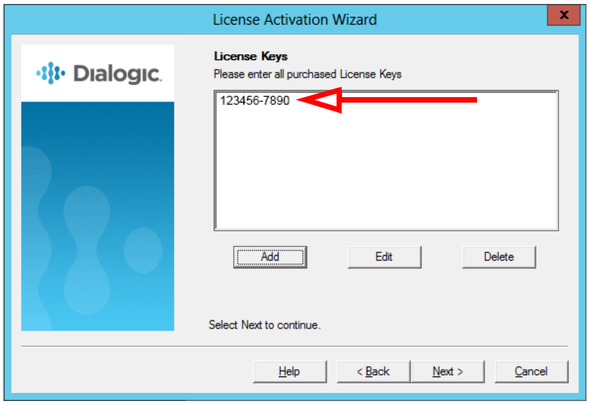
6. Enter the SR140 license key number that came with the fax software package. Click **OK** when ready.



Please enter License Key

123456-7890

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



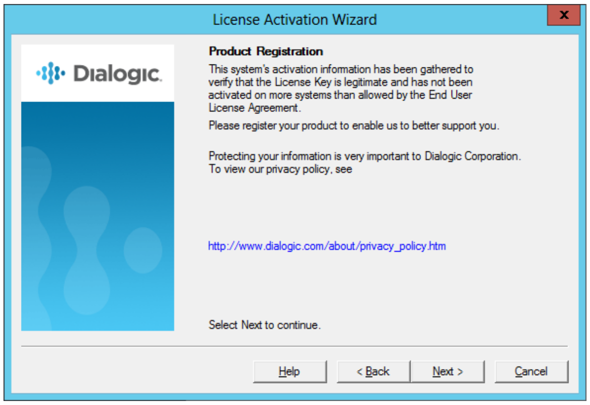
License Keys

Please enter all purchased License Keys

123456-7890

Select Next to continue.

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



Product Registration

This system's activation information has been gathered to verify that the License Key is legitimate and has not been activated on more systems than allowed by the End User License Agreement.

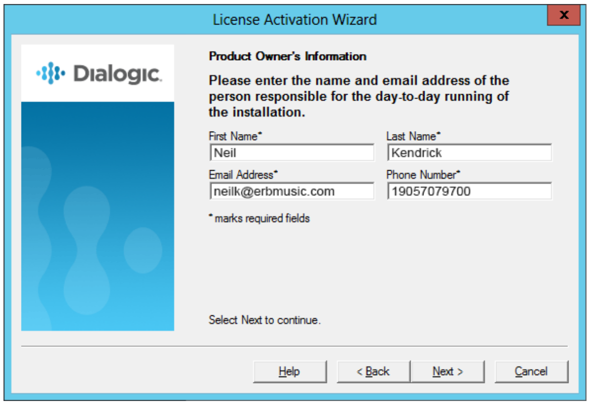
Please register your product to enable us to better support you.

Protecting your information is very important to Dialogic Corporation. To view our privacy policy, see

http://www.dialogic.com/about/privacy_policy.htm

Select Next to continue.

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



Product Owner's Information

Please enter the name and email address of the person responsible for the day-to-day running of the installation.

First Name* Neil

Last Name* Kendrick

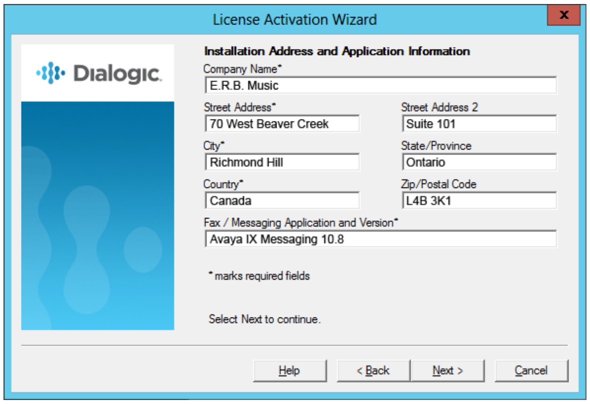
Email Address* neilk@erbmusic.com

Phone Number* 19057079700

* marks required fields

Select Next to continue.

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



License Activation Wizard

Installation Address and Application Information

Company Name*: E.R.B. Music

Street Address*: 70 West Beaver Creek

Street Address 2: Suite 101

City*: Richmond Hill

State/Province: Ontario

Country*: Canada

Zip/Postal Code: L4B 3K1

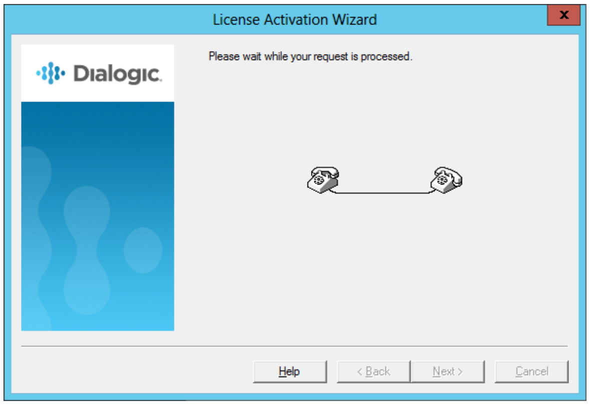
Fax / Messaging Application and Version*: Avaya IX Messaging 10.8

*marks required fields

Select 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 will be activated.

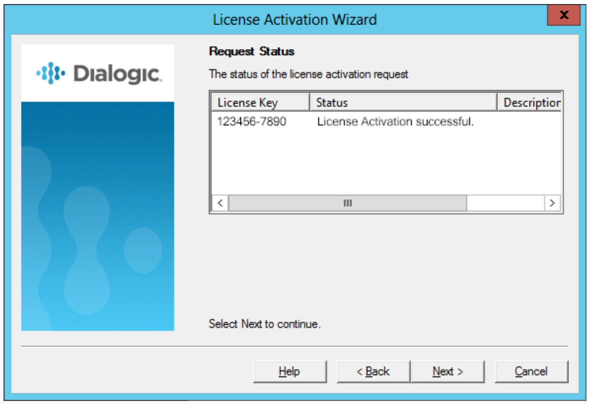
When it has finished, click **Next** to continue.



License Activation Wizard

Please wait while your request is processed.

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



License Activation Wizard

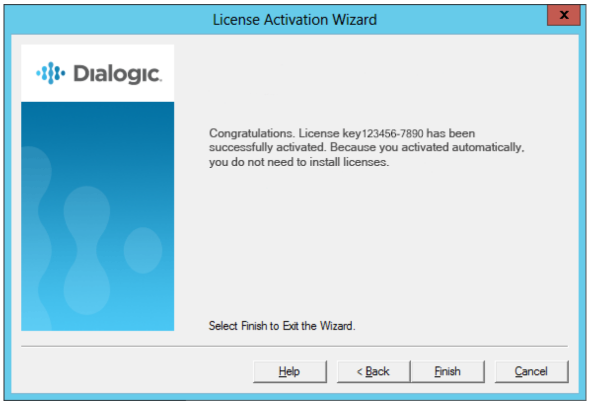
Request Status

The status of the license activation request

License Key	Status	Descriptior
123456-7890	License Activation successful.	

Select Next to continue.

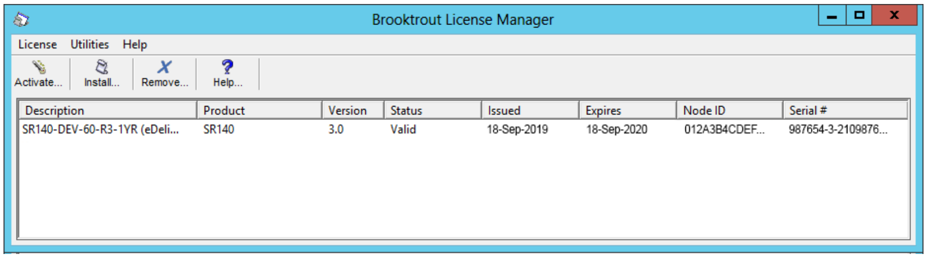
13. Click **Next** to complete the activation Wizard.



Congratulations. License key123456-7890 has been successfully activated. Because you activated automatically, you do not need to install licenses.

Select Finish to Exit the Wizard.

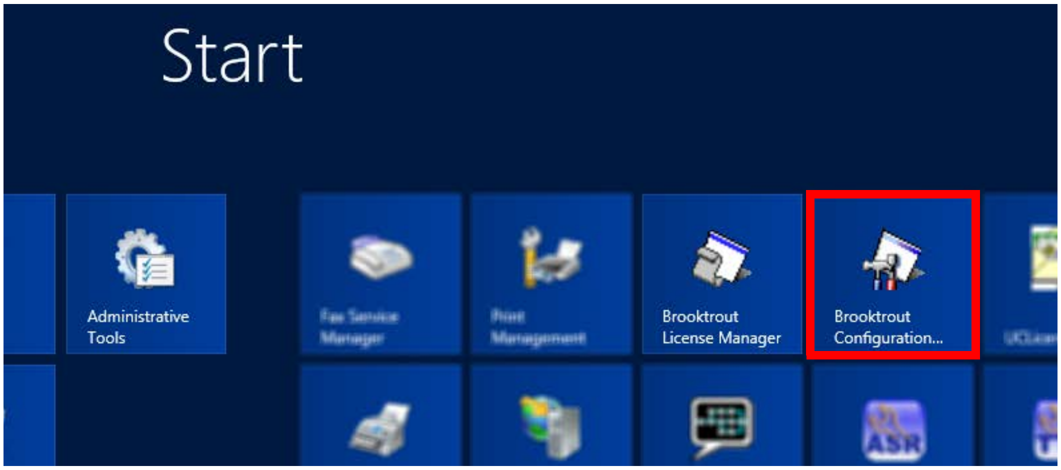
14. The added license appears in the **Brooktrout License Manager**.



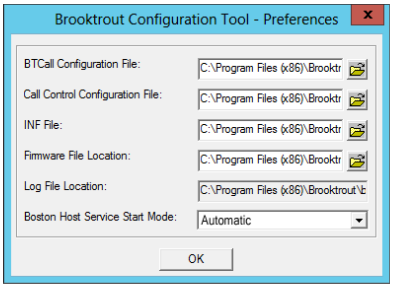
Description	Product	Version	Status	Issued	Expires	Node ID	Serial #
SR140-DEV-60-R3-1YR (eDeli...	SR140	3.0	Valid	18-Sep-2019	18-Sep-2020	012A3B4CDEF...	987654-3-2109876...

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**.



Brooktrout Configuration Tool - Preferences

BTCall Configuration File: C:\Program Files (x86)\Brooktr

Call Control Configuration File: C:\Program Files (x86)\Brooktr

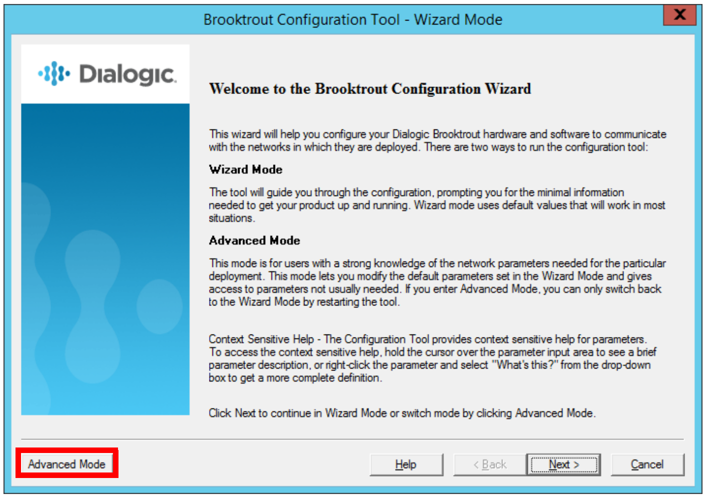
INF File: C:\Program Files (x86)\Brooktr

Firmware File Location: C:\Program Files (x86)\Brooktr

Log File Location: C:\Program Files (x86)\Brooktrout\t

Boston Host Service Start Mode: Automatic

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



Brooktrout Configuration Tool - Wizard Mode

Welcome to the Brooktrout Configuration Wizard

This wizard will help you configure your Dialogic Brooktrout hardware and software to communicate with the networks in which they are deployed. There are two ways to run the configuration tool:

Wizard Mode

The tool will guide you through the configuration, prompting you for the minimal information needed to get your product up and running. Wizard mode uses default values that will work in most situations.

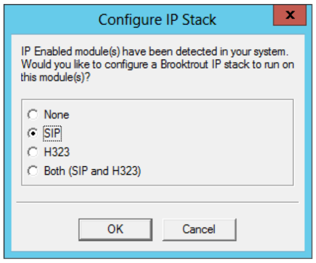
Advanced Mode

This mode is for users with a strong knowledge of the network parameters needed for the particular deployment. This mode lets you modify the default parameters set in the Wizard Mode and gives access to parameters not usually needed. If you enter Advanced Mode, you can only switch back to the Wizard Mode by restarting the tool.

Context Sensitive Help - The Configuration Tool provides context sensitive help for parameters. To access the context sensitive help, hold the cursor over the parameter input area to see a brief parameter description, or right-click the parameter and select "What's this?" from the drop-down box to get a more complete definition.

Click Next to continue in Wizard Mode or switch mode by clicking Advanced Mode.

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



Configure IP Stack

IP Enabled module(s) have been detected in your system. Would you like to configure a Brooktrout IP stack to run on this module(s)?

○ None
● SIP
○ H323
○ Both (SIP and H323)

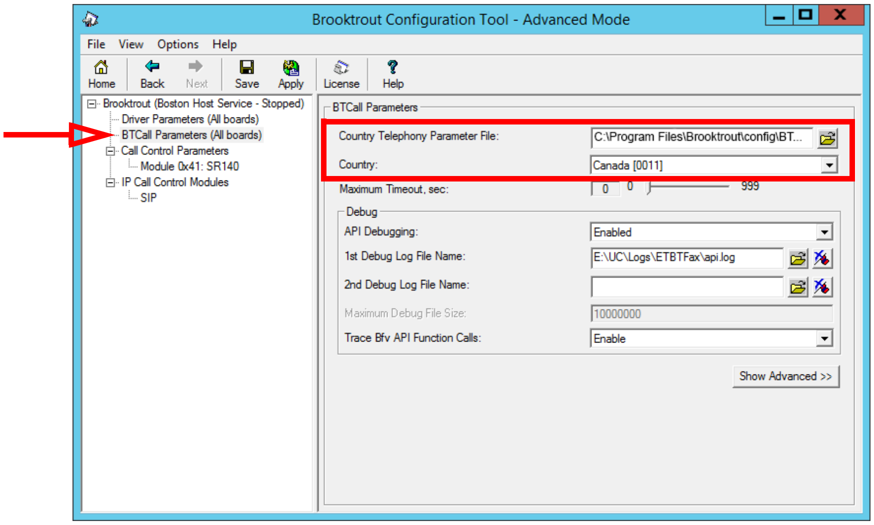
1. Select **BTCall Parameters (All boards)**.

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.



Brooktrout Configuration Tool - Advanced Mode

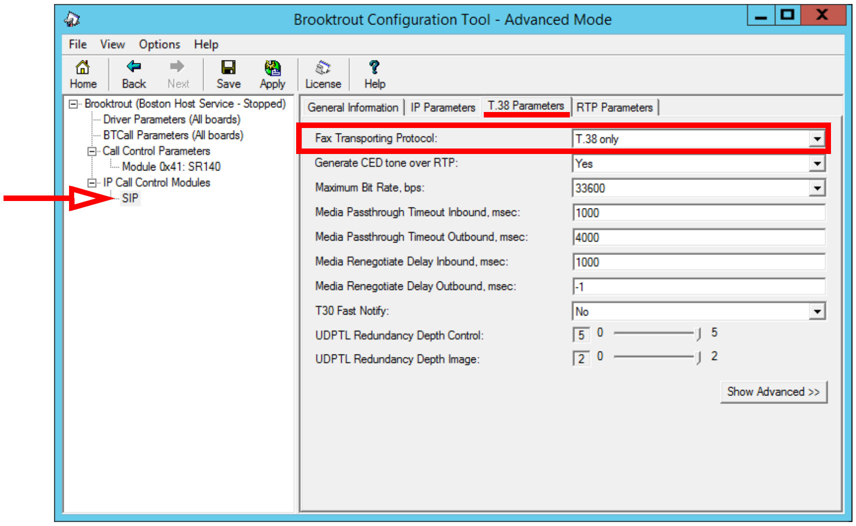
BTCall Parameters

Country Telephony Parameter File: C:\Program Files\Brooktrout\config\BT...
Country: Canada [0011]
Maximum Timeout, sec: 0 (0 – 999)

Debug
API Debugging: Enabled
1st Debug Log File Name: E:\UC\Logs\ETBTFax\api.log
2nd Debug Log File Name:
Maximum Debug File Size: 10000000
Trace Bfv API Function Calls: Enable

2. 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**.

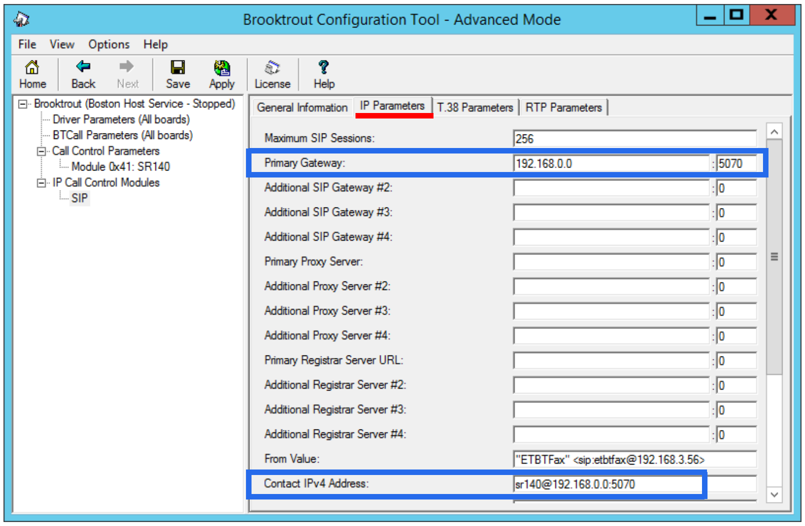


Brooktrout Configuration Tool - Advanced Mode

Fax Transporting Protocol: T.38 only
Generate CED tone over RTP: Yes
Maximum Bit Rate, bps: 33600
Media Passthrough Timeout Inbound, msec: 1000
Media Passthrough Timeout Outbound, msec: 4000
Media Renegotiate Delay Inbound, msec: 1000
Media Renegotiate Delay Outbound, msec: -1
T30 Fast Notify: No
UDPTL Redundancy Depth Control: 5 (0 – 5)
UDPTL Redundancy Depth Image: 2 (0 – 2)

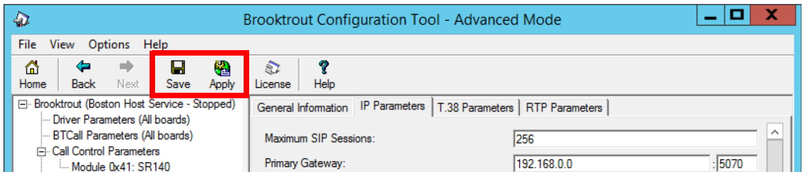
3. Move to the **IP Parameters** tab.

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



Maximum SIP Sessions: 256
Primary Gateway: 192.168.0.0 : 5070
Additional SIP Gateway #2: : 0
Additional SIP Gateway #3: : 0
Additional SIP Gateway #4: : 0
Primary Proxy Server: : 0
Additional Proxy Server #2: : 0
Additional Proxy Server #3: : 0
Additional Proxy Server #4: : 0
Primary Registrar Server URL: : 0
Additional Registrar Server #2: : 0
Additional Registrar Server #3: : 0
Additional Registrar Server #4: : 0
From Value: "ETBTFax" <sip:etbtfax@192.168.3.56>
Contact IPv4 Address: sr140@192.168.0.0:5070

4. 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).
5. Click **Save** to confirm the changes.
6. Click **Apply** to restart all affected services.



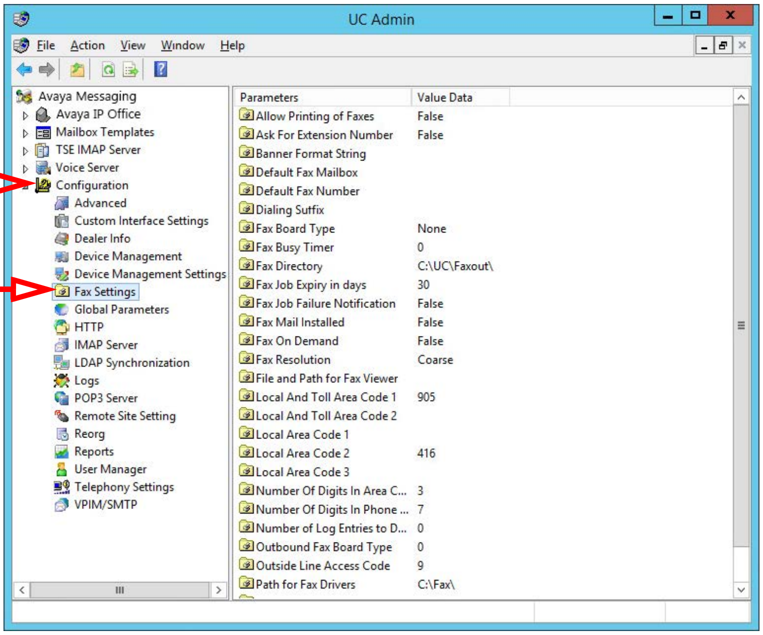
Maximum SIP Sessions: 256
Primary Gateway: 192.168.0.0 : 5070

The configuration of the SR140 software is complete.

Avaya Messaging Configuration

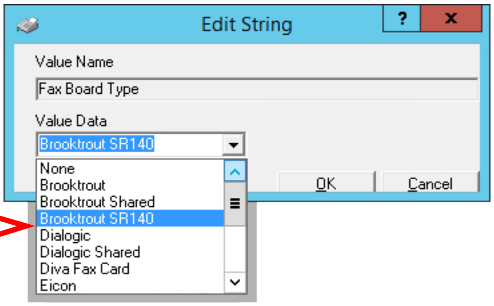
The voice server must be configured to send faxes to the SR140, and to prepare to receive them across the same channel. A setting for incoming, and another for outgoing faxes must be configured on the server using Avaya Messaging Admin.

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**.



Parameters	Value Data
Allow Printing of Faxes	False
Ask For Extension Number	False
Banner Format String	
Default Fax Mailbox	
Default Fax Number	
Dialing Suffix	
Fax Board Type	None
Fax Busy Timer	0
Fax Directory	C:\UC\Faxout\
Fax Job Expiry in days	30
Fax Job Failure Notification	False
Fax Mail Installed	False
Fax On Demand	False
Fax Resolution	Coarse
File and Path for Fax Viewer	
Local And Toll Area Code 1	905
Local And Toll Area Code 2	
Local Area Code 1	
Local Area Code 2	416
Local Area Code 3	
Number Of Digits In Area C...	3
Number Of Digits In Phone ...	7
Number of Log Entries to D...	0
Outbound Fax Board Type	0
Outside Line Access Code	9
Path for Fax Drivers	C:\Fax\

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**.



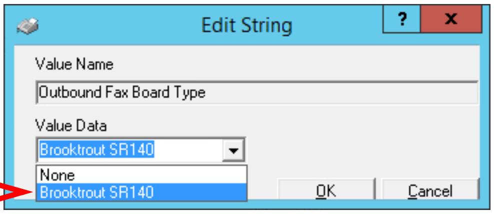
Value Name

Fax Board Type

Value Data

Brooktrout SR140

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



Value Name

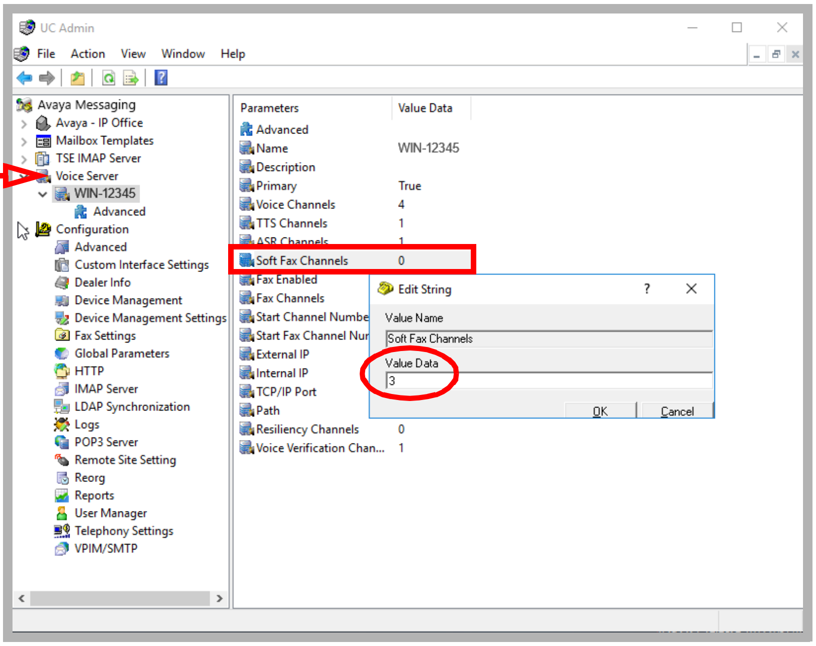
Outbound Fax Board Type

Value Data

Brooktrout SR140

Hint: If faxes will only be **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.



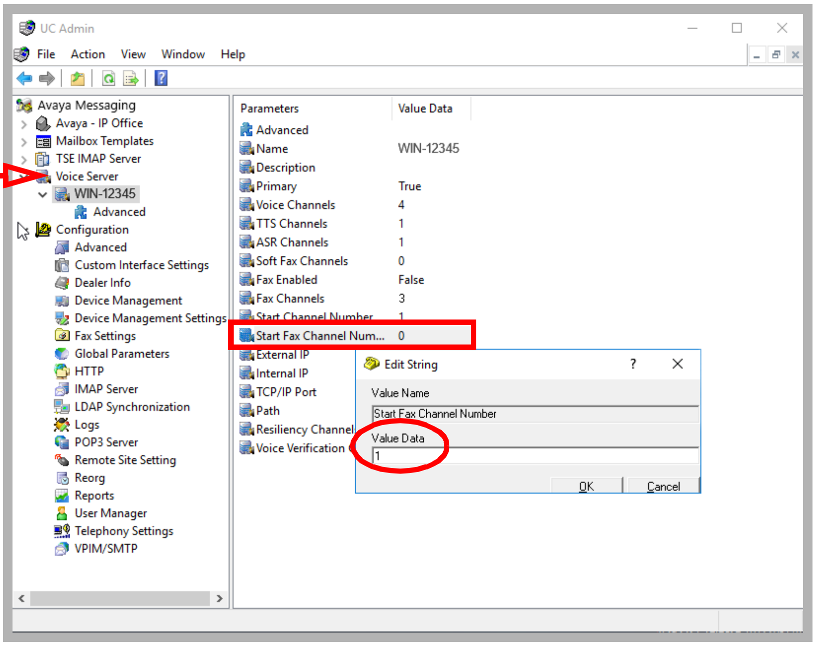
Parameters	Value Data
Advanced	
Name	WIN-12345
Description	
Primary	True
Voice Channels	4
TTS Channels	1
ASR Channels	1
Soft Fax Channels	0
Fax Enabled	
Fax Channels	
Start Channel Numbe	
Start Fax Channel Nur	
External IP	
Internal IP	
TCP/IP Port	
Path	
Resiliency Channels	0
Voice Verification Chan...	1

Edit String

Value Name: Soft Fax Channels

Value Data: 3

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



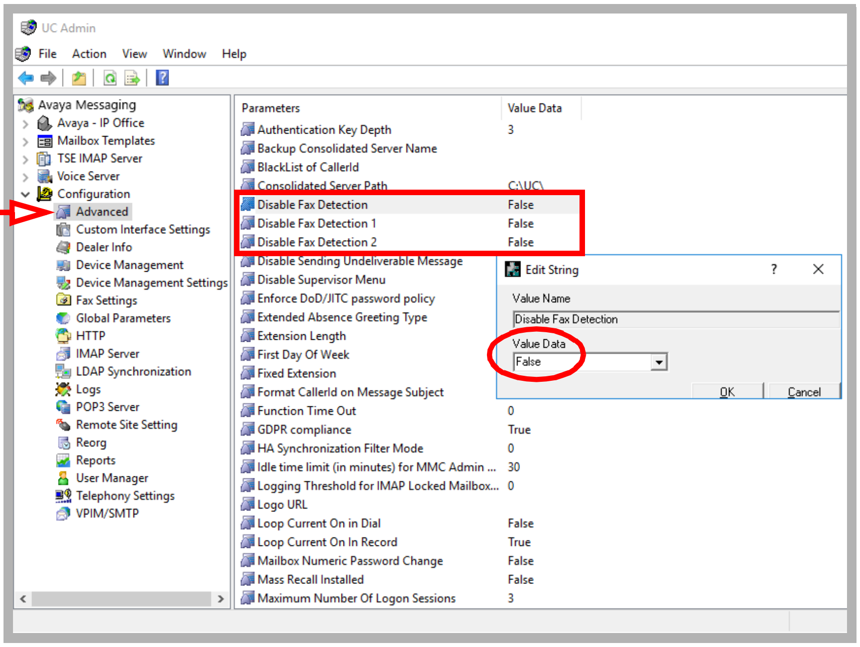
Parameters	Value Data
Advanced	
Name	WIN-12345
Description	
Primary	True
Voice Channels	4
TTS Channels	1
ASR Channels	1
Soft Fax Channels	0
Fax Enabled	False
Fax Channels	3
Start Channel Number	1
Start Fax Channel Num...	0
External IP	
Internal IP	
TCP/IP Port	
Path	
Resiliency Channel	
Voice Verification	

Edit String

Value Name: Start Fax Channel Number

Value Data: 1

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

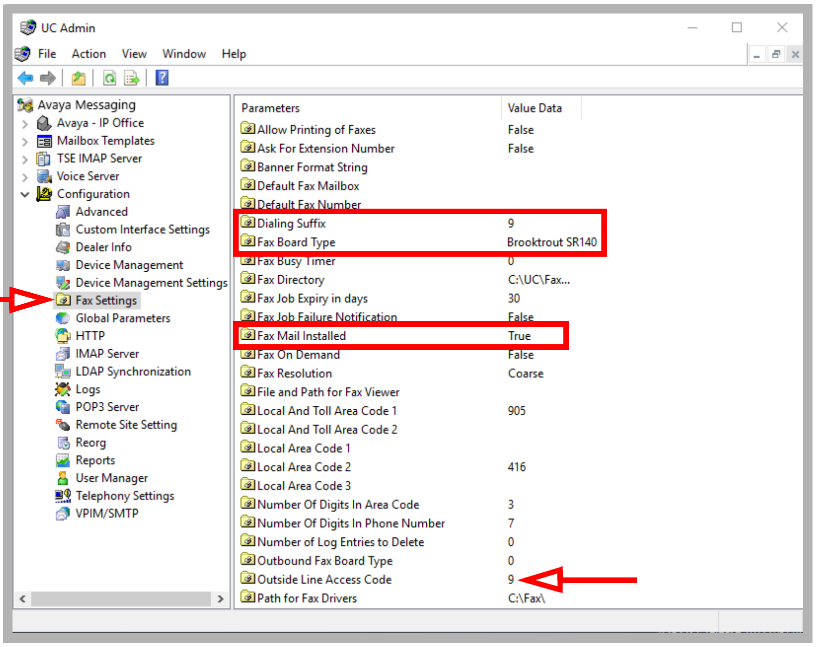


Parameters	Value Data
Authentication Key Depth	3
Backup Consolidated Server Name	
BlackList of CallerId	
Consolidated Server Path	C:\UC\
Disable Fax Detection	False
Disable Fax Detection 1	False
Disable Fax Detection 2	False
Disable Sending Undeliverable Message	
Disable Supervisor Menu	
Enforce DoD/JITC password policy	
Extended Absence Greeting Type	
Extension Length	
First Day Of Week	
Fixed Extension	
Format CallerId on Message Subject	
Function Time Out	0
GDPR compliance	True
HA Synchronization Filter Mode	0
Idle time limit (in minutes) for MMC Admin ...	30
Logging Threshold for IMAP Locked Mailbox...	0
Logo URL	
Loop Current On in Dial	False
Loop Current On In Record	True
Mailbox Numeric Password Change	False
Mass Recall Installed	False
Maximum Number Of Logon Sessions	3

Value Name
Disable Fax Detection
Value Data
False

8. Go to **Configuration > Fax Settings**.

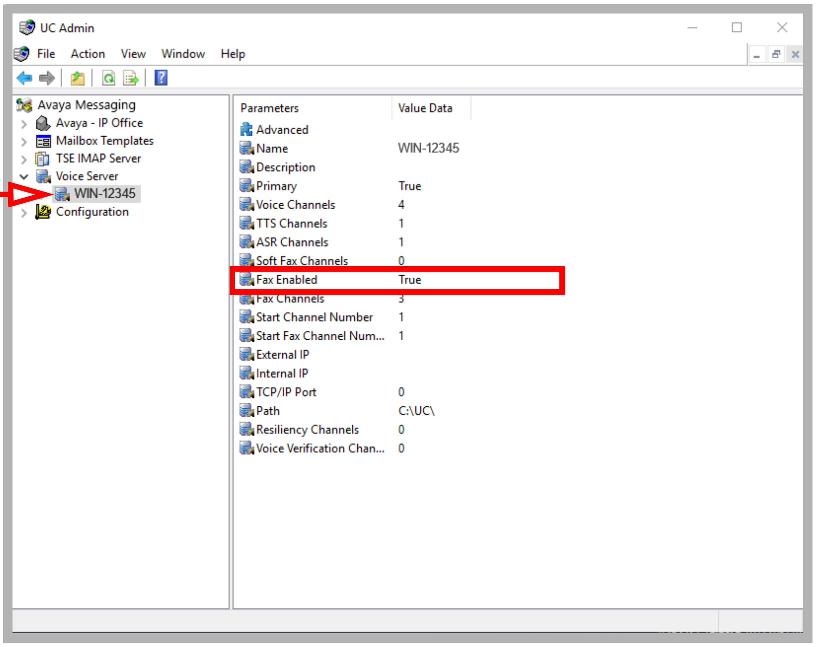
   Double-click **Dialing Suffix** and set the **Value Data** field match your **Outside Line Access Code**. Click **OK**.
   Double-click **Fax Board Type** and set the **Value Data** field to **Brooktrout SR140**. Click **OK**.
   Double-click **Fax Mail Installed** and set the **Value Data** field to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



Parameters	Value Data
Allow Printing of Faxes	False
Ask For Extension Number	False
Banner Format String	
Default Fax Mailbox	
Default Fax Number	
Dialing Suffix	9
Fax Board Type	Brooktrout SR140
Fax Busy Timer	0
Fax Directory	C:\UC\Fax...
Fax Job Expiry in days	30
Fax Job Failure Notification	False
Fax Mail Installed	True
Fax On Demand	False
Fax Resolution	Coarse
File and Path for Fax Viewer	
Local And Toll Area Code 1	905
Local And Toll Area Code 2	
Local Area Code 1	
Local Area Code 2	416
Local Area Code 3	
Number Of Digits In Area Code	3
Number Of Digits In Phone Number	7
Number of Log Entries to Delete	0
Outbound Fax Board Type	0
Outside Line Access Code	9
Path for Fax Drivers	C:\Fax\

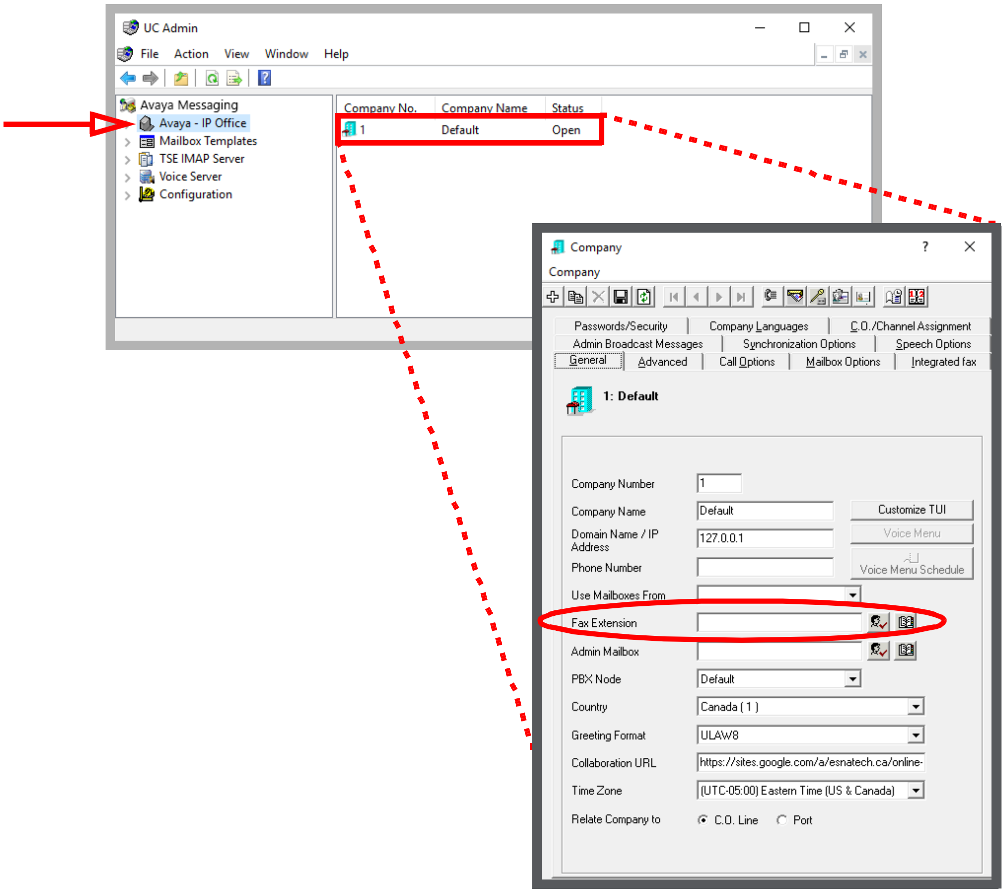
9. Restart the voice server.

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



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. Setup 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**.

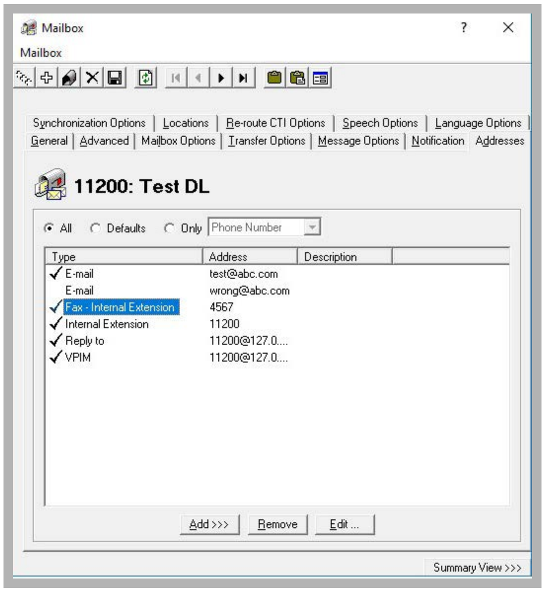


Company No.	Company Name	Status
1	Default	Open

1: Default

Company Number	1
Company Name	Default
Domain Name / IP Address	127.0.0.1
Phone Number	
Use Mailboxes From	
Fax Extension	
Admin Mailbox	
PBX Node	Default
Country	Canada (1)
Greeting Format	ULAW8
Collaboration URL	https://sites.google.com/a/esnatech.ca/online-
Time Zone	(UTC-05:00) Eastern Time (US & Canada)
Relate Company to	● C.O. Line ○ Port

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.



11200: Test DL

● All ○ Defaults ○ Only Phone Number

Type	Address	Description
✓ E-mail	test@abc.com	
E-mail	wrong@abc.com	
✓ Fax - Internal Extension	4567	
✓ Internal Extension	11200	
✓ Reply to	11200@127.0....	
✓ VPIM	11200@127.0....	

Monitoring Channel Activity

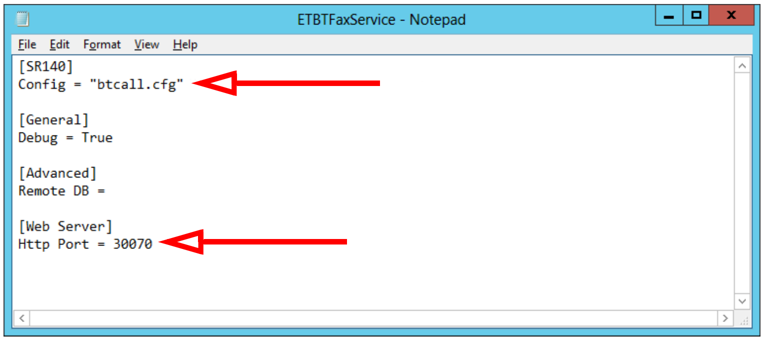
Setup

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.



```
[SR140]
Config = "btcall.cfg"

[General]
Debug = True

[Advanced]
Remote DB =

[Web Server]
Http Port = 30070
```

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.

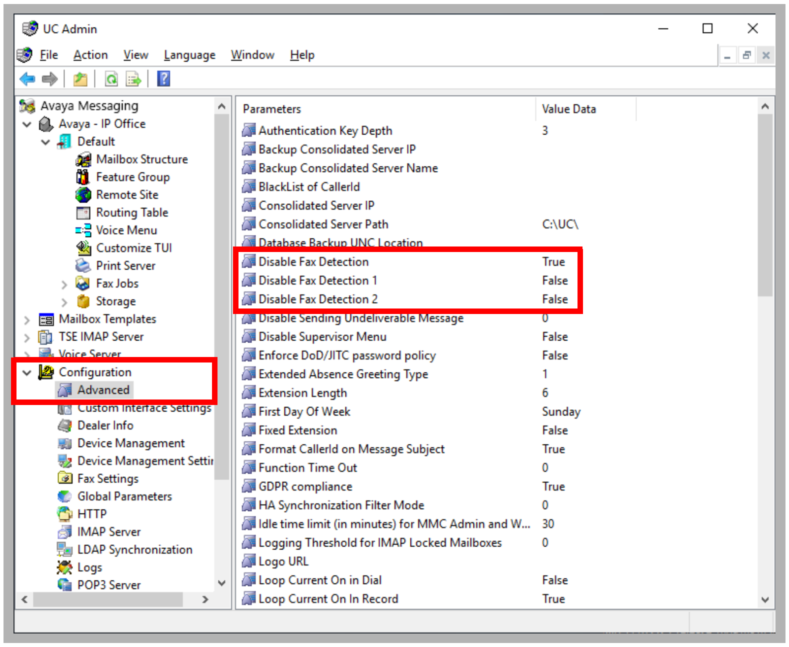
During the auto attendant playback, and also during the personal message playback, the system monitors the call for the presence of a fax signal.

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.

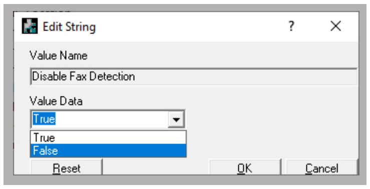
Configuring Avaya Messaging

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



Parameters	Value Data
Authentication Key Depth	3
Backup Consolidated Server IP	
Backup Consolidated Server Name	
BlackList of CallerId	
Consolidated Server IP	
Consolidated Server Path	C:\UC\
Database Backup UNC Location	
Disable Fax Detection	True
Disable Fax Detection 1	False
Disable Fax Detection 2	False
Disable Sending Undeliverable Message	0
Disable Supervisor Menu	False
Enforce DoD/JITC password policy	False
Extended Absence Greeting Type	1
Extension Length	6
First Day Of Week	Sunday
Fixed Extension	False
Format CallerId on Message Subject	True
Function Time Out	0
GDPR compliance	True
HA Synchronization Filter Mode	0
Idle time limit (in minutes) for MMC Admin and W...	30
Logging Threshold for IMAP Locked Mailboxes	0
Logo URL	
Loop Current On in Dial	False
Loop Current On In Record	True

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**.

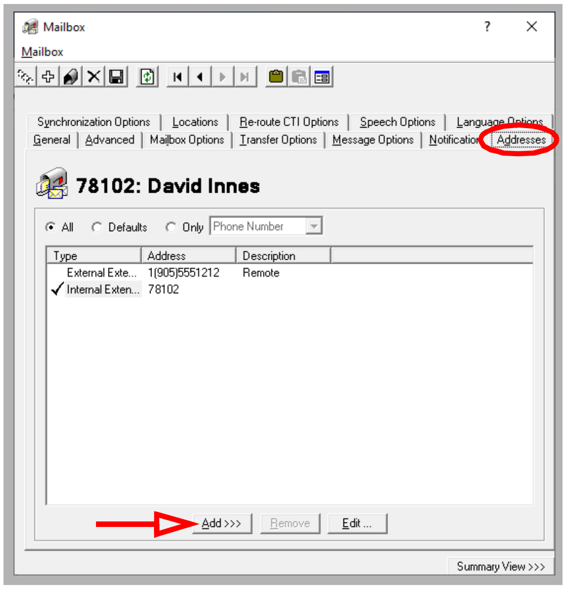


Value Name
Disable Fax Detection

Value Data
True

True
False

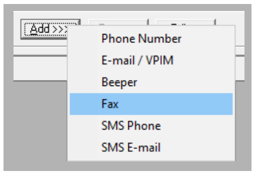
5. Open a user mailbox and go to the **Addresses** tab.


Mailbox
Mailbox
Synchronization Options | Locations | Re-route CTI Options | Speech Options | Language Options
General | Advanced | Mailbox Options | Transfer Options | Message Options | Notification | Addresses
All
Defaults
Only
Phone Number
Add >>>
Remove
Edit ...
Summary View >>>

78102: David Innes

Type	Address	Description
External Exte...	1(905)5551212	Remote
✓ Internal Exten...	78102	

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



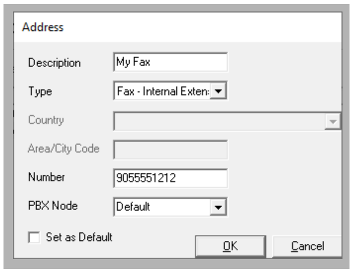
7. Provide a human readable description for the fax connection.
Type: Select one of the following options from the dropdown list.

   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.

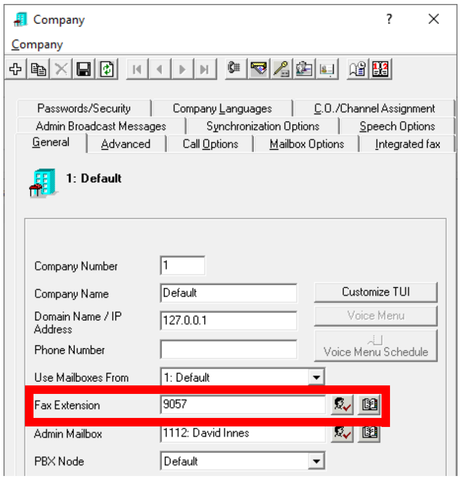
   When ready, click **OK**.



Description: My Fax
Type: Fax - Internal Exten:
Number: 9055551212
PBX Node: Default

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**.


Company
Company
Passwords/Security | Company Languages | C.O./Channel Assignment
Admin Broadcast Messages | Synchronization Options | Speech Options
General | Advanced | Call Options | Mailbox Options | Integrated fax
Customize TUI
Voice Menu
Voice Menu Schedule

1: Default

Company Number: 1
Company Name: Default
Domain Name / IP Address: 127.0.0.1
Phone Number:
Use Mailboxes From: 1: Default
Fax Extension: 9057
Admin Mailbox: 1112: David Innes
PBX Node: Default

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, enable 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. Communication Manager must be configured to use the 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.

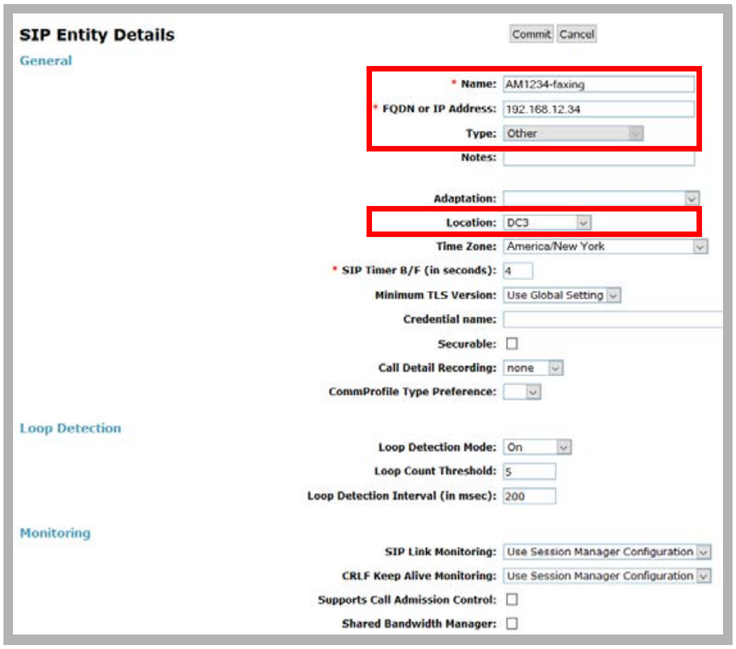
The Caller hits the Send button on the fax machine as soon as call is answered. The Avaya Messaging server detects the fax tone and initiates a call transfer (SIP REFER) to user 78102’s internal fax extension (52002) via Session Manager.

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.



SIP Entity Details

General

* Name:	AM1234-faxing
* FQDN or IP Address:	192.168.12.34
Type:	Other
Notes:	
Adaptation:	
Location:	DC3
Time Zone:	America/New York
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	none
CommProfile Type Preference:	

Loop Detection

Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

Monitoring

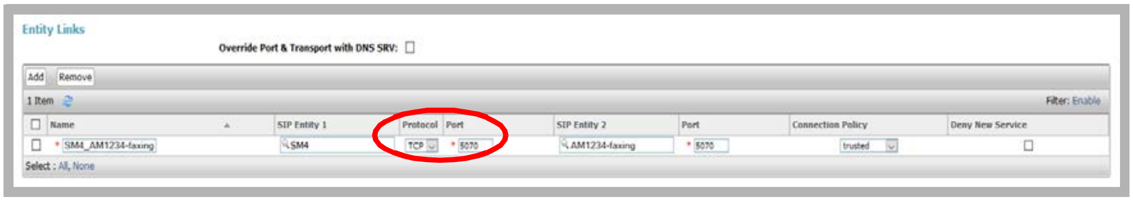
SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration
Supports Call Admission Control:	□
Shared Bandwidth Manager:	□

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

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* SM4_AM1234-faxing	SM4	TCP	* 5070	AM1234-faxing	* 5070	trusted	□

Select : All, None

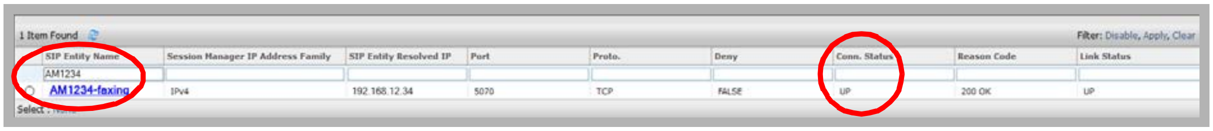
Entity Links: Use port **5070** and the **TCP** protocol to route to the Avaya Messaging server SR140 faxboard.

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**.



1 Item Found

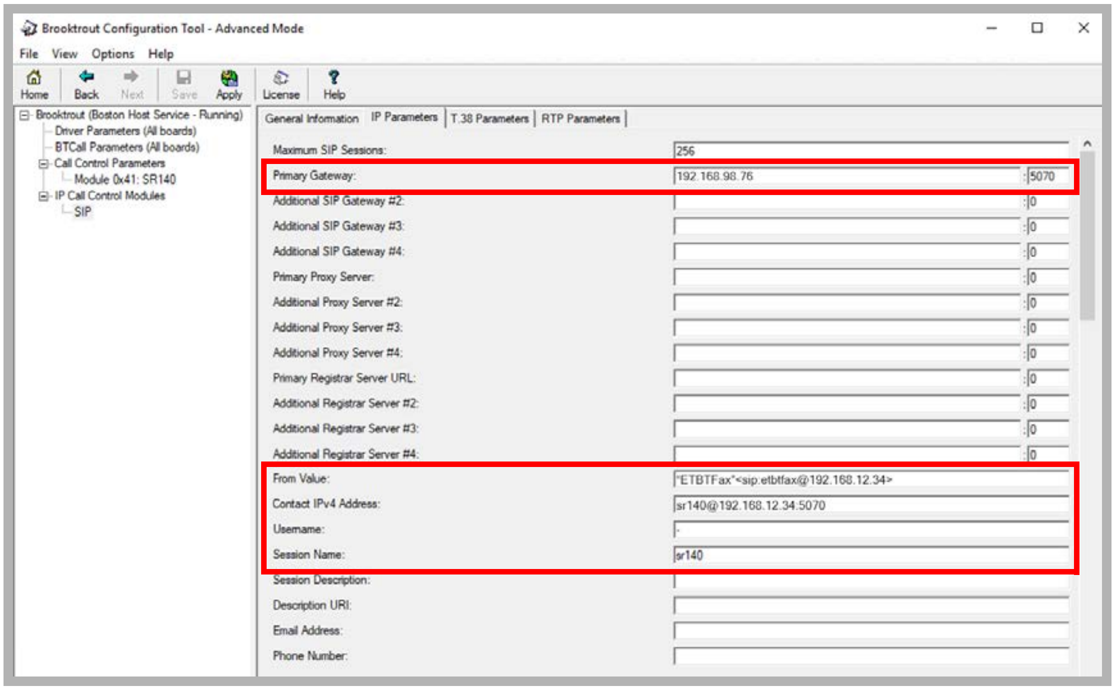
Filter: Disable, Apply, Clear

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
	AM1234								
○	AM1234-faxing	IPv4	192.168.12.34	5070	TCP	FALSE	UP	200 OK	UP

Select : None

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.



Maximum SIP Sessions:	256	
Primary Gateway:	192.168.98.76	5070
Additional SIP Gateway #2:		0
Additional SIP Gateway #3:		0
Additional SIP Gateway #4:		0
Primary Proxy Server:		0
Additional Proxy Server #2:		0
Additional Proxy Server #3:		0
Additional Proxy Server #4:		0
Primary Registrar Server URL:		0
Additional Registrar Server #2:		0
Additional Registrar Server #3:		0
Additional Registrar Server #4:		0
From Value:	"ETBTFax"<sip:etbtfax@192.168.12.34>	
Contact IPv4 Address:	sr140@192.168.12.34:5070	
Username:	-	
Session Name:	sr140	
Session Description:		
Description URI:		
Email Address:		
Phone Number:		

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.

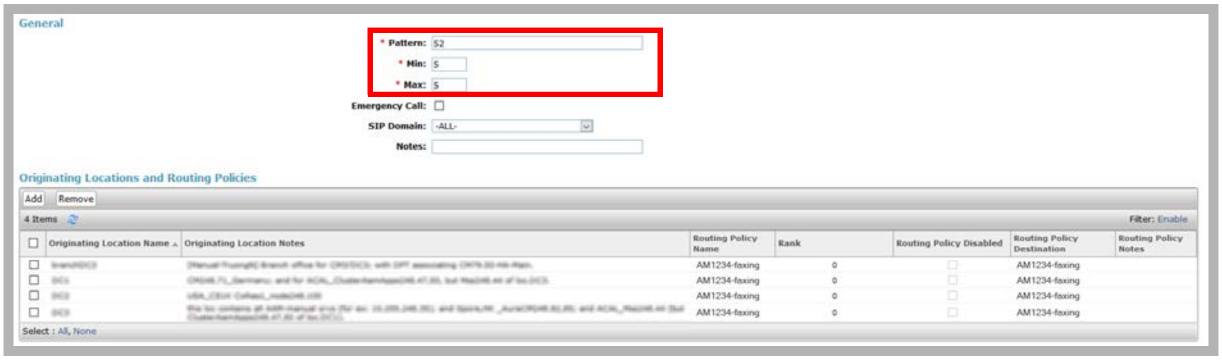
Session Name: Type **sr140** here.

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.



General

* Pattern: 52
* Min: 5
* Max: 5

Emergency Call: □
SIP Domain: -ALL-
Notes:

Originating Locations and Routing Policies

4 Items

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	[redacted]	[redacted]	AM1234-faxing	0	□	AM1234-faxing	
□	[redacted]	[redacted]	AM1234-faxing	0	□	AM1234-faxing	
□	[redacted]	[redacted]	AM1234-faxing	0	□	AM1234-faxing	
□	[redacted]	[redacted]	AM1234-faxing	0	□	AM1234-faxing	

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

1. Create a Mailbox for the Fax Extension

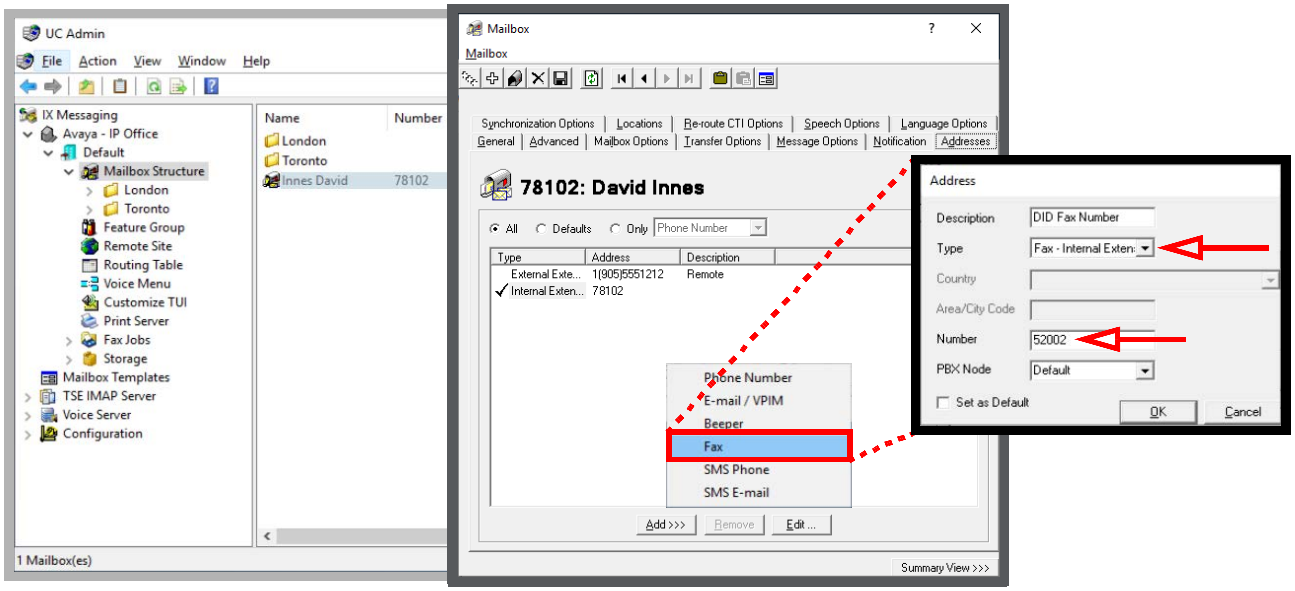
Launch Avaya Messaging Admin and open the user's mailbox at the **Addresses** tab.

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**.



Name	Number
London	
Toronto	
Innes David	78102

78102: David Innes

Type	Address	Description
External Exte...	1(905)5551212	Remote
✓ Internal Exten...	78102	

Description: DID Fax Number

Type: Fax - Internal Exten:

Number: 52002

PBX Node: Default

Note: The Fax number must begin with the prefix created in the **Dial Pattern**.

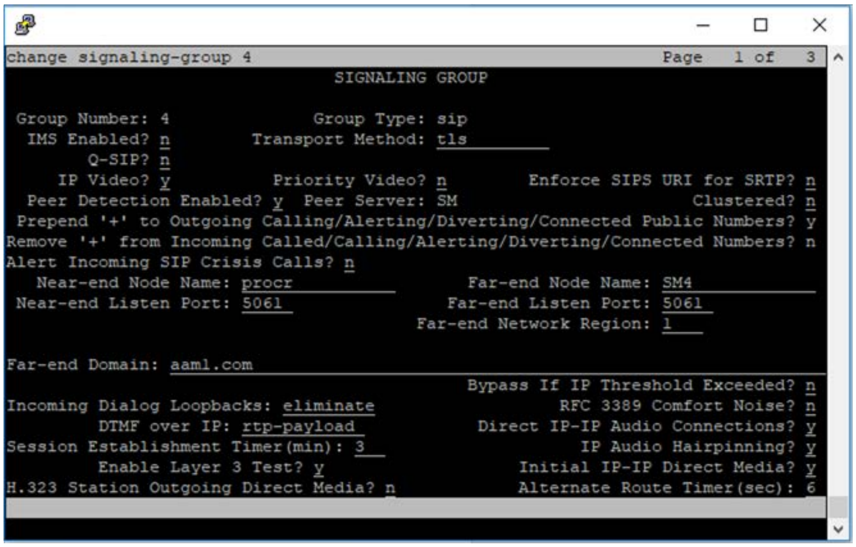
Note: Each mailbox must have a unique fax extension. In this example, mailboxes 78103 and 78104 have the fax internal extension numbers 52003 and 52004 respectively.

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**.

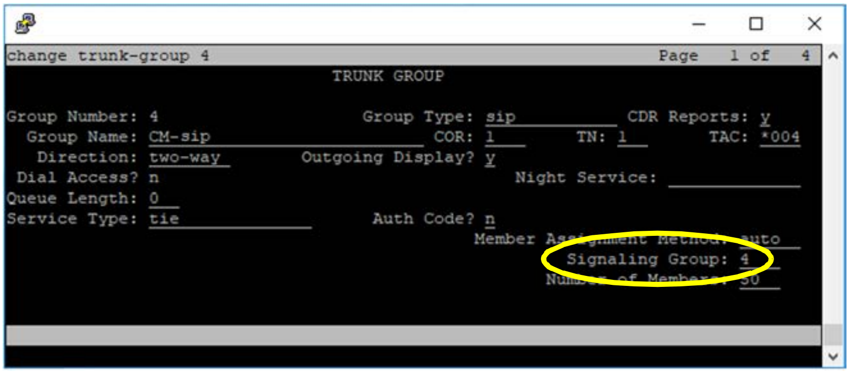


```
change signaling-group 4                                        Page   1 of   3
                                SIGNALING GROUP

 Group Number: 4             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n
     IP Video? y           Priority Video? n        Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                     Far-end Node Name: SM4
 Near-end Listen Port: 5061                    Far-end Listen Port: 5061
                                            Far-end Network Region: 1

Far-end Domain: aaml.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? y
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

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.

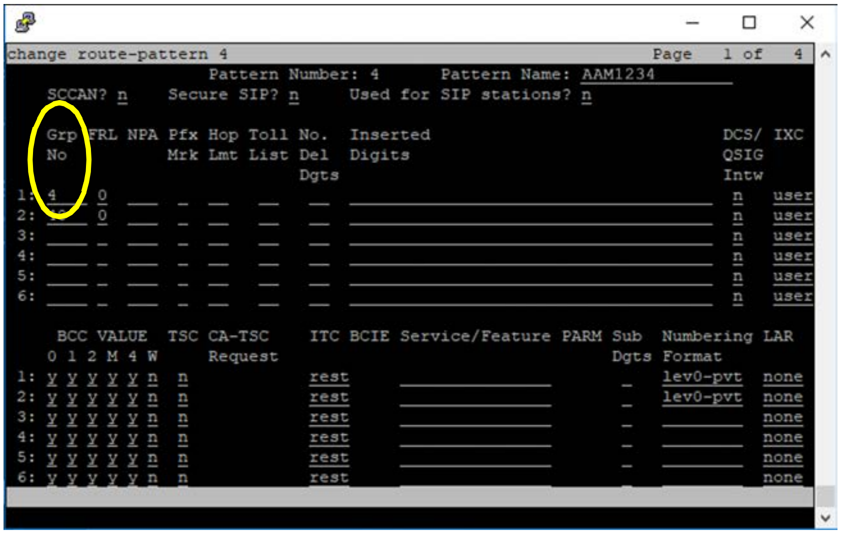


```
change trunk-group 4                                            Page   1 of   4
                                TRUNK GROUP

Group Number: 4                    Group Type: sip            CDR Reports: y
  Group Name: CM-sip                      COR: 1          TN: 1        TAC: *004
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                          Member Assignment Method: auto
                                                   Signaling Group: 4
                                                 Number of Members: 50
```

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.

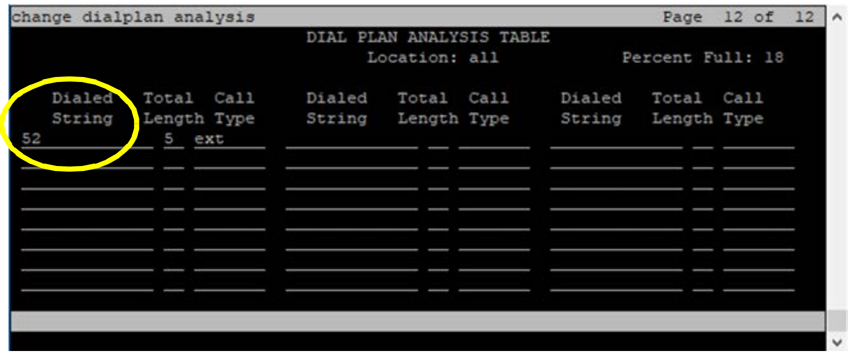


```
change route-pattern 4                                          Page   1 of   4
                          Pattern Number: 4      Pattern Name: AAM1234
     SCCAN? n     Secure SIP? n     Used for SIP stations? n

     Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
     No          Mrk Lmt List Del  Digits                                  QSIG
                              Dgts                                         Intw
  1: 4    0                                                                  n   user
  2:      0                                                                  n   user
  3:                                                                         n   user
  4:                                                                         n   user
  5:                                                                         n   user
  6:                                                                         n   user

      BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
     0 1 2 M 4 W     Request                                 Dgts Format
  1: y y y y y n  n            rest                          _    lev0-pvt  none
  2: y y y y y n  n            rest                          _    lev0-pvt  none
  3: y y y y y n  n            rest                          _              none
  4: y y y y y n  n            rest                          _              none
  5: y y y y y n  n            rest                          _              none
  6: y y y y y n  n            rest                                         none
```

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.

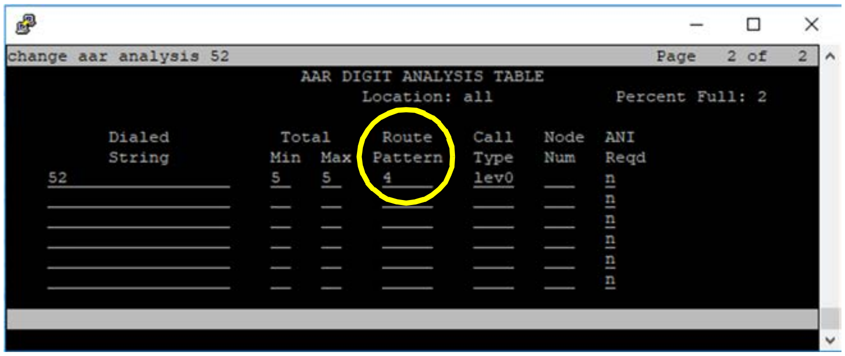


```
change dialplan analysis                                          Page  12 of  12
                              DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 18

         Dialed    Total  Call       Dialed    Total  Call       Dialed    Total  Call
         String    Length Type       String    Length Type       String    Length Type
   52                5    ext
```

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.

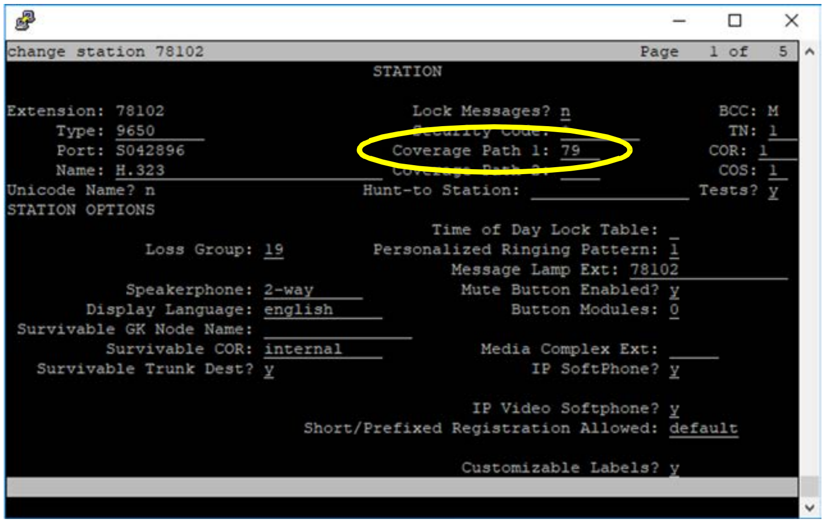


```
change aar analysis 52                                          Page   2 of   2
                          AAR DIGIT ANALYSIS TABLE
                                Location: all             Percent Full: 2

             Dialed            Total    Route    Call   Node  ANI
             String           Min  Max  Pattern  Type   Num   Reqd
          52                  5    5     4       lev0         n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
```

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.



```
change station 78102                                            Page   1 of   5
                                  STATION

Extension: 78102                        Lock Messages? n              BCC: M
     Type: 9650                         Security Code:                 TN: 1
     Port: S042896                    Coverage Path 1: 79             COR: 1
     Name: H.323                      Coverage Path 2:                COS: 1
Unicode Name? n                      Hunt-to Station:               Tests? y
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19       Personalized Ringing Pattern: 1
                                              Message Lamp Ext: 78102
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english               Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal           Media Complex Ext:
   Survivable Trunk Dest? y                       IP SoftPhone? y

                                             IP Video Softphone? y
                              Short/Prefixed Registration Allowed: default

                                             Customizable Labels? y
```

The configuration is complete.

22 DIALOGIC SR140 SECURE FAX

In This Chapter:

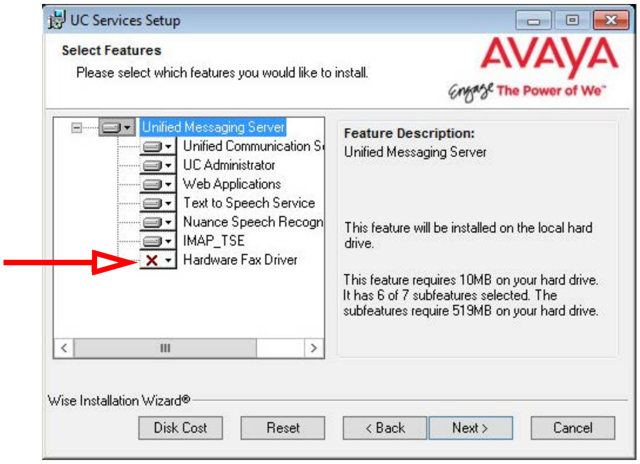
Introduction

Avaya Messaging can be setup 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 setup 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.



UC Services Setup

Select Features

Please select which features you would like to install.

- Unified Messaging Server
  - Unified Communication S
  - UC Administrator
  - Web Applications
  - Text to Speech Service
  - Nuance Speech Recogn
  - IMAP_TSE
  - Hardware Fax Driver

Feature Description:
Unified Messaging Server

This feature will be installed on the local hard drive.

This feature requires 10MB on your hard drive. It has 6 of 7 subfeatures selected. The subfeatures require 519MB on your hard drive.

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

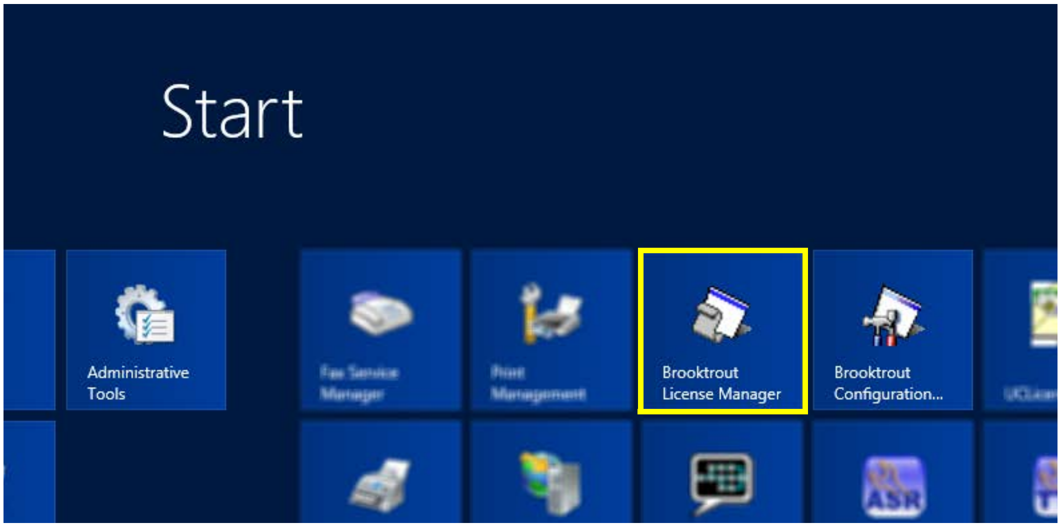
Important! Secure Fax using the SR140 fax software requires 2 licenses from Dialogic; the standard fax license, and a secure fax license.

Configuration

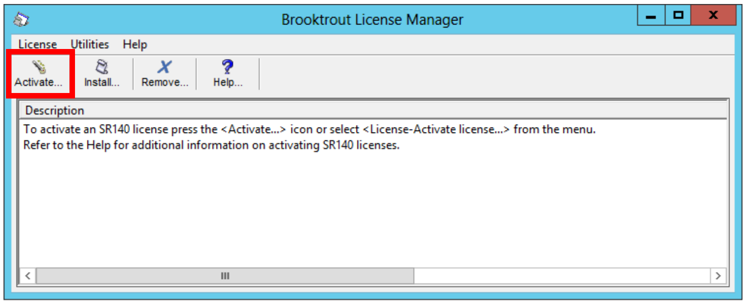
Once the Dialogic SR140 and the Avaya Messaging voice server are both operating, the fax software must be configured to communicate with the UC platform.

License Manager

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



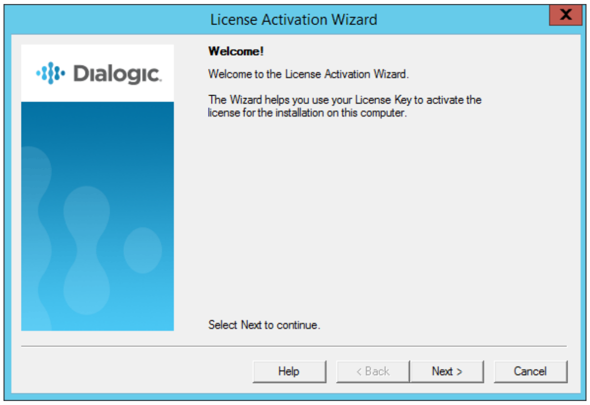
2. Enable the SR140 license by clicking the **Activate** button.



To activate an SR140 license press the <Activate...> icon or select <License-Activate license...> from the menu.
Refer to the Help for additional information on activating SR140 licenses.

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**.



License Activation Wizard

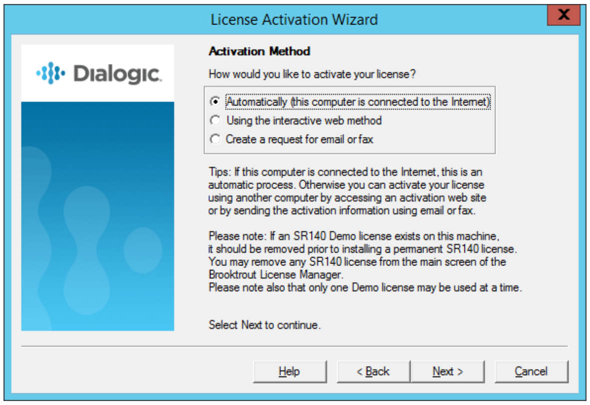
Welcome!

Welcome to the License Activation Wizard.

The Wizard helps you use your License Key to activate the license for the installation on this computer.

Select Next to continue.

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



License Activation Wizard

Activation Method

How would you like to activate your license?

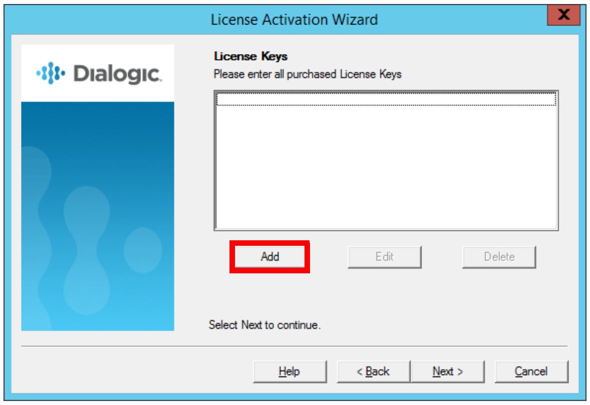
- ● Automatically (this computer is connected to the Internet)
- ○ Using the interactive web method
- ○ Create a request for email or fax

Tips: If this computer is connected to the Internet, this is an automatic process. Otherwise you can activate your license using another computer by accessing an activation web site or by sending the activation information using email or fax.

Please note: If an SR140 Demo license exists on this machine, it should be removed prior to installing a permanent SR140 license. You may remove any SR140 license from the main screen of the Brooktrout License Manager.
Please note also that only one Demo license may be used at a time.

Select Next to continue.

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



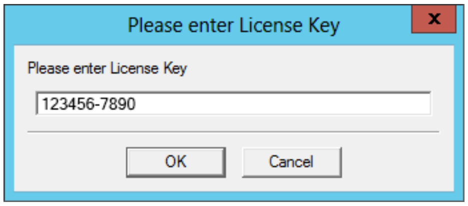
License Activation Wizard

License Keys

Please enter all purchased License Keys

Select Next to continue.

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

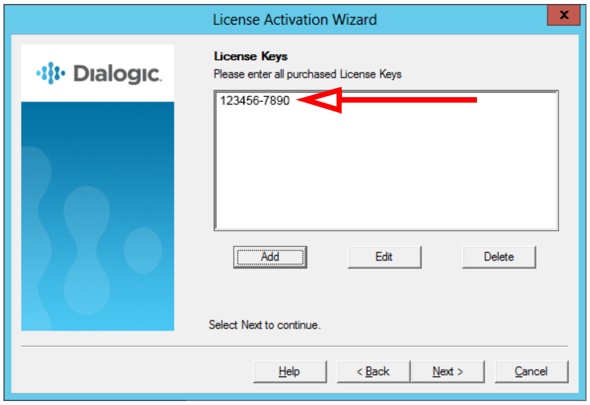


Please enter License Key

Please enter License Key

123456-7890

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



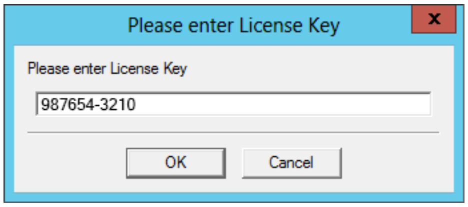
License Keys

Please enter all purchased License Keys

123456-7890

Select Next to continue.

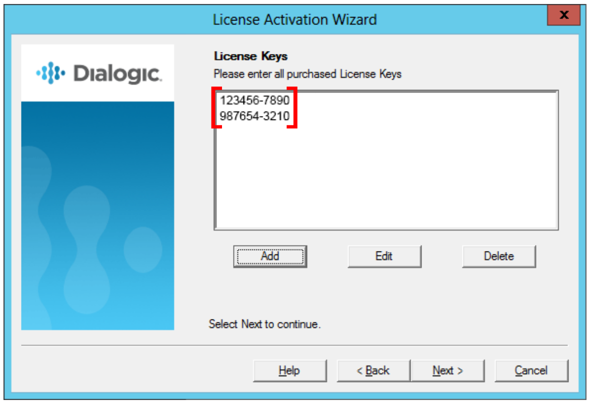
8. Enter the SR140 **secure** fax license key number. Click **OK**.



Please enter License Key

987654-3210

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



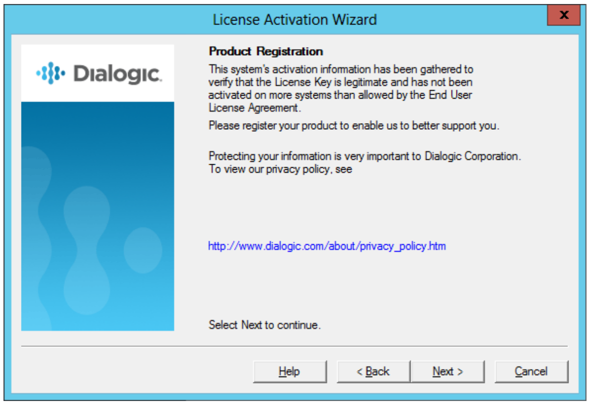
License Keys

Please enter all purchased License Keys

123456-7890
987654-3210

Select Next to continue.

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



Product Registration

This system's activation information has been gathered to verify that the License Key is legitimate and has not been activated on more systems than allowed by the End User License Agreement.

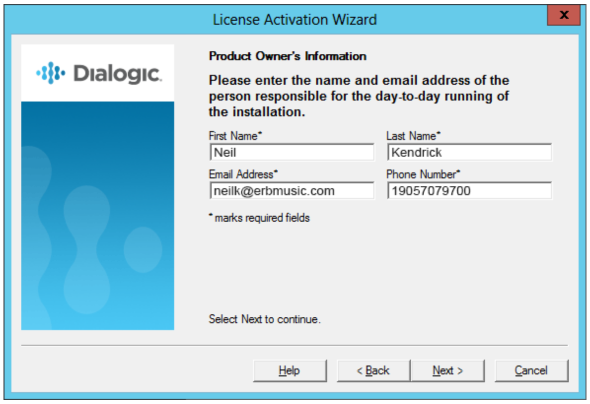
Please register your product to enable us to better support you.

Protecting your information is very important to Dialogic Corporation. To view our privacy policy, see

http://www.dialogic.com/about/privacy_policy.htm

Select Next to continue.

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



Product Owner's Information

Please enter the name and email address of the person responsible for the day-to-day running of the installation.

First Name*: Neil

Last Name*: Kendrick

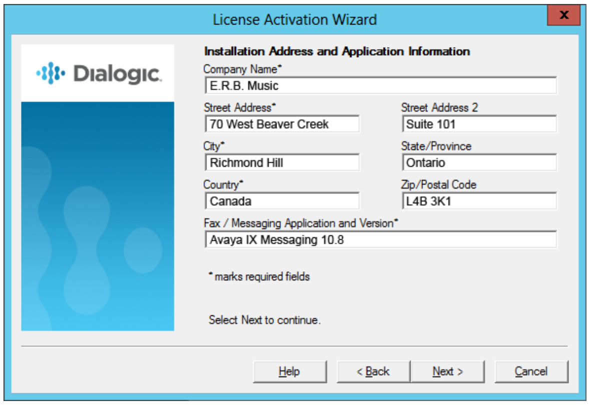
Email Address*: neilk@erbmusic.com

Phone Number*: 19057079700

* marks required fields

Select Next to continue.

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



Installation Address and Application Information

Company Name*: E.R.B. Music

Street Address*: 70 West Beaver Creek

Street Address 2: Suite 101

City*: Richmond Hill

State/Province: Ontario

Country*: Canada

Zip/Postal Code: L4B 3K1

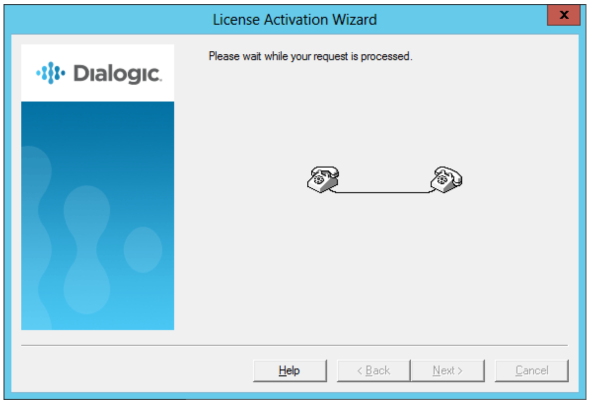
Fax / Messaging Application and Version*: Avaya IX Messaging 10.8

* marks required fields

Select Next to continue.

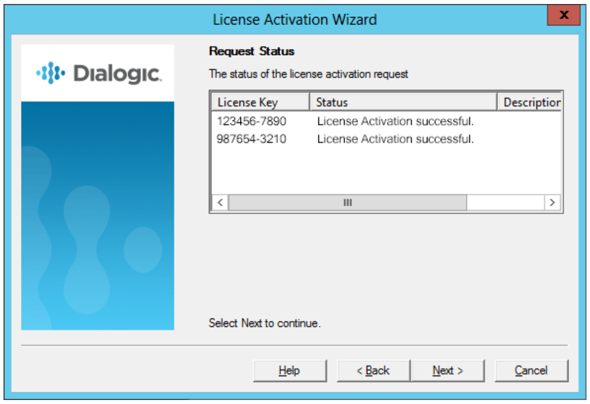
13. The program will connect to the Dialogic servers to upload the registration details. This requires a working Internet connection, and must be completed before the license will be activated.

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



Please wait while your request is processed.

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



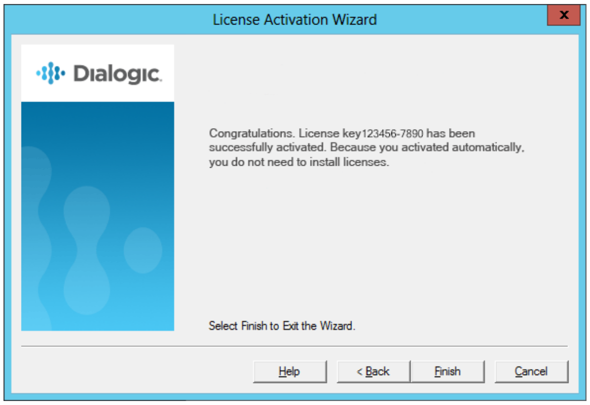
Request Status

The status of the license activation request

License Key	Status	Descriptior
123456-7890	License Activation successful.	
987654-3210	License Activation successful.	

Select Next to continue.

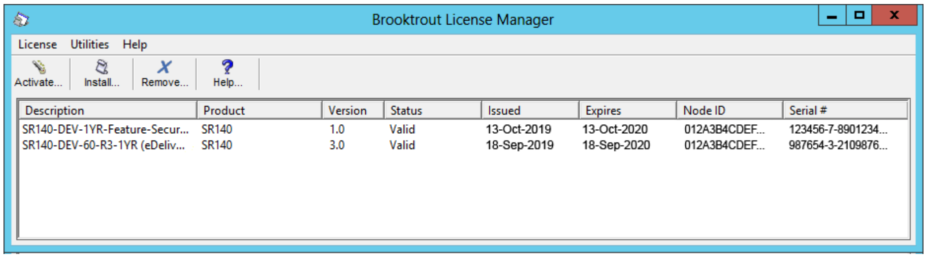
15. Click **Finish** to complete the Wizard.



Congratulations. License key123456-7890 has been successfully activated. Because you activated automatically, you do not need to install licenses.

Select Finish to Exit the Wizard.

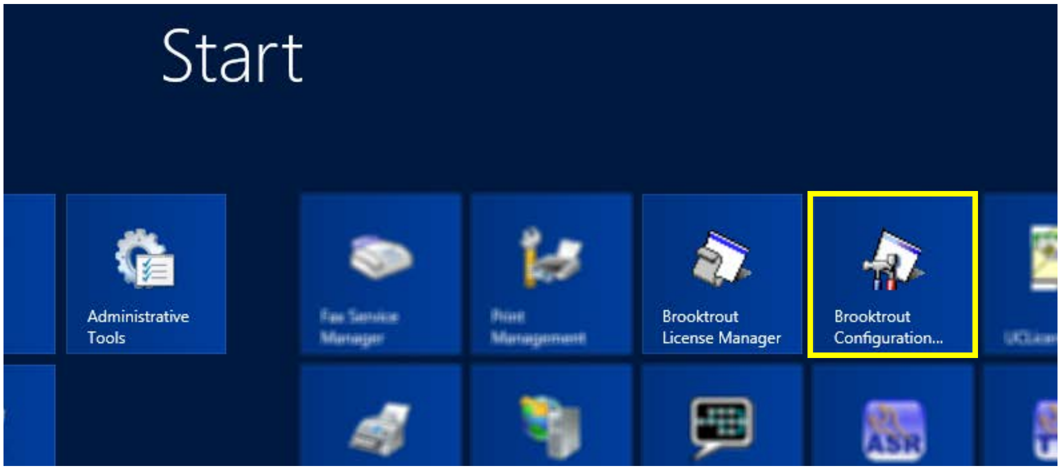
16. The added licenses appear in the **Brooktrout License Manager**.



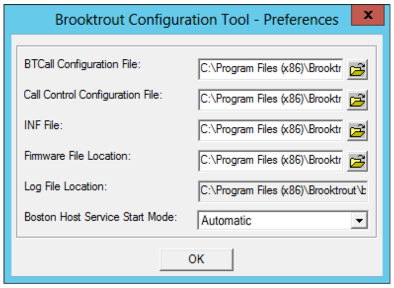
Description	Product	Version	Status	Issued	Expires	Node ID	Serial #
SR140-DEV-1YR-Feature-Secur...	SR140	1.0	Valid	13-Oct-2019	13-Oct-2020	012A3B4CDEF...	123456-7-8901234...
SR140-DEV-60-R3-1YR (eDeliv...	SR140	3.0	Valid	18-Sep-2019	18-Sep-2020	012A3B4CDEF...	987654-3-2109876...

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**.

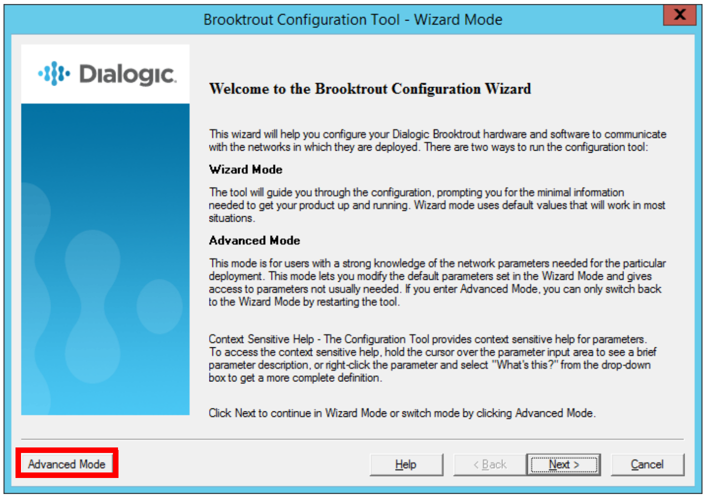


Brooktrout Configuration Tool - Preferences

BTCall Configuration File: C:\Program Files (x86)\Brooktr
Call Control Configuration File: C:\Program Files (x86)\Brooktr
INF File: C:\Program Files (x86)\Brooktr
Firmware File Location: C:\Program Files (x86)\Brooktr
Log File Location: C:\Program Files (x86)\Brooktrout\b
Boston Host Service Start Mode: Automatic

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**.



Brooktrout Configuration Tool - Wizard Mode

Welcome to the Brooktrout Configuration Wizard

This wizard will help you configure your Dialogic Brooktrout hardware and software to communicate with the networks in which they are deployed. There are two ways to run the configuration tool:

Wizard Mode

The tool will guide you through the configuration, prompting you for the minimal information needed to get your product up and running. Wizard mode uses default values that will work in most situations.

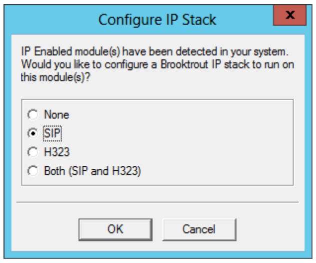
Advanced Mode

This mode is for users with a strong knowledge of the network parameters needed for the particular deployment. This mode lets you modify the default parameters set in the Wizard Mode and gives access to parameters not usually needed. If you enter Advanced Mode, you can only switch back to the Wizard Mode by restarting the tool.

Context Sensitive Help - The Configuration Tool provides context sensitive help for parameters. To access the context sensitive help, hold the cursor over the parameter input area to see a brief parameter description, or right-click the parameter and select "What's this?" from the drop-down box to get a more complete definition.

Click Next to continue in Wizard Mode or switch mode by clicking Advanced Mode.

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



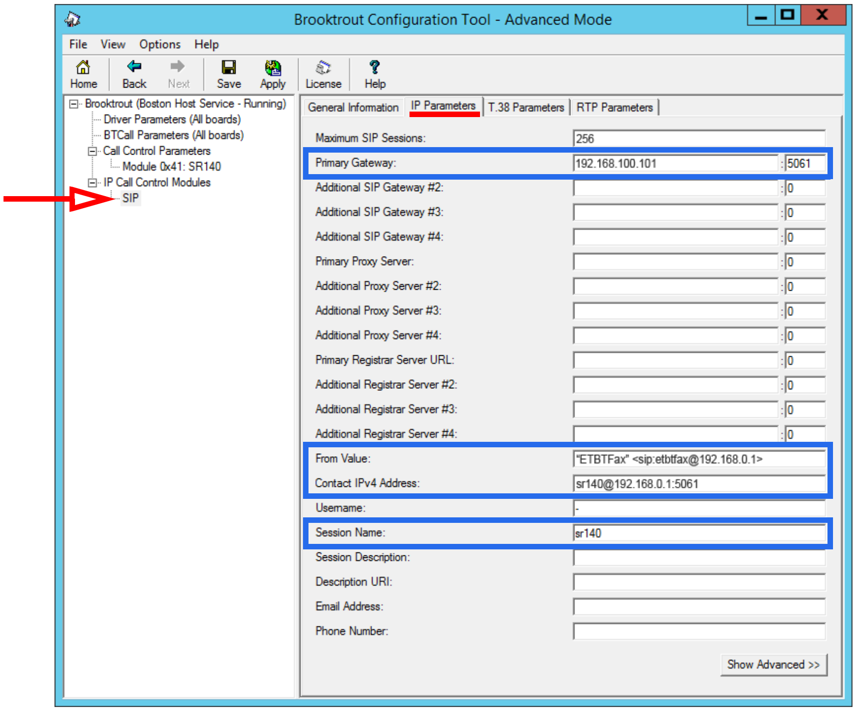
Configure IP Stack

IP Enabled module(s) have been detected in your system. Would you like to configure a Brooktrout IP stack to run on this module(s)?

○ None
● SIP
○ H323
○ Both (SIP and H323)

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.



Brooktrout Configuration Tool - Advanced Mode

Maximum SIP Sessions: 256
Primary Gateway: 192.168.100.101 : 5061
Additional SIP Gateway #2: : 0
Additional SIP Gateway #3: : 0
Additional SIP Gateway #4: : 0
Primary Proxy Server: : 0
Additional Proxy Server #2: : 0
Additional Proxy Server #3: : 0
Additional Proxy Server #4: : 0
Primary Registrar Server URL: : 0
Additional Registrar Server #2: : 0
Additional Registrar Server #3: : 0
Additional Registrar Server #4: : 0
From Value: "ETBTFax" <sip:etbtfax@192.168.0.1>
Contact IPv4 Address: sr140@192.168.0.1:5061
Username: -
Session Name: sr140
Session Description:
Description URI:
Email Address:
Phone Number:

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.

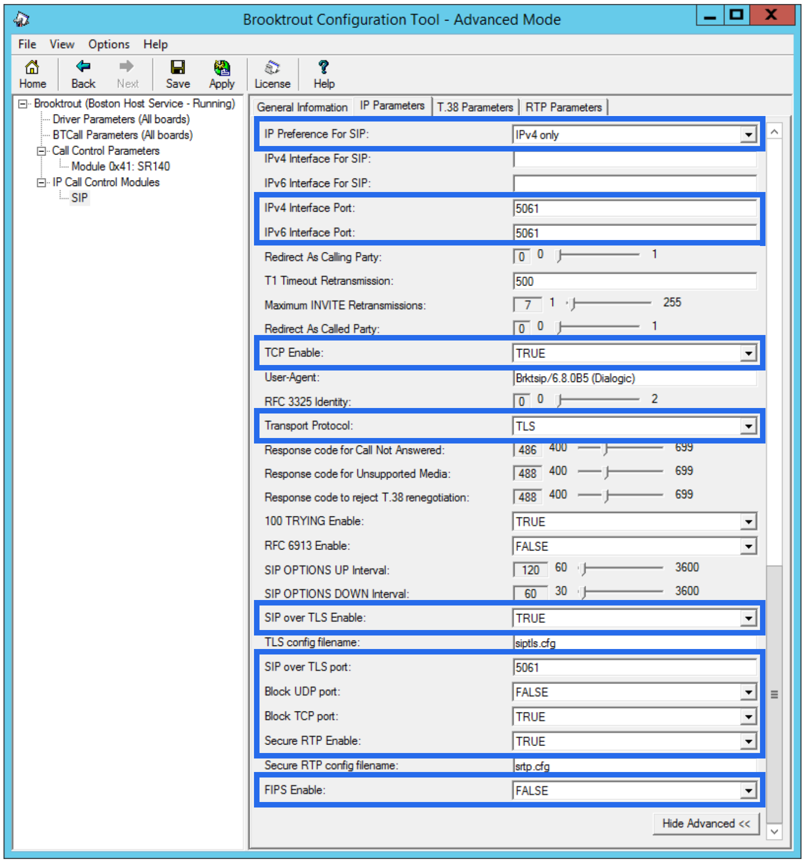
From Value: In this field, (including the quotes) type **"ETBTFax" <sip:etbtfax@** followed by the IP address of the Avaya Messaging voice server. For example: **"ETBTFax" <sip:etbtfax@192.168.0.1>** .

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>>**.

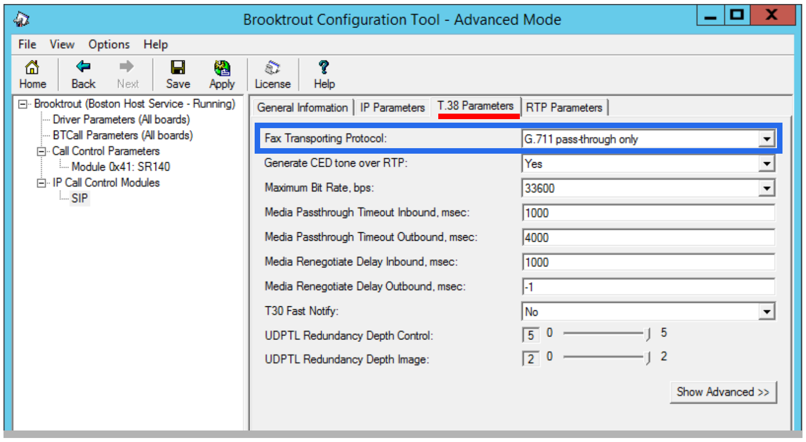
6. Specify the following for your site.



IP Preference For SIP: IPv4 only
IPv4 Interface For SIP:
IPv6 Interface For SIP:
IPv4 Interface Port: 5061
IPv6 Interface Port: 5061
Redirect As Calling Party: 0 (0 – 1)
T1 Timeout Retransmission: 500
Maximum INVITE Retransmissions: 7 (1 – 255)
Redirect As Called Party: 0 (0 – 1)
TCP Enable: TRUE
User-Agent: Brktsip/6.8.0B5 (Dialogic)
RFC 3325 Identity: 0 (0 – 2)
Transport Protocol: TLS
Response code for Call Not Answered: 486 (400 – 699)
Response code for Unsupported Media: 488 (400 – 699)
Response code to reject T.38 renegotiation: 488 (400 – 699)
100 TRYING Enable: TRUE
RFC 6913 Enable: FALSE
SIP OPTIONS UP Interval: 120 (60 – 3600)
SIP OPTIONS DOWN Interval: 60 (30 – 3600)
SIP over TLS Enable: TRUE
TLS config filename: siptls.cfg
SIP over TLS port: 5061
Block UDP port: FALSE
Block TCP port: TRUE
Secure RTP Enable: TRUE
Secure RTP config filename: srtp.cfg
FIPS Enable: FALSE

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**.

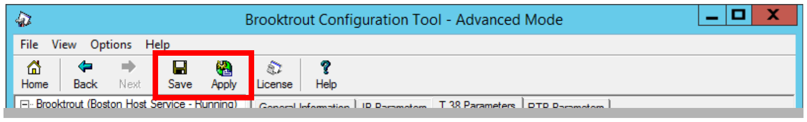
7. Go to the **T.38 Parameters** tab and specify the following for your site.


Brooktrout Configuration Tool - Advanced Mode
File View Options Help
Home Back Next Save Apply License Help
Brooktrout (Boston Host Service - Running)
Driver Parameters (All boards)
BTCall Parameters (All boards)
Call Control Parameters
Module 0x41: SR140
IP Call Control Modules
SIP
General Information
IP Parameters
T.38 Parameters
RTP Parameters
Show Advanced >>

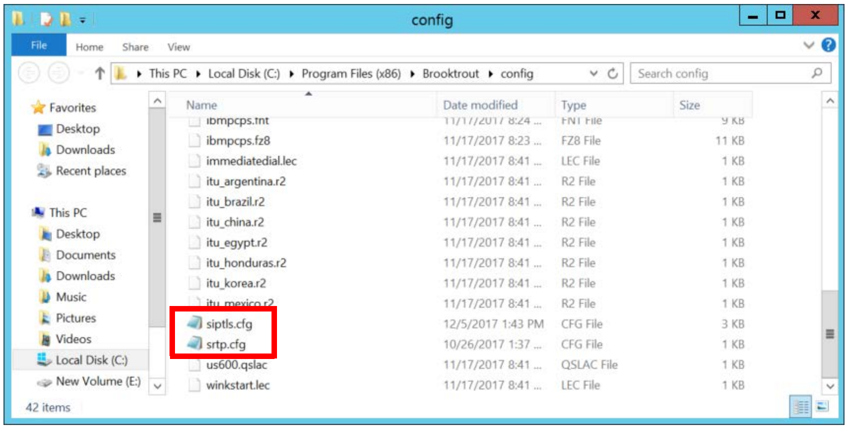
Fax Transporting Protocol:	G.711 pass-through only
Generate CED tone over RTP:	Yes
Maximum Bit Rate, bps:	33600
Media Passthrough Timeout Inbound, msec:	1000
Media Passthrough Timeout Outbound, msec:	4000
Media Renegotiate Delay Inbound, msec:	1000
Media Renegotiate Delay Outbound, msec:	-1
T30 Fast Notify:	No
UDPTL Redundancy Depth Control:	5 (0 – 5)
UDPTL Redundancy Depth Image:	2 (0 – 2)

Fax Transport Protocol: Select **G.711 pass-through only** from the dropdown list.

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

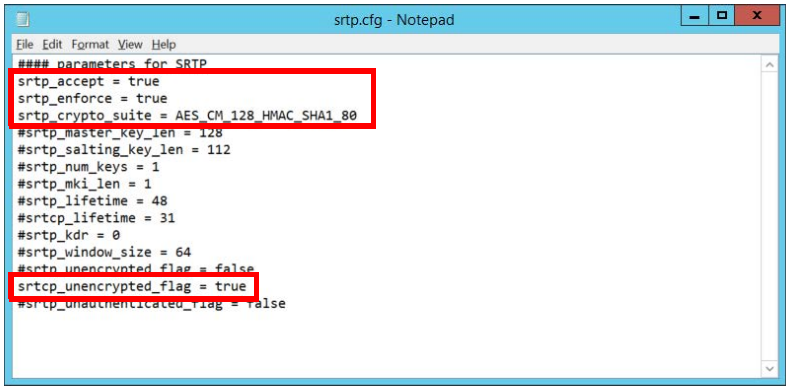

Brooktrout Configuration Tool - Advanced Mode
File View Options Help
Home Back Next Save Apply License Help
Brooktrout (Boston Host Service - Running)
General Information IP Parameters T.38 Parameters RTP Parameters

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



Name	Date modified	Type	Size
ibmpcps.fnt	11/17/2017 8:24 ...	FNT File	9 KB
ibmpcps.fz8	11/17/2017 8:23 ...	FZ8 File	11 KB
immediatedial.lec	11/17/2017 8:41 ...	LEC File	1 KB
itu_argentina.r2	11/17/2017 8:41 ...	R2 File	1 KB
itu_brazil.r2	11/17/2017 8:41 ...	R2 File	1 KB
itu_china.r2	11/17/2017 8:41 ...	R2 File	1 KB
itu_egypt.r2	11/17/2017 8:41 ...	R2 File	1 KB
itu_honduras.r2	11/17/2017 8:41 ...	R2 File	1 KB
itu_korea.r2	11/17/2017 8:41 ...	R2 File	1 KB
itu_mexico.r2	11/17/2017 8:41 ...	R2 File	1 KB
siptls.cfg	12/5/2017 1:43 PM	CFG File	3 KB
srtp.cfg	10/26/2017 1:37 ...	CFG File	1 KB
us600.qslac	11/17/2017 8:41 ...	QSLAC File	1 KB
winkstart.lec	11/17/2017 8:41 ...	LEC File	1 KB

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.



```
#### parameters for SRTP
srtp_accept = true
srtp_enforce = true
srtp_crypto_suite = AES_CM_128_HMAC_SHA1_80
#srtp_master_key_len = 128
#srtp_salting_key_len = 112
#srtp_num_keys = 1
#srtp_mki_len = 1
#srtp_lifetime = 48
#srtcp_lifetime = 31
#srtp_kdr = 0
#srtp_window_size = 64
#srtp_unencrypted_flag = false
srtcp_unencrypted_flag = true
#srtp_unauthenticated_flag = false
```

srtp_accept = true

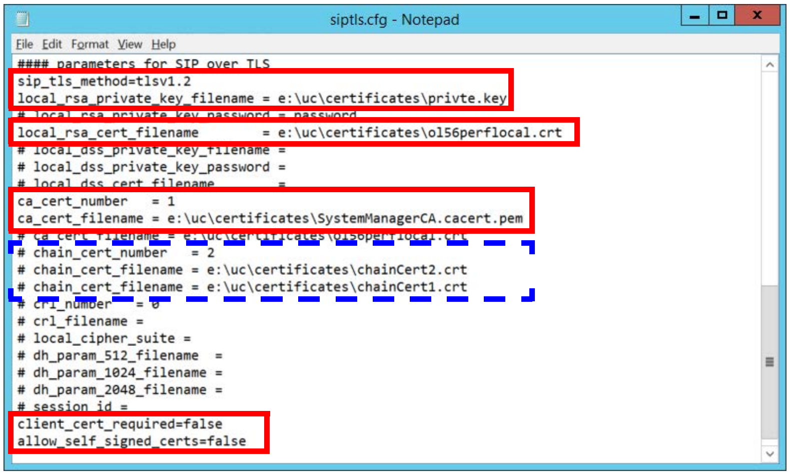
srtp_enforce = true

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.



```
#### parameters for SIP over TLS
sip_tls_method=tlsv1.2
local_rsa_private_key_filename = e:\uc\certificates\privte.key
# local_rsa_private_key_password = password
local_rsa_cert_filename        = e:\uc\certificates\ol56perflocal.crt
# local_dss_private_key_filename =
# local_dss_private_key_password =
# local_dss_cert_filename        =
ca_cert_number   = 1
ca_cert_filename = e:\uc\certificates\SystemManagerCA.cacert.pem
# ca_cert_filename = e:\uc\certificates\ol56perflocal.crt
# chain_cert_number   = 2
# chain_cert_filename = e:\uc\certificates\chainCert2.crt
# chain_cert_filename = e:\uc\certificates\chainCert1.crt
# crl_number    = 0
# crl_filename =
# local_cipher_suite =
# dh_param_512_filename  =
# dh_param_1024_filename =
# dh_param_2048_filename =
# session_id =
client_cert_required=false
allow_self_signed_certs=false
```

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

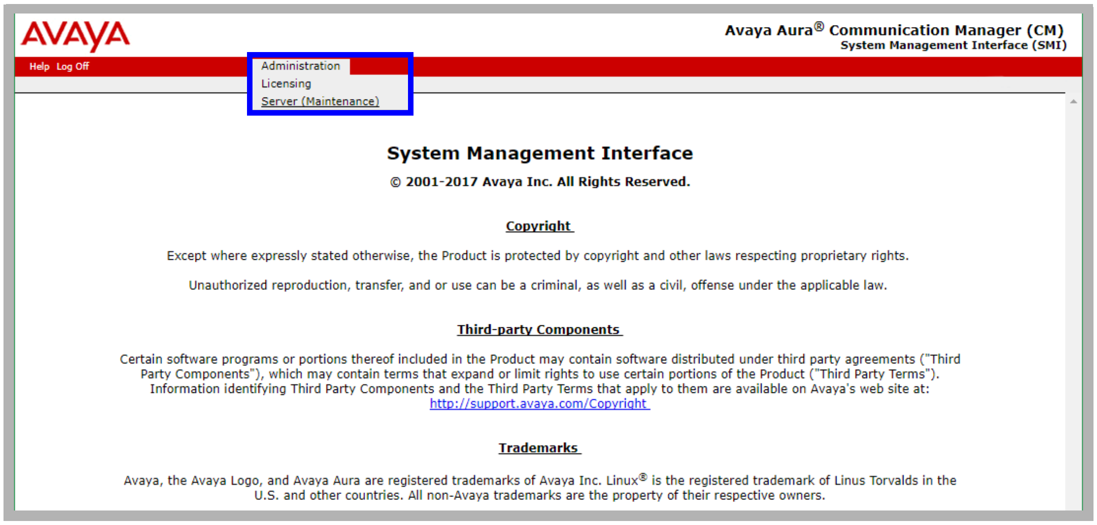
allow_self_signed_certs = false

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)**.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

System Management Interface

© 2001-2017 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

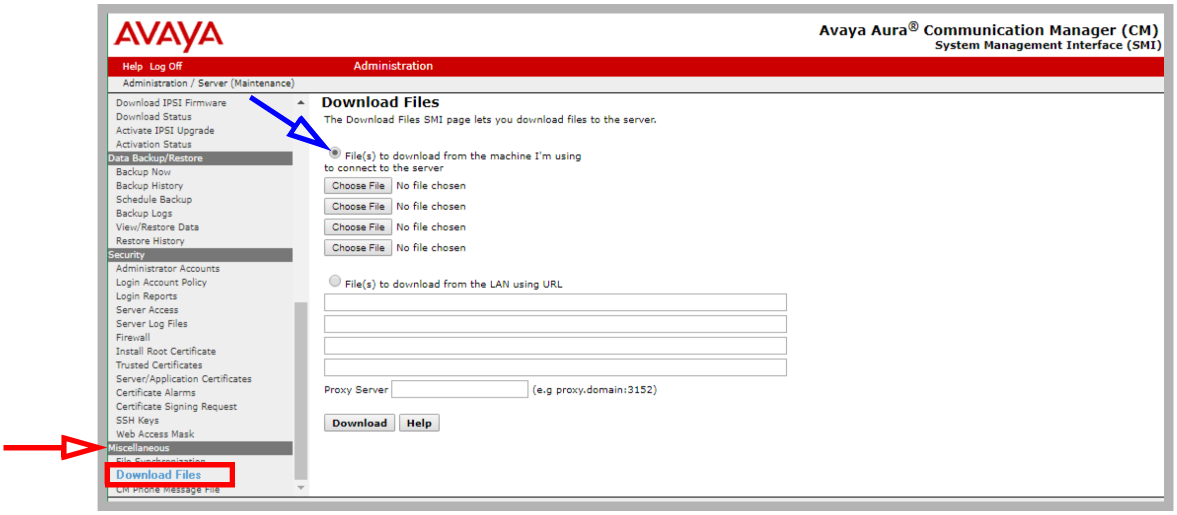
Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/Copyright

Trademarks

Avaya, the Avaya Logo, and Avaya Aura are registered trademarks of Avaya Inc. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All non-Avaya trademarks are the property of their respective owners.

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.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Download Files

The Download Files SMI page lets you download files to the server.

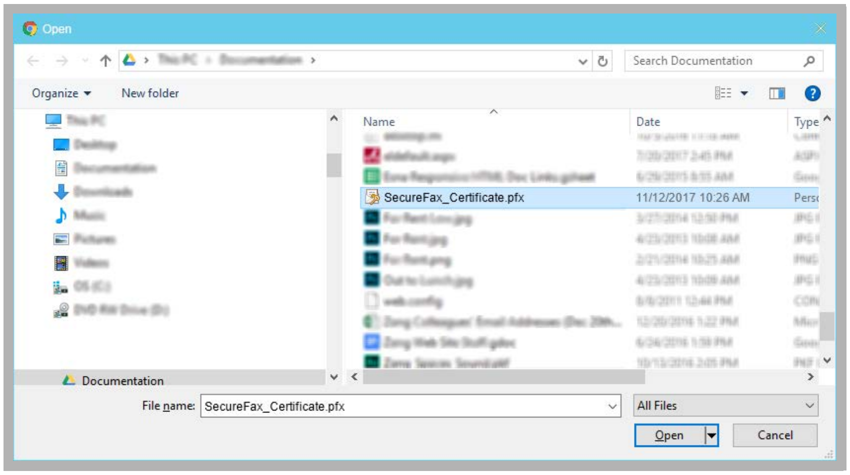
● File(s) to download from the machine I'm using to connect to the server

No file chosen
No file chosen
No file chosen
No file chosen

○ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

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.).

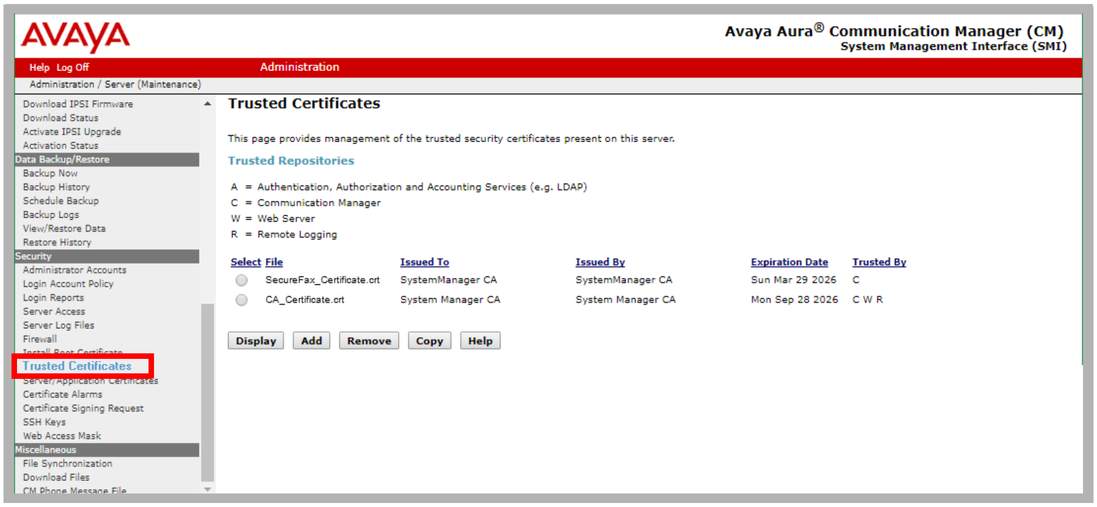


Name	Date	Type
SecureFax_Certificate.pfx	11/12/2017 10:26 AM	Perso

File name: SecureFax_Certificate.pfx

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.



Trusted Certificates

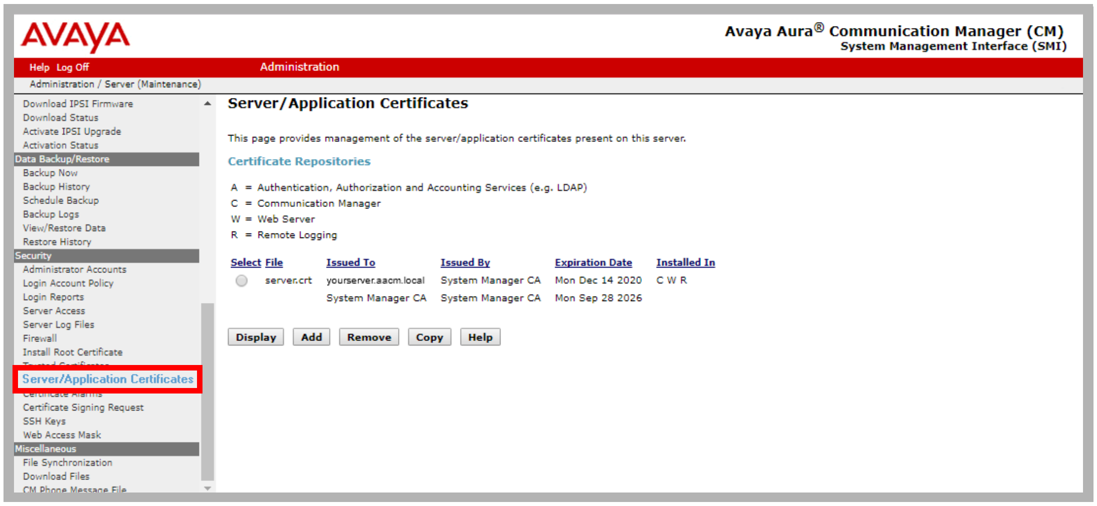
This page provides management of the trusted security certificates present on this server.

Trusted Repositories

A = Authentication, Authorization and Accounting Services (e.g. LDAP)
C = Communication Manager
W = Web Server
R = Remote Logging

Select	File	Issued To	Issued By	Expiration Date	Trusted By
○	SecureFax_Certificate.crt	SystemManager CA	SystemManager CA	Sun Mar 29 2026	C
○	CA_Certificate.crt	System Manager CA	System Manager CA	Mon Sep 28 2026	C W R

5. In the left-hand column, click **Server/Application Certificates**.
Click **Add** and attach the server certificate downloaded in step 3.



Server/Application Certificates

This page provides management of the server/application certificates present on this server.

Certificate Repositories

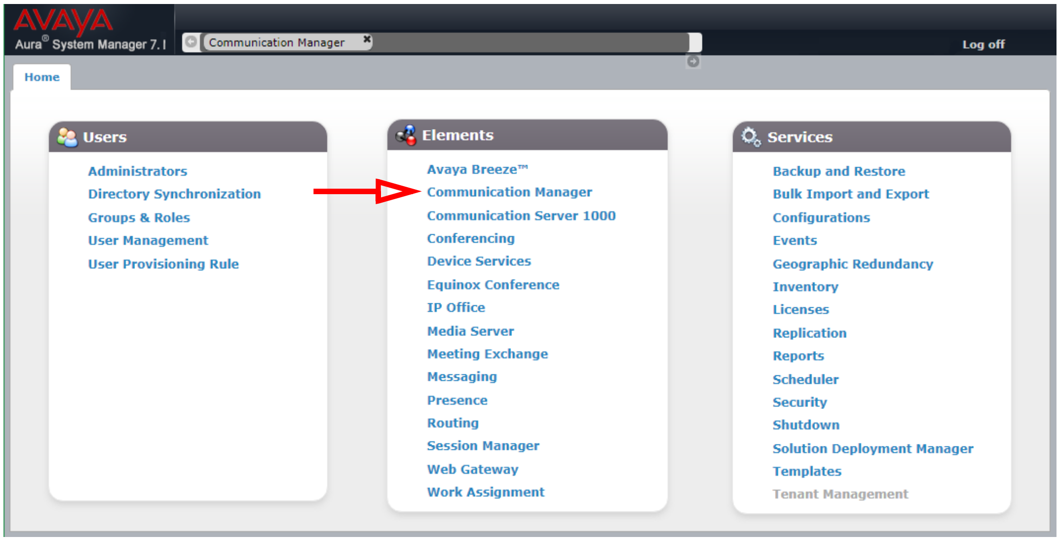
A = Authentication, Authorization and Accounting Services (e.g. LDAP)
C = Communication Manager
W = Web Server
R = Remote Logging

Select	File	Issued To	Issued By	Expiration Date	Installed In
○	server.crt	yourserver.aacm.local System Manager CA	System Manager CA System Manager CA	Mon Dec 14 2020 Mon Sep 28 2026	C W R

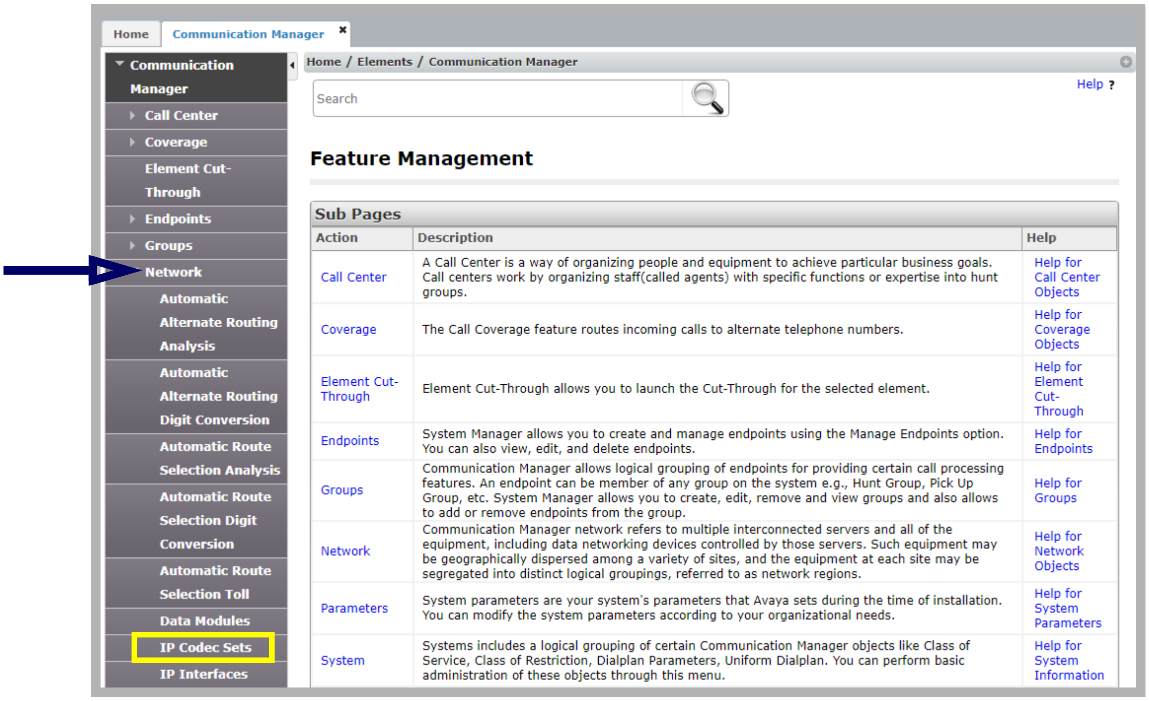
6. Close the **Communication Manager** console.

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**.

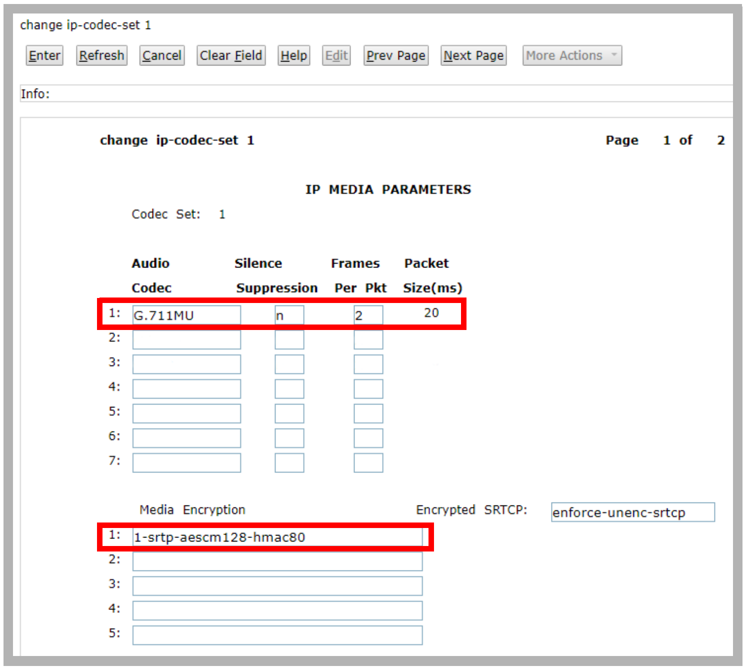

Home
Communication Manager
Communication Manager
Call Center
Coverage
Element Cut-Through
Endpoints
Groups
Network
Automatic Alternate Routing Analysis
Automatic Alternate Routing Digit Conversion
Automatic Route Selection Analysis
Automatic Route Selection Digit Conversion
Automatic Route Selection Toll
Data Modules
IP Codec Sets
IP Interfaces
Home / Elements / Communication Manager
Search
Help ?

Feature Management

Sub Pages

Action	Description	Help
Call Center	A Call Center is a way of organizing people and equipment to achieve particular business goals. Call centers work by organizing staff(called agents) with specific functions or expertise into hunt groups.	Help for Call Center Objects
Coverage	The Call Coverage feature routes incoming calls to alternate telephone numbers.	Help for Coverage Objects
Element Cut-Through	Element Cut-Through allows you to launch the Cut-Through for the selected element.	Help for Element Cut-Through
Endpoints	System Manager allows you to create and manage endpoints using the Manage Endpoints option. You can also view, edit, and delete endpoints.	Help for Endpoints
Groups	Communication Manager allows logical grouping of endpoints for providing certain call processing features. An endpoint can be member of any group on the system e.g., Hunt Group, Pick Up Group, etc. System Manager allows you to create, edit, remove and view groups and also allows to add or remove endpoints from the group.	Help for Groups
Network	Communication Manager network refers to multiple interconnected servers and all of the equipment, including data networking devices controlled by those servers. Such equipment may be geographically dispersed among a variety of sites, and the equipment at each site may be segregated into distinct logical groupings, referred to as network regions.	Help for Network Objects
Parameters	System parameters are your system's parameters that Avaya sets during the time of installation. You can modify the system parameters according to your organizational needs.	Help for System Parameters
System	Systems includes a logical grouping of certain Communication Manager objects like Class of Service, Class of Restriction, Dialplan Parameters, Uniform Dialplan. You can perform basic administration of these objects through this menu.	Help for System Information

3. **Add** / **Edit** an audio codec set.

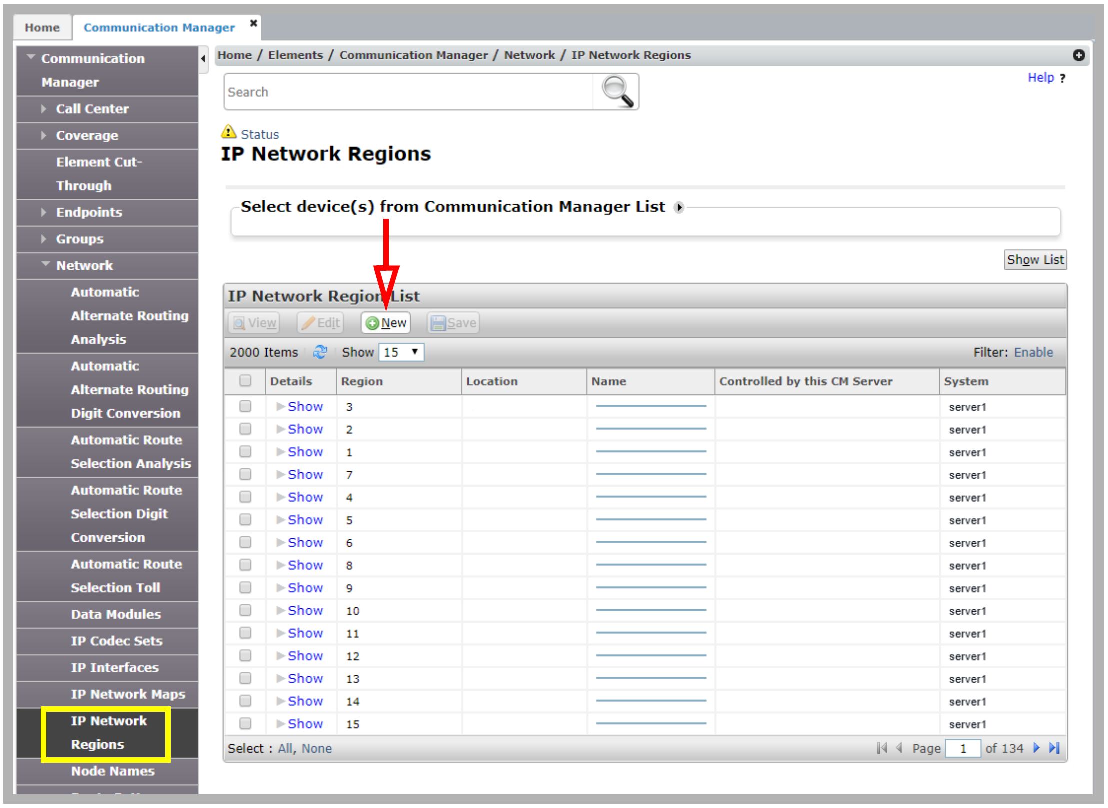


Info:

```
        change ip-codec-set 1                                        Page   1 of   2

                                  IP MEDIA PARAMETERS
            Codec Set: 1

            Audio           Silence       Frames     Packet
            Codec           Suppression   Per Pkt    Size(ms)
         1: G.711MU         n             2           20
         2:
         3:
         4:
         5:
         6:
         7:

             Media Encryption                         Encrypted SRTCP:  enforce-unenc-srtcp
         1: 1-srtp-aescm128-hmac80
         2:
         3:
         4:
         5:
```

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.



Home / Elements / Communication Manager / Network / IP Network Regions

IP Network Regions

Select device(s) from Communication Manager List

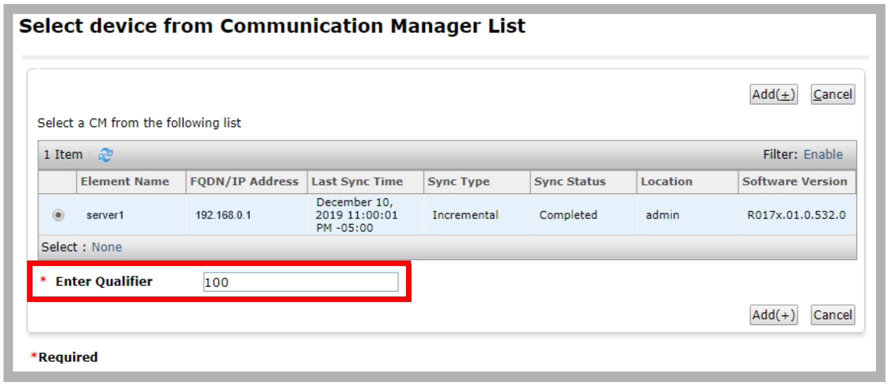
IP Network Region List

2000 Items   Show 15   Filter: Enable

□	Details	Region	Location	Name	Controlled by this CM Server	System
□	▶ Show	3				server1
□	▶ Show	2				server1
□	▶ Show	1				server1
□	▶ Show	7				server1
□	▶ Show	4				server1
□	▶ Show	5				server1
□	▶ Show	6				server1
□	▶ Show	8				server1
□	▶ Show	9				server1
□	▶ Show	10				server1
□	▶ Show	11				server1
□	▶ Show	12				server1
□	▶ Show	13				server1
□	▶ Show	14				server1
□	▶ Show	15				server1

Select : All, None   Page 1 of 134

5. Enter an available **Network Region** qualifier (a number between 1-250), then click **Add**.



Select device from Communication Manager List

Select a CM from the following list

1 Item | Filter: Enable

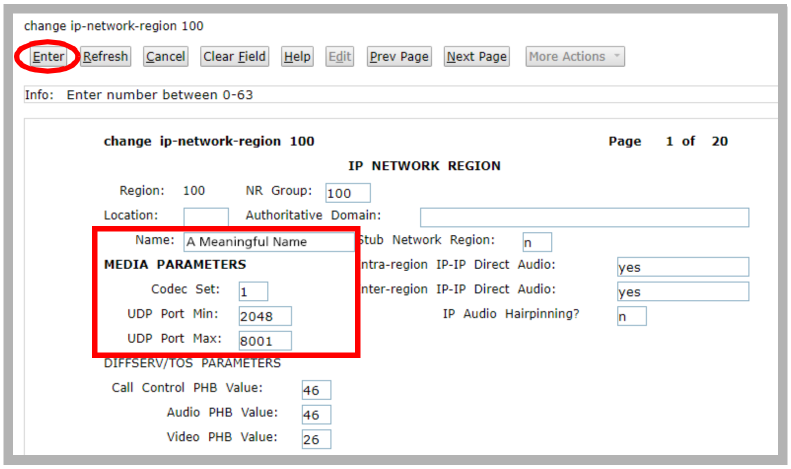
	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
●	server1	192.168.0.1	December 10, 2019 11:00:01 PM -05:00	Incremental	Completed	admin	R017x.01.0.532.0

Select : None

* **Enter Qualifier** 100

***Required**

6. Enter the following parameters.



change ip-network-region 100

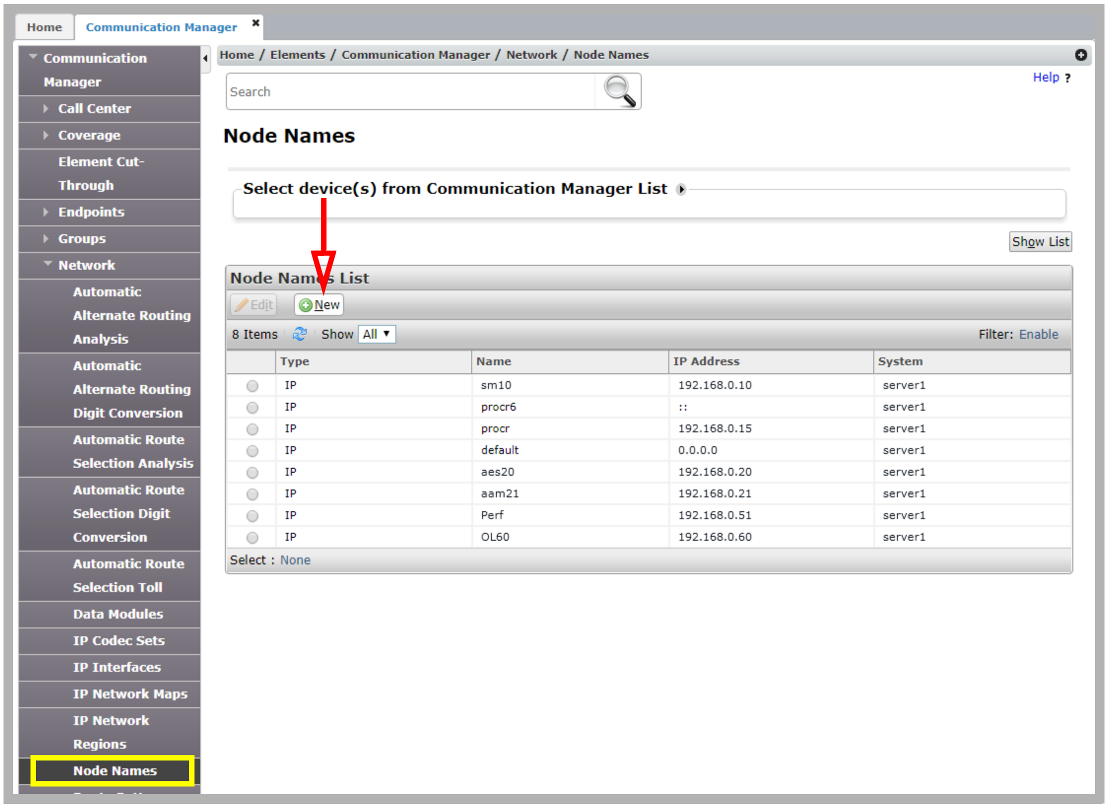
Info: Enter number between 0-63

```
          change ip-network-region 100                                    Page   1 of   20
                                        IP NETWORK REGION
            Region:  100       NR Group: 100
          Location:            Authoritative Domain:
              Name: A Meaningful Name         tub Network Region: n
          MEDIA PARAMETERS                     ntra-region IP-IP Direct Audio:   yes
                Codec Set: 1                  nter-region IP-IP Direct Audio:   yes
             UDP Port Min: 2048                           IP Audio Hairpinning?  n
             UDP Port Max: 8001
          DIFFSERV/TOS PARAMETERS
           Call Control PHB Value:   46
                  Audio PHB Value:   46
                  Video PHB Value:   26
```

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**.


Home
Communication Manager
Communication Manager
Call Center
Coverage
Element Cut-Through
Endpoints
Groups
Network
Automatic Alternate Routing Analysis
Automatic Alternate Routing Digit Conversion
Automatic Route Selection Analysis
Automatic Route Selection Digit Conversion
Automatic Route Selection Toll
Data Modules
IP Codec Sets
IP Interfaces
IP Network Maps
IP Network Regions
Node Names
Home / Elements / Communication Manager / Network / Node Names
Search
Help ?
Show List
Edit
New
Show All
Filter: Enable

Node Names

Select device(s) from Communication Manager List

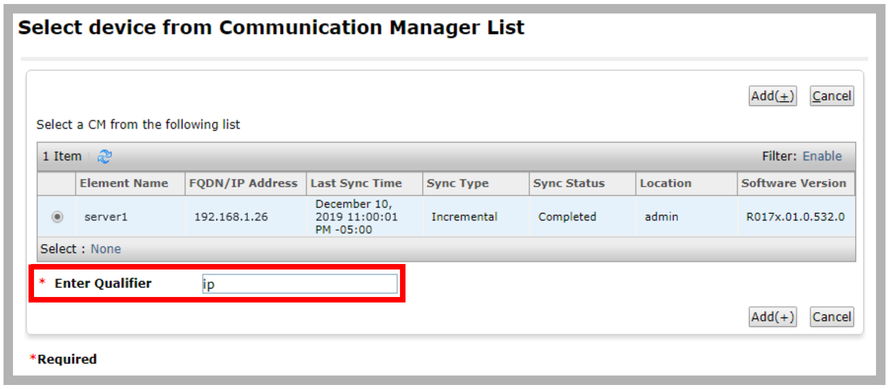
Node Names List

8 Items

	Type	Name	IP Address	System
○	IP	sm10	192.168.0.10	server1
○	IP	procr6	::	server1
○	IP	procr	192.168.0.15	server1
○	IP	default	0.0.0.0	server1
○	IP	aes20	192.168.0.20	server1
○	IP	aam21	192.168.0.21	server1
○	IP	Perf	192.168.0.51	server1
○	IP	OL60	192.168.0.60	server1

Select : None

8. Select **IP** from the qualifier dropdown list, then click **Add**.



Select device from Communication Manager List

Select a CM from the following list

1 Item

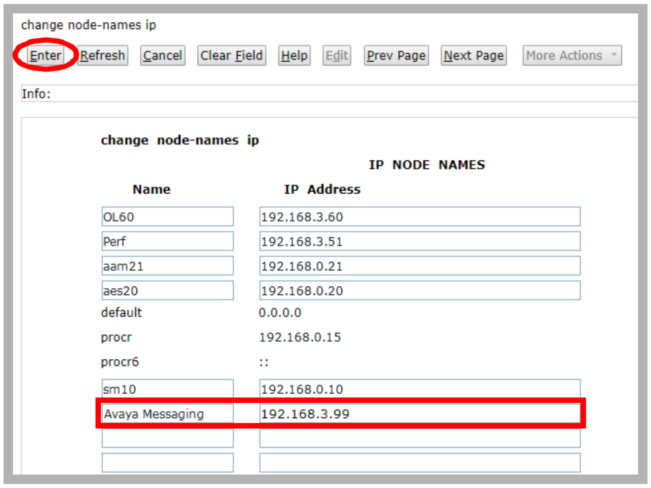
	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
●	server1	192.168.1.26	December 10, 2019 11:00:01 PM -05:00	Incremental	Completed	admin	R017x.01.0.532.0

Select : None

* Enter Qualifier ip

*Required

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.



change node-names ip

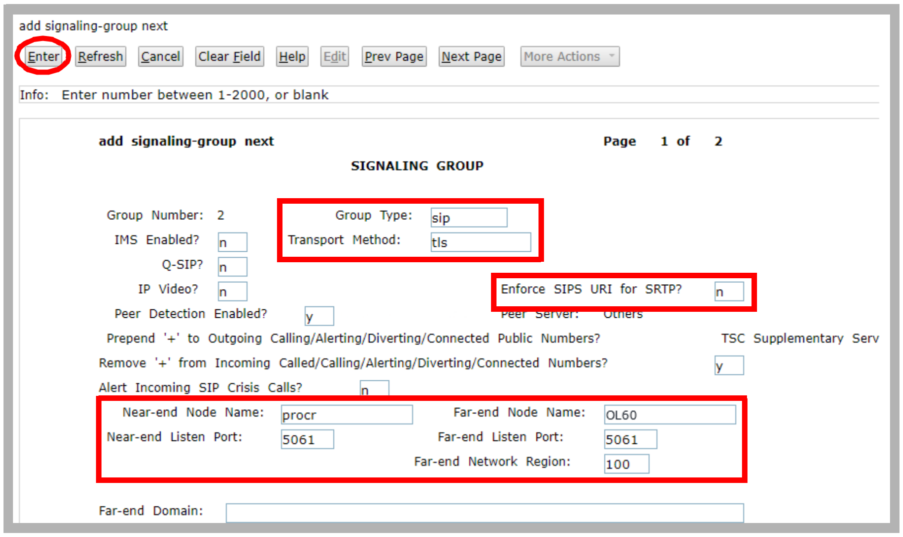
Info:

change node-names ip

IP NODE NAMES

Name	**IP Address**
OL60	192.168.3.60
Perf	192.168.3.51
aam21	192.168.0.21
aes20	192.168.0.20
default	0.0.0.0
procr	192.168.0.15
procr6	::
sm10	192.168.0.10
Avaya Messaging	192.168.3.99

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 for a Qualifier, enter **NEXT**. Enter the required values.



add signaling-group next

Info: Enter number between 1-2000, or blank

add signaling-group next **Page 1 of 2**

SIGNALING GROUP

Group Number: 2 Group Type: sip

IMS Enabled? n Transport Method: tls

Q-SIP? n

IP Video? n Enforce SIPS URI for SRTP? n

Peer Detection Enabled? y Peer Server: Others

Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? TSC Supplementary Serv

Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y

Alert Incoming SIP Crisis Calls? n

Near-end Node Name: procr Far-end Node Name: OL60

Near-end Listen Port: 5061 Far-end Listen Port: 5061

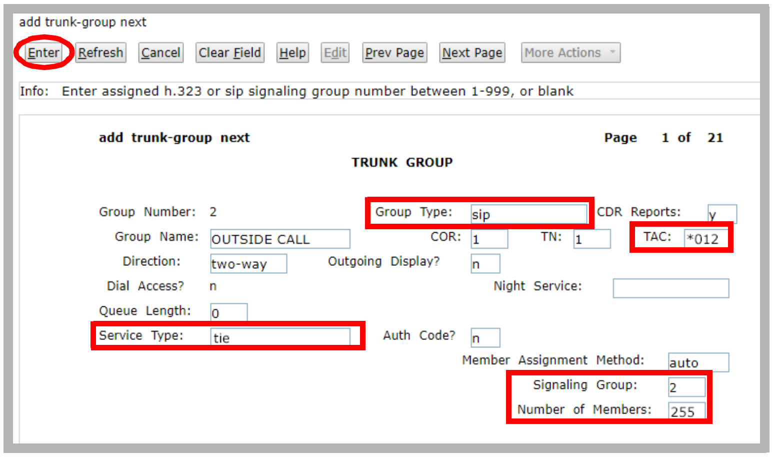
Far-end Network Region: 100

Far-end Domain:

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**.



add trunk-group next

Info: Enter assigned h.323 or sip signaling group number between 1-999, or blank

add trunk-group next   Page 1 of 21

TRUNK GROUP

Group Number: 2	Group Type: sip		CDR Reports: y
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: *012
Direction: two-way	Outgoing Display? n		
Dial Access? n		Night Service:	
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method:	auto
		Signaling Group:	2
		Number of Members:	255

TAC (Trunk Access Code): Enter any unique number. Any four digits, or # and *

Group Type: Select **SIP** from the dropdown list.

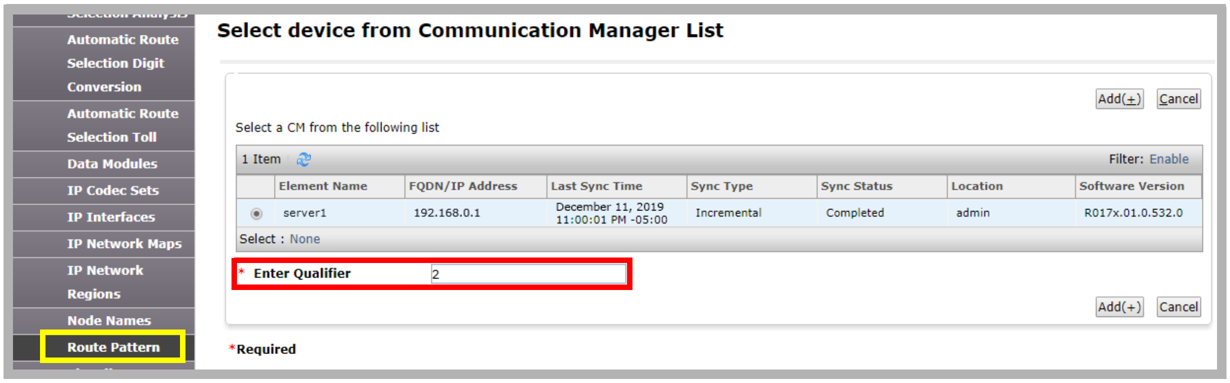
Signaling Group: Enter the number of the signaling group from step 10.

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**.



Select device from Communication Manager List

Select a CM from the following list

1 Item   Filter: Enable

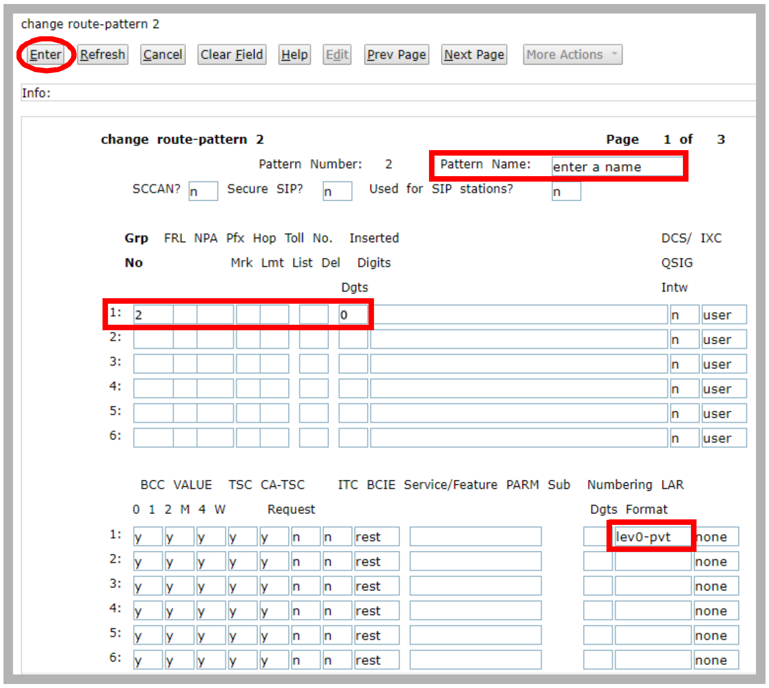
	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
◉	server1	192.168.0.1	December 11, 2019 11:00:01 PM -05:00	Incremental	Completed	admin	R017x.01.0.532.0

Select : None

* Enter Qualifier 2

*Required

13. Enter the values required.



change route-pattern 2 — Page 1 of 3

Pattern Number: 2 — Pattern Name: enter a name

SCCAN? n — Secure SIP? n — Used for SIP stations? n

	Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del Dgts	Inserted Digits	DCS/ QSIG Intw	IXC
1:	2						0		n	user
2:									n	user
3:									n	user
4:									n	user
5:									n	user
6:									n	user

	BCC VALUE 0	1	2	M	4	W	TSC	CA-TSC Request	ITC	BCIE	Service/Feature PARM	Sub Numbering Dgts	Format	LAR
1:	y	y	y	y	y	n	n		rest				lev0-pvt	none
2:	y	y	y	y	y	n	n		rest					none
3:	y	y	y	y	y	n	n		rest					none
4:	y	y	y	y	y	n	n		rest					none
5:	y	y	y	y	y	n	n		rest					none
6:	y	y	y	y	y	n	n		rest					none

Grp No : Enter the trunk group number configured in step 10.

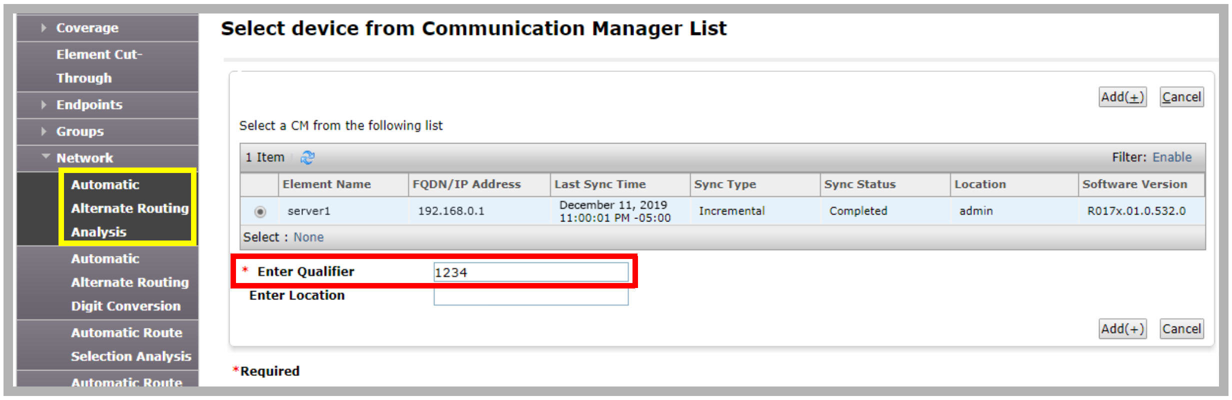
No. Del Dgts: Usually, set this value to **0**.

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**.


Coverage
Element Cut-Through
Endpoints
Groups
Network
Automatic Alternate Routing Analysis
Automatic Alternate Routing Digit Conversion
Automatic Route Selection Analysis
Automatic Route
Add(+)
Cancel

Select device from Communication Manager List

Select a CM from the following list

1 Item — Filter: Enable

	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
◉	server1	192.168.0.1	December 11, 2019 11:00:01 PM -05:00	Incremental	Completed	admin	R017x.01.0.532.0

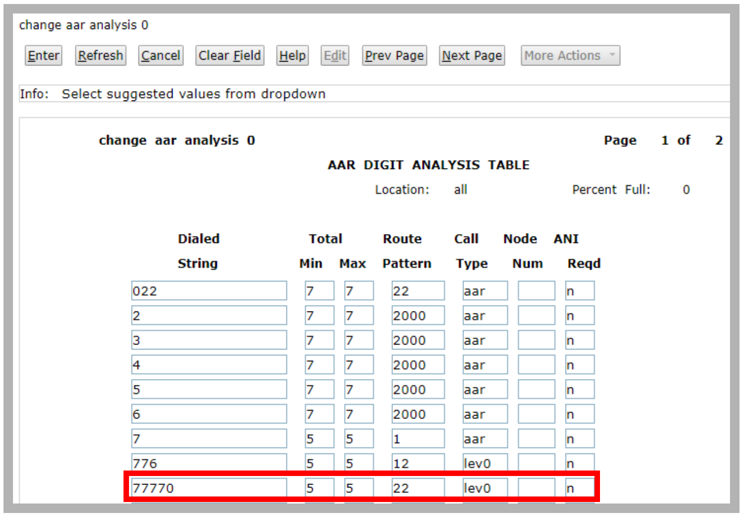
Select : None

* Enter Qualifier: 1234

Enter Location:

*Required

15. Modify a Dialed String entry.



change aar analysis 0

Info: Select suggested values from dropdown

change aar analysis 0 Page 1 of 2

AAR DIGIT ANALYSIS TABLE

Location: all Percent Full: 0

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
022	7	7	22	aar		n
2	7	7	2000	aar		n
3	7	7	2000	aar		n
4	7	7	2000	aar		n
5	7	7	2000	aar		n
6	7	7	2000	aar		n
7	5	5	1	aar		n
776	5	5	12	lev0		n
77770	5	5	22	lev0		n

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.

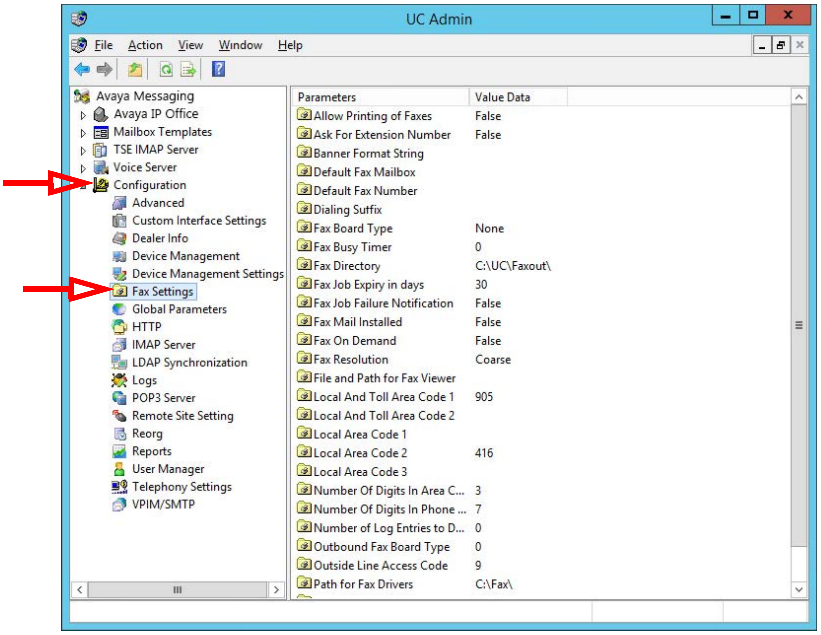
Call Type: Select **lev0** from the dropdown list.

When ready, click the **ENTER** button.

Avaya Messaging Configuration

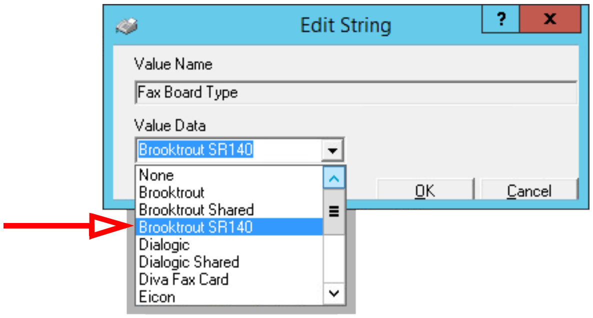
The voice server must be configured to send faxes to the SR140, and to prepare to receive them across the same channel. A setting for incoming, and another for outgoing faxes must be configured on the server using Avaya Messaging Admin.

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**.



Parameters	Value Data
Allow Printing of Faxes	False
Ask For Extension Number	False
Banner Format String	
Default Fax Mailbox	
Default Fax Number	
Dialing Suffix	
Fax Board Type	None
Fax Busy Timer	0
Fax Directory	C:\UC\Faxout\
Fax Job Expiry in days	30
Fax Job Failure Notification	False
Fax Mail Installed	False
Fax On Demand	False
Fax Resolution	Coarse
File and Path for Fax Viewer	
Local And Toll Area Code 1	905
Local And Toll Area Code 2	
Local Area Code 1	
Local Area Code 2	416
Local Area Code 3	
Number Of Digits In Area C...	3
Number Of Digits In Phone ...	7
Number of Log Entries to D...	0
Outbound Fax Board Type	0
Outside Line Access Code	9
Path for Fax Drivers	C:\Fax\

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**.



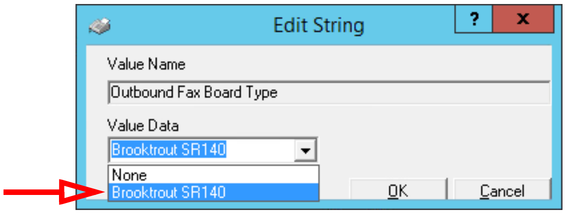
Value Name

Fax Board Type

Value Data

Brooktrout SR140

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



Value Name

Outbound Fax Board Type

Value Data

Brooktrout SR140

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

23 WEB ACCESS

In This Chapter:

Introduction

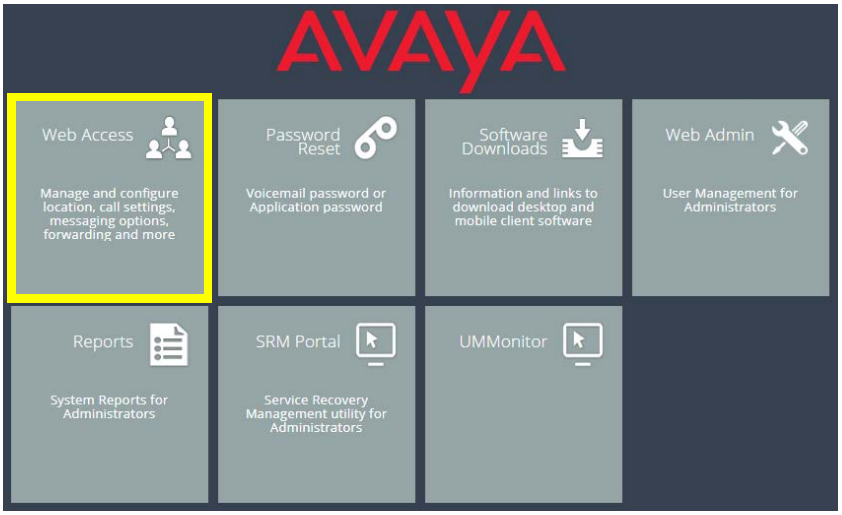
Business today requires flexibility and mobility. Company personnel find it increasingly necessary to go where the customers are. Advances in technology allow people to work from home or other locations away from the office. The Avaya Messaging Web Access is an Internet browser based application that 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.

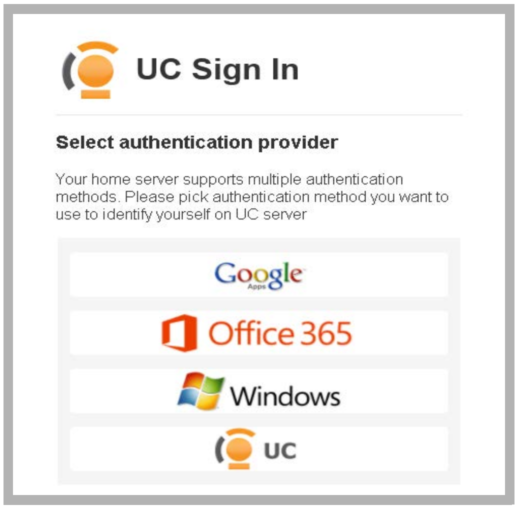
Getting Started

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.


AVAYA
Web Access
Manage and configure location, call settings, messaging options, forwarding and more
Password Reset
Voicemail password or Application password
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

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.



UC Sign In

Select authentication provider

Your home server supports multiple authentication methods. Please pick authentication method you want to use to identify yourself on UC server

Note: This screen does not appear if you login without having logged out from a previous session.

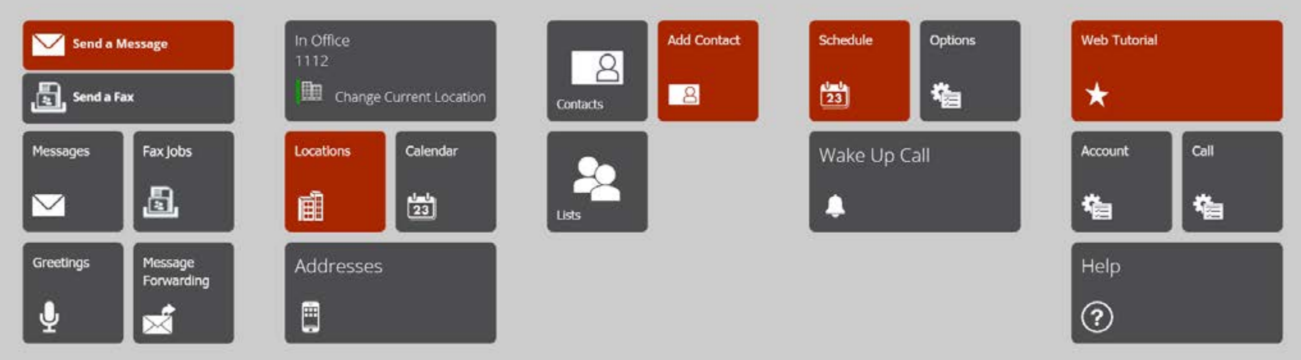
Logging In

Refer to page 95 of the Client Applications Guide for complete details on signing on to Web Access.

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 mange them. You also have complete access to manage your UC presence, location, schedule and contacts.

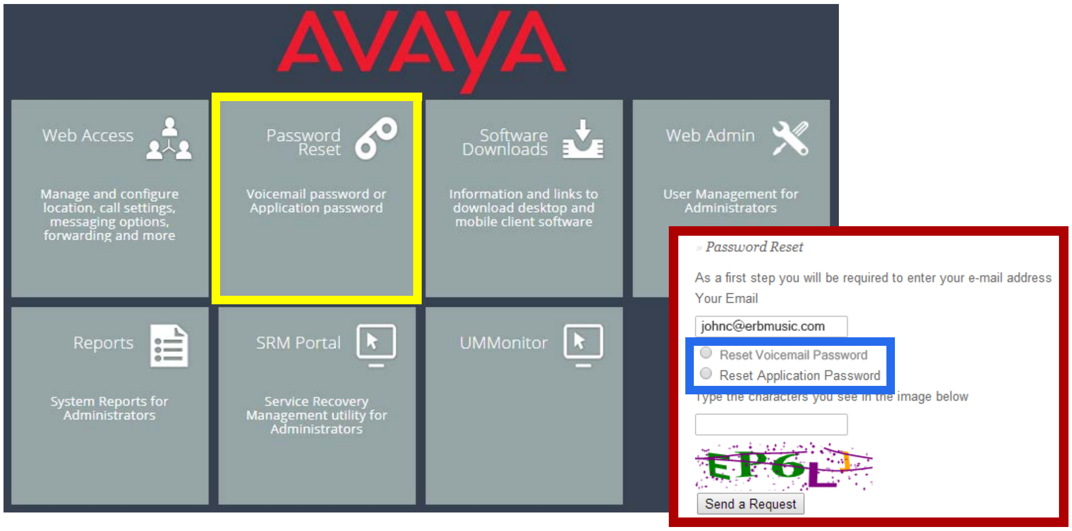


For more details on Web Access, please refer to page 95 of the Client Applications Guide.

24 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 **Reset Password**.
2. Enter an **email address** and select the password to reset: reset **Voicemail Password** or **Application Password**.


AVAYA
Web Access
Manage and configure location, call settings, messaging options, forwarding and more
Password Reset
Voicemail password or Application password
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
EP6L1

» *Password Reset*

As a first step you will be required to enter your e-mail address

Your Email

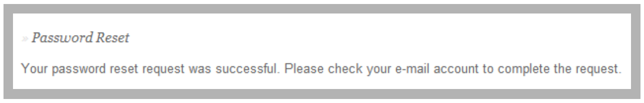
johnc@erbmusic.com

○ Reset Voicemail Password
○ Reset Application Password

Type the characters you see in the image below

Send a Request

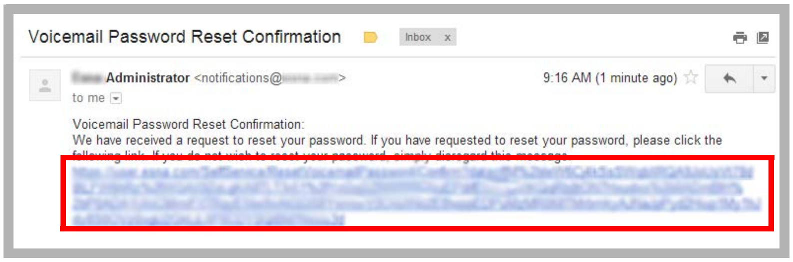
3. Enter the security code in the space provided, Click **Send a Request** when ready.



» *Password Reset*

Your password reset request was successful. Please check your e-mail account to complete the request.

4. The specified email address will receive a message with a link. Click on the link to enter the details of the new password.



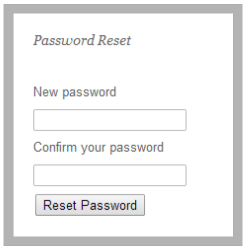
Voicemail Password Reset Confirmation   Inbox x

[redacted] Administrator <notifications@[redacted]>   9:16 AM (1 minute ago)

to me

Voicemail Password Reset Confirmation:
We have received a request to reset your password. If you have requested to reset your password, please click the following link. If you do not wish to reset your password, simply disregard this message.
[redacted]

5. Enter a new password in the spaces provided, then click **Reset Password**.

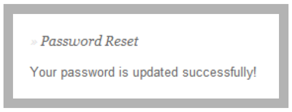


Password Reset

New password

Confirm your password

6. The account password will be changed to the new value.



Password Reset

Your password is updated successfully!

25 WEB UM MONITOR

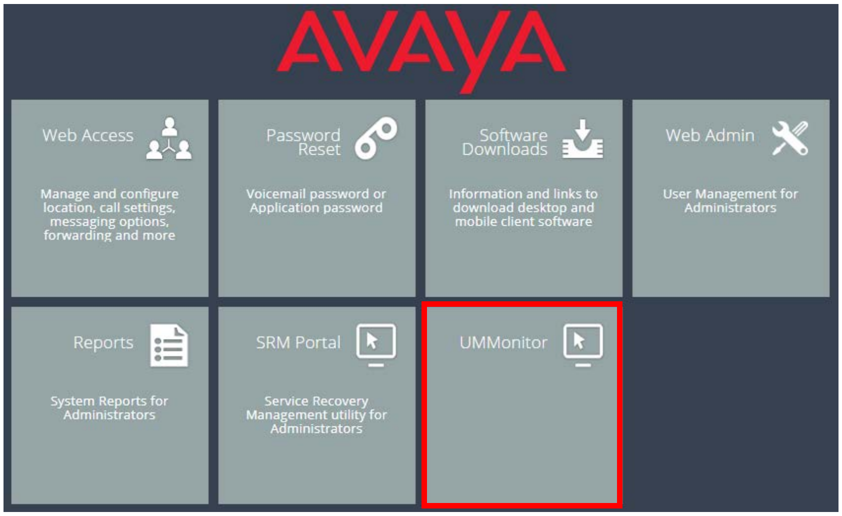
Introduction

The Web UM Monitor is a suite of tools to watch the performance of the system for the purposes of troubleshooting.

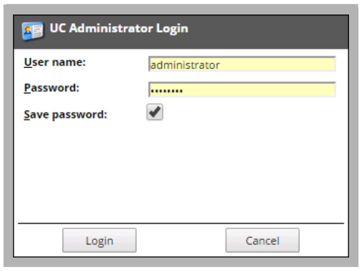
Getting Started

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.


AVAYA
Web Access
Manage and configure location, call settings, messaging options, forwarding and more
Password Reset
Voicemail password or Application password
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

2. Enter the administrator username and password for the voice server.



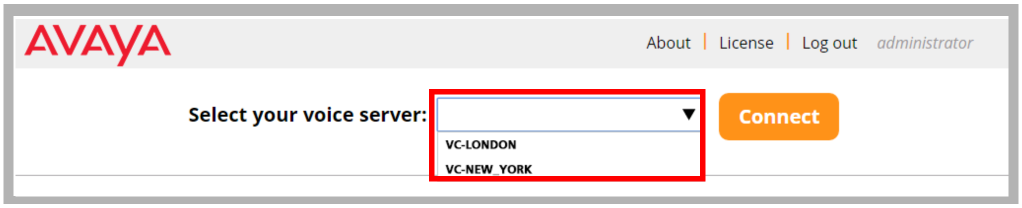
UC Administrator Login

User name: administrator

Password: ••••••••

Save password: ☑

3. From the dropdown menu, select the voice server you want to monitor.

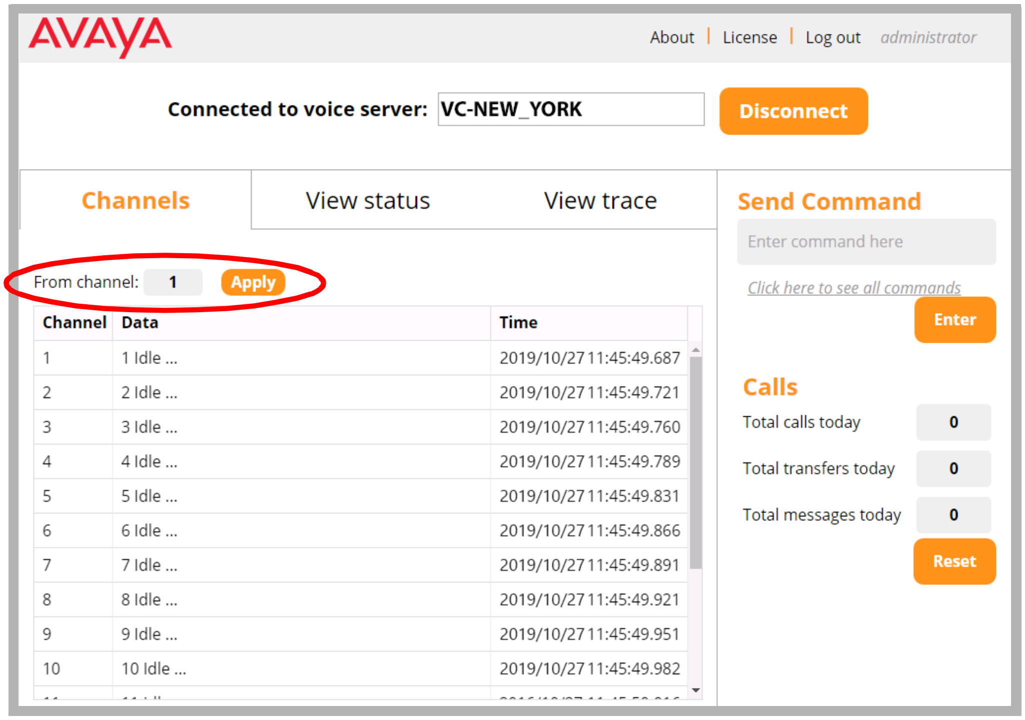

AVAYA
About | License | Log out administrator
Select your voice server:
▼
VC-LONDON
VC-NEW_YORK
Connect

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 is displayed the current status of each channel working on the voice server.



Connected to voice server: VC-NEW_YORK

From channel: 1

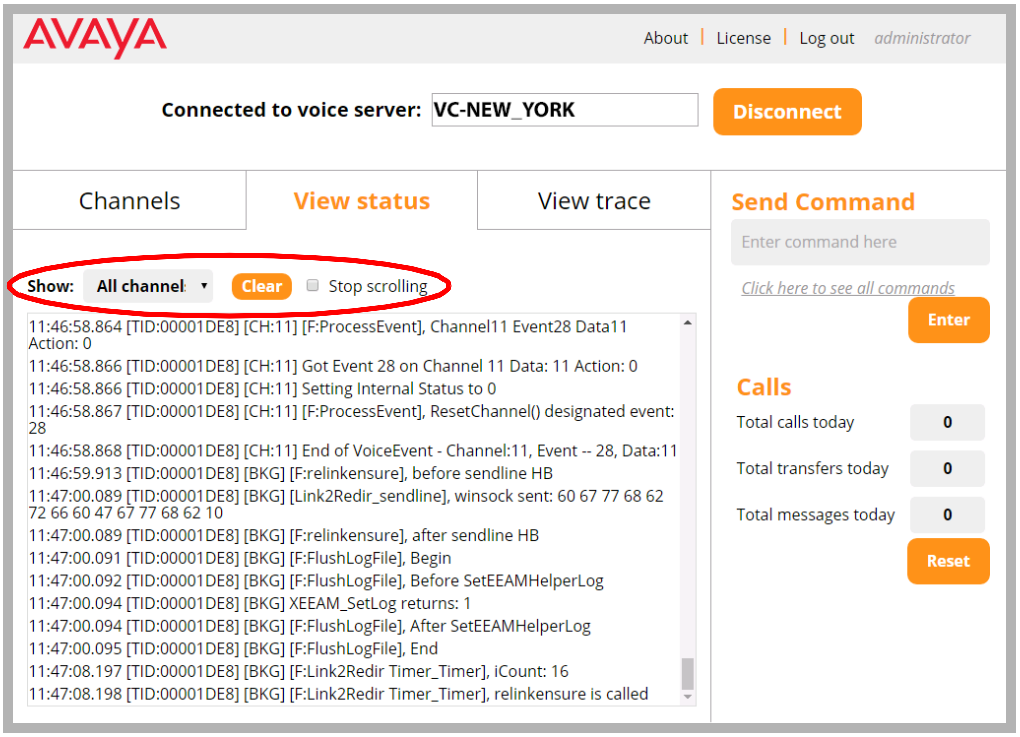
Channel	Data	Time
1	1 Idle ...	2019/10/27 11:45:49.687
2	2 Idle ...	2019/10/27 11:45:49.721
3	3 Idle ...	2019/10/27 11:45:49.760
4	4 Idle ...	2019/10/27 11:45:49.789
5	5 Idle ...	2019/10/27 11:45:49.831
6	6 Idle ...	2019/10/27 11:45:49.866
7	7 Idle ...	2019/10/27 11:45:49.891
8	8 Idle ...	2019/10/27 11:45:49.921
9	9 Idle ...	2019/10/27 11:45:49.951
10	10 Idle ...	2019/10/27 11:45:49.982

Total calls today	0
Total transfers today	0
Total messages today	0

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.



Connected to voice server: VC-NEW_YORK

Show: All channel ▾ Clear □ Stop scrolling

```
11:46:58.864 [TID:00001DE8] [CH:11] [F:ProcessEvent], Channel11 Event28 Data11
Action: 0
11:46:58.866 [TID:00001DE8] [CH:11] Got Event 28 on Channel 11 Data: 11 Action: 0
11:46:58.866 [TID:00001DE8] [CH:11] Setting Internal Status to 0
11:46:58.867 [TID:00001DE8] [CH:11] [F:ProcessEvent], ResetChannel() designated event:
28
11:46:58.868 [TID:00001DE8] [CH:11] End of VoiceEvent - Channel:11, Event -- 28, Data:11
11:46:59.913 [TID:00001DE8] [BKG] [F:relinkensure], before sendline HB
11:47:00.089 [TID:00001DE8] [BKG] [Link2Redir_sendline], winsock sent: 60 67 77 68 62
72 66 60 47 67 77 68 62 10
11:47:00.089 [TID:00001DE8] [BKG] [F:relinkensure], after sendline HB
11:47:00.091 [TID:00001DE8] [BKG] [F:FlushLogFile], Begin
11:47:00.092 [TID:00001DE8] [BKG] [F:FlushLogFile], Before SetEEAMHelperLog
11:47:00.094 [TID:00001DE8] [BKG] XEEAM_SetLog returns: 1
11:47:00.094 [TID:00001DE8] [BKG] [F:FlushLogFile], After SetEEAMHelperLog
11:47:00.095 [TID:00001DE8] [BKG] [F:FlushLogFile], End
11:47:08.197 [TID:00001DE8] [BKG] [F:Link2Redir Timer_Timer], iCount: 16
11:47:08.198 [TID:00001DE8] [BKG] [F:Link2Redir Timer_Timer], relinkensure is called
```

Total calls today	0
Total transfers today	0
Total messages today	0

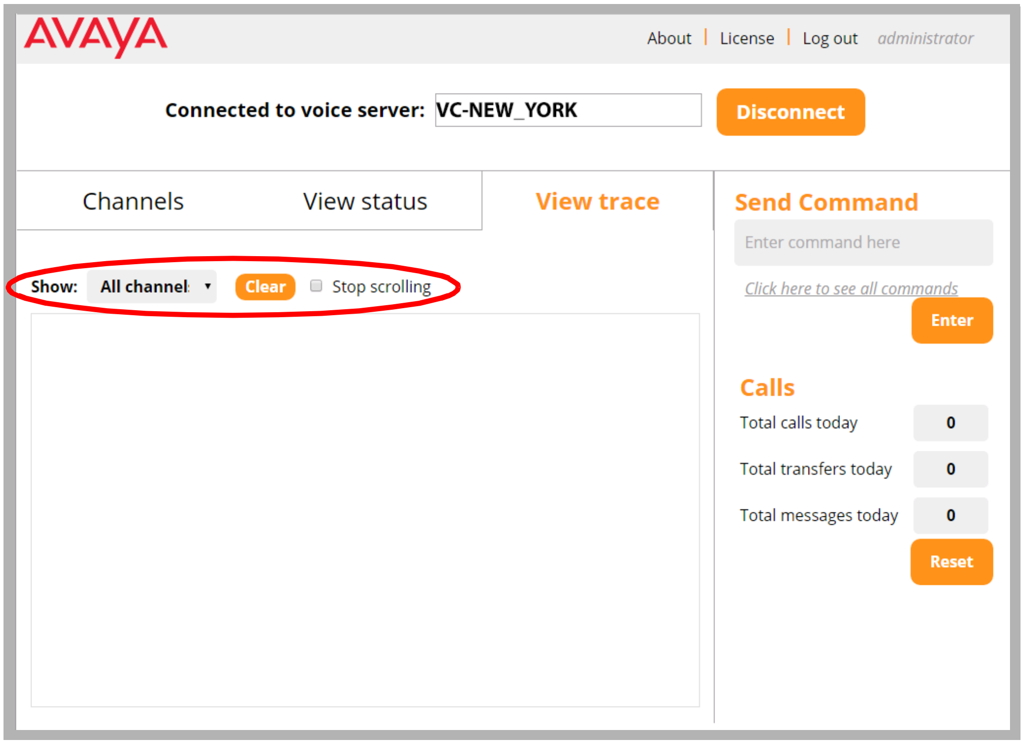
Select either **All channels** or a specific channel to monitor from the dropdown list.

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.

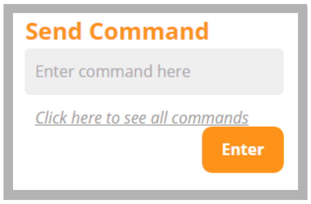
Use **Clear** to remove all status entries from the display. New status entries will begin to fill the screen.

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.

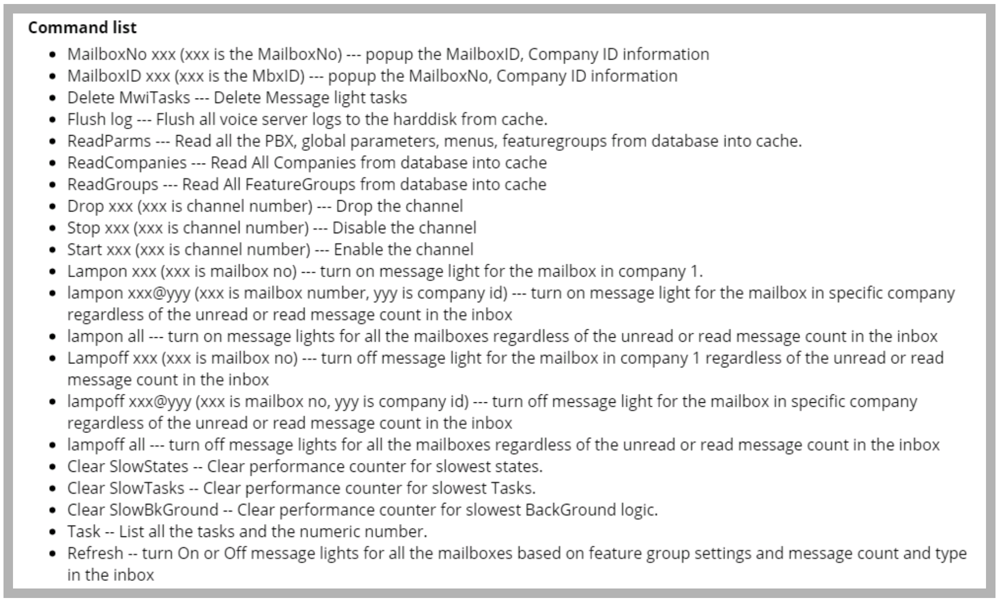
Sending Commands

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.

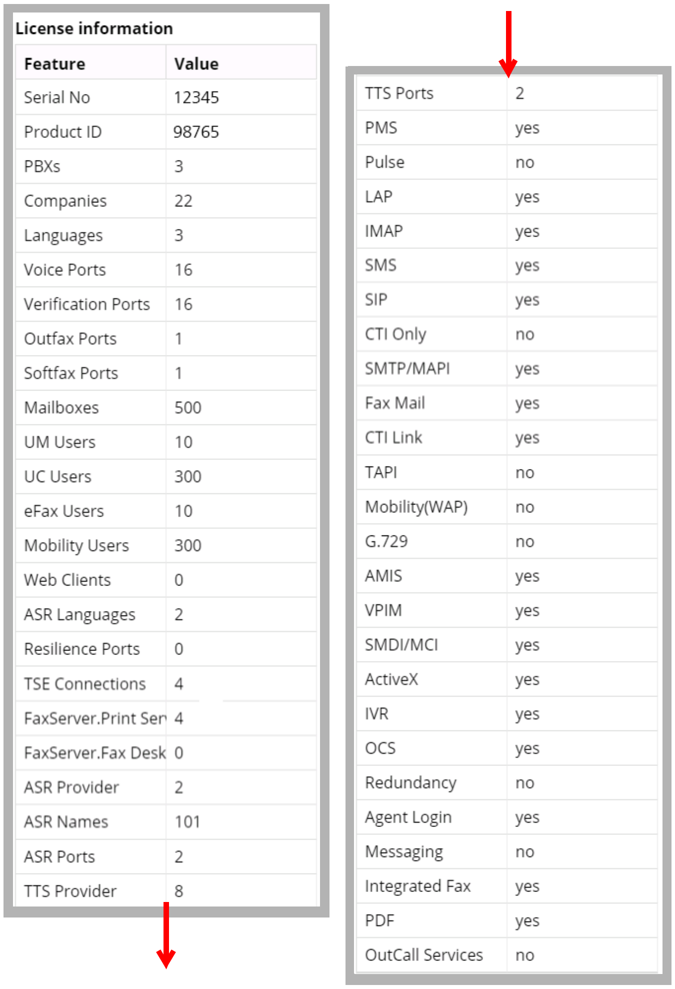


Command list

- 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

26 INTEGRATION WITH AVAYA CPaaS

In This Chapter:

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.

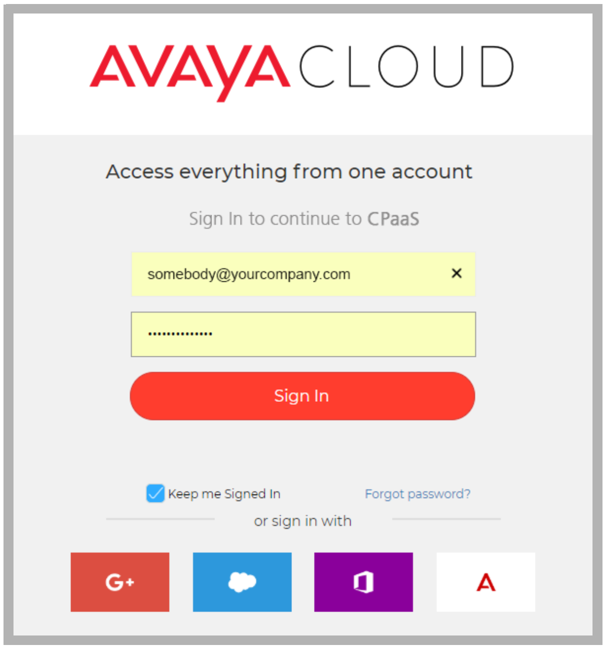
Pre-requisites

- 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 accounts.avayacloud.com. Enter your Avaya account credentials and click **Log In**.

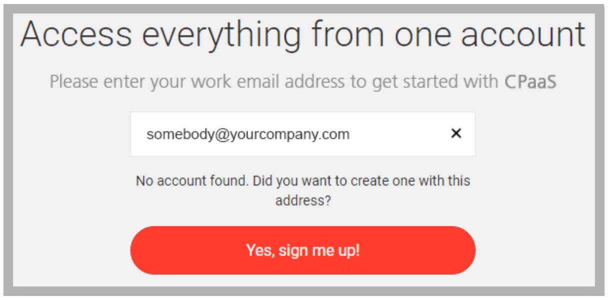


Access everything from one account

Sign In to continue to CPaaS

somebody@yourcompany.com

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.



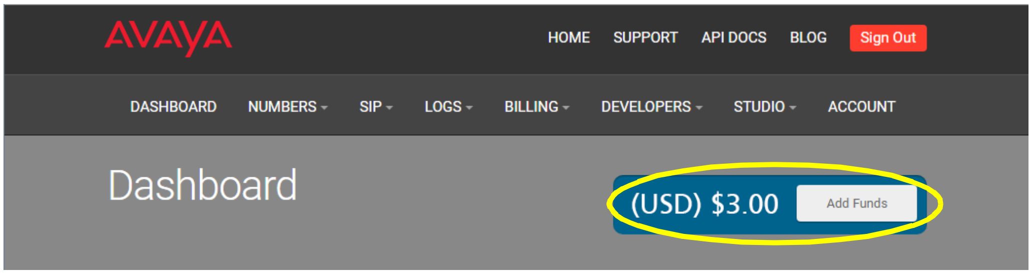
Access everything from one account

Please enter your work email address to get started with CPaaS

somebody@yourcompany.com

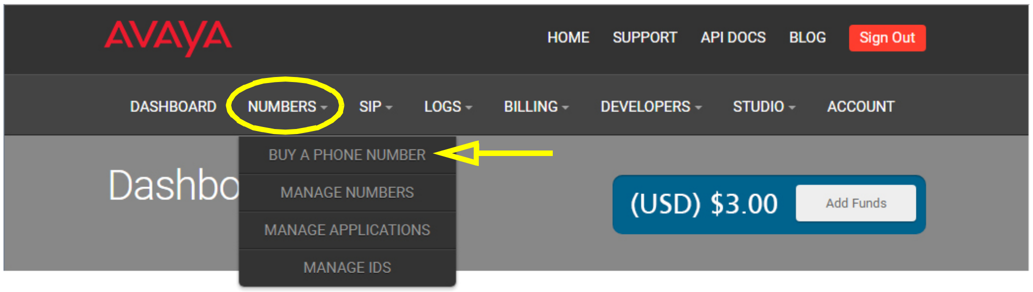
No account found. Did you want to create one with this address?

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.

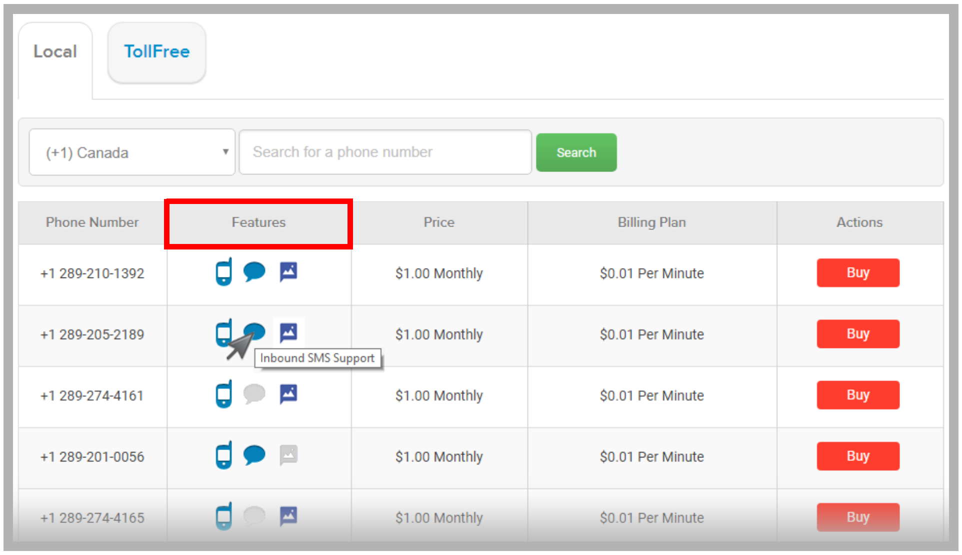


(USD) $3.00

3. With your account properly funded, select **Numbers** and click **Buy a Phone Number**.



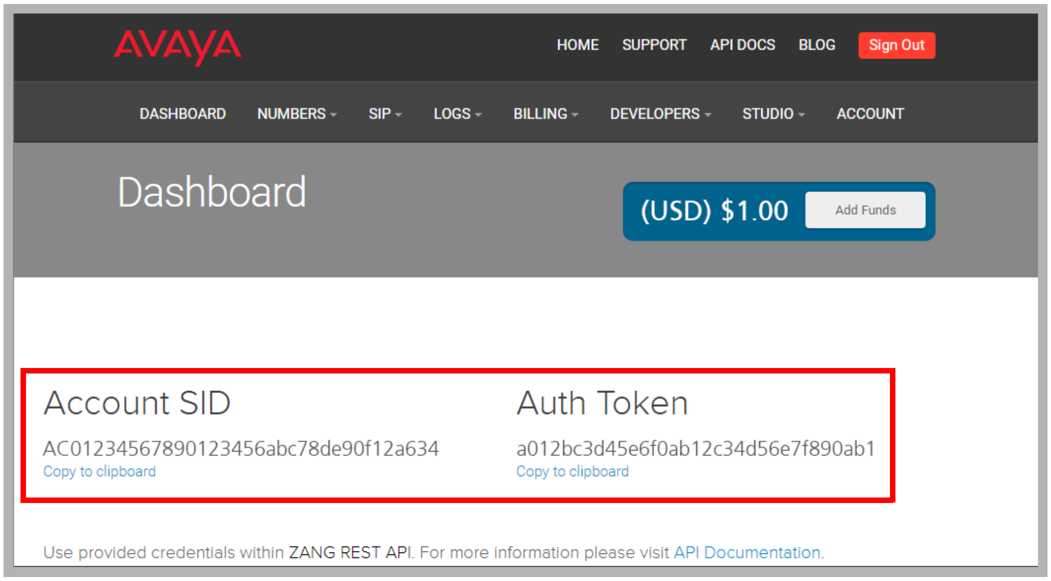
4. Choose between **Local** or **TollFree** numbers.
Select the **country** that will host the number. You can also enter the area / city code to narrow the search. Leave the search field empty to view all numbers available in the selected country.
When ready, click **Search** and the list of available numbers will appear.



Phone Number	Features	Price	Billing Plan	Actions
+1 289-210-1392	☎ 💬 🖼	$1.00 Monthly	$0.01 Per Minute	Buy
+1 289-205-2189	☎ 💬 🖼	$1.00 Monthly	$0.01 Per Minute	Buy
+1 289-274-4161	☎ ○ 🖼	$1.00 Monthly	$0.01 Per Minute	Buy
+1 289-201-0056	☎ 💬 ▢	$1.00 Monthly	$0.01 Per Minute	Buy
+1 289-274-4165	☎ ○ 🖼	$1.00 Monthly	$0.01 Per Minute	Buy

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.



Account SID

AC01234567890123456abc78de90f12a634

Auth Token

a012bc3d45e6f0ab12c34d56e7f890ab1

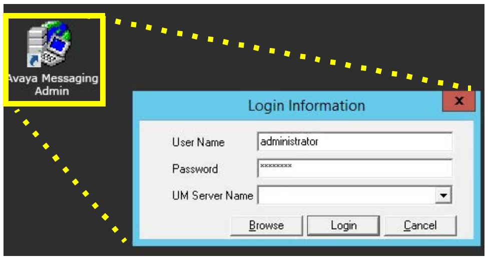
Use provided credentials within ZANG REST API. For more information please visit API Documentation.

Continue with the configuration of Avaya Messaging.

Avaya Messaging Voice Server Configuration

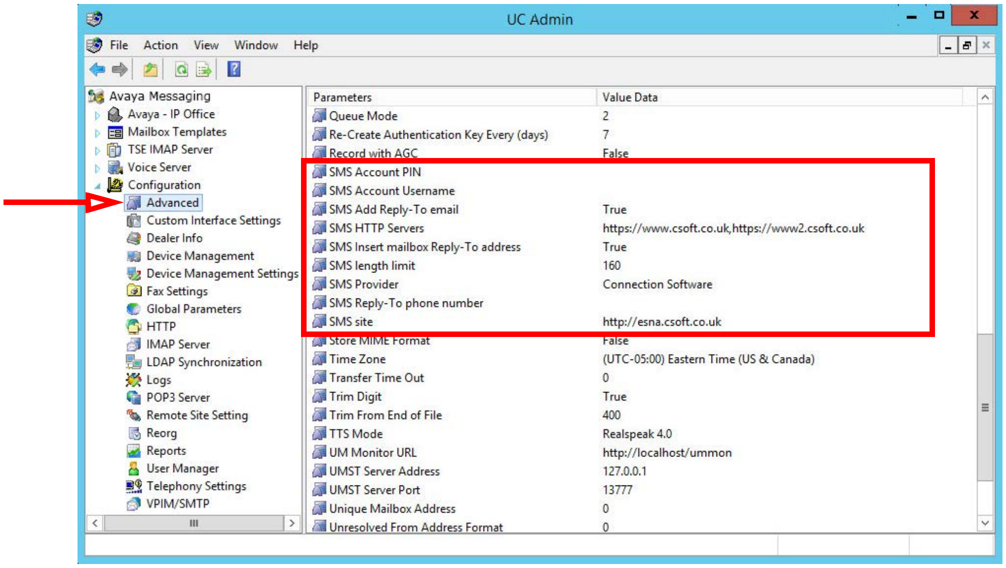
The configuration of Avaya Messaging is done using the Avaya Messaging Admin program on the Voice Server. In a High Availability environment, the configuration is done on the Consolidated Server only.

1. On the Avaya Messaging Voice Server, or the HA Consolidated Server, open **Avaya Messaging Admin** and login.



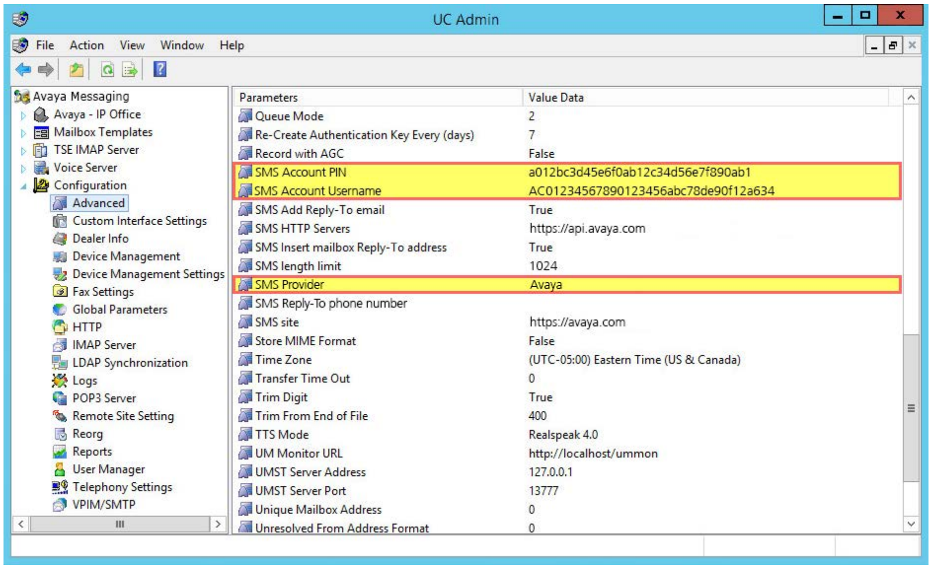
User Name: administrator
Password: ********
UM Server Name:

2. Go to **Configuration > Advanced** and scroll down to the SMS options.



Parameters	Value Data
Queue Mode	2
Re-Create Authentication Key Every (days)	7
Record with AGC	False
SMS Account PIN	
SMS Account Username	
SMS Add Reply-To email	True
SMS HTTP Servers	https://www.csoft.co.uk,https://www2.csoft.co.uk
SMS Insert mailbox Reply-To address	True
SMS length limit	160
SMS Provider	Connection Software
SMS Reply-To phone number	
SMS site	http://esna.csoft.co.uk
Store MIME Format	False
Time Zone	(UTC-05:00) Eastern Time (US & Canada)
Transfer Time Out	0
Trim Digit	True
Trim From End of File	400
TTS Mode	Realspeak 4.0
UM Monitor URL	http://localhost/ummon
UMST Server Address	127.0.0.1
UMST Server Port	13777
Unique Mailbox Address	0
Unresolved From Address Format	0

3. Make the following configuration changes. For each entry, double-click the item and modify the details where necessary.



Parameters	Value Data
Queue Mode	2
Re-Create Authentication Key Every (days)	7
Record with AGC	False
SMS Account PIN	a012bc3d45e6f0ab12c34d56e7f890ab1
SMS Account Username	AC01234567890123456abc78de90f12a634
SMS Add Reply-To email	True
SMS HTTP Servers	https://api.avaya.com
SMS Insert mailbox Reply-To address	True
SMS length limit	1024
SMS Provider	Avaya
SMS Reply-To phone number	
SMS site	https://avaya.com
Store MIME Format	False
Time Zone	(UTC-05:00) Eastern Time (US & Canada)
Transfer Time Out	0
Trim Digit	True
Trim From End of File	400
TTS Mode	Realspeak 4.0
UM Monitor URL	http://localhost/ummon
UMST Server Address	127.0.0.1
UMST Server Port	13777
Unique Mailbox Address	0
Unresolved From Address Format	0

- **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

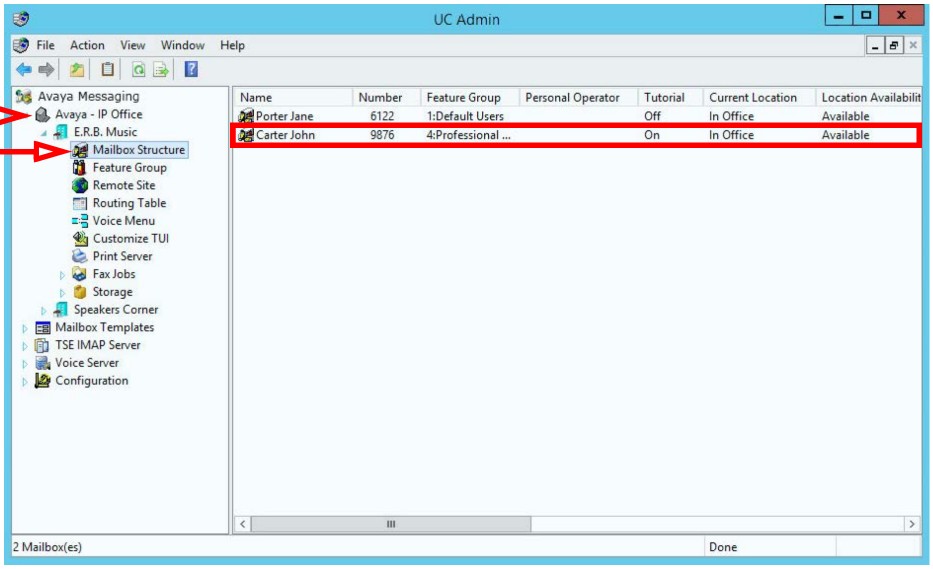
Use one of these methods if each user has exclusive use of a Avaya CPaaS telephone number.

44 20 3002 6798
905 707 9700

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**.

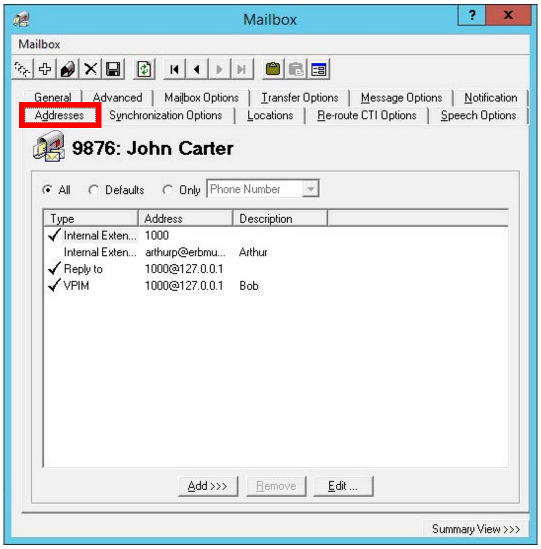


Name	Number	Feature Group	Personal Operator	Tutorial	Current Location	Location Availabilit
Porter Jane	6122	1:Default Users		Off	In Office	Available
Carter John	9876	4:Professional ...		On	In Office	Available

2 Mailbox(es)

Done

2. Double-click a user and open the **Addresses** tab.

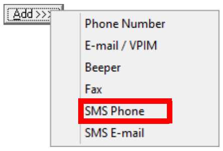


9876: John Carter

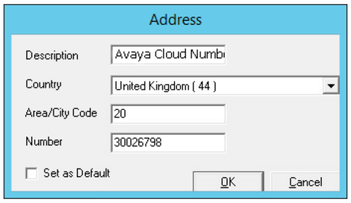
● All ○ Defaults ○ Only Phone Number

Type	Address	Description
✓ Internal Exten...	1000	
Internal Exten...	arthurp@erbmu...	Arthur
✓ Reply to	1000@127.0.0.1	
✓ VPIM	1000@127.0.0.1	Bob

3. Click **Add** and choose **SMS Phone**.



4. Enter the required information and click **OK** when ready.

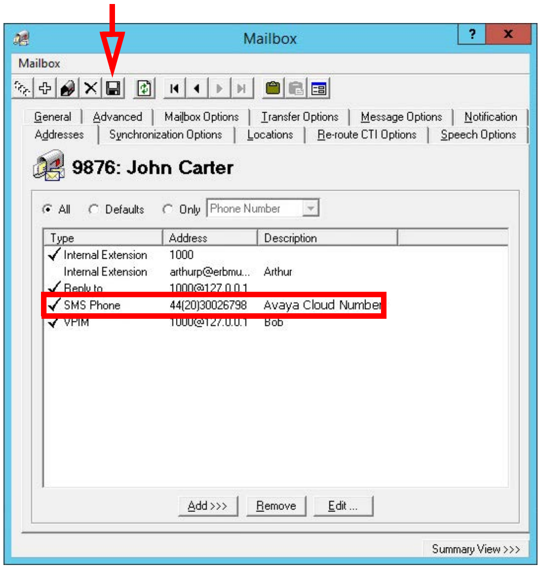


Description	Avaya Cloud Numbe
Country	United Kingdom (44)
Area/City Code	20
Number	30026798

☐ Set as Default

- **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**.



9876: John Carter

● All ○ Defaults ○ Only Phone Number

Type	Address	Description
✓ Internal Extension	1000	
Internal Extension	arthurp@erbmu...	Arthur
✓ Reply to	1000@127.0.0.1	
✓ SMS Phone	44(20)30026798	Avaya Cloud Number
✓ VPIM	1000@127.0.0.1	Bob

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.

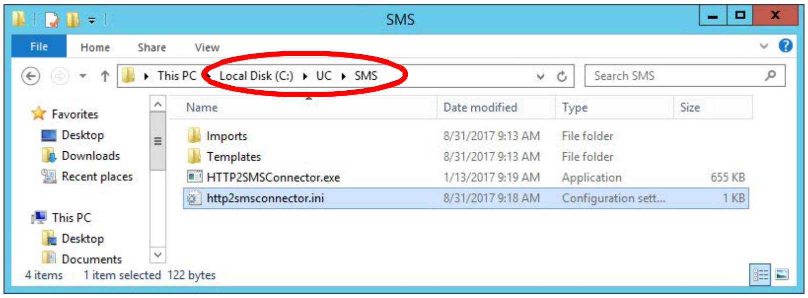
```
[Application1]
Number= 1(905)707-9700
Mailbox= 9876
Company= 1

[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.

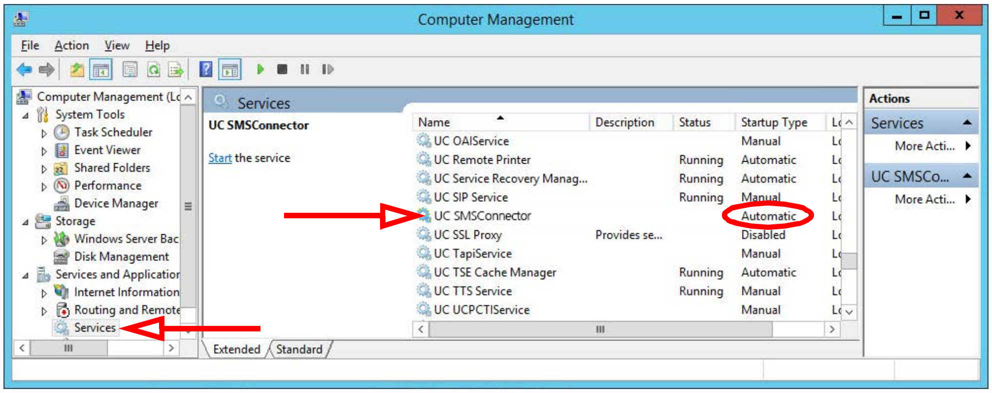
- **Mailbox=** : Enter the mailbox for the recipient. The incoming SMS message will be delivered here.
- **Company=** : For sites that have multiple tenants / companies, enter the company number for this user here. This value must match the company numbers defined on the Avaya Messaging voice server. 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.



Name	Date modified	Type	Size
Imports	8/31/2017 9:13 AM	File folder	
Templates	8/31/2017 9:13 AM	File folder	
HTTP2SMSConnector.exe	1/13/2017 9:19 AM	Application	655 KB
http2smsconnector.ini	8/31/2017 9:18 AM	Configuration sett...	1 KB

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.



Name	Description	Status	Startup Type
UC OAIService			Manual
UC Remote Printer		Running	Automatic
UC Service Recovery Manag...		Running	Automatic
UC SIP Service		Running	Manual
UC SMSConnector			Automatic
UC SSL Proxy	Provides se...		Disabled
UC TapiService			Manual
UC TSE Cache Manager		Running	Automatic
UC TTS Service		Running	Manual
UC UCPCTIService			Manual

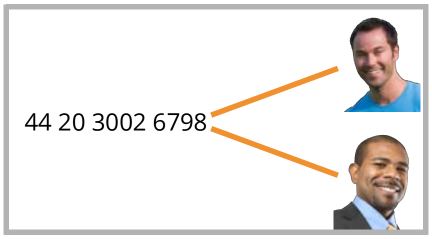
Note: You can combine both **Direct number** and **Keyword** entries in the same INI file. Only the information in each entry will change.

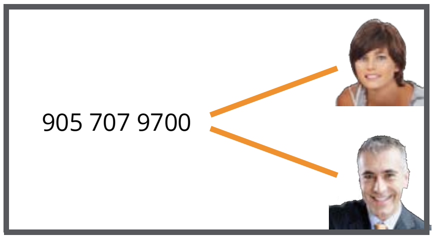
```
[Keyword1]
Value= ASKJohnC,JohnC
Mailbox= 9876
Company= 1

[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.



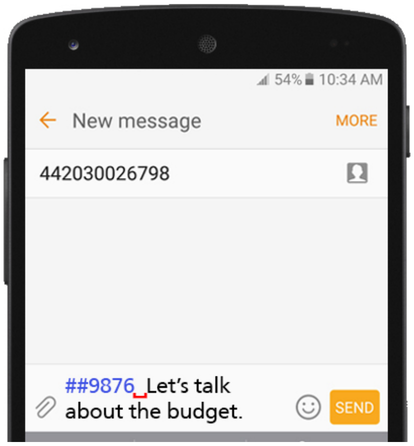


Mailbox

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.



442030026798

##9876 Let's talk about the budget.

All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to the user's mailbox 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.

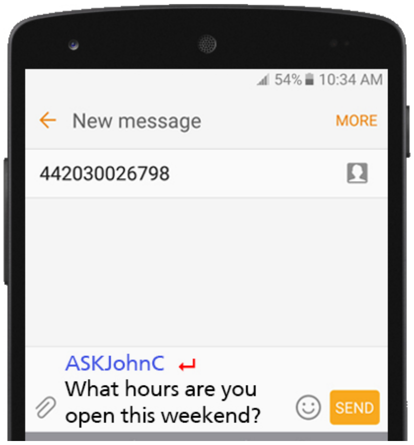
1. Open a text editing software program such as Windows Notepad and create/modify the INI file.
2. Each person using **Keyword** must have an entry in the INI file, and each entry contains four elements.

```
[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.

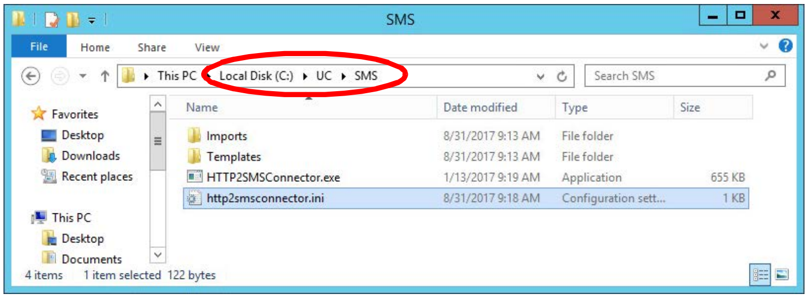
- **Mailbox=** : Enter the mailbox for the recipient. The incoming SMS message will be delivered here.
- **Company=** : For sites that have multiple tenants / companies, enter the company number for this user here. This value must match the company numbers defined on the Avaya Messaging Voice Server. In most cases, where there is only a single company configured, set this value to **1**.



442030026798

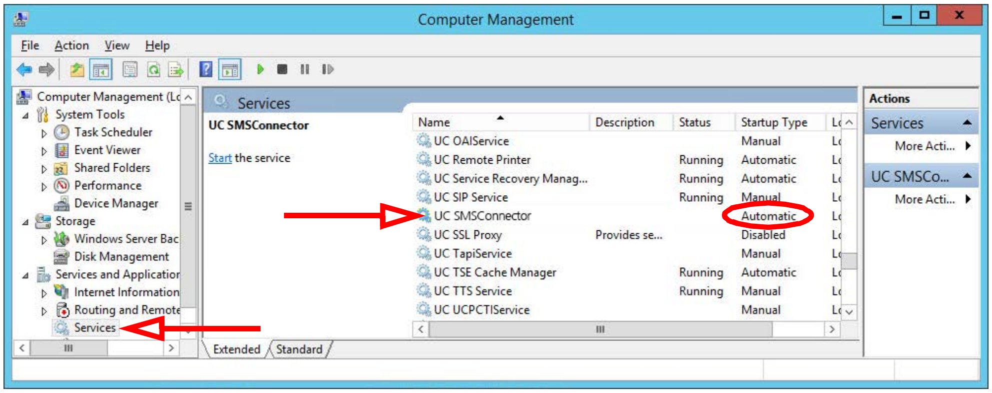
ASKJohnC ↵
What hours are you open this weekend?

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.



Name	Date modified	Type	Size
Imports	8/31/2017 9:13 AM	File folder	
Templates	8/31/2017 9:13 AM	File folder	
HTTP2SMSConnector.exe	1/13/2017 9:19 AM	Application	655 KB
http2smsconnector.ini	8/31/2017 9:18 AM	Configuration sett...	1 KB

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.



Name	Description	Status	Startup Type	Lo
UC OAIService			Manual	Lo
UC Remote Printer		Running	Automatic	Lo
UC Service Recovery Manag...		Running	Automatic	Lo
UC SIP Service		Running	Manual	Lo
UC SMSConnector			Automatic	Lo
UC SSL Proxy	Provides se...		Disabled	Lo
UC TapiService			Manual	Lo
UC TSE Cache Manager		Running	Automatic	Lo
UC TTS Service		Running	Manual	Lo
UC UCPCTIService			Manual	Lo

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
```

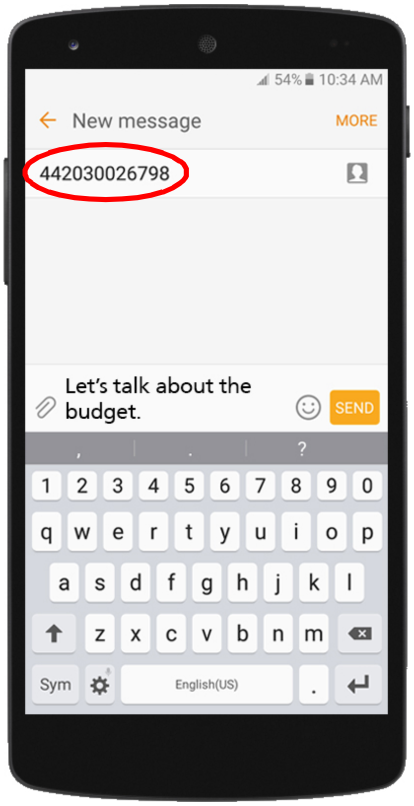
Addressing SMS Messages

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.



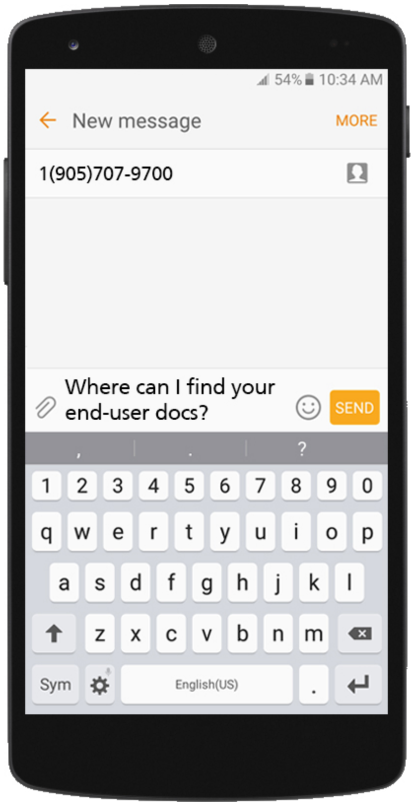
442030026798

Let's talk about the budget.

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.



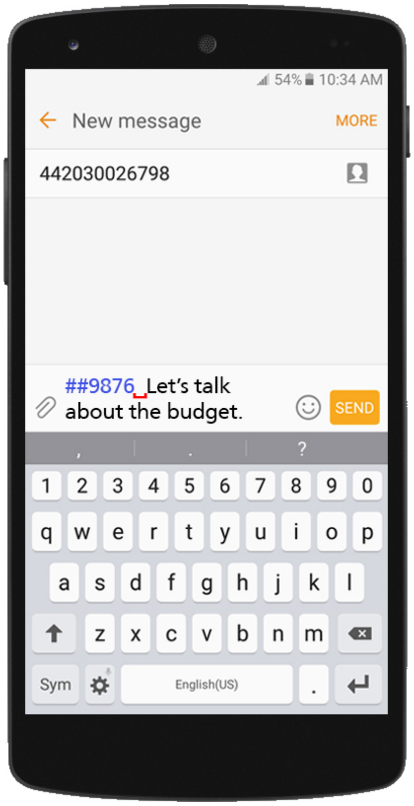
1(905)707-9700

Where can I find your end-user docs?

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**).



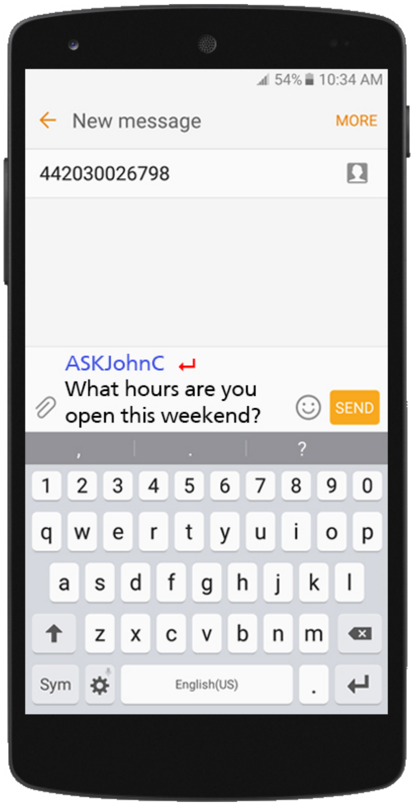
442030026798

##9876 Let's talk about the budget.

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.



442030026798

ASKJohnC ↵
What hours are you open this weekend?

The Voice Server spots the keyword and uses the INI file to direct the message to the correct mailbox.

27 ONAVAYA AUTHENTICATION

In This Chapter:

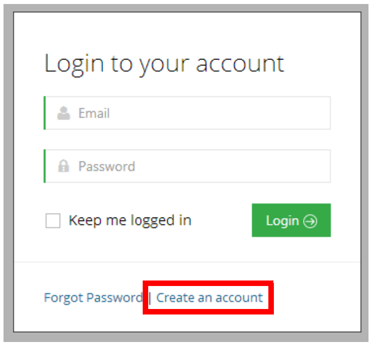
Introduction

Logging in to an application using **Avaya credentials** provides a web-based authentication solution (**OnAvaya**) for sites where Gmail and Salesforce are not available. Creating a user account with OnAvaya allows access to a range of programs using secure access protocols.

Creating an Account with OnAvaya

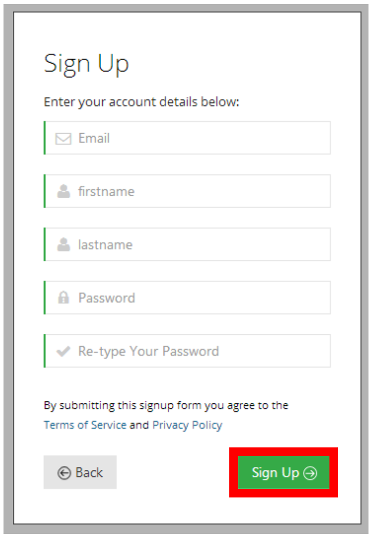
Before attempting to login using Avaya credentials for the first time, it is necessary to create an account at OnAvaya.

1. Open a browser and go to https://accounts.avayacloud.com.
2. At the login screen, click **Create an account**.



3. On the **Sign Up** screen, enter your corporate email address, your first and last names, and the password you want to use with OnAvaya. Re-enter the password to confirm.

   When finished, click **Sign Up**.

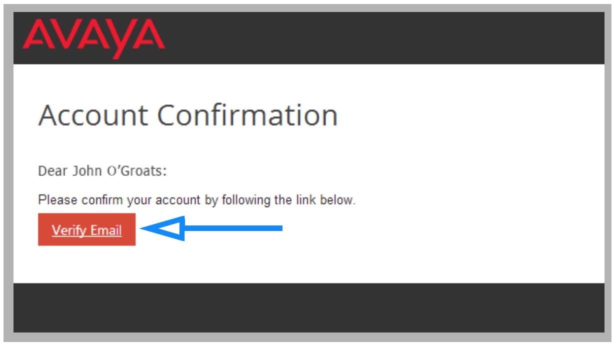


Enter your account details below:

By submitting this signup form you agree to the Terms of Service and Privacy Policy

4. A confirmation email will be sent to the address provided.

   Open the message and click **Verify Email**.

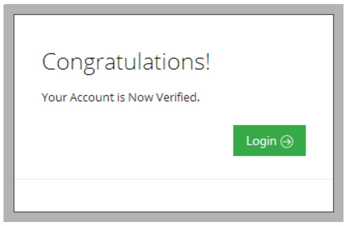


Account Confirmation

Dear John O'Groats:

Please confirm your account by following the link below.

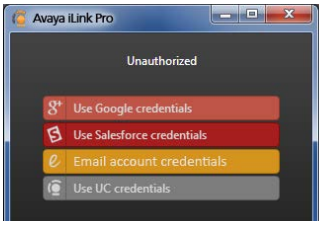
5. OnAvaya account setup is complete. Click **Login**.



Congratulations!

Your Account is Now Verified.

Logging In Through OnAvaya



Important: The system administrator can enable a security policy to limit the login credentials available. Contact your administrator for more information.

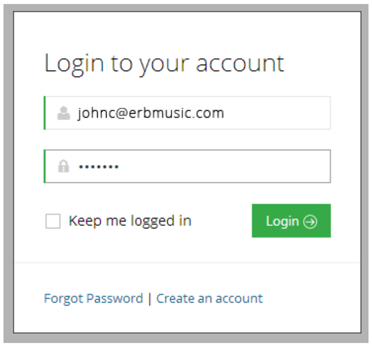
For all applications, the login procedure is the same when you select **Email Credentials** to start the program.

1. At the login page, choose **Email account** from the drop down list.

Hint: From the **Connection** page, click the **Utility Menu** and select **Clear credentials** to delete all login details and restart the login procedure.

2. When prompted, enter your username and password. Click **Login**.

Note: Enable **Keep me logged in** to have OnAvaya automatically use the same credentials on all subsequent login attempts. You will be seamlessly logged in to all client extension each time the browser is launched.


Login to your account

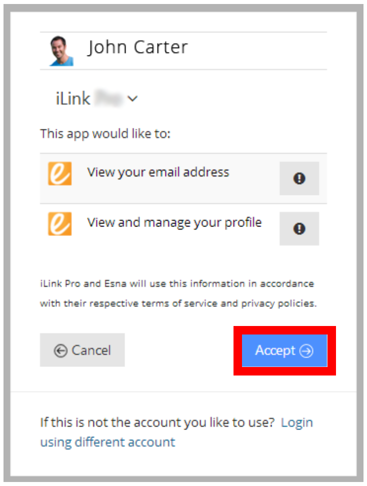
johnc@erbmusic.com

•••••••

□ Keep me logged in

3. If prompted to grant Avaya iLink permissions, click **Accept**.

Note: This only needs to be done the first time you login to the client.


John Carter

iLink

This app would like to:

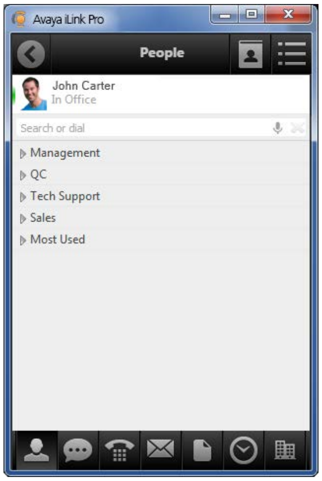
View your email address

View and manage your profile

iLink Pro and Esna will use this information in accordance with their respective terms of service and privacy policies.

If this is not the account you like to use? Login using different account

4. The Avaya iLink client will start.



Note: In order for the program to save your settings, you must allow your web browser to **accept 3rd party cookies**. Some browsers may reject 3rd party cookies either as a default setting or through an organizational policy.

28 ACCESSIBILITY

Introduction

Avaya Messaging provides greater accessibility to people with special needs. Avaya Messaging offers 508 compliance and TTY integration.

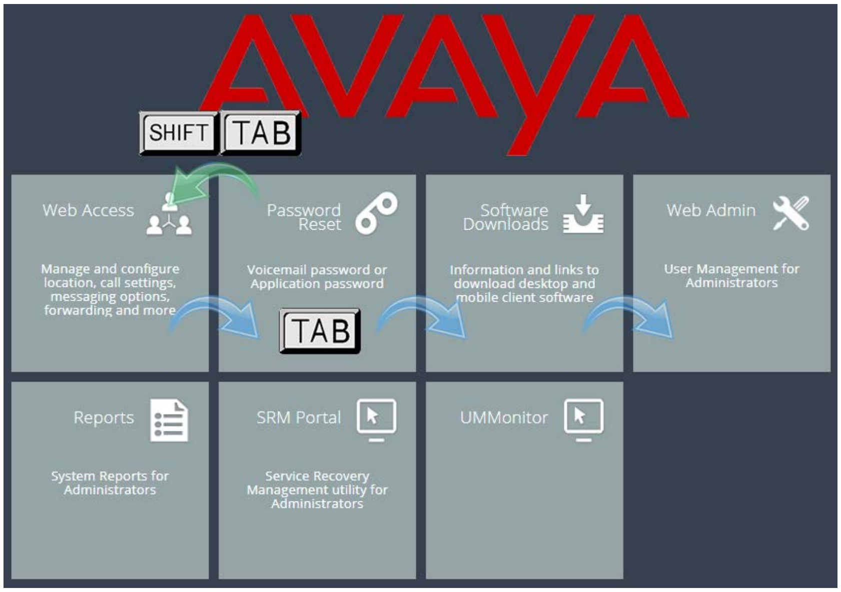
508 Compliance

Complying with the 508 standard 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.



Web Access: Manage and configure location, call settings, messaging options, forwarding and more

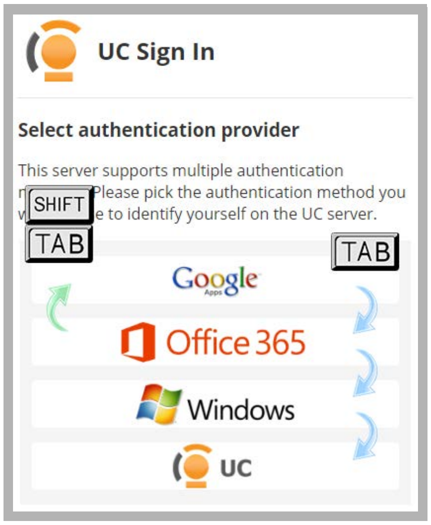
Password Reset: Voicemail password or Application password

Software Downloads: Information and links to download desktop and mobile client software

Web Admin: User Management for Administrators

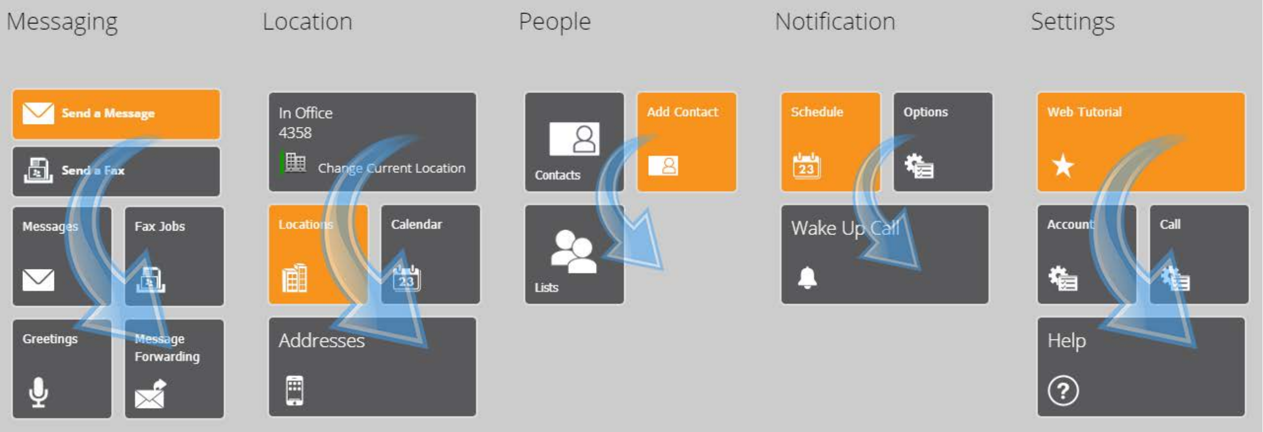
Reports: System Reports for Administrators

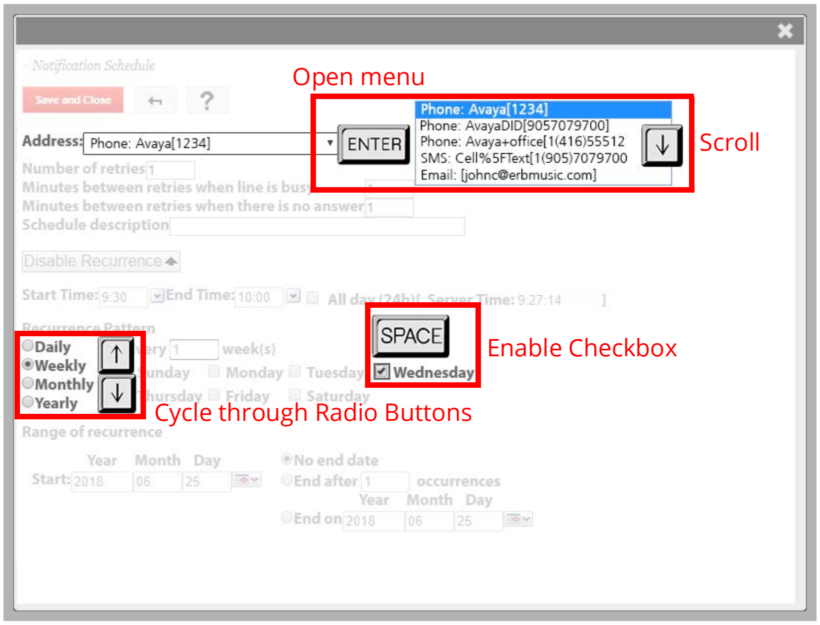
SRM Portal: Service Recovery Management utility for Administrators



Select authentication provider

This server supports multiple authentication r... Please pick the authentication method you w... e to identify yourself on the UC server.





Open menu

Scroll

Enable Checkbox

Cycle through Radio Buttons

Address: Phone: Avaya[1234]

- Phone: Avaya[1234]
- Phone: AvayaDID[9057079700]
- Phone: Avaya+office[1(416)55512
- SMS: Cell%5FText[1(905)7079700
- Email: [johnc@erbmusic.com]

Number of retries 1

Minutes between retries when line is busy 1

Minutes between retries when there is no answer 1

Schedule description

Start Time: 9:30 End Time: 10:00 □ All day (24h) [Server Time: 9:27:14]

Recurrence Pattern

○ Daily
● Weekly
○ Monthly
○ Yearly

Every 1 week(s)

□ Sunday □ Monday □ Tuesday ☑ Wednesday
□ Thursday □ Friday □ Saturday

Range of recurrence

Start: Year 2018 Month 06 Day 25

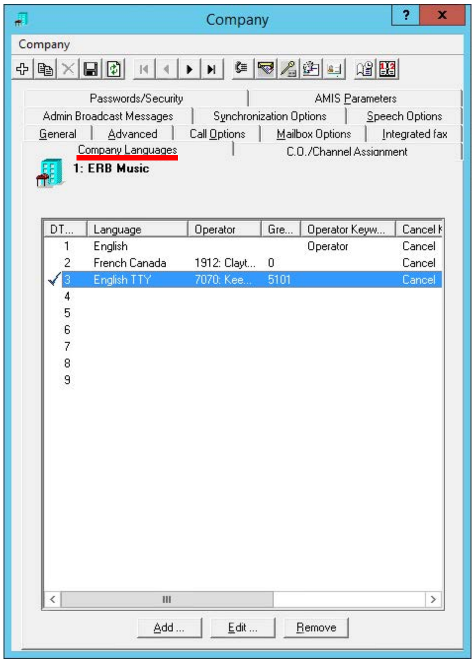
● No end date
○ End after 1 occurrences
○ End on Year 2018 Month 06 Day 25

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**.

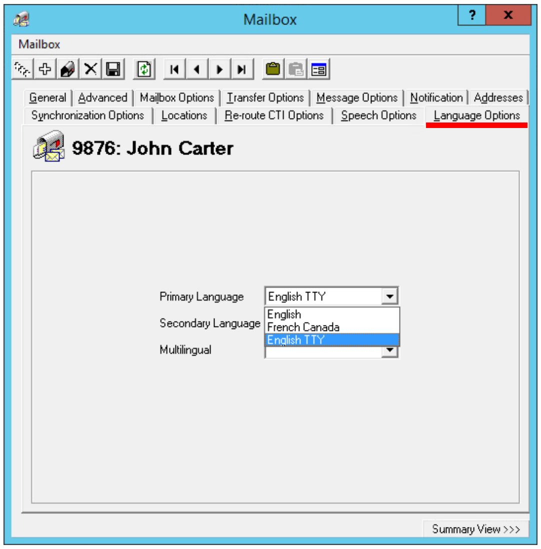
Install the language pack according to the instructions found on page 635 of the **Server Installation Guide**.

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.



1: ERB Music

DT...	Language	Operator	Gre...	Operator Keyw...	Cancel K
1	English			Operator	Cancel
2	French Canada	1912: Clayt...	0		Cancel
✓ 3	English TTY	7070: Kee...	5101		Cancel
4					
5					
6					
7					
8					
9					



9876: John Carter

Primary Language: English TTY

Secondary Language: English / French Canada / English TTY

Multilingual

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.

APPENDIX A: REVISION HISTORY

Date	Change Summary
27 April, 2021	Initial Document Release.
29 April, 2021	Updated the EWS OAuth configuration procedure.
23 September, 2021	Corrected some configuration issues (Block UDP Port=False). Note regarding HA time zones all being the same.
12 October, 2021	Updated the ASR section to include verification of the license using WebLM.
13 October, 2021	Updated the OAuth 2 configuration section for Google integration.
29 October, 2021	Added section for configuring a single DID to handle both fax and voice traffic.
17 December, 2021	New note regarding the minimum length of voice greeting to allow fax detection to occur.
4 February, 2022	Removed non-Avaya brands from list of supported platforms.
18 March, 2022	Updated notification regarding the maximum length of a transcribed message (from 60 seconds to unlimited (subject to admin config)).
24 June, 2022	Updated the MS Graph integration guide.
29 June, 2022	Corrected issue with Google integration.