Officelinx is a feature rich application which offers a solution for virtually any organization or situation. The productivity enhancing nature of Officelinx 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 Officelinx 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 Officelinx, this guide separates each feature and explains in detail how it 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 ACCESES 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 dif-
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

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.
# AVAYA OFFICELINX FEATURE DESCRIPTION GUIDE

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>21</strong> AUTOMATIC SPEECH RECOGNITION (ASR)</td>
<td></td>
</tr>
</tbody>
</table>
| **22** INTRODUCTION | Visual Guide
| **22** Requirements | |
| **23** SERVER CONFIGURATION | License Confirmation
| **24** OL Admin Configuration | |
| **25** ASR Configurator | |
| **27** ENHANCED CALL CONTROL | |
| **28** INTRODUCTION | Visual Guide
| **29** Requirements | |
| **30** SERVER CONFIGURATION | Company
| **30** Feature Group | |
| **31** USER GUIDE | ECC Command List
| **31** Initiating a Handoff to Predefined Numbers | |
| **31** Initiating a Handoff to Custom Numbers | |
| **33** SPEECH COMMANDS | |
| **34** INTRODUCTION | Visual Guide
| **34** Requirements | |
| **35** SERVER CONFIGURATION | Company Properties
| **35** Feature Group Properties | |
| **36** Mailbox Properties | |
| **36** Customize TUI Configuration | |
37 USER GUIDE
37 Basic TUI Navigation
37 Temporarily Disable Speech Command

39 SPEECH CONTACTS

40 INTRODUCTION
40 Visual Guide
40 Requirements

41 SERVER CONFIGURATION
41 Procedure

43 USER GUIDE
43 Enabling Speech Contacts

45 GOOGLE INTEGRATION

46 INTRODUCTION
47 Implementation Example
47 Requirements

48 SERVER CONFIGURATION
48 Synchronization for a Single User
48 TSE IMAP Configuration
49 Mailbox
50 Feature Group

51 INSTALL AND CONFIGURE OAUTH2.0
51 OAuth 2.0 Setup
57 Domain Setup
60 Minimum Required Scopes and APIs by Product
61 Configuring Officelinx
63 Contact & Calendar Synchronization
63 OL Admin
64 Feature Group
65 Synchronizing Contacts and/or Calendar Only
65 TSE IMAP Configuration
66 Mailbox
67 Feature Group
69 Google Desktop, Google Talk & Web Gadgets
69 ISA Settings for Google Web Gadget Integration
70 Adding a MIME Type for .GG Files
71 Disable IMAP

72 USER GUIDE
72 iLink Pro On Google Web Gadgets
72 Web Gadget From UC Server
73 Using UC Web Gadgets
Message Synchronization
Contact & Calendar Synchronization
Contact Sync
Calendar Sync
Manual Contact Importing

WEBLINKS

INTRODUCTION
Configuration Process
Configuration with IIS 7
Configuration with IIS 6
Officelinx Configuration
Weblinks Example

EMAIL ACTION SCHEMA

INTRODUCTION

ENABLE ACTION SCHEMA

EMAIL BUTTONS
Dial
View
Contact Location

MUTARE TRANSCRIPTION SERVICE

INTRODUCTION
Visual Guide
Requirements

LICENSING
Upgrading the License

OFFICELINX SERVER CONFIGURATION
Transcription Configuration Tool

VERIFICATION

USER GUIDE

EXCHANGE 2016/2013 INTEGRATION: USING EWS

INTRODUCTION
Visual Guide
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>106</td>
<td>Requirements</td>
</tr>
<tr>
<td>107</td>
<td>SERVER CONFIGURATION</td>
</tr>
<tr>
<td>107</td>
<td>Exchange Superuser Creation/Configuration</td>
</tr>
<tr>
<td>109</td>
<td>OL Admin Configuration</td>
</tr>
<tr>
<td>109</td>
<td>Adding the TSE Endpoint for EWS</td>
</tr>
<tr>
<td>110</td>
<td>Feature Group Configuration</td>
</tr>
<tr>
<td>110</td>
<td>Individual Mailbox Configuration</td>
</tr>
<tr>
<td>111</td>
<td>Certificate Configuration</td>
</tr>
<tr>
<td>113</td>
<td>Contact and Calendar Sync</td>
</tr>
<tr>
<td>113</td>
<td>Windows Configuration</td>
</tr>
<tr>
<td>115</td>
<td>Officelinx Configuration - Feature Group</td>
</tr>
<tr>
<td>116</td>
<td>USER GUIDE</td>
</tr>
<tr>
<td>116</td>
<td>Calendar Synchronization</td>
</tr>
<tr>
<td>116</td>
<td>Contact Synchronization</td>
</tr>
<tr>
<td>117</td>
<td>Synchronization Limits</td>
</tr>
<tr>
<td>117</td>
<td>MS Exchange Performance Considerations</td>
</tr>
<tr>
<td>119</td>
<td>EXCHANGE 2013 INTEGRATION: NON-EWS</td>
</tr>
<tr>
<td>120</td>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>120</td>
<td>Visual Guide</td>
</tr>
<tr>
<td>120</td>
<td>Requirements</td>
</tr>
<tr>
<td>121</td>
<td>SERVER CONFIGURATION</td>
</tr>
<tr>
<td>121</td>
<td>Exchange 2013 superuser Creation/Configuration</td>
</tr>
<tr>
<td>126</td>
<td>OL Admin Configuration</td>
</tr>
<tr>
<td>126</td>
<td>Adding the TSE Endpoint</td>
</tr>
<tr>
<td>127</td>
<td>Individual Mailbox Configuration</td>
</tr>
<tr>
<td>128</td>
<td>Feature Group Configuration</td>
</tr>
<tr>
<td>129</td>
<td>Registry Settings</td>
</tr>
<tr>
<td>130</td>
<td>Certificate Configuration</td>
</tr>
<tr>
<td>132</td>
<td>Contact and Calendar Sync</td>
</tr>
<tr>
<td>133</td>
<td>Windows Configuration</td>
</tr>
<tr>
<td>134</td>
<td>Officelinx Configuration - Feature Group</td>
</tr>
<tr>
<td>135</td>
<td>USER GUIDE</td>
</tr>
<tr>
<td>135</td>
<td>Calendar Synchronization</td>
</tr>
<tr>
<td>135</td>
<td>Contact Synchronization</td>
</tr>
<tr>
<td>136</td>
<td>MS Exchange Performance Considerations</td>
</tr>
<tr>
<td>137</td>
<td>EXCHANGE 2010 INTEGRATION</td>
</tr>
<tr>
<td>138</td>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>138</td>
<td>Visual Guide</td>
</tr>
<tr>
<td>138</td>
<td>Requirements</td>
</tr>
</tbody>
</table>
139  SERVER CONFIGURATION
139   Creating a superuser from Active Directory
141   Exchange 2010 superuser Creation/Configuration
145   Exchange 2010 Shell Configuration
145     Configuring the IMAP server
145     Start the IMAP Service
146   IMAP Enabling All Existing Mailboxes in a Store
146   Configuring Permissions for the superuser Account
147   IMAP Enable a New Mailbox
148   OL Admin Configuration
148     Adding the TSE Endpoint
148     Individual Mailbox Configuration
149   Feature Group Configuration
150   Registry Settings
151   Certificate Configuration
153   Contact and Calendar Sync
154   Feature Group

155  USER GUIDE
155   Calendar Synchronization
155   Contact Synchronization
156   MS Exchange Performance Considerations

157  OFFICELINX TO OFFICE 365 INTEGRATION WITH EWS

158  INTRODUCTION

158  PRE-REQUISITES

159  OFFICE 365 CONFIGURATION
159   Web Interface Configuration (Part 1)
162   Windows PowerShell configuration
163   Web Interface Configuration (Part 2)

165  AVAYA OFFICELINX SERVER
165   Server Configuration

167  VERIFY CONFIGURATION SETTING

169  IBM DOMINO INTEGRATION

170  INTRODUCTION
170   Visual Guide
170   Requirements

171  SERVER CONFIGURATION
171   Setting up IMAP TSE Synchronization
172   Officelinx Configuration: Single User
172   To create TSE IMAP connections
173  Setting Up Unified Messaging (UM)
175  Installing UC Forms for IBM Notes
175  Using the Provided Template as Design (Method A)
181  Adding UC Forms to Existing Design (Method B)

182  USER GUIDE
182  Installing UC Forms in IBM Notes
182  Installing UC Bar and iLink Pro Desktop
183  Verifying the IBM Notes client ECL setup
184  Using UC Forms in IBM Notes
184  Composing a Voice Message
185  Listening to a Voice Message
186  Configuring UC Mailbox to Synchronize with IBM Notes

187  FIND ME FOLLOW ME ON CTI INTEGRATION

188  INTRODUCTION
188  Visual Guide
188  Requirements

190  USER GUIDE
190  Find me Follow me with CTI Integration
191  Addresses
193  Configuring Find me Follow me features

199  PROPERTY MANAGEMENT SYSTEM

200  INTRODUCTION
200  Check-in overview
200  Supported Vendors
201  PMS features
201  Connections
201  Supported functions
203  Maid Status
204  Message type examples
204  From Property Management Interface:
204  From Voice Mail Server:
205  Display
205  Class of Service
205  Wake-Up Call

206  SETTING UP PMS INTEGRATION
206  Step 1 - Verify connections
207  Step 2 - Specify PMS configuration settings
207  To specify PMS configuration settings:
209  Settings for your PMS package
210  Step 3 - Create mailboxes and assign feature groups
210  Feature Group 1 - for room mailboxes
MASS RECALL

INTRODUCTION
Visual Guide
Requirements

SERVER CONFIGURATION
Message as an outside caller
Message sent by a user from their Mailbox

ACTIVATING MASS RECALL LOGS

MASS RECALL EXAMPLE
Mass Recall Destination Mailbox
Mass Recall Activation/Cancellation Mailbox
Mass Recall Activation
Mass Recall Cancellation

OUTCALL TASK MANAGER (ABSENTEEISM)

INTRODUCTION
Visual Guide
Requirements

SERVER CONFIGURATION
Creating an Outcall List
Import from File
Open File
Add an Entry Manually
Setting the Outcall Schedule
Creating a Custom Outcall Message
Managing the Outcall Tasks

THE RESPONSE LOG

MULTIPLE TIME ZONE SUPPORT

INTRODUCTION
Visual Guide
Requirements

SERVER CONFIGURATION
General Settings
REMOTE ADMINISTRATION

INTRODUCTION
Visual Guide
Requirements

INSTALLING REMOTE ADMIN

CONNECTING TO REMOTE ADMIN

REMOTE PRINTER

INTRODUCTION

REMOTE PRINTER HOST INSTALLATION AND SETUP

OFFICELINX VOICE SERVER REMOTE PRINTER SETUP

AVAYA OFFICELINX FAXING

INTRODUCTION
Requirements

FAX VIA WINDOWS FAX SERVICES (WINDOWS 7)
Configuration
Sending Fax from an Application

FAX VIA WINDOWS FAX SERVICES (WINDOWS XP)
Configuration
Sending Fax from an Application
Viewing the Status of a Fax
Receiving and Viewing a Fax
Canceling a Fax Job
Automatically Send Retry
Automatically Canceling a Fax

EMAIL TO FAX
Administrator Setup
Sending a Fax
Fax Activation
Sending a Fax through Fax Gadget

FAX JOBS

SOFTFAX
INTRODUCTION

Visual Guide
Requirements
Specifications
PC usage:

SERVER CONFIGURATION

Licensing Information
Admin Settings
Confirmation of Service for IIS7
Setting up mailboxes for soft fax

DIALOGIC SR140 FAX INTEGRATION

INTRODUCTION

SR140 VS SOFTFAX

PRE-REQUISITES

CONFIGURATION

License Manager
Configuration Manager
Officelinx Configuration
Monitoring Channel Activity
Setup
Monitoring via Browser

DIALOGIC SR140 SECURE FAX

INTRODUCTION

PRE-REQUISITES

CONFIGURATION

License Manager
Configuration Manager
Avaya Aura Communication Manager Configuration
Avaya Aura System Manager Setup
Officelinx Configuration

WEB ACCESS

INTRODUCTION

GETTING STARTED

Logging In
1 AUTOMATIC SPEECH RECOGNITION (ASR)

In This Chapter:

- 22 Introduction
- 22 Visual Guide
- 22 Requirements
- 23 Server Configuration
- 23 License Confirmation
- 24 OL Admin Configuration
- 25 ASR Configurator
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.

Visual Guide

ASR provides the base for all speech recognition functions, such as Speech Contacts and Speech Commands. ASR interprets a user’s voice input as a number or a character (e.g. alphabet) based on the grammar settings on the server. This allows users to speak the name of the contact they want to dial, or to say a number instead of pressing the digit on the telephone keypad. By replacing traditional input with speech, users can efficiently find what they were looking for. It also 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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>ASR License</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.x or higher</td>
</tr>
</tbody>
</table>
Server Configuration

Server configuration for ASR is completed in several steps.
First, verify the Officelinx 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 Officelinx 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.

Check the UC License Upgrade Utility under Programs > Officelinx. Ensure that the information in the ASR section of the license contains the appropriate details.

With the license confirmed, launch the Officelinx Administrator to configure the application.
OL Admin Configuration

1. Open OL Admin and go to Configuration > Advanced. In the right pane, set Voice recognition mode to Nuance 8.5.
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.
Automatic Speech Recognition (ASR)

ASR Configurator

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

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

Since the FA rate for **Very-High** is the lowest, it may seem logical to always choose this option. However, while the number of FAs decreases, the number of **FRs (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**:

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

**Caution**: The Voice Verification feature will shortly be discontinued.
In This Chapter:

28 Introduction
28 Visual Guide
29 Requirements
30 Server Configuration
30 Company
30 Feature Group
31 User Guide
31 ECC Command List
31 Initiating a Handoff to Predefined Numbers
32 Initiating a Handoff to Custom Numbers
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 Officelinx server as long as the call itself was connected through the Officelinx 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 Officelinx 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 Officelinx 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.
## Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>---</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 9.0 or higher</td>
</tr>
</tbody>
</table>
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

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

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

Feature Group

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

- **Internal Extension** will enable the ECC for user’s dedicated internal device only.
- **External or External/Internal (FindMe) Extension** will enable the ECC for both internal and external device as long as the call is made to the user through auto attendant.

**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.

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

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.
In This Chapter:

34 Introduction
34 Visual Guide
34 Requirements
35 Server Configuration
35 Company Properties
35 Feature Group Properties
36 Mailbox Properties
36 Customize TUI Configuration
37 User Guide
37 Basic TUI Navigation
37 Temporarily Disable Speech Command
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. Officelinx 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.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>---</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 9.0 or higher</td>
</tr>
</tbody>
</table>
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 **OL Admin > Company**, and on the **Speech Options** tab, ensure that **Voice Recognition** is enabled for the company.

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

Feature Group Properties

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

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

From OL 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.

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.
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:

40 Introduction
40 Visual Guide
40 Requirements
41 Server Configuration
41 Procedure
43 User Guide
43 Enabling Speech Contacts
Introduction

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

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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>ASR</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.1 or higher</td>
</tr>
</tbody>
</table>
Server Configuration

For the following steps, launch the OL Admin program.

Procedure

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

2. From the Contact Priority dropdown list, select which of your contacts (Public, Private or None) are more important when doing speech recognition of contacts.
   
   For example, if in a mailbox you choose to 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.
5. Move onto the Advanced tab. Ensure that Messaging & Collab is selected under Desktop Capabilities.

6. Save the Mailbox settings.
User Guide

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

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

Enabling Speech Contacts

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

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

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

2. Select the Enable Speech radio button.

   If you wish to enable 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.

   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.
GOOGLE INTEGRATION

In This Chapter:

46  Introduction
47  Implementation Example
47  Requirements
48  Server Configuration
48  Synchronization for a Single User
51  Install and configure OAuth2.0
63  Contact & Calendar Synchronization
65  Synchronizing Contacts and/or Calendar Only
69  Google Desktop, Google Talk & Web Gadgets
71  Disable IMAP
72  User Guide
72  iLink Pro On Google Web Gadgets
76  Message Synchronization
76  Contact & Calendar Synchronization
78  Manual Contact Importing
Introduction

Avaya iLink Pro transforms the Chrome browser, Chromebook, and Internet Explorer into a real-time communications hub. With iLink Pro 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 Google Apps, Salesforce.com and others. With iLink Pro you're never more than a click away from finding people, to see their availability and to communicate with them anytime, anywhere.

With iLink Pro you can:

- Check people's availability.
- Chat one-to-one with a contact or involve an entire group using Google Hangouts.
- Click-to-call any phone number found in a browser window.
- Share your location with others, and find out where they are at.
- Access your corporate and personal contacts.

iLink Pro also offers:

- **Message Integration**: iLink Pro 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.

- **Contact & Calendar Integration**: iLink Pro can synchronize contact entries and calendar events with Google Apps or Gmail. Any entry that the user creates within Google will be automatically updated on Web Access and vice versa, reducing repetition.

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

- **Multi-browser support**: Add iLink Pro as an extension to the Google Chrome web browser, or as an Add-in to Microsoft Internet Explorer. Access all of your UC needs from within your favorite browser.

- **Integrated collaboration tools**: iLink Pro unites your everyday communications with industry leading collaboration applications such as Cisco's WebEx and Google Hangouts. Transform an Internet chat session into a web based video conference with the capacity to bring many others participants into the discussion. Take a telephone call with a single contact and turn it into a conference call with many.

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.

iLink Pro can also forward incoming messages (voice, email, fax) to a Google Docs collection making all of your communications available from anywhere in the world through the Internet.

**Note**: iLink Pro requires your organization to be running the Avaya Officelinx Unified Communications server. Integration with 3rd party applications, such as WebEx, may require additional licensing from those providers.
Implementation Example

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

End user applications become accessible through plug-ins.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>---</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 9.1+</td>
</tr>
</tbody>
</table>
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 to communicate properly with the worldwide web, users will be able to configure all their gadgets and plug-ins on their own through the **User Guide on page 72**.

Client authentication and synchronization is handled by one of the following:

- **Synchronization for a Single User**
- **Install and configure OAuth2.0 and the Google API**

The chosen method will depend upon site specific preferences.

Synchronization for a Single User

In order to achieve IMAP synchronization between Google Apps and Officelinx, set the Google Apps mail mode to IMAP. All other configuration takes place in OL Admin where individual mailboxes hold the credentials for the corresponding Google Apps email account.

TSE IMAP Configuration

Before you can synchronize your mailboxes with a Gmail account you must first configure your OL Admin so that it can access the Gmail IMAP server.

1. Locate and run **OL Admin** console.

2. From the left hand menu locate the **TSE IMAP Server**.

3. Right click on the **TSE IMAP Server** and the following menu appears. Select **New > TSE IMAP Server**.

4. The **TSE IMAP Server** creation window opens. Fill out the boxes as follows:
   - **IMAP Server Name**: Gmail (or Google Apps name for your company)
   - **IMAP Server Address**: imap.gmail.com
   - **IMAP Server Port**: 993

   Click **OK**.

5. Restart the **TSE Cache Manager** service from the Services panel.

The Officelinx UC platform is now ready to synchronize system mailboxes with Google Gmail accounts.
Mailbox

In order for your mailboxes to be synchronized with a Google Apps account, you must individually setup each of the mailboxes accordingly. Ensure that the Google Apps/Gmail account that Officelinx will be synchronizing with is configured for IMAP connection.

1. Locate and run OL Admin console.

2. Locate the mailbox you wish to sync with a Google Apps account.

3. Double click on the mailbox to load the following configuration window. Select the Synchronization Options tab.

4. Fill out all the information as follows:
   - **User Name**: Type in the email address of the Gmail account that you have created for this mailbox.
   - **User Password**: Type in the password for the Gmail account.
   - **Confirm Password**: Type in the password for the Gmail account again to verify.
   - **IMAP Server**: From the dropdown menu select Gmail.
   - **IMAP Language**: From the dropdown menu select the language you will be using.
   - **Storage Mode**: From the dropdown menu select IMAP.

   **Note**: For details on contact and calendar sync, refer to Contact & Calendar Synchronization on page 63.

5. Close the configuration window and save your settings. Your messages to this mailbox will now be directly synchronized with the Gmail account that was configured.

Proceed to the next section to modify the Feature Group.
Feature Group

In order to ensure that there are no conflicts between Officelinx and Gmail, please follow these steps to configure the Feature Group to synchronize the required information.

1. Locate and run OL Admin console.
2. From the left hand menu locate the Feature Group. Find the Feature Group that the mailboxes with Gmail synchronization are located in. Double click on the feature group to load the configuration window.

3. From the Feature Group configuration window, open the Synchronization Options tab.
4. Under Synchronization Settings, enable all of the checkboxes that apply. These are the data types that will be synchronized between Officelinx and Gmail.
5. Save and close the window after the changes are complete.

**Note:** For details on contact and calendar sync, refer to Contact & Calendar Synchronization on page 63.

6. Your Officelinx mailbox is now fully synchronized with the Gmail IMAP account.

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

2. Click the Google menu. Select IAM & admin > Manage resources.
3. Click Create project.
4. Give the new project a name, then click Create.
5. Return to the **IAM & admin** page, then select **Service accounts**. Click **Create service account**.

6. Give the connection a name. Expand the **Role** menu, then select **Project > Owner**. Click **Furnish a new private key**, then enable **P12**. When ready click **Create**.
7. The project file will be created with a .p12 extension. Make note of where the file is saved. Copy the file to both the C:\UC\UCCE and C:\UC\IMAPTE folders. (Change the path accordingly if your program is installed on a different drive.)

8. Record the Private key password (notasecret) and click Close.

9. Select the account you just created, click the menu icon and choose Edit.
10. Turn on **Enable G Suite Domain-wide Delegation**.
   Click **Configure Consent Screen**.

11. Enter a product name and click **Save**.

12. Click **Save** to complete the delegation.
13. Click View Client ID.

14. Record the Client ID and the Service account email address for the project. Click Save.

15. Rename both copies of the P12 file from step 7 to match the email address recorded in step 14. Include the domain and the .com extension.

Caution: Do Not change the extension of the file. Always ensure it retains the P12 extension.
16. In the left-hand pane, click **Library > G Suite**.

17. Click **Admin SDK**, then select **Enable**.

18. Once it has been activated, click the arrow to return to G Suite page. Repeat to enable all of the following APIs:
   - **Google Calendar API**
   - **Google Drive API**
   - **Gmail API**

19. From the Library, click **Social** and enable the **Contacts API**.

**Hint:** While these settings will work for most sites, not all sites will want to open all of these channels if it is not required. See **Minimum Required Scopes and APIs by Product** for details.
Domain Setup

1. Login to Google Apps as an administrator.
2. Click Settings ⚙️ and choose Manage this domain.
3. If prompted, provide the necessary administrator account and password details to login.
4. At the Admin Console, choose Security and click API Reference.
5. In the section for API access, place a check in the **Enable API access** box. Click **Save Changes**.

6. Return to the Security page and click **Advanced settings**.

7. Click **Manage API client access**.
8. Enter the Client ID value from step 14 into the **Client Name** field. In the space for **One or More API Scopes**, enter the following string:

```
```

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

**Hint:** While these settings will work for most sites, not all sites will want to open all of these channels if it is not required. See **Minimum Required Scopes and APIs by Product** for details.

**Note:** When configuring for Zang Connect for Cisco TelePresence (TMS), an additional scope must be defined (**Calendar Resources (Read/Write)**). To the above list, add the following:

```
https://apps-apis.google.com/a/feeds/calendar/resource/
```

9. When ready, click the **Authorize** button.
10. Verify that the selected scopes were successfully installed.

---

**OAuth2 and Officelinx 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\IMAPSE** 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.

<table>
<thead>
<tr>
<th>SCOPES * (see below)</th>
<th>AVAYA CLOUD APPLICATION LINK</th>
<th>AVAYA AURA COMMUNICATOR FOR WEB</th>
<th>AVAYA COMMUNICATOR FOR WEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth/admin</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>auth/calendar</td>
<td></td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>auth/drive</td>
<td></td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>auth/drive.file</td>
<td></td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>calendar.feeds</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>calendar/resource</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m8/feeds</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>mail.google.com</td>
<td>•</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APIs</th>
<th>AVAYA CLOUD APPLICATION LINK</th>
<th>AVAYA AURA COMMUNICATOR FOR WEB</th>
<th>AVAYA COMMUNICATOR FOR WEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin SDK</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Contacts API</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Google Calendar API</td>
<td></td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Google Drive API</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>GMail API</td>
<td>•</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 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.googleapis.com/m8/feeds/
- **mail.google.com** - https://mail.google.com/
Configuring Officelinx

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

1. Open OL Admin.

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

3. Open the Synchronization Options tab. Enter values in the following fields:
   - **IMAP Account**: Enter your company domain, followed by a forward slash then the Service account value from step 14. For example, yourdomain/avaya-secure-connection@avayacloud...
   - **Password** and **Confirm Password**: Type in the Private Key password for the client ID received in step 7.

4. Click **Save** to preserve the changes.
5. In OL Admin, open Mailbox Structure and double-click a client to modify.

6. Open the Synchronization Options tab.

7. 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  

8. Click Save to preserve the changes.
9. Repeat steps 5 through 8 for each client that requires OAuth 2.0 synchronization.
10. On the Voice Server, open the UC/UCCSE folder.
11. Edit the `$CSE.exe.config` file using any text editor (e.g. Notepad).

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

   ![CSE.exe.config Notepad](image)

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

12. Stop and Start the **UC Content Synchronization Engine** service on the Voice Server, or restart the server.

   **Caution:** If this is an High Availability system, restart this service **only on the Consolidated Server.**

   The setup is complete.

### Contact & Calendar Synchronization

Once you have configured the IMAP TSE server with your mail server, you will be able to assign the degree of synchronization from the Feature Group. While the server side configuration is simple, you must ensure that you verify that all of the information is correct so that your users do not lose any calendar, contact or message data during synchronization.

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

### OL Admin

From OL Admin, configure the IMAP TSE server so that Officelinx can successfully communicate with the Gmail server.

Enter the following information:

**IMAP Server Name:** Enter the name of your mail server. This name is for reference only and will not have an impact on functionality.

**IMAP Server Address:** Enter `imap.gmail.com`. This is same for Gmail and Google Apps applications.

**IMAP Server Port:** Enter the port that your mail server uses during communication. For the Gmail server, this value is usually **993.**

**IMAP Server Voice Format:** Select the voice file format to be used to synchronize voice messages with the Google server.

**IMAP Server Domain:** This field is not required for most Google Apps integration scenarios. This field is mainly used to define the domain name of the mail server to verify the **Reply to** address of each mailbox. This prevents message loops during synchronization.
Feature Group

Feature Group configuration must be done in two places: the **Synchronization Options** tab, and the **Mailbox Options** tab. You will be able to define exactly what data will be synchronized from these two sections.

From the **Synchronization Options** tab you can specify which messages are going to be synchronized between the servers. You may also define how the calendar and contacts are will be managed through the same connection.

1. From **Calendar Mode** dropdown menu, select **Sync with Mail Server** if you wish to enable calendar synchronization between the servers.
2. Enable the **Contacts** checkbox to synchronize the contacts between the two servers.

The other fields, such as Inbox Folder, are used for message synchronization. Refer to **Server Configuration on page 48** for details regarding this matter.

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

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

By customizing these settings you can easily segregate calendar and contact synchronization from message synchronization when enabling features for the users. This provides control over who has access to each feature.
Synchronizing Contacts and/or Calendar Only

It is also possible to synchronize contacts and/or the calendar without synchronizing messages. Follow the configuration settings for a full synchronization, but disable message folders from the Feature Group.

TSE IMAP Configuration

Before you can synchronize your mailboxes with a Gmail account you must first configure OL Admin so that it can access the Gmail IMAP server.

1. Locate and run OL Admin console.

2. From the left hand menu locate the TSE IMAP Server.

3. Right click on the TSE IMAP Server and the following menu appears. Select New > TSE IMAP Server.

4. The TSE IMAP Server creation window opens. Fill out the boxes as follows:
   - **IMAP Sever Name**: Gmail (or Google Apps name for your company)
   - **IMAP Server Address**: imap.gmail.com
   - **IMAP Server Port**: 993

   Click OK.

5. Restart the TSE Cache Manager service from the Services panel.

The Officelinx UC platform is now ready to synchronize system mailboxes with Google Gmail accounts.
Mailbox

In order for your mailboxes to be synchronized with a Google Apps IMAP account you must individually setup each of the mailboxes accordingly. You must also ensure that the Google Apps/Gmail account that Officelinx will be synchronizing with is configured for IMAP connection.

1. Locate and run OL Admin console.

2. Locate the mailbox you wish to sync with a Google Apps IMAP account.

3. Double click on the mailbox to load the following configuration window. Select the Synchronization Options tab.

4. Fill out all the information as follows:
   - **User Name**: Type in the email address of the Gmail account that you have created for this mailbox.
   - **User Password**: Type in the password for the Gmail account.
   - **Confirm Password**: Type in the password for the Gmail account again to verify.
   - **IMAP Server**: From the dropdown menu select Gmail.
   - **IMAP Language**: From the dropdown menu select the language you will be using.
   - **Storage Mode**: From the dropdown menu select IMAP.

5. Close the configuration window and save your settings. Your messages to this mailbox will now be directly synchronized with the Gmail account that was configured.

Proceed to the next section to modify the Feature Group.
Feature Group

In order to ensure that there are no conflicts between Officelinx and Gmail, please follow these steps to configure the Feature Group to synchronize the required information.

1. Locate and run OL Admin console.
2. From the left hand menu locate the Feature Group. Find the Feature Group that the mailboxes with Gmail synchronization are located in. Double click on the feature group to load the Feature Group configuration window.

3. From the Feature Group configuration window, open the Synchronization Options tab.
4. Under Synchronization Settings, enable all of the checkboxes that apply. These are the data types that will be synchronized between Officelinx and Gmail.

5. From Calendar Mode dropdown menu, select Sync with Mail Server if you wish to enable calendar synchronization between the two servers.
6. Enable the Contacts checkbox at the bottom to synchronize the contact entries between the two servers.
7. From the **Mailbox Options** tab, enable **Change Location** to allow an event on your mail server’s calendar to automatically change the UC location of the user. This setting is meant to work with the calendar synchronization feature. Save and close the window after the settings are complete.

8. Your Officelinx mailbox will now synchronize contacts and/or calendar information with the Gmail IMAP account.

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

**Note:** Recurring events will only be synchronized within 1 week of the current date.
Google Desktop, Google Talk & Web Gadgets

Since Google Desktop and Google Talk integration occurs on the desktop, there is no need to configure the voice server. However, if you are pushing the iLink Pro software to users in a managed network, you should ensure that all the gadgets are properly installed and updated. Also keep in mind that Google Desktop and Google Talk integration requires the correct Internet access privileges to function properly. If your UC server is connected to the Internet through a managed ISA server, you must ensure that there are custom policies configured to enable it to function.

Note: If you are deploying the Google Gadget file from Windows 2008 or Windows 7, you must have the .GG MIME type registered on the IIS server. Refer to Adding a MIME Type for .GG Files on page 70.

The following installations are required at the client desktop for full integration:

- iLink Pro 2.5 or higher
- Google Desktop
- Google Talk

ISA Settings for Google Web Gadget Integration

If your UC server is managed by the ISA server, you must ensure that the policy that affects its web connection is configured properly.
1. From the ISA control panel open the configuration for the policy in question.
2. Ensure that the following settings are disabled:
   - Verify normalization
   - Block high bit characters
3. Click OK to save the policy.
Adding a MIME Type for .GG Files

In Windows 2008 and Windows 7, a MIME type has to be defined in order for end users to successfully download the Google Gadget file from the OL server. If the MIME type isn't defined, users will see a following error when trying to download the gadget.

1. To add a MIME type, open your IIS Manager then open the MIME Type options from the upper most folder.
2. From the **Actions** pane, click on **Add...**

3. For **File name extension**, enter `.gg`. For **MIME type**, enter `application/octet-stream`.

   Click **OK** to save your settings.

The MIME type will now be added to your IIS server. Since you have added this entry to the upper most folder, the settings will be pushed down to all Officelinx related folders.

---

**Disable IMAP**

Where necessary, site administrators can disable IMAP for clients while leaving the domain settings unaffected. To disable IMAP for users, run the following script at the GAM (Google Apps Manager) command prompt:

```
Gam user <username> | group <groupname> | ou <ouname> | all users imap on|off
```

For example, this script will turn IMAP off for all users in the current domain:

```
Gam all users imap off
```
User Guide

This user guide is divided into two sections. The first covers installing and using the various versions of iLink Pro. The other is configuring your message, contact, and calendar synchronization between Officelinx (which can be directly accessed through Web Access) and Google Apps. While the installation and configuration related to these features are straightforward, please backup important data before configuring any synchronization.

iLink Pro On Google Web Gadgets

iLink Pro can be accessed as an extension to the Chrome and IE browsers, and as a Gadget web page on the UC server.

Note: To save your settings, your web browser must accept 3rd party cookies. Some browsers reject 3rd party cookies either as a default setting, or due to company policy.

Hint: For complete details on using the application, refer to the chapter on iLink Pro (page 67 ff) in the Client Application Guide.

Web Gadget From UC Server

Even without a Google Apps account, you can still take advantage of iLink Pro. To access the Web Gadget directly from your UC server, enter the following into the address bar of a web browser.

http://USER.YOUR.SERVER.COM/ucwebaccess/

Replace USER.YOUR.SERVER.COM with the address of your own UC server. When you visit the page, you will see the page shown here. The functionality of the web based iLink Pro is identical to the Google Web Gadget variations.

Note: To save your settings, your web browser must accept 3rd party cookies. Some browsers reject 3rd party cookies either as a default setting, or due to company policy.
Using UC Web Gadgets

Hint: For a complete description of all of the features of the gadget, consult the Client Applications Guide, chapter 5, iLink Pro, starting on page 67.

Logging In

When you first access the gadget, you will have to configure your credentials in order to log in.

1. Choose the login method to use:
   - **Google Account**: Login to the client using your Google credentials.
   - **UC Account**: Login using the UC Client credentials.

2. Enter all necessary login information. Google credentials require no additional input.
   - **Company**: Enter the company number that your mailbox is associated with.
   - **Mailbox**: Enter your mailbox number.
   - **Password**: Enter the password for your mailbox.

3. Click **Save** and the program will automatically log in.

Messages

When you log into web gadget, go to the **Messages** tab to receive a quick summary of messages available in your UC mailbox. The icons represent unread voicemail 📞, email 💌 (text) and Fax 📄 messages. Clicking an icon will send you to Web Access where you will be able to access the messages.
Locations, Availability and Extensions

Location and availability can be modified using the gadget. To change a setting, click on the My Location icon and select a new location and availability setting. Once an item has been chosen, the location icon will change to match your selection.

- Use this icon to set your location to In Office.
- The At home icon will change your location accordingly.
- Select this item to change your location to in a Meeting.
- Click Follow Calendar to clear all manual settings and return to following your locations calendar. The calendar is setup and maintained through Web Access. This icon will be absent if you are currently following the calendar.
- Change your Availability status. This item toggles between set to available and unavailable.
- Choose this icon to access the full range of Locations and options available, including custom locations. A check is placed beside the current selections. The green/red bar to the left of the icon shows your default availability for that location. This screen also provides access to change Availability and the Follow calendar option. The numbers where you can be reached is also shown.

The locations, default availability, and the numbers where you can be reached at each location are automatically adjusted based upon the settings for each item established through Web Access.

Work Groups & Directory Search

Users can access their personal contacts, work groups and the company directory through the People page of the Gadget.

The green/red/yellow bar to the left of the contact's picture indicates that person's Availability (available, unavailable, on the phone). Their location is shown in the text below their name. All status indicators are updated in real-time.

Workgroups are collections of related contacts. These are created by the user as required. Use this option to create, rename and delete workgroups, or to modify the contacts included within them. From here, you can send an instant message (Chat) to all members of the group.
Choosing this option from the People utility menu will open a list of all current groups. Click on a group to open the list of options.

The number of members in the group is shown at the top of the list.

- **Chat** - Broadcast an instant message to all members of the current group.
- **Timeline** - Show the tracked timeline events for all members of the current group.
- **Show on a map** - Display the locations of all group members using Google Maps.
- **Rename** - Change the name of the group.
- **Delete** - Remove the group from the list. Contacts in the group are not deleted and continue to appear in the directory.

**Directory Search**

To search your personal contacts list or the company directory, type the mailbox number, extension, or the contact’s first or last name into the **Search or dial** field. The search function also supports `lastname,firstname` or `initial` (i.e. “smith,j” or “smith,john”). All matching contacts will be displayed.

Click the **X** to close the search window.

**Dialing & Call Control**

The Calls window shows the status of active telephone calls. The progress of the call is displayed beneath the number.

Click on the progress window to open the Call Control menu.

- **Hangup** icon will terminate the call.
- **Put on hold** will pause the call, muting the microphone and allowing another call to be placed.
- **Transfer** is selected, the call is put on hold and you will be prompted to enter the extension or telephone number to send the call to.
- **Remove** will close the Call Control window without affecting the call.

After the call has finished, Call Control provides the following options.

- **Callback** to initiate a new telephone call to this number.
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. If your organization opts for individual synchronization, do the following.

Log into your Web Access, click the Client icon and scroll down to Synchronization Options. Enter the following:

**User Name:** Your full Google Apps email address (e.g. user@gmail.com)
**Password:** Your password for the above email address.
**Confirm Password:** Confirmation of the above password.

Click the Save button. Messages in the main inbox will be synchronized between Google Apps and the UC server.

**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 Officelinx mailbox as well. The following are typical behaviors that the synchronization will follow so that you can understand exactly how your calendar and contact entries are being handled by the servers.

**Note:** When creating a calendar event from Google, you must ensure that the reminder time 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 Officelinx 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 Officelinx, such as a weekly meeting, will only be synchronized with the Google calendar 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 Officelinx contacts.

![Contact Sync Example]

The contact information is automatically sent to the Officelinx contact list.

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

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

Manual Contact Importing

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

1. To export your contacts from Google Apps, log into your Google email account and open your Contacts list.
2. Click on More, then Export...
   This opens the Export contacts window.
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.
6. With the CSV file ready, open Web Access and click Contacts.
   Click the Import button.
7. Click **Choose File** and select the CSV file exported from Google.
8. Click **Next** to proceed after the file has been selected.

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

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

82 Introduction
82 Configuration Process
83 Configuration with IIS 7
84 Configuration with IIS 6
85 Officelix Configuration
87 Weblinks Example
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 83.

If the server has IIS 6 installed, begin the process on page 84.

Regardless of which version of IIS is present, the Officelinx setup remains the same. Once the appropriate version of IIS has been configured, continue with the Officelinx setup on page 85.
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 84.

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**.

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

   **Important:** Continue with the section **Officelinx Configuration on page 85**.
Configuration with IIS 6

**Warning:** Use these instructions if you have IIS 6 on your system. If you have IIS7, then use the section Configuration with IIS 7 on page 83.

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

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

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

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

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

**Important:** Continue with the section **Officelinx Configuration** on page 85.
Officelinx Configuration

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

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

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

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

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

   From OL 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.

   Warning: Please keep in mind that this step is only for users who will be using email forwarding instead of IMAP TSE Synchronization. If you configure forwarding for users who are using IMAP TSE 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 Officelinx folder (by default, this is \UC). From Windows, go to Start > Run and enter the full path and file name in the space provided. Add the /i parameter, and the URL of the server where the files will be kept. For example:

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

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

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

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

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

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.
7

EMAIL ACTION SCHEMA

In This Chapter:

90
Introduction

90
Enable Action Schema

92
Email Buttons
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 OL Admin program.

1. Start OL Admin and open the **Mailbox** folder.

2. Double-click one of the listed mailboxes, and open the **Message Options** tab.
3. Click **Add** to create a new **Address**, or select an existing address and choose **Edit**.

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

   ![Action Schema Configuration](image)

   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** section, page 120, 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.

**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.
Play

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

Stream

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

Phone

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

Google+ Hangout

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

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

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

Twitter

The Tweet button allows the user to share the audio file with their Twitter followers.
**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 Messages** opens a list of voice messages left in the mailbox. Details include the name of the contact who left the message, their number or extension, and the date and time the message was received.

Click on an item to playback the message.
Contact Location

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

**Mail**: Opens an email client program to compose and send an email message to the contact.

**Call**: Places a telephone call to the contact. Your desktop telephone will ring, and you will be connected with the contact once they answer.
MUTARE TRANSCRIPTION SERVICE

In This Chapter:

- Introduction (98)
- Visual Guide (98)
- Requirements (99)
- Licensing (100)
- Upgrading the License (100)
- Officelinx Server Configuration (102)
- Transcription Configuration Tool (102)
- Verification (103)
- User Guide (103)
Introduction

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 Officelinx 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 OL Admin on the Advanced tab for each mailbox.

---

**Visual Guide**

![Visual Guide Diagram]

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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Mutare Subscription available from Avaya</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 10.6 or higher</td>
</tr>
<tr>
<td>Hardware</td>
<td>A computer that meets Mutare server requirements.</td>
</tr>
</tbody>
</table>

- 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 Officelinx license but is available as an option from Avaya. These instructions are only required if a Mutare transcription license is purchased after Officelinx 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 **Officelinx Server Configuration**.

---

**Upgrading the License**

If Officelinx 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 **Officelinx Server Configuration**.

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

---

**License Upgrade Utility**

- **Product**: IsDN32/56
- **License**: SoftLicense
- **License ID**: 30180597
- **License Date**: 2017/08/05 14:44
- **Services**
  - **DHCP**
  - **PCN**
  - **SIP**
  - **NAT**
  - **UPC**
  - **MobiVoIP**
  - **Messaging**
  - **CTI User**
  - **Voice**
  - **343**
  - **SS7/GSM**
  - **TAPI**
  - **Integration**
  - **PDF**
  - **Reflection**
  - **Call Center**
- **ASR**
  - **ASR Provider**
  - **ASR Speech**
- **None**

---

**License Configuration**

- **Transcription Provider**: None
- **Transcription Type**: None
- **Transcription Entry**: None
- **Transcription User**: None

**Activation Date**: 2017/05/16 14:44

---

**UCLicenseUpgrade**

**License ID**: 30180597
**License Date**: 2017/08/05 14:44
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 Officelinx license.
   **Site ID**: Enter the site ID for your location.

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

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

   Click **Set as Active License**. Click **OK**.

Your Mutare transcription license is activated.
Officelinx Server Configuration

Officelinx 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 Officelinx server, go to **Start > All Programs > Officelinx > UCTranscriptionConfig**.
2. Enter all required information.

![Transcription Configuration Tool](image)

**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 (Cloud-based) or internally (On-premise) accessible URL of your Officelinx Voicemail server to which 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 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 Officelinx 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:** The maximum message length that can be transcribed is 60 seconds. The portion of the message beyond 60 seconds will not be transcribed. The voice recording of the message will not be affected.
EXCHANGE 2016/2013
INTEGRATION: USING EWS

In This Chapter:

106 Introduction
106 Visual Guide
106 Requirements
107 Server Configuration
107 Exchange Superuser Creation/Configuration
109 OL Admin Configuration
113 Contact and Calendar Sync
116 User Guide
116 Calendar Synchronization
116 Contact Synchronization
117 MS Exchange Performance Considerations
Introduction

Officelinx and an Exchange server are able to integrate through the IMAP/SE 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 Officelinx 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 2016 is recommended since the use of IMAP no longer supports contact and calendar synchronization. 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 Officelinx 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.

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

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

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>IMAP/SE License</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 10.5 or higher</td>
</tr>
</tbody>
</table>
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 Exchange Web Services (EWS) enabled in order for Officelinx to communicate properly.

Caution: Exchange 2016 does not support IMAP connections. Only Exchange Web Services can be used. For Exchange 2013, EWS is optional and replaces 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. Open a web browser and go to the Exchange Admin Center.

   Under recipients > mailboxes, click the + symbol to add a new user.

2. At the new user mailbox page, on the general tab, fill in the account details in the spaces provided.

   Remember the Alias for the account (Superuser in this example) as that will be used later in the setup.

3. At the Microsoft Exchange Management Shell, 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:

   - New-ManagementRoleAssignment -User Superuser -Role ApplicationImpersonation -Name OLName
4. To verify that the Super User has the **ApplicationImpersonation** management role, run the following command.

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

Verify that one of the accounts has Super User enabled.
OL Admin Configuration

For Officelinx and Exchange to be able to synchronize data, Officelinx 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 TSE Endpoint for EWS

In order for the Officelinx server to recognize the Exchange server, you must configure a TSE Endpoint entry in the OL Admin > TSE IMAP Server section to use the EWS server. A entry should already be present in OL Admin based upon the choice of email client you made during installation.

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

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

**IMAP Server Address**: Enter the IP address of the EWS server. The address MUST be prefixed with ews: (all lower case, with a colon).

**IMAP Server Port**: Set this to the port number of the EWS server. The default is 443.

**Voice Format**: Select the voice format used when sending voice messages to external voice servers.
Feature Group Configuration

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

**IMAP Account**: Enter the account name for the EWS superuser. The format will be `superuser_name@domain.com`.

**Account Password**: Enter the password of the superuser account.

**Confirm Password**: Re-enter the password.

**IMAP Server**: Select the TSE Endpoint created in the previous steps.

**Calendar Mode**: If calendar synchronization is required, select *Sync with Mail Server Calendar* from the dropdown list.

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 `IMAP`.

**Note**: The user must be a Messaging & Collab or Messaging user to utilize synchronization.

Assign the mailbox to the Feature Group that is going to have the superuser account credentials.

Save all changes and move onto Feature Group Configuration.
Certificate Configuration

In order to ensure that the communication between Officelinx and the Exchange server is not interrupted by security measures, install the certificate from the Exchange server computer on the Officelinx 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 Officelinx server computer, which can be accomplished manually by the system administrator.

1. Open the [Internet Explorer](https://exchange_2016/owa) web browser, then navigate to the OWA page (e.g. [https://exchange_2016/owa](https://exchange_2016/owa)).

   You will see the following security warning popup.

   Click on **View Certificate**.

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.

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

![Certificate Import Wizard](image)

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

![Certificate Import Wizard](image)

6. The following popup confirms the import was successful. Click **OK**.

![Certificate Import Wizard](image)

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](image)

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.

   ![Security Warning](image)

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

![Windows Configuration Image]

2. 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 Image]
3. 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-CE IM Integration Engine Properties](image)

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

4. Restart the service.
Officelinx 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 Mail Server from the Calendar Mode dropdown menu.

The other fields, such as Inbox Folder, are used for message synchronization between the servers. Refer to the message integration section for details.

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

By customizing these settings you can easily segregate calendar and contact synchronization along with message synchronization when enabling features for your users, allowing you to control exactly who has access to certain features.
Once calendar and contact synchronization has been enabled, all transactions occur on the server in the background, so you do not have to configure anything on your own. Use your mail server as you normally would, and any calendar or contact entries will now be mirrored in your Officelinx 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 Officelinx 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 Officelinx mailbox.

The time and date of the meeting is automatically sent to the Officelinx 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.

### Contact Synchronization

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

Contact information is automatically sent to the Officelinx mailbox.

**Caution:** Deleting contacts is also synchronized. If you delete an entry from Outlook, it will also be deleted from Officelinx, and vice versa.
Synchronization Limits

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

Messages moved to the deleted items folder in Officelinx will also be moved in Gmail. If a message is deleted in Gmail, it will be unreadable in Officelinx.

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

Microsoft ([http://support.microsoft.com/kb/905803](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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages</td>
<td>&lt;20000</td>
<td>&lt;100000</td>
<td>&lt;100000</td>
</tr>
<tr>
<td>Contact and Calendar Entries</td>
<td>&lt;5000</td>
<td>&lt;10000</td>
<td>&lt;10000</td>
</tr>
</tbody>
</table>
## In This Chapter:

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>120</td>
<td>Introduction</td>
</tr>
<tr>
<td>120</td>
<td>Visual Guide</td>
</tr>
<tr>
<td>120</td>
<td>Requirements</td>
</tr>
<tr>
<td>121</td>
<td>Server Configuration</td>
</tr>
<tr>
<td>121</td>
<td>Exchange 2013 superuser Creation/Configuration</td>
</tr>
<tr>
<td>126</td>
<td>OL Admin Configuration</td>
</tr>
<tr>
<td>132</td>
<td>Contact and Calendar Sync</td>
</tr>
<tr>
<td>135</td>
<td>User Guide</td>
</tr>
<tr>
<td>135</td>
<td>Calendar Synchronization</td>
</tr>
<tr>
<td>135</td>
<td>Contact Synchronization</td>
</tr>
<tr>
<td>136</td>
<td>MS Exchange Performance Considerations</td>
</tr>
</tbody>
</table>
Introduction

Officelinx and an Exchange server are able to integrate through the IMAPTSE 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 Officelinx 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. Please refer to the Exchange 2016/2013 Integration: Using EWS chapter for details on EWS configuration.

Visual Guide

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

Administrators can also customize what 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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>IMAPTSE License</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 9.0 or higher</td>
</tr>
</tbody>
</table>
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 Officelinx 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 2013 environment.

1. Open a web browser and go to the Exchange 2013 Admin Center.

Under recipients > mailboxes, click the + symbol to add a new user.

2. At the new user mailbox page, on the general tab, fill in the account details in the spaces provided.

Remember the Alias for the account (Superuser in this example) as that will be used later in the setup.
3. On the **mailbox features** tab, ensure that **IMAP** and **MAPI** are both **Enabled**.

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

   ``` powershell
   Get-Mailbox | Add-MailboxPermission -User Superuser -AccessRights FullAccess -InheritanceType All
   ```

5. 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.
6. From the **Exchange 2013 Admin Center**, go to **Servers** and open **Exchange 2013**.

![Exchange 2013 Admin Center](image)

7. Choose **IMAP 4**. Click **More Options**, and scroll down to find **Maximum connections from a single user**. Set this value to **2000**.

![Exchange Server - Windows Internet Explorer](image)
8. 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.

![Windows Server Manager MMC](image1)

9. 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 console](image2)

10. Stop the **UC CSE PIM Synchronization Engine** service.
11. 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-CE PBX Synchronization Engine Properties](image)

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

12. Restart the service.
OL Admin Configuration

For Officelinx and Exchange to be able to synchronize data, Officelinx 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 TSE Endpoint

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

**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 143.

**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 TSE 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 IMAP TSE 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).

**Note**: The user must be a **Messaging & Collab** or **Messaging** user to utilize synchronization.

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

The Feature Group plays a key role in IMAPTE 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 TSE Endpoint created in the previous steps.

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 > Officelinx. Double-click on the Superuser account to open the IMAP Settings window.

2. Click **Verify** to run the test.
3. If successful, the result will include the entry for **OK LOGIN completed**.

Registry Settings

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

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

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

The new registry entry will appear in the Registry.

Proceed with Certificate Configuration.
Certificate Configuration

In order to ensure that the communication between Officelinx and the Exchange server is not interrupted by security measures, install the certificate from the Exchange server computer on the Officelinx 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 Officelinx 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_2013/owa).
   
   You will see the following security warning popup.
   
   Click on View Certificate.

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.

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

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

6. The following popup confirms the import was successful. Click **OK**.

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.

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.

   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 TSE 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 Officelinx installation, you must do so manually now by running the `ExchangeMapiCdo.msi` file from `MSExchange` folder on Officelinx 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. Ensure that the Superuser account created has the proper permissions on the Windows environment.

2. 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**.
Officelinx 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.

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.

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 Officelinx 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 Officelinx 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 Officelinx mailbox.

The time and date of the meeting is automatically sent to the Officelinx 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.

**Contact Synchronization**

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

Contact information is automatically sent to the Officelinx mailbox.

---

**Caution:** Deleting contacts is also synchronized. If you delete an entry from Outlook, it will also be deleted from Officelinx, and vice versa.
MS Exchange Performance Considerations

Microsoft ([http://support.microsoft.com/kb/905803](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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages</td>
<td>&lt;5000 combined</td>
<td>&lt;20000</td>
<td>&lt;100000</td>
</tr>
<tr>
<td>Contact and Calendar Entries</td>
<td>&lt;5000</td>
<td>&lt;5000</td>
<td>&lt;10000</td>
</tr>
</tbody>
</table>
11 EXCHANGE 2010 INTEGRATION

In This Chapter:

138 Introduction
138 Visual Guide
138 Requirements
139 Server Configuration
139 Creating a superuser from Active Directory
141 Exchange 2010 superuser Creation/Configuration
145 Exchange 2010 Shell Configuration
148 OL Admin Configuration
153 Contact and Calendar Sync
155 User Guide
155 Calendar Synchronization
155 Contact Synchronization
156 MS Exchange Performance Considerations
Introduction

Officelinx and an Exchange server are able to integrate through the IMAP/TSE 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 Officelinx 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

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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>IMAP/TSE License</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.5 or higher</td>
</tr>
</tbody>
</table>
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 Officelinx 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.

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.

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

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.


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

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

7. The superuser account has been created. Click **Finish** to exit the wizard.
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.

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

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

   Click **OK** to save your changes.

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**.

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.

   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.

Configuring the IMAP server

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

`Get-imapsettings`

For integration with the IMAPTESE, 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.
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.

**Note:** All mailbox accounts that require IMAPTE 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 `COMPANY.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 Officelinx 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.

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.
OL Admin Configuration

For Officelinx and Exchange to be able to synchronize data, Officelinx 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 TSE Endpoint

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

- **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 143.
- **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 TSE 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 IMAP TSE 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 a Messaging & Collab or Messaging user to utilize synchronization.
Assign the mailbox to the Feature Group that is going to have the superuser account credentials.

Save all changes and move onto Feature Group Configuration.

Feature Group Configuration

The Feature Group plays a key role in IMAPTE 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 TSE Endpoint created in the previous steps.

Save all changes and proceed to Registry Settings.
Registry Settings

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

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

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

The new registry entry will appear in the Registry.

Proceed with Certificate Configuration.
Certificate Configuration

In order to ensure that the communication between Officelinx and the Exchange server is not interrupted by security measures, install the certificate from the Exchange server computer on the Officelinx 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 Officelinx 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**.

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.

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

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

6. The following popup confirms the import was successful.

   Click **OK**.

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.

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.

   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 TSE 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 Officelinx installation, you must do so manually now by running the `ExchangeMapiCdo.msi` file from `MSExchange` folder on Officelinx 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.

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.

By customizing these settings you can easily segregate calendar and contact synchronization along with message synchronization when enabling features for your users, allowing you to control exactly who has access to certain features.
Once calendar and contact synchronization has been enabled, all transactions occur on the server in the background, so you do not have to configure anything on your own. Use your mail server as you normally would, and any calendar or contact entries will now be mirrored in your Officelinx 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.

### Calendar Synchronization

When you create a calendar entry in Outlook, or most other email programs, the same entry will appear in your Officelinx mailbox.

The time and date of the meeting is automatically sent to the Officelinx 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.

### Contact Synchronization

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

Contact information is automatically sent to the Officelinx mailbox.

---

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

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

---

**Caution:** Deleting contacts is also synchronized. If you delete an entry from Outlook, it will also be deleted from Officelinx, 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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages</td>
<td>&lt;5000 combined</td>
<td>&lt;20000</td>
<td>&lt;100000</td>
</tr>
<tr>
<td>Contact and Calendar Entries</td>
<td>&lt;5000</td>
<td>&lt;5000</td>
<td>&lt;10000</td>
</tr>
</tbody>
</table>
OFFICELINX TO OFFICE 365
INTEGRATION WITH EWS

In This Chapter:

158    Introduction
158    Pre-requisites
159    Office 365 Configuration
159    Web Interface Configuration (Part 1)
163    Web Interface Configuration (Part 2)
165    Avaya Officelinx Server
167    Verify Configuration Setting
165    Server Configuration
Introduction

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

**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 Officelinx 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).
- Administrative access to the Office 365 domain. Web and PowerShell access is required.
- Officelinx Server installed and running (refer to Avaya's documentation web site).
Office 365 Configuration

Web Interface Configuration (Part 1)

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

   Go to Management > Users and create a new user (New > User).

2. Enter the required details and user name for the superuser (service) account. No Additional Details are required.

   Click Next.
3. Set the user’s geographic location.

Note: This account does not require administrator permissions. Specific roles and security access will be assigned later using PowerShell.

Click Next.

4. Assign the appropriate licenses. For Avaya Officelinx, only the Exchange Online (Plan 2) license is required.

Click Next.
5. Choose whether or not you wish to receive account creation results by e-mail.

Click Create.

6. Verify that the account was created successfully.

Record the Temporary Password and click Finish.
Windows PowerShell configuration

On your Windows desktop, start a PowerShell session. Initiate the connection to the Office 365 domain with the following commands:

```powershell
$User-Credential = Get-Credential

At the prompt, enter the full username (e.g. account@here.yourdomain.com) and password of the Administrator account.

Initiate the connection using:

```powershell
PS > Import-PSSession $Session
```

**Note**: If running the following command causes an error, it is necessary to run this command first:

```powershell
PS > Enable-OrganizationCustomization
```

Enter the following command. Replace the **User** parameters (in orange) with the superuser account details created above:

```powershell
PS > Get-Mailbox | Add-MailboxPermission -User superuser@here.yourdomain.com -AccessRights FullAccess -InheritanceType All
```

Verify that it runs successfully. Enter:

```powershell
PS > New-ManagementRoleAssignment -Name "OLSUAcct" -Role "ApplicationImpersonation" -User superuser@here.yourdomain.com
```
Web Interface Configuration (Part 2)

Log on to the service account to change the temporary password before it can be used with Officelinx.

1. In a browser, log in to the account at http://login.microsoftonline.com/. Set the password for the service account and record it for later use.
2. After logging in (specifying a time zone if required), select **Outlook Options**.

3. Go to **Outlook Web App > Account > My Account**. Click **Settings for POP, IMAP, and SMTP access**.
4. In the pop-up window, note the server address for the IMAP connection (e.g. under IMAP setting, record **Server name: pod#####.outlook.com**).
1. In Officelinx 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. Office 365).
   - **IMAP Server Address**: Type in the IMAP server name setting from previous section (e.g. ews:pod#####.outlook.com).
   - **IMAP Server Port**: Set to 993 to enable SSL connectivity.
   - **Voice Format**: Select MPEG-1 Audio Layer 3 (MP3) for client playback.
   - **IMAP Server Domain**: Enter the Office 365 domain name (e.g. here.yourdomain.com).

2. Once the TSE IMAP Server entry has been created, go to Feature Group > Synchronization Settings and modify the Office 365 user mailboxes as follows:
   - **IMAP Account**: Enter the super user/service account created previously. Include the complete user@domain.com (e.g. superuser@here.yourdomain.com).
   - **Account / Confirm Password**: Enter the super user/service account password.
   - **IMAP Server**: Type in the name of the IMAP TSE Server (e.g. Office 365).
   - **Calendar Mode**: Select None.

*Note*: Calendar synchronization is not supported with Office 365. If both Outlook and the UC Client desktop software are being used, Outlook Client Calendar push mode can be enabled. Select this option from the Calendar Mode drop down menu.
**Synchronization Settings:** Set these options to specify which information will be synchronize.

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

configuration is complete. Proceed with verification of the configuration file.

**Note:** Contact integration is not supported with Office 365.
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.

   ![File Explorer](image1)

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

   ![File Explorer](image2)

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:

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

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.
13 IBM DOMINO INTEGRATION

In This Chapter:

170 Introduction
170 Visual Guide
170 Requirements
171 Server Configuration
171 Setting up IMAP TSE Synchronization
172 Officelinx Configuration: Single User
175 Installing UC Forms for IBM Notes
182 User Guide
182 Installing UC Forms in IBM Notes
183 Verifying the IBM Notes client ECL setup
184 Using UC Forms in IBM Notes
186 Configuring UC Mailbox to Synchronize with IBM Notes
Introduction

Officelinx and a IBM Domino server are able to integrate through the IMAPTSE 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 OL 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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>IMAPTSE License</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.5 or higher</td>
</tr>
</tbody>
</table>
Server Configuration

IBM Domino configuration is largely divided into two parts. First is the configuration of both the Domino server and the Officelinx 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 Officelinx.

Setting up IMAP TSE Synchronization

To configure IBM Notes for Officelinx 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**.
Officelinx Configuration: Single User

**Note:** Configuring Officelinx for use with Superuser credentials is no longer supported.

With this option, Officelinx 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 TSE connections **before** setting up Unified Messaging.

To begin the setup of your unified messaging you need to create a TSE 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 TSE IMAP connections

1. Login to OL 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.
   - 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:** 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**.
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 Officelinx 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 OL 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.

   **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

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.

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.
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 Officelinx 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.
4. Expand **Shared Elements > Subforms** in the left pane of the Designer window. From the main pane locate **UCPlayer** and double click to open.

![Designer window with UCPlayer subform](image1)

5. The fields associated with the UC Player subform appear. Open the **UCIBMSRV** variable and enter the Officelinx 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.

![UCPlayer subform with UCIBMSRV variable](image2)

**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**.
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**.

2. From the **Workstation Security: Execution Control List** window, click on the **Add** button.

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**.

5. Repeat for both the **Java applet security** and **JavaScript security** radio buttons.

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.

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.
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.

**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.

9. Click OK. The UCPlayer subform will be inserted into the Message form.

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 178 to complete the process.
Installing UC Forms in IBM Notes

To use UC forms within IBM Notes, you must install iLink Pro Desktop. Obtain iP 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.

5. IBM Notes will open a web page to download the iLink Pro Desktop software. iP must be installed for UC forms to work.

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.

**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.

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.

   - 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.
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.
   • 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.

   ![Image of UC forms with voice message options]

   **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.

   ![Image of UC forms with phone call options]

   **Note:** Some actions may not be available depending on site settings.
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.

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.
   - **Password:** Enter the password for your mail account.
   - **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.

**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.

**Note:** The password you enter in this field will be the same password for the email account as it exists on the mail server.
14 FIND ME FOLLOW ME ON CTI INTEGRATION

In This Chapter:

188 Introduction
188 Visual Guide
188 Requirements
190 User Guide
190 Find me Follow me with CTI Integration
Introduction

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

This document is intended for technicians who have some familiarity with the Officelinx 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. In the case of Iwatsu ECS, the stations need to be monitored with the CTI Link, and the calls need to be forwarded to the UC Locations options in the feature group.

Refer to the Technical Operating Guidelines for details on PBX’s.

Note: The Hunt Group field should be left bank.

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, Officelinx will try to locate the user through a broadcast rather than through a single phone number or device. Whenever a call comes in, Officelinx will try to locate the user through multiple devices simultaneously (or as configured). Once the user accepts the call on one device, Officelinx will connect the caller with the user and terminate the other calls.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>---</td>
</tr>
<tr>
<td>Requirements</td>
<td>Details</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Software</td>
<td>OfficeLinx version 8.5 or higher</td>
</tr>
</tbody>
</table>
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 OL 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 OL Admin console, please contact your System Administrator.

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

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

The Find Me Rules page displays all of the options available for that location. It is important to note that this section will configure how the Auto attendant will behave for incoming calls. However, it is necessary to set the current location as well as availability. Refer to page 275 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).

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

In order for outside calls to be dialed by the voice server, configure outcalling through Windows Control Panel > Phone and Modem Options and make sure the local area code is selected.
If the call will be forwarded to a long distance number, enable **Long Distance** under **Feature Group > Notification Options > Outcalling Options** for the group containing the member.
Configuring Find me Follow me features

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

**Only call me at the first number assigned to this location**

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

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

Click on the **Save and Close** button

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

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

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

**Automatically find me:**

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

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

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

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

  When a call is transferred by the Auto attendant or when a call is made to a DID that rings the extension directly, the Auto attendant will 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:

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

---

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

---

Click on the **Save and Close** button

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

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

---

**Note**: 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

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

When this feature is selected it is necessary to specify the channels used for the broadcast in **Company Properties > C.O./Channel Assignment**.

**Automatically find me:**

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

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

Click on the **Save and Close** button

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

When a call is made to a DID and the default internal extension is in the list of numbers assigned to the location, that internal extension will always ring first and if there is no answer then the Auto attendant will automatically dial the rest of
the numbers in the list simultaneously.

**Note:** 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 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:

![Find me rules tab](image)

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 tab](image)

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.
PROPERTY MANAGEMENT SYSTEM

In This Chapter:

200 Introduction
200 Check-in overview
200 Supported Vendors
201 PMS features
201 Connections
201 Supported functions
203 Maid Status
204 Message type examples
206 Setting up PMS integration
206 Step 1 - Verify connections
207 Step 2 - Specify PMS configuration settings
210 Step 3 - Create mailboxes and assign feature groups
213 Step 4 - Record prompts
Introduction

This guide provides an overview of the Property Management System Interface for Officelinx. The Property Management Systems (PMS) is an add-on module for the Officelinx platform. The PMS acts as a bridge between a hotel's 3rd-party application and the Officelinx voice server.

A typical third-party PMS application gives hotel employees control over their guest database (check-in and check-out, for example). Any hotel that uses their third-party application with an Officelinx voice server uses PMS to enable communication between the two.

**Warning:** The Property Management System feature of Officelinx is not supported under a High Availability (HA) environment.

Check-in overview

The following steps detail a typical PMS check-in scenario:

1. User checks into hotel.
2. Hotel employee checks user into room and saves user info using PMS application.
3. The hotel's PMS application sends “check-in” packet (room, guest name, etc.) to the Officelinx PMS service.
4. Using EEAM, Officelinx PMS creates new mailbox or updates an existing mailbox.

Supported Vendors

The following PMS vendors are supported by the Officelinx Property Management System:
PMS features

The Officelinx Property Management System provides the following features:

- When a **Check-In** function is performed on an extension, the mailbox is automatically logged in and the tutorial is activated. The first time a user calls into their mailbox, they are greeted with a welcoming tutorial.
- When a **Check-Out** function is performed, the mailbox logs out and automatically re-routes messages that have not been deleted to a **phantom** mailbox. Messages can still be retrieved from this storage mailbox.
- When a user accesses their mailbox, new messages will play automatically, and users can save or delete them. This option can be changed so that a default action, either save or delete, is performed once the message has been played.
- When users access their mailbox, they have the option to **save**, **delete** or **review** their messages, or **listen to the time and date** the message was received.
- Users can listen to voicemail commands and options **in a language other than English**.
- **Housekeeping can call from a room and report on the room’s status**.
- Use the LAP module to have housekeeping paged through the hotel over a wireless transmitter.

Connections

Establish a connection with a 3rd-party hotel application using a serial port or a TCP/IP connection.

If you are using TCP/IP, the hotel application acts as a server by listening for incoming connections on a particular port. The PMS server acts as a client by connecting to the specified port.

Supported functions

The interfaces listed in the following table may or may not be supported, depending on the PMS protocol being used. If a PMS can only partially support an interface, then only supported messaging can be used.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check-In</td>
<td>A message is sent when a room changes from Vacant to Occupied. The voice mailbox is turned on. This message is not sent for Shares.</td>
</tr>
<tr>
<td>Check-Out</td>
<td>A message is sent when the last account has checked out of the room. The voice mailbox is turned off.</td>
</tr>
<tr>
<td>Room Change</td>
<td>A message sent on a room change.</td>
</tr>
<tr>
<td>Room Merge</td>
<td>A message sent on merging a room.</td>
</tr>
<tr>
<td>Room Reset</td>
<td>A message is sent to reset the room to default values.</td>
</tr>
<tr>
<td>Name Change</td>
<td>A message is sent to indicate the changing of a guest name.</td>
</tr>
<tr>
<td>Message Lamp On</td>
<td>A message is sent to the VM to activate the Message Waiting Indicator in the room.</td>
</tr>
<tr>
<td>Message Lamp Off</td>
<td>A message is sent to the VM to deactivate the Message Waiting Indicator in the room.</td>
</tr>
<tr>
<td>Set Wakeup Call</td>
<td>A message is sent to request a wakeup call at a defined time and date.</td>
</tr>
<tr>
<td>Clear Wakeup Call</td>
<td>A message is sent to cancel any existing wakeup calls to the room.</td>
</tr>
<tr>
<td>Maid Status</td>
<td>A message is sent to PM when the maid enters a code on the phone in the room.</td>
</tr>
<tr>
<td>FEATURE</td>
<td>CENTIGRAM</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>CHECK IN</td>
<td>●</td>
</tr>
<tr>
<td>CHECK OUT</td>
<td>●</td>
</tr>
<tr>
<td>DND ON/OFF</td>
<td></td>
</tr>
<tr>
<td>LANGUAGE CHANGE</td>
<td></td>
</tr>
<tr>
<td>MWI ON/OFF</td>
<td>●</td>
</tr>
<tr>
<td>NAME CHANGE</td>
<td>●</td>
</tr>
<tr>
<td>RESET WAKEUP</td>
<td></td>
</tr>
<tr>
<td>ROOM MERGE</td>
<td>●</td>
</tr>
<tr>
<td>ROOM MOVE</td>
<td>●</td>
</tr>
<tr>
<td>ROOM SWAP</td>
<td></td>
</tr>
<tr>
<td>SET WAKEUP</td>
<td></td>
</tr>
<tr>
<td>STATUS CHANGE TO IN OFFICE</td>
<td></td>
</tr>
<tr>
<td>WAKEUP RESET</td>
<td>●</td>
</tr>
</tbody>
</table>
Maid Status

**Note:** The Property Management System service is the means by which a hotel's third party PMS acts together with the Officelinx Voice Server.

**Note:** The Property Management Interface is what the User interacts with when using the PMS, depending upon the protocol supported.

The Voicemail server will send a room status message to the Property Management server when a maid inputs a code on the phone in the room. The following Maid Status Codes are recognized by the PMI:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CL, AV, 1</td>
<td>clean</td>
</tr>
<tr>
<td>DI, NA, 2</td>
<td>dirty</td>
</tr>
<tr>
<td>MI, 3</td>
<td>questionable</td>
</tr>
</tbody>
</table>

The PMS will update the room status for only the values listed above. All other values will be ignored. The hotel staff will need to be instructed on how to enter the maid status information from the telephone in the room.

**Note:** The following protocols support Maid Status: AVT, RAMESYS, MCORP, FIDELIOXPRESS, COMTROL, PMS1, PMS3.
Message type examples

The following are examples of each message type.

From Property Management Interface:

Check-In John Smith into Room 123, password 9876, Language 1
<STX>CHKIN 123 SMITH, JOHN 9876 1 <STX><BCC>

Check-Out Room 123
<STX>CHKOUT 123 <STX><BCC>

Room Change John Smith from Room 123 to Room 456, password 9876, Language 1
<STX>ROOMCHG 123 456 SMITH, JOHN 9876 1 <ETX><BCC>

Room Merge room 123 and 456
<STX>ROOMMRG 123 456 <ETX><BCC>

Reset Room 123
<STX>ROOMRST 123 <ETX><BCC>

Change Name on Room 123 to Tom Jones, Language 2
<STX>NAMCHG 123 JONES, TOM 2 <ETX><BCC>

Set or Cancel MWI on Room 123
<STX>MSGON 123 <ETX><BCC>
<STX>MSGOFF 123 <ETX><BCC>

Set or Cancel a Wakeup Call for Room 123
<STX>WAKESET 123 0630 <ETX><BCC>
<STX>WAKECLR 123 <ETX><BCC>

From Voice Mail Server:

Maid Status for Room 123 to 1
<STX>MAID 123 1 999 <ETX><BCC>

Additional CSTA Functions are available if your PBX CTI support them. Panasonic supports all additional functions.
Display

- At Check-In, the guest name will be automatically shown on the telephone display in the appropriate room.
- At Check-Out, the guest name will be cleared to show a blank screen on the telephone display in the appropriate room.

Class of Service

The Check-In and Check-Out services can be defined in the registry settings as follows:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Tolee (UCP, MN6510UC)\General Settings\CheckIn ClassOfService Number (REG_SZ)
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Tolee(UCP,MN6510UC)\General Settings\CheckOut ClassOfService Number (REG_SZ)

- Class of Service for Check-In = 2
- Class of Service for Check-Out = 7

Wake-Up Call

- When the guest has requested a wake-up call on the system, the switch will handle the action rather than the Officelinx software.
Setting up PMS integration

**Warning:** The Property Management System feature of Officelixn is not supported under a High Availability (HA) environment.

There are 4 steps to a successful integration.

1. Verify connections
2. Specify config settings
3. Create mailboxes and assign feature groups
4. Record prompts

**Step 1 - Verify connections**

The Hospitality Server couples to the voicemail system via the PBX (incorporating a serial link through the serial port). The type of integration between the voicemail server and the PBX depends solely on the PBX.

In the following example, the switch sends Inband digits:
Step 2 - Specify PMS configuration settings

Perform the following procedure to allow interaction with the PMS for hotel applications.

To specify PMS configuration settings:

1. Open the Officelinx Admin console.
2. In the Admin tree (left hand pane), expand Configuration, and right click on Device Management.
3. From the menu, select New > PMS Device. The following screen appears.
4. Specify the following:
   - From the COM Port Number dropdown list, select the port where your PMS device is connected.
   - In the TCP/IP Address text field, enter the TCP/IP address where your PMS device is connected.
   - In the TCP/IP Port text field, enter the TCP/IP port number where your PMS device is connected.

5. Click Settings and the PMS Settings dialog box appears.

Note: PMS settings allows you to control the information that the UC Server receives from the Property Management software.
See Settings for your PMS package on page 209.
6. Specify the following:
   • Select the **PMS Installed** checkbox if a Proprietary Management System is installed.
   • Enable **Welcome Message Active** to activate a welcome message in a room voicemail every time a room is reset.
   • In the **PMS Mode** text field, specify the mode to use.

   **Note:** This field is content-sensitive. Make sure not to misspell the mode.

   • In the **PMS Type** text field, indicate the type of serial port protocol to use (i.e. Fidelio, Lanmark, or CAPA).
   • In the **Polling Interval** text field, enter the time interval - measured in seconds - to poll the COM port for PMS events. The default value is 5.
   • In the **PMS Shared Directory** text field, enter the directory path where the PMS stores its files so that Officelinx may access them.
   • In the **Local PMS Shared Directory** text field, enter a local directory where these files are stored.
   • In the **Auto Action On Message** text field, specify an automatic action the system will perform when a message is received.
   • In the **PMS Check Out Message Destination** text field, specify the integer value that will be placed before the mailbox number of a departed client.

   **Note:** This feature applies solely to hotel applications. It will create a phantom mailbox where messages will be forwarded for a client to retrieve. For example, if the PMS Checkout Message Destination value is set at 7 and a customer checks out from room #197, messages can still be retrieved from phantom mailbox 7197 until the next checkout action from that room. The next person to check out of room #197 will overwrite the old mailbox with the new one.

7. Click **OK** twice.
Settings for your PMS package

The settings for the Hospitality packages currently supported are almost identical. The settings that remain the same for all are:

- **PMS Installed** = Enabled
- **PMS Mode** = Serial

Settings that depend upon the connection type, and may differ between systems are:

- **Com Port Number** = 1 (may be any available Com Port number)
- **Device** serial communication settings = 9600 / None / 8 / 1
- **PMS Check Out Message Destination** = 7 (varies by customer preference)

**Note:** For Landmark, Capa, and Fidelio, the PMS Type is set to Alcatel, but for MSI the Type is AVT. See below.

**Auto Action On Message** = Save

**Note:** This field tells the voicemail system to automatically perform the specified action after each message is played. The options are **Save**, **Delete**, and **None**.
Step 3 - Create mailboxes and assign feature groups

Now setup mailboxes and associate them with feature groups. You will need to create 2 feature groups.

Feature Group 1 - for room mailboxes

1. In the Admin tree (left hand pane), expand Company and highlight Feature Group.
2. Right click on Feature Group and select New > Feature Group. The Feature Group screen appears.
3. Click on the Notification Options tab.

4. Enable Message Light Activation to employ the message waiting light feature. Enabling the checkbox activates:
   - ON For All Msgs to indicate that the message light on code will be set for all messages.
   - OFF For All Msgs to indicate that the message light off code will be set for all messages.
   - OFF When No New Msg to indicate that the message light off code will be set only when there are no new messages in the user’s mailbox.
   - No of ON Retries - enter the number of times the system will retry message light activation.
   - No of OFF Retries - enter the number of times the system will retry message light deactivation.
   - ON Between Retries - enter the time (in minutes) to wait between retry attempts to activate the message light.
   - OFF Between Retries - enter the time (in minutes) between retries to deactivate the message light.
   - ON Code - enter the code to turn on message waiting lights.
   - OFF Code - enter the code to turn off message waiting lights.

   **Note:** The ON Code and OFF Code fields should be used in situations where the code is too long to be input in the ON Code field in the PBX Message Light tab (usually MCI). In addition, for multi-PBX configurations different codes must be used for different PBXs. In this situation, certain feature groups can be assigned to a message waiting light code that reflects the different PBXs being used.

   - In the Channels text field, enter the channel number that will be used to send message light notification.

5. In the Message Light Type feature box, select the checkbox that indicates which message type is to be associated with the message lights:
   - Select the All checkbox for all messages.
   - Select the Fax checkbox for fax messages only.
   - Select the Voice checkbox for phone calls only.
6. In the **Outcalling Options** feature box:
   - Select the **Beeper** checkbox to allow the system to notify a user via beeper, voice pager, or alpha-numeric pager when a message is recorded to the user’s mailbox.
   - Select **Outcall** checkbox to allow the system to notify a user at a specified telephone number when a message is received to the user’s mailbox.

**Warning:** If the telephone number is long distance, the **Long Distance** checkbox must also be checked to allow long distance dialing.

7. Click on the **Save Feature Group** button.

**Note:** All other feature group options are set at the discretion of the system administrator.

You will now create a mailbox for each hotel room. It is important that you:
- make sure the **Ask for Password** checkbox (**Feature Group > Mailbox Options**) is disabled.
- link each mailbox to the feature group you have just created.

For in-depth information on setting up feature groups, refer to the **Officelinx Server Configuration Guide**.
Feature Group 2 - for storage mailboxes

The second feature group you create will be associated with the mailboxes that store the messages that are not deleted when a user checks out of the hotel. These mailboxes will start with the digit you specified in the PMS Check Out Message Destination field, back in your configuration parameters (Device Management Settings > PMS Settings).

For example, if you set the value in that field at 7, messages from mailbox 237 (room 237) will be automatically moved to mailbox 7237 when a user checks out.

You would have a 3-digit mailbox assigned to each hotel room and a 4-digit phantom mailbox to complement it.

1. In the Admin tree (left hand pane), highlight Feature Group.
2. Right click on Feature Group and select New > Feature Group. The Feature Group screen appears.
3. Click on the Notification Options tab.
5. Click on the Mailbox Options tab:

![Feature Group Screen](image)

6. Hit the Save Feature Group button.

**Note:** All other feature group options are set at the discretion of the system administrator.

You will now create a storage mailbox for each of your existing room mailboxes. In this example, there are mailboxes for rooms 100-119, 200-219 and 300-319. If, back in Device Management Settings > PMS Settings, you entered a 7 in the PMS Check Out Message Destination field, you will create new storage mailboxes starting with 7. Therefore, your first mailbox would be 7100, then 7101, following that 7102, and so on.
Step 4 - Record prompts

The `C:\WINVM\MESS820.VOX` prompt exists specifically for use with PMS integration. For information on re-recording prompts, refer to the Officelinx Server Configuration Guide. Prompt 820 is a welcome greeting that says:

Welcome to your voice mail. Your mailbox is where your messages will be stored. It is simple to use. If you have any questions about using your mailbox, please contact the front desk.

**Warning**: PMS is a feature that is purchased separately. Please contact your Sales Representative for further details.
16 MASS RECALL

In This Chapter:

216 Introduction
216 Visual Guide
216 Requirements
217 Server Configuration
217 Message as an outside caller
220 Message sent by a user from their Mailbox
222 Activating Mass Recall Logs
223 Mass Recall Example
223 Mass Recall Destination Mailbox
225 Mass Recall Activation/Cancellation Mailbox
228 Mass Recall Activation
228 Mass Recall Cancellation
Introduction

Officelinx has built in capability for broadcasting messages in case of emergency. For some markets, such as the prison system, health care system, etc., this is known as Mass Recall. The primary function of Mass Recall is to send emergency messages to a set of mailboxes, which in-turn activates the broadcast functions setup in the destination mailboxes. This chapter outlines the steps to configure the Officelinx Server to use Mass Recall. For an actual implementation of Mass Recall, please refer to Mass Recall Example on page 223.

**Note:** In the Admin, Advanced > Mass Recall Installed must be set to True.

**Note:** In the Admin, LOG > Log Mass Recall must be set to True.

Visual Guide

A member of the organization records a voice message, and initiates a Mass Recall when an emergency occurs.

Officelinx dials each person on the Mass Recall list to notify them there is a new message waiting in their mailbox.

When the required number of people have responded, the initiator of the Mass Recall cancels the action.

Officelinx stops the Mass Recall and no further calls are made.

When an emergency occurs, personnel may initiate a Mass Recall by recording a message for broadcast. Once initiated, Mass Recall will start calling everyone on the list with the recorded message. Once the necessary people have responded and reported into the organization, the initiator of the Mass Recall cancels the action preventing further dialing.

By utilizing this tool, an organization can easily reach on-call or emergency staff members should the need arise.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>---</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.5 or higher</td>
</tr>
</tbody>
</table>
Server Configuration

There are 2 ways to leave a message for Mass Recall:

- Message as an outside caller that is left to a mailbox predefined for Mass Recall.
- Message sent by a user while logged in to their mailbox. This method requires the TUI assigned to the user’s mailbox to have the ability to flag messages for Mass Recall.

Message as an outside caller

1. To create a Voice Menu, right-click on the Voice Menu icon, and select **New > Voice Menu**.

2. Name the Voice Menu **Mass Recall**.

   If an initial greeting should play before sending a Mass Recall message, select the greeting from the Sub Menu Phrase dropdown list. If not, then set the Phrase to Nothing.

3. From the list of Actions, select **Send a Mass Recall Message** and drag this to the DTMF key it is to be assigned to.

   In this example, by assigning this to Default, the Mass Recall action will be triggered at the end of the greeting.

4. Double-click on the action, and select the mailbox or destination for the Mass Recall Message.

   Click **OK**.

5. Click **Save**.
6. Right-click on Mailbox Structure, and select **New > Mailbox**.

7. **Assign a Mailbox Number**.
   - Enter a **First Name** and **Last Name**.
   - Leave the user name and password fields blank.

8. Go to the Advanced Tab and enable **Voice Menu**. Use the dropdown list to find the Voice Menu for Mass Recall.

   **Click Save.**

   **Note:** This mailbox will be the main mailbox for Mass Recall. To cancel Mass Recall messages sent via the Voice Menu, log into this mailbox to cancel.
9. In the destination mailboxes for the Mass Recall messages, as defined in the Voice Menu, you must define the notification rules to enable notification to each destination. Refer to the Server Administration Guide to configure notification.

In this example, Mailbox 3000 must be properly configured for notification.

**Warning:** There must be at least 1 notification address listed in order for it to qualify for a Mass Recall.
Message sent by a user from their Mailbox

1. The Customized TUI of the user must have a Send Message Menu which offers the option of setting the Mass Recall flag.

Double-click the default for your Company to open the Properties window.

2. Click Customize TUI.

3. Find your default menu and verify that it is checked.

Highlight the menu and click OK.

4. Select the Send Message Option.

You can see the Next Sub Menu is number 6.

Go to Sub Menu 6.
5. Make sure there is an Action to **Toggle Mass Recall**.

If not, select Toggle Mass Recall from the list of actions, and drag it to a DTMF Key.

6. To send a message from a mailbox, the user must first log into their mailbox on the phone. To login, dial the access number to reach the main company greeting. **Press #**, then enter your **mailbox number** and **password**. Send a message normally. To mark the message for Mass Recall delivery, choose the Mass Recall Toggle action at the end of the message.
Activating Mass Recall Logs

The Mass Recall Logs allows you to keep track of events related to the Mass Recall function.

1. From the OL Admin program, go to **Configuration > Advanced.**
   Locate **Mass Recall Installed** from the right pane and make sure that it is set to **True.**
   Double-click the item and change the value if necessary.

2. Once set, click on **Logs** in the left-hand menu.
   In the right-hand window, set **Log Mass Recall** to **True.**

3. Once the logging becomes active, Mass Recall will create a log file named **Mrecall.log** in the **UC\Logs\Vserver** folder. This log may be opened by any type of text editor.
Mass Recall Example

The following is a sample of Mass Recall configuration and usage.

Mass Recall Destination Mailbox

The following are the extensions/mailboxes that are the target of the Mass Recall. The extensions are organized into a Distribution List (DL).

- **DL 912 - All Staff:**
  - EXT 200, 201, 202, 203
- **DL 913 - Executive Staff:**
  - EXT 200, 201, 202
- **DL 914 - Daily Staff:**
  - EXT 200, 201
- **DL 915 - Managers:**
  - EXT 200

The contact in the Mass Recall Distribution Lists must have external phone numbers available as a **Notification Address**. Ensure that the **Notification Schedule** is setup so that it is always active. When configuring the Notification Schedule please configure as shown below.
Each Distribution List created must be **connected to a mailbox** in order for Mass Recall to access it. Create a mailbox with the same number as the DL (i.e. DL 912 will be connected to mailbox 912).

### Hint

The Distribution List number and the mailbox number do not have to match for this function to work. It is done here to make keeping track of things easier.

Each mailbox created for this purpose must be configured as follows:

- **Destination Type:** Target Distribution List
- **Forward Type:** Relay
- **Message Type:** Voice

This process will be repeated for mailbox 913, 914 and 915. The only difference between the configurations will be the Distribution List selected.

With this setup, Mass Recall can target specific groups depending on the event requiring Mass Recall. Once the Mass Recall destinations have been defined, you must create a mailbox to utilize the Mass Recall function.
Mass Recall Activation/Cancellation Mailbox

Create and use mailbox number 911 as a point of access to the Mass Recall function.
1. Create mailbox 911.
2. The user initiates Mass Recall by accessing the voice menu of mailbox 911. The voice menu is configured to ask the user for a password. Once the password is accepted, the user is sent to the sub menu with access to the following:

   **Note:** You should also record a greeting/salutation to attach to the Voice Menu as well. Having this prompt will allow the Mass Recall system to be more user friendly.

   **Press 1** to recall All Staff (DL/mailbox 912)
   DTMF digit 1 is set to Send a Mass Recall Message mailbox=912 Mass Recall All Staff

   **Press 2** to recall Executive Staff (DL/mailbox 913)
   DTMF digit 2 is set to Send a Mass Recall Message mailbox=913 Mass Recall Executive Staff

   **Press 3** to recall Daily Staff (DL/mailbox 914)
   DTMF digit 3 is set to Send a Mass Recall Message mailbox=914 Mass Recall Daily Staff

   **Press 4** to recall Managers (DL/mailbox 915)
   DTMF digit 4 is set to Send a Mass Recall Message mailbox=915 Mass Recall Managers
3. Create a Custom TUI for mailbox 911 to have the option of canceling the Mass Recall.

**Note**: You should also record a salutation to attach to the Custom TUI. Having this prompt will allow the Mass Recall system to be more user friendly.

- Press 1 to Cancel Mass Recall
  
  Upon the cancellation of Mass Recall, the user must be disconnected from the telephone. To do this, add the following option.

- Press # to Send to Sub Menu 1.
  
  The Default Action of Sub Menu 1 will be **Disconnect**, and the Number of Retries will be set to 1 to disconnect the user after they enter Sub Menu 1.

- Record a voice prompt for the Custom TUI that states **Press 1 then # to cancel the Mass Recall**. When the user follows the action, they will cancel the Mass Recall by pressing 1, and then be disconnected from the system by pressing #.

4. Attach the Voice Menu and Custom TUI to mailbox 911.
5. Set the mailbox to be Unavailable. This allows users to leave a message immediately after calling the mailbox, then send that message to the target Mass Recall list through the voice menu.
Mass Recall Activation

In a typical scenario:
1. Call in to the system and access mailbox 911.
2. Enter the access code defined in the Voice Menu configuration.
3. Record the message that will be sent out to the Mass Recall distribution list members.
4. Once the recording is complete, there are 4 options. Presses the DTMF key that corresponds to the Distribution List to send the Mass Recall to.
5. Push 1 to send the message. Hangs up the phone after the confirmation message is heard. The Mass Recall is now active.

Mass Recall Cancellation

1. The user logs into mailbox 911 to access the Custom TUI.
2. After listening to the prompt, the user pushes 1 then # to cancel the Mass Recall.
   The user is disconnected from the mailbox and all remaining Mass Recall activity is cancelled.
OUTCALL TASK MANAGER (ABSENTEEISM)

In This Chapter:

230 Introduction
230 Visual Guide
230 Requirements
231 Server Configuration
231 Creating an Outcall List
234 Setting the Outcall Schedule
235 Creating a Custom Outcall Message
236 Managing the Outcall Tasks
237 The Response Log
Introduction

The Outcall Task Manager in Officelinx can be used to make automated calls to any designated number, both internal and external. The Outcall Manager may also collect DTMF response from the receivers.

A typical scenario for Outcall Task Manager is a school verifying a list of absent students. A staff member can place a list of students that are absent into a database using a CSV (comma separated value) file, which can be automatically exported from a spreadsheet program. Alternatively, each of the student’s information can be entered manually into the Outcall Task Manager.

Once the list has been created, the staff member must also create the greetings, DTMF responses to be accepted, and schedule the outcall. When ready, the Outcall Task Manager will start calling everyone on the list, and will keep a log of all the responses received for each call.

Visual Guide

Staff member at the school receives a list of absent students from the faculty, then creates a list for Outcall Task Manager.

The list is entered into the application and the outcall is initiated by the staff. The outcall message and list of responses have already been created. Officelinx calls each student's contact number individually to obtain a response.

Successful responses which were received are compiled by Officelinx.

Faculty members are able to mark their students' absences accordingly depending on the response received.

Staff member retrieves the list of responses when the outcall process is finished, then delivers the results to the faculty.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>License to enable Outcall Task Manager</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.5 or higher</td>
</tr>
</tbody>
</table>
Server Configuration

Outcall Task Manager is a stand alone program that resides on the server computer. For this reason, and due to the nature of automated outcalling, it is best to limit user access to Outcall Task Manager.

Creating an Outcall List

Launch the **Outcall Task Manager**. The following window will appear.
Import from File

Click on the **Import from File** button. The following window will appear.

Select the CSV formatted text file to be imported then click **OK**. The outcall list will be populated from the file.
Open File

Click on the **Open File** button to check the contents of the text file before you import it. This will open the file selection window.

Choose the CSV formatted file and click **Open**. The default text editor will open the target text file.

The **CSV** file may be exported from a spreadsheet program. The first entry is the **phone number for the outcall**. The second is the **student's name**, and the third is the **parent's name**. The last entry signifies the **student's gender**.

Add an Entry Manually

Enter the phone number to be called in the **Phone** textbox, then click **Add**.

Enter the student and the parent's name. The default gender of the student is male. Enable the Female checkbox will designate the student as female.

Click **OK** when finished.
Setting the Outcall Schedule

You may specify the outcall times so that the call task ends at the end of the day. To specify the start and end times, click on the **ellipsis** \( \ldots \) beside the Start and End times. The calendar dialogue will open. Select a specific date and time from the calendar to start/end outcalling.

Click **OK** to add the selection to the schedule.
Creating a Custom Outcall Message

You may create a custom outcall message through the `absence.ini` file. The contents of this file will be spoken to call recipients using TTS (text-to-speech).

To create a custom outcall message, click on the View INI File button. The following window will appear.

Under the Absence Reason section, create a list of responses that the call receiver can enter. These entries must follow the format `#=message`. The list created here will be spoken to the call receiver in the format of **Press 1 if he/she is Sick, Press 2 if he/she is On Vacation** and so on. You may only use single digit numbers to receive a response. This limits the number of responses to **10 (0 - 9)**.

The greeting section holds the text of the greeting and the good bye messages. The text typed after Greeting Text= will be spoken to the call receiver. The string `<NAME>` may be inserted in the greetings to customize each message for the receiver. This string will be automatically replaced by the current student's name. The string `<DTMF>` at the end will invoke the list of responses defined in the Absence Reason section.

**Hint**: Having no `<DTMF>` string at the end will suppress the reading of the Absence Reason list. Use this option if you want to include the reasons within the greeting itself.

**Goodbye Text=** is the response given to the call receiver once they have given a response.
Managing the Outcall Tasks

Once the list has been completed, click on the Create Outcall Task button. The outcall list will be generated using the database shown in the left-hand window. The outcalls will begin and end at the designated times.

For additional outcall management and configuration, refer to the list below.

- **Pause**: This button will pause the outcall task.
- **Refresh**: This button will refresh the list of outcalls.
- **Clean outcall Tasks**: This button will delete all pending outcalls that are on the list.
- **Delete Duplicate tasks with same phone numbers and names**: Enable this option to eliminate any duplicate entries among the pending outcalls.
- **Channel Range**: You may configure the range of channels that the Outcall Task Manager can use depending on your usage. For example, if you need to make as many calls as possible at once, you may allocate most of the channels to the task, but if you need to use your phone system you may allocate only a few channels to the Outcall Task Manager so that regular phone service is not interrupted.
The Outcall Task Manager keeps a log of all the outcalls that are made. This log is especially useful if you are requesting a response from recipients since all responses are included in the log. To view the logs, click on the View Log File button. The log file will be opened by the default text editor.

The information shown is in the following order:

- **Call Time** (13:50:35.367)
- **Channel Used for Outcall** (CH:001)
- **State** (State 3) *this information is for development purposes and may be discarded
- **Phone Number Called** (1235551234)
- **Name of Student** (Tom Doe)
- **Type of Response** (Responded:2 [On Vacation])
MULTIPLE TIME ZONE SUPPORT

In This Chapter:

240  Introduction
240  Visual Guide
240  Requirements
241  Server Configuration
Introduction

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

Visual Guide

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

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>---</td>
</tr>
<tr>
<td>Software</td>
<td>Officelinx version 8.5 or higher</td>
</tr>
</tbody>
</table>
Server Configuration

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

**General Settings**

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

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

Your system is now ready to manage multiple time zones.

---

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

**Note:** If the user does not have access to Web Access to specify their location calendar, an Administrator will need to set this using OL 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.
19

REMOTE ADMINISTRATION

In This Chapter:

244 Introduction
244 Visual Guide
244 Requirements
245 Installing Remote Admin
246 Connecting to Remote Admin
Introduction

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

Visual Guide

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
</table>
| 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 Officelixnx 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 Officelinx must be installed and operating normally on the voice server before proceeding.

**Important:** Remote Admin must be installed on the same subnet as the Officelinx 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 Officelinx installation directory (this is `C:\UC` by default). Share the UC folder with the Windows user(s) who will be running OL 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.

5. When prompted, enter the computer name for the Officelinx voice server, or the Consolidated Server. Click **Next**.

6. The program is ready. Click **Next** to begin installing the program.
7. Remote Administrator will be installed on the system.

8. When finished, the wizard will report that the installation was successful.

   Click **Finish** to complete the installation.

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

### Connecting to Remote Admin

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

1. Run the OL Admin shortcut from the desktop. The OL Admin login screen appears.
2. Enter the User Name and Password in the appropriate fields. Click **OK**.

   **Caution:** The computer launching Remote Admin must be a member of the same domain as the Officelinx server in order to make the connection.

3. You will be remotely connected to the OL Admin of the remote server.
20 REMOTE PRINTER

In This Chapter:

248 Introduction

248 Remote Printer Host Installation and Setup

251 Officelinx Voice Server Remote Printer Setup
Introduction

The Officelinx 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 Officelinx. It is installed by default as part of Officelinx 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: Officelinx 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 Officelinx DVD at: D:\UC\UCPrint (change "D:" to the correct location of your DVD drive).
2. Double-click this file to start the installation.
3. Click Next to continue.

Note: Officelinx 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 Officelinx DVD at: D:\UC\UCPrint (change "D:" to the correct location of your DVD drive).
2. Double-click this file to start the installation.
3. Click Next to continue.
3. The wizard will install the program. When ready, click Finish.

4. Go to Start>Administrative Tools>Services and verify that the UC Remote Printer service is installed and running. This service should be configured to start automatically.

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

5. Go to Start>Run and type regedit in the text entry box. Click OK.
6. 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).

7. In the right pane, double-click UMSTServer and enter the IP Address of the Officelinx server for the value data. Click OK and close the regedit screen.

The client side configuration is complete. Proceed with the setup of the Officelinx voice server.
Officelinx Voice Server Remote Printer Setup

The following instructions are performed on the Officelinx voice server.

**Note:** These instructions assume that Officelinx has already been installed and configured on the voice server. For details on the installation and setup of Officelinx, 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 Officelinx installation.
2. Open Officelinx Admin and click **Print Server**.
3. Right-click on **Print Server** and choose **Add**.

4. Fill in the required fields.
   - **Description**: Enter a descriptive name for the remote print server.
   - **Workstation Name**: Enter the PC name or the IP Address of the remote printer host computer.
   - **Available**: Enable this checkbox.

   Click **OK** when finished.

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

   Click **OK** when finished.

6. Go to **Start>Administrative Tools>Services** and disable the **UC Remote Printer** service.
7. Go to **Start>Administrative Tools>Services**. Stop then start the following services: 
   **UC Unified Messaging System Tasks Service** and **UC VPIMServer**.

8. On the computer acting as the remote printer host, stop then start the **UC Remote Printer** Service.

The setup of the Remote Printer feature is now complete.
In This Chapter:

- Introduction (254)
- Requirements (254)
- Fax via Windows Fax Services (Windows 7) (255)
- Configuration (255)
- Sending Fax from an Application (259)
- Fax via Windows Fax Services (Windows XP) (260)
- Configuration (260)
- Sending Fax from an Application (261)
- Viewing the Status of a Fax (264)
- Receiving and Viewing a Fax (264)
- Canceling a Fax Job (264)
- Automatically Send Retry (265)
- Automatically Canceling a Fax (265)
- eMail to Fax (266)
- Administrator Setup (266)
- Sending a Fax (267)
- Fax Activation (267)
- Sending a Fax through Fax Gadget (268)
- Fax Jobs (270)
Introduction

While most business interactions occur digitally, faxing still remains a required feature for many people. This is especially true when there are technical limitations or legal requirements involved. Rather than having to purchase a fax machine to handle this traffic, UC users can conveniently send faxes from their computer desktop digitally through the Officelinx 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 Officelinx. However, this method requires some advanced configuration.

  Refer to [Fax via Windows Fax Services (Windows 7)](page 255) or [Fax via Windows Fax Services (Windows XP)](page 260) 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 Officelinx 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 266](page 266) 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 268](page 268) 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 Officelinx DVD) or earlier for pdf, etc.). Ensure that this software is installed and working (run at least once) before attempting to send a fax using that format.

1. Launch the **Programs and Features** application within **Control Panel**.

   **Note:** Change your viewing style to icons to view the list of applications instead of categories.

2. Click on the **Turn Windows features on or off** link on the left-hand pane.
3. From the feature window, enable the following features.

**Print and Document Services**
- Internet Printing Client
- Windows Fax and Scan

Click **OK** when you’re done.

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

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

5. If you are asked to restart your computer, click **Restart Now** to reboot.

6. Once the computer has restarted, install iLink Pro Desktop. Refer to the **Client Applications Guide** for more information.

7. When iLink Pro Desktop has been installed, go to **Start > Programs** and launch **Windows Fax and Scan**.

8. Go to **Tools > Fax Settings...**
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 Officelinx server. Only enable this checkbox if you have a specific reason to do so.

Click **OK** to save your changes.

10. Open **Tools > Fax Accounts...**

11. Click the **Add...** button.

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

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

15. If you are prompted regarding your Firewall, click to **Allow access** at the bottom of the window.

Your computer is now ready to send fax messages.

**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.

A new window will open to define the destination and any other components required for the fax.

The document being sent as a fax will appear as an attachment.

Ensure that you enter the correct fax number on the **To:** field.

Set the **Dialing rule** to **UC Location**.

All other fields, such as **Cover Page**, **Subject** and **Body** are optional fields which you can utilize to customize your fax message.

When you are ready to send the fax, click the **Send** button.

The Fax status window will appear to notify you of the fax’s status. Once transmission has completed successfully, you will be notified here.

If the fax fails for any reason, the details will be shown here. Consult with your system administrator if you are having trouble sending faxes.

**Note:** You can track of all your outgoing faxes from the **Windows Fax and Scan** application available on the **Start** menu.
Fax via Windows Fax Services (Windows XP)

Configuration

Please follow the below steps to configure your client machine for use with Windows Fax services.

**Warning:** 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 Officelinx DVD) or earlier for pdf, etc.). Ensure that this software is installed and working (run at least once) before attempting to send a fax using that format.

1. Go to **Start > Settings > Control Panel**. Double-click **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. Enable **Fax Services**. Click **Next**.
4. Once the process is complete, you will have the ability to send faxes from your desktop.

**Note:** You may be asked to provide a Windows installation disc depending on the computer settings.
Sending Fax from an Application

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

4. The Send Fax Wizard screen appears:

5. Click Next. The Recipient Information screen appears:
6. Specify the following:
   - In the To field, enter the name of the intended recipient.
   - 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.

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

   **Note:** To create a new set of dialing rules, click on the Dialing rules button.
7. Click on the **Add** button to add the recipient whose information you have just specified.

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

8. Click **Next** when you have added all desired recipients. The **Preparing the Cover Page** screen appears:

9. From the **Cover page template** dropdown list, select the cover page template you want to use.

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

11. In the **Note** box, enter message text for the fax cover page.

12. Click **Next**. The **Schedule** screen appears:

13. Select one of the **When do you want to send this fax?** radio buttons:
   - **Now** - send the fax immediately
   - **When 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
15. Click **Next**. The following screen appears:
16. If you want to preview your fax, click on the **Preview Fax** button. Otherwise, click **Finish**.

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

1. Select **Start > All Programs > Accessories > Communications > Fax > Fax Console**.
2. In the left hand pane, click to expand Fax. The following list describes the folders under Fax:
   - The **Incoming** folder contains faxes that are currently being received.
   - The **Inbox** folder contains faxes that have been received.
   - The **Outbox** folder contains faxes that are scheduled to be sent.
   - The **Sent Items** folder contains faxes that have been successfully sent.
3. In the left hand pane, highlight a folder.
4. In the right hand pane right click on the fax you want and select **Properties**.
5. On the General tab, check the status of the fax under **Status**.

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

Receiving and Viewing a Fax

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

Canceling a Fax Job

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

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

You can set up Fax so that it continues trying to send your fax if the receiving fax machine is busy.

**Note:** Fax is automatically set up to retry three (3) times at 10-minute intervals.

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

Automatically Canceling a Fax

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

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

Sending a fax via email may be accomplished using virtually any email client. This feature 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 Officelinx 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 Officelinx server must be properly configured before users can send fax messages through an email client. **Send URL** must be configured and activated on the voice server (see the Security Enhancements chapter in Avaya's Server Configuration Guide). Also, SMTP port 25 needs to be opened on any firewall or security services.

An active email account and client are also required.

Under **Officelinx Admin>Configuration>VPIM/SMTP**, set **Use email verification for outbound faxing** to **True**.
Sending a Fax

**Note:** This guide will use Gmail to send the fax email. However, this process can be repeated with virtually any email client including web based email.

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 Officelinx DVD), DOC / DOCX need MS Office).

Send the email when you’re ready.

The message will be accepted by your server and processed into an outgoing fax job.

Fax Activation

To prevent spam, once you have clicked the **Send** button, the Officelinx Server will send you an email to confirm that the fax message is to be sent.

This email includes a link which you must click on to authorize the server to send the fax message. Click on the link.

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

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**.

The selected file will now be added as fax content.

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

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

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

**Outgoing**: This folder contains the details of all faxes that are currently being sent that have neither finished nor failed.

**Completed**: This folder contains the details of all faxes that have been successfully sent.

**Failed**: This folder contains the details of all faxes that could not be sent. The system has stopped trying to send the fax.

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

- **Number**: This field displays the job number assigned to the fax.
- **Sender**: This field displays the individual who sent the fax.
- **Destination**: This field displays the Mailbox number to which the fax is directed.
- **Status**: This field displays the current status of the fax (Initial / Pending / Sending / Sent / Canceled / Failed-Busy / Failed-No Answer / Failed-Other / Failed).
- **Created**: This field displays date and time the fax was sent.
- **Completed**: This field displays date and time the transmission of the fax was completed.
## In This Chapter:

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>272</td>
<td>Introduction</td>
</tr>
<tr>
<td>272</td>
<td>Visual Guide</td>
</tr>
<tr>
<td>273</td>
<td>Requirements</td>
</tr>
<tr>
<td>273</td>
<td>Specifications</td>
</tr>
<tr>
<td>274</td>
<td>Server Configuration</td>
</tr>
<tr>
<td>274</td>
<td>Licensing Information</td>
</tr>
<tr>
<td>275</td>
<td>Admin Settings</td>
</tr>
</tbody>
</table>
Introduction

Soft fax eliminates the need and the cost of a dedicated fax boards by emulating all the necessary fax protocols through software. Fax messages that are received by Officelinx server will be stored in the TIFF format allowing the fax messages to be accessible to all users regardless of the device that they are using. While Softfax is not designed to replace a fax centric ecosystem, it offers a convenient alternative to organization which requires occasional fax usage by eliminating the need for dedicated fax hardware.

Visual Guide

In a typical organization, users are either assigned individual fax machines or share a common fax machine depending on faxing requirements and policies of the organization. But if the users are not a heavy fax user, being tied to the machine can be a nuisance. From maintenance cost to actual usage, fax machines can easily become a burden to the organization as well.

Since it is difficult to eliminate fax usage completely, Officelinx offers a software solution to faxing, allowing users to both send and receive fax machines through the Officelinx server. Incoming faxes are converted into a TIFF file and can be sent to each individual user’s mailbox. Users can also send out digital documents as faxes to actual fax machines or emulators such as Officelinx.

Note: Other document formats can be used to send faxes if the server has been configured to use them. The other supported formats are PDF, DOC, DOCX, and TXT.
Requirements

The following are the minimum requirements for soft fax:

<table>
<thead>
<tr>
<th>Processor</th>
<th>P4 2.4GHz or higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Windows 2000 Server SP2 or higher</td>
</tr>
</tbody>
</table>

Specifications

Officelinx conforms to the following ITU-T specifications:

- **V.17** -- 2-wire modem for fax applications with data rates of 14.4, 12.0, 9.6, 7.2 kbits/s
- **V.29** -- Fax modem with data rates of 9.6 and 7.2 kbits/s
- **V.27ter** -- Fax modem with data rates of 4.8 and 2.4 kbits/s
- **V.21 channel 2** -- Used to transfer T.30 control frames
- **T.30** - procedures for document fax transmission in general switched telephone network

PC usage:

- **40 MHz of CPU** is used for every fax channel for send/receive functions
- **100 KB of RAM** is used to load the fax application on the startup of the 6510 UM
- **80 KB of RAM** is used for every fax channel that is actively sending or receiving faxes.

Note: Before configuring your system for softfax, it is necessary to determine that your fax board(s) are capable of exploiting this feature. The Dialogic JCT series of boards - JCT denoting the board as Full Duplex - can support softfax. IP configuration can support softfax.
Server Configuration

Licensing Information

Before you begin configuring your soft fax you should make sure that you have the required licenses.

**Fax Mail**: This is the core component to enable the fax services. SoftFaxPorts: The number of available ports for softfаксing. More can be purchased for sites with higher traffic volumes.

**Integrated Fax**: Enable to turn on outbound faxing.

**EFax Users**: Licenses only for outbound faxing.
Admin Settings

1. Ensure that you have soft fax ports purchased and available on the license.
2. Log in to the Admin Console.
3. Open Voice Server for your PBX. Make sure that the following settings are correct.
   **Number of Soft Fax Channels:** The number of soft fax ports that you are licensed for (if using a soft fax board type).
   **Fax Enabled:** Must be set to **True**.
   **Number of Fax Channels:** The number of fax channels you are licensed for.
   **Start Fax Channel Number:** Must be set to 1.
4. In the Value Data text field, enter the number of ports available on your license. Click **OK**.
5. Return to the Admin Console. Navigate to **Configuration > Fax Settings**:
   - In the right-hand pane, locate the **Dialing Suffix** parameter and double-click. An Edit String dialogue box appears. In the **Value Data** text field, enter 9. Click **OK**.
   - In the right-hand pane, locate the **Fax Board Type** parameter and double-click. An Edit String dialogue box appears. In the **Value Data** text field, enter **SoftFax**. Click **OK**.
   - In the right-hand pane, locate the **Fax Mail Installed** parameter and double-click. An Edit String dialogue box appears. In the **Value Data** text field, enter **True**. Click **OK**.
6. Return to the Admin Console. Navigate to **Configuration > Advanced**:
   - In the right-hand pane, locate the **Disable Fax Detection** parameter and double-click. An Edit String dialogue box appears. In the **Value Data** text field, enter **False**. Click **OK**.
   - In the right-hand pane, locate the **Disable Fax Detection1** parameter and double-click. An Edit String dialogue box appears. In the **Value Data** text field, enter **False**. Click **OK**.
   - In the right-hand pane, locate the **Disable Fax Detection2** parameter and double-click. An Edit String dialogue box appears. In the **Value Data** text field, enter **False**. Click **OK**.
7. Reboot the server to load the soft fax ports.
8. Following the reboot, UM Monitor will display - if fax ports have been properly loaded.


**Note:** If the fields mentioned above are not visible in **UM Monitor**, then the fax ports have not loaded properly. UM Monitor may be accessed from the system tray.
Confirmation of Service for IIS7

Due to the way in which IIS7 manages FTP services, you will have to perform extra configuration to ensure that your fax related services will be running. When you open Windows Services panel, you will see the **FTP Publishing Service** entry. Open the properties of this item as shown here. Set this service’s **Startup Type** to **Automatic** then restart your computer.

After the reboot, open your IIS panel and check for FTP services, you should see the Default FTP Site state set to **Running**. If this service is not running, the fax feature will not function properly.

Setting up mailboxes for soft fax

There are two alternatives available, the first involving a separate DID number for phone and fax, and the second involving an identical DID number for phone and fax. The case of a separate DID (Direct Inward Dialing) number is as follows:

1. In the Admin Console, navigate to **Company > Mailbox > Addresses**. Click on **Add** and select **Fax** from the menu. The Address dialogue box appears.
2. From the **Type** dropdown list, select **Fax - Internal Extension**.
3. In the **Number** text field, enter the four-digit DID number.
4. Select the **Set As Default** checkbox to designate that particular number as the default fax number.
5. Click **OK**.
6. Or, in the case of an identical DID number for phone and fax, the process is as follows:
   - **Either** perform the fax detection at the greeting level. On receiving the call/fax, the mailbox will, on receiving the fax tone, deposit the fax message directly into that mailbox.
   - Or the User may create a voice menu, giving the caller the option of delivering a fax. In this case, a voice menu must be attached to the mailbox, with the option **Send To Fax Start Tone** selected and **Send To Voicemail Record Tone** the default option. Consult the Server Configuration Guide chapter entitled "Maintaining A Voice Menu" for detailed instructions.

*Note: The **Number** field value cannot exist anywhere else in the system as a phone or fax extension.*
DIALOGIC SR140 FAX INTEGRATION

In This Chapter:

280 Introduction
280 SR140 vs Softfax
280 Pre-Requisites
281 Configuration
281 License Manager
286 Configuration Manager
289 Officelinx Configuration
290 Monitoring Channel Activity
Introduction

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

SR140 vs Softfax

This table provides a comparison between the SR140 and the Softfax applications.

<table>
<thead>
<tr>
<th></th>
<th>SR140</th>
<th>SOFTFAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Channels Supported</td>
<td>up to 60/node 1</td>
<td>up to 16/node 1</td>
</tr>
<tr>
<td>Support for Inbound Faxing</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Support for Outbound Faxing</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Can use T.38 protocol</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Internal Fax Transmission to Softfax</td>
<td>2</td>
<td>•</td>
</tr>
</tbody>
</table>

1 - Varies depending upon license.
2 - Internal Fax Transmission to Softfax allows items to be sent from the desktop and received by another user on the same system.

Mixed environments are also supported. For example, inbound faxing can be handled by Softfax, while outbound faxing is sent through the SR140.

Pre-Requisites

Install the Officelinx 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 Officelinx.

Install the SR140 fax software onto the computer according to the manufacturer's instructions.
Configuration

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

License Manager

1. Open the Brooktrout License Manager program.

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

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

4. Make sure that **Automatically** is selected as the **Activation Method**, then click **Next**.

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

6. Enter the SR140 license key number that came with the fax software package. Click **OK** when ready.
7. The new license key has been successfully added to the system. Click **Next**.

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

9. Enter the details of the site administrator. All fields are required for registration. Click **Next** when ready.
10. Enter all of the required information into the fields provided. This is the site where the software is installed. Click **Next** to continue.

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

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

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

![License Activation Wizard](image1)

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

![Brooktrout License Manager](image2)
Configuration Manager

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

![Start](image1)

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

![Configuration Tool - Preferences](image2)

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

![Brooktrout Configuration Tool - Wizard Mode](image3)
4. Enable the option for **SIP**. Click **OK** to continue.

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.

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**.
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.

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 Officelinx voice server (5060).

5. Click **Save** to confirm the changes.

6. Click **Apply** to restart all affected services.

The configuration of the SR140 software is complete.
Officelinx 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 OL Admin.

1. Go to Start > All Programs > Office-LinX > Office-LinX Admin, or click the OL Admin icon on the server desktop. Enter the username and password at the prompt.
2. Open Configuration and click on Fax Settings.

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

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

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

Setup

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

1. On the computer where Officelinx 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.

![Image showing Notepad with configuration file open](image)

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.
24

DIALOGIC SR140 SECURE FAX

In This Chapter:

292 Introduction
292 Pre-Requisites
293 Configuration
293 License Manager
298 Configuration Manager
313 Officelinx Configuration
Introduction

Officelinx 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 Officelinx 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 Officelinx.

For High Availability (HA) installations, the SR140 can be installed on the Master 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 Officelinx voice server are both operating, the fax software must be configured to communicate with the UC platform.

License Manager

1. Open the Brooktrout License Manager program.

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

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

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

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

6. Enter the SR140 **standard** license key number that came with the fax software package. Click **OK** when ready.
7. The new license key has been successfully added to the system. Click Add.

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

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

10. Click Next to continue to the Product Registration pages.
11. Enter the details of the site administrator. All fields are required for registration. Click **Next**.

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

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

   When it has finished, click **Next** to continue.
14. The new licenses have been activated on the system. Click **Next**.

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

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

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

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

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

3. When the Configuration Wizard starts, choose **Advanced Mode**.
4. Enable the stack option for SIP, then click OK to continue.

![Configure IP Stack](image)

**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](image)

**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 Officelinx 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 Officelinx voice server. For example: sr140@192.168.0.1:5061.

**Session Name:** Enter sr140 in this field.

When ready, click Show Advanced>>.
6. Specify the following for your site.

**IP Preference for SIP**: Select **IPv4 only** from the dropdown list.

**IPv4 Interface Port**: Enter the port used for faxing.

**IPv6 Interface Port**: Enter the port used for faxing.

**TCP Enable**: Set this to **TRUE**.

**Transport Protocol**: Choose **TLS** from the dropdown list.

**SIP over TLS Enable**: Set this to **TRUE**.

**SIP over TLS Port**: Enter the port used for faxing.

**Block UDP port**: Set this to **TRUE**.

**Block TCP port**: Set this to **TRUE**.

**Secure RTP Enable**: Set this to **TRUE**.

**FIPS Enable**: Set this to **FALSE**.
7. Go to the **T.38 Parameters** tab and specify the following for your site.

   **Fax Transport Protocol**: Select **G.711 pass-through only** from the dropdown list.

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

9. On the Avaya Officelinx voice server, go to the installation drive and locate the folder `\Program Files (x86)\Brooktrout\config`.
10. In the folder, open the SRTP.cfg file using a text editor such as NotePad. Remove the # (uncomment) at the start of the following lines, and verify their values are as shown.

```
 srtp_accept = true
 srtp_enforce = true
 srtp_crypto_suite = AES_CM_128_HMAC_SHA1_80
 srtcp_unencrypted_flag = true
```

Save the file when finished.

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

```
 sip_tls_method = : Leave this field at its default value.
 local_rsa_private_key_filename = : Enter the path to the location of your private key file.
 local_rsa_cert_filename = : Enter the path to the location of your server certificate file.
 ca_cert_number = : Put the number of the cert you are using here. Add as many as are required.
 ca_cert_filename = : Put the name of the certificate file you are using here. Add as many as are required.
 (optional) chain_cert_number = : Put the number of the cert you are using here. Add as many as are required. This is only required if you are using Intermediate certificates.
 (optional) chain_cert_filename = : Put the name of the certificate file you are using here. Add as many as are required. This is only required if you are using Intermediate certificates.
 client_cert_required = false
 allow_self_signed_certs = false
```

12. When finished, restart the UC BTFaxServer and the Dialogic Corporation Boston Host Service services on the computer, or reboot the server.
Avaya Aura Communication Manager Configuration

The certificate files must be copied to the AACM server.

1. Login to the AACM server using administrator credentials. Go to Administration > Server (Maintenance).

2. Go to Miscellaneous > Download Files. Enable the File(s) to download from the machine I’m using to connect to the server radio button.
3. Click **Choose File** and find the certificate file. Select the file and click **Open** to add it to the list. Repeat for each certificate file (CA, Intermediate, Server, etc.).

When finished, click the **Download** button to copy the files to the server.

4. In the left-hand column, select **Security > Trusted Certificates**. Click **Add** and attach each of the CA and Intermediate certificates downloaded in step 3.

5. In the left-hand column, click **Server/Application Certificates**. Click **Add** and attach the server certificate downloaded in step 3.

6. Close the **Communication Manager** console.
Avaya Aura System Manager Setup

1. Login to the System Manager using an administrator account. Under **Elements**, select **Communication Manager**.

2. Go to **Network > IP Codec Sets**.
3. **Add** / **Edit** an audio codec set.

   ![Codec Setting UI]

   **Audio Codec:** Set this to **G.711MU**.
   **Silence Suppression:** Choose **n**.
   **Frames Per Pkt:** Enter a value of **2**.
   **Media Encryption:** Select **1-srtp-aescm128-hmac80** from the dropdown list.

4. Go to **IP Network Regions** in the left-hand column. Click **New** to create an entry.
5. Enter an available **Network Region** qualifier (a number between 1-250), then click **Add**.

![Select device from Communication Manager List](image)

*Enter Qualifier: 100

6. Enter the following parameters.

![change ip-network-region 100](image)

**Name**: Enter a meaningful, human readable name.

**Codec Set**: Set this to the codec set number configured in step 3.

**UDP Port Min**: Enter **2048** here.

**UDP Port Max**: Enter **8001** here.

Click the **ENTER** button when finished.
7. Open **Node Names** in the left-hand column. Click **New**.

8. Select **IP** from the qualifier dropdown list, then click **Add**.
9. In a blank space on the page, name the node, then enter the **IP address** of the Avaya Officelinx voice server. When ready, click the **ENTER** button.

![Image of node names](image1.png)

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.

![Image of signaling group](image2.png)

- **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 Screen](image)

- **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](image)
13. Enter the values required.

**Grp No**: Enter the trunk group number configured in step 10.
**No. Del Dgts**: Usually, set this value to 0.
**Pattern Name**: Give the route pattern a human readable name.
**Numbering Format**: Select lev0-pvt from the dropdown list.

When ready, click the ENTER button.

14. Open **Automatic Alternate Routing Analysis** in the left-hand column. Click **New** and enter the hunt group number for your system. Or select an existing extension and choose **Edit**. Click **Add**.
15. Modify a Dialed String entry.

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total</th>
<th>Min</th>
<th>Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node</th>
<th>ANI</th>
<th>Head</th>
</tr>
</thead>
<tbody>
<tr>
<td>722</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>22</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2000</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2000</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2000</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2000</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2000</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2000</td>
<td>aar</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>12</td>
<td>lev0</td>
<td>n</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
Officelinx 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 OL Admin.

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

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

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

*Hint*: If faxes will only be received through the SR140 software, the Outbound Fax Board Type can be set to another value if required.
25

WEB ACCESS

In This Chapter:

316 Introduction
316 Getting Started
317 Logging In
317 Navigation
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 Officelinx 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

To launch Web Access, open a web browser and navigate to the corporate UC server site. Click the Web Access icon to start the program.

These links provide 3 authentication methods to access Web Access: UC requires your UC Server credentials, Google needs a Google account setup, and Windows will use your computer or network login details.

Note: This screen does not appear if you login without having logged out from a previous session.
Logging In

Refer to the Client Applications Guide, page 241, for complete details on the single sign-on requirements for 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 manage them. You also have complete access to manage your UC presence, location, schedule and contacts.

For more details on Web Access, please refer to Web Access on page 239 of the Client Applications Guide.
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.

3. Enter the security code in the space provided, Click Send a Request when ready.

4. The specified email address will receive a message with a link. Click on the link to enter the details of the new password.
5. Enter a new password in the spaces provided, then click **Reset Password**.

6. The account password will be changed to the new value.
Introduction

The Web UM Monitor is a suite of tools to watch the performance of the system for the purposes of troubleshooting.

Getting Started

1. To launch Web UM Monitor, open a web browser and navigate to the corporate UC server site. Click the UM Monitor icon to start the utility.

2. Enter the administrator username and password for the voice server.

3. From the dropdown menu, select the voice server you want to monitor.

4. Click Connect to begin monitoring the voice server.

**Hint:** When finished, click Disconnect to stop monitoring that voice server.
The Channels Tab

The Channels Tab is the starting point for the program. In this panel is displayed the current status of each channel working on the voice server.

Hint: To view only a range of channels, enter the starting channel number in the box and click Apply. Only the channels from there up to the last will be shown.
The View Status Tab

This pane shows the commands that are being sent and received through all of the voice server channels.

Select either **All channels** or a specific channel to monitor from the dropdown list. Use **Clear** to remove all status entries from the display. New status entries will begin to fill the screen. Enable **Stop scrolling** to freeze the window. New entries will continue to be added to the bottom of the list, but the pane will not move until you manually begin scrolling.
The View Trace Tab

The View Trace tab allows you to get a clearer idea of what each channel is doing.

Select either **All channels** or a specific channel to monitor from the dropdown list.

Use **Clear** to remove all status entries from the display. New status entries will begin to fill the screen.

Enable **Stop scrolling** to freeze the window. New entries will continue to be added to the bottom of the list, but the pane will not move until you manually begin scrolling.
Sending Commands

Use Send Commands to issue commands directly to the voice server. Enter the command into the space provided and click the Enter button.

You can also view all available commands and their format by clicking the link.

<table>
<thead>
<tr>
<th>Command list</th>
</tr>
</thead>
<tbody>
<tr>
<td>- MailboxNo xxx (xxx is the Mailbox No) — pop up the Mailbox ID, Company ID information</td>
</tr>
<tr>
<td>- MailboxID xxx (xxx is the MbxID) — pop up the Mailbox No, Company ID information</td>
</tr>
<tr>
<td>- Delete MwiTasks — Delete Message light tasks</td>
</tr>
<tr>
<td>- Flush log — Flush all voice server logs to the hard disk from cache.</td>
</tr>
<tr>
<td>- ReadParms — Read all the PBX, global parameters, menus, FeatureGroups from database into cache.</td>
</tr>
<tr>
<td>- ReadCompanies — Read All Companies from database into cache</td>
</tr>
<tr>
<td>- ReadFeatureGroups — Read All FeatureGroups from database into cache</td>
</tr>
<tr>
<td>- Drop xxx (xxx is channel number) — Drop the channel</td>
</tr>
<tr>
<td>- Stop xxx (xxx is channel number) — Disable the channel</td>
</tr>
<tr>
<td>- Start xxx (xxx is channel number) — Enable the channel</td>
</tr>
<tr>
<td>- LampOn xxx (xxx is mailbox no) — Turn on message light for the mailbox in company 1.</td>
</tr>
<tr>
<td>- 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.</td>
</tr>
<tr>
<td>- 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.</td>
</tr>
<tr>
<td>- 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.</td>
</tr>
<tr>
<td>- Clear SlowTasks — Clear performance counter for slowest Tasks.</td>
</tr>
<tr>
<td>- Clear SlowBgGround — Clear performance counter for slowest BackGround logic.</td>
</tr>
<tr>
<td>- Task — List all the tasks and the numeric number.</td>
</tr>
<tr>
<td>- Refresh — Turn On or Off message lights for all the mailboxes based on feature group settings and message count and type in the inbox.</td>
</tr>
</tbody>
</table>
Display License Details

This menu displays the details of the license for the selected voice server.

<table>
<thead>
<tr>
<th>License information</th>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial No</td>
<td>12345</td>
<td></td>
</tr>
<tr>
<td>Product ID</td>
<td>98765</td>
<td></td>
</tr>
<tr>
<td>PBXs</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Companies</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Languages</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Voice Ports</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Verification Ports</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Outfax Ports</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Softfax Ports</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Mailboxes</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>UM Users</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>UC Users</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>eFax Users</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Mobility Users</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>Web Clients</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ASR Languages</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Resilience Ports</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TSE Connections</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>FaxServer.Print Ser</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>FaxServer.Fax Desk</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ASR Provider</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ASR Names</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>ASR Ports</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>TTS Provider</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

TT5 Ports 2
PMS yes
Pulse no
LAP yes
IMAP yes
SMS yes
SIP yes
CTI Only no
SMTP/IMAP yes
Fax Mail yes
CTI Link yes
TAPI no
Mobility(WAPI) 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
INTEGRATION WITH AVAYA CPaaS

In This Chapter:

328 Introduction
329 Avaya CPaaS Configuration
332 Avaya Officelinx Voice Server Configuration
334 Avaya Officelinx User Configuration
335 One-to-one
335 Personal number
337 Direct number
339 Any-to-many
339 Mailbox
340 Keyword
342 Addressing SMS Messages
Introduction

Avaya CPaaS is a robust development platform — create what you need and integrate it seamlessly with Avaya Officelinx and go!

Integrating with an Officelinx 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 Officelinx mailbox.

Pre-requisites

- Officelinx 10.5 or later.
- An Internet connection.
- An Avaya CPaaS account and telephone number.
Avaya CPaaS Configuration

An account with Avaya Cloud 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 cloud.zang.io. Enter your Avaya Cloud account credentials and click Log In.

   ![Login Screen]

   If you do not already have one, you can create a new account now. Enter your email address in the space provided, click Yes, sign me up! and follow the prompts to create a new account.

2. New accounts are given a few dollars to get started. If necessary, click Add Funds and add cash to your account balance. Numbers typically cost from $1 to $3 / month, depending upon the country and if it is local or toll free.

   ![Dashboard Screen]
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.

5. Locate the number you want. For the number to work with Officelinx, 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. Numbers with gray 📨 icons do NOT have that feature available. When you have located a suitable number, click **Buy** to add the number to your account.
6. From the Avaya CPaaS Dashboard, record the **Account SID** and the **Auth Token** values.

Continue with the configuration of Avaya Officelinx.
Avaya Officelinx Voice Server Configuration

The configuration of Avaya Officelinx is done using the OL Admin program on the Voice Server. In a High Availability environment, the configuration is done on the Consolidated Server only.

1. On the Officelinx Voice Server, or the HA Consolidated Server, open OL Admin and login.

2. Go to Configuration > Advanced and scroll down to the SMS options.
3. Make the following configuration changes. For each entry, double-click the item and modify the details where necessary.

- **SMS Provider**: From the dropdown menu, select **Avaya Cloud**. 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 Officelinx 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 OL 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.

<table>
<thead>
<tr>
<th>METHOD</th>
<th>MODIFY MAILBOX</th>
<th>INI FILE ENTRY</th>
<th>SENDER ADDRESSING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal number</td>
<td>✅</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct number</td>
<td></td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Mailbox</td>
<td></td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td>Keyword</td>
<td></td>
<td></td>
<td>✅</td>
</tr>
</tbody>
</table>
One-to-one

Use one of these methods if each user has exclusive use of an Avaya CPaaS telephone number.

Personal number

Associating the number with the mailbox is done by modifying the user profile in OL Admin. No INI file entry or additional Sender Addressing is required.

1. In OL Admin, open the PBX and go to the Company menu. Select Mailbox Structure.
2. Double-click a user and open the **Addresses** tab.

3. Click **Add** and choose **SMS Phone**.

4. Enter the required information and click **OK** when ready.

- **Description**: Give this address a label.
- **Country**: From the dropdown menu, select the country that this number applies to.
- **Area/City Code**: Enter the city or area code for this number.
- **Number**: Enter the Avaya CPaaS telephone number here.
- **Set as Default**: This field should be disabled.
5. The new address has been added to the user. Click **Save**.

All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to this user’s mailbox.

**Direct number**

Associating the number with the mailbox is done through the INI file. No additional Sender Addressing or changes to the user profile are required.

1. Open a text editing software program such as Windows Notepad and create/modify the INI file.
2. Each person using **Direct number** must have an entry in the INI file, and each entry contains four elements.

```
[Application1]
Number= 1(905)707-9700
Mailbox= 9876
Company= 1

[Application2]
Number= 1(905)707-9170
Mailbox= 9877
Company= 1
```

- **[ApplicationX]**: This is an incrementing label, ApplicationX, where X is a unique identifier for each user (i.e. [Application1], [Application2], etc.). There are no spaces in this title, and it must be enclosed in square brackets.
- **Number=**: Specify the Avaya CPaaS telephone number for the recipient. This is where the sender addresses the message.

**Caution**: The number in an incoming message must match this value exactly or the message cannot be delivered.

- **Mailbox=**: Enter the mailbox for the recipient. The incoming SMS message will be delivered here.
- **Company=**: For sites that have multiple tenants/companies, enter the company number for this user here. This value must match the company numbers defined on the Avaya Officelinx 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 Officelinx Voice Server installation drive in the **UC/SMS** folder.

4. Stop and re-Start the **UC SMSConnector** service on the Voice Server, or reboot the server.
   This service should also be configured to start automatically.

---

**Note:** You can combine both **Direct number** and **Keyword** entries in the same INI file. Only the information in each entry will change.

```
[Keyword1]
Value= ASKJohnC,JohnC
Mailbox= 9876
Company= 1

[Application1]
Number= 1(905)707-9700
Mailbox= 9876
Company= 1
```

All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to the user’s mailbox defined in the INI file.
Any-to-many

Use one of these methods if your company has one or more Avaya CPaaS telephone numbers with many people using each one.

Mailbox

The sender must begin the message with ## followed by the mailbox number of the recipient. This mailbox must be followed by Space or Enter.

Associating the number with the mailbox is done explicitly by the sender within the body of the message. No INI file entry or changes to the user profile are required.

All incoming SMS messages sent to the Avaya CPaaS telephone number will be directed to the user’s mailbox 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.

   - **[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 a space or Enter.
   - **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 Officelinx Voice Server. In most cases, where there is only a single company configured, set this value to 1.

---

**Caution**: Keyword values **are case sensitive**. The keyword in an incoming message must match this value exactly or the message cannot be delivered.

---
3. Once all users have been added, save the file with the name:  **http2smsconnector.ini**  
   Save it on the Officelinx Voice Server installation drive in the **UC/SMS** folder.

4. Stop and re-Start the **UC SMSConnector** service on the Voice Server, or reboot the server.  
   This service should also be configured to start automatically.

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 Officelinx configured to use it, messages sent to that number will be received in the recipient's inbox.

Contacts wishing to send a message to the user address it to the Avaya CPaaS telephone number. Additional addressing by the sender may be required.

Personal number

The sender only needs to provide the number (e.g. 442030026798) to address the message.

The Voice Server spots the telephone number and uses the OL Admin Addresses tab to direct the message to the correct mailbox.
Direct number

Enter the recipient’s Avaya CPaaS telephone number (e.g. 1(905)707-9700) exactly as it is configured in the INI file.

The Voice Server spots the telephone number and uses the INI file to direct the message to the correct mailbox.
Mailbox

The sender must include the recipient’s mailbox number in the body of the message. The number must be preceded by `##` (e.g. `##9876`).

The `##` marker tells the server that the number that follows is the extension of the recipient and the message is delivered accordingly.
Keyword

The sender must include the keyword exactly as it is configured for that user in the INI file (e.g. **ASKJohnC**). The keyword is case sensitive.

![Example of a mobile phone with a text message]

The Voice Server spots the keyword and uses the INI file to direct the message to the correct mailbox.
In This Chapter:

348  Introduction

348  Creating an Account with OnEsna

349  Logging In Through OnEsna
Introduction

Logging in to an application using **Avaya credentials** provides a web-based authentication solution (**OnEsna**) for sites where Gmail and Salesforce are not available. Creating a user account with OnEsna allows access to a range of programs using secure access protocols.

Creating an Account with OnEsna

Before attempting to login using Avaya credentials for the first time, it is necessary to create an account at OnEsna.

1. Open a browser and go to [https://www.OnEsna.com](https://www.OnEsna.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 OnEsna. Re-enter the password to confirm.

   When finished, click **Sign Up**.

4. A confirmation email will be sent to the address provided.

   Open the message and click **Verify Email**.

5. OnEsna account setup is complete. Click **Login**.
Logging In Through OnEsna

**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 OnEsna username and password. Click Login.

**Note:** Enable Keep me logged in to have OnEsna 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.

3. If prompted to grant iLink permissions, click Accept.

**Note:** This only needs to be done the first time you login to the client.
4. The 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.
Introduction

Avaya Officelinx provides greater accessibility to people with special needs. Officelinx 10.7 and later offer 508 compliance and TTY integration.

508 Compliance

Complying with the 508 standard in Officelinx 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:

<table>
<thead>
<tr>
<th>KEYSTROKE</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAB</td>
<td>Skip to next item.</td>
</tr>
<tr>
<td>SHIFT + TAB</td>
<td>Return to the previous item.</td>
</tr>
<tr>
<td>ENTER or SPACE</td>
<td>Enable or Select the current item.</td>
</tr>
<tr>
<td></td>
<td>Expand / Collapse menus.</td>
</tr>
<tr>
<td></td>
<td>Scroll Up and Down within a menu. Toggle the current radio button.</td>
</tr>
</tbody>
</table>
The login, splash screen and Web Access interface are all 508 compliant.
TTY Integration

Avaya Officelinx includes support for TTY devices on your corporate voicemail system. TTY compatibility is provided through a language pack which can be downloaded from www.onesna.com. Go to Manage Downloads and select Officelinx 10.7 Language Packs. On the Versions tab, select TTY English and download the file to your hard drive.

Install the language pack according to the instructions found in the Server Installation Guide under Language Pack Installation on page 581.

Once the language pack for TTY English has been installed, it can be chosen as the default language for your company and for each user's mailbox.

Hint: It is recommended that a separate telephone number be used for the company for TTY language prompts. This prevents TTY callers from getting no response on their device from a voice enabled system, and hearing callers receiving unintelligible signals on their handset from the TTY service.
Voice Recordings and TTY

The TTY system automatically converts system prompts into signals compatible with TTY devices. However, voice recordings made on-site cannot be converted.

To build greetings that appear on TTY devices, the greeting must be typed into a software program that converts the text into a TTY compatible audio format, which is then saved as a WAV file. These audio files can then be uploaded into Officelinx 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 Officelinx Web Access is preferred.
## APPENDIX A: REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Sept., 2018</td>
<td>10.7 (2)</td>
<td>Updated instructions for O365 and AWS integration (added “Grant permissions”).</td>
</tr>
<tr>
<td>22 Nov., 2018</td>
<td>10.7 (3)</td>
<td>Updated with new Avaya branding.</td>
</tr>
<tr>
<td>4 March, 2019</td>
<td>10.7.0.1 (4)</td>
<td>SP 1 Initial Release. OL now supports VMWare 6.7. Scalability to 80000 users. Integration with Avaya S8300E. Added Group Mailboxes.</td>
</tr>
<tr>
<td>8 April, 2019</td>
<td>10.7.0.1 (5)</td>
<td>Modified the chapter for Office 365 integration using EWS.</td>
</tr>
<tr>
<td>27 June, 2019</td>
<td>10.7.0.1 (6)</td>
<td>Corrected a setup issue / URL with Mutare.</td>
</tr>
</tbody>
</table>