Avaya Officelinx
Server Installation Guide

The Server Installation Guide is designed to be used as a reference when deploying Avaya Officelinx at a given site. While the settings and configuration of each site differs, the way in which Officelinx is installed at each site is very similar. For example, no matter which type of integration a site is using (e.g. SIP, SMDI, etc.) with their PBX, Officelinx installer is designed to be as consistent as possible to allow technicians to easily deploy & configure each site. Other than the specific integration related settings or site specific settings (e.g. PBX and voice server’s IP addresses, extension numbers, etc.), the installation experience will largely remain identical from deployment to deployment.

As a final note, please keep in mind that the procedures shown in this guide are not always meant to be followed literally. This guide will often use IP addresses, user names or other values which will vary from site to site. Using the values which are shown on this guide as an example can easily be a cause for improper integration.
© 2018-2019, Avaya Inc.
All Rights Reserved.

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

Documentation disclaimer
“Documentation” means information published in varying 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
SERVER INSTALLATION GUIDE

## Table of Contents

19  AVAYA OFFICELINX INSTALLATION SUMMARY
19  MINIMUM HARDWARE SPECIFICATIONS
19  CONSIDERATIONS:
20  SUPPORTED OPERATING SYSTEMS
21  STANDARD INSTALLATION SUMMARY
22  MAXIMUM SYSTEM CAPACITY

23  INSTALLATION CHECKLIST
23  OVERVIEW
23  VALIDATION CHECKS
23   Inbound Calls
24   Transfer Calls

25  DOWNLOADING AVAYA OFFICELINX
25  INTRODUCTION
25  DOWNLOADING FROM ACCOUNTS.ZANG.IO

29  WINDOWS SERVER 2016 INSTALLATION (SIP)
30  INTRODUCTION
31  INSTALLATION PREPARATION
31   Deployment Configuration Considerations
31   Antivirus Applications
31   Required Server Components
31   Digital Certificates
32  SERVER ROLES AND FEATURES
41   Disabling User Account Control Notification
44   IIS Certificates
44   IIS Certificate Bindings
113 INSTALLATION PREPARATION
113 Deployment Configuration Considerations
113 Antivirus Applications
113 Required Server Components
113 Digital Certificates

114 SERVER MANAGER CONFIGURATION
123 Installing Microsoft .NET Framework 4.6
124 Disabling User Access Control Notification
125 IIS Certificates
125 IIS Certificate Bindings
128 Installation

137 WINDOWS 7 INSTALLATION (SIP)

138 INTRODUCTION
138 Requirements

139 INSTALLATION PREPARATION
139 Deployment Configuration Considerations
139 Antivirus Applications
139 Required Components
139 Digital Certificates
140 Installing Windows Components
143 Disabling User Access Control Notification
143 Installing Microsoft .NET Framework 4.6
144 IIS Certificates
144 IIS Certificate Bindings
147 Installation

157 HIGH AVAILABILITY INSTALLATION

158 INTRODUCTION
158 Requirements

159 PREPARING THE SERVERS
159 Antivirus, Firewall and Automatic Updates
159 Disabling User Access Control Notification
159 32-bit Windows:
160 64-bit Windows:
160 Required Server Components

161 SERVER MANAGER CONFIGURATION (ALL SERVERS)
170 Installing Microsoft .NET Framework 4.6

171 IIS CERTIFICATES (ALL SERVERS)
305 INTRODUCTION

305 INSTALLING THE OFFICELINX LICENSE

307 LICENSING
307 Soft License
307 Initial Installation
307 Normal Operation
307 License Upgrades
308 License Expiration
308 Offline Verification
308 High Availability Licensing
308 Demo Mode
309 License Expiration Milestones
309 Licensing Grace Periods and Actions

309 CHANGING TO WEBLM LICENSING

311 SECURING OFFICELINX COMMUNICATIONS USING TLS

311 INTRODUCTION

311 ARCHITECTURE

312 CONFIGURING TLS WITH OFFICELINX FOR SIP
313 Key

315 INSTALL AND CONFIGURE CLOUD GATEWAY

316 INTRODUCTION

316 PRE-REQUISITES
316 Windows Configuration

317 INSTALLATION

324 CONFIGURING OFFICELINX

327 AVAYA OFFICELINX 7.X TO 10.7 UPGRADE

328 SINGLE SERVER

328 PREPARATION
328 Backup
328 Avaya Officelinx Installation
328 Stop Officelinx Processes

329 UPDATING THE DATABASE TO 7.1
VIRTUAL ENVIRONMENT DEPLOYMENT EXAMPLE

CPU Usage
Datastore Latency
Disk Usage Rate
Network Usage Rate

CONCLUSION

VIRTUALIZED ENVIRONMENT: MICROSOFT HYPER-V

INTRODUCTION
Requirements
Virtual Environment Limitations

ADDING HYPER-V TO THE HOST
Host Operating System
Guest Operating System
Adding the Hyper-V Role

CREATING THE GUEST ENVIRONMENT ON THE HOST

HYPER-V SERVER 2012

AMAZON WEB SERVICES

INTRODUCTION

PRE-REQUISITES
Important Note
When using Esna licensing:
When using WebLM licensing:

INSTALLATION

CONFIGURE MULTIPLE PBX ON THE SAME SYSTEM

INTRODUCTION

ADDING THE NEW PBX
Using Independent Channel Pools
Using Channel Port Pools

ROUTING THROUGH THE PBX
Configuring a Mailbox
Configuring an Organizational Unit
Configuring a Company
Minimum Hardware Specifications

Specifications for server hardware vary considerably depending upon the environment and the anticipated traffic capacity. For detailed server specifications, please refer to Avaya’s Technical Operating Guidelines.

A client workstation should meet the following minimum hardware specifications:

- Multimedia PC (sound card + speakers for multimedia playback)
- Pentium 4 processor (2.0 GHz)
- 512 MB of RAM

>Note: These specifications should be adjusted accordingly depending on other applications that may be running alongside end user Officelinx applications.

In addition to these specifications the client workstations must also be running the following software applications:

- For Web Access: Internet Explorer 6.0+ or Mozilla Firefox 3.0+ or Apple Safari 4.0+ or Google Chrome 3.0+
- A media player that can play GSM-compatible WAV files or MP3
- Outlook 2002 or greater (for Outlook Plug-in only)

>Caution: It is strongly recommended that, for Windows Server 2008, 2012 and 2016 the operating system drive has a minimum of 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Officelinx voice server installation.

Considerations:

Officelinx uses a dedicated server to enable high performance operation of the program. Other applications running on the same server as Officelinx can severely reduce the capacity of the voice server. Processing voice, messaging, presence and telephony data requires a dedicated system if it is to operate quickly and efficiently.

Some pre-requisites and considerations for installing Officelinx:

- Email clients must be setup and operating according to specifications.
- Create all accounts on any cloud-based software where necessary (i.e. Google Apps).
- The corporate telephone system and PBX must be installed and functioning properly.
- The computer that will host Officelinx must have its operating system installed, patched and completely updated. There must also be a functioning connection to the corporate network and to the Internet.
- What impact will the addition of the voice server have on existing network traffic loads?
- What additional software drivers will be required? (i.e. MS Word)
Supported Operating Systems

Officelinx can be installed on any of the following Windows based operating systems.

- Windows Server 2008 (32-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 or 2012 R2 - Standard Edition
- Windows Server 2016

**Note:** Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Caution:** The MAC operating system is **NOT** supported for server installations.
Standard Installation Summary

This table summarizes the steps needed to setup an Officelinx Unified Communications System at your site. Please refer to the listed documentation for more detailed information about each step. The installation proceeds from the top of the table downward. All documents are available from Avaya except for the PBX Documents which should be available from your dealer.

<table>
<thead>
<tr>
<th>System</th>
<th>Operation</th>
<th>Detailed Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBX</td>
<td>Install, configure and connect for normal operation.</td>
<td>PBX Branded Documentation</td>
</tr>
<tr>
<td></td>
<td>Install Windows Features</td>
<td>Server Install Guide</td>
</tr>
<tr>
<td></td>
<td>Add certificates to the O/S.</td>
<td>Consult your certificate provider</td>
</tr>
<tr>
<td></td>
<td>Install Officelinx</td>
<td>Server Install Guide</td>
</tr>
<tr>
<td></td>
<td>Configure company and users under Officelinx.</td>
<td>Server Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Record company telephone greetings.</td>
<td>Server Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Add any optional modules to Officelinx.</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td>Integrate Officelinx with the switch.</td>
<td>Officelinx integration documents</td>
</tr>
<tr>
<td>Desktop Workstation (optional)</td>
<td>Install the iLink Pro Desktop Client.*</td>
<td>Client Application Guide Ch4</td>
</tr>
<tr>
<td>Devices (optional)</td>
<td>Navigate to the device store, download and install the mobile client.</td>
<td>Client Application Guide Ch10ff</td>
</tr>
</tbody>
</table>

* The iLink Pro Desktop Client software can be found in the Officelinx installation directory.
  
  .../UC/WebClient/Download/UCClientManager.exe (for Windows)
  
  .../UC/WebClient/Download/UCClientManager.dmg (for Apple OS)
It can also be downloaded from the corporate UC Server site:
go to user.yourcompany.com, select Software Downloads, then click on the iLink Pro Desktop link.

Maximum System Capacity

<table>
<thead>
<tr>
<th>Feature</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Directory</td>
<td>60,000 entries</td>
</tr>
<tr>
<td>Voice Mailboxes</td>
<td>60,000 - on Distributed Server</td>
</tr>
<tr>
<td></td>
<td>20,000 - on Standalone Server</td>
</tr>
<tr>
<td>Unified Messaging Users</td>
<td>20,000 - on Distributed Server</td>
</tr>
<tr>
<td></td>
<td>1,000 - on Standalone Server</td>
</tr>
<tr>
<td>Voice Channels</td>
<td>48 ports - SIP with Iwatsu ECS</td>
</tr>
<tr>
<td></td>
<td>120 ports - SIP integration, per voice server</td>
</tr>
<tr>
<td></td>
<td>2000 ports - High Availability Environment</td>
</tr>
<tr>
<td>Text to Speech Ports</td>
<td>64 ports</td>
</tr>
<tr>
<td>Automatic Speech Recognition</td>
<td>64 ports</td>
</tr>
<tr>
<td>Extension Dialing</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Number of Tenants</td>
<td>999</td>
</tr>
</tbody>
</table>

For more detailed information, please refer to Avaya's Technical Operating Guidelines.

**Note:** Depending on the level of functionality desired, the appropriate license has to be purchased. Purchase of Officelinx itself is insufficient.
## Overview

This chapter provides a check-list to employ when validating the success of any installation/integration of the Officelinx System. It is recommended that you go through each scenario listed on these tables and verify the performance of all features. Carefully read through the notes for each test to make sure that you understand its purpose, process and expected results.

## Validation Checks

### Inbound Calls

<table>
<thead>
<tr>
<th>Test #</th>
<th>Description</th>
<th>Notes</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Direct call to hunt group.</td>
<td>The calling party number is expected to be contained in the From header of the Invite.</td>
<td>Y / N</td>
</tr>
<tr>
<td>2</td>
<td>Internal ring-no-answer forward.</td>
<td>The called party will be shown in the Diversion header of the invite. The calling party will be contained in the From header. The reason in the diversion header is shown as <strong>no-answer</strong>.</td>
<td>Y / N</td>
</tr>
<tr>
<td>3</td>
<td>External ring-no-answer forward.</td>
<td>The called party will be shown in the Diversion header of the invite. The calling party (if available) will be contained in the From header. The reason in the diversion header is shown as <strong>no-answer</strong>.</td>
<td>Y / N</td>
</tr>
<tr>
<td>4</td>
<td>Internal busy forward from a subscriber's station set.</td>
<td>The called party will be shown in the Diversion header of the invite. The calling party will be contained in the From header. The reason in the diversion header is shown as <strong>busy</strong>.</td>
<td>Y / N</td>
</tr>
<tr>
<td>5</td>
<td>External busy forward from a subscriber's station set.</td>
<td>The called party will be shown in the Diversion header of the invite. The calling party will be contained in the From header. The reason in the diversion header is shown as <strong>busy</strong>.</td>
<td>Y / N</td>
</tr>
<tr>
<td>6</td>
<td>Internal all call forward from a subscriber's station set.</td>
<td>The called party will be shown in the Diversion header of the invite. The calling party will be contained in the From header. The reason in the diversion header is shown as <strong>fwd-all</strong>.</td>
<td>Y / N</td>
</tr>
<tr>
<td>7</td>
<td>External all call forward from a subscriber's station set.</td>
<td>The called party will be shown in the Diversion header of the invite. The calling party will be contained in the From header. The reason in the diversion header is shown as <strong>fwd-all</strong>.</td>
<td>Y / N</td>
</tr>
</tbody>
</table>
## Transfer Calls

<table>
<thead>
<tr>
<th>Test #</th>
<th>Description</th>
<th>Notes</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Blind transfer to a station from messaging server where the destination answers the call.</td>
<td>The transfer is completed once the destination is judged as connected. Depending upon the speed that the destination is answered the caller and called parties may be connected together with a slight bit of the called parties voice clipped.</td>
<td>Y / N</td>
</tr>
<tr>
<td>9</td>
<td>Blind transfer to a station from messaging server where the destination does not answer the call.</td>
<td>If the station is configured to forward back to the gateway then the call will arrive as a forwarded call with the called party being the transfer destination, but the calling party may be the gateway port performing the transfer, depending on how quickly the transfer to the destination can be completed.</td>
<td>Y / N</td>
</tr>
<tr>
<td>10</td>
<td>Blind transfer to a subscriber's station from messaging server where the destination is busy.</td>
<td>The transfer should fail.</td>
<td>Y / N</td>
</tr>
<tr>
<td>11</td>
<td>Blind transfer to an invalid number.</td>
<td>The transfer should fail.</td>
<td>Y / N</td>
</tr>
<tr>
<td>12</td>
<td>Supervised transfer to a subscriber's station from messaging server where the user does not answer the call.</td>
<td>The transfer completion speed and timing is up to the application. The application should decide to either complete the transfer and let the station's forwarding carry it back to the gateway, or abort it before the forwarding.</td>
<td>Y / N</td>
</tr>
<tr>
<td>13</td>
<td>Supervised transfer to a subscriber's station from messaging server where the destination is busy.</td>
<td>The transfer completion speed and timing is up to the application.</td>
<td>Y / N</td>
</tr>
<tr>
<td>14</td>
<td>Supervised transfer to a subscriber's station from messaging server where the user answers the call.</td>
<td>The transfer completion speed and timing is up to the application. The application should decide to either complete the transfer and let the station's forwarding carry it back to the gateway, or abort it before the forwarding.</td>
<td>Y / N</td>
</tr>
<tr>
<td>15</td>
<td>Supervised transfer to an invalid number.</td>
<td>The transfer completion speed and timing is up to the application.</td>
<td>Y / N</td>
</tr>
<tr>
<td>16</td>
<td>Outbound call to a subscriber's station that answers.</td>
<td>The call is flagged to the application as completed when the gateway can determine that the call has been connected. The application should take this into account when making the decision about when to start the audio stream.</td>
<td>Y / N</td>
</tr>
<tr>
<td>17</td>
<td>Outbound call to a subscriber's station that does not answer.</td>
<td>The application needs to take into account if the destination has been set to forward back to the gateway for a ring no answer condition, and judge accordingly when to either stop waiting for an answer and cancel the call, or know that it will end up arriving back at the gateway as a forwarded call.</td>
<td>Y / N</td>
</tr>
<tr>
<td>18</td>
<td>Outbound call to a subscriber's station that is busy.</td>
<td>The application needs to take into account if the destination has been set to forward back to the gateway for a ring no answer condition, and judge accordingly when to either cancel the call, or know that it will end up arriving back at the gateway as a forwarded call.</td>
<td>Y / N</td>
</tr>
<tr>
<td>19</td>
<td>Outbound call to an external number.</td>
<td>Depending on the state of the destination, the call will either be judged as connected, or fail due to busy / error tone conditions.</td>
<td>Y / N</td>
</tr>
</tbody>
</table>
DOWNLOADING AVAYA OFFICELINX

Introduction

Avaya Officelinx can be downloaded from accounts.zang.io or through the Avaya PLDS portal. The same downloaded file can be used to install any version of the program including Single Server, High Availability (Master, Secondary, Consolidated), Cloud Gateway, etc.

Download and save the file to a computer hard drive. It is a single, self-extracting executable file. Copy the file to the destination computer(s) and double-click to extract all of the installation files to the local hard drive.

Run the Setup.exe file to launch the installer.

Downloading from accounts.zang.io

Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that Windows Firewall is disabled, and that Windows Automatic Update is turned off.

1. Open a web browser and go to https://accounts.zang.io. Create a new account (Get Started), or login using your existing credentials. You can also login using your Google+, Salesforce, or Office 365 account details.
2. On the Dashboard, select Edit Profile.

3. From the Downloads tab, choose the version of Officelinx you want to download. Click the download icon beside the program.
4. Specify the location on your computer hard drive where you want to save the file.

The saved file is a self-extracting executable (.exe) file. Copy the file to any and all servers where Avaya Officelinx will be installed.
Continue with the chapter appropriate for your operating system (i.e. Windows 2016) or feature set (i.e. JITC).
In This Chapter:

30 Introduction
31 Installation Preparation
32 Server Roles and Features
41 Disabling User Account Control Notification
44 IIS Certificates
47 Installation
Introduction

When installing Avaya Officelinx version 10.7, almost all choices regarding program configuration are asked at the beginning so that the many components can be installed without interruption. The only variation that occurs after the initial selection is the PBX and integration type, which will be unique to most sites.

**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.

### Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>A Full License for 10.7.</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
</tbody>
</table>

**Note:** Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Note:** Avaya Officelinx should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.

**Caution:** It is strongly recommended that, for Windows Server 2016, the operating system drive has a minimum of 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Officelinx voice server installation.
Installation Preparation

Deployment Configuration Considerations

- An Avaya Officelinx server may be installed on the root drive (the same drive where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- An Officelinx server may be installed on a secondary drive (on a different drive from where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- The drives may each be a physical drive (for best performance), or a single drive with partitions.
- The folders \uc\logs, \uc\DB, and \uc\messages may be mounted to a local drive. Network or mapped drives are not supported.
- In an ESX(i)/VMWare environment, SAN/iSCSI is supported, but only at the ESX(i) level. The iSCSI target must be mounted and managed by the ESX(i) host. If a virtual machine is to have a C drive and a D drive, they must be added as a virtual hard disk using the VMWare client.
- The rules for drive types and options are the same for virtual machine environments. The storage must be local, Direct Attached Storage or SAN.

Warning: These configurations have been tested and approved by Avaya for use with Officelinx. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Required Server Components

For Microsoft Windows Server 2016, you must ensure that all the necessary server roles and features are installed on the system before proceeding with Officelinx installation.

Digital Certificates

Avaya Officelinx requires that signed digital certificates be installed on the voice server before attempting an installation. Certificates are used to create secure connections between the voice server and the client. The client uses the certificate to authenticate the signature stored on the server while negotiating a secure connection.

Digital certificates can be purchased from any trusted Certificate Authority (CA), such as GoDaddy™ and Symantec™. It is also possible to create a self-signed certificate for use with the program.
Server Roles and Features

1. From the **Server Manager Dashboard**, click **Add roles and features**.

   ![Server Manager Dashboard](image1.png)

   If this screen is hidden, go to **View** and select **Show Welcome Tile**.

2. Click **Next**.

   ![Add Roles and Features Wizard](image2.png)
3. Leave the default settings as they are. Click **Next**.

4. Leave the default settings as they are. Click **Next**.
5. Enable **Fax Server**. When prompted, select **Add Features**.

6. Enable **Web Server (IIS)**. When prompted, select **Add Features**. Click **Next**.
7. On the **Features** panel, open **.NET Framework 3.5 Features** and enable **HTTP Activation**. When prompted, select **Add Features**.

8. On the **Fax Server** screen, click **Next**.
9. On the **Print and Document Services** screen, click **Next**.

10. No changes are required here. Click **Next**.
11. On the **Web Server Role (IIS)** screen, click **Next**.

12. Under **Web Server > Common HTTP Features**, enable **HTTP Redirection**.


Under **FTP Server**, enable **FTP Service**.

Click **Next** when ready.

16. Review the selections here. When ready to proceed, click **Install**.
17. Windows will now start the installation process for the chosen items. This process may take a while.

![Add Roles and Features Wizard](image.png)

**Note:** This window can be closed without interrupting the installation procedure.

18. Once all changes are complete, **Restart the server**.
Disabling User Account Control Notification

1. Open the Windows Control Panel and select User Accounts.

   Again, click User Accounts.

2. Select Change User Account Control settings.

3. Click and drag the slider down to Never Notify.

   Click OK and Close.
4. On the keyboard, click the **Start button**, and select **Windows Administrative Tools**.

5. Double-click **Local Security Policy**.

7. Select **Disabled**. Click **OK**.

8. Restart the computer to make the changes active.

**Note**: UAC Notifications can be restored after Officelinx has been installed.
IIS Certificates

The site administrator must install either a self-signed certificate, or a certificate purchased from a Certification Authority. It is **not** necessary to install both types of certificate.

**Note:** Corporate security protocols may require the use of certificates purchased from an appropriate authority. High-security (JITC) installations always require a CA issued certificate for the Encrypted File System (EFS).

Additional information on installing certificates onto the voice server can be found here:


Once the certificates have been installed, continue with **IIS Certificate Bindings**.

IIS Certificate Bindings

To enable an HTTPS connection, a certificate has to be installed on the voice server. The HTTPS protocol must be enabled, and HTTP disabled.

1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.
2. Right-click in the right-hand pane and choose Import from the pop-up menu.

3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.

4. Go to **Sites > Default Web Site**. Click **Bindings...**
5. Add the HTTPS binding type. Set the **IP Address** to **All Unassigned**. Leave Port at its default. Change **SSL Certificate** to the certificate name installed above. Click **OK**.

6. Remove HTTP from the list of bindings. Click **Close**.
Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

**Note:** If the user who will be installing Avaya Officelinx has not logged in as the system administrator, that user must be given full rights to the root of the C drive.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe as administrator** to install Avaya Officelinx onto your voice server.

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically add the necessary packages if they do not already exist on the system. These packages may include **Sentinel Protection**, and **Microsoft Visual C++ Redistributable**. This process may take a while depending on the missing components.

**Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx. They can also be downloaded from resources.zag.io in both PDF and HTML format.
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

Click **OK** after entering the credentials.

5. Review the license agreements and enable **I accept the license agreement**.

Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.

**Note:** It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Single UC Server**.

Click **Next**.

**Single UC Server:** When operating Officelinx on a single voice server computer.

**Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select the license type you will using for this installation. Most sites will use the WebLM License option.

Note: If you select Officelinx, go to chapter 12, Installing the Officelinx License. When finished, return here and continue the installation from step 11. Skip step 9 through 10.

Warning: It is essential that the system/PC clock be properly set before activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

9. The License Upgrade Utility program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

Enter the address in the space provided, then click OK.

Important: This step requires that the Web License Manager has been installed and configured on the license server computer. See Installing the WebLM License and Server on page 297.
10. The utility will retrieve your license details from the server and display them here. Review the license details and click Exit when ready.

11. Select the Components required at your site. Disable any components that are not needed.

   Click Next.

   **Note:** If the Dialogic SR140 fax software will be used with this installation, ensure that the Hardware Fax Driver option is enabled here.

12. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

   **Note:** This screen will only appear if one or more required components are not installed on the computer.

   For all items that are not checked, return to Windows and add any missing pieces to the operating system.

   Click Next when finished or to refresh the display.

   **Note:** The installation will not continue until all of the required components have been added to Windows. This screen does not refresh until you click Next.
13. This screen shows the IIS settings that Officelinx requires to operate.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.

14. Select your PBX Brand then click **Next**.

15. Select your PBX model from the dropdown menu.

Click **Next**.

16. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.

When ready, click **Next**.
17. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

**Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

18. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya Officelinx.

**Hint:** The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

20. The preliminary information required for installation is now complete.

Click **Next**.
21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the **Automatic Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site’s PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration if necessary.

   Click **Next** to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.
26. Confirm the information then click **Finish**.

**Note**: Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the SIP Configuration Tool in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. At the OAI Configuration Wizard screen:
   - Enable **Direct TCP/IP**.
   - **Set Number of Nodes** = 1.
   - Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.

   Click **Next**.

28. On the Link Information page, enter the **IP Address** of the PBX. Leave **Port** at its default setting (4000). Leave the **Login Password** field blank.

   Click **Next**.

29. At the **Dialog** screen, from the lists on the left-hand side, choose the desired **Stations** (extensions and voicemail ports), **Hunt Groups** and **Trunks** to use with OAI.

   Select an item on the left, then click **Add** to move it into the right-hand pane.

30. Click **Save** to finish the OAI setup and continue with the Officelinx installation.
31. Click **Finish** to restart the server.

If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

The Officelinx installation is complete.
In This Chapter:

58 Introduction

59 Installation Preparation

59 Deployment Configuration Considerations

59 Antivirus Applications

59 Required Server Components

69 Disabling User Account Control Notification

75 Installation

75 User Rights
Introduction

When installing Avaya Officelinx version 10.7, almost all choices regarding program configuration are asked at the beginning so that the many components can be installed without interruption. The only variation that occurs after the initial selection is the PBX and integration type, which will be unique to most sites.

**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.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>A Full License for 10.7.</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
</tbody>
</table>

**Note**: Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Note**: Avaya Officelinx should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.

**Caution**: It is strongly recommended that, for Windows Server 2012, the operating system drive has a minimum of 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Officelinx voice server installation.
Installation Preparation

Deployment Configuration Considerations

- An Avaya Officelinx server may be installed on the root drive (the same drive where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- An Officelinx server may be installed on a secondary drive (on a different drive from where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- The drives may each be a physical drive (for best performance), or a single drive with partitions.
- The folders \uc\logs, \uc\DB, and \uc\messages may be mounted to a local drive. Network or mapped drives are not supported.
- In an ESX(i)/VMWare environment, SAN/iSCSI is supported, but only at the ESX(i) level. The iSCSI target must be mounted and managed by the ESX(i) host. If a virtual machine is to have a C drive and a D drive, they must be added as a virtual hard disk using the VMWare client.
- The rules for drive types and options are the same for virtual machine environments. The storage must be local, Direct Attached Storage or SAN.

**Warning:** These configurations have been tested and approved by Avaya for use with Officelinx. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Required Server Components

For Microsoft Windows Server 2012, you must ensure that all the necessary server roles and features are installed on the system before proceeding with Officelinx installation.

Digital Certificates

Avaya Officelinx requires that signed digital certificates be installed on the voice server before attempting an installation. Trusted certificates are used to create secure connections between the voice server and the client. The client uses the certificate to authenticate the signature stored on the server while negotiating a secure connection.

For High Availability installations, the certificates must be installed on the Consolidated server.

Digital certificates can be purchased from any trusted Certificate Authority (CA), such as GoDaddy™ and Symantec™. Contact your CA for more information on obtaining and installing the certificate on the server.
Server Roles and Features

1. From the **Server Manager Dashboard**, click **Add roles and features**.

   ![Server Manager Dashboard]

   If this screen is hidden, go to **View** and select **Show Welcome Tile**.

2. Click **Next**.

   ![Add Roles and Features Wizard]

   Before you begin
3. Leave the default settings as they are. Click **Next**.

![Add Roles and Features Wizard](image1)

4. Leave the default settings as they are. Click **Next**.

![Add Roles and Features Wizard](image2)
5. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes. Click **Next**.

**Note**: Throughout this installation, whenever you are prompted to confirm additions, always select **Add Features**.
6. Enable the .NET Framework 3.5 Features checkbox. Click **Next**.

7. Review the information, then click **Next**.
8. Ensure that **HTTP Activation**, under **Windows Process Activation Service Support** is enabled. Click **Next**.

9. On the **Fax Server** screen, click **Next**.
10. On the **Print and Document Services** screen, click **Next**.

![Print and Document Services screen](image1)

11. No changes are required here. Click **Next**.

![Select role services](image2)
12. On the **Web Server Role (IIS)** screen, click **Next**.

13. Open **Web Server > Common HTTP Features**. Enable **Directory Browsing**, **HTTP Errors**, **Static Content** and **HTTP Redirection**.

Scroll down to **Security**, and enable **Windows Authentication**.


Locate **FTP Server** and enable **FTP Service**.

Enable all options under **Management Tools > IIS 6 Management Compatibility**.

Click **Next** when ready.
14. Review the selections here. When ready to proceed, click **Install**.

15. If prompted to provide the Windows disk to load the files, click **Specify an alternate source path** and direct it to the appropriate drive.

**Hint:** This is particularly important for virtual machine installations where there may not be a drive configured locally.
16. Windows will now start the installation process for the chosen items. This process may take a while.

Note: This window can be closed without interrupting the installation procedure

17. Once all changes are complete, Restart the server.

Installing Microsoft .NET Framework 4.6

The Microsoft .NET Framework 4.6 is a required Windows component but it cannot be installed as part of the program package. It must be added by the administrator.

The installer can be downloaded from the Microsoft site here:


Follow the instructions provided to install .NET Framework 4.6 onto the server.
Disabling User Account Control Notification


2. Select Change Account Settings.

   On the User Account Control Settings screen, click and drag the slider down to Never Notify.

   Click OK and Close.
3. On the keyboard, click the **Start button**, and select **Administrative Tools**.

4. Double-click **Local Security Policy**.
5. Under **Security Settings > Local Policies > Security Options**, double-click **User Account Control: Run all administrators in Admin Approval Mode**.

![Local Security Policy](image)

6. Select **Disabled**. Click **OK**.

![User Account Control: Run all administrators in Admin Approval Mode](image)

**Note**: UAC Notifications can be restored after Officelinx has been installed.
IIS Certificates

The site administrator must install either a self-signed certificate, or a certificate purchased from a Certification Authority. It is **not** necessary to install both types of certificate.

*Note*: Corporate security protocols may require the use of certificates purchased from an appropriate authority. High-security (JITC) installations always require a CA issued certificate for the Encrypted File System (EFS).

Additional information on installing certificates onto the voice server can be found here:


Once the certificates have been installed, continue with **IIS Certificate Bindings**.

IIS Certificate Bindings

To enable an HTTPS connection, a certificate has to be installed on the voice server. The HTTPS protocol must be enabled, and HTTP disabled.

1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.
2. Right-click in the right-hand pane and choose Import from the pop-up menu.

3. Enter the path to the certificate file and the password. Select Personal as the Certificate Store. Click OK.

4. Go to Sites > Default Web Site. Click Bindings....
5. Add the HTTPS binding type.
Set the **IP Address** to **All Unassigned**. Leave Port at its default.
Change **SSL Certificate** to the certificate name installed above.
Click **OK**.

![Add Site Binding](image1)

6. Remove HTTP from the list of bindings.
Click **Close**.

![Site Bindings](image2)
Installation

User Rights

If the user who will be installing Officelinx has not logged in as the system administrator, that user must be given full rights to the root of the C drive.

2. Click Add. Enter the installation user's name in the space provided.
3. The system will locate that user's account and display its current rights to the C drive. Enable Full control, and click OK.
Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

![Setup.exe](image)

2. In the extraction folder, run **Setup.exe** as administrator to install Avaya Officelinx onto your voice server.

![Windows Installer](image)

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically add the necessary packages if they do not already exist on the system. These packages may include **Sentinel Protection**, **Microsoft Visual C++ Redistributable** and **Microsoft .Net Framework 4.5**. This process may take a while depending on the missing components.

**Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

Click **OK** after entering the credentials.

5. Review the license agreements and enable **I accept the license agreement**.

Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.

**Note**: It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Single UC Server**.

Click **Next**.

**Single UC Server**: When operating Officelinx on a single voice server computer.

**Multiple UC Servers in High Availability**: When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway**: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select the license type you will using for this installation. Most sites will use the WebLM License option.

**Note:** If you select Officelinx, go to chapter 12, Installing the Officelinx License. When finished, return here and continue the installation from step 11. Skip step 9 through 10.

**Warning:** It is essential that the system/PC clock be properly set before activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

9. The License Upgrade Utility program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   Enter the address in the space provided, then click **OK**.

**Important:** This step requires that the Web License Manager has been installed and configured on the license server computer. See Installing the WebLM License and Server on page 297.
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.

![License Upgrade Utility](image)

**Note:** The number of voice ports is calculated based upon your license.

\[
\text{Number of voice ports} = \left( \frac{\# \text{Basic users} + \# \text{Mainstream users}}{40} \right) + \text{Number of voice ports in license}
\]

Click **Exit** to close the license window and continue with the installation.

11. Select the **Components** required at your site. Disable any components that are not needed.

Click **Next**.

12. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more required components are not installed on the computer.

For all items that are not checked, return to Windows and add any missing pieces to the operating system.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required components have been added to Windows. This screen does not refresh until you click **Next**.
13. This screen shows the IIS settings that Officelixn requires to operate.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.

14. Select your PBX Brand then click **Next**.

15. Select your PBX model from the dropdown menu.

   Click **Next**.

16. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.
17. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

**Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

18. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya Officelinx.

**Hint:** The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

20. The preliminary information required for installation is now complete.

Click **Next**.
21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the ** Automatically Close** option or manually close the process which is interfering with the installation.

   Click OK when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration if necessary.

   Click Next to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click Next when ready.
26. Confirm the information then click **Finish**.

**Note:** Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. At the OAI Configuration Wizard screen:
   - **Enable Direct TCP/IP**.
   - **Set Number of Nodes = 1**.
   - **Activate the Enable logs radio button**. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.
   
   Click **Next**.

28. On the Link Information page, enter the **IP Address** of the PBX. Leave **Port** at its default setting (4000). Leave the **Login Password** field blank.

   Click **Next**.

29. At the **Dialog** screen, from the lists on the left-hand side, choose the desired **Stations** (extensions and voicemail ports), **Hunt Groups** and **Trunks** to use with OAI.

   Select an item on the left, then click **Add** to move it into the right-hand pane.

30. Click **Save** to finish the OAI setup and continue with the Officelinx installation.
31. Click **Finish** to restart the server.

If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

The Officelinx installation is complete.
In This Chapter:

86  Introduction
86  Requirements
87  Installation Preparation
87  Deployment Configuration Considerations
87  Antivirus Applications
87  Required Server Components
101  Installation
Introduction

With Avaya Officelinx version 10.7, the installation process has become simpler than ever before. Virtually all choices regarding the installation will be asked at the beginning so that the numerous components can be installed without interruption. The only variation which will occur after this initial selection will be the PBX and integration type related configuration which will be unique to most sites.

Please keep in mind that this guide is only meant to provide an overview of the process as opposed to an exact step-by-step guide. Since all sites vary in configuration you must take that into consideration and ensure that you approach the installation process dynamically rather than to fully rely on this manual.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>A Full License for 10.7.</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
</tbody>
</table>

*Note:* Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

*Note:* Officelinx should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.

*Caution:* It is strongly recommended that, for Windows Server 2008, 2012, and 2016 the operating system drive has a minimum of 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Officelinx voice server installation.
Installation Preparation

Deployment Configuration Considerations

- An Avaya Officelinx server may be installed on the root drive (the same drive where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- An Officelinx server may be installed on a secondary drive (on a different drive from where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- The drives may each be a physical drive (for best performance), or a single drive with partitions.
- The folders \uc\logs, \uc\DB, and \uc\messages may be mounted to a local drive. Network or mapped drives are not supported.
- In an ESX(i)/VMWare environment, SAN/iSCSI is supported, but only at the ESX(i) level. The iSCSI target must be mounted and managed by the ESX(i) host. If a virtual machine is to have a C drive and a D drive, they must be added as a virtual hard disk using the VMWare client.
- The rules for drive types and options are the same for virtual machine environments. The storage must be local, Direct Attached Storage or SAN.

Warning: These configurations have been tested and approved by Avaya for use with Officelinx. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Required Server Components

For Microsoft Windows Server 2008 R2, you must ensure that all the necessary server roles are installed on the system before proceeding with Officelinx installation.

Digital Certificates

Avaya Officelinx requires that signed digital certificates be installed on the voice server before attempting an installation. Trusted certificates are used to create secure connections between the voice server and the client. The client uses the certificate to authenticate the signature stored on the server while negotiating a secure connection.

For High Availability installations, the certificates must be installed on the Consolidated server. Digital certificates can be purchased from any trusted Certificate Authority (CA), such as GoDaddy and Symantec. Contact your CA for more information on obtaining and installing the certificate on the server.
Server Manager Configuration

1. Go to **Start>Administrative Tools>Server Manager**.

2. Click on **Roles** in the left-hand pane.
   Click **Add Roles** in the right-hand pane.
3. The Wizard will launch, allowing you to easily install the necessary components. 

Click **Next**.

4. Enable the Application Server, Fax Server and Web Server (IIS) checkboxes.

Click **Next**.

**Note:** Throughout this installation, whenever you are prompted about other required services, always select Add Required Role Services.
5. Review the information then click **Next**.

6. Ensure that the necessary accounts have access to the services. For most cases, a single account with local admin rights should be used throughout Officelinx configuration. Click **Next**.
7. Select **Only routing assistants can access the fax server inbox** radio button. Click **Next**.

8. Confirm the account for access rights again then click **Next**.
9. Review the information then click **Next**.

10. Enable **Print Server** then click **Next**.
11. Review the information then click **Next**.

12. Ensure that **.NET Framework 3.5.1** is checked.

Also, under **Windows Process Activation Service Support**, enable **HTTP Activation**, **TCP Activation**, and **Named Pipes Activation**.

Click **Next**.
13. Review the information then click **Next**.

14. Enable the **Static Content**, **Directory Browsing**, **HTTP Errors**, **HTTP Redirection**, **ASP .NET**, **ASP** and **CGI** checkboxes. Choose to accept any requirements as well if prompted.

Scroll down the list once these items are enabled.

Click **Next**.

16. Confirm the installation items then click **Install**.
17. Windows will now start the installation process for the chosen items. This process may take a while.

18. When the installation is finished, click **Close**.

19. Installed components will now appear under the Roles Summary.
Disabling User Account Control Notification

In order to install the Officelinx application on a Windows Server 2008 R2 environment, you must turn off the UAC notification feature on the local Admin user which will be used with Officelinx.

   Click on Change User Account Control Settings.

2. Drag the slider to the bottom of its range (Never Notify).
   Click OK.

Note: UAC Notifications can be restored after Officelinx has been installed.

Installing Microsoft .NET Framework 4.6

The Microsoft .NET Framework 4.6 is a required Windows component but it cannot be installed as part of the program package. It must be added by the administrator.

The installer can be downloaded from the Microsoft site here:


Follow the instructions provided to install .NET Framework 4.6 onto the server.
IIS Certificates

The site administrator must install either a self-signed certificate, or a certificate purchased from a Certification Authority. It is **not** necessary to install both types of certificate.

*Note:* Corporate security protocols may require the use of certificates purchased from an appropriate authority. High-security (JITC) installations always require a CA issued certificate for the Encrypted File System (EFS).

Additional information on installing certificates onto the voice server can be found here:


Once the certificates have been installed, continue with **IIS Certificate Bindings**.

IIS Certificate Bindings

To enable an HTTPS connection, a certificate has to be installed on the voice server. The HTTPS protocol must be enabled, and HTTP disabled.

1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.
2. Right-click in the right-hand pane and choose Import from the pop-up menu.

3. Enter the path to the certificate file and the password. Select Personal as the Certificate Store. Click OK.

4. Go to Sites > Default Web Site. Click Bindings....
5. Add the HTTPS binding type. Set the **IP Address** to **All Unassigned**. Leave Port at its default. Change **SSL Certificate** to the certificate name installed above. Click **OK**.

6. Remove HTTP from the list of bindings. Click **Close**.
Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that Windows Firewall is disabled, and that Windows Automatic Update is turned off.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe** as administrator to install Avaya Officelinx onto your voice server.

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically add the necessary packages if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the missing components.

**Note:** Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

Click **OK** after entering the credentials.

5. Review the license agreements and enable **I accept the license agreement**.

Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.

**Note**: It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Single UC Server**.

Click **Next**.

**Single UC Server**: When operating Officelinx on a single voice server computer.

**Multiple UC Servers in High Availability**: When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway**: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select the license type you will use for this installation. Most sites will use the WebLM License option.

   **Note**: If you select Officelinx, go to chapter 12, Installing the Officelinx License. When finished, return here and continue the installation from step 11. Skip step 9 through 10.

   **Warning**: It is essential that the system/PC clock be properly set before activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

9. The License Upgrade Utility program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   Enter the address in the space provided, then click OK.

   **Important**: This step requires that the Web License Manager has been installed and configured on the license server computer. See Installing the WebLM License and Server on page 297.
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.

   ![License Upgrade Utility](image)

   *Note: The number of voice ports is calculated based upon your license.*

   \[ \left( \frac{\text{# Basic users} + \text{# Mainstream users}}{40} \right) + \text{Number of voice ports in license} \]

11. Select the **Components** required at your site. Disable any components that are not needed.

    Click **Next**.

12. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

    *Note: This screen will only appear if one or more required components are not installed on the computer.*

    For all items that are not checked, return to Windows and add any missing pieces to the operating system.

    Click **Next** when finished or to refresh the display.

    *Note: The installation will not continue until all of the required components have been added to Windows.*

    This screen does not refresh until you click **Next**.
13. This screen shows the IIS settings that Officelinx requires to operate.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

14. Select your PBX Brand then click **Next**.

15. Select your PBX model from the dropdown menu.

   Click **Next**.

16. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.
17. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

*Note*: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

18. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya Officelinx.

*Hint*: The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

20. The preliminary information required for installation is now complete.

Click **Next**.
21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the **Automatic Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site’s PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration if necessary.

   Click **Next** to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.
26. Confirm the information then click Finish.

**Note:** Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the SIP Configuration Tool in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. At the OAI Configuration Wizard screen:
   - Enable Direct TCP/IP.
   - Set Number of Nodes = 1.
   - Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.
   
   Click Next.

28. On the Link Information page, enter the IP Address of the PBX. Leave Port at its default setting (4000). Leave the Login Password field blank.
   
   Click Next.

29. At the Dialog screen, from the lists on the left-hand side, choose the desired Stations (extensions and voicemail ports), Hunt Groups and Trunks to use with OAI.
   
   Select an item on the left, then click Add to move it into the right-hand pane.

30. Click Save to finish the OAI setup and continue with the Officelinx installation.

**Note:** This section is for installations where Mitel 5000 (All) was chosen at the PBX selection screen. Skip the next 4 steps if this does not apply.
31. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

   The Officelinx installation is complete.
In This Chapter:

- 112 Introduction
- 112 Requirements
- 113 Installation Preparation
- 113 Deployment Configuration Considerations
- 113 Antivirus Applications
- 113 Required Server Components
- 128 Installation
Introduction

With Officelinx version 10.7, the installation process has become simpler than ever before. Virtually all choices regarding the installation will be asked at the beginning so that the numerous components can be installed without interruption. The only variation which will occur after this initial selection will be the PBX and integration type related configuration which will be unique to most sites.

Please keep in mind that this guide is only meant to provide an overview of the process as opposed to an exact step-by-step guide. Since all sites vary in configuration you must take that into consideration and ensure that you approach the installation process dynamically rather than to fully rely on this manual.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>A Full License for 10.7</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
</tbody>
</table>

**Note:** Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Note:** Officelinx should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.

**Caution:** It is strongly recommended that, for Windows Server 2008, 2012, and 2016 the operating system drive has a minimum of 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Officelinx voice server installation.
Installation Preparation

Deployment Configuration Considerations

- An Officelinx server may be installed on the root drive (the same drive where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- An Officelinx server may be installed on a secondary drive (on a different drive from where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- The drives may each be a physical drive (for best performance), or a single drive with partitions.
- The folders \uc\logs, \uc\DB, and \uc\messages may be mounted to a local drive. Network or mapped drives are not supported.
- In an ESX(i)/VMWare environment, SAN/iSCSI is supported, but only at the ESX(i) level. The iSCSI target must be mounted and managed by the ESX(i) host. If a virtual machine is to have a C drive and a D drive, they must be added as a virtual hard disk using the VMWare client.
- The rules for drive types and options are the same for virtual machine environments. The storage must be local, Direct Attached Storage or SAN.

**Warning:** These configurations have been tested and approved by Avaya for use with Officelinx. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Required Server Components

For Microsoft Windows Server 2008, you must ensure that all the necessary items are installed on the system before proceeding with Officelinx installation.

Digital Certificates

Avaya Officelinx requires that signed digital certificates be installed on the voice server before attempting an installation. Trusted certificates are used to create secure connections between the voice server and the client. The client uses the certificate to authenticate the signature stored on the server while negotiating a secure connection.

For High Availability installations, the certificates must be installed on the Consolidated server.

Digital certificates can be purchased from any trusted Certificate Authority (CA), such as GoDaddy and Symantec. Contact your CA for more information on obtaining and installing the certificate on the server.
Server Manager Configuration

1. Launch the Server Manager application from the Administrative Tools programs folder.

2. You will be installing various roles required by Officelinx from here.

   Click on Roles from the left side pane, then click on Add Roles from the right side pane.
3. The Wizard will launch, allowing you to easily install the necessary components.

   Click **Next**.
4. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes. Click **Next**.

**Note**: When you are prompted about other required services, always select **Add Required Role Services**.

5. Review the information then click **Next**.
6. Ensure that the necessary accounts have access to the services. For most cases, a single account with local admin rights should be used throughout Officelinx configuration. Click **Next**.

7. Select **Only routing assistants can access the fax server inbox** radio button then click **Next**.
8. Confirm the account for access rights again then click **Next**.

9. Review the information then click **Next**.
10. Enable **Print Server** then click **Next**.

11. Review the information then click **Next**.
12. Ensure that Application Server Foundation is enabled.

Under Windows Process Activation Service Support, enable HTTP Activation, TCP Activation, and Named Pipes Activation.

Click Next.

13. Review the information then click Next.
14. Enable the **Static Content, Directory Browsing, HTTP Errors, HTTP Redirection, CGI, ASP .NET** and **ASP** checkboxes. 
Choose to accept any requirements as well if prompted.
Scroll down the list when these items are enabled.

Click **Next**.
16. Confirm the installation items then click **Install**.

17. Windows will now start the installation process for the chosen items. This process may take a while.
18. When the installation is finished, click **Close**.

19. Installed components will now appear under the Roles Summary.

---

**Installing Microsoft .NET Framework 4.6**

The Microsoft .NET Framework 4.6 is a required Windows component but it cannot be installed as part of the program package. It must be added by the administrator.

The installer can be downloaded from the Microsoft site here:


Follow the instructions provided to install .NET Framework 4.6 onto the server.
Disabling User Access Control Notification

In order to install the Officelinx application on a Windows Server 2008 environment, you must turn off the UAC notification feature on the local Admin user which will be utilized with Officelinx.

1. Open the User Account panel from the Control Panel then click on the Turn User Account Control on or off link.

2. Disable Use User Account Control... then click OK.

3. You will be prompted to restart your computer. Click Restart Now to restart the system.
IIS Certificates

The site administrator must install either a self-signed certificate, or a certificate purchased from a Certification Authority. It is **not** necessary to install both types of certificate.

**Note:** Corporate security protocols may require the use of certificates purchased from an appropriate authority. High-security (JITC) installations always require a CA issued certificate for the Encrypted File System (EFS).

Additional information on installing certificates onto the voice server can be found here:


Once the certificates have been installed, continue with **IIS Certificate Bindings**.

IIS Certificate Bindings

To enable an HTTPS connection, a certificate has to be installed on the voice server. The HTTPS protocol must be enabled, and HTTP disabled.

1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.
2. Right-click in the right-hand pane and choose Import from the pop-up menu.

3. Enter the path to the certificate file and the password. Select Personal as the Certificate Store. Click OK.

4. Go to Sites > Default Web Site. Click Bindings....
5. Add the HTTPS binding type. Set the IP Address to All Unassigned. Leave Port at its default. Change SSL Certificate to the certificate name installed above. Click OK.

6. Remove HTTP from the list of bindings. Click Close.
## Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

![Avaya Officelinx Setup](image)

2. In the extraction folder, run **Setup.exe** as **administrator** to install Avaya Officelinx onto your voice server.

![Avaya Officelinx Setup Wizard](image)

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically add the necessary packages if they do not already exist on the system. These packages may include **Sentinel Protection**, **Microsoft Visual C++ Redistributable**, and **Microsoft .Net Framework 4.5**. This process may take a while depending on the missing components.

**Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.

5. Review the license agreements and enable **I accept the license agreement**.

   Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click **Next** to continue.

   **Note:** It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Single UC Server**.

   Click **Next**.

   **Single UC Server:** When operating Officelinx on a single voice server computer.

   **Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

   **Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select the license type you will use for this installation. Most sites will use the WebLM License option.

**Note:** If you select Officelinx, go to [chapter 12, Installing the Officelinx License](#). When finished, return here and continue the installation from step 11. Skip step 9 through 10.

**Warning:** It is essential that the system/PC clock be properly set **before** activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

9. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   Enter the address in the space provided, then click **OK**.

**Important:** This step requires that the Web License Manager has been installed and configured on the license server computer. See [Installing the WebLM License and Server](#) on page 297.
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.

![License Upgrade Utility](image)

**Note:** The number of voice ports is calculated based upon your license.  
\[
\left( \frac{\text{# Basic users} + \text{# Mainstream users}}{40} \right) + \text{Number of voice ports in license}
\]

11. Select the **Components** required at your site. Disable any components that are not needed.

**Click Next.**

12. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more required components are not installed on the computer.

For all items that are not checked, return to Windows and add any missing pieces to the operating system.

**Click Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required components have been added to Windows.  
This screen does not refresh until you click **Next.**
13. This screen shows the IIS settings that Officelinx requires to operate.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.

14. Select your PBX Brand then click **Next**.

15. Select your PBX model from the dropdown menu.

Click **Next**.

16. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.
17. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

*Note:* If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

18. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya Officelinx.

*Hint:* The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

20. The preliminary information required for installation is now complete.

Click **Next**.
21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the **Automatic Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration if necessary.

   Click **Next** to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.
26. Confirm the information then click **Finish**.

**Note:** Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. At the OAI Configuration Wizard screen:
   - Enable **Direct TCP/IP**.
   - Set **Number of Nodes = 1**.
   - Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.

Click **Next**.

28. On the Link Information page, enter the **IP Address** of the PBX. Leave **Port** at its default setting (4000). Leave the **Login Password** field blank.

Click **Next**.

29. At the **Dialog** screen, from the lists on the left-hand side, choose the desired **Stations** (extensions and voicemail ports), **Hunt Groups** and **Trunks** to use with OAI.

Select an item on the left, then click **Add** to move it into the right-hand pane.

30. Click **Save** to finish the OAI setup and continue with the Officelinx installation.

**Note:** This section is for installations where **Mitel 5000 (All)** was chosen at the PBX selection screen. Skip the next 4 steps if this does not apply.
31. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

   The Officelinx installation is complete.
In This Chapter:

138  Introduction
138  Requirements
139  Installation Preparation
139  Deployment Configuration Considerations
139  Antivirus Applications
139  Required Components
147  Installation
Introduction

With Avaya Officelinx version 10.7, the installation process has become simpler than ever before. Virtually all choices regarding the installation will be asked at the beginning so that the numerous components can be installed without interruption. The only variation which will occur after this initial selection will be the PBX and integration type related configuration which will be unique to most sites.

Please keep in mind that this guide is only meant to provide an overview of the process as opposed to an exact step-by-step guide. Since all sites vary in configuration you must take that into consideration and ensure that you approach the installation process dynamically rather than to fully rely on this manual.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>A Full License for 10.7</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
</tbody>
</table>

**Note:** Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Note:** Officelinx should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.
Installation Preparation

Deployment Configuration Considerations

- An Officelinx server may be installed on the root drive (the same drive where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- An Officelinx server may be installed on a secondary drive (on a different drive from where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- The drives may each be a physical drive (for best performance), or a single drive with partitions.
- The folders \\uc\logs, \\uc\DB, and \\uc\messages may be mounted to a local drive. Network or mapped drives are not supported.
- In an ESX(i)/VMWare environment, SAN/iSCSI is supported, but only at the ESX(i) level. The iSCSI target must be mounted and managed by the ESX(i) host. If a virtual machine is to have a C drive and a D drive, they must be added as a virtual hard disk using the VMWare client.
- The rules for drive types and options are the same for virtual machine environments. The storage must be local, Direct Attached Storage or SAN.

**Warning:** These configurations have been tested and approved by Avaya for use with Officelinx. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Required Components

For Microsoft Windows 7, you must ensure that all the necessary items are installed on the system before proceeding with the Officelinx installation.

Digital Certificates

Avaya Officelinx requires that signed digital certificates be installed on the voice server before attempting an installation. Trusted certificates are used to create secure connections between the voice server and the client. The client uses the certificate to authenticate the signature stored on the server while negotiating a secure connection.

For High Availability installations, the certificates must be installed on the Consolidated server.

Digital certificates can be purchased from any trusted Certificate Authority (CA), such as GoDaddy and Symantec. Contact your CA for more information on obtaining and installing the certificate on the server.
Installing Windows Components

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 pane.
3. From the Features window, enable **Internet Information Services**, then manually enable the following entries in the order listed:
   - **FTP Server**
   - **FTP Extensibility**
   - **FTP Service**
   - **Web Management Tools**
     - **IIS 6 Management Compatibility** (all components under this tree)
     - **IIS Management Console**
   - **World Wide Web Services**
     - **Application Development Features**
     - **.NET Extensibility**
     - **ASP**
     - **ASP .NET**
     - **CGI**
     - **ISAPI Extensions**
     - **ISAPI Filters**
     - **Common HTTP Features**
     - **Directory Browsing**
     - **HTTP Errors**
     - **HTTP Redirection**
     - **Static Content**
     - **Security**
     - **Windows Authentication**

   **Warning**: Some components may automatically be enabled for you due to dependencies. It is vital that you **do not disable** any of these components. The order in which components are selected is also vital to ensure the proper implementation of IIS.

4. Scroll down and enable the following under **Print and Document Services**.
   - **Internet Printing Client**
   - **Windows Fax and Scan**
5. Scroll down and enable the following features **Windows Process Activation Service**.
   - .NET Environment
   - Configuration APIs
   - Process Model

6. Click **OK** when finished.

7. Windows will add the selected components. This process may take a while.

8. When the process is complete, click **Restart Now** to reboot your server.

**Note:** If you are not prompted to restart your computer, you may do so after disabling User Access Control on the next section.

**Note:** To confirm if IIS has been enabled correctly, open your web browser and type `http://localhost` in the address bar. You should see an IIS welcome screen if everything is running correctly.
Disabling User Access Control Notification

In order to install the Officelinx application on a Windows 7 environment, you must turn off the UAC notification feature on the local Admin user which will be utilized with Officelinx. To do so, open User Account from the Control Panel then click on the Change User Account Control settings link.

Move the notification bar on the left to the bottom to select Never notify then click OK. If you are warned about the changes, approve the change.

Restart your server so that the settings can take affect right away.

Installing Microsoft .NET Framework 4.6

The Microsoft .NET Framework 4.6 is a required Windows component but it cannot be installed as part of the program package. It must be added by the administrator.

The installer can be downloaded from the Microsoft site here:


Follow the instructions provided to install .NET Framework 4.6 onto the server.
IIS Certificates

The site administrator must install either a self-signed certificate, or a certificate purchased from a Certification Authority. It is **not** necessary to install both types of certificate.

**Note**: Corporate security protocols may require the use of certificates purchased from an appropriate authority. High-security (JITC) installations always require a CA issued certificate for the Encrypted File System (EFS).

Additional information on installing certificates onto the voice server can be found here:


Once the certificates have been installed, continue with **IIS Certificate Bindings**.

IIS Certificate Bindings

To enable an HTTPS connection, a certificate has to be installed on the voice server. The HTTPS protocol must be enabled, and HTTP disabled.

1. Open **Control Panel > Administrative Tools** and select the **IIS Manager console**.
   Select the local computer. Open **Server Certificates** in the right-hand pane.
2. Right-click in the right-hand pane and choose Import from the pop-up menu.

3. Enter the path to the certificate file and the password. Select Personal as the Certificate Store. Click OK.

4. Go to Sites > Default Web Site. Click Bindings....
5. Add the HTTPS binding type. Set the **IP Address** to **All Unassigned**. Leave Port at its default. Change **SSL Certificate** to the certificate name installed above. Click **OK**.

6. Remove HTTP from the list of bindings. Click **Close**.
Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe** as administrator to install Avaya Officelinx onto your voice server.

3. Once the Windows components have been verified, click **Next** to begin the installation.

   **Note:** The installer will automatically add the necessary packages if they do not already exist on the system. These packages may include **Sentinel Protection**, **Microsoft Visual C++ Redistributable** and **Microsoft .Net Framework 4.5**. This process may take a while depending on the missing components.

   **Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

Click OK after entering the credentials.

5. Review the license agreements and enable **I accept the license agreement**.

Click Next to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click Next to continue.

**Note:** It is highly recommended that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Single UC Server**.

Click Next.

**Single UC Server:** When operating Officelinx on a single voice server computer.

**Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select the license type you will using for this installation. Most sites will use the WebLM License option.

Note: If you select Officelinx, go to chapter 12, Installing the Officelinx License. When finished, return here and continue the installation from step 11. Skip step 9 through 10.

Warning: It is essential that the system/PC clock be properly set before activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

9. The License Upgrade Utility program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

Enter the address in the space provided, then click OK.

Important: This step requires that the Web License Manager has been installed and configured on the license server computer. See Installing the WebLM License and Server on page 297.
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.

![License Upgrade Utility](image)

**Note:** The number of voice ports is calculated based upon your license.

\[
\text{[ (# Basic users + # Mainstream users) / 40 ] + Number of voice ports in license}
\]

11. Select the **Components** required at your site. Disable any components that are not needed.

Click **Next**.

![UC Services Setup](image)

12. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more required components are **not** installed on the computer.

For all items that are not checked, return to Windows and add any missing pieces to the operating system.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required components have been added to Windows. This screen does not refresh until you click **Next**.
13. This screen shows the IIS settings that Officelinx requires to operate.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

14. Select your PBX Brand then click **Next**.

15. Select your PBX model from the dropdown menu.

   Click **Next**.

16. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.
17. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

**Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

18. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya Officelinx.

**Hint:** The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

20. The preliminary information required for installation is now complete.

Click **Next**.
21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the **Automatic Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site’s PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration if necessary.

   Click **Next** to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.
26. Confirm the information then click Finish.

**Note:** Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the SIP Configuration Tool in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. At the OAI Configuration Wizard screen:
   - Enable Direct TCP/IP.
   - Set Number of Nodes = 1.
   - Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.

   Click Next.

28. On the Link Information page, enter the IP Address of the PBX. Leave Port at its default setting (4000). Leave the Login Password field blank.

   Click Next.

29. At the Dialog screen, from the lists on the left-hand side, choose the desired Stations (extensions and voicemail ports), Hunt Groups and Trunks to use with OAI.

   Select an item on the left, then click Add to move it into the right-hand pane.

30. Click Save to finish the OAI setup and continue with the Officelinx installation.

**Note:** This section is for installations where Mitel 5000 (All) was chosen at the PBX selection screen. Skip the next 4 steps if this does not apply.

**Note:** Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the SIP Configuration Tool in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.
31. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

   The Officelinx installation is complete.
In This Chapter:

158 Introduction
159 Preparing the Servers
174 Master Voice Server
183 Consolidated Server
189 Secondary Voice Server
196 Verifying File Sync
196 Verifying File Sync
197 Upgrading an Existing HA Installation
201 Upgrading from a non-HA Installation
203 Sharing the UC Folder
205 MWI Configuration
Introduction

**Warning:** Avaya Officelinx High Availability Edition **must** only be installed by properly trained and certified personnel.

This document provides the installation procedure for Avaya Officelinx with a **High Availability Server (Master, Secondary & Consolidated)**. The purpose of a High Availability Installation is operational continuity, in which the Secondary PCs provide your organization with full and complete Officelinx functionality in case of a Master PC failure. A second Secondary PC can perform the same service in case of a Master or first Secondary PC failure. The purpose of the Consolidated PC is to synchronize the voice servers (Master and all Secondaries).

**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.

- If one of the voice servers (Master or Secondary) fails, traffic is routed away from that server to the still active ones.
- The license details reside on the Master Server. If it fails, you have 28 days to restore the connection before the system will revert to demo mode.
- If the Consolidated Server fails, the remaining voice servers will continue to process voice traffic, but UM services (calendar sync, Gmail integration, transcription, etc.) will not be available.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>A Full License for 10.7 that includes HA.</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 or 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>

A High Availability installation requires a minimum of 3 computers, each setup as a server. One server is defined as the Master Voice Server. Between 1 and 19 additional servers are designated as Secondary Voice Servers. Controlling traffic flow, synchronization, load balancing and failover is a single Consolidated Server (also called the Database Server).

**Note:** Officelinx should only be installed on dedicated servers specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.

**Note:** Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Warning:** Once all of the HA servers (Consolidated, Master and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Master or Secondary servers before the synch is complete will corrupt the database preventing all logins on all servers. Refer to **Verifying File Sync** for complete details.
Preparing the Servers

Antivirus, Firewall and Automatic Updates

It is recommended that any antivirus and firewall applications currently active on the server computer be disabled during installation. It is also necessary to turn off Automatic Updates during the installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Disabling User Access Control Notification

In order to install Avaya Officelinx on a Windows Server environment, you must turn off the UAC notification feature on the local Admin user which will be utilized with Officelinx.

32-bit Windows:

2. Click Turn User Account Control on or off.
3. Disable Use User Account Control then click OK.
4. You will be prompted to restart your computer. Click Restart Now to restart the system.
64-bit Windows:

2. On this screen, click Change User Account Control settings.
3. Pull the slider to the bottom or its range, until Never notify me when... is selected.
4. Click OK.
5. Restart the computer.

Required Server Components

Ensure that all the necessary items are installed on the system before proceeding with Officelinx installation.
Server Manager Configuration (All Servers)

Perform the following steps on all servers; Consolidated, Master, and all Secondaries.

**Consolidated**: Where necessary, special instructions specific to the Consolidated Server setup are provided where there is a difference in the process from the Master and Secondary Servers.

**Note**: Some of these steps may require additional files from the Windows disk or other storage location.

1. From the Server Manager Dashboard, click **Add roles and features**.

   ![Server Manager Dashboard](image)

   If this screen is hidden, go to **View** and select **Show Welcome Tile**.
2. Click **Next**.

![Add Roles and Features Wizard](image)

3. Leave the default settings as they are. Click **Next**.

![Add Roles and Features Wizard](image)
4. Leave the default settings as they are. Click **Next**.
5. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes.

Click **Next**.

**Note:** Throughout this installation, whenever you are prompted to confirm additions, always select **Add Features**.
6. Enable the **.NET Framework 3.5 Features** checkbox. Click **Next**.

![Select features screenshot](image1)

7. Review the information, then click **Next**.

![Application Server screenshot](image2)
8. Ensure that **HTTP Activation**, under **Windows Process Activation Service Support** is enabled. Click **Next**.

9. On the **Fax Server** screen, click **Next**.
10. On the **Print and Document Services** screen, click **Next**.

![Print and Document Services Screen](image1)

11. No changes are required here. Click **Next**.

![Select role services](image2)
12. On the **Web Server Role (IIS)** screen, click **Next**.

13. Open **Web Server > Common HTTP Features**. Enable **Directory Browsing, HTTP Errors, Static Content** and **HTTP Redirection**.

   Scroll down to **Security**, and enable **Windows Authentication**.


   Locate **FTP Server** and enable **FTP Service**.

   Enable all options under **Management Tools > IIS 6 Management Compatibility**.

   Click **Next** when ready.
14. Review the selections here. When ready to proceed, click **Install**.

15. If prompted to provide the Windows disk to load the files, click **Specify an alternate source path** and direct it to the appropriate drive.

**Hint:** This is particularly important for virtual machine installations where there may not be a drive configured locally.
16. Windows will now start the installation process for the chosen items. This process may take a while.

17. Once all changes are complete, **Restart the server**.

**Installing Microsoft .NET Framework 4.6**

The Microsoft .NET Framework 4.6 is a required Windows component but it cannot be installed as part of the program package. It must be added by the administrator.

The installer can be downloaded from the Microsoft site here:


Follow the instructions provided to install .NET Framework 4.6 onto the server.
IIS Certificates (All Servers)

The site administrator must install either a self-signed certificate, or a certificate purchased from a Certification Authority. It is **not** necessary to install both types of certificate.

**Note**: Corporate security protocols may require the use of certificates purchased from an appropriate authority. High-security (JITC) installations always require a CA issued certificate for the Encrypted File System (EFS).

Additional information on installing certificates onto the voice server can be found here:


Once the certificates have been installed, continue with **IIS Certificate Bindings**.

IIS Certificate Bindings

To enable an HTTPS connection, a certificate has to be installed on the voice server. The HTTPS protocol must be enabled, and HTTP disabled.

1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.
2. Right-click in the right-hand pane and choose Import from the pop-up menu.

3. Enter the path to the certificate file and the password. Select Personal as the Certificate Store. Click OK.

4. Go to Sites > Default Web Site. Click Bindings....

5. Add the HTTPS binding type. Set the IP Address to All Unassigned. Leave Port at its default.
Change **SSL Certificate** to the certificate name installed above. Click **OK**.

6. Remove HTTP from the list of bindings. Click **Close**.
Master Voice Server

**Important:** The Master Server **MUST** be the first server to be setup since the Master holds the license for your site. The Consolidated Server should be next, and only when the database has synchronized between them should the Secondary Servers be installed. See Verifying File Sync on page 196.

**Installation**

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file from (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe** as administrator to install Avaya Officelinx onto the Master server.

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the required components.

**Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click OK after entering the credentials.

**Hint**: Wherever possible, this password should be setup with no expiration date. If the password does expire, then it must be changed on every computer that uses it. Many services will be unavailable until the change has been made everywhere.

5. Review all the license agreements and enable **I accept the license agreement**.

   Click Next to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click Next to continue.

**Note**: It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Multiple UC Servers in High Availability**.

   Click Next.

**Single UC Server**: When operating Officelinx on a single server computer.

**Multiple UC Servers in High Availability**: When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway**: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select **Master Voice Server**.
   Click **Next**.

9. Select the license type you will using for this installation.
   Most sites will use the WebLM License option.
   
   **Note:** If you select Officelinx, go to chapter 12, Installing the Officelinx License. When finished, return here and continue the installation from step 13. Skip step 10 through 12.

   **Warning:** It is essential that the system/PC clock be properly set **before** activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

10. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   Enter the address in the space provided, then click **OK**.

   **Important:** This step requires that the Web License Manager has been installed and configured on the license server computer. See Installing the WebLM License and Server on page 297.
11. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.

![License Upgrade Utility](image)

**Note:** The number of voice ports is calculated based upon your license.

\[
\text{Number of voice ports} \ = \ \left( \frac{\text{Basic users} + \text{Mainstream users}}{40} \right) + \text{Number of voice ports in license}
\]

12. This reminder may appear.

   Click **OK**.

![Redundancy license](image)

13. Select the **Components** required at your site.

   Click **Next**.

**Note:** If the Dialogic SR140 fax software will be used with this installation, ensure that the Hardware Fax Driver option is enabled here.

![UC Services Setup](image)
14. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more required components are not installed on the computer.

For all items that are not checked, return to Windows and add any missing pieces to the operating system.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required components have been added to Windows. This screen does not refresh until you click **Next**.

15. This screen shows IIS settings that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.

16. Select your PBX Brand then click **Next**.

17. Select your PBX model from the dropdown menu.

Click **Next**.
18. Enter the **IP Address** for the Consolidated Server.

   Click **Next**.

19. Enter the number of ports your system will use.

   Click **Next**.

20. The preliminary information required for installation is now complete.

   Click **Next**.

21. The selected components will now be installed. This process may take a while.
22. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration.

   Click **Next** to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.

26. Confirm the information then click **Finish**.

   **Note:** Depending on the type of SIP integration you'll be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.
27. At the OAI Configuration Wizard screen:
   - Enable Direct TCP/IP.
   - Set Number of Nodes = 1.
   - Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.

   Click Next.

28. On the Link Information page, enter the IP Address of the PBX. Leave Port at its default setting (4000). Leave the Login Password field blank.

   Click Next.

29. At the Dialog screen, from the lists on the left-hand side, choose the desired Stations (extensions and voicemail ports), Hunt Groups and Trunks to use with OAI.

   Select an item on the left, then click Add to move it into the right-hand pane.

30. Click Save to finish the OAI setup and continue with the Officelinx installation.

31. Click Finish to restart the server.

   If you wish to restart your computer at a later time, disable the Restart check box then click Finish.
32. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

Click **OK** to restart the computer.

---

**Warning:** Once all of the HA servers (Consolidated, Master and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Master or Secondary servers before the synch is complete will corrupt the database preventing all logins on all servers. Refer to [Verifying File Sync](#) for complete details.
Consolidated Server

**Important:** The Master Server MUST be the first server to be setup since the Master holds the license for your site. The Consolidated Server should be next, and only when the database has synchronized between them should the Secondary Servers be installed. See Verifying File Sync on page 196.

Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that Windows Firewall is disabled, and that Windows Automatic Update is turned off.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run Setup.exe as administrator to install Avaya Officelinx onto your Consolidated server.

3. Once the Windows components have been verified, click Next to begin the installation procedure.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the required components.

**Note:** Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click **OK** after entering the necessary credentials.

   **Hint:** Wherever possible, this password should be setup with no expiration date. If the password does expire, then it must be changed on every computer that uses it. Many services will be unavailable until the change has been made everywhere.

5. Review all the license agreements and select **I accept the license agreement**.

   Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click **Next** to continue.

   **Note:** It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

   **Single UC Server:** When operating Officelinx on a single server computer.

   **Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

   **Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select **Consolidated Database/File Server**. Click **Next**.

9. Select the **Components** required at your site. Click **Next**.

10. This screen shows all of the Windows roles and features that the Consolidated server requires to operate properly.

    **Note:** This screen will only appear if one or more required components are not installed on the server.

    For all items that are not checked, return to Windows and install any missing components into the operating system.

    Click **Next** when finished or to refresh the display.

    **Note:** The installation will not continue until all of the required components have been added to the server. The screen does not refresh until you click **Next**.

11. Select your PBX Brand then click **Next**.
12. Select your PBX model from the dropdown menu. Click Next.

13. Unless the Master Server has been upgraded from a Single Server installation, choose No. Click Next.

14. Select the Email Server Type from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.

15. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

   Select the country from the dropdown menu, and enter the area code in the space provided.

   Click Next to continue.

**Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.
16. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of the system.

**Hint:** The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

**Warning:** Once all of the HA servers (Consolidated, Master and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Master or Secondary servers before the synch is complete will corrupt the database preventing all logins on all servers. Refer to **Verifying File Sync** for complete details.

17. Create a new user administrator account on the local computer. Type and confirm a password for the new account.

   Click **Next** to continue.

18. The preliminary information required for installation is now complete.

   Click **Next**.
19. The selected components will now be installed. This process may take a while.

20. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

21. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site’s PBX exactly as required.

22. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

23. This alert is to remind you to properly share the UC installation folder (see for page 203 details).

   Click **OK** to restart the computer.

---

**Important:** Do not proceed with any Secondary Server installations until the synchronization between the Consolidated and Master Servers has completed or the database may become corrupted.
Secondary Voice Server

**Important:** The Master Server MUST be the first server to be setup since the Master holds the license for your site. The Consolidated Server should be next, and only when the database has synchronized between them should the Secondary Servers be installed. See Verifying File Sync on page 196.

### Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe** as administrator to install Avaya Officelinx onto all of your Secondary servers.

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the required components.

**Note:** Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click **OK** after entering the necessary credentials.

**Hint**: Wherever possible, this password should be setup with no expiration date. If the password does expire, then it must be changed on every computer that uses it. Many services will be unavailable until the change has been made everywhere.

5. Review all the license agreements and enable **I accept the license agreement**.

   Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click **Next** to continue.

**Note**: It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

**Single UC Server**: When operating Officelinx on a single server computer.

**Multiple UC Servers in High Availability**: When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway**: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.

9. Enter the IP Address of the Master Voice Server. Click Next.

10. Select the Components required at your site. Click Next.

**Note:** If the Dialogic SR140 fax software will be used with this installation, ensure that the Hardware Fax Driver option is enabled here.

11. Select your PBX Brand then click Next.
12. Select your PBX model from the dropdown menu. Click **Next**.

13. Unless the Master Server has been upgraded from a Single Server installation, enable **No**. Click **Next**.

14. Enter the number for this Secondary Server. Each Secondary must have a unique number assigned between 2 and 20. Click **Next**.

   **Note:** The Master Server is automatically assigned # 1.

15. Enter the **IP Address** for the Consolidated Server. Click **Next**.
16. Enter the number of ports your system will use.
   Click Next.

17. The preliminary information required for installation is now complete.
   Click Next.

18. The selected components will now be installed. This process may take a while.

19. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.
   Click OK when ready.

20. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.
21. In this section of the installation wizard you will be asked to provide additional settings for SIP integration.

Click **Next** to continue.

22. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

**Trunk** is selected by default, and is the best option for most installations.

Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

Click **Next** when ready.

23. Confirm the information then click **Finish**.

**Note:** Depending on the type of SIP integration you’ll be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

24. Click **Finish** to restart the server.

If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.
25. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

Click OK to restart the computer.

Warning: Once all of the HA servers (Consolidated, Master and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Master or Secondary servers before the synch is complete will corrupt the database preventing all logins on all servers. Refer to Verifying File Sync for complete details.
Verifying File Sync

Once Master and Consolidated servers have been installed, it is important to complete a full synch of all data before attempting to add any Secondary servers. Once a each Secondary has been attached, it too must be fully synchronized. Attempting to login to the Master or Secondary servers before the synchronization is complete will corrupt the database preventing all logins on all servers.

Data synchronization will begin once the sync service has been started on each server. On the Consolidated server, it is MobiLink - Consolidated. On the Master and all Secondary servers, this service called SQL Anywhere - MobiLink Remote.

Open the services window and check that the named services are running on each server. If any are not active, then select it and press Start.

Use any text editor (e.g. Windows Notepad) to open the Mobiclient.log file in the DB/Logs folder of the UC installation directory.

The message Completed processing of download stream will appear once the synch has finished.
Upgrading an Existing HA Installation

Use this section to upgrade an existing (≤ 7.x) Officelinx HA installation to 10.7 HA. Please make sure that your license has also been properly upgraded.

Stopping and Disabling Services

1. To stop the Services, click on **Start > Settings > Control Panel > Administrative Tools > Services**. Double-click **Services**. The Services screen appears:

2. Double-click the service to be stopped. The Service Properties screen appears.
3. Click the **Stop** button to halt the service.
4. From the **Startup type** dropdown list, select **Disabled**.
5. Click **OK**.
Upgrade Procedure for High Availability

**Warning:** Ensure that the correct machine (Consolidated, Master, Secondary) is being used at all times.

**Hint:** For safety, copy the DB, Messages and Prompts folders from the UC directory to the computer desktop.

**Hint:** Record the Startup Type of all services (Manual or Automatic) before proceeding so you can properly reset them afterwards.

1. On the Consolidated server, stop and disable the UC Service Recovery Manager service.
2. On the Master server, stop and disable these services: UC Voice Server, UC Background Task Manager, UC Background File Organizer, DBWatcher. Stop UC SIP Service and UC FaxService.
3. Wait 2-5 minutes until all syncs are successful (in Mobiclient.log verify “Completed processing of download stream”).
4. On the Master, stop and disable SQL Anywhere-MobiLink Remote_<computer name> (Mobilink).
5. Backup the database on the Master server.
6. Gracefully stop and then start SQL Anywhere-ASADB_UC (database) on the Master server.
7. Upgrade the Master server to the current release of Officelinx as per Installing the Upgrade on page 199.
8. Check that the SQL Anywhere-MobiLink Remote_<computer name> service is still disabled then restart the Master server.
9. Once the Master server has rebooted, start the UC Voice Server service and check that the Master accepts calls.
10. On all Secondaries, stop and disable these services: UC Voice Server, UC Background Task Manager, UC Background File Organizer, DBWatcher. Stop UC SIP Service and UC FaxService.
11. Wait 2-5 minutes until all syncs are successful (in Mobiclient.log verify “Completed processing of download stream”).
12. Stop and disable SQL Anywhere-MobiLink Remote_<computer name> (Mobilink) on all Secondaries.
13. On all Remote TSE servers, stop and disable the UC TSE Cache Manager service.
15. On the Consolidated, stop and disable these services: DBWatcher, MobiLink_Consolidated_<computer name>(Mobilink), UC Unified Messaging System Tasks Service, UC Background Task Manager, UC VPIM Server.
16. Backup the database on the Consolidated server.
17. Gracefully stop and then start the SQL Anywhere-ASADB_UC (database) service on the Consolidated.
18. Upgrade the Consolidated server to current release of Officelinx as per Installing the Upgrade on page 199.
19. On all Secondaries, backup the database.
20. Gracefully stop and then start the SQL Anywhere-ASADB_UC service on all Secondaries.
21. Upgrade all Secondaries to the current release of Officelinx as per Installing the Upgrade on page 199.
22. After the upgrade to the Consolidated server has completed, confirm that the UC Service Recovery Manager service is disabled and restart the server.
23. On both the Consolidated and the Master servers, stop and disable DBWatcher. Then start Mobilink - Consolidated on the Consolidated server, and SQL Anywhere - MobilinkRemote on the Master server.
24. Wait until the Master has synchronized with the Consolidated server (in the Mobiclient.log file, verify “Completed processing of download stream”).
25. Restart one-by-one all Secondaries after the upgrade is complete. Stop and disable DBWatcher and start the SQL Anywhere - MobilinkRemote services.
26. Wait until all Secondaries have synchronized with the Consolidated server.
27. On the Consolidated, Master, and all Secondaries start all UC Services except UC Service Recovery Manager.
28. Upgrade all Remote TSE servers to the current release of Officelinx as per Installing the Upgrade on page 199.
29. Start the Remote TSE servers.
30. Enable and start UC Service Recovery Manager services on the Consolidated server.
31. Upgrade all Remote Admin servers to the current release of Officelinx as per Installing the Upgrade on page 199.
32. Return all services to their original Startup Type and restart.
Installing the Upgrade

1. Run the update program. The following screen appears.

   Click **Next**.

2. If the installer determines that the administrator password is not sufficiently secure (e.g. **1111**), this screen will appear requiring it to be changed.

   The password cannot be left blank, it must contain both letters and numbers, and should be at least 6 characters long.

3. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

   Select the country from the dropdown menu, and enter the area code in the space provided.

   Click **Next** to continue.

   **Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, steps step 2 and step 4 will not appear. The values entered there will be used automatically.

4. The preliminary information required for installation is now complete.

   Click **Next**.
5. Applicable services will be stopped by the program.

6. The wizard will continue with the upgrade.

7. When finished, the following screen will appear. Click Finish to complete the upgrade.

8. You will be reminded to start the Mobilink service on the Consolidated server before you use the program.

9. When prompted to restart the server, choose Cancel and return to the appropriate step of the Upgrade Procedure for High Availability on page 198 of this manual.

Note: Remember to restart all services that were stopped. Or reboot each server to restart the services.
Upgrading from a non-HA Installation

Use this section if you have an existing Avaya Officelinx installation that you want to upgrade to High Availability. Please make sure that your license has also been properly upgraded.

**Caution:** It is strongly recommended that the Officelinx data files be backed up before performing any updates. Copy the database (C:\UC\DB), messages (C:\UC\Messages), and the prompts (C:\UC\Prompts) files.

**Update to 10.7**

Before installing High Availability, Avaya Officelinx must first be updated to the latest 10.7 release. See the appropriate sections of this manual for detailed information on updating Officelinx.

- Avaya Officelinx 7.x to 10.7 Upgrade on page 327.
- Avaya Officelinx 8.5 SP2+ to 10.7 Upgrade (SIP) on page 337.
- Short Upgrade on page 201.

**Upgrade to HA**

Once Avaya Officelinx has been updated to 10.7, High Availability can be installed.

The High Availability system requires at 3-10 computers to act as servers: 1 Master, 1-19 Secondary, and 1 Consolidated servers.

**Preparing the Servers**

All of the server computers must be prepared according to the steps outlined in this manual (see page 159-161).

**Master Voice Server**

**Warning:** The Master Voice Server must be the first server installed on an HA system.

The machine where the Single Server version of Avaya Officelinx is installed will become the Master Voice Server under HA. The licenses for both versions reside on this machine.

1. On the Single Server computer, launch the Officelinx installation wizard from the DVD.
2. You will be asked whether you want to repair the current installation, to modify the current installation, or to remove the program from the computer. Choose **Modify**. Click **OK** to continue.
3. The installation wizard will run. Continue with the Master Voice Server installation procedure as outlined beginning on page 174.

**Secondary Voice Servers**

Once the installation of the Master Voice Server is complete, all of the Secondary Voice Servers can be installed.

On all of the Secondary Voice Server machines, launch the installation wizard from the DVD and follow the setup process outlined beginning on page 189.
Consolidated Server

After the Master and all of the Secondary Voice Servers have been installed, the Consolidated Server can be setup. On the Consolidated Server computer, launch the installation wizard from the DVD and follow the setup process outlined beginning on page 196.
 Sharing the UC Folder

It is necessary to share the UC installation folder so that all of the programs and users have the required access. The following user accounts require full permissions to the UC folder:

**UCIIS** (local) - this is called **UCIISUser**.
**DCOM** (user) - the name of the domain user with admin rights on the local machine.

Follow this procedure on the Master, the Consolidated, and on each Secondary server on the system. Also share the folder if you are using a Remote Web Server. If you are using Remote TSE Servers, the folder only needs to be shared with the DCOM user.

**Procedure**

1. Locate the UC folder in Windows Explorer, then **Right-click > Properties > Sharing**.

2. Click **Advanced Sharing**. Enable the **Share this folder** checkbox.
3. Click Permissions, and Add the required users, giving each Full control of the folder.

   Remove the user Everyone.

4. Click Apply and return to the Windows desktop.
MWI Configuration

By default, during a failover condition, the Message Waiting Indicator (MWI) functions are not automatically re-routed to the alternate servers.

You can manually enable this functionality.

**Note:** This configuration is optional.

- Add a new line to the `ETSIPSERVICE.INI` file found in `/UC/Configuration` folder.

- Open the INI file with a text editor (e.g. Notepad). Locate the `PBX` section and append the following line:

  ```
  Fail Over=Yes
  ```

- Ensure that `Keep Alive` is also enabled ( `Keep Alive=Yes` ).

- Verify that there are at least 2 IP addresses listed under `IP`. These are for your PBXs and can be entered here if necessary, or configured through the SIP Configurator.

- Save the file and reboot the server.

**Note:** This must be done on each voice server (the Master and all Secondary servers) in the array.
10 JITC INSTALLATIONS

In This Chapter:

208 Introduction
209 Installation Preparation
209 Pre-requisites
209 Deployment Configuration Considerations
209 Antivirus Applications
209 Required Server Components
210 Server Roles and Features
218 Installing Microsoft .NET Framework 4.6
219 Installing Certificates for Encrypted File System (EFS)
219 Installing a CA Signed Certificate
223 Backup and Restore the Certificate File
234 IIS Certificate Bindings
237 Disabling User Account Control Notification
240 For Sites that use Windows Hardening
241 Installing Officelinx for JITC on a Single Server
249 Installing Officelinx for JITC with High Availability
249 Master Voice Server
259 Consolidated Server
267 Secondary Voice Servers
276 JITC Passwords
280 Configuring TLS with Officelinx for SIP
283 Installing Remote CSE Under JITC
290 Installing Remote Web Server Under JITC
Introduction

**Important:** Avaya Officelinx 10.7 and 10.6 has been approved by JITC for all applications.

Avaya Officelinx is available in a version that is certified JITC compliant.

The Joint Interoperability Test Command (JITC) is a certifying agency for I.T. products for the U.S. Department of Defense. Corporations that deal with the various branches of the U.S. government may be required to have their software JITC certified to maintain the highest levels of interoperability, safety and security. JITC certified software has additional layers to help protect the client than non-certified software products.

Avaya Officelinx can be purchased in a JITC certified format which encrypts the database files using FIPS approved encryption. Other security sensitive files and folders within Officelinx are encrypted using Windows EFS. Communications use encrypted TLS (Transport Layer Security) protocols. This keeps all of your data and communications secure. Please contact your reseller for details.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>JITC License for 10.7.</td>
</tr>
<tr>
<td>Software</td>
<td>For details on Officelinx 10.7 Hardware and Software requirements please consult the Technical Operating Guidelines.</td>
</tr>
</tbody>
</table>

**Note:** The steps in this chapter only apply to sites that have purchased a JITC license for Avaya Officelinx. If your site will not use JITC, you can skip this chapter.

When installing Avaya Officelinx version 10.5+, almost all choices regarding program configuration are asked at the beginning so that the many components can be installed without interruption. The only variation that occurs after the initial selection is the PBX and integration type, which will be unique to most sites.

**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:** Avaya Officelinx has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

**Note:** Avaya Officelinx should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Officelinx from functioning properly.

**Caution:** It is strongly recommended that the operating system drive has a minimum of 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Officelinx voice server installation.
Installation Preparation

Pre-requisites

- A JITC specific license for Avaya Officelinx must be purchased.
- JITC installations are only supported on Windows Server 2012 R2 (64-bit).

All other system requirements are the same as for any other Officelinx installation.

Deployment Configuration Considerations

- An Avaya Officelinx server may be installed on the root drive (the same drive where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- An Officelinx server may be installed on a secondary drive (on a different drive from where Windows is installed). This must be a local drive. iSCSI targets are not supported.
- The drives may each be a physical drive (for best performance), or a single drive with partitions.
- The folders \uc\logs, \uc\DB, and \uc\messages may be mounted to a local drive. Network or mapped drives are not supported.
- In an ESX(i)/VMWare environment, SAN/iSCSI is supported, but only at the ESX(i) level. The iSCSI target must be mounted and managed by the ESX(i) host. If a virtual machine is to have a C drive and a D drive, they must be added as a virtual hard disk using the VMWare client.
- The rules for drive types and options are the same for virtual machine environments. The storage must be local, Direct Attached Storage or SAN.

**Warning:** These configurations have been tested and approved by Avaya for use with Officelinx. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

Required Server Components

For Microsoft Windows Server 2012 R2, you must ensure that all the necessary server roles and features are installed on the system before proceeding with Officelinx installation.

For Sites with Hardened Windows

For sites where a hardened version of Windows is to be used, an added step is needed. Install the O/S, then reboot the server and harden the drive. When ready, begin the installation of Officelinx until you reach the section for Disabling User Account Control Notification on page 237, then add the step outlined under For Sites that use Windows Hardening on page 240.

This step is to be performed on all servers, whether in a Single Server install, or at a site running High Availability.
Server Roles and Features

1. From the **Server Manager Dashboard**, click **Add roles and features**.

   ![Server Manager Dashboard](image)

   If this screen is hidden, go to **View** and select **Show Welcome Tile**.

2. Click **Next**.
3. Leave the default settings as they are. Click **Next**.

4. Leave the default settings as they are. Click **Next**.
5. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes. Click **Next**.

**Note:** Throughout this installation, whenever you are prompted to confirm additions, always select **Add Features**.
6. Enable the .NET Framework 3.5 Features checkbox. Click **Next**.

7. Review the information, then click **Next**.
8. Ensure that **HTTP Activation**, under **Windows Process Activation Service Support** is enabled. Click **Next**.

9. On the **Fax Server** screen, click **Next**.
10. On the **Print and Document Services** screen, click **Next**.

11. No changes are required here. Click **Next**.
12. On the Web Server Role (IIS) screen, click Next.


Scroll down to Security, and enable Windows Authentication.


Locate FTP Server and enable FTP Service.

Enable all options under Management Tools > IIS 6 Management Compatibility.

Click Next when ready.
14. Review the selections here. When ready to proceed, click **Install**.

15. If prompted to provide the Windows disk to load the files, click **Specify an alternate source path** and direct it to the appropriate drive.

**Hint:** This is particularly important for virtual machine installations where there may not be a drive configured locally.
16. Windows will now start the installation process for the chosen items. This process may take a while.

![Add Roles and Features Wizard](image.png)

**Note:** This window can be closed without interrupting the installation procedure.

17. Once all changes are complete, **Restart the server**.

### Installing Microsoft .NET Framework 4.6

The Microsoft .NET Framework 4.6 is a required Windows component but it cannot be installed as part of the program package. It must be added by the administrator.

The installer can be downloaded from the Microsoft site here:


Follow the instructions provided to install .NET Framework 4.6 onto the server.
Certificates

Installing Certificates for Encrypted File System (EFS)

Avaya Officelinx requires that signed certificates be installed on all of the servers before attempting an installation. Certificates are used to encrypt security sensitive files on the server. Digital certificates can be purchased from a trusted Certificate Authority (CA), such as GoDaddy™ and Symantec™. Self-signed certificates can be generated using the operating system on the voice server, but this approach is not permitted with JITC installations. A CA signed certificate must be used.

Installing a CA Signed Certificate

A Certifying Authority can issue a certificate to your company. They will provide a file containing the certificate and the password that opens it. Save the file to a known location on the voice server hard drive.

1. Open the Windows Control Panel and select User Accounts.

2. Click Manage your file encryption certificates.
3. Select **A certificate issued by my domain’s certification authority**. Click **Next**.

![Certificate Selection Screenshot](image1)

4. Enable **Backup the certificate and key now**, fill in the path to where the backup file will be saved, and give it a password. Click **Next**.

![Backup Certificate Screenshot](image2)

**Important**: If you are using a different certificate file, make sure to back it up once installation has finished. Instructions can be found in the **Backup and Restore the Certificate File** section.
5. Enable **All Logical Drives**, then click **Next**.

![Image of Encrypting File System dialog](image-url)

6. The files will be encrypted. When it is finished, a result summary will be displayed. Click **Close**.

![Image of Encrypting File System progress and result](image-url)
7. You can verify the success of the installation by opening the `certmgr.msc`. Go to **Personal > Certificates** and verify that the certificate appears under your user name.
Backup and Restore the Certificate File

If you are using a certificate file from another source, or if you have not done so already, you should create a backup copy of the file. If the certificate becomes corrupt, none of your data will be accessible unless the certificate can be restored. This section covers how to backup and restore the certificate file.

Backing-up the Certificate

To create a backup copy of the certificate file...

1. Launch the **Certificate Manager** console in Windows. Right-click the Windows icon and choose **Run**. Enter `certmgr.msc` and hit **OK**.

2. In the left-hand pane, open **Personal > Certificates**. Your certificate(s) will be displayed in the right-hand pane.
3. Right-click the certificate and select **All Tasks > Export**.

4. When the Certificate Export Wizard starts, click **Next**.

5. Enable **Yes, export the private key** and click **Next**.
6. Enable **Export all extended properties**. Choose **Next**.

7. The backup copy of the certificate file requires a password for encryption. Enable **Password**, then enter a password and re-enter to confirm. When ready, click **Next**.

---

**Important**: Record this password and keep it in a safe location. The loss of this password will lead to the complete and unrecoverable loss of data if you ever need to restore the certificate file.
8. Save the file to your hard drive. Click **Next**.

9. All parameters have been configured. Review the settings and click **Finish** when ready.

10. A backup of the certificate file has been successfully created. Click **OK**.

For maximum security, copy the file you just created to another drive (e.g. on another computer, network storage, on a thumb drive, etc.). If the original computer is completely inaccessible, saving the file to another location will still allow you regain access to the system.
Restore the Certificate

To restore the certificate file from a backup...

1. Launch the **Certificate Manager** console in Windows. Right-click the Windows icon and choose **Run**. Enter `certmgr.msc` in the space, then hit **Enter**.

2. In the left-hand pane, the **Personal** folder will be empty. Right-click in the right-hand pane. Select **All Tasks > Import**.

3. When the **Certificate Import Wizard** starts, click **Next**.
4. Locate the backup file and select **Next**.

5. Enter the password that was used to secure the backup file. Enable **Include all extended properties**.

6. Ensure that the restored certificate will be copied to the **Personal** store and click **Next**.
7. The configuration is complete. Review the settings and click **Finish** when ready.

8. The certificate file will be copied onto the operating system of the current computer.

The certificate file has been successfully restored. **Reboot** the server to have the changes take effect.
Import the Certificate on All Servers

**Important:** The following procedure must be completed on all servers in a High Availability installation;

- **Master**, **Consolidated**, and all **Secondary** servers.

1. Login to the server as any user.
2. Right-click **Start > Run** and enter **CMD** to launch the command line editor.

3. At the command line, enter the following inserting your credentials:
   
   ```
   runas /user:computername\UciisUser "mmc certmgr.msc"
   ```
   
   Click **OK**.

   When prompted at the command line, enter the password for the UCIISUser.
   The **Certificate Manager** console will open.

**Important:** The following command must also be run on the Consolidated server only.

```
runas /user:computername\ucAdminUser "mmc certmgr.msc"
```
4. In the left-hand pane, the **Personal** folder will be empty. Right-click in the right-hand pane. Select **All Tasks > Import**.

5. When the **Certificate Import Wizard** starts, click **Next**.

6. Locate the backup file and select **Next**.
7. Enter the password that was used to secure the backup file. Enable **Include all extended properties**.

8. Ensure that the restored certificate will be copied to the **Personal** store and click **Next**.

9. The configuration is complete. Review the settings and click **Finish** when ready.
10. The certificate file will be copied onto the operating system of the current computer.

![Certificate file in Personal store](image)

The certificate file has been successfully restored. **Reboot** the server to have the changes take effect.
IIS Certificate Bindings

To enable an HTTPS connection, another certificate has to be installed in IIS. This certificate must be acquired from a certifying authority.

The HTTPS protocol must be enabled, and HTTP disabled.

1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.

2. Right-click in the right-hand pane and choose Import from the pop-up menu.
3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.

![Import Certificate dialog](image1)

4. Go to **Sites > Default Web Site**. Click **Bindings...**

![Internet Information Services (IIS) Manager](image2)

5. Add the HTTPS binding type. Set the **IP Address** to **All Unassigned**. Leave Port at its default. Change **SSL Certificate** to the certificate name installed above. Click **OK**.

![Add Site Binding](image3)
6. Remove HTTP from the list of bindings. Click Close.
Disabling User Account Control Notification


2. Select Change Account Settings.

On the User Account Control Settings screen, click and drag the slider down to Never Notify.

Click OK and Close.
3. On the keyboard, click the **Start button**, and select **Administrative Tools**.

4. Double-click **Local Security Policy**.
5. Under **Security Settings > Local Policies > Security Options**, double-click **User Account Control: Run all administrators in Admin Approval Mode**.

6. Select **Disabled**. Click **OK**.

7. Reboot the server.

**Note:** UAC Notifications can be restored after Officelinx has been installed.
For Sites that use Windows Hardening

**Warning:** This section only applies to sites that employ Windows Hardening for added security. All other sites can skip this section.

Add this step to the Officelinx installation procedure at the point where you must disable UAC. Apply this procedure on all servers, whether in a Single Server or a High Availability configuration.

1. Go to the **Local Security Policy** window and under **Local Policies > User Rights Assignment**, double-click **Deny access to this computer from the network**.

   ![Screenshot of Local Security Policy window](image1)

2. Highlight **Local account** and click **Remove** to delete that item.

   ![Screenshot of Deny access to this computer from the network](image2)

3. Click **Save** and continue with the Officelinx installation [here](#).

   **Note:** If required, this item can be restored once the Officelinx installation is complete.
Installing Officelinx for JITC on a Single Server

This section covers installing Officelinx in Single Server configuration. If you are planning a High Availability installation, jump to page 249.

Continue with the Avaya Officelinx installation. The presence of a JITC license will be noted during installation and the appropriate files will be loaded. Encryption will be automatically enabled at that time.

Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe as administrator** to install Avaya Officelinx onto your voice server.

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include **Sentinel Protection**, **Microsoft Visual C++ Redistributable** and **Microsoft .Net Framework 4.5**. This process may take a while depending on the required components.

**Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

Click **OK** after entering the necessary credentials.

5. Review all the license agreements and select **I accept the license agreement**.

Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.

**Note**: It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Single UC Server**.

Click **Next**.

**Single UC Server**: When operating Officelinx on a single server computer.

**Multiple UC Servers in High Availability**: When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway**: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select the license type you will using for this installation. Most sites will use the WebLM License option.

**Note:** If you select Officelinx, go to chapter 12, Installing the Officelinx License. When finished, return here and continue the installation from step 11. Skip step 9 through 10.

**Warning:** It is essential that the system/PC clock be properly set before activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

9. The License Upgrade Utility program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   Enter the address in the space provided, then click **OK**.

**Important:** This step requires that the Web License Manager has been installed and configured on the license server computer. See Installing the WebLM License and Server on page 297.
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.

![License Upgrade Utility](image)

**Note:** The number of voice ports is calculated based upon your license.

\[
\text{Number of voice ports} = \left( \frac{\text{# Basic users} + \text{# Mainstream users}}{40} \right) + \text{Number of voice ports in license}
\]

11. Select the **Components** required at your site. Disable any components that are not needed.

Click **Next**.

12. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more required components are **not** installed on the computer.

For all items that are not checked, return to Windows and add any missing pieces to the operating system.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required components have been added to Windows. This screen does not refresh until you click **Next**.
13. This screen shows IIS settings that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished or to refresh the display.

**Note:** The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.

14. Select your PBX Brand then click **Next**.

15. Select your PBX model from the dropdown menu.

Click **Next**.

16. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

**Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.
17. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

18. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of the system.

**Hint:** The password cannot be left blank. It must contain both letters, numbers and characters, and must be at least 15 characters long. See page 276 for a complete list of password requirements.

19. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms. This password must meet the requirements outlined here.

**Important:** Record this password and keep it in a safe location. The loss of this password will lead to the complete and unrecoverable loss of data.

20. The preliminary information required for installation is now complete. Click Next.
21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the **Automatic Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site’s PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration.

   Click **Next** to continue.

25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.

   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.
26. Confirm the information then click **Finish**.

**Note:** Depending on the type of SIP integration you'll be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. Click **Finish** to restart the server.

If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

28. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 223). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

Click **OK** to restart the computer.
Installing Officelinx for JITC with High Availability

This section covers installing Officelinx for JITC in a High Availability (HA) configuration. If you are planning a Single Server installation, jump to page 241.

An HA installation involves up to 21 servers: 1 Master voice server, 1 Consolidated server, and up to 19 Secondary servers. The program must be installed and configured on all 3 types of server. If any of the servers fail, the remaining servers take over with no interruption in service. The multiple server configuration also spreads large traffic loads across many machines to improve performance.

Continue with the Avaya Officelinx installation.

**Important:** The presence of a JITC license will be noted by the Wizard during installation and the appropriate files will be loaded. Encryption will be automatically enabled at that time.

The installation process for each type of server is slightly different and each will be covered separately here:

- Master Voice Server
- Consolidated Server
- Secondary Voice Servers

**Warning:** It is important to login to the servers (Master, Consolidated and all Secondaries) using a domain account that has full administrative rights on the local machine.

Master Voice Server

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that Windows Firewall is disabled, and that Windows Automatic Update is turned off.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.
2. In the extraction folder, run Setup.exe as administrator to install Avaya Officelinx onto the Master server.

![Image of Windows Installer preparing to install]

3. Once the Windows components have been verified, click Next to begin the installation.

   **Note:** The installer will automatically add the necessary components if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the required components.

   **Note:** Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.

4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click OK after entering the necessary credentials.

5. Review the license agreement and select I accept the license agreement.

   Click Next when ready.
6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click Next to continue.

   **Note:** It is highly recommended that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Multiple UC Servers in High Availability**.

   Click Next.

   **Single UC Server:** When operating Officelinx on a single server computer.

   **Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

   **Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.

8. Select **Master Voice Server**.

   Click Next.

9. When prompted, click **Run** to confirm the installation. The necessary files will be installed.

   **Note:** This screen may not appear, depending upon your system settings.
10. Once the process is complete the licensing screen will appear. It is recommended that you use Online Activation whenever possible. To do so, simply enter the **Serial Number** and **Site ID**.

   **Click Request Online Activation when finished.**

   **Warning:** It is essential that the system/PC clock be properly set **before** activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

11. Most of the fields in the **Customer Site Registration** window should already be filled in based upon the license and site numbers entered. Complete the form where necessary (all fields are required).

12. Confirm the contents of your license then click on the **Set as Active License button**.

   **Caution:** Verify that the JITC checkbox has been enabled. If it is empty, pause the installation immediately and contact your dealer. The license must be upgraded **before** you continue.

**Note:** Whenever your license is updated after the initial installation (e.g. through the addition of new features, extensions, etc.) please restart the server after activating the license so that the new parameters can become active.
13. If the process was successful the following confirmation screen will appear.

   Click **OK**.

14. Click **Exit** to close the license window and continue with the installation.

15. This reminder may appear.

   Click **OK**.

16. Select the **Components** required at your site.

   Click **Next**.

17. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

   **Note**: This screen will only appear if one or more required components are **not** installed on the computer.

   For all items that are not checked, return to Windows and add any missing pieces to the operating system.

   Click **Next** when finished.

   **Note**: The installation will not continue until all of the required components have been added to Windows. This screen does not refresh until you click **Next**.

18. This screen shows IIS settings that Officelinx requires to operate properly.

   **Note**: This screen will only appear if one or more of the required settings has not been made on the computer.

   For all items not checked, refer to **IIS Certificate Bindings** for configuration details.

   Click **Next** when finished.

   **Note**: The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.
19. Select your PBX Brand then click **Next**.

20. Select your PBX model from the dropdown menu.

   Click **Next**.

21. Enter the **IP Address** for the Consolidated Server.

   Click **Next**.

22. Enter the number of ports your system will use.

   Click **Next**.
23. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click Next to continue.

**Note:** If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

24. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

25. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms. This password must meet the requirements outlined here.

    **Important:** Record this password and keep it in a safe location. The loss of this password will lead to the complete and unrecoverable loss of data.

26. Enter the values in the spaces provided. These are provided with the certificate (either self-signed or a CA signed).

    These values are used when configuring the certificates on page 279.
27. The preliminary information required for installation is now complete.  
   Click **Next**.

28. The selected components will now be installed. This process may take a while.

29. If you are warned about components being in use, either use the automatic option or manually close the process which is interfering with the installation.
   
   Click **OK** when ready.

30. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.

31. In this section of the installation wizard you will be asked to provide additional settings for SIP integration.
   
   Click **Next** to continue.
32. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

   **Trunk** is selected by default, and is the best option for most installations.
   Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

   Click **Next** when ready.

33. Confirm the information then click **Finish**.

   **Note:** Depending on the type of SIP integration you’ll be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

34. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

35. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

   **Important:** The installation folder **MUST** be shared before proceeding with the Consolidated and Secondary server installations.
36. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 223). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

Click **OK** to restart the computer.
Consolidated Server

Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that Windows Firewall is disabled, and that Windows Automatic Update is turned off.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run Setup.exe as administrator to install Avaya Officelinx onto your Consolidated server.

3. Once the Windows components have been verified, click Next to begin the installation procedure.

Note: The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the required components.

Note: Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

Click **OK** after entering the necessary credentials.

5. Review all the license agreements and select **I accept the license agreement**.

Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.

**Note:** It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Multiple UC Servers in High Availability**.

Click **Next**.

**Single UC Server:** When operating Officelinx on a single server computer.

**Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

**Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google’s Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select **Consolidated Database/File Server**.
   Click **Next**.

9. Enter the **IP address** for the Master voice server.
   Click **Next**.
10. On the C drive, open the **Logs** folder.

Open the file named **icense** using any text editor (e.g. Notepad).

Verify **Highsecurity=1**. If it does not, verify that the same file (OL Installation drive:\UC) on the Master voice server does have this setting. If the setting is valid on the Master, there is a connection or a sharing problem between the two machines. If the Master is not correctly set, contact your reseller for an updated license.

Once any connection or sharing problems have been fixed, return to step 9 and check again for this file.

---

**Caution:** Do not continue the installation until this file has the Highsecurity setting equal to 1.

11. Select the **Components** required at your site.

Click **Next**.
12. This screen shows all of the Windows roles and features that the Consolidated server requires to operate properly.

**Note**: This screen will only appear if one or more required components are not installed on the server.

For all items that are not checked, return to Windows and install any missing pieces into the operating system.

Click **Next** when finished.

**Note**: The installation will not continue until all of the required components have been added to the server. The screen does not refresh until you click **Next**.

13. Select your PBX Brand then click **Next**.

14. Select your PBX model from the dropdown menu.

Click **Next**.

15. Unless the Master Server has been upgraded, enable **No**.

Click **Next**.
16. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of the system.

**Hint:** Passwords cannot be left blank. In a high-security installation, all passwords must contain letters, numbers and characters, and must be at least 15 characters long. See page 276 for a complete list of password requirements.

17. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

18. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms. This password must meet the requirements outlined [here](#).

**Important:** Record this password and keep it in a safe location. The loss of this password will lead to the complete and unrecoverable loss of data.

19. Enter an encryption password to protect Mobilink communications.
20. Enter a password for the Mobilink identity file.
   
   Click **Next**.

21. The preliminary information required for installation is now complete.
   
   Click **Next**.

22. The selected components will now be installed. This process may take a while.

23. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

24. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.
25. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

26. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

   **Important:** The installation folder **MUST** be shared before proceeding with the Consolidated and Secondary server installations.

27. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 223). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

   Click **OK** to restart the computer.
Secondary Voice Servers

Up to 19 Secondary servers can be added to a High Availability environment. Each must be given its own, unique identification number (e.g. 2-20) which is assigned during installation.

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that Windows Firewall is disabled, and that Windows Automatic Update is turned off.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run Setup.exe as administrator to install Avaya Officelinx onto all of your Secondary servers.

3. Once the Windows components have been verified, click **Next** to begin the installation procedure.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 4.5. This process may take a while depending on the required components.

**Note:** Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights. Click **OK** after entering the necessary credentials.

5. Review all the license agreements and select **I accept the license agreement**. Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive. Click **Next** to continue.

   **Note:** It is **highly recommended** that you install the program to a drive other than C to prevent any conflicts or performance issues.

7. Enable **Multiple UC Servers in High Availability**. Click **Next**.

   **Single UC Server:** When operating Officelinx on a single server computer.

   **Multiple UC Servers in High Availability:** When running Officelinx in High Availability mode for redundancy.

   **Officelinx Cloud Gateway:** Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya Officelinx message sync and the CSE. Refer to chapter 14, Install and Configure Cloud Gateway for complete details.
8. Select **Voice Server**.

   Click **Next**.

9. Select the **IP Address** of the Master Voice Server.

   Click **Next**.
10. On the Officelinx installation drive, open the **Logs** folder.

Open the file named **license** using any text editor (e.g. Notepad).

Verify **Highsecurity=1**. If it does not, verify that the same file (OL Installation drive:\UC) on the Master voice server does have this setting. If the setting is valid on the Master, there is a connection or a sharing problem between the two machines. If the Master is not correctly set, contact your reseller for an updated license.

Once any connection or sharing problems have been fixed, return to step 8 and check again for this file.

---

**Caution**: Do not continue the installation until this file has the **HIGHSECURITY** setting equal to 1.

11. Select the **Components** required at your site.

Click **Next**.
12. Select your PBX Brand then click **Next**.

13. Select your PBX model from the dropdown menu.

   Click **Next**.

14. Enter the number for this Secondary Server. Each Secondary must have a unique number assigned between 2 and 20.

   Click **Next**.

15. Enter the **IP Address** for the Consolidated Server.

   Click **Next**.
16. Enter the number of ports your system will use.

   Click Next.

17. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

18. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms. This password must meet the requirements outlined here.

   **Important**: Record this password and keep it in a safe location. The loss of this password will lead to the complete and unrecoverable loss of data.

19. Enter the values in the spaces provided. These are provided with the certificate.

   These values must be the same as are used during the Master voice server installation (step 26).
20. The preliminary information required for installation is now complete.

   Click **Next**.

21. The selected components will now be installed. This process may take a while.

22. If you are warned about components being in use, either use the automatic option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

23. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.

24. In this section of the installation wizard you will be asked to provide additional settings for SIP integration.

   Click **Next** to continue.
25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

**Trunk** is selected by default, and is the best option for most installations. Select **Extension** if it is available through the PBX, and if Pre-Paging is required. If Extension is enabled, enter the **Start Extension Number** established during PBX setup.

Click **Next** when ready.

26. Confirm the information then click **Finish**.

**Note:** Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Officelinx programs folder after installation.

27. Click **Finish** to restart the server.

If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.

28. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

**Important:** The installation folder **MUST** be shared before proceeding with the Consolidated and Secondary server installations.
29. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 223). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

![Reminder]

Click **OK** to restart the computer.
JITC Passwords

More stringent rules for user passwords are also required for a JITC certified installation. These include:

- Passwords must be at least 15 characters long.
- It must include at least one uppercase character (A-Z).
- ...include at least one lowercase character (a-z).
- ...include at least one non-alphabetic character (0-9, !@#$% etc.).
- A passwords must be changed every 60 days.
- No new password can be the same as a previous password extending back 10 iterations.
- The administrator can change the password at any time.
- The client can change their password only once within a 24 hour period.
- A client password can only be changed by the client or the administrator.
- A password cannot contain any personal information, such as names, telephone numbers, birthdates, etc.

These rules are enabled by automatically when installing the JITC compliant edition of Avaya Officelinx. They can also be manually enabled through the OL Admin MMC under Configuration > Advanced.
Logging In

When logging in to Avaya Officelinx applications (i.e. OL Admin, Web Admin), after putting in a correct password, the user is shown the details for the last successful and unsuccessful login attempts through their account. The details include the date and time of the attempt and the IP address of the machine where the attempt was launched.

Review the details as necessary, then click OK to complete the login process and launch the application.
Creating Public and Private Keys

Use the included utility to generate the required public and private keys used by Mobilink services to encrypt data in the synchronization process.

1. On the Master computer, open the drive where Avaya Officelinx has been installed. Open the `Sybase\SQL Anywhere 17\BIN64` folder and run the `createkey` program.

2. At the prompt, enter `2048`, then press Enter.

3. Key in the location where you want the public key to be stored. Include the name of the key. The name MUST be `e2ee_PublicKey2048.pem`. Press Enter.

4. Key in the location where you want the private key to be stored. Include the name of the key. The name MUST be `e2ee_PrivateKey2048.pem`. Press Enter.

5. Enter a password for Mobilink end-to-end encryption and press Enter. The password is the same as the one entered during the Consolidated server installation step 19.

6. Copy the file generated for the public key to the Master voice server, and to all Secondary servers. Paste the file into the `UC\Certificates` folder on the drive where Avaya Officelinx was installed.

   Copy the file generated for the private key to the same folder on the Consolidated server.
Certificates for Mobilink Connection

1. If you are using a self-signed certificate, run the following script from the command prompt to generate the Consolidated server identity and public certificates used by Mobilink services for authentication.

Change the highlighted sections so that they apply to your installation. Enter the same values as were used during the installation of the Master voice server (step 26).

Enter the password you chose for the Consolidated server during installation.

```
createcert -t rsa -b 2048 -sc CA -sst ON -sl Toronto -so "Test Org" -sou "Test OU" -scn "Test Cert" -x -m 0 -v 5 -ca 0 -u 1,3,4,5,6 -co c:\MobilinkPublicCertificate.crt -ko c:\ConsPrivateKey.pem -io c:\ConsolidatedIdentity.pem -kp Abc123def456gh!
```

2. Copy the ConsolidatedIdentity.pem certificate file to the UC\Certificates folder on the Consolidated server to the drive where Avaya Officelinx was installed.

For a certificate provided by a CA, rename the private key file and copy here. The self-signed certificate created in step will already have this name.

3. Copy the MobilinkPublicCertificate.crt certificate file to the UC\Certificates folder on the Master and all Secondary servers to the drive where Avaya Officelinx was installed.

For a certificate provided by a CA, rename the public key file and copy here. The self-signed certificate created in step will already have this name.
Configuring TLS with Officelinx for SIP

After Avaya Officelinx has been installed, modifications must be made to the **ETSIPService.ini** file. This will enable TLS security with the correct settings for use with Officelinx.

The ETSIPService.ini file is located in the **UC/Configuration** folder on the voice server hard drive.

Open it using Notepad or any similar text editor.

Make the necessary changes to the data in the file. If an item is not present, add it to the appropriate section. Create a new section at the end of the file if necessary.
This is an example of additions and changes that can be made to the file. Make the changes required for your site.

```
[PBX1]
Transport protocol=3
Enforce Secure RTP=1

[SIP settings]
Ignore Local Addresses=Yes
TCP Enabled = Yes
TLS IP = 192.168.0.1:5061

[TLS Manager]
FIPS=0

[TLS Server]
Private Key=@sip.key
Certificate=@sip.crt
Certificate Depth=5
Method=2

[TLS Client]
CA Certificates=@BobsCertsClass2Certificate.pem;
Intermediate Certificates=@BobsCertsSecureCertificateAuthority-G2.pem
Certificate Depth=5
Method=2
```

**Key**

**Transport protocol**: Set this value to 3. A TLS IP address must be defined under SIP settings.

**Enforce Secure RTP**: Enter 1 to allow both AVP and SAVP. Setting this to 2 will use secure RTP.

**Ignore Local Addresses**: Allows control of automatic stack binding with all available interfaces. This must be set to Yes when using TLS.

**TCP Enabled**: TCP is required for use with TLS. Set this option to Yes.

**TLS IP**: List all of the TLS local IP addresses for the Officelinx server. The format must be address, colon, port. For example, **IP Address:port**. Separate multiple server addresses in the list using a comma.

**FIPS**: Enables the FIPS module for an OpenSSL library.

**Private Key**: Enter the full path to the private key file (i.e. `c:\security\certificates\sip.key`). Adding the prefix @ will automatically include the path to the Officelinx certificates folder: entering @sip.key expands the path to `C:\UC\Certificates\sip.key` (where C is the drive where Officelinx is installed). The certificate file must be in PEM format.

**Certificate**: Enter the full path to the certificate file (i.e. `c:\security\certificates\sip.crt`). Adding the prefix @ will automatically include the path to the Officelinx certificates folder: entering @sip.crt expands the path to `C:\UC\Certificates\sip.crt` (where C is the drive where Officelinx is installed).

**Certificate Depth**: Defines the depth that an engine will consider legal in a certificate chain (certificates authorizing certificates). The default value is 5.
**Method:** Specify the version of TLS to use. The default value is 2 (TLS 1.2). If your installation requires an earlier version of TLS, change the value accordingly.

<table>
<thead>
<tr>
<th>VALUE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>TLS 1.0</td>
</tr>
<tr>
<td>3</td>
<td>TLS 1.1</td>
</tr>
<tr>
<td>2</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>1</td>
<td>SSL 3.1</td>
</tr>
</tbody>
</table>

**CA Certificates:** Enter the full path to the PEM certificate file. Adding the prefix `@` will automatically include the path to the Officelinx certificates folder. A TLS engine can trust zero, one or more root certificates. Once an engine trusts a root certificate, it will approve all valid certificates issued by that root certificate.

**Intermediate Certificates:** Enter the full path to the PEM certificate file. Adding the prefix `@` will automatically include the path to the Officelinx certificates folder. An engine may hold a certificate that is not issued directly by a root certificate, but by a certificate authority delegated by that root certificate. To add this intermediate certificate to the chain of certificates that the engine will present during a handshake.

**Certificate Depth:** Defines the depth that an engine will consider legal in a certificate chain (certificates authorizing certificates). The default value is 5.

**Method:** Specify the version of TLS to use. The default value is 2 (TLS 1.2). If your installation requires an earlier version of TLS, change the value accordingly.

<table>
<thead>
<tr>
<th>VALUE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>TLS 1.0</td>
</tr>
<tr>
<td>3</td>
<td>TLS 1.1</td>
</tr>
<tr>
<td>2</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>1</td>
<td>SSL 3.1</td>
</tr>
</tbody>
</table>

**Note:** Some sites may require Mutual Certification between the Officelinx voice server and the PBX. To configure this item, copy the Private Key and Certificate elements from TLS Server into the TLS Client section.

```
[TLS Client]
CA Certificates=@BobsCertsClass2Certificate.pem;
Intermediate Certificates=@BobsCertsSecureCertificateAuthority-G2.pem
Certificate Depth=5
Method=2
Private Key=@sip.key
Certificate=@sip.crt
```
Installing Remote CSE Under JITC

When adding a Remote CSE server as part of a High Availability JITC installation, extra steps must be taken. JITC uses encryption to secure data and communications between devices, so this extra layer must be incorporated into the configuration to ensure compliance.

The communications channel between the CSE Server and the Officelinx Servers must be encrypted in a JITC compliant installation. Similarly, the database on the CSE server must also be encrypted for data storage.

**Important**: The presence of a JITC license will be noted by the Wizard during installation and the appropriate files will be loaded. Encryption will be automatically enabled at that time.

Traffic Flow through a Remote CSE Server
Installation Procedure

1. On the computer designated as the Remote CSE Server, open the Avaya Officelinx folder on your server hard drive and run Setup.exe as administrator to launch the installer.

   When prompted, click Next.

2. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click OK after entering the credentials.

3. Review the license agreement. Click Continue, enable the I accept the license agreement checkbox, then click Next.
4. You will be asked to select the destination directory for the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click **Next** to continue.

   **Note**: It is highly recommended that you install the program to a drive other than C to prevent any conflicts or performance issues.

5. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

6. Select **Remote CSE Server (only)** (formerly the Imap TSE Server).

   Click **Next**.

7. Enter a number between 1-25 for this server.

   If you configure multiple CSE servers, each must be given a unique number; no two servers can share the same number.

   Avaya Officelinx supports up to 25 CSE servers.

   Click **Next**.

   **Note**: Each CSE server can support up to 5000 users.
8. Enter the IP Address of the **Master** server.
   
   Click **Next**.

9. On the C drive, open the **Logs** folder.
   
   Open the file named **license** using any text editor (e.g. Notepad).
   
   Verify **Highsecurity=1**. If it does not, verify that the same file (OL
   Installation drive:\UC) on the Master voice server does have this
   setting. If the setting is valid on the Master, there is a connection or a
   sharing problem between the two machines. If the Master is not
   correctly set, contact your reseller for an updated license.
   
   Once any connection or sharing problems have been fixed, return to
   step 9 and check again for this file.

10. Select the **Components** required at your site. Disable any
    components that are not needed.
    
    Click **Next**.

    **Caution**: Do not continue the installation until this file has the Highsecurity setting equal to 1.
11. Enter the IP Address for the **Consolidated** server.

   Click **Next**.

12. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.

   When ready, click **Next**.

13. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.

   This password must meet the requirements outlined [here](#).

**Important**: Record this password and keep it in a safe location. **The loss of this password will lead to the complete and unrecoverable loss of data.**

14. Enter the values in the spaces provided. These are provided with the certificate.

   These values must be the same as are used during the Master voice server installation (step 26).
15. The preliminary information required for installation is now complete.
   
   Click Next.

16. The selected components will now be installed. This process may take a while.

17. Click Finish to restart the server.
   
   If you wish to restart your computer at a later time, disable the Restart check box, then click Finish.

18. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

   **Important:** The installation folder **MUST** be shared before proceeding with the Consolidated and Secondary server installations.
19. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 223). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

Click OK to restart the computer.

The Remote CSE server installation is complete.
Installing Remote Web Server Under JITC

When adding a Remote Web server as part of a High Availability JITC installation, extra steps must be taken. JITC uses encryption to secure data and communications between devices, so this extra layer must be incorporated into the configuration to ensure compliance.

The communications channel between the Web Server and the Officelinx Servers must be encrypted in a JITC compliant installation. Similarly, the database on the Web server must also be encrypted for data storage.

**Important**: The presence of a JITC license will be noted by the Wizard during installation and the appropriate files will be loaded. Encryption will be automatically enabled at that time.

**Installation Procedure**

1. On the computer designated as the Remote Web Server, open the Avaya Officelinx folder on your server hard drive and run `Setup.exe` as administrator to launch the installer.

   When prompted, click **Next**.

2. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.
3. Review the license agreement. Click Continue, enable the I accept the license agreement checkbox, then click Next.

4. You will be asked to select the destination directory for the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click Next to continue.

   Note: It is highly recommended that you install the program to a drive other than C to prevent any conflicts or performance issues.

5. Enable Multiple UC Servers in High Availability.

   Click Next.
6. Select Remote Web Application server (only).
   Click Next.

7. Enter a number between 1-14 for this server.
   If you configure multiple Web servers, each must be given a unique number; no two servers can share the same number.
   Avaya Officelix supports up to 14 Web servers.
   Click Next.

8. Enter the IP Address of the Master server.
   Click Next.
9. On the C drive, open the Logs folder.

Open the file named icense using any text editor (e.g. Notepad).

Verify **Highsecurity=1**. If it does not, verify that the same file (OL Installation drive:\UC) on the Master voice server does have this setting. If the setting is valid on the Master, there is a connection or a sharing problem between the two machines. If the Master is not correctly set, contact your reseller for an updated license.

Once any connection or sharing problems have been fixed, return to step 9 and check again for this file.

---

10. Select the **Components** required at your site. Disable any components that are not needed.

Click **Next**.

---

**Caution**: Do not continue the installation until this file has the Highsecurity setting equal to 1.
11. Enter the IP Address for the **Consolidated** server.

   Click **Next**.

12. Enter and confirm the password for the UCIIS user. This must be the same UCIIS password that was created on the other servers.

13. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.

   This password must meet the requirements outlined [here](#).

---

**Important:** Record this password and keep it in a safe location. The **loss of this password will lead to the complete and unrecoverable loss of data.**
14. Enter the values in the spaces provided. These are provided with the certificate.

These values must be the same as are used during the Master voice server installation.

15. The preliminary information required for installation is now complete.

Click Next.

16. The selected components will now be installed. This process may take a while.

17. Click Finish to restart the server.

If you wish to restart your computer at a later time, disable the Restart check box, then click Finish.
18. This alert is to remind you to properly share the UC installation folder (see page 203 for details).

**Important:** The installation folder **MUST** be shared before proceeding with the Consolidated and Secondary server installations.

19. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 223). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

Click **OK** to restart the computer.

The Remote Web server installation is complete.
11 INSTALLING THE WEBLM LICENSE AND SERVER

Introduction

The Web License Manager (WebLM) is a standard way of implementing feature licensing across various Avaya products. The WebLM program administers your Officelinx license, providing access to all of the mailboxes and features that you are entitled to. If the connection to the WebLM server is interrupted, then Officelinx will revert to demo mode after a grace period (see page 302).

Before installing Avaya Officelinx onto the voice server, the site administrator must designate another computer to act as the license server, and then load the Web License Manager software onto that machine.

Server Specifications

The license server requires the following O/S and software to be installed and configured before proceeding.

<table>
<thead>
<tr>
<th>SOFTWARE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web LM</td>
<td>7+</td>
</tr>
<tr>
<td>Windows Server</td>
<td>2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td>Java</td>
<td>1.8.0.77 64-bit</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>8.0.18.0</td>
</tr>
</tbody>
</table>

Note: Both virtual and physical server types are supported, as well as WebLM on System Manager.
Configuring Web License Manager

1. On the computer designated as the license server, install the WebLM program according to the Avaya documentation.
2. When finished, launch the Web License Manager and login using administrator credentials.

3. Go to the Server properties tab and record the Primary Host ID. This is used to generate an XML license file specific to this machine.

4. Send the Host ID to your vendor, and they will provide the license XML file for your program.
5. Return to WebLM and go to the Install License tab. Enable the Accept License Agreement button. Select Choose file, locate the license XML file on your computer and click Install.
6. Once the license has been installed, you can verify the details of your license from the Licensed products > OL > OL > View License Capacity tab.

7. Record the IP Address for this machine. This is used when installing the license in Officelinx.
Installing the Officelinx License

During the standard installation procedure, when you reach the License Type selection screen:

1. Choose Web LM as the license type.

2. At the prompt, enter the IP address for the server configured in step 7 above. When ready, click OK.

**Hint:** You can close and exit the installation at any time, although the program will operate in demo mode until a license is applied. To add the license information at a later time, or to modify your license with new features, go to Start > Officelinx > UCLicenseWebLM and enter the details.
3. The license screen will be populated by the details shown in step 6.

4. Return to the appropriate installation chapter and step to complete the installation.
Licensing

Soft License

Avaya OfficeLine program authorization is managed through a “soft” license. Activation of the program features and capacity (mailboxes) requires an connection to the license server. OfficeLine will periodically contact the license server to enable continued use of the program at the appropriate service level. If the connection is lost for a long enough period, then the software will fall into Demo Mode until the connection is re-established.

Initial Installation

During the initial installation, the administrator will upload the license XML file onto the license server.

After the initial installation, if the license server hardware changes (i.e. the program has been moved to a new server), OfficeLine will immediately revert to Demo Mode. Contact customer service to reactivate the license.

Normal Operation

Once OfficeLine has been installed and is operating, the program will contact the license server each day for authentication. In the case of a connection failure or other errors that prevent authorization, the program will continue to operate properly for 28 days. If the problems are not corrected and the connection re-established before then, the program will revert to Demo Mode. When errors with authentication do occur, the administrator will receive notifications from OfficeLine with details of the problem.

If the program detects that the license details are different between the OfficeLine and license servers, and no updates have been included, the system will immediately revert to Demo Mode until the issue can be resolved.

In the case where 2 computers are associated with the same license, only the first machine to be authenticated will receive the license. The second machine must wait up to 24 hours for authorization, and only if the first machine has relinquished the license.

License Expiration

Term based licenses last for a specific length of time. As the program nears its termination date, it will begin sending the administrator email reminders that the license is due to expire soon. These messages are sent at 90 days, 60 days, and 30 days prior to expiration. For the last 15 days, notifications will be sent out daily. If the license has not been renewed by the expiration date, the program will continue to operate, but at only 25% of its former capacity. For example, if there were 100 ports and 100 mailboxes licensed, there will now only be 25 ports and 25 mailboxes available on the system. This reduction lasts for 60 days, with reminders sent to the administrator each day, and then OfficeLine will fall into Demo Mode until a new license is purchased.

The program can be reactivated at any time once a new term has been purchased and the license is refreshed. Please make the necessary arrangements in plenty of time to avoid any disruptions in service.

High Availability Licensing

In a High Availability (HA) installation, only the Master connects to the license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Master. Therefore, it is imperative that the Master Server is the first one installed and operating because the other servers will install only the features appropriate to the license data they receive from the Master.
Demo Mode

The program can be put into Demo Mode for many reasons, such as the license expiring, or an extended loss of connection to license server.

Demo Mode maintains all licensed features, but operational capacity is reduced to a single port with 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Officelinx will continue to run in Demo Mode until the cause for the service reduction has been addressed (i.e. a new license is purchased, and fixing any connection problems).

License Expiration Milestones

<table>
<thead>
<tr>
<th>Time Before Expiration</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>+90 days</td>
<td>eMail Administrator</td>
</tr>
<tr>
<td>+60 days</td>
<td>eMail Administrator</td>
</tr>
<tr>
<td>+30 days</td>
<td>eMail Administrator</td>
</tr>
<tr>
<td>+15 days to 0 days</td>
<td>daily eMails to Administrator</td>
</tr>
</tbody>
</table>

**License Expires**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action Taken after Grace Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to authenticate license</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>Upgraded license not activated</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>Hardware changes</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>License Mismatch (not an upgrade)</td>
<td>Demo Mode</td>
</tr>
</tbody>
</table>
12 INSTALLING THE OFFICELINX LICENSE

Introduction

As an alternative to the Avaya WebLM license, Officelinx also operates with a native license process. This option does not require setting up your own corporate license server. It does require an Internet connection to access the Officelinx license server.

Installing the Officelinx License

During the standard installation procedure, when you reach the License Type selection screen:

1. Choose Officelinx as the license type instead of Web LM.

2. When prompted, click Run to confirm the installation. The necessary files will be installed.

   "Note: This screen may not appear, depending upon your Windows operating system and settings."

3. Once the process is complete the licensing screen will appear. It is recommended that you use Online Activation whenever possible. To do so, simply enter the Serial Number and Site ID.

   Click Request Online Activation when finished.

   "Warning: It is essential that the system/PC clock be properly set before activating the license. Any subsequent changes to the clock can adversely affect or terminate the license."
4. Most of the fields in the **Customer Site Registration** window are already filled in based upon the license and site numbers entered. Complete the form where necessary (all fields are required). When ready, click **Submit**.

5. Confirm the contents of your license then click on the **Set as Active License button**.

   **Note:** Whenever your license is updated (e.g. through the addition of new features, extensions, etc.) please restart the server after activating the license so that the new parameters can become active.

6. If the process was successful the following confirmation screen will appear.

   Click **OK**.

7. Click **Exit** to close the license window.

8. Return to the appropriate installation chapter and step to complete the installation.
Licensing

Soft License

Avaya Officelinx program authorization is managed through a “soft” license. Activation of the program (UC, UM, eFax, etc.), capacity (ports and mailboxes) and features (ASR, TTS) requires an Internet connection. Officelinx uses this connection to periodically contact the license server to enable continued use of the program at the appropriate service level. If the connection to the Internet is lost for a long enough period, then the software will fall into Demo Mode until the connection is re-established. Renewing a license, upgrading or adding new features can be completed with a telephone call to customer service and a refreshing of the license.

Initial Installation

During the initial installation, the administrator will enter the Serial Number and Site ID information included with the installation package. These numbers are unique for each site. The program will also generate a hardware profile of the server computer which becomes a part of the license.

After the initial installation, if the server hardware changes (i.e. the program has been moved to a new server), Officelinx will again require an on-line activation with the Site ID and Serial Number to rebuild the license file. This is only permitted once by the software, and subsequent hardware changes will cause the program to immediately revert to Demo Mode. Contact customer service to reactivate the license in this case.

Normal Operation

Once Officelinx has been installed and is operating, the program will contact the license server each day through the Internet for authentication. In the case of a connection failure or other errors that prevent authorization, the program will continue to operate properly for 28 days. If the problems are not corrected and the connection re-established before then, the program will revert to Demo Mode. When errors with authentication do occur, the administrator will receive notifications from Officelinx with details of the problem.

If the program detects that the license details are different between the Officelinx and license servers, and no updates have been included, the system will immediately revert to Demo Mode until the issue can be resolved.

In the case where 2 computers are associated with the same license, only the first machine to be authenticated will receive the license. The second machine must wait up to 24 hours for authorization, and only if the first machine has relinquished the license.

License Upgrades

To upgrade the Officelinx license, such as adding new features or adding more ports or mailboxes, contact your customer service representative. The new details are added to the license server and an email is sent to the administrator with a reminder to refresh the license. The next time that the program contacts the license server for authentication, it will see that the licenses do not match due to the upgrade, and it will prompt the administrator to refresh the license.

To activate the upgrades, run the license activation wizard, verify the updated terms for the license, and click the “Set as Active License” button.

Until the license has been updated, Officelinx will continue to operate at its previous levels for another 28 days, then it will revert to Demo Mode if it has still not been refreshed.
License Expiration

Term based licenses last for a specific length of time. As the program nears its termination date, it will begin sending the administrator email reminders that the license is due to expire soon. These messages are sent at 90 days, 60 days, and 30 days prior to expiration. For the last 15 days, notifications will be sent out daily. If the license has not been renewed by the expiration date, the program will continue to operate, but at only 25% of its former capacity. For example, if there were 100 ports and 100 mailboxes licensed, there will now only be 25 ports and 25 mailboxes available on the system. This reduction lasts for 60 days, with reminders sent to the administrator each day, and then Officelinx will fall into Demo Mode until a new license is purchased.

The program can be reactivated at any time once a new term has been purchased and the license is refreshed. Please make the necessary arrangements in plenty of time to avoid any disruptions in service.

Offline Verification

For sites that do not permit access to the Internet for security reasons, customers can request an installation that uses Offline License Verification. The licensing information resides upon the voice server computer and does not need to be refreshed each day. This installation comes with a hardware USB dongle/key, and a license file that is copied to the hard drive of the voice server. This file contains the hardware profile and licensed feature information that normally resides on the Avaya license server. Both are required for the program to be authorized.

Any hardware changes or program upgrades require a new license file. These are generated by the customer service department and are sent to the customer. Run the license activation routine again to enable updates.

High Availability Licensing

In a High Availability (HA) installation, only the Master connects to the license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Master. Therefore, it is imperative that the Master Server is the first one installed and operating because the other servers will install only the features appropriate to the license data they receive from the Master.

Demo Mode

The program can be put into Demo Mode for many reasons, such as the license expiring, or an extended loss of connection to Avaya’s license server.

Demo Mode maintains all of the previously licensed features, but operational capacity is reduced to a single port with 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Officelinx will continue to run in Demo Mode until the cause for the service reduction has been addressed (i.e. a new license is purchased, and fixing any connection problems).
License Expiration Milestones

<table>
<thead>
<tr>
<th>Time Before Expiration</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>+90 days</td>
<td>eMail Administrator</td>
</tr>
<tr>
<td>+60 days</td>
<td>eMail Administrator</td>
</tr>
<tr>
<td>+30 days</td>
<td>eMail Administrator</td>
</tr>
<tr>
<td>+15 days to 0 days</td>
<td>daily eMails to Administrator</td>
</tr>
<tr>
<td>-1 day to -60 days</td>
<td>Program capacity reduced to 25%</td>
</tr>
<tr>
<td>-61 days and over</td>
<td>Demo Mode</td>
</tr>
</tbody>
</table>

License Expires

<table>
<thead>
<tr>
<th>Condition</th>
<th>Grace Period</th>
<th>Action Taken after Grace Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to authenticate license</td>
<td>28 days</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>Upgraded license not activated</td>
<td>28 days</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>1st Hardware change</td>
<td>-</td>
<td>Refresh license to continue</td>
</tr>
<tr>
<td>2nd Hardware change</td>
<td>-</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>License Mismatch (not an upgrade)</td>
<td>-</td>
<td>Demo Mode</td>
</tr>
</tbody>
</table>

Licensing Grace Periods and Actions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Grace Period</th>
<th>Action Taken after Grace Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to authenticate license</td>
<td>28 days</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>Upgraded license not activated</td>
<td>28 days</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>1st Hardware change</td>
<td>-</td>
<td>Refresh license to continue</td>
</tr>
<tr>
<td>2nd Hardware change</td>
<td>-</td>
<td>Demo Mode</td>
</tr>
<tr>
<td>License Mismatch (not an upgrade)</td>
<td>-</td>
<td>Demo Mode</td>
</tr>
</tbody>
</table>

Changing to WebLM Licensing

Once Officelinx has been installed and is operating with the native license, you can change to WebLM licensing.

**Important:** You must purchase a WebLM license from Avaya before you can convert to the new license. Avaya will provide you with an XML file once it has received the **Host ID** of the **WebLM License Manager**.

**Note:** You cannot change from a WebLM license to an Officelinx native license.

- Reinstall Officelinx from the original executable file. (If prompted, choose **Modify**.)
- Proceed with the installation normally, but when asked which license type to use, select **WebLM License**.

- Enter the settings for your WebLM license server. Refer to chapter 11: **Installing the WebLM License and Server** in this manual for complete details.
- Finish the installation of Officelinx. Be careful not to change any other settings on your system.
Introduction

*Note:* Configuring a site to use TLS communications is optional. It is not required for normal operations.

By default, Avaya Officelinx communicates with the PBX using UDP (User Defined Protocol). This can be enhanced by activating the TLS (Transport Layer Security) if the added security it provides is desirable. This is part of all JITC installations, but is also available to all sites where required.

Architecture

TLS communications are established between the Officelinx voice server(s) and the site PBX. Both ends must be configured to use TLS to make the connection.

For Single Server Installations

Configure the Officelinx server to use TLS.

For High Availability Installations

Configure the *Master* and all *Secondary* servers to use TLS. It is *not* necessary to configure the *Consolidated* server to use TLS since there is no link to the PBX.

Configuring TLS on the PBX

Refer to the hardware documentation for details on configuring your PBX to use TLS.
Configuring TLS with Officelinx for SIP

After Avaya Officelinx has been installed, modifications must be made to the ETSIPService.ini file. This will enable TLS security with the correct settings for use with Officelinx.

The ETSIPService.ini file is located in the UC/Configuration folder on the voice server hard drive.

Open it using Notepad or any similar text editor.

Make the necessary changes to the data in the file.

- Change an existing entry to the value required.
- If the item is not in the file, add it to the appropriate section (shown in [square brackets]).
  Do not create duplicate sections!
- If the section itself does not exist, add a new section to the end of the file and include the value.

[Section Name]
Field Name = Value
This is an example of additions and changes that can be made to the file. Make the changes required for your site.

```
[PBX1]
Transport protocol=3

[SIP settings]
Ignore Local Addresses=Yes
TCP Enabled = Yes
TLS IP = 192.168.0.1:5061,192.168.1.10:5061

[TLS Manager]
FIPS=0

[TLS Server]
Private Key=@sip.key
Certificate=@sip.crt
Certificate Depth=5
Method=2

[TLS Client]
CA Certificates=@CertificateName.pem;
Intermediate Certificates=@CertificateName-G2.pem
Certificate Depth=5
Method=2
```

**Key**

**Transport protocol**: Set this value to 3. A TLS IP address must be defined under SIP settings.

**Ignore Local Addresses**: Allows control of automatic stack binding with all available interfaces. This must be set to **Yes** when using TLS.

**TCP Enabled**: TCP is required for use with TLS. Set this option to **Yes**.

**TLS IP**: List all of the TLS local IP addresses for the Officelinx server. The format must be address, colon, port. For example, `IPAddress:port`. Separate multiple server addresses in the list using a comma.

**FIPS**: Enables the FIPS module for an OpenSSL library.

**Private Key**: Enter the full path to the private key file (i.e. `c:\security\certificates\sip.key`). Adding the prefix @ will automatically include the path to the Officelinx certificates folder: entering @sip.key expands the path to `C:\UC\Certificates\sip.key` (where C is the drive where Officelinx is installed). The certificate file must be in PEM format.

**Certificate**: Enter the full path to the certificate file (i.e. `c:\security\certificates\sip.crt`). Adding the prefix @ will automatically include the path to the Officelinx certificates folder: entering @sip.crt expands the path to `C:\UC\Certificates\sip.crt` (where C is the drive where Officelinx is installed).

**Certificate Depth**: Defines the depth that an engine will consider legal in a certificate chain (certificates authorizing certificates). The default value is 5.
**Method:** Specify the version of TLS to use. The default value is 2 (TLS 1.2). If your installation requires an earlier version of TLS, change the value accordingly.

<table>
<thead>
<tr>
<th>VALUE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>TLS 1.0</td>
</tr>
<tr>
<td>3</td>
<td>TLS 1.1</td>
</tr>
<tr>
<td>2</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>1</td>
<td>SSL 3.1</td>
</tr>
</tbody>
</table>

**CA Certificates:** Enter the full path to the PEM certificate file. Adding the prefix @ will automatically include the path to the Officelinx certificates folder. A TLS engine can trust zero, one or more root certificates. Once an engine trusts a root certificate, it will approve all valid certificates issued by that root certificate.

**Intermediate Certificates:** Enter the full path to the PEM certificate file. Adding the prefix @ will automatically include the path to the Officelinx certificates folder. An engine may hold a certificate that is not issued directly by a root certificate, but by a certificate authority delegated by that root certificate. To add this intermediate certificate to the chain of certificates that the engine will present during a handshake.

**Certificate Depth:** Defines the depth that an engine will consider legal in a certificate chain (certificates authorizing certificates). The default value is 5.

**Method:** Specify the version of TLS to use. The default value is 2 (TLS 1.2). If your installation requires an earlier version of TLS, change the value accordingly.

<table>
<thead>
<tr>
<th>VALUE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>TLS 1.0</td>
</tr>
<tr>
<td>3</td>
<td>TLS 1.1</td>
</tr>
<tr>
<td>2</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>1</td>
<td>SSL 3.1</td>
</tr>
</tbody>
</table>

**Note:** Some sites may require **Mutual Certification** between the Officelinx voice server and the PBX. To configure this item, copy the **Private Key** and **Certificate** elements from TLS Server into the TLS Client section.

```plaintext
[TLS Client]
CA Certificates=@CertificateName.pem;
Intermediate Certificates=@CertificateName-G2.pem
Certificate Depth=5
Method=2
Private Key=@sip.key
Certificate=@sip.crt
```
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>316</td>
<td>Introduction</td>
</tr>
<tr>
<td>316</td>
<td>Pre-requisites</td>
</tr>
<tr>
<td>316</td>
<td>Windows Configuration</td>
</tr>
<tr>
<td>317</td>
<td>Installation</td>
</tr>
<tr>
<td>324</td>
<td>Configuring Officelinx</td>
</tr>
</tbody>
</table>
Introduction

Setting up a Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya Officelinx message sync and the CSE.

Pre-requisites

The Avaya Aura Messaging server must be installed, properly configured and working before proceeding with the Officelinx installation.

Windows Configuration

Add all of the necessary Roles and Services to the Officelinx server for your version of Windows. Install all required Windows components and certificates onto the server. Consult the appropriate chapter of this document for complete details regarding the configuration of your version of Windows.

Return here when you are ready to install Avaya Officelinx.
Installation

**Note:** Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update is turned off**.

1. Download the installation file (see chapter 3). Run the file (double-click) to extract the contents. Specify the location on your hard drive where you want to save the files.

2. In the extraction folder, run **Setup.exe** to install Avaya Officelinx onto your voice server.

3. Once the Windows components have been verified, click **Next** to begin the installation.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include **Sentinel Protection**, **Microsoft Visual C++ Redistributable** and **Microsoft .Net Framework 4.5**. This process may take a while depending on the required components.

**Note:** Clicking on the **Documentation** button will provide you with the default set of PDF documents which comprehensively cover most aspects of Officelinx.
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click **OK** after entering the necessary credentials.

5. Review all the license agreements and select **I accept the license agreement**.

   Click **Next** to continue.

6. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click **Next** to continue.

7. Enable **Officelinx Cloud Gateway**.

   Click **Next**.
8. When prompted, click **Run** to confirm the installation. The necessary files will be installed.

   ![Sentinel Protection Installer 7.3.2](image)

**Note:** This screen may not appear, depending upon your Windows operating system and settings.

9. Once the process is complete the licensing screen will appear. It is recommended that you use Online Activation whenever possible. To do so, simply enter the **Serial Number** and **Site ID**.

   ![License-Activation](image)

   Click **Request Online Activation** when finished.

**Warning:** It is essential that the system/PC clock be properly set **before** activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

10. Most of the fields in the **Customer Site Registration** window should already be filled in based upon the license and site numbers entered. Complete the form where necessary (all fields are required).
11. Confirm the contents of your license then click on the **Set as Active License button**.

**Note:** Whenever your license is updated (e.g. through the addition of new features, extensions, etc.) please restart the server after activating the license so that the new parameters can become active.

12. If the process was successful the following confirmation screen will appear.

   Click **OK**.

13. Click **Exit** to close the license window and continue with the installation.

14. Select the **Components** required at your site. Disable any components that are not needed.

   Click **Next**.

15. This screen shows all of the Windows roles and features that Officelinx requires to operate properly.

   **Note:** This screen will only appear if one or more required components are **not** installed on the computer.

   For all items that are not checked, return to Windows and add any missing pieces to the operating system.

   Click **Next** when finished.

   **Note:** The installation will not continue until all of the required components have been added to Windows.

   This screen does not refresh until you click **Next**.
16. This screen shows IIS settings that Officelinx requires to operate properly.

**Note:** This screen will only appear if one or more of the required settings has not been made on the computer.

For all items that are not checked, return to the IIS Manager in Windows and set these options as required.

Click **Next** when finished.

**Note:** The installation will not continue until all of the required IIS settings have been made. This screen does not refresh until you click **Next**.

17. Select your PBX Brand then click **Next**.

18. Select your PBX model from the dropdown menu.

   Click **Next**.

19. Select the **Email Server Type** from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.
20. Enter the primary location from which most telephone calls will be placed. This will normally be where the corporate office is situated. Additional dialing locations and rules may be defined after the installation is complete.

Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.

**Note**: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

21. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

22. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of the system.

**Hint**: The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

23. The preliminary information required for installation is now complete.

Click **Next**.
24. The selected components will now be installed. This process may take a while.

25. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.

   Click **OK** when ready.

26. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site’s PBX exactly as required.

27. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box then click **Finish**.
Configuring Officelinx

1. Open Avaya Aura Messenger. Identify an administrator account, or create a new one, that has superuser access to all mailboxes. This account will be used to manage message synchronization between Aura and Officelinx.

2. On the voice server, open the Officelinx Admin program. Login using the administrator password created during program installation.

3. From UC Admin, open the **Message Sync Source** menu. Right-click in the right-hand pane and select **New > Message Sync Source** from the pop-up menu.

4. Enter the details of the AAM server in the spaces provided.

   - **Name**: Enter a user friendly name for the connection. This will be used later.
   - **Address**: Enter the IP address for the AAM System Manager server.
   - **Port**: Configure the port value to **993**.
   - **Voice Format**: Set the Voice Format field used by your network.
   - **Domain**: Enter the domain name of the AAM Server.
5. Under the PBX, open the company menu and select **Feature Group**.

![Feature Group](image)

6. Open a Feature Group in the right-hand pane and go to the Synchronization Options tab.

7. Add AAM superuser credentials to the **Message Sync Source Settings** fields.

   - **Account**: Enter the account name configured for superuser access.
   - **Message Sync Source**: Type in the name of the Sync Source created in step 4.
   - **Password / Confirm Password**: Put the password for the account in these two spaces.

8. Configure the CSE server settings according to your site requirements. Complete instructions can be found in the Server Configuration Guide chapter Understanding CSE.

9. Restart the following services: UC CSE Service, UC CSE PIM SYNC Service, UC Aura Service. You can also reboot the server.

10. Verify the gateway connection by sending an email to a mailbox on the AAM server. If the connection is working, the email will also appear in the corresponding Gmail account inbox.
15

AVAYA OFFICELINX 7.X TO 10.7 UPGRADE

In This Chapter:

328 Single Server
328 Preparation
329 Updating the Database to 7.1
332 Migration Procedure (SIP)
334 Migration Procedure: Dialogic or Mitai (non-SIP)
336 Upgrading a High Availability Installation
Single Server

A direct upgrade to Officelinx 10.7 from version 7.x and earlier is not supported due to changes in operating system and database requirements.

To upgrade an older system, it is necessary to install Officelinx 10.7 on a new computer, and then to migrate the data across from the old machine.

Please refer to the appropriate chapter in this document for further details on database and message migration.

Quick Start:

1. Install Avaya Officelinx 10.7 onto a new computer. The new computer must meet the minimum requirements for 10.7. This includes the limitations on operating system (i.e. Windows XP is no longer supported).
2. Copy the database, log, message and prompt files from the old machine to the appropriate location on the new one.
3. Run the database migration utility included on the program DVD.

Preparation

Backup

It is strongly recommended that you back up certain files from the \UC folder on the old system before starting the migration. The following folders should be backed up to a safe location:

- C:\UC\DB
- C:\UC\Messages
- C:\UC\Prompts

Note: Close all Server-related programs (i.e. OL Admin, UM Monitor).

Avaya Officelinx Installation

Before migrating the data from the old server, Avaya Officelinx must be installed on the new server(s). For more information on installing Officelinx, consult the appropriate chapter for your operating system in this guide.

- Windows Server 2008 on page 111.
- Windows Server 2008 R2 on page 85
- Windows Server 2012 on page 57.
- Windows 7 on page 137.
- Windows 8 on page 119.
- High Availability on page 157.

Stop Officelinx Processes

While the migration tool is designed to stop most of the necessary services and inform you of any other requirements during the process, the best practice is to manually stop all Officelinx related services and applications before continuing with the installation.
Updating the Database to 7.1

Caution: This section does NOT apply to High Availability installations. It is for Single Server sites only.

To migrate a database to 10.7, you must first ensure that your existing database is at least at the 7.1 version. Follow these steps to update your database to 7.1.

1. In a web browser, go to https://accounts.zang.io. Create a new account (Get Started), or login using your existing credentials. You can also login using your Google+, Salesforce, or Office 365 account details.

2. On the Dashboard, select Edit Profile.
3. From the Downloads tab, choose the version of Officelinx you want to download. Click the download icon beside the program.

4. Specify the location on your voice server hard drive where you want to save the file.

5. The saved file is a self-extracting executable (.exe) file. Run the file (double-click) to extract the contents to the hard drive. Specify the location on your hard drive where you want to extract the files.

6. In the extraction folder, locate the **DBMigration\Pre91DBUpdate.EXE** file and copy it to your old system drive, placing it in the \UC\DB folder.

7. Double-click on the **Pre91DBUpdate.EXE** file to launch the pre-migration utility.

   Click **Next** to continue.

8. The application will stop all of the necessary services before proceeding.
9. You will be prompted when the application is ready to start the conversion process.
   Click **Next** to continue.

10. Your database will now be updated.
    
    **Note:** This process may take some time depending on the size of your database. Please be patient.

11. Once the process is complete, the application will validate the conversion. This process may also take a long time depending on the size of your database. Please be patient.

12. You will see this screen when the process has completed.
    
    Click **Finish** to exit the application.
Migration Procedure (SIP)

Caution: If your current system is not SIP compatible, use the Non-SIP (Dialogic or Mitai) Migration Procedure on page 334 instead.

Once all of the preparations have been made, and the database has been updated to 7.1 (where applicable), proceed with the migration of the data files to the new Officelinx 10.7 server.

1. Copy the DB (EEAM20.DB) file and LOG (EEAM20.LOG) file from the \UC\DB\ folder of your old server to the same folder on the 10.7 system.

To keep the same Company Salutation, Personal Prompts or Messages from the old system, copy those files to the appropriate folders on the new system: Messages should be copied to the new 10.7 system’s Messages folder (c:\uc\messages\), personal prompts to the prompts folder (c:\uc\prompts\) and so on.

Note: For Company Salutations, the name of the file must be unique since the new 10.7 system already has existing salutations. If there is a conflict between file names, you must rename/renumber the previous system’s files before copying them into the 10.7 folders. Please keep in mind that changing the file names may cause your old DB to use incorrect salutations. You must manually change the salutations from the Admin Console after migration to resolve the issue.

2. From the installation DVD, copy the Migration Utility (71_to_91Migration_Utility.EXE) file to the \UC\DB\ folder on the new server.

3. Run (double-click) the application that you have just copied. The Migration Utility Wizard will start.

   Click Next to continue.

4. Ensure that the Run conversion utility... checkbox is disabled.

   Click Next.

5. The application will stop the necessary services before proceeding.
6. Your database will first be unloaded to prepare for the migration. This process may take a while depending on the size of your database. Please be patient.

7. Once the unload process is complete, the application will migrate the database. This process may take a while depending on the size of your database. Please be patient.

8. Files will be moved and replaced accordingly.

9. You will see this screen when the process has completed. Click **Finish** to exit the Migration Wizard.

10. When prompted, click **OK** to restart your computer.
The old database is now ready to be used with the new 10.7 system.
Migration Procedure: Dialogic or Mitai (non-SIP)

**Caution:** If your current system is SIP compatible, use the SIP Migration Procedure on page 332 instead.

Once all of the preparations have been made, and the database has been updated to 7.1 (where applicable), proceed with the migration of the data files to the new Officelinx 10.7 server.

1. Copy the DB file and LOG file from the \UC\DB\ folder of your old server to the same folder on the 10.7 system.

To keep the same Company Salutation, Personal Prompts or Messages from the old system, copy those files to the appropriate folders on the new system: Messages should be copied to the new 10.7 system's Messages folder (c:\uc\messages\), personal prompts to the prompts folder (c:\uc\prompts\) and so on.

**Note:** For Company Salutations, the name of the file must be unique since the new 10.7 system already has existing salutations. If there is a conflict between file names, you must rename/renumber the previous system’s files before copying them into the 10.7 folders. Please keep in mind that changing the file names may cause your old DB to use incorrect salutations. You must manually change the salutations from the Admin Console after migration to resolve the issue.

2. From the installation DVD, copy the Migration Utility (71_to_91Migration_Utility.EXE) file to the \UC\DB\ folder on the new server.

3. Run (double-click) the application that you have just copied. The Migration Utility Wizard will start.

   Click **Next** to continue.

4. Ensure that the checkbox is enabled if you wish to convert your voice files as well.

   Click **Next**.

5. The application will stop the necessary services before proceeding.

6. Your database will first be unloaded to prepare for the migration. This process may take a while depending on the size of your database. Please be patient.
7. Once the unload process is complete, the application will migrate the database. This process may take a while depending on the size of your database. Please be patient.

8. Files will be moved and replaced accordingly.

9. Once the database is ready, your Company Salutation, Personal Prompts and Messages can be converted.

   Select the **Company** which the salutations belong to from the Company drop down menu.

   From **Convert To** menu, select the target voice format.

   Select the type of voice files to convert with the checkboxes.

   Click **Start** to begin the conversion.

10. You will see this screen when the process has completed.

    Click **Finish** to exit the Migration Wizard.

11. When prompted, click **OK** to restart your computer.

    The old database is now ready to be used with the new 10.7 system.
Upgrading a High Availability Installation

When upgrading an HA installation from 7.1 SP4 to 10.7, **each** of the component servers (Master, Consolidated, all Secondaries) must be upgraded individually.

**Note:** For HA installations older than 7.1 SP4, the system must first be upgraded to SP4 before migrating to 9.1.

Create a new server for each of the servers on the old system, then follow the SIP migration procedure outlined above on each of these machines to move the data across.

For HA installations, use **SP4To91Migration_Utility.EXE** instead of the **71_to_91Migration_Utility.EXE** file.
In This Chapter:

338 Introduction
338 Requirements
338 Upgrade Preparation
338 Backup
338 Stop Officelinx Processes
339 8.5 SP2+ to 10.7 Upgrade Installation
Introduction

Upgrading an Avaya Officelinx version 8.5 SP2 and later to 10.7 is a very simple process which may be completed quickly for most sites.

However, please keep in mind that this manual is only meant to provide an overview of the process and is not an exact step-by-step guide. Since all sites vary in configuration you must take that into consideration and ensure that you approach the upgrade process dynamically rather than to fully rely on this manual.

Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Existing 8.5 SP2 or later license</td>
</tr>
<tr>
<td>Software</td>
<td>Avaya Officelinx 10.7 Hardware and Software requirements differ from previous versions. Please consult the Technical Operating Guidelines for detailed information.</td>
</tr>
</tbody>
</table>

Upgrade Preparation

Backup

It is suggested that the User back up certain files in the C:\UC folder on the system before beginning the upgrade. The following folders must be backed up:

- C:\UC\DB
- C:\UC\Messages
- C:\UC\Prompts

*Note: Take care to refer to Internet Information Services (IIS) on your PC and ensure that the FTP server is installed and running. Also, close all Server-related programs (i.e. UM Admin, UM Monitor).*

Stop Officelinx Processes

While the upgrade process is designed to stop most of the necessary services and inform you of any other requirements, the best practice is to manually stop all of the following Officelinx related services and applications before continuing the installation.

- SQL Anywhere-ASADB_UC
- EEFaxService
- IMAP Server
- UC Voice Server
- UC TSE Cache Manager
- Unified Messaging System Tasks Service
- VPIM Server
- World Wide Web Publishing Service
8.5 SP2+ to 10.7 Upgrade Installation

**Note:** If you have Autorun disabled on your system, please browse into the DVD and double-click the `InstallUC.bat` file to begin the upgrade process.

1. Insert the Avaya Officelinx installation DVD into the DVD drive. The following screen will appear.

**Note:** The installer will automatically install the necessary packages at the beginning of the installation if they do not already exist on the system. These packages may include Sentinel Protection, Microsoft Visual C++ Redistributable and Microsoft .Net Framework 3.5. This process may take a while depending on the required components.

2. Once the Windows components have been verified, the following screen will appear.

   Click **Next** to begin the installation procedure.

   **Note:** Clicking on the Documentation button will provide you with the default set of PDF documents which comprehensively cover most aspects of Avaya Officelinx.

3. If the installer determines that the administrator password is not sufficiently secure (e.g. 1111), this screen will appear requiring it to be changed.

   The password cannot be left blank, it must contain both letters and numbers, and should be at least 6 characters long.
4. The preliminary information required for installation is now complete. Click **Next**.

5. When the migration and other related configurations are complete, you will see the following screen. Click **Finish** to complete the installation.

6. You must restart the server to finish the installation. Click **OK** to restart. If you wish to restart your computer at a later time, click **Cancel**.
17 DATABASE MIGRATION TOOL

In This Chapter:

342  Introduction
342  Requirements
343  Preparation
343  Backup
343  Officelinx Installation
343  Stop Officelinx Processes
344  Migration Procedure (SIP)
Introduction

Many users of Officelinx may opt to upgrade their hardware while upgrading the software. Unlike a simple upgrade, a migration also involves moving the Officelinx server to a different computer in addition to updating the software. To support these customers, a database migration tool is available on the Officelinx version 10.7 installation DVD.

Regardless of what version of Avaya Officelinx you are starting from, the migration procedure is largely the same. Extra steps specific to a certain version are added where indicated.

**Warning:** Officelinx 8.5 SP1 and earlier cannot be upgraded directly and must be migrated to a new machine.

<table>
<thead>
<tr>
<th>Single Server (SS)</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current version 8.5 SP2 and later (SS) updating to 10.7 (SS)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Availability (HA)</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current version 8.5 SP2 and later (HA) updating to 10.7 (HA)</td>
<td></td>
</tr>
<tr>
<td>Current version 8.5 SP2 and later (SS) updating to 10.7 (HA)</td>
<td></td>
</tr>
</tbody>
</table>

**Warning:** The database update and migration process may take a long time to complete (up to several hours) depending upon the size of the database. Please ensure that you allocate enough time for this procedure.

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>Existing 8.5 SP2 and later system with proper database and New 10.7 software and license</td>
</tr>
</tbody>
</table>

If your system is of an older version, you will first have to update the database to the 7.1. Once this has been done, you will be able to convert it into the 10.7 format, allowing you to use the database on your newly installed 10.7 system on the new hardware.
Preparation

Backup

It is strongly recommended that you back up certain files from the \UC folder on the old system before starting the migration. The following folders should be backed up to a safe location:

- C:\UC\DB
- C:\UC\Messages
- C:\UC\Prompts

**Note:** Check the Internet Information Services (IIS) on your PC to ensure that the FTP Server is installed and running.

**Note:** Close all Server-related programs (i.e. OL Admin, UM Monitor).

Officelinx Installation

Before migrating the data from the old server, Officelinx must be installed on the new server(s). For more information on installing Officelinx, consult the appropriate chapters in this guide.

- Windows Server 2008 on page 111.
- Windows Server 2008 R2 on page 85
- Windows Server 2012 on page 57.
- Windows 7 on page 137.
- High Availability on page 157.

Stop Officelinx Processes

While the migration tool is designed to stop most of the necessary services and inform you of any other requirements during the process, the best practice is to manually stop all Officelinx related services and applications before continuing with the installation.
Migration Procedure (SIP)

Once all of the preparations have been made, and the database has been updated to 7.1 (where applicable), proceed with the migration of the data files to the new Avaya Officelinx 10.7 server.

1. On the new server, stop all Officelinx services, then delete the **EEAM21.db** and **EEAM21.log** files found in the **UC\DB** folder.
   Also delete any transaction log files in this directory. Transaction logs have a name similar to **140504AA.log**.
2. Copy the **DB** file and **LOG** file from the **UC\DB\** folder of the old server to the same folder on the 10.7 system.
   Use the following table to determine the file names you need to copy.

<table>
<thead>
<tr>
<th>Officelinx Version</th>
<th>DB File Name</th>
<th>LOG File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior to 8.0</td>
<td>EEAM20.DB</td>
<td>EEAM20.LOG</td>
</tr>
<tr>
<td>8.0 and later</td>
<td>EEAM21.DB</td>
<td>EEAM21.LOG</td>
</tr>
</tbody>
</table>

To keep the same **Company Salutation**, **Personal Prompts** or **Messages** from the old system, copy those files to the appropriate folders on the new system: Messages should be copied to the new 10.7 system's Messages folder (**c:\uc\messages\**), personal prompts to the prompts folder (**c:\uc\prompts\**) and so on.

**Note**: For Company Salutations, the name of the file must be unique since the new 10.7 system already has existing salutations. If there is a conflict between file names, you must rename/renumber the previous system's files before copying them into the 10.7 folders. Please keep in mind that changing the file names may cause your old DB to use incorrect salutations. You must manually change the salutations from the Admin Console after migration to resolve the issue.

3. From the installation DVD, copy the **Migration Utility** file to the **UC\DB\** folder on the new server.
   Use the following table to determine the specific utility file to use.

<table>
<thead>
<tr>
<th>Old Officelinx Version</th>
<th>Type</th>
<th>Migration Utility File</th>
</tr>
</thead>
<tbody>
<tr>
<td>OL 10.7</td>
<td>SS &amp; HA</td>
<td>Migration_Utility.EXE</td>
</tr>
<tr>
<td>OL 8.5+ SS</td>
<td>HA</td>
<td>SingleServerToHAMigration_Utility.EXE</td>
</tr>
<tr>
<td>OL 8.5+</td>
<td>SS &amp; HA</td>
<td>MigrationUtility_RebuildDatabase.exe</td>
</tr>
</tbody>
</table>

1 - Run this utility on all voice servers in the HA array; Master, Consolidated, and all Secondaries.
2 - The server migrated through using this utility will become the Master server on the new HA system. The Consolidated and Secondary servers will all be fresh installs; no migration is required.
4. Run (double-click) the application that you have just copied. The Migration Utility Wizard will start.  
   Click **Next** to continue.

5. Ensure that the **Run conversion utility...** checkbox is disabled.  
   Click **Next**.

6. The application will stop the necessary services before proceeding.

7. Your database will first be unloaded to prepare for the migration. This process may take a while depending on the size of your database. Please be patient.

8. Once the unload process is complete, the application will migrate the database. This process may take a while depending on the size of your database. Please be patient.

9. Files will be moved and replaced accordingly.

10. You will see this screen when the process has completed.  
    Click **Finish** to exit the Migration Wizard.
11. When prompted, click **OK** to restart your computer.

The old database is now ready to be used with the new 10.7 system.
DEDICATED CSE SERVER INSTALLATION

In This Chapter:

- Introduction 348
- Requirements 348
- Dedicated CSE Server Installation 349
- Configuration For Remote TSE server installations 354
- Configuration For Remote TSE server installations 354
Introduction

Due to a physical limitations on the server for the number of users who utilize the UC function, you must install additional dedicated CSE servers in order to increase the limit of UC users. The dedicated CSE server will handle CSE related jobs relieving the voice server of these tasks. In order to add a dedicated TSE server to your system please follow the instructions in this document accurately.

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>Existing Avaya Officelinx system to integrate with.</td>
</tr>
</tbody>
</table>
Dedicated CSE Server Installation

1. On the computer designated as the Remote CSE Server, open the Avaya Officelinx folder on your server hard drive or the Officelinx DVD and run Setup.exe to launch the installer.

   When prompted, click **Next**.

2. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.

3. Review the license agreement. Click **Continue**, enable the **I accept the license agreement** checkbox, then click **Next**.

   ![Image of license agreement](image-url)
4. You will be asked to select the destination directory for the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.

5. Enable **Multiple UC Servers in High Availability**.

Click **Next**.

6. Select **Remote CSE Server (only)** (formerly the Imap TSE server).

Click **Next**.

7. Enter a number between 1-25 for this server.

If you configure multiple CSE servers, each must be given a unique number; no two servers can share the same number.

Avaya Officelinx supports up to 4 CSE servers.

Click **Next**.

**Note:** Each CSE server can support up to 5000 users.
8. Enter the IP Address of the **Master** server.
   Click **Next**.

9. Select the **Components** required at your site. Disable any components that are not needed.
   Click **Next**.

10. Unless the Master Server has been upgraded from a Single Server configuration, choose **No**.
    Click **Next**.

11. Enter the IP Address for the **Consolidated** server.
    Click **Next**.
12. Select the Email Server Type from the list of available options. This allows the system to set basic parameters which help to improve performance and reliability.

When ready, click Next.

13. The preliminary information required for installation is now complete.

Click Next.

14. The selected components will now be installed. This process may take a while.

15. Click Finish to restart the server.

If you wish to restart your computer at a later time, disable the Restart check box, then click Finish.
16. This alert is to remind you to properly share the UC installation folder.

Click OK to restart the computer
(see page 203 for details).

The Remote CSE server installation is complete.
Configuration For Remote TSE server installations

Once you have finished configuring the dedicated TSE server, you must configure your voice server to finalize the changes.

1. On the Consolidated and the Remote TSE servers, locate the CSE.EXE config file in the UC/UCCSE folder. Edit the file using Notepad or similar text editor.

   Locate the entry for `<setting name="Primary Instance">`. Ensure that the value is False. Change the value if necessary, then Save the file.

2. On both of the Consolidated and the Remote TSE servers, open the Registry.

   Right-click the Start menu, select Run and enter regedit in the space provided. Click OK.

   On 64-bit operating systems, scroll down to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Generic\UMS\IMAPTSE\Cache.

   On 32-bit operating systems, scroll down to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache.

   Verify that the value for Primary is 0.

3. Restart the server to complete the configuration changes.
4. Open a Feature Group in the OL Admin program. On the Synchronization Options tab, in the TSE Location text field, type in the computer name of the Remote CSE or the Consolidated servers.

5. From Control Panel > Administrative Tools > Services make sure that the UC TSE Manager service on the voice server is set to Disabled. If this service is running on the voice server, it will interrupt the dedicated CSE server.
DEDICATED WEB SERVER INSTALLATION

In This Chapter:

358 Introduction

359 Dedicated Web Server Installation

362 The Remote Web server installation is complete.

362 The Remote Web server installation is complete.
Introduction

The Dedicated Web Server allows you to separate web portions of Avaya Officelinx from the voice server so that you to balance the work load on each system and facilitate a customized network environment. Most web related Officelinx features, such as Web Client or UC Gadgets will all be available from the dedicated web server.

**Warning:** You must have IIS installed and running on your operating system in order for the Dedicated Web Server to function. You may refer to below sections for details regarding IIS requirements.

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>Existing Avaya Officelinx system to integrate with IIS installed on the OS.</td>
</tr>
</tbody>
</table>
Dedicated Web Server Installation

1. On the computer designated as the Remote Web Server, open the Avaya Officelinx folder on your server hard drive or the Officelinx DVD and run Setup.exe to launch the installer.

   When prompted, click Next.

2. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click OK after entering the credentials.

3. Review the license agreement. Click Continue, enable the I accept the license agreement checkbox, then click Next.
4. You will be asked to select the destination directory for the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

   Click Next to continue.

5. Enable Multiple UC Servers in High Availability.

   Click Next.

6. Select Remote Web Application server (only).

   Click Next.

7. Enter a number between 1-14 for this server.

   If you configure multiple Web servers, each must be given a unique number; no two servers can share the same number.

   Avaya Officelinx supports up to 14 Web servers.

   Click Next.
8. Enter the IP Address of the Master server.
   Click Next.

9. Select the Components required at your site. Disable any components that are not needed.
   Click Next.

10. Unless the Master Server has been upgraded from a Single Server configuration, choose No.
    Click Next.

11. Enter the IP Address for the Consolidated server.
    Click Next.
12. The preliminary information required for installation is now complete.

   Click **Next**.

13. The selected components will now be installed. This process may take a while.

14. Click **Finish** to restart the server.

   If you wish to restart your computer at a later time, disable the **Restart** check box, then click **Finish**.

15. This alert is to remind you to properly share the UC installation folder.

   Click **OK** to restart the computer (see page 203 for details).

The Remote Web server installation is complete.
## 20 LANGUAGE PACK INSTALLATION

In This Chapter:

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>364</td>
<td>Introduction</td>
</tr>
<tr>
<td>364</td>
<td>Available Languages</td>
</tr>
<tr>
<td>365</td>
<td>Upgrade Preparation</td>
</tr>
<tr>
<td>365</td>
<td>Backup</td>
</tr>
<tr>
<td>365</td>
<td>Stop Officelinx Processes</td>
</tr>
<tr>
<td>365</td>
<td>Downloading the Files</td>
</tr>
<tr>
<td>366</td>
<td>Language Pack Installation</td>
</tr>
<tr>
<td>369</td>
<td>Deleting Languages from the Server</td>
</tr>
</tbody>
</table>
Introduction

By installing a language onto an existing Officelinx system, you will be able to address the needs of specific regions and audiences. This transforms the Officelinx suite into a full fledged localization solution for organizations dealing with audiences with multiple language requirements.

Available Languages

One language (English) is included with the program DVD.
The following table lists the languages available.

<table>
<thead>
<tr>
<th>Language</th>
<th>Regional Variation (if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>(program default)</td>
</tr>
<tr>
<td>English AU</td>
<td></td>
</tr>
<tr>
<td>English UK</td>
<td></td>
</tr>
<tr>
<td>French</td>
<td>North America</td>
</tr>
<tr>
<td>French EU</td>
<td>Europe</td>
</tr>
<tr>
<td>German</td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td></td>
</tr>
<tr>
<td>Portuguese BR</td>
<td>Brazil</td>
</tr>
<tr>
<td>Spanish</td>
<td>Americas</td>
</tr>
<tr>
<td>Spanish EU</td>
<td>Europe</td>
</tr>
</tbody>
</table>
Upgrade Preparation

Backup

It is suggested that the User back up certain files in the C:\UC folder on the system before beginning the upgrade.

The following files need to be backed up:

- C:\UC\DB
- C:\UC\Messages
- C:\UC\Prompts

Note: Take care to refer to Internet Information Services (IIS) on your PC and ensure that the FTP server is installed and running. Close all Server-related programs (i.e. UM Admin, UM Monitor).

Stop Officelinx Processes

Before you begin the installation, ensure that all necessary services have been stopped.

To stop services:

1. To stop services, open Control Panel > Administrative Tools > Services. Double-click the Services icon.

2. Highlight the UC Voice Server service and click the Stop icon in the toolbar.

3. Continue with the installation.

Downloading the Files

Standard English is included on the Avaya Officelinx DVD. All other languages are available for download from Avaya Inc. Contact your reseller for more details.

The downloaded files are in executable (EXE) format, and there is a single file for each available language. Download the file to a local drive and double-click to install the chosen language onto the voice server.

Note: Once installed on the server, the language must be selected through OL Admin before it will be available.
Language Pack Installation

**Note:** The Officelinx program must already be installed on the voice server before the language packs can be applied.

1. Download the language exe file and save it on the voice server drive.
2. Double-click the file to launch the installation routine.

3. The program will begin preparing to install the language pack.

4. At the Welcome screen, click Next to continue.
5. When prompted with the **End User License Agreement**, enable **I accept the license agreement**.

   Click **Next** to continue.

6. Select the appropriate format for voice prompts (**Mulaw** or **Alaw**).

   Click **Next**.

7. The wizard is ready to install the language pack.

   Click **Next** to begin the installation.

8. If you have not stopped all the necessary services, you will be prompted to do so at this point.

   Stop the services then click **OK** to continue.

9. Installation will begin and all of the components for the selected language will be copied to the server.
10. You will be notified when the installation is complete. Click Finish.

11. When prompted, click OK to restart the server.

12. After the server has finished rebooting, confirm that the language pack has been installed properly.

Open the OL Admin > Company Properties > Company Languages tab.

Add: Use this button to add more languages to the voice server. Once the new language installation is complete, they will appear in the list here. Changing the default will play all company telephone greetings and prompts in the equivalent in the new language.

Edit: Select an existing language and click Edit to change the settings for the chosen language.

Remove: This option will delete languages from the selection list. It does not delete the language files from the server; they can be added again later using the Add button.

Set Language as Default: Enable this option to set the current language as the first one that callers will hear when connecting to the system.

Active: When multiple languages are installed on a system, the first thing a caller will hear is a menu asking them to select the language they wish to hear. Put a checkmark in the box to add this language to the menu.

Note: Each language has its own TTS Voices included with the install. It is recommended that the appropriate voices be used with each language.
Deleting Languages from the Server

1. To remove the language pack and files from the voice server, begin by Removing the language from the system in OL Admin.

2. Open **Program and Features** from the Windows Control Panel.

3. Scroll down to locate the entries for Real Speak. Remove the TTS Voice characters for the language you want to remove from the system.

   The server must be restarted after the files have been removed.

4. After the server has rebooted, delete the language file from the Programs and Features window.
<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>372</td>
<td>Introduction</td>
</tr>
<tr>
<td>373</td>
<td>Failover using Carbonite Availability - LAN</td>
</tr>
<tr>
<td>373</td>
<td>Configuring the Network Cards</td>
</tr>
<tr>
<td>375</td>
<td>Installing Carbonite Availability on the Servers</td>
</tr>
<tr>
<td>380</td>
<td>Installing Carbonite Availability on the Client</td>
</tr>
<tr>
<td>382</td>
<td>Configuring Failover</td>
</tr>
<tr>
<td>388</td>
<td>On Failover</td>
</tr>
<tr>
<td>390</td>
<td>Failover using Carbonite Availability (WAN)</td>
</tr>
<tr>
<td>391</td>
<td>Installing Carbonite Availability on the Servers (WAN)</td>
</tr>
<tr>
<td>396</td>
<td>Installing Carbonite Console on the Client (WAN)</td>
</tr>
<tr>
<td>398</td>
<td>Configuring Failover (WAN)</td>
</tr>
<tr>
<td>405</td>
<td>Triggering Failover (WAN)</td>
</tr>
<tr>
<td>407</td>
<td>Failover Recovery</td>
</tr>
<tr>
<td>411</td>
<td>Reversing Protection After Failover</td>
</tr>
</tbody>
</table>
Introduction

**Note:** Carbonite Availability was previously known as Double-Take Availability.

**Important:** Carbonite Availability is not compatible with a High Security installation.

An Avaya OfficeLinx High Availability installation provides the means to maintain operations through failures in the Master and Secondary servers. The Consolidated server, however, cannot be protected in the same way. **Carbonite Availability** is a third party application that provides data protection and failover support, providing immediate recovery from any Consolidated server outages. Carbonite Availability can also be applied to the Master and Secondary servers.

There are two options for installing Carbonite Availability.

- **All servers are on a single network (LAN).**
- **You have a distributed network (WAN).**

Carbonite Availability requires another computer to mirror each voice server onto. This server must at least meet the minimum requirements needed to run the live server it is backing up. A third computer is required to run the client software that controls the behavior of the servers, but this computer can be any machine on the same network.

The Carbonite Availability backup system can be applied to an existing installation, or to a new installation. The Carbonite Availability software is downloaded from the link provided by your vendor. Carbonite Availability requires additional licensing, available through your Avaya representative, or directly from Carbonite.com.

Before proceeding, the OfficeLinx servers must be configured and operating properly. The Backup server must have the same operating system as the live server, fully installed and patched.
Failover using Carbonite Availability - LAN

The basic configuration for Carbonite Availability has both servers existing within the same network environment, where IP addresses and other routing details can be managed.

Both the HA server (Master, Secondary or Consolidated) and the backup machines (a server pair) must be using the same operating system with identical hardware.

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carbonite Availability</td>
<td>v. 8.2 or higher</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 or 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Network Cards</td>
<td>2 NICs are required in both the Consolidated and Backup servers</td>
</tr>
</tbody>
</table>

Terminology

Carbonite Availability uses the terms Source and Target to describe the two servers in each pairing.

**Source**: This is the live system server. All traffic and processing is handled by the Source. This is the computer that is being backed up.

**Target**: This is the backup server. The Target is a real-time mirror of the Source, but does not itself handle live traffic. The Carbonite Availability Client server regularly polls the Source. If it gets no response for a set period of time, it will assume that the Source is broken, and a failover condition is set.

Configuring the Network Cards

Both servers (source and target) in each pair must have **2 NICs** installed. On each machine, designate one to be the primary and the other as the secondary NIC. Perform the following procedure on both the Source and Target servers.

1. Configure the **Primary** card on each machine as you normally would for any node on the network.
2. To configure the **Secondary** NIC, open its the properties page.
3. Enter the IP Address that the secondary NIC is to use.

   Leave the DNS server details empty.

   ![Image of Internet Protocol Properties dialog box]

4. Click **Advanced** and open the **DNS** tab.

   **Disable** the option to **Register this connection's addresses in DNS**.

   ![Image of Advanced TCP/IP Settings dialog box]

5. Click **OK** to save the configuration. If prompted, click **Yes** to continue passed the warning.
Installing Carbonite Availability on the Servers

The Carbonite Availability software is downloaded from the link provided by your vendor. Save the file to a local drive and perform the following procedure on each server pair (Source and Target).

1. Double-click the program to start the installation.
2. Specify the location on your hard drive where the compressed files should be extracted to. Click Unzip.

3. The files will be unpacked onto your drive. When finished, click OK to continue.
4. From the main screen, select **Install Carbonite Availability**.

5. Any required applications that are not installed on your system will be added now. Click **Install** to continue.

6. When prompted to check for the latest installation, select **No** and click **Next** to continue.
7. Accept the terms of the license agreement and click **Next** to continue.

8. Click **Next** to activate the license.

9. Enable **Server Components Only**, then click **Next**.
10. Enter the license key that came with the program into the space provided. Click **Add** to install the license onto the computer. Click **Next** to continue.

11. Leave all settings at their defaults. Click **Next** to continue.
12. Click **Next** at the **Security Groups** screen.

13. Click **Install** to begin adding the program to the server.

14. The program will be installed. Click **Finish** when prompted.
Installing Carbonite Availability on the Client

A computer is required to act as the client/manager for the servers. This machine can be any other computer that has network access to all of the Source and Target servers. It can be installed on any of the Source or Target servers, or one or more other computers on the network. The client can be installed on any computer with the same operating system requirements as Carbonite Availability. It can also be installed (32-bit and 64-bit) on Windows XP SP 2+, Windows Vista, Windows 7, Windows 8 or Windows 10. The client can also be installed onto a virtual machine connected to the network.

**Note:** The client software does **NOT** require a license to operate.

1. Install the software on the client computer as shown above, but when step 9 is reached, choose **Client Components Only** instead and continue.

2. Complete the installation.
3. The Carbonite Replication console will be installed onto the client machine. Use this application to configure the disaster recovery and failover details for the 2 servers.
Configuring Failover

Setting up the details of the failover is done from the client computer using the Carbonite Replication Console.

1. Double-click the console icon on the Client computer to start the console.
2. From the main screen, click the **Add servers** icon.

3. On the **Manual Entry** tab, enter the required details for the **Primary NIC** on one of the **Source** servers. Click **Add** when ready.

   Repeat for the Primary NIC on the other server.

   Click **OK** when finished to add both servers to the console.
4. The Primary NICs for both servers appear on the main screen of the console. Under the Activity column, anything other than Idle means that an error has occurred. Delete the server and repeat step 1 to 3.

5. Select the Source server. Click the Create New Job icon and choose Protect from the dropdown menu.
6. Choose **Full Server** and click **Next**.

![Choose Data for ABC-123](image1)

7. Choose the **Target** machine to mirror the Source files onto, and click **Next**.

![Choose Target Server](image2)

8. Configure the settings for the failover monitor. Scroll down to reveal additional options.

**General**
- **Job name** can be anything. Make it user friendly to make the job easier to manage.

**Failover Monitor**
- Enable **Total time to failure** and enter the maximum time that the Source can be unresponsive before initiating the failover. Entering a value that is too small may trigger failovers during a scheduled reboot of the Source. The Target server monitors this connection as it continuously mirrors data, and will trigger the failover after the specified period without a response.
• Enable **Network monitoring** and select the IP Addresses for both NICs on the **Source** server.

![Network monitoring setup](image)

**Failover Options**

• Disable **Wait for user to initiate failover** to make the process automatic.

![Failover options setup](image)
Failover Identity
- Enable Apply source network configuration to the target. This allows the Target server to take over as the Source without having to reconfigure the remaining servers on the network.

Reverse Protection and Routing
- Turn on Enable reverse protection. This allows the Source and Target servers to reverse roles permanently when the original Source is brought back online after recovering from a failure.
- Use the dropdown menu beside Select a reserved IP Address on the source to pick the address for the Secondary NIC on the Source.
- Use the dropdown menu beside Select a reserved IP Address on the target to pick the address for the Secondary NIC on the Target.
Network Adapter Options
• Under Map source network adapters to target network adapters, use the dropdown menus to match the Primary NIC on the Source server with the Primary NIC on the Target server. Do the same for the Secondary cards.

Leave all other settings at their default values.

Click Next to continue.

9. Review the output and correct any errors that are found. When all items are correct, click Finish.

10. The new job has been created. The Target server will begin scanning and copying files. When it has finished, the Source server will be protected with the failover service configured here.
On Failover

Under normal conditions, the Source will manage the Officelinx HA operations, while the Target continuously mirrors the data.

Triggering Failover

If the Target server stops receiving feedback from the Source for the amount of time specified in the Failover Monitor above, the Target server will initiate a failover. It will change its network settings, computer name and addresses to match the original Source server, reboot, and become the new Source server for the HA system. This happens without the need to reconfigure the remaining servers on the HA system to point to the new machine.

Failover Recovery

When the original Source server is brought back online, how this is handled by Carbonite Availability depends upon why it failed.

Hard Drive Intact

If the hard drive of the Source was not compromised from the crash, the computer can be returned to service. On boot, Carbonite Availability will detect the IP address conflict with the old Target server and reset the address for the old Source server to another value (i.e. 169.255.xxx.xxx). From the Carbonite Availability console, initiate Reverse Protection. This will cause Carbonite Availability to change the computer name and IP Address to those of the original Target. The original Target machine will continue as the new Source, and the old Source machine becomes the new Target server. The two computers have swapped functions on the network.

Drives Damaged/Formatted/Replaced

If the hard drive or the data on the original Source server is damaged, nothing from the original job can be salvaged. Delete the job from the Carbonite Availability console, configure the recovered computer with the appropriate operating system and settings as outlined above, install Carbonite Availability, and create a new job with this machine now designated as the Target.

The original Target server will continue to operate as the Source.
License Recovery

If it was the Master server that failed, the software license must be re-activated. Since the servers have changed, the Hardware Signature will have changed as well, and the license will fail if it is not updated with the latest values.

1. On the new Master server, from the Windows start menu, go to **All Programs > Office-LinX > UCLicenseUpgrade**. Select **Upgrade**, and click **Request Online Activation**.

2. At the prompt, click **Yes**.

3. Returning to the License Upgrade Utility main page, click **Set as Active License**. Click **OK** at the prompt.

**Note:** Ensure that your **Serial Number** and **Site ID** are correct. This information was included with your original package documents.
Failover using Carbonite Availability (WAN)

For instances where the Disaster Recovery (DR) site is at a remote location from the primary data center, Carbonite Availability can be configured to offer protection across a WAN, and where a VLAN extension is not possible. Both the Consolidated server and the Carbonite Availability backup machines must be using the same operating system with identical hardware.

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carbonite Availability</td>
<td>v. 8.2 or higher</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 or 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Network Cards</td>
<td>1 NIC is required in both the Consolidated and Backup servers</td>
</tr>
</tbody>
</table>

* - When configuring Carbonite Availability to work over a WAN, only a **single** NIC is required on the Source and on the Target.

Unlike an installation where all servers reside on a single network, in a WAN installation, the source and the target server IP addresses do not change during a failover. Consequently manual intervention is required during a failover.

Carbonite Availability requires additional licensing, available through your Avaya representative, or directly from Carbonite.

Before proceeding, the Officelinx servers must be configured and operating properly. The backup server must have the same operating system as the live server, fully installed and patched.

Terminology

Carbonite Availability uses the terms Source and Target to describe the server pairs.

- **Source:** This is the live system server. All traffic and processing is handled by the Source machine. This is the computer that is being backed up.

- **Target:** This is the backup server. The Target is a real-time mirror of the Source machine, but does not itself handle any live traffic.

The Carbonite Availability Client regularly polls the Source. If it gets no response for a set period of time, it will assume that the Source is broken, and a failover condition is set.
Installing Carbonite Availability on the Servers (WAN)

The Carbonite Availability software is downloaded from the link provided by your vendor. Save the file to a local drive and perform the following procedure on both of the servers.

1. Double-click the program to start the installation. Click **Run** to continue.

2. Specify the location on your hard drive where the compressed files should be extracted to. Click **Unzip**.

3. The files will be unpacked onto your drive. When finished, click **OK** to continue.
4. From the main screen, select **Install Carbonite Availability**.

5. Any required applications that are not installed on your system will be added now. Click **Install** to continue.

6. When prompted to check for the latest installation, select **No** and click **Next** to continue.
7. Accept the terms of the license agreement and click **Next** to continue, then click **Next** to activate the license.

8. Enable **Server Components Only**, then click **Next**.
9. Enter the license key that came with Carbonite Availability into the space provided. Click Add to install the license onto the computer. Click Next to continue.

10. Leave all settings at their defaults. Click Next to continue.
11. Click **Next** at the **Security Groups** screen. Click **Install** to begin adding the program to the server.

![Image of Security Groups screen]

12. The program will be installed. Click **Finish** when prompted.

![Image of program installation]

![Image of installation completed]

Installing Carbonite Console on the Client (WAN)

A computer is required to act as the client/manager for the servers. This machine can be any other computer that has network access to both the Source and the Target servers. It can be installed on either of the Source or Target servers, or one or more other computers on the network. The client can be installed on any computer with the same operating system requirements as Carbonite Availability. It can also be installed (32-bit and 64-bit) on Windows XP SP 2+, Windows Vista, Windows 7, or Windows 8. The client can also be installed onto a virtual machine connected to the network.

1. Install the software on the client computer as shown above, but when step 9 is reached, choose Client Components Only instead and continue.

2. Complete the installation.
3. The Carbonite Availability console will be installed onto the client machine. Use this application to configure the disaster recovery and failover details for the servers.
Configuring Failover (WAN)

Setting up the details of the failover is done from the client computer using the Carbonite Availability Console.

1. Double-click the console icon on the client computer to open the program.
2. From the main screen, under Servers click Add servers to your console.

3. On the Manual Entry tab, enter the required details for the NIC on one of the servers. Click Add when ready. Repeat for the NIC on the other server. Click OK when finished to add both servers to the console.

- **Server**: Enter the IP address for the Carbonite server.
- **User name**: Type in the domain, forward slash, and the administrator username in this space. For example, domain/username.
- **Password**: Add the password for the administrator account here.

When ready, click Add.
4. Repeat step 3, adding the details for the other Carbonite server. Both servers will appear in the right hand window of this screen.

5. Under the Activity column, anything other than Idle means that an error has occurred. Delete the server and repeat step 1 to 3 for the affected server.
6. Select a server, click the **Create Job** icon, and select **Protect**.

7. On the Choose Data screen, select **Full Server** and click **Next**.
8. Select the server where the protected data will be stored, then click **Next**.

Make the following changes to **Set Options**.

9. Scroll down and expand **Failover Options**. Enable **Wait for user to initiate failover**.
10. Scroll down and expand **Failover Identity**. Enable **Retain target network configuration**.

11. Scroll down and expand **Reverse Protection**. Turn off **Enable reverse protection**.

12. Scroll down and expand **Network Adapter Options**. Map the network interface adapter card on the Target server to the card on the Source.
13. Leave all other settings at their default values and click **Next**.

14. The program will make the specified changes and verify all connections. Fix and Recheck any items that failed during testing. When all items appear green, click **Finish**.

15. The program will begin synchronizing all data. This may take some time. Job errors are normal during this period.
16. Once the synchronization is complete, your system will be protected against a server failure.
Triggering Failover (WAN)

In a WAN configuration, the failover is not automatic, and requires administrator intervention. Under normal conditions, the Source will manage the Officelinx traffic, while the Target continuously mirrors the data. If the Target stops receiving feedback from the Source for the amount of time specified in the Failover Monitor settings, a failover condition is triggered.

1. Once a failure condition is detected, the console will display a Server Communication Error, and Mirror Status will become Unknown.

2. The failover procedure is triggered by selecting the job, then clicking the failover icon 🔄.

3. Enable Failover to live data. From the Apply target data menu, select Apply data in the target queues before failover or cutover.

   Click Failover when ready to begin Data Recovery.

While the servers are in failure mode, there will be no services. The time required to complete the failover depends upon the speed of the drives and the amount of data the staging folder contains. The console allows you to monitor the progress of the failover.
Once the failover is complete, a **Failed Over** confirmation message appears in the console.

**Note**: The job entry includes a warning icon to remind you that the site is no longer being backed-up. Once the failure is corrected, enable Reverse protection to restore backup security.
Failover Recovery

Once failover is complete and the Target is active as the new Source, the voice servers must re-establish communication before voicemail functions will start working.

Enabling Voicemail Functions on HA Servers

For Consolidated Servers

After a failover, the IP addresses of the live servers have changed. Update Officelinx to re-establish voicemail functions.

1. Stop and disable the **SQL Mobilink Service** on the Master and all Secondary servers.
2. Change the IP address of the Consolidated server on the Master and Secondary servers only. This is the Mobilink connection that allows the servers to sync the database. Run the **UpdateDBHA_64.exe** utility from the server's hard drive. This program is available from your vendor.
3. At the prompt, enter 1 to change the IP address of the Consolidated server. Click **OK**.

4. Enter the new IP address of the backup Consolidated server, then click **OK**.

5. The IP Address for the Consolidated server will be changed. Click **OK**.

6. Any errors can be viewed in the log file. When finished, click **OK** to complete the change.

Start the **SQL Mobilink** service on all servers in the HA environment.
For Consolidated Server only if the Consolidated has failed

After failing over to the Target server, the voicemail application cannot be activated since the IP address of the server has changed. To re-establish the voicemail functions:

7. Change the IP address of the UMST (Consolidated) server to the IP address the server attained during failover. Open OL Admin, and go to Configuration > Advanced.
8. Double-click UMST Server Address in the right-hand pane and enter the updated IP address for the UMST server.

For the Master Server only if the Master has failed

10. Change **CTI Service IP** to the new IP address of the Target Master server. Click **OK**.

![CTI Settings](image)

On the **Master** server, the software license must be re-activated. Since the servers have changed, the Hardware Signature will have changed as well, and the license will fail if it is not updated with the latest values.

11. From the Windows start menu, go to **All Programs > Office-LinX > UCLicenseUpgrade**. Select **Upgrade**, and click **Request Online Activation**.

![License Activation](image)

**Note:** Ensure that your **Serial Number** and **Site ID** are correct. This information was included with your original package documents.

12. At the prompt, click **Yes**.
13. Returning to the License Upgrade Utility main page, click **Set as Active License**. Click **OK** at the prompt.

14. In Officelinx, update the IP address of the Master and all Secondaries. Open OL Admin, and under **Voice Server**, choose your servers and set the **Internal IP** address in the right-hand pane to the current value.

15. Restart the **Master** server.

**Important:** The PBX needs to have the IP address of the **Master** server updated so calls are also redirected to the new Master / Secondary servers.
Reversing Protection After Failover

After failover, the old Target server has become the new Source server. Once the cause of the failure has been corrected, the original Source is can become the new Target, thereby restoring failover protection to the system.

1. Open the Carbonite Availability monitor. Failover protection is no longer active.

2. To initiate Reverse Protection, click the Reverse button in the toolbar.

This initiates a synchronization of the servers, with the original Target as the new Source, and the original Source now the Target. The monitor displays the progress of the synchronization.

When the synchronization is complete, the system is again safe with failover protection.

Compare the configuration from before and after the failover. The two servers have traded positions.

Reverse protection has been enabled successfully.
In This Chapter:

414  Introduction
414  Virtual Environment Limitations
415  Virtual Machine Environment Hardware Requirements
415  VMware Technology Guidelines
416  VM Environment Feature Comparison Chart
417  VMware: HA for the Consolidated Server
420  Virtual Environment Deployment Example
420  CPU Usage
421  Datastore Latency
421  Disk Usage Rate
422  Network Usage Rate
422  Conclusion
Introduction

Many organizations are turning to virtual environments for their server needs due to their cost and efficiency. Instead of a room full of servers, virtual servers on hosted or in-house environments can perform the functions of multiple computers.

Avaya Officelinx can be installed on a virtual environment enabling you to reuse the equipment you already have. Instead of buying a new computer to host the voice server, upgrades to existing hardware may be sufficient through virtualization.

Pre-Requisites

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Software</td>
<td>VMware ESXi 4.x / 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 6.7&lt;br&gt;Hyper-V Server 2012&lt;br&gt;Windows Terminal Services ¹</td>
</tr>
<tr>
<td>OS for Officelinx</td>
<td>Microsoft Windows 7 (32 and 64-bit),&lt;br&gt;Server 2008 (32-bit),&lt;br&gt;Server 2008 R2 (64-bit)&lt;br&gt;Server 2012 or 2012 R2&lt;br&gt;Server 2016</td>
</tr>
</tbody>
</table>

Note: ESXi has been tested on versions 4.x / 5.0 / 5.1 / 5.5 / 6.0 / 6.7. Hyper-V Server 2012 has also been tested.

<table>
<thead>
<tr>
<th>Hardware</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Requires Intel® CPU which meets or exceeds the requirements of ESXi 4+</td>
</tr>
</tbody>
</table>

¹ - Windows Terminal Services only supports the installation of the client software. The Officelinx server cannot be installed here.

Virtual Environment Limitations

You cannot directly upgrade an existing Avaya Officelinx server to a virtual environment. However, you can move an existing server onto a virtual machine by migrating the database using the utilities provided on the Officelinx installation DVD. You can transfer both 7.x and 8.x systems to an 10.7 virtual environment. Officelinx must be installed on a new virtual machine with a clean operating system.

Warning: Importing an existing Avaya Officelinx environment to a virtual image is not supported.

Officelinx installed on a virtual environment requires the same hardware resource as non-virtual machine environments.

Note: The fax capability of Officelinx within a virtual environment is limited to 24 ports.
Virtual Machine Environment Hardware Requirements

The hardware requirements for setting up Officelinx within a virtual environment are the same as for a physical machine. See the Environmental Considerations chapter of this guide for more information.

The configuration of the virtual environment does create other considerations for server installation.

VMware Technology Guidelines

VMware offers a wide range of technologies which may be implemented on a virtual machine for greater redundancy and ease of maintenance. This section explains which features are compatible with the Officelinx server application and how to utilize VMware solutions with Officelinx in mind.

- **vMotion**: vMotion allows for the migration of an active server without affecting its operational status. This means you can move a virtual machine that is currently active from one ESXi host to another without having to shut it down. For Officelinx, this means that you will be able to move the voice server without having to turn it off first. This allows system administrators to migrate the system at any time during the day without down time. Depending on timing and available resources, you may or may not see a disruption in service during the transfer. For example, if the voice server has an active call when you start the migration, the call may be dropped or it may stay connected after a short pause depending on how quickly the migration can finalize. vMotion is a manual process.

- **High Availability**: VMware also offers its own High Availability solution, which should not be confused with Officelinx HA. VMware’s HA model is initiated in 2 ways: one is hardware (machine) failure and the other is software (Operating System) failure. When the ESXi hardware fails on a system monitored by HA, VMware will automatically restart the Virtual Machine image on another ESXi host. If the OS becomes unresponsive, VMware HA will start the virtual machine on another ESXi host and bring the server back online. This will lead to down time while VMware moves operations onto another host. Officelinx will be down during the recovery period and will not be able to answer calls until the secondary virtual image is fully up and running. The recovery occurs automatically, but it must be ‘hard coded’ to a specific recovery ESXi server. If there are no available resources on the recovery server, Officelinx may fail to restart.

- **Distributed Resource Scheduler**: Distributed Resource Scheduler is intended for sites with multiple physical ESXi servers available. DRS keeps track of hardware resources, and is able to see the current availability of CPUs, RAM, etc. on all servers. When the main server crashes, DRS will automatically allocate the necessary resources and restart the virtual machine in a suitable environment. This means that Officelinx will be guaranteed a minimum level of resources upon recovery to ensure there is no reduction in service. This is an advantage offered by DRS when compared to HA alone since HA does not consider hardware requirements when allocating space for a new virtual machine to replace the crashed server.

- **Fault Tolerance**: Fault Tolerance offers a higher level of protection than HA by eliminating downtime. A virtual machine being monitored by an FT system will have a shadow image created that is identical to the monitored virtual machine. When the main server becomes unavailable for any reason, the shadow image which has been reproducing all activity on the main server will become active, instantly replacing the crashed server. This reduces the chance of an interruption or data loss in most active environments. However, due to the extensive nature of FT’s monitoring, FT can only support virtual machines with a single core CPU. This does not meet Officelinx Voice Server’s minimum hardware requirements, so Officelinx will remain incompatible with FT until the algorithm is changed to support the resources required.
VM Environment Feature Comparison Chart

<table>
<thead>
<tr>
<th></th>
<th>vMotion</th>
<th>HA</th>
<th>DRS</th>
<th>FT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Migration</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Recovery from Hardware Crash</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Recovery from Software Crash</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>0 Down Time during Crash</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Smart Allocation of Hardware Resources</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Officelinx Support</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N*</td>
</tr>
</tbody>
</table>

**Known Behaviors:**

- Voice Traffic: Potential loss of ongoing calls during migration. (Tested with registered SIP extensions)  
  - Interrupted until HA recovers  
  - Interrupted until HA recovers  
  - N/A*

- iLink Pro Desktop: Potential for disconnect during migration  
  - Interrupted until HA recovers  
  - Interrupted until HA recovers  
  - N/A*

- Messaging: No interruption  
  - Interrupted until HA recovers  
  - Interrupted until HA recovers  
  - N/A*

- CTI: No interruption  
  - Interrupted until HA recovers  
  - Interrupted until HA recovers  
  - N/A*

* Due to the way in which Fault Tolerance is designed, Avaya Officelinx cannot function within the FT model. FT is limited with regard to computer resources (e.g. single core processor) while Officelinx has specific minimum resource requirements to function properly. Until VMware upgrades the FT system to support higher amounts of resources, Officelinx cannot be deployed under the FT model.
VMware: HA for the Consolidated Server

In a High Availability environment, the Master and all Secondaries act as backups for each other. If one server fails, the Consolidated server redirects traffic through the remaining operational units preventing any service interruptions. However, the Consolidated server has no such protection. If the Consolidated server fails, the entire system will fail. VMware includes an HA option for its Hosts, providing failover support for the Consolidated server.

1. The site admin must install and configure VMware vSphere on the network. There should also be an external SAN for data storage.

2. Create a Cluster within vSphere.
   - When configuring the Cluster, under vSphere Availability, ensure that Turn ON vSphere HA is enabled.

3. Add 2 or more Hosts within the Cluster. One Host contains the virtual machine that houses the Consolidated server, while the others are available should the active Host fail.

   **Important**: It is essential that all of the Host servers have their clocks synchronized. Certain critical functions within Officelinx are time sensitive and will fail if the Hosts are not coordinated.

4. For each Host, open the Configuration tab and go to System > Time Configuration.
   - Enable Use Network Time Protocol (Enable NTP client).
   - Set the NTP Service Startup Policy to Start and stop with host.
   - Enter one or more NTP servers in the space provided. The time signals will be synchronized with these sites.
- Start / Restart the NTP Service to activate the changes.

5. Create virtual machines and choose the SAN as the data storage location.
6. Edit the settings for each virtual machine. Under VM Options > VMware Tools > Time, enable Synchronize guest time with host.
7. Install the Officelinx Consolidated server onto one of the virtual machines. If the Host with the virtual machine running the Consolidated server fails, VMware will automatically move the server to another Host within the Cluster and restart the virtual machine.

**Important:** The Officelinx system will be unavailable during the changeover and reboot process.
Virtual Environment Deployment Example

The following are performance results from a virtualized Avaya Officelinx system running 100 active voice ports with 1,000 users registered under the system. Please keep in mind that this is a limited test run to showcase how a typical operation may perform under a virtual environment. This example does not guarantee an identical level of performance on every virtual environment, but rather serves as a guideline with regards to Officelinx’s behavior under virtual environments.

CPU Usage

Avaya Officelinx used an average of 58.945% of the CPU capacity, which equates to 5,643.95 MHz. When considering the Maximum requirement, providing at least 6.8 GHz of CPU resources to Officelinx will guarantee a consistent level of performance.
Avaya Officelinx achieved a low average latency of 5.356ms for reading and 2.378ms for writing.

Avaya Officelinx had an average disk usage rate of 1,106.344 KBps with a peak of 1,767 KBps. Ensuring a data transfer
rate of 1,800 KBps to Officelinx will guarantee a consistent level of performance.

Network Usage Rate

Avaya Officelinx had an average network usage rate of 870.094 KB/s with a peak of 1,185 KB/s. Providing 1,500 KB/s of network bandwidth to Officelinx will guarantee a consistent level of performance.

Conclusion

Since Avaya Officelinx is designed to be the sole application running on a given Virtual Machine, it is easy to assign the necessary resources for Officelinx. By ensuring that Officelinx always has access to the required resources, you will be able to guarantee the level of performance required by your site.
VIRTUALIZED ENVIRONMENT: MICROSOFT HYPER-V

In This Chapter:

424   Introduction
424   Requirements
424   Virtual Environment Limitations
425   Adding Hyper-V to the Host
425   Adding the Hyper-V Role
432   Creating the Guest Environment on the Host
439   Hyper-V Server 2012
Introduction

Many organizations are turning to virtual environments for their server needs due to their cost and efficiency. Instead of a room full of servers, a single virtual server on a hosted or in-house environment can perform the functions of many individual computers. Avaya Officelinx can be installed in a virtual environment enabling you to reuse the equipment you already have. Instead of buying a new computer to host the voice server, upgrades to existing hardware may be sufficient through virtualization.

Avaya Officelinx supports both VMWare and Microsoft’s Hyper-V for the virtualized environment. In this chapter, we will create and configure a Hyper-V virtual environment to host the voice server.

Requirements

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyper-V</td>
<td>Windows Server 2012 or 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Hyper-V Server 2012*</td>
</tr>
<tr>
<td>OS for Officelinx</td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 or 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>

* - Hyper-V Server 2012 is not a full version of Windows Server 2012. It is a stand-alone product that contains only the resources necessary to support and manage virtual environments, and is available free from Microsoft. However, a full version of Windows Server 2012 is still required to create the virtual environments on each Hyper-V Server only machine. See page 439 for more details on using Hyper-V Server 2012.

Virtual Environment Limitations

You cannot directly upgrade an existing Officelinx server to a virtual environment. However, you can move an existing server onto a virtual machine by migrating the database using the utilities provided on the Officelinx installation DVD. You can transfer both 7.x and 8.x systems to an 9.0 virtual environment. Officelinx must be installed on a new virtual machine with a clean operating system.

Officelinx installed on a virtual environment requires the same hardware resources as non-virtual machine installations.

**Note:** The fax capability of Avaya Officelinx within a virtual environment is limited to 8 ports.

**Warning:** Moving an existing Officelinx environment to a virtual image is not supported. However, after installing Officelinx onto the virtual machine, the data files can be migrated to the new location.
Adding Hyper-V to the Host

Before installing Avaya Officelinx onto a virtual server, the computer must be configured for the environment, and the operating system must be installed. The virtual environments have the same hardware requirements as a standalone machine.

Host Operating System

The physical computer (Host) that will have Microsoft Hyper-V installed must be running Windows Server 2012 or 2012 R2. Microsoft Hyper-V Server 2012 can be installed on the Host, but one full version of Windows Server 2012 is still required to create the virtual environments on each of these machines.

Guest Operating System

The environment created (Guest) on the host must have its own licensed copy of Windows installed, configured and fully patched. The version of Windows required must be one supported by Officelinx.

Adding the Hyper-V Role

Note: These steps are performed on Windows Server 2012, not Hyper-V Server 2012. See page 439 for details on using Hyper-V Server.

Once the Host has had Windows Server 2012 installed and patched, follow the directions below to add the Hyper-V role.

1. On the Host computer, open the Server Manager utility and add a new role.
2. Proceed through the screens. At the Select server roles pane, enable **Hyper-V** from the available options. Click **Next**.

![Select server roles](image)

3. At the prompt, confirm the selection by clicking **Add Features**.

![Add Features](image)

4. Continue until you reach the Hyper-V setup screen. Click **Next**.

![Hyper-V setup](image)
5. Disable all of the virtual switches on the **Host**, then click **Next**.

6. At the **Virtual Machine Migration** screen, leave the values at their defaults, and click **Next**.
7. For Default Stores, specify the hard drive and file location on the Host where the virtual hard disk and configuration files will be kept.

Click Next.

8. The Host has all of the information it needs. Click Install to add the Hyper-V role to the server.
9. Support for Hyper-V virtual environments will be installed on the computer.

When finished, click **Close**, then **restart the server**.

10. After the restart, open the **Start** window and select **Hyper-V Manager**.
11. Right-click the Host, then click Virtual Switch Manager... from the pop-up menu.

12. Select External for the type of virtual switch to create. Click Create Virtual Switch.
13. Enter a name for the switch.

Select a virtual switch from the list of those available on the dropdown menu. One switch is typically used exclusively for managing the virtual environment. Choose any other switch than the one used for management functions.

Ensure that **Allow management operating system to share this network adapter** is disabled. Ensure that **Enable single-root I/O virtualization (SR-IOV)** is enabled.

Click **Apply**, then **OK**.

14. Click **Yes** to confirm the changes.

The **Host** has been configured and is ready to create new virtual environments.
Creating the Guest Environment on the Host

With the Hyper-V role installed, the individual environments for each Guest can be created and configured.

1. On the Host server, open the Start window and select Hyper-V Manager.

2. On the Manager screen, right-click the Host computer and select New > Virtual Machine....

3. The New Virtual Machine Wizard will guide you through the process to create a new virtual environment on the selected server.

   Click Next to continue.
4. Give the **Guest** a name. You can also choose to store the data for the environment in a different location.

5. Specify the amount of memory the **Guest** will have. This must be at least as much as required by the version of Officelinx to be installed. It is recommended that a minimum of 4GB be configured.

*Note:* The **Host** must have sufficient RAM installed to dedicate the desired amount of memory to the **Guest** environment, and still have enough remaining for its own needs.
6. To connect this environment to other systems, a virtual switch is required. Choose a switch for the environment to use from the dropdown menu. Officelinx requires this connection to provide access to the network and to the Internet.

7. Select Attach a virtual hard disk later. Click Next.
8. The **Host** has all of the necessary information to build the virtual machine. Review the settings and click **Finish** to create the new **Guest** environment.

![Virtual Machine Wizard](image)

9. When the virtual machine has been created, you are returned to the Hyper-V Manager screen. The new **Guest** environment is displayed.

![Hyper-V Manager](image)
10. Open **Settings** for the **Guest** machine, and verify or set the number of processors needed to properly support Officelinx.

11. Open the settings for **IDE Controller 0**.

12. Select **Hard Drive**, then click **Add**.

13. Enable **Virtual hard disk**. Click **New**.
14. In the **New Virtual Hard Disk Wizard**, click **Next** until you reach **Choose Disk Type**.

   Enable **Fixed size**, and click **Next**.

15. Specify the name for the drive, and a path to its location on the disk. Click **Next**.
16. Enable **Create a new blank virtual hard disk**.

Enter the size for the drive in the space provided.

![Create a new blank virtual hard disk](image)

**Note**: The size for the drive is calculated in the same way as it is for any other voice server. Be sure to reserve enough space to handle all of the traffic that will be passing through the system.

17. Click **Finish** to complete the installation.

18. The virtual environment is now ready to use. The device is currently **Turned Off**. Turn it on ✅ to proceed with the installation of the operating system and the Avaya Officelinx software.

![Guest on host - virtual machine connection](image)

**Note**: The virtual machine has no operating system and no applications installed. Once the machine is on, it must be treated as a new computer. Install and configure an appropriate version of Windows and Avaya Officelinx.
Hyper-V Server 2012

Microsoft Hyper-V Server 2012 is a stripped down version of Windows Server 2012 intended only for use as a Hyper-V server. It has no desktop or other GUI components. It includes only the pieces of Windows required to host and manage a virtual machine environment. It is freely available from Microsoft, and can be installed on any currently empty computer.

Hyper-V Server cannot set up an environment on its own. A fully licensed version of Windows Server 2012 is still required to create and manage the environment, but only a single license of Windows is required to administer many Hyper-V servers.

1. On a computer with a full version of Windows, use an Internet browser to download the Hyper-V Server installation ISO file from the Microsoft web site. Burn this file onto a CD/DVD.

2. Place the disk into the drive of the computer that will become a Hyper-V server. The computer's hard drive must be empty. Boot the computer from the disk. The installation of the Hyper-V Server will begin automatically.

3. When finished, reboot the computer.

4. When the computer restarts, use the management interface to configure the network settings for that computer.

Define the following items according to your site's networking requirements:

- Domain/Workgroup
- Computer Name
- Windows Update Settings
- Download and Install Updates
- Network Settings
- Date and Time
- Help improve the product with CEIP

All of the other items are optional.
5. From a computer that has Windows Server 2012 with the Hyper-V Role installed, open **Hyper-V Manager**.

6. Right-click **Hyper-V Manager** in the left-hand pane and select **Connect to Server...** from the dropdown menu.

7. When prompted, select **Another computer**. In the space provided, enter the **IP Address** or the **name** of the Hyper-V Server machine. Click **OK**.

8. The server will appear on the list on the Hyper-V Manager main page. Follow the instructions for creating a virtual environment as outlined beginning on page 432.

**Note:** The Hyper-V server management interface is only used to configure the domain and perform other network setup procedures on that computer. All of the virtual environments are managed using the Windows Server 2012 machine.
AMAZON WEB SERVICES

Introduction

Many organizations are turning to virtual environments for their server needs due to their cost and efficiency. Instead of a room full of servers, virtual servers on hosted environments can perform the functions of multiple computers. Avaya Officelinx can be installed into an Amazon Web Services (AWS) virtual network in the Cloud.

Pre-requisites

You must have an account with Amazon Web Services before proceeding. Servers on AWS must also be purchased and configured. This can be a single server, or multiple machines in a virtual network.

The PBX for your company must be installed and operating correctly on one of the AWS servers.

The AWS servers should be specified with sufficient resources (CPU, RAM and HDD) for the program. The specifications should be equal to or above those used for an on-premise installation of Officelinx.


For HA installations: Hardware Requirements on page 51 in the Technical Operating Guide.

During testing, the following AWS server configurations were validated.

<table>
<thead>
<tr>
<th>MODEL</th>
<th>INSTANCE TYPE</th>
<th>vCPU (#)</th>
<th>MEMORY (GiB)</th>
<th>STORAGE (GiB)</th>
<th>BANDWIDTH (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4.xlarge</td>
<td>General Purpose</td>
<td>4</td>
<td>16</td>
<td>EBS only</td>
<td>750</td>
</tr>
<tr>
<td>m5.xlarge</td>
<td>General Purpose</td>
<td>4</td>
<td>16</td>
<td>EBS only</td>
<td>Up to 2120</td>
</tr>
<tr>
<td>c5.xlarge</td>
<td>Compute Optimized</td>
<td>4</td>
<td>8</td>
<td>EBS only</td>
<td>Up to 2250</td>
</tr>
</tbody>
</table>

Important Note

When using Esna licensing:

In a **Single Server** environment, the AWS **Voice** server must have Internet access enabled for the program to validate the license.

In a **High Availability** environment, the **Master** Server in AWS must have Internet access. Without this connection, the program will only operate in Demo mode.

When using WebLM licensing:

If you install the WebLM license server within the AWS cluster, then no Internet access is required to validate your license details.

If the license server is **NOT** part of the AWS cluster, then the Voice server (single server) or the Master server (HA) **DO** require an Internet connection to validate the license.
Avaya Officelinx can be installed in a Single Server (SS) or High Availability (HA) configuration. Follow the standard installation procedures for Officelinx based upon the version of Windows being used.

- Purchase the correct type and number of AWS server(s) for your requirements.
- Configure Windows on each server with the appropriate roles.
- Install Avaya Officelinx as you would on a local machine. Refer to the appropriate chapter of this document for complete instructions based upon your server operating system. For HA environments, ensure that the servers are installed in the correct order.
In This Chapter:

444 Introduction

444 Adding the New PBX

452 Routing Through the PBX

452 Configuring a Mailbox

453 Configuring an Organizational Unit

454 Configuring a Company
Introduction

Avaya Officelinx is able to integrate with multiple PBXs or nodes at the same time, allowing you to take advantage of all the capacity a site may have. This is also a great option for legacy sites which are adding another PBX to increase capacity. A site can add new PBXs to their legacy system and use them as though they were a single unit through Officelinx without worries about compatibility.

The only requirement for multi-PBX / multi-node support is that the PBXs are compatible with Avaya Officelinx. It is recommended that all PBXs / nodes use SIP trunks.

Adding the New PBX

Multiple PBXs can be setup to use independent channels for each, or to share resources through port pooling.

Using Independent Channel Pools

1. From the Windows program menu, under the Officelinx group, open the SIP Configurator.
2. Login using administrator credentials.

3. In the left hand pane, right-click on PBX and choose the unit to add.
4. Enter the details on each tab for the new PBX. Refer to the integration notes for your make and model if necessary.

![Configuration Screen](image)

**Note**: The channel range for the new PBX should not overlap with the channel range of other PBXs.

5. Click **OK** when finished.
6. Return to the Officelix program group and select **Office-LinX Admin**.

![Program Group](image)

7. Login with administrator credentials.
8. From the navigation bar on the left, right-click on your PBX and select Properties.

![Properties](image)

9. Open the PBX Node tab and select Add.

![Add Node](image)

10. Fill in the details for the new PBX.

![Node Details](image)

**Note:** Make sure that your Node Address matches what you have defined in your SIP configurator. Remember the Node ID for use when configuring call routing.
Using Channel Port Pools

1. From the Windows program menu, under the Officelix group, open the **SIP Configurator**.

2. Login using administrator credentials.
3. In the left hand pane, right-click on PBX and choose the unit to add.

4. Fill in all of the necessary details for the PBX. Leave the Channels field blank.

5. Navigate to the PBX > ANI tab and specify the voicemail pilot or hunt group in the Voice Port Alias field.
6. Navigate to the **Extension Pool** settings and define a starting extension number (generally 1), the number of extensions (total port quantity), and the alias (trunked connectivity can be defined as *).

![Extension Pool Settings](image)

7. Set the **PBX Network ID** to correspond to the entry order in the SIP Configuration Tool.

8. For the node description, each unique SIP endpoint (rather than logical PBX endpoint) must be defined within curled braces "( )" as shown. The string within the braces must be unique for each endpoint.

![Node Description](image)

9. Verify in the definitions for the **Voice Mail Extensions** (on the **General** tab) that connectivity is defined as trunks (*) and that no PBX nodes are assigned for a pooling configuration.

![Voice Mail Extensions](image)
10. Verify under Advanced voice server configuration that **Outcall address with NodeID** is set to **True**.
Routing Through the PBX

Officelinx will attempt to route a call, first using a Mailbox address, then an Organizational Unit, and finally using Company settings.

Configuring a Mailbox

1. Login with to OL Admin using the administrator credentials.

2. Select the mailboxes to assign to the new PBX, or create a new mailbox and select the Address tab.

3. If there is already an extension associated with the mailbox, select it and click Edit. Or create a new extension by clicking Add > Phone Number.
4. Assign the extension to the new PBX node.

Configuring an Organizational Unit

1. Login with to OL Admin using the administrator credentials.

2. Right-click an Organizational unit and select **Properties**.

3. Assign the Organizational unit to the new PBX.
Configuring a Company

1. Login with OL Admin using the administrator credentials.

2. Select existing company, or create a new one. Right-click the company and choose Properties.

3. On the General tab, assign the desired PBX node to the company.

The setup is complete.
## APPENDIX A: REVISION HISTORY

<table>
<thead>
<tr>
<th>DATE</th>
<th>ISSUE</th>
<th>CHANGE SUMMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 July, 2018</td>
<td>10.7 (1)</td>
<td>Initial Document Release</td>
</tr>
<tr>
<td>9 November, 2018</td>
<td>10.7 (2)</td>
<td>Added details on adding HA backup to the Consolidated server through VMware.</td>
</tr>
<tr>
<td>23 November, 2018</td>
<td>10.7 (3)</td>
<td>Updated Avaya branding.</td>
</tr>
<tr>
<td>4 December, 2018</td>
<td>10.7 (4)</td>
<td>Included the chapter on using Carbonite Availability as a backup solution.</td>
</tr>
<tr>
<td>1 February, 2019</td>
<td>10.7 (5)</td>
<td>Modified the WebLM installation with several new items. Added more detail to restoring certificates for HA installations.</td>
</tr>
<tr>
<td>1 March, 2019</td>
<td>10.7.0.1 (6)</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>14 March, 2019</td>
<td>10.7.0.1 (7)</td>
<td>Updates for High Security installations.</td>
</tr>
<tr>
<td>17 April, 2019</td>
<td>10.7.0.1 (8)</td>
<td>Corrected instructions regarding the use of the SR140 fax module with HA installations. Changed references to OnEsna to accounts.zang.io.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Restored some parts of the database migration chapter. Changed DCOM login account for HA installations.</td>
</tr>
<tr>
<td>26 April, 2019</td>
<td>10.7.0.1 (9)</td>
<td>Adjusted ratio from 10:1 to 40:1 for calculating the number of ports required for an installation.</td>
</tr>
<tr>
<td>19 June, 2019</td>
<td>10.7.0.1 (10)</td>
<td>Added procedure for converting from an Officelinx native license to Avaya WebLM (PLDS) licensing. Removed references to TSE and IMAP where possible.</td>
</tr>
<tr>
<td>22 July, 2019</td>
<td>10.7.0.1 (12)</td>
<td>Modified HA chapter to include the option to enable MWI on failover. Updated JJTC certification notice. Changed note for that Carbonite is not compatible with High Security installations. Added section for installing Officelinx on a hardened Windows server.</td>
</tr>
</tbody>
</table>