AVAYA

Experiences That Matter

IX MESSAGING™

Server Installation Guide

Version 10.8 (36) | Dec 2021.

Avaya IX Messaging Server Installation Guide

The Server Installation Guide is designed to be used as a reference when deploying Avaya IX Messaging at a given site. While the settings and configuration of each site differs, the way in which Messaging 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, Messaging 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.

Notice

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

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON

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

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

License types

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

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

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

Copyright

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

Virtualization

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that

apply is available in the products, Documentation or on Avaya's website at: https:// support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP:// WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

AVAYA IX MESSAGING SERVER INSTALLATION GUIDE

Table of Contents

1 AVAYA IS MESSAGING INSTALLATION SUMMARY

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)
- Avaya IX Messaging servers must be installed on a RAID 10 hard drive array, including both virtual and physical machine installations
- 512 MB of RAM

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

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

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

Caution: The operating system drive must have at least 100GB reserved exclusively for the O/S. This is in addition to any amount required for the Messaging voice server installation.

Considerations:

Messaging uses a dedicated server to enable high performance operation of the program. Other applications running on the same server as Messaging 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 Messaging:

- 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 Messaging 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

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

- Windows Server 2012 or 2012 R2 - Standard Edition
- Windows Server 2016
- Windows Server 2019

Note: Avaya IX Messaging 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 Messaging 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.

System	Operation	Detailed Documentation
PBX	Install, configure and connect for normal operation.	PBX Branded Documentation
Voice Server Computer	Configure Server for necessary roles.	Server Install Guide
	Install Windows Features	Server Install Guide
	Add certificates to the O/S.	Consult your certificate provider
	Install Messaging	Server Install Guide
	Configure company and users under Messaging.	Server Configuration Guide
	Record company telephone greetings.	Server Configuration Guide Ch22
	Add any optional modules to Messaging.	Various
	Integrate Messaging with the switch.	Messaging integration documents
Desktop Workstation (optional)	Install the iLink Pro Desktop Client.*	Client Application Guide Ch2
Devices (optional)	Navigate to the device store, download and install the mobile client.	Client Application Guide Ch7ff

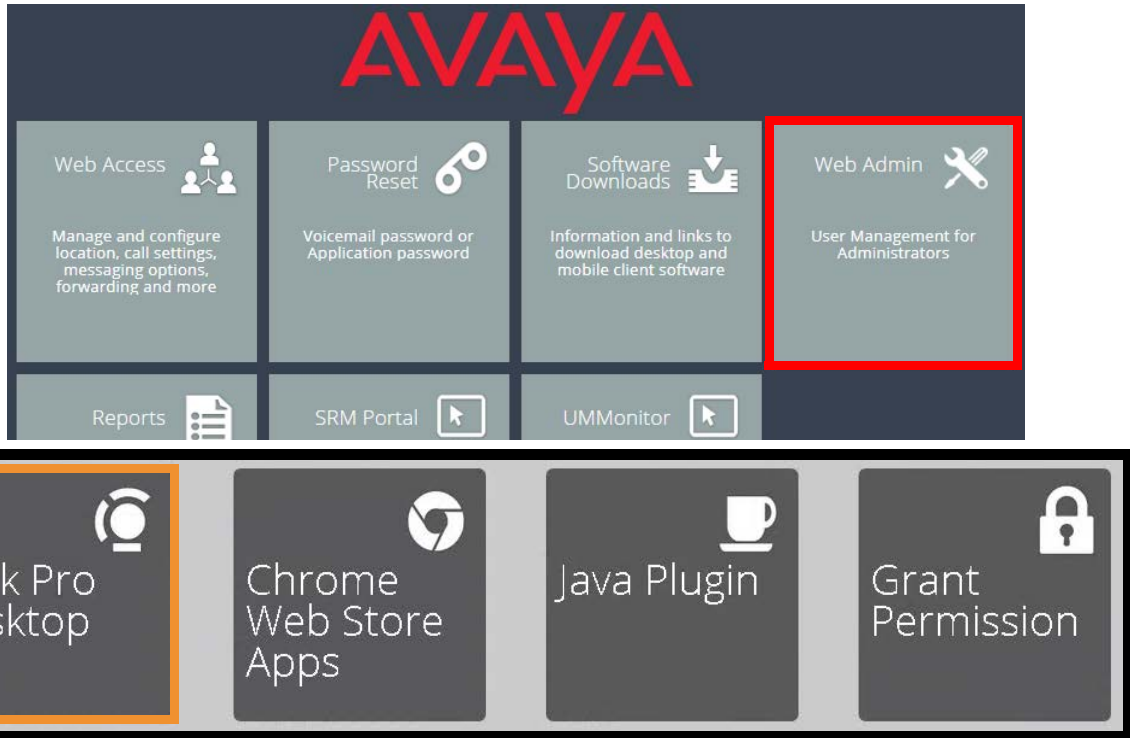
* The iLink Pro Desktop Client software can be found in the Messaging installation directory.

.../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

Feature	Capacity
Company Directory	80,000 entries *
Voice Mailboxes	80,000 - on High Availability Server * 4,800 - on Single Server
Messaging Users	20,000 - on High Availability Server 1,000 - on SIngle Server
Voice Channels	48 ports - SIP with Iwatsu ECS 120 ports - SIP integration, per voice server 2,400 ports - High Availability Environment
Text to Speech Ports	64 ports per server
Automatic Speech Recognition	64 ports per server
Extension Dialing	Unlimited
Number of Tenants	999

* This is 80,000 users in total, with **up to** 20,000 of those being Advanced users.

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 Messaging itself is insufficient.

2 SYSTEM REQUIREMENTS AND CAPACITY

In This Chapter:

General Requirements

Maximum System Capacity

Feature	Capacity
Company Directory	80,000 entries [1] [3]
Voice Mailboxes	80,000 - High Availability Server [1] [2] [3] 4,800 - Single Server
Messaging Users	20,000 - High Availability [2] 1,000 - Single Server
Voice Channels	48 ports - SIP with Iwatsu ECS 120 ports - SIP integration, per voice server 2,400 ports - High Availability Environment
Text to Speech Ports	64 ports per server
Automatic Speech Recognition	64 ports per server
Extension Dialing	Unlimited
Number of Tenants	999

1 See the table below for details on calculating this value.

2 The Distributed Server model moves IMAP CSE functions to a separate server from the primary voice server.

3 This is 80,000 users in total, with **up to** 20,000 of those being Advanced users.

Note: Additional licensing may be required to access all program features.

Note: Avaya IX Messaging is a dedicated application which should only be installed as a primary application on any server. Sharing system resources with other applications may reduce the performance.

Hint: For optimal **UC Mobile** performance, it is recommended that the maximum number of users within a single Organizational Unit (OU) be kept below 500.

Bandwidth Requirements

The network bandwidth required to properly support Avaya IX Messaging is dependent upon the number of channels installed onto the system. As a guide, every channel needs 15 kbps bandwidth for inbound, and another 15 kbps for outbound traffic.

# Channels	Recommended Total Bandwidth (incoming + outgoing)
10	300 kbps
20	600 kbps
50	1,500 kbps
100	3 Mbps
2,000	60 Mbps

Maximum Processing Capacity

Messaging can successfully process up to **4000 messages per minute** (combined email and voice) without loss of data, regardless of the number of users. This includes messages left on and retrieved from the system. Traffic loads in excess of this value may result in some loss of information or a decrease in performance.

Storage Capacity

The maximum storage capacity for the system is not a function of the software, but a limitation on the hard drive space available. Be sure to allot sufficient space to handle the expected voice and email traffic for all users, as well as the average time each message is kept on the system before being deleted.

Hard Drives

Avaya IX Messaging must be installed onto servers with a system with a RAID 10 array. Database performance is tied to hard disk performance. RAID 10 provides the same or faster read/write speeds when compared to a single hard disk.

Requirements for High Availability Installations

In addition to all of the normal specifications, High Availability installations have several other requirements that must be met:

- All servers must be in the same local area network.
- All servers must have a minimum 1 GB/s connection to the network.
- The maximum round-trip latency between the servers must be no more than 10 ms.
- The maximum round-trip latency between the voice servers and the PBX must not exceed 200 ms. Optimal round-trip latency is less than 150 ms.
- The path of connectivity must have 20 MB/s guaranteed bandwidth with no steady-state congestion.

Language Support

The languages supported by Messaging in Release 10.8 are:

Chinese (CN, Mandarin)	French	Portuguese BR
Chinese (HK, Cantonese)	French EU	Russian
Chinese (TW, Traditional)	German	Spanish
Dutch	Italian	Spanish EU
English	Japanese	Thai
English UK	Korean	
English AU		
English NZ		

One language is included with the program license, with the files for standard English included with the installation package. Other languages (see the table above) are available for download from Avaya.

Language licenses are not specific to a language. Multiple concurrent languages can be enabled by purchasing additional languages for the license.

All documentation is available in English only.

Pre-Installation Considerations

Avaya IX Messaging uses a dedicated server to enable high performance operation of the program. Other applications running on the same server as Messaging 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.

Before installing Avaya IX Messaging, you must have:

- the corporate telephone system and PBX installed and functioning properly.
- the voice server computer operating system installed and fully patched.
- a connection between the voice server to the corporate network and to the Internet.
- all email clients setup and operating according to specifications.
- created all accounts on any cloud-based applications where necessary (i.e. Google Apps).

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

Some additional items to consider before installing the voice server:

- How many users will there be in each category - voice / email / fax?
- The expected number of messages of each type per day.
- The number of corporate sites / office locations that are being serviced.
- On-premise versus off-site / mobile traffic.
- Integration with email clients and cloud applications.
- Disaster recovery and redundancy planning.
- The impact of the voice server on network traffic loads and Internet traffic.
- How will Messaging affect any integrated 3rd party and cloud based applications? Email servers?
- What additional software drivers will be required? (i.e. MS Word)

Estimating the Maximum Numbers of Users

Voice Users

Based upon testing by Avaya, Messaging supports up to **80,000**[1] users (see the table below for test criteria). Adding users above this value could impact performance, and may lead to loss of data.

CALCULATING AVAYA IX MESSAGING LIMITATIONS FOR VOICE TRAFFIC

Total Number of Mailboxes Supported based upon Performance Testing = 80,000[1]

Assumptions	
% Heavy Users	5%
% Medium Users	30%
% Light Users	65%
# Daily Voice Messages for Heavy Users	15
# Daily Voice Messages for Medium Users	5
# Daily Voice Messages for Light Users	1
Average Message Length (sec)	40
Average Call Length (sec)	60
Number of Channels	2,400
Operating Hours per Day	13

Test Results	
Total Voice Messages per Day	232,000
Total Calls per Day[2]	464,000
Total Call Minutes per Day	464,000

1 This is 80,000 users in total, with **up to** 20,000 of those being Advanced users.

2 Each message is left on the system by the caller, then retrieved by the callee, requiring 2 calls to complete the messaging process.

Legacy Licensing (Esna)

This section applies to customers with existing licenses issued by Esna. For Officlinx / IX Messaging licenses purchased through Avaya, please refer to the WebLM Licensing (Avaya) section on page 28.

Soft License

Avaya IX Messaging 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. Messaging uses this connection to periodically contact the Avaya 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), Messaging 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 Messaging has been installed and is operating, the program will contact the Avaya 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 Messaging with details of the problem.

If the program detects that the license details are different between the Messaging 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 Messaging 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 (UCLicenseUpgrade.exe), verify the updated terms for the license, and click the “Set as Active License” button.

Until the license has been updated, Messaging 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 Messaging 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 Primary connects to the license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Primary. Therefore, it is imperative that the Primary 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 Primary.

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 reduce to a single port with 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Messaging 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 connection problems).

WebLM Licensing (Avaya)

This section applies to current customers that purchased the product through Avaya. For long term customers that purchased Officelinx through Esna, please refer to the Legacy Licensing (Esna) section on page 26.

Soft License

Avaya IX Messaging program authorization is managed through a “soft” license. Activation of the program (UC, UM, eFax, etc.), capacity (ports and mailboxes) and features (ASR, TTS) is controlled by the license which resides on a server on your corporate network. Messaging uses the corporate network to regularly contact the Avaya WebLM license server to enable continued use of the program at the appropriate service level. If the connection to the license server 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.

Host ID and License File

During the initial installation, the administrator must create a Host ID from the WebLM License Server. This number is then sent to Avaya so that a license file can be generated and sent back to the customer. It is this license file that Officelinx / Messaging read to unlock the program features.

Afterwards, if the server hardware changes (i.e. the program has been moved to a new server), the license file must be replaced. Generate a new Host ID from the WebLM server and send that to Avaya Customer Service to receive an updated file.

Normal Operation

Once Messaging has been installed and is operating, the program is in constant contact with the WebLM license server 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 Messaging with details of the problem.

License Upgrades

To upgrade the Messaging license, such as adding new features or adding more ports or mailboxes, contact your customer service representative. The new details will be added to the license file and an email is sent to the administrator for them to refresh the license. You may be required to generate a new Host ID number from the WebLM server.

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 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 mailboxes licensed, there will now only 25 mailboxes available on the system. This reduction lasts for 60 days, with reminders sent to the administrator each day, and then Messaging 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 file 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 Primary voice server connects to the WebLM license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Primary. Therefore, it is imperative that the Primary 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 Primary.

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 the license server.

Demo Mode maintains all of the previously licensed features, but operational capacity is reduce to 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Messaging 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 connection problems).

License Expiration Milestones

These benchmarks apply to all licenses (legacy and WebLM).

Time Before Expiration	Action Taken
+90 days	eMail Administrator
+60 days	eMail Administrator
+30 days	eMail Administrator
+15 days to 0 days	daily eMails to Administrator
License Expires	
Demo Mode	

Licensing Grace Periods and Actions

Condition	Grace Period	Action Taken after Grace Period
Failure to authenticate license	28 days	Demo Mode
Upgraded license not activated	28 days	Demo Mode
1st Hardware change	-	Refresh license to continue
2nd Hardware change	-	Demo Mode
License Mismatch (not an upgrade)	-	Demo Mode

Network Requirements and Specifications

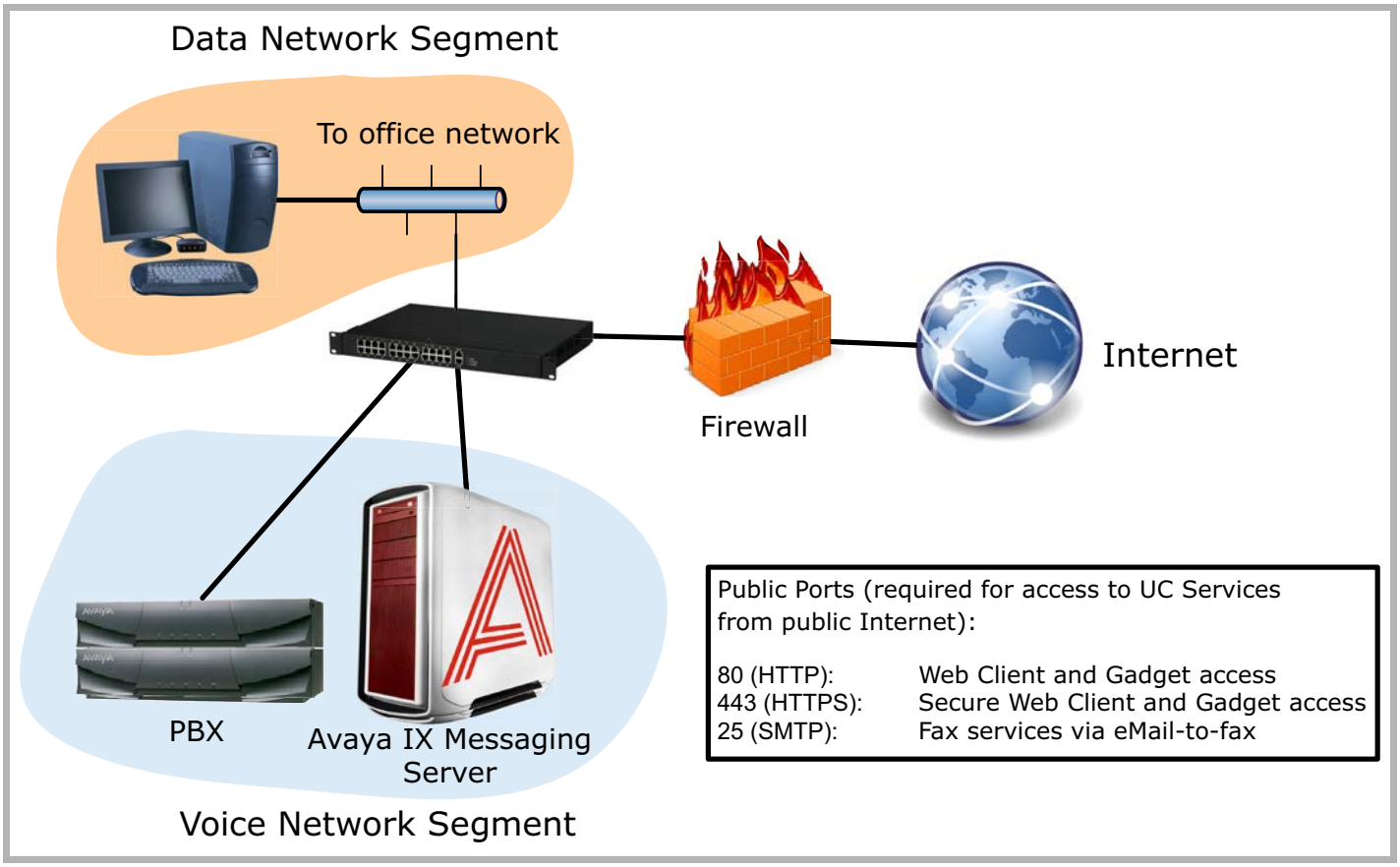
Avaya IX Messaging can exist as a standalone server on a local area network which allows for network-based user and system administration.

For proper deployment, connect the Messaging server through the NIC interface and then boot up the server. A 1GB/s or better connection is recommended, but 100 kbps is acceptable.

Warning: There can be a maximum of **2** network cards installed in a single server computer.

Note: The Messaging server must be provided with sufficient administrative rights to the network so it can co-exist as another workstation on your local area network. For more information contact your LAN Administrator.

The following is an example of how Messaging can be configured within an organization's network. By having a network infrastructure as shown here, you can ensure the functionality of the Messaging server within the organization while protecting all assets through the necessary security measures (e.g. firewall) from Internet or other external connections.



Before adding Messaging, you must have on of the following operating systems installed and fully patched:

- Windows Server 2012 or 2012 R2 - Standard Edition
- Windows Server 2016
- Windows Server 2019

Caution: The MAC operating systems is NOT supported for the voice server.

Note: It is recommended that the operating system be installed on a partition with at least 100 GB of space. This is in addition to any space requirements set aside for Avaya IX Messaging.

Note: Disable the User Access Control (**UAC**) feature of Windows to ensure proper operation of the software. Refer to the Server Install Guide for more details.

TCP/IP ports used by the application

PORT #	SERVER / CLIENT APPLICATION	SERVICE	DIRECTION	TCP/IP	UDP	SINGLE SERVER	PRIMARY SERVER	SECONDARY SERVER (S)	CONSOLIDATED SERVER	CSE SERVER	REQUIRED
25	VPIM-Smart Host Supported	Used for VM networking	Out	SMTP		●	●	●	●		1
80	Web Access		In	HTTP		●	●	●	●		●
135 *	MAPI/RPC	Contact and Calendar Synchronization	Both	MAPI/RPC		●					
389	LDAP Connector	AD Synch	Both	LDAP		●			●		2
443	Web Access	IIS Secure Services	In			●			●		●
443	Access to OEM Avaya	License Service	In	HTTPS		●	●				●
445	Microsoft File Sharing	File Sharing	Both	TCP			●	●	●	●	●
465/587	SMTP VPIM Google Mail	Mail Common	Out	TLS/SSL		●			●		●
2439	Sybase Mobilink	Database Connection	Both	TCP			●	●	●		●
2638	IXM Admin Sybase	MMC Service	Both	TCP		●			●	●	●
5060	SIP Channels	Voice Application	Both	SIP	UDP [3]	●	●	●			●
5061	SIP Channels	Voice Application	Both	SIP	TLS						
8201	UC Nuance Loader - Speech	Server/Client ASR	Both	TCP	UDP	●	●	●			●
10008 [4]	AACC	Call Center Integration	Both	TCP		●	●				
11000	UM Monitor	Local App Services	Both	TCP	UDP	●	●	●			●
12000	WebLM	License Service	Both	TCP		●	●				
13777	iLink Pro Desktop	UC Mobile	Both	TCP		●			●		●
13780	ASR Distributed	Speech Service	Both	TCP	UDP	●	●	●			●
13888	CTIClient Manager	UC CTI manager	Both	TCP	UDP	●	●	●	●		●
20002-x	RTP Media	Voice Application	Both		UDP	●	●	●			●
52233	WebLM	License Service	Both	TCP		●	●				
†	Nuance Speech Suite	Nuance Watcher Daemon	Both	TCP	UDP	●	●	●			

1 - Only required for sending messages via SMTP.

2 - Only required for LDAP synchronization.

3 - Only required for SIP with a Dialogic Media Gateway.

4 - Only required for Call Center integration with AACC environments.

* - Calendar and Contact Synchronization use MAPI, which uses RPC (Remote Procedure Call). RPC port assignment is handled dynamically, with port 135 used to locate the correct port. Both 135 and the MAPI / RPC ports must be open.

† - These port numbers are automatically assigned by the operating system. All associated traffic is local and no firewall adjustments are required.

For more information, click here: **http://technet.microsoft.com/en-us/library/cc875824.aspx**

Software Requirements

Minimum software requirements to run the Avaya IX Messaging server:

Software	Version
OS	Windows Server 2012 R2 - Standard Edition Windows Server 2016 Windows Server 2019
ASR	Nuance 10
TTS	RealSpeak 4.0 or 4.5

Media Support Requirements

If you wish to utilize additional media support within the voice server (e.g. DOC or DOCX support for fax), you must install the necessary components on the server so that the file formats can be recognized. Please refer to the chart below for requirement examples.

File Format	Application Required	Comments
DOC, DOCX	Microsoft Office	Required for additional file format support.

Note: The Remote Printer feature of Avaya IX Messaging can be used to redirect printer/fax traffic to another computer that already has the necessary licenses installed. Please refer to chapter 18 of the Feature Guide.

Note: Avaya IX Messaging versions prior to 8.2 require a separate application, such as Windows Media Player, to access MP3 files. Starting with version 8.2, Messaging supports MP3 files natively, with no additional software required.

ANTIVIRUS Software Installation

Avaya IX Messaging has only been validated with Norton Anti-virus Corporate Edition. Other anti-virus software applications that have been installed with Messaging are:

- McAfee VirusScan
- BitDefender

Note: Please ensure that, after installing your antivirus program, the UC folder and all of its subfolders are excluded from the scan. Scanning the UC folder can significantly decrease performance.

Fax Support

Messaging supports the Group 3 (G3) fax protocol, which conforms to the ITU-T specifications for T.30, T.4 and T.6.

Hardware Requirements

This table displays the recommended hardware values for different numbers of users, and the different types (single server, HA) of Avaya IX Messaging installation. Use these values to guide design and scope considerations for a new site.

For all sites:

- All processors are to be 2.0 GHz or better.
- All hard drives must be high performance, server grade drives.
- Configure the CPU for **Performance** mode in each server's BIOS settings.
- Virtual CPU's (vCPU) are shown as hyperthreaded and can be cut in half to equal physical cores.
- The same configurations can be used for both **physical** and **virtual servers**.
- Avaya IX Messaging must be installed onto servers with a RAID 10 array.
- Fragmentation management software, such as **Diskeeper**, should be installed on each server to prevent any drop in performance. This can be scheduled to run primarily during off hours.

SAN Usage

Storage Area Network (SAN) devices can be used with Messaging if they meet the necessary specifications.

- The device must provide a sustained throughput capacity of 250 requests per second, with peak traffic of up to 500 requests per second.
- This traffic is split 20% / 80% for read / write operations respectively.

Table Key

Profile: Use this tag to identify to your vendor which system configuration meets your needs.

 # CPU: The number of cores the server requires to quickly process data. All should be Intel® 2.0 GHz or better. The number of cores can be reached either through physical CPU cores, or by using Hyper-Threading Technology if available.

RAM: The amount of memory that each server must have.

Storage: This is the amount of storage space required for the hard drive where Avaya IX Messaging is installed.

Note: Running **Carbonite Availability** backup software requires additional space on the IXM Drive. Make sure that there is at least twice as much free space on the drive as is occupied by the program's files. For example, if there are 100MB of files, the IXM Drive must be at least 200MB in size. Carbonite needs this space to create the initial swap files before passing the data to the backup server. The specifications for Carbonite servers is the same as for the live voice servers.

Content Synchronization Engine (CSE): This is the server that will perform the sync with Gmail, Office 365, and MS Exchange.

Important: The **operating system** for each server must be on a different partition, or on another hard drive, than Avaya IX Messaging. The drive for the operating system must be **100 GB or greater**.

Recommended Configurations

The listed specifications are for each instance of the application. For example, in an HA environment, a minimum of 3 servers are required (Primary, Consolidated, and 1+ Secondaries). Each server must be appropriately configured.

All systems must use a RAID 10 (RAID 1+0) configuration.

For Standalone Deployment (SA)

SEAT LICENSES	PROFILE	Stand Alone Solution		
		# CPU	RAM (GB)	Storage (GB)
1-1000	SA1	4	8	400
1001-4800	SA2	8	16	400

For High Availability Deployments (HA)

SEAT LICENSES	PROFILE	Primary / Secondary Voice Servers			Consolidated Server		
		# CPU	RAM (GB)	Storage (GB)	# CPU	RAM (GB)	Storage (GB)
1-5000	HA1	8	16	400	8	16	400
5001-10000	HA2	8	16	600	8	16	600
10001-15000	HA3	8	16	700	8	16	700
15001-20000	HA4	8	16	900	8	16	900
20001-40000	HA5	8	32	1100	8	32	1100
40001-60000	HA6	8	32	1800	8	32	1800
60001-80000 [1]	HA7	8	32	2600	8	32	2600

1 - This is 80,000 users in total, with **up to** 20,000 of those being Advanced users performing UM sync.

For Unified Messaging Sync Users (UM)

UM USERS	PROFILE	Each Content Synchronization Engine [2] [3]		
		# CPU	RAM (GB)	Storage (GB) [4]
1-3000 (SA)	N/A	CSE Running on Voice Server		
1-5000 (HA)	N/A	CSE Running on CS [5]		
5001-10000 (HA)	UM1	8	8	600
10001-15000 (HA)	UM2	8	8	700
15001-20000 (HA)	UM3	8	8	900

2 - The number of CSE Servers required depends upon the number of Advanced users that will be working on the system. One server is required for every **5,000 Advanced users**.

3 - Each Remote CSE Server supports a single email type (e.g. Exchange, Office 365, Gmail, etc.). If more than one email type is required, the Consolidated Server cannot be used for synchonization.

4 - Additional hard drive space may be required if full logging is enabled.

5 - For optional Remote CSE Server, use Profile UM1.

Note: Expanding your operation and moving from one profile to a larger one may also require changes to the system hardware (# CPU, RAM, Storage, etc.) needed to support it.

CSE Gateway Requirements

In order to use CSE, the IMAP mail server must support the following standards:

- Messaging integrates with MS Exchange 2010 / 2013, Gmail (Google Apps) and MS Office 365.
- IMAP services enabled on the email server
- IMAP services must be installed and fully operational prior to deploying Messaging with the IMAP Gateway
- MS Exchange 2010 / 2013 should be operational ahead of time if Messaging is desired
- User name and password (with permission) so UC can access user mailboxes on existing mail server
- Free IMAP TCP/IP port available between the Messaging and email server

Server Network Requirements

Networking requirements depend on what configuration and traffic load the system will bear. In most cases 100 Mbps (minimum 100BaseT) will suffice between the Messaging, IMAP CSE and the Email servers. In larger (500+ UC user) configurations a 1 GB/s network connection between the Messaging and Email servers is required. In such cases a 1GB/s layer 2-switch between all servers is also required.

The voice server can exist as a network-connected server on a LAN allowing for network-based user and system administration.

Server Email Integration Requirements

The Server can be a voicemail-only system although most deployments will involve some degree of email functionality.

Refer to **Server Messaging Type Characteristics And Deployment Scenarios on page 111** in this document for more information on the possible system deployment scenarios.

Message Compression and Storage

Depending on which deployment scenario you select, messages may be stored on the Messaging Server, on the Email Server or both.

For more information on deployment scenarios visit Deployment: Basic Unified Messaging on page 113.

It is very important that you know the message storage requirements of your particular environment. The following factors will affect this calculation:

- days to keep read messages
- days to keep unread messages
- message format used
- maximum message length
- maximum number of messages allotted per user (inbox only)
- number of Messaging users (must account for email on the Messaging Server)

The message format is the factor used to calculate storage capacity as the format determines the size of the actual messages.

File Format	KBytes/sec	KBytes/min	KB/hour	MB/hour	GB/hour
Wave A-Law 8kHz (G711)	8	480	28800	28.1	0.0275
Wave μ-Law 8kHz (G711)	8	480	28800	28.1	0.0275

In certain deployments where copies of voicemail messages are stored on the Email Server, storage capacities per email mailbox remain the same.

System Configuration Options

Messaging can be configured to support many user environments:

- Basic (Messaging)
  - Basic + ASR / TTS
  - Basic + Transcription
  - Basic + ASR / TTS + Transcription
- Advanced (Messaging & Collaboration)
  - Advanced + ASR / TTS
  - Advanced + Transcription
  - Advanced + ASR / TTS + Transcription

The following options which can be added to a license:

- SR140 Fax Ports
- ASR / TTS by user
- Transcription by user
- Upgrade the User type to Access Increased Functionality
- G.729 Support

Server Requirement Q & A

Please refer to the below Q&A article for a general understanding of the hardware requirement of the Messaging system.

What is a RAID 10 system?

RAID 10, also known as RAID 1+0 or RAID 0+1, is a RAID system where 2 drives are mirrored and then spanned with 2 other mirrored drives. This gives you the ability to lose 1 of each in the set in each mirror (1/2 of the drives) and still work at full speed. RAID 10 is required for all Avaya IX Messaging servers, physical or virtual.

How about RAID 6 or RAID 5?

RAID 5 and 6 would be an optimal choice if the Messaging system were to be a read only system. Unfortunately the act of writing burdens the RAID system since every log entry requires the entire span to be updated (parity needs to be updated with every change). If a RAID 5 or RAID 6 becomes fragmented there is a problem since small pieces of info will still take the entire stripe and parity needs to be calculated for every change once again.

What speed Hard Drives should we use?

Most typical server Hard Drives will be either 10,000 RPM or 15,000 RPM. Either one will suffice for the Messaging system. The 15,000 RPM drives are much hotter but are also 50% faster. The trade off is the electric consumption over performance. If it is a huge install base that has lots of UM with IP voice ports, we suggest the 15,000 RPM but this is not a requirement.

What can I do to increase the effectiveness of the RAID system?

An extra drive (one or more) may be configured as a hot swap spare. This is generally a good practice since it will automatically start rebuilding the RAID if one of the drives fail, removing the need for human interaction.

What is the total storage of a RAID system?

Total storage would be approximately ½ of the combined storage of all the drives.

Is there a numerical restriction on the RAID system?

The number of drives that can be used in the RAID system must be even, with 4 being the minimum (4, 6, 8 etc).

Can I install Messaging on an existing server that is already in use?

Messaging is a dedicated application which should only be installed as a **primary application** on any server. Sharing system resources with other applications may keep Messaging for working correctly.

3 INSTALLATION CHECKLIST

Overview

This chapter provides a check-list to employ when validating the success of any installation/integration of the Messaging 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

Test #	Description	Notes	Success
1	Direct call to hunt group.	The calling party number is expected to be contained in the From header of the Invite.	Y / N
2	Internal ring-no-answer forward.	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 **no-answer**.	Y / N
3	External ring-no-answer forward.	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 **no-answer**.	Y / N
4	Internal busy forward from a subscriber's station set.	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 **busy**.	Y / N
5	External busy forward from a subscriber's station set.	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 **busy**.	Y / N
6	Internal all call forward from a subscriber's station set.	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 **fwd-all**.	Y / N
7	External all call forward from a subscriber's station set.	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 **fwd-all**.	Y / N

Transfer Calls

Test #	Description	Notes	Success
8	Blind transfer to a station from messaging server where the destination answers the call.	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.	Y / N
9	Blind transfer to a station from messaging server where the destination does not answer the call.	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.	Y / N
10	Blind transfer to a subscriber's station from messaging server where the destination is busy.	The transfer should fail.	Y / N
11	Blind transfer to an invalid number.	The transfer should fail.	Y / N
12	Supervised transfer to a subscriber's station from messaging server where the user does not answer the call.	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.	Y / N
13	Supervised transfer to a subscriber's station from messaging server where the user answers the call.	The transfer completion speed and timing is up to the application.	Y / N
14	Supervised transfer to a subscriber's station from messaging server where the destination is busy.	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.	Y / N
15	Supervised transfer to an Invalid number.	The transfer completion speed and timing is up to the application.	Y / N
16	Outbound call to a subscriber's station that answers.	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.	Y / N
17	Outbound call to a subscriber's station that does not answer.	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.	Y / N
18	Outbound call to a subscriber's station that is busy.	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.	Y / N
19	Outbound call to an external number.	Depending on the state of the destination, the call will either be judged as connected, or fail due to busy / error tone conditions.	Y / N

4 DOWNLOADING AVAYA IX MESSAGING

Introduction

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

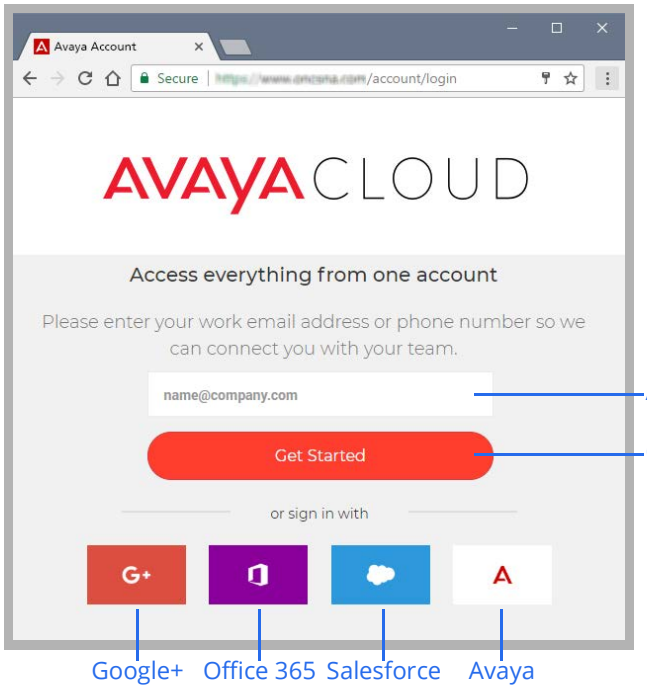
Download and save the file to a computer hard drive. It is a single, self-extracting executable file. Copy the file to the destination computer(s) and double-click to extract all of the installation files to the local hard drive.

Run the **Setup.exe** file to launch the installer.

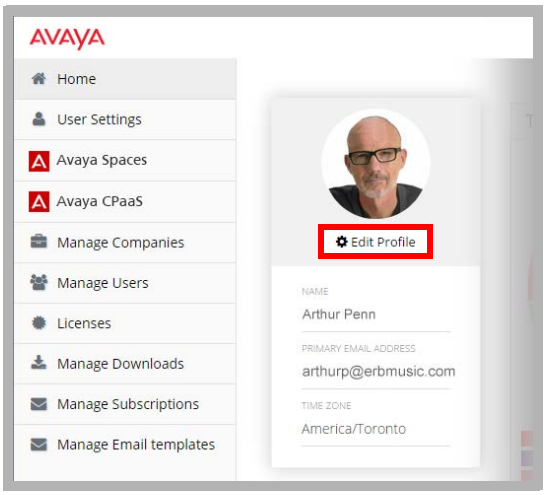
Downloading from accounts.zang.io

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**.

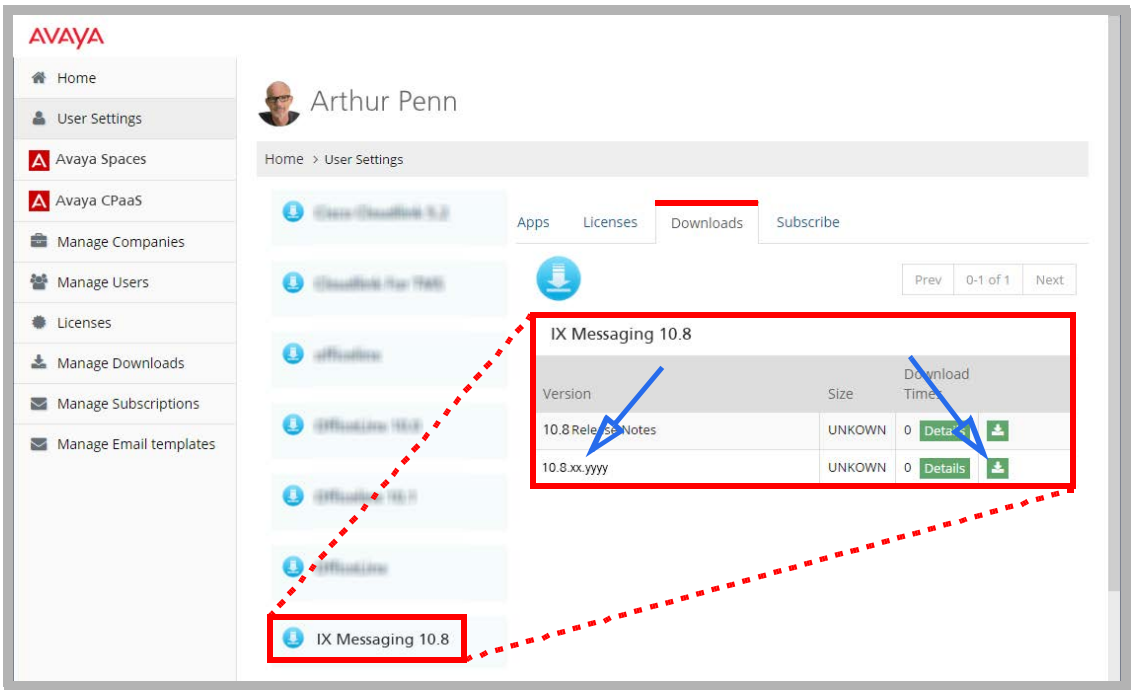
1. Open a web browser and go to https://accounts.zang.io. Create a new account (Get Started), or login using your existing credentials. You can also login using your Google+, Salesforce, or Office 365 account details.



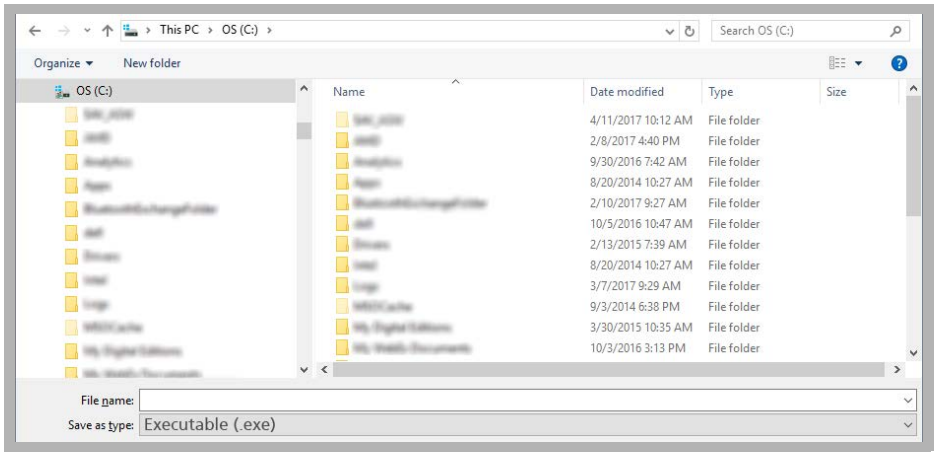
2. On the **Dashboard**, select **Edit Profile**.



3. From the **Downloads** tab, choose the version of Messaging 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 IX Messaging will be installed.

Continue with the chapter appropriate for your operating system (i.e. Windows 2016) or feature set (i.e. JITC).

5 WINDOWS SERVER 2019 INSTALLATION (SIP)

In This Chapter:

Introduction

When installing Avaya IX Messaging version 10.8, 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

Requirements	Details
License	A Full License for 10.8.
Software	For details on Messaging 10.8 Hardware and Software requirements please consult the Technical Operating Guidelines.

Important: Microsoft Windows is not provided with any version of IX Messaging. The customer must install and fully update a suitable, licensed version of Windows onto the hardware platform before proceeding with the Avaya IX Messaging software installation.

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

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

Caution: It is strongly recommended that, for Windows Server 2019, 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 Messaging voice server installation.

Installation Preparation

Deployment Configuration Considerations

- An Avaya IX Messaging 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 Messaging 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 Messaging. 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 2019, you must ensure that all the necessary server roles and features are installed on the system before proceeding with Messaging installation.

Digital Certificates

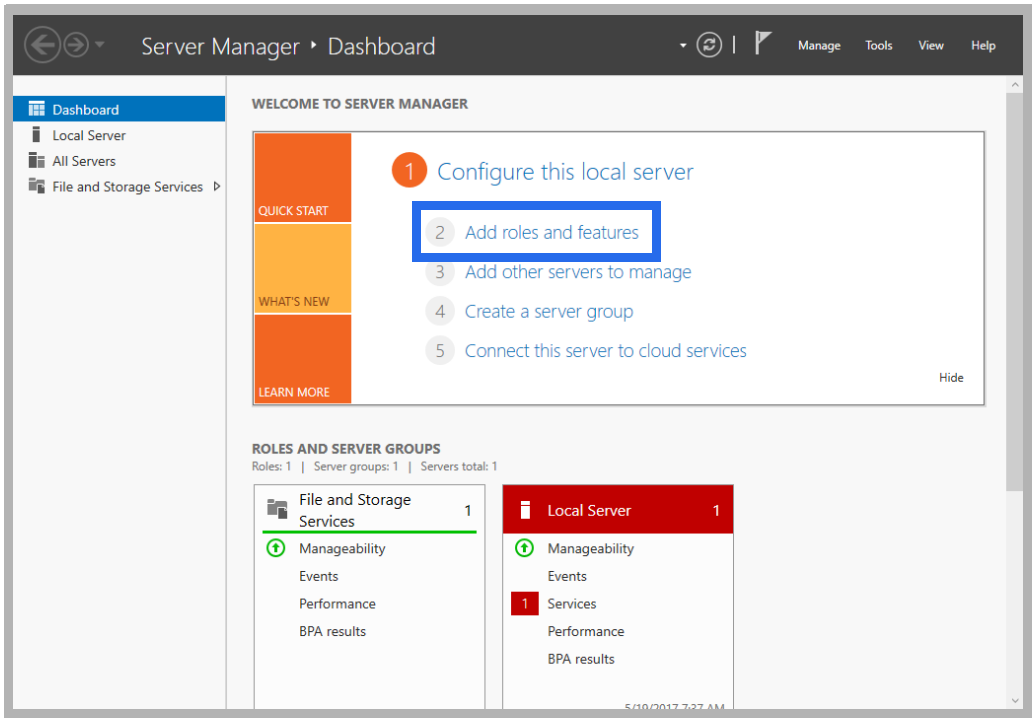
Avaya IX Messaging requires that signed digital certificates be installed on the voice server before attempting an installation.

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.

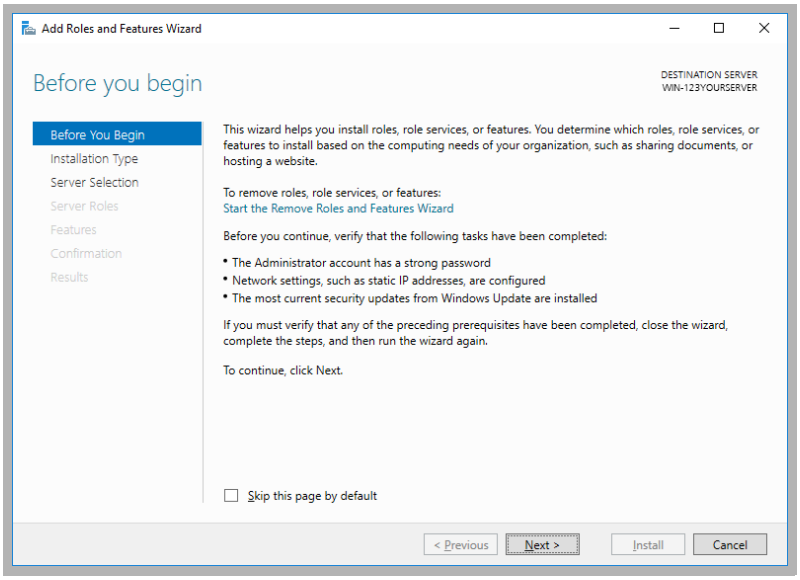
Server Roles and Features

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

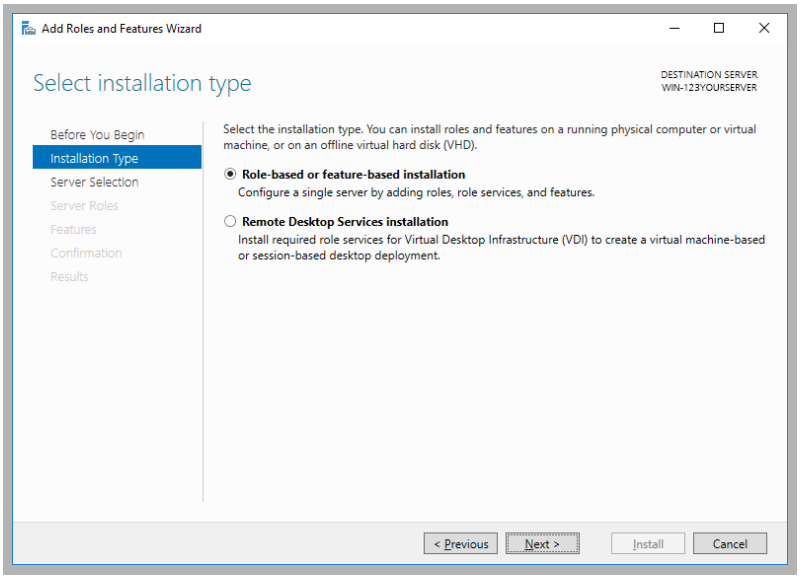


If this screen is hidden, go to **View** and select **Show Welcome Tile**.

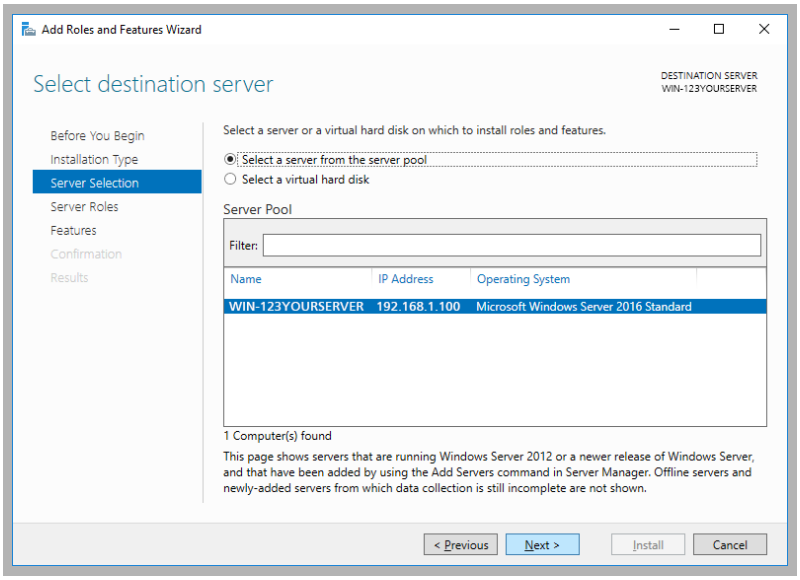
2. Click **Next**.



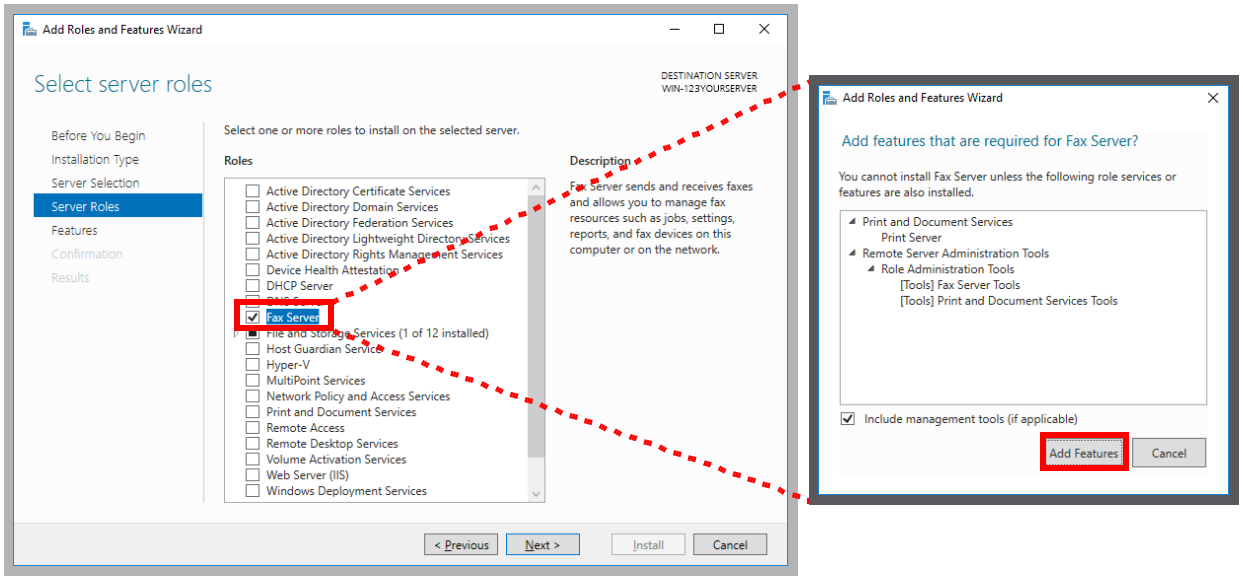
3. Leave the default settings as they are. Click **Next**.



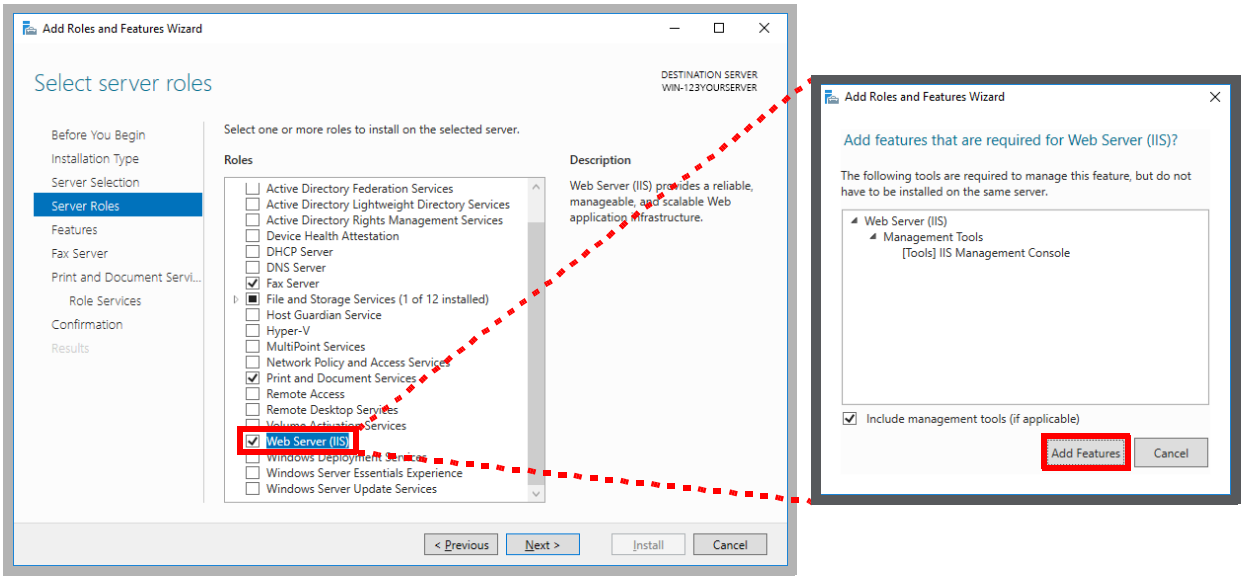
4. Leave the default settings as they are. Click **Next**.



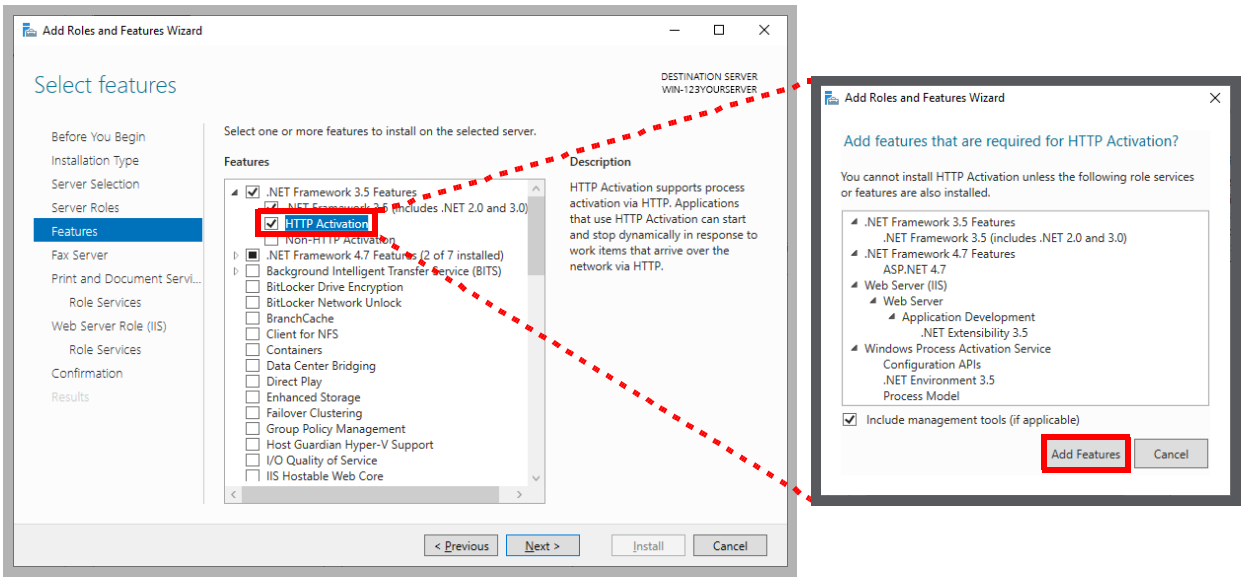
5. Enable **Fax Server**. When prompted, select **Add Features**.



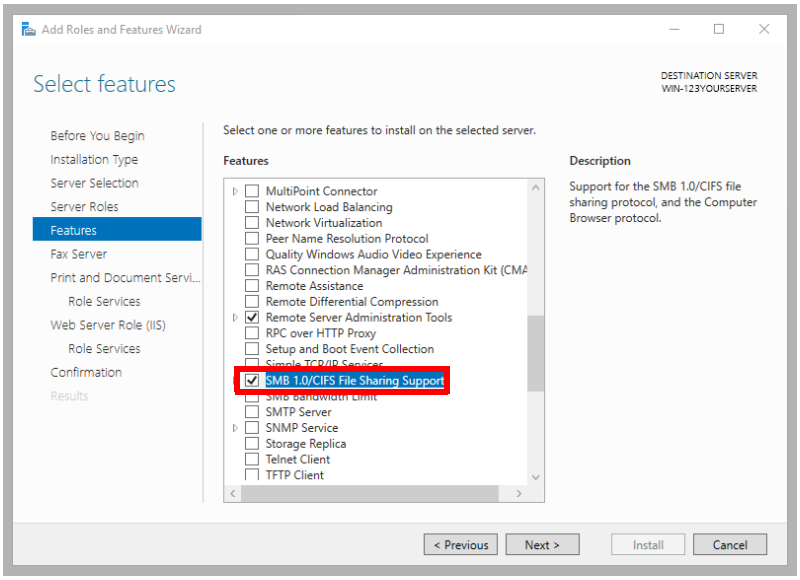
6. Enable **Web Server (IIS)**. When prompted, select **Add Features.** Click **Next**.



7. On the **Features** panel, open **.NET Framework 3.5 Features** and enable **HTTP Activation**. When prompted, select **Add Features**.



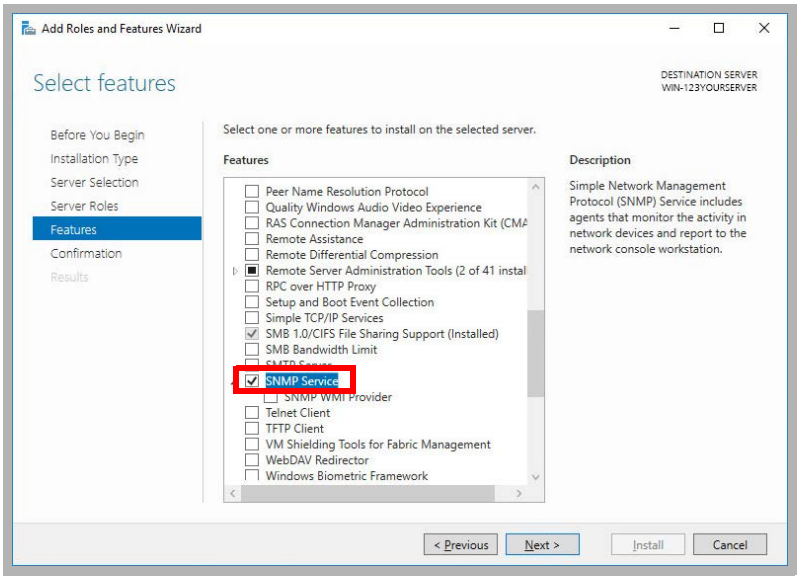
8. Scroll down and enable **SMB 1.0/CIFS File Sharing Support**.



9. **Optional**: If you plan to use **SNMP Alarms** with Messaging, the **SNMP Service** must be added to Windows before the program can be installed.

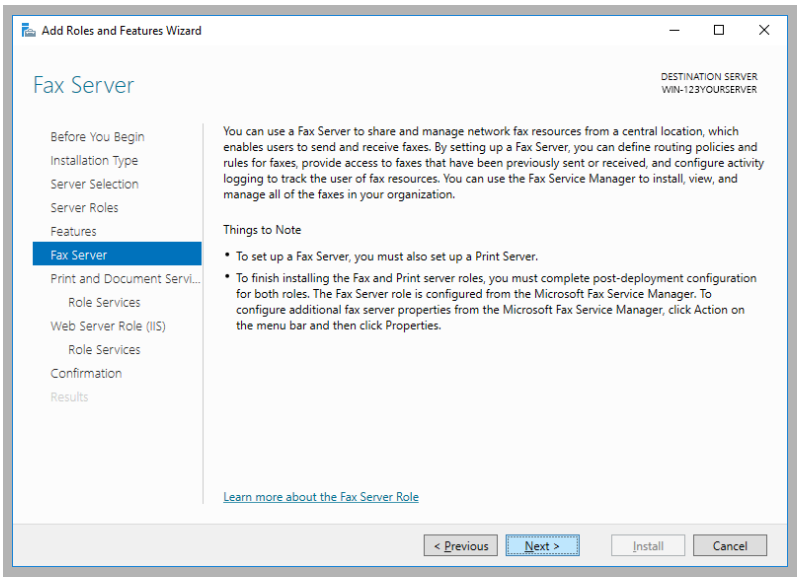
   If SNMP Alarms are required, scroll down and enable SNMP Service.

If SNMP Alarms are not required, skip this step.

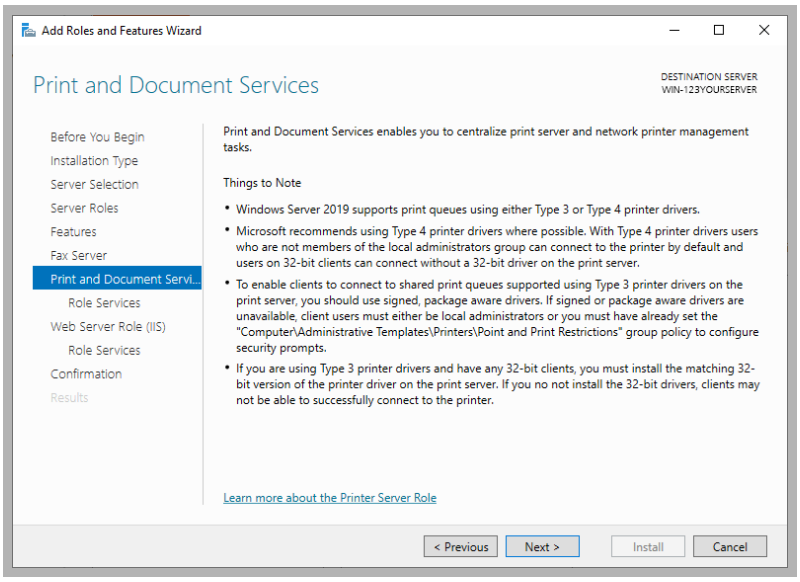


10. Click **Next**.

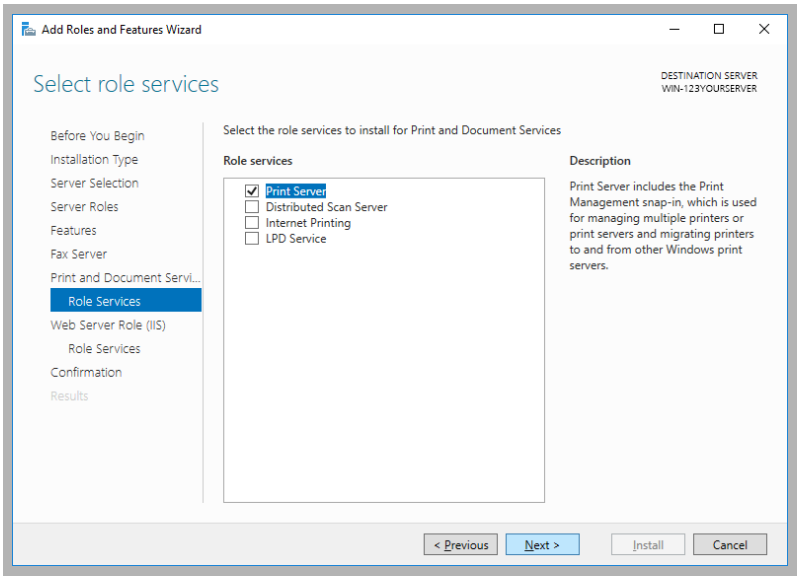
11. On the **Fax Server** screen, click **Next**.



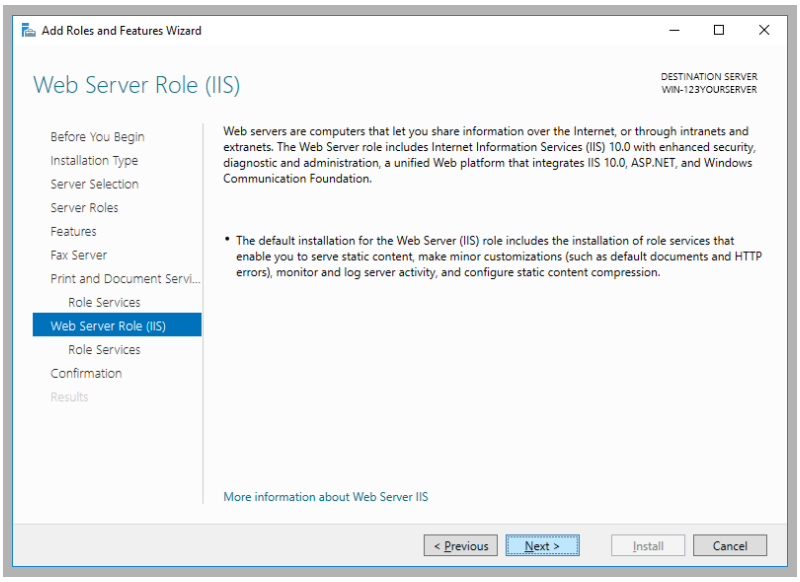
12. On the **Print and Document Services** screen, click **Next**.



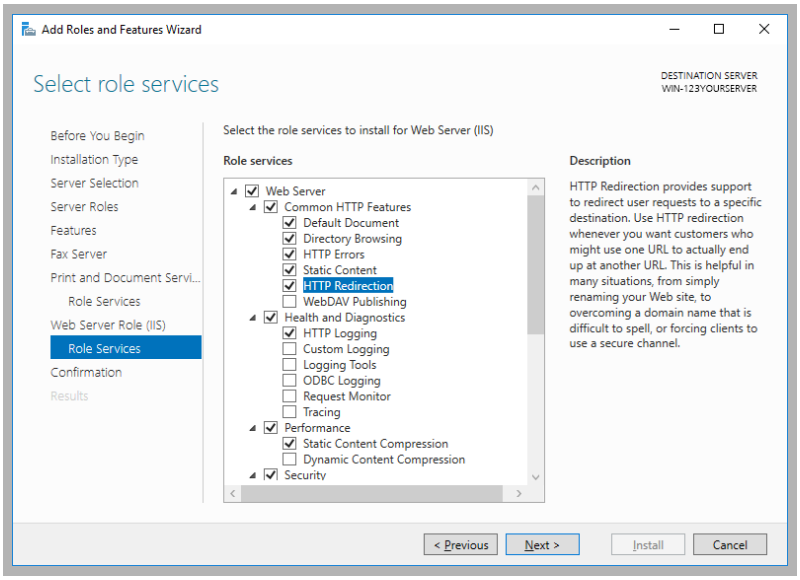
13. No changes are required here. Click **Next**.



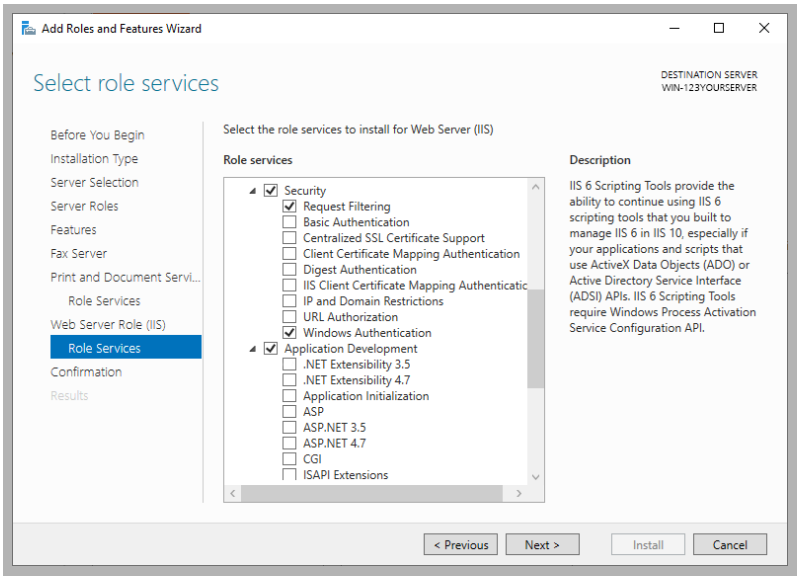
14. On the **Web Server Role (IIS)** screen, click **Next**.



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

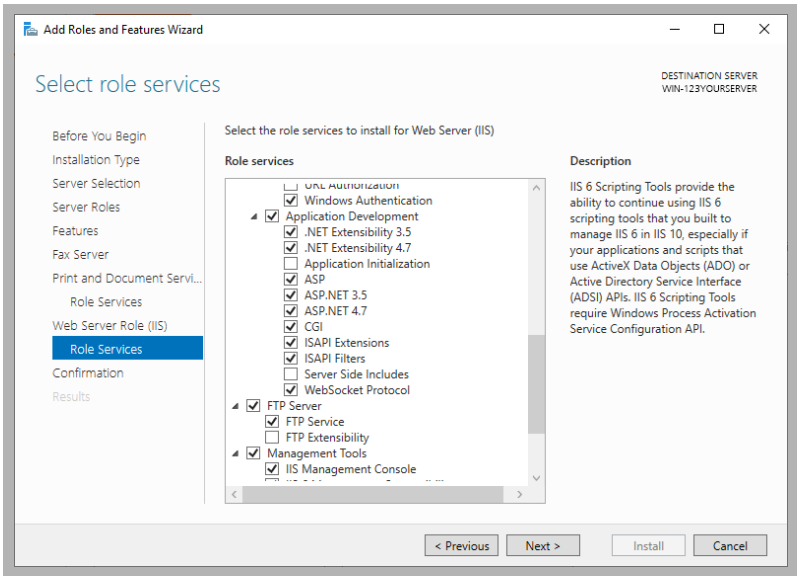


16. Under **Web Server > Security**, enable **Windows Authentication**.



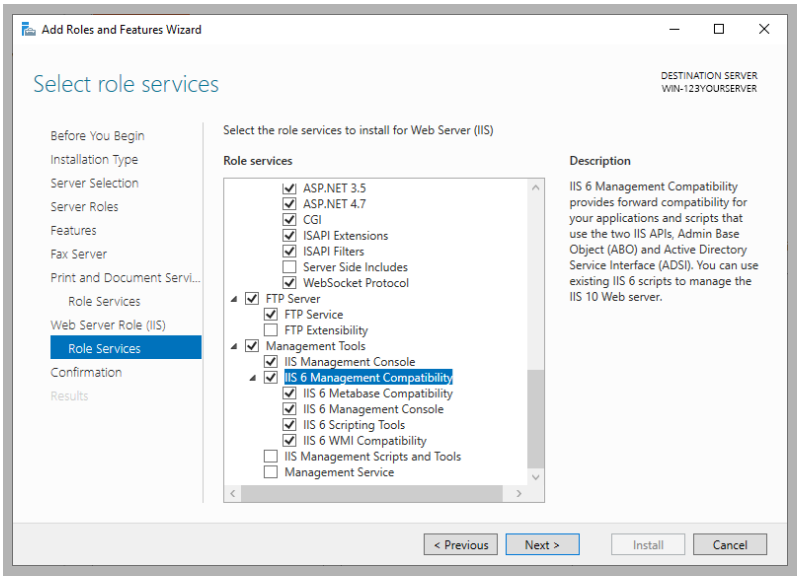
17. Under **Web Server > Application Development**, enable **.NET Extensibility 3.5**, **.NET Extensibility 4.7**, **ASP**, **ASP .NET 3.5**, **ASP .NET 4.7**, **CGI**, **ISAPI Extensions**, **ISAPI Filters** and **WebSocket Protocol**.

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

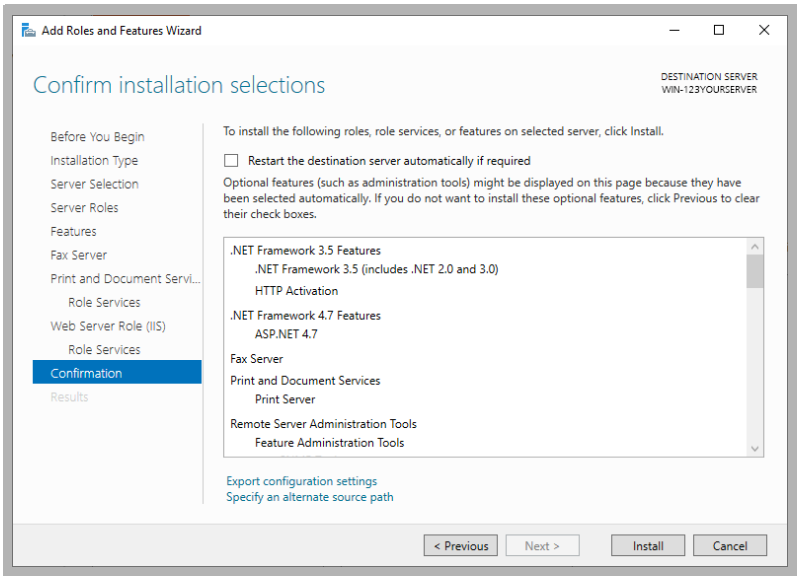


18. Under **Management Tools > IIS 6 Management Compatibility**, enable all items.

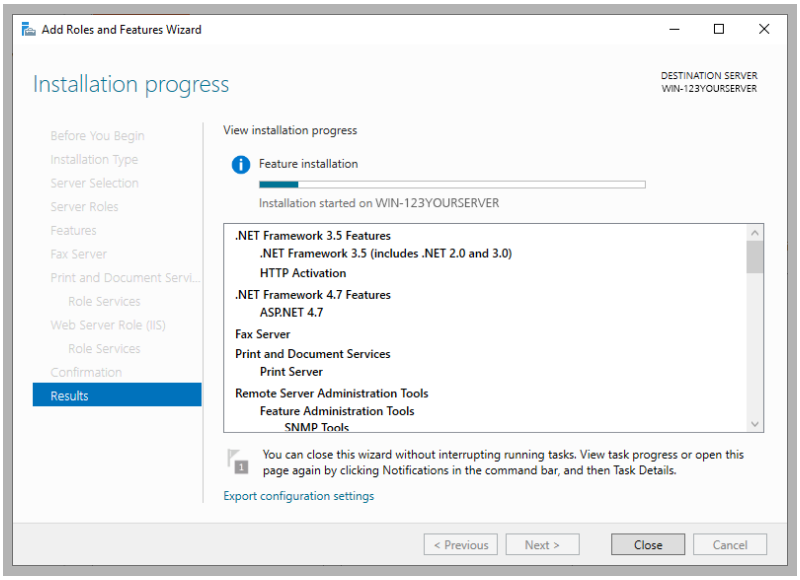
    Click **Next** when ready.



19. Review the selections here. When ready to proceed, click **Install**.



20. Windows will now start the installation process for the chosen items. This process may take a while.



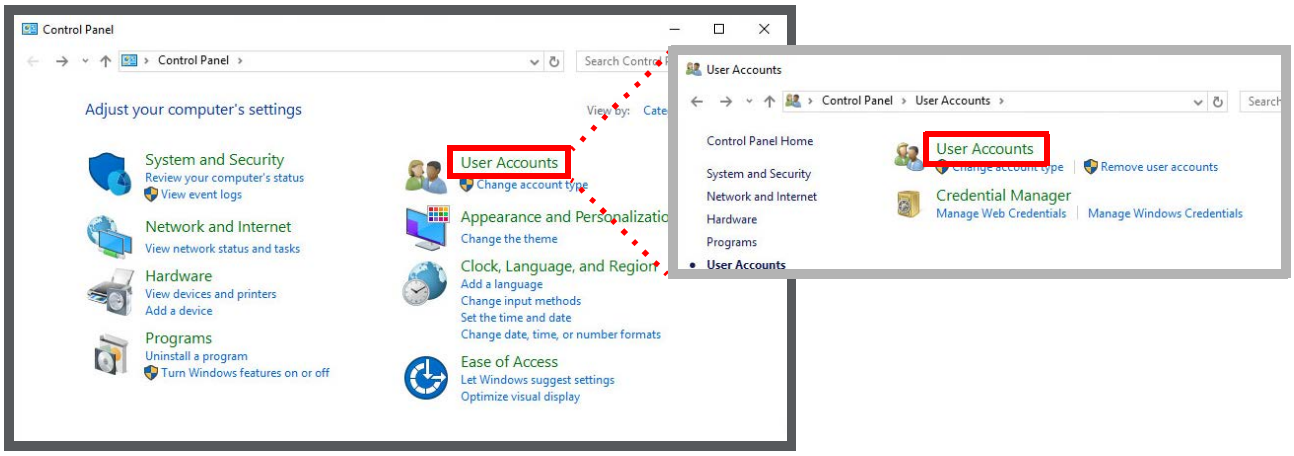
Note: This window can be closed without interrupting the installation procedure

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

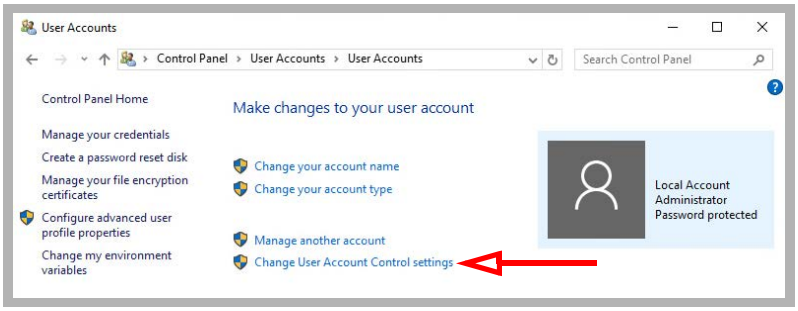
Disabling User Account Control Notification

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

   Again, click **User Accounts**.

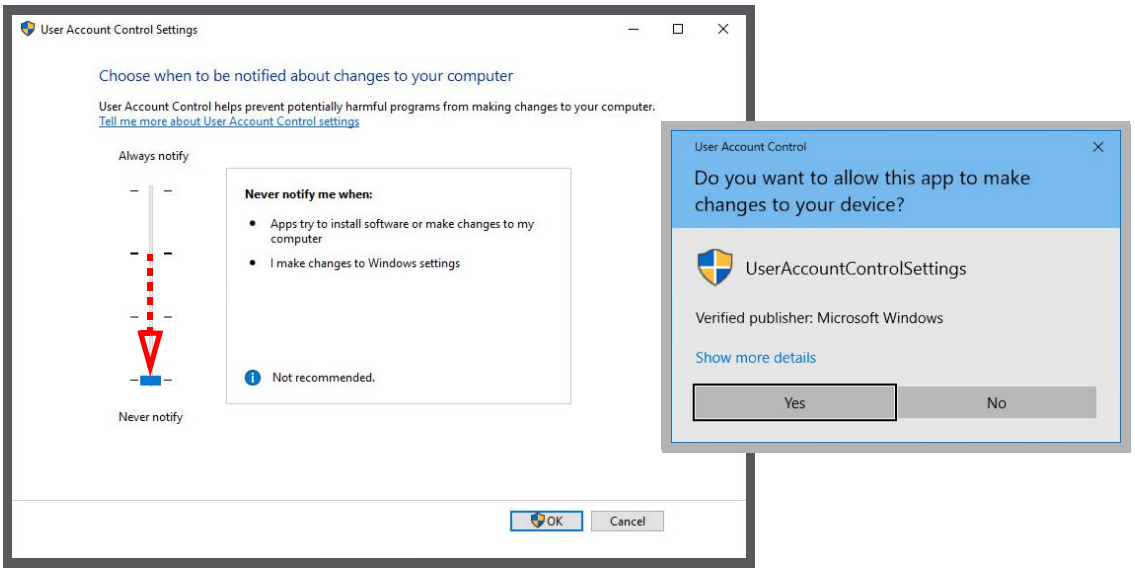


2. Select **Change User Account Control settings**.

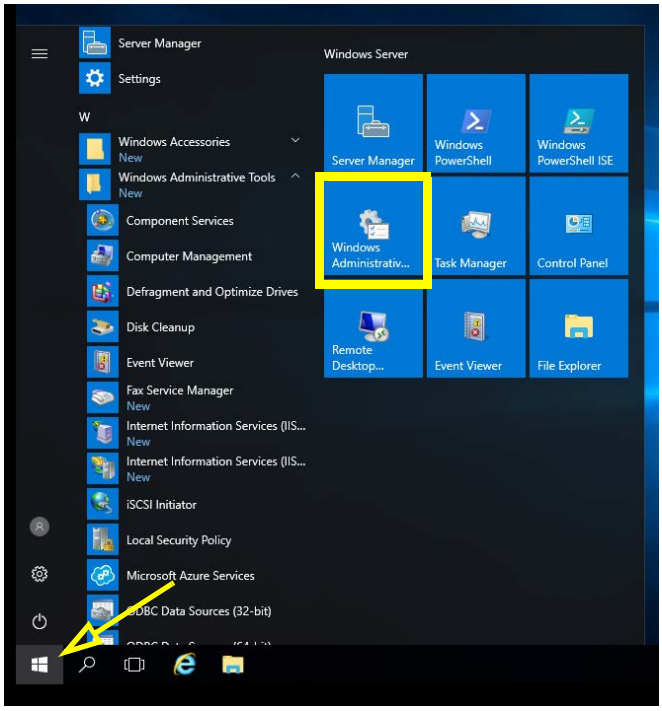


3. Click and drag the slider down to **Never Notify**.

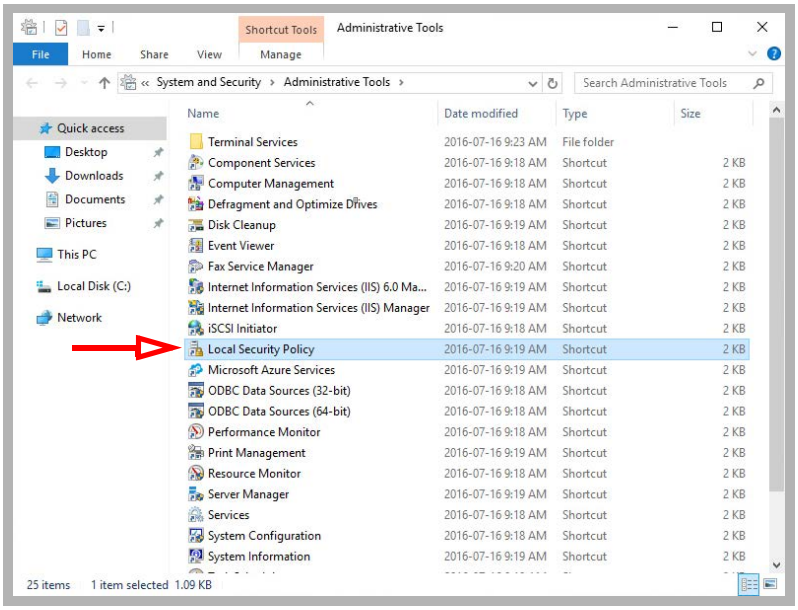
   Click **OK** and **Close**.



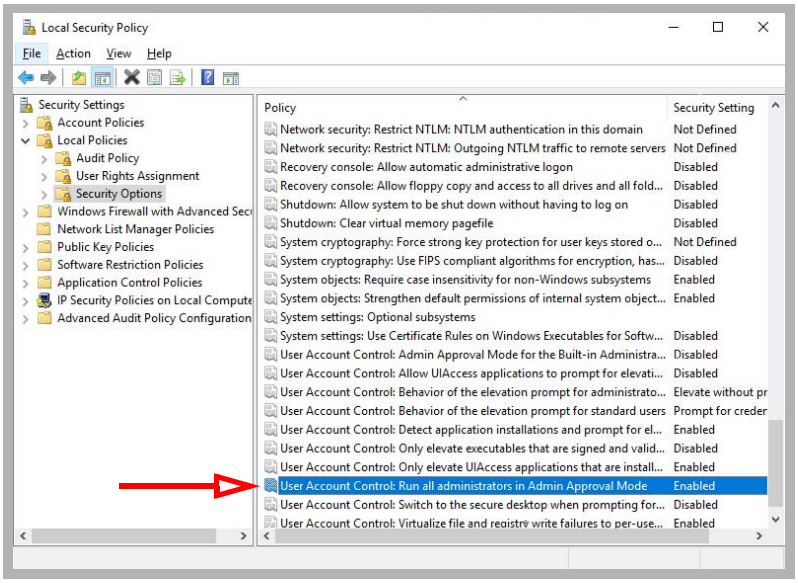
4. Open the **Start** menu and select **Windows Administrative Tools**.



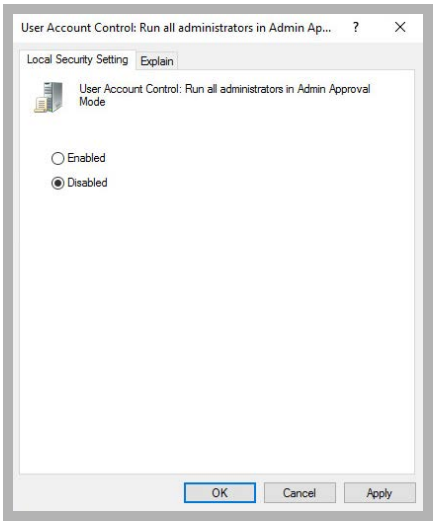
5. Double-click **Local Security Policy**.



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



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



8. Restart the computer to make the changes active.

Note: UAC Notifications can be restored after Messaging 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:

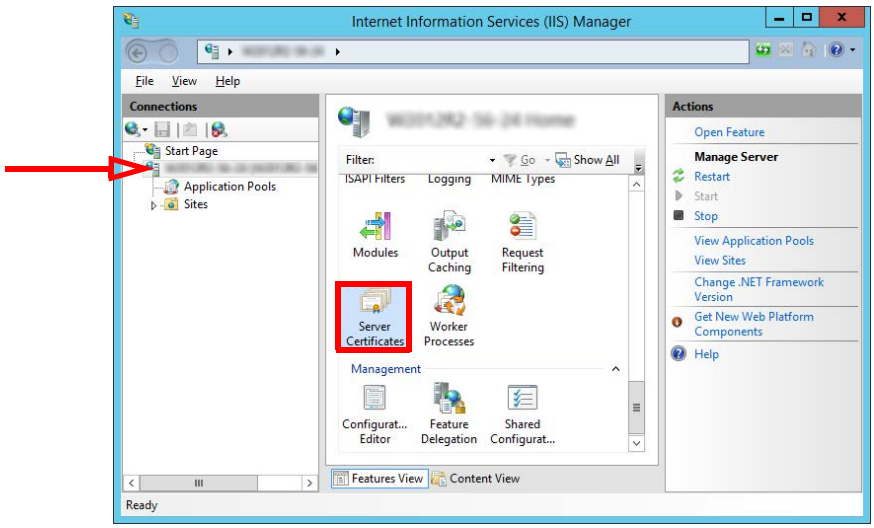
https://technet.microsoft.com/en-ca/library/cc753127(v=ws.10).aspx

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

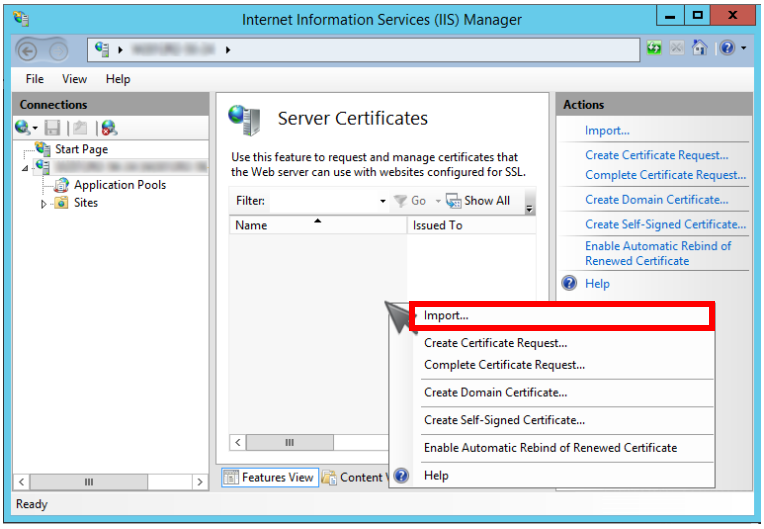
IIS Certificate Bindings

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

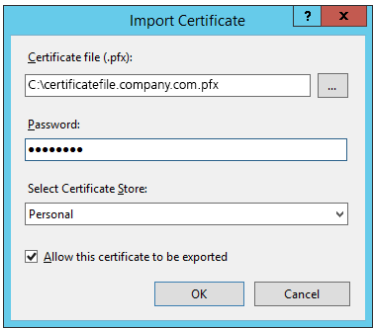
1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.



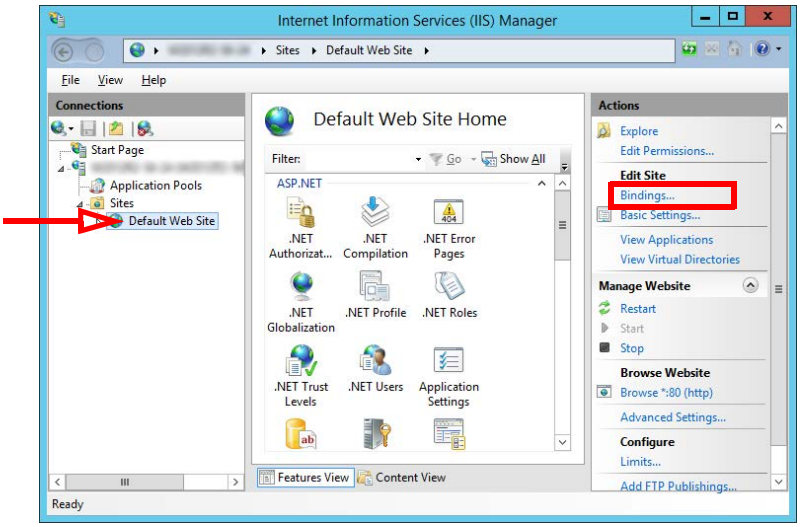
2. Right-click in the right-hand pane and choose Import from the pop-up menu.



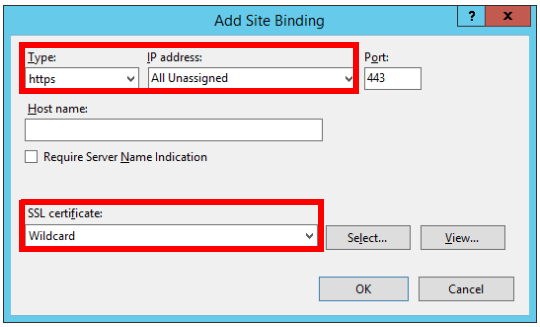
3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.



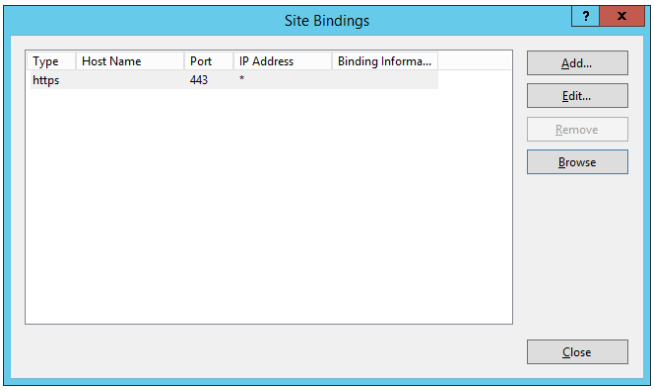
4. Go to **Sites > Default Web Site**.
Click **Bindings...**.



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 IX Messaging has not logged in as the system administrator, that user must be given full rights to the root of the C drive.

About Passwords

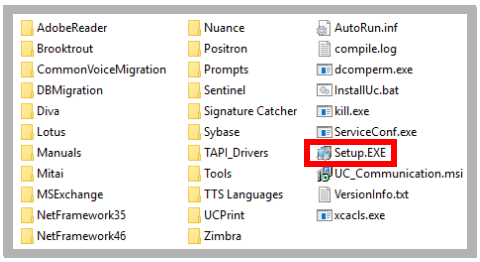
These rules are applied to all passwords created or used with Avaya Messaging, including those created during installation (Note: JITC installations have more stringent requirements). These include:

- **Length**: Passwords must be at least **14** characters long.
- **Class**: A password can contain upper and lower case characters, numbers and special characters. No minimum requirements for each character class are set by default, but this can be changed by the administrator.
- **Repeating Characters**: No character can be repeated more than 2 times consecutively (he**ll**o, world**!!**). This value can be modified by the administrator.
- **Repeating a Character Class**: No class of character can be repeated more than 4 times consecutively (ABCD, !@#$). This value can be modified by the administrator.
- **Reusing Passwords**: No new password can be the same as a previous password extending back 10 iterations. This value can be modified by the administrator.
- **Sharing Passwords**: Passwords must not be shared between users. Only one login per account is allowed at one time. Other users must login using different credentials.

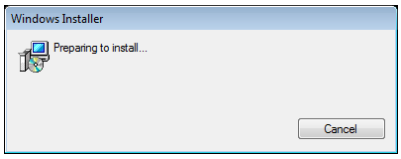
Note: Using an administrator account to perform routine functions leaves the servers open to malicious software attacks. Therefore, it is **strongly recommended** that each user with administrative privileges is also assigned a standard user account. To maintain security integrity, the administrator account should only be used when necessary, and should be immediately logged out afterwards.

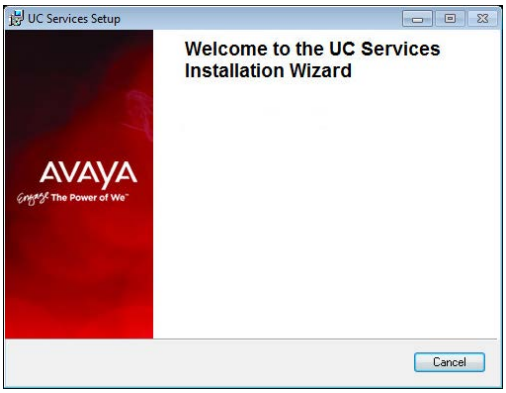
Procedure

1. Download the installation file (see chapter 4). 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 IX Messaging onto your voice server.





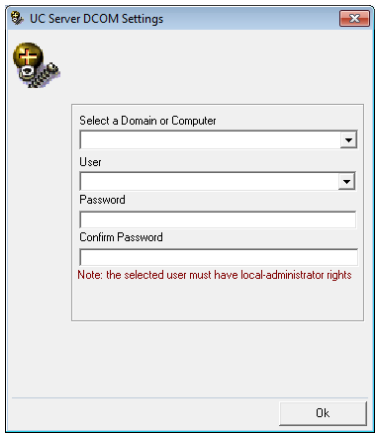
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging. They can also be downloaded from resources.zag.io in both PDF and HTML format.

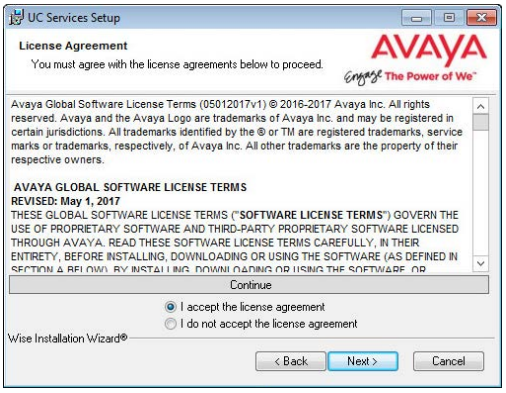
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.



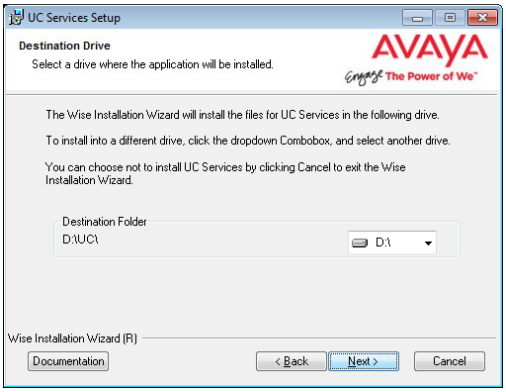
5. Review the license agreements and enable **I accept the license agreement**.

   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.

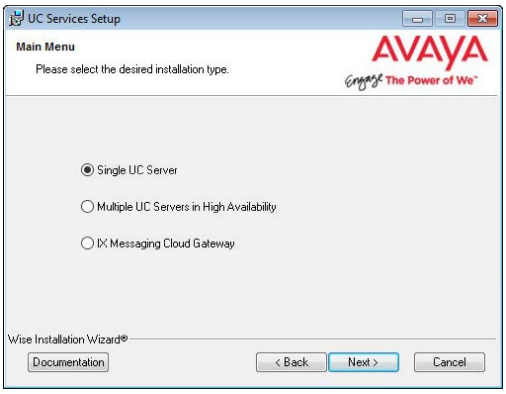
7. Enable **Single UC Server**.

   Click **Next**.

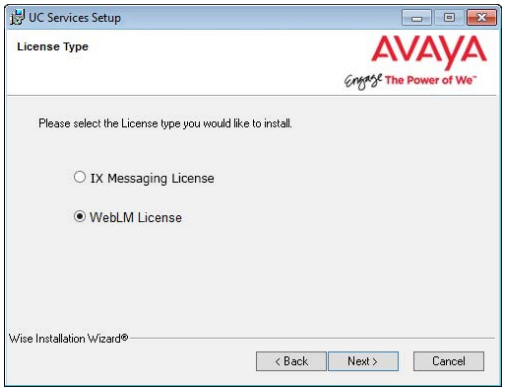
   Single UC Server: When operating Messaging on a single voice server computer.

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

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, 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.

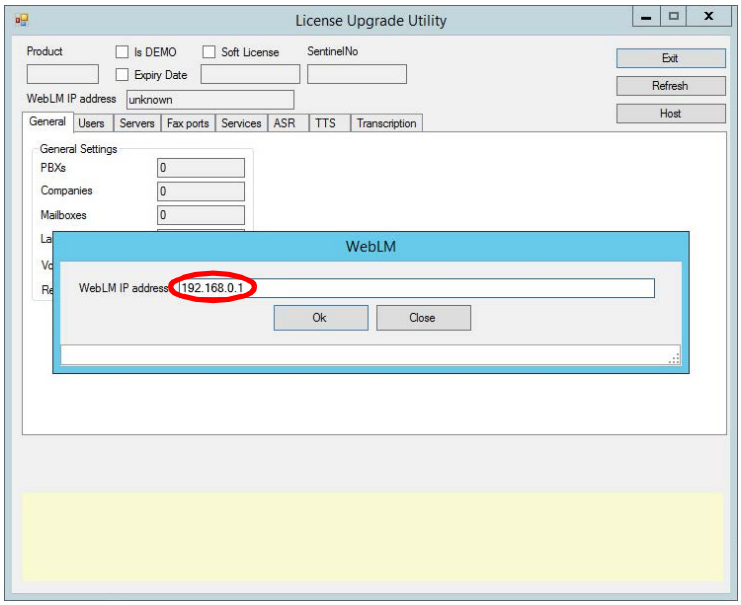


Note: If you select Messaging, go to **chapter 13, Installing the Messaging License**. When finished, return here and continue the installation from **step 11**. Skip step 9 through 10.

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.

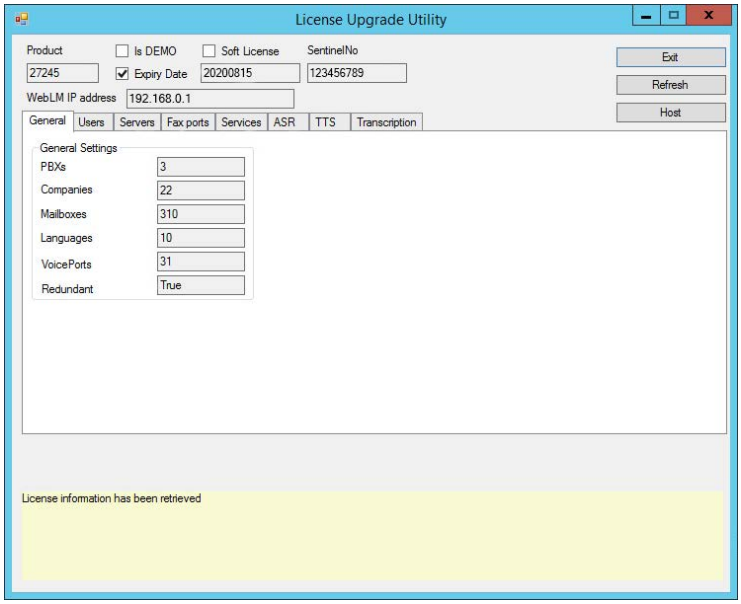
9. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   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 309.

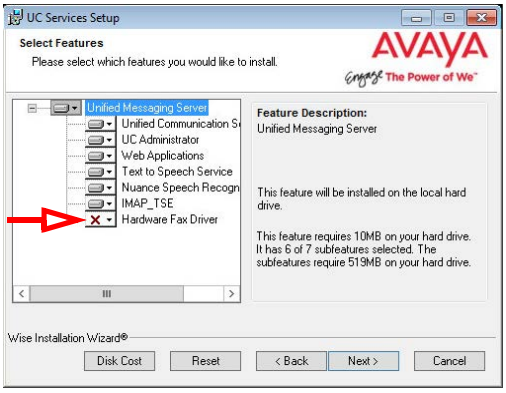
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.



Note: The number of voice ports is calculated based upon your license.
[(# Basic users + # Mainstream users) / 40] + Number of voice ports in license

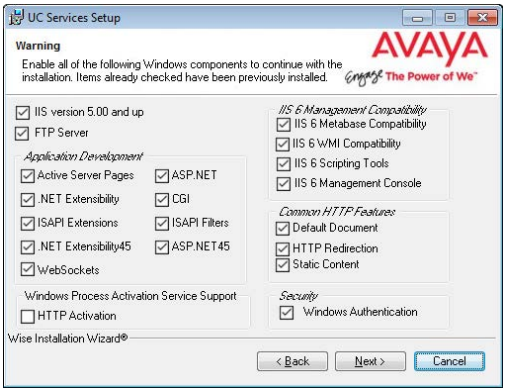
11. Select the **Components** required at your site. Disable any components that are not needed.

    Click **Next**.



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 Messaging requires to operate properly.



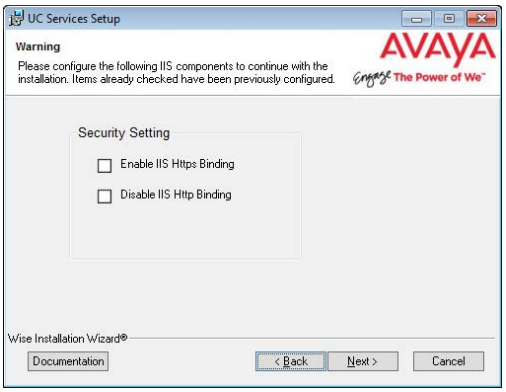
Note: This screen will only appear if one or more required components are **not** installed on the computer.

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 Messaging requires to operate.



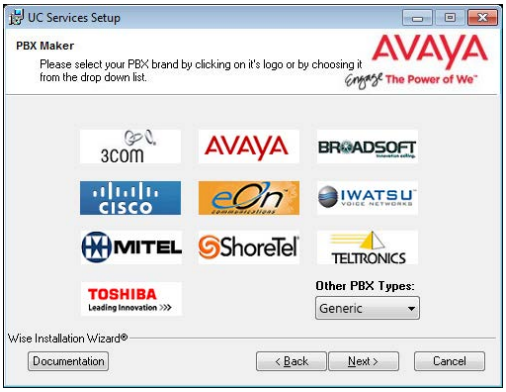
Note: This screen will only appear if one or more of the required settings has not been made on the computer.

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.

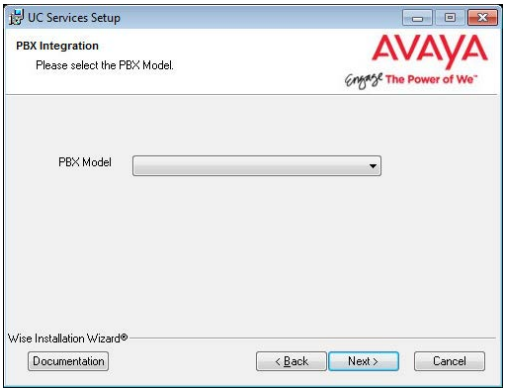
Note: The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

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



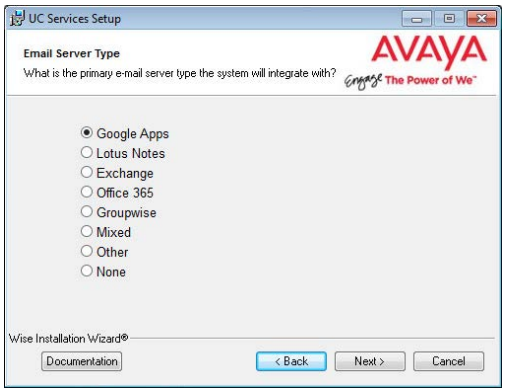
15. Select your PBX model from the dropdown menu.

    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.

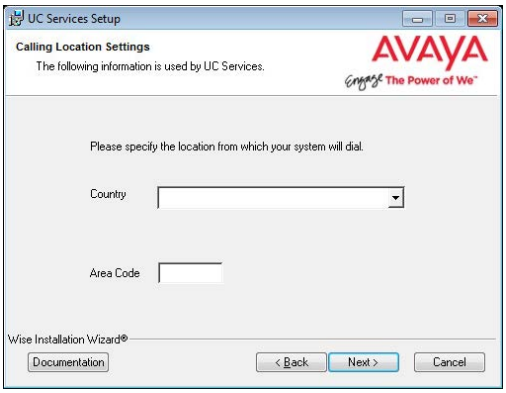
    When ready, click **Next**.



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.

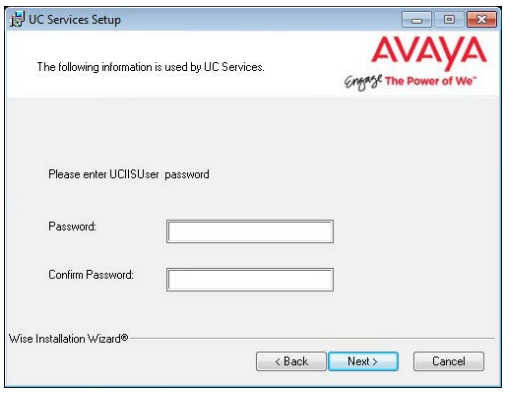
    Select the country from the dropdown menu, and enter the area code in the space provided.

    Click **Next** to continue.

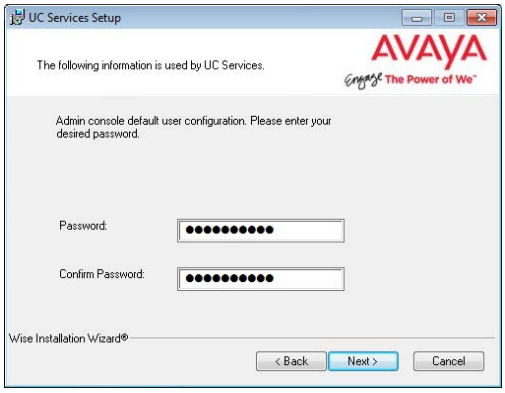


Note: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

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

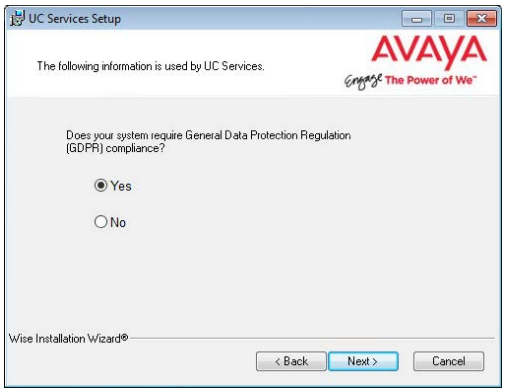


19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya IX Messaging.



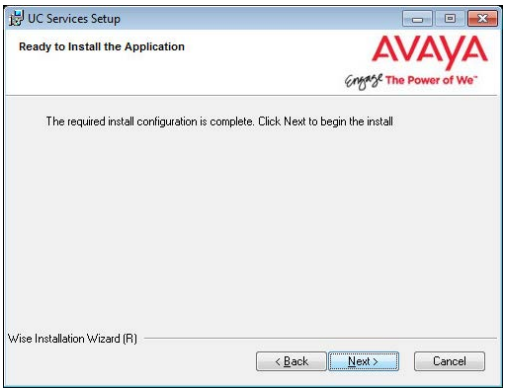
Hint: The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.

20. Choose either **Yes** or **No** to determine whether the system will apply General Data Protection Regulation (GDPR) compliance procedures to your data.
With this option enabled, users and callers are notified that personal information will be collected. This information can also be completely removed from the system upon request.

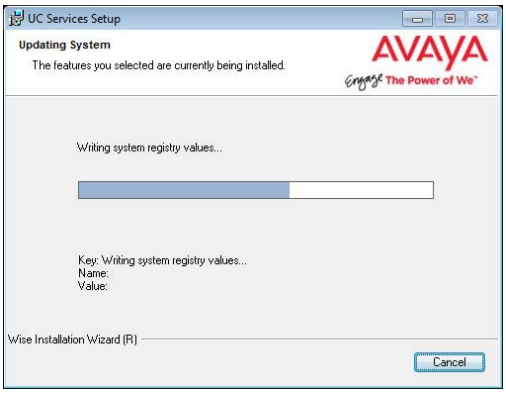


21. The preliminary information required for installation is now complete.

    Click **Next**.

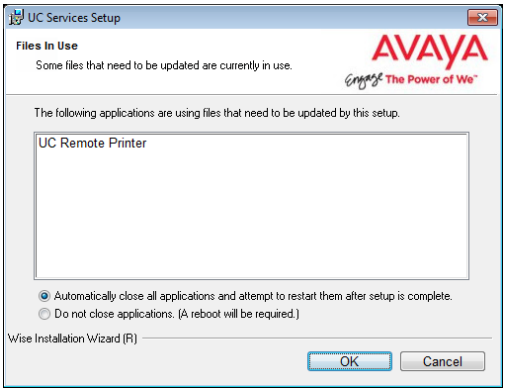


22. The selected components will now be installed. This process may take a while.



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

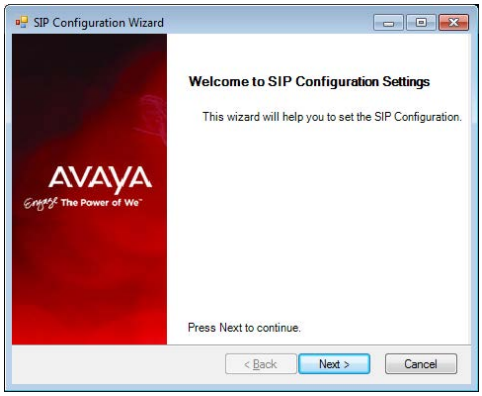
    Click **OK** when ready.



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

    Click **Next** to continue.

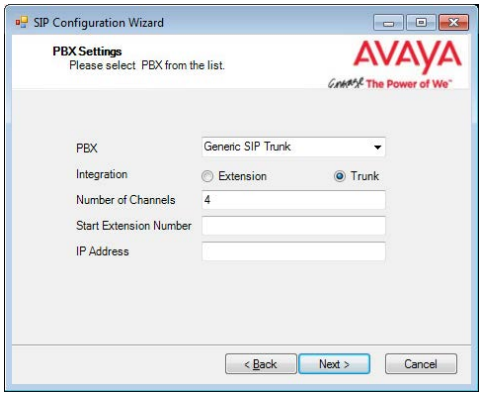


26. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.



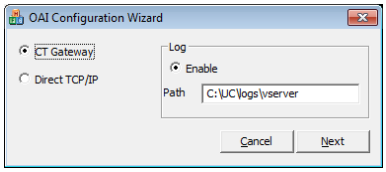
27. Confirm the information then click **Finish**.

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 Messaging programs folder after installation.

Note: This section is for installations where **Mitel 5000 (All)** was chosen at the PBX selection screen. Go directly to step 32 if this does not apply to your site.

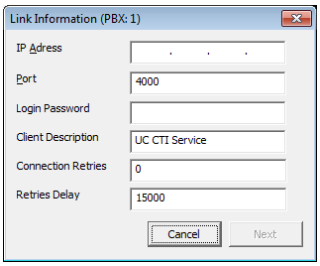
28. At the OAI Configuration Wizard screen:
    - Enable **Direct TCP/IP**.
    - **Set Number of Nodes = 1.**
    - **Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.**

    Click **Next**.



29. 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.

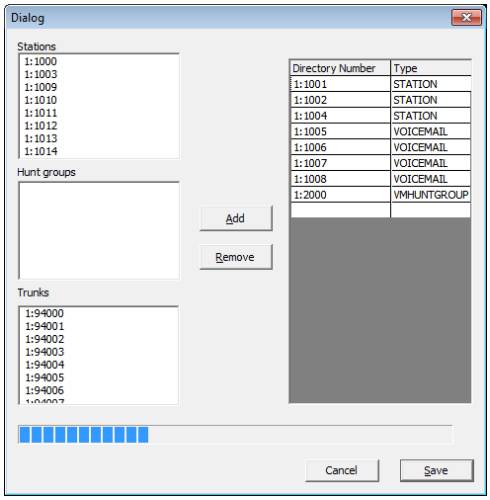
    Click **Next**.



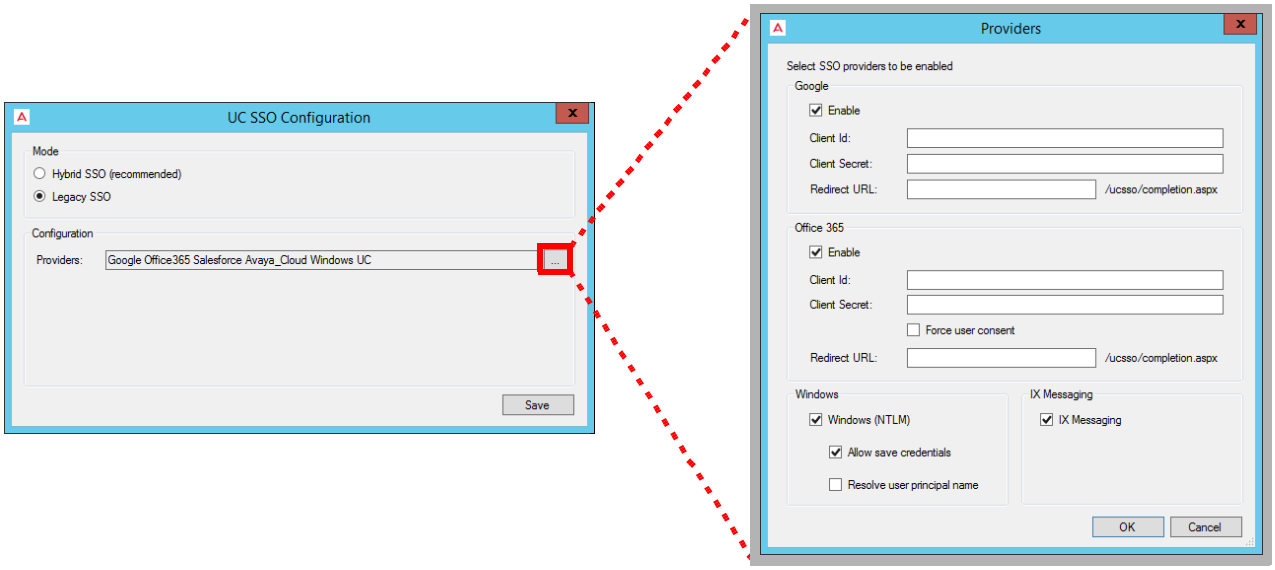
30. At the **Dialog** screen, from the lists on the left-hand side, choose the desired **Stations** (extensions and voicemail ports), **Hunt Groups** and **Trunks** to use with OAI.

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

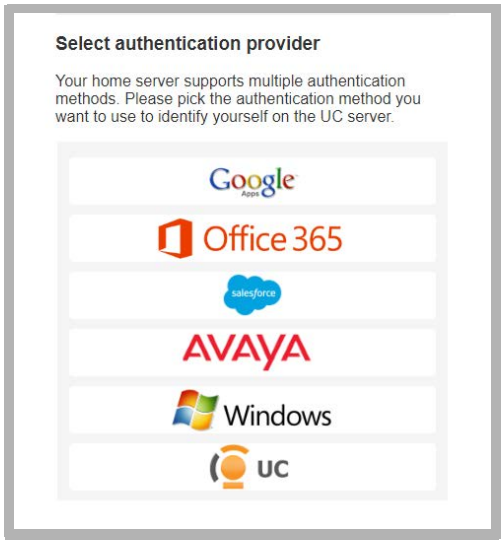
31. Click **Save** to finish the OAI setup and continue with the Messaging installation.

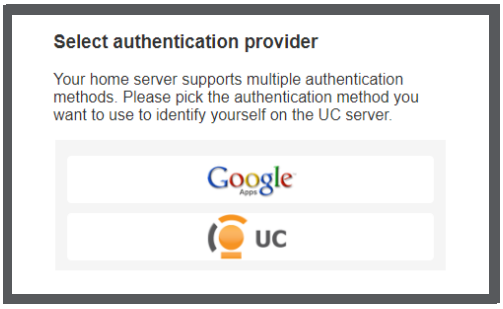


32. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



When clients / admins want access to these programs, they login using their credentials for one of the listed programs. They must have an account with that application before they can login.





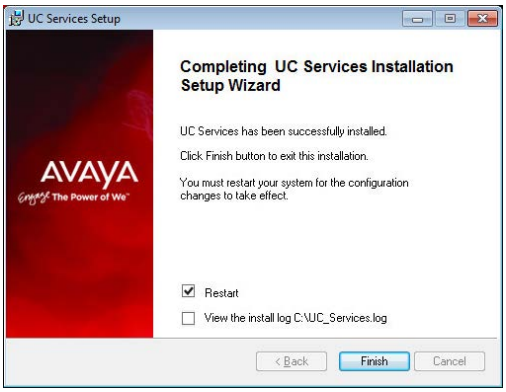
Enable all that apply, then click **OK**.

Click **Save** when finished.

Note: For complete details on using legacy and hybrid SSO, refer to chapter 25 of this document.

33. 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 Messaging installation is complete.

5 WINDOWS SERVER 2016/2019 INSTALLATION (SIP)

In This Chapter:

Introduction

When installing Avaya IX Messaging version 10.8, 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

Requirements	Details
License	A Full License for 10.8.
Software	For details on Messaging 10.8 Hardware and Software requirements please consult the Technical Operating Guidelines.

Important: Microsoft Windows is not provided with any version of IX Messaging. The customer must install and fully update a suitable, licensed version of Windows onto the hardware platform before proceeding with the Avaya IX Messaging software installation.

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

Note: Avaya IX Messaging should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Messaging 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 Messaging voice server installation.

Installation Preparation

Deployment Configuration Considerations

- An Avaya IX Messaging 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 Messaging 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 Messaging. 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 Messaging installation.

Digital Certificates

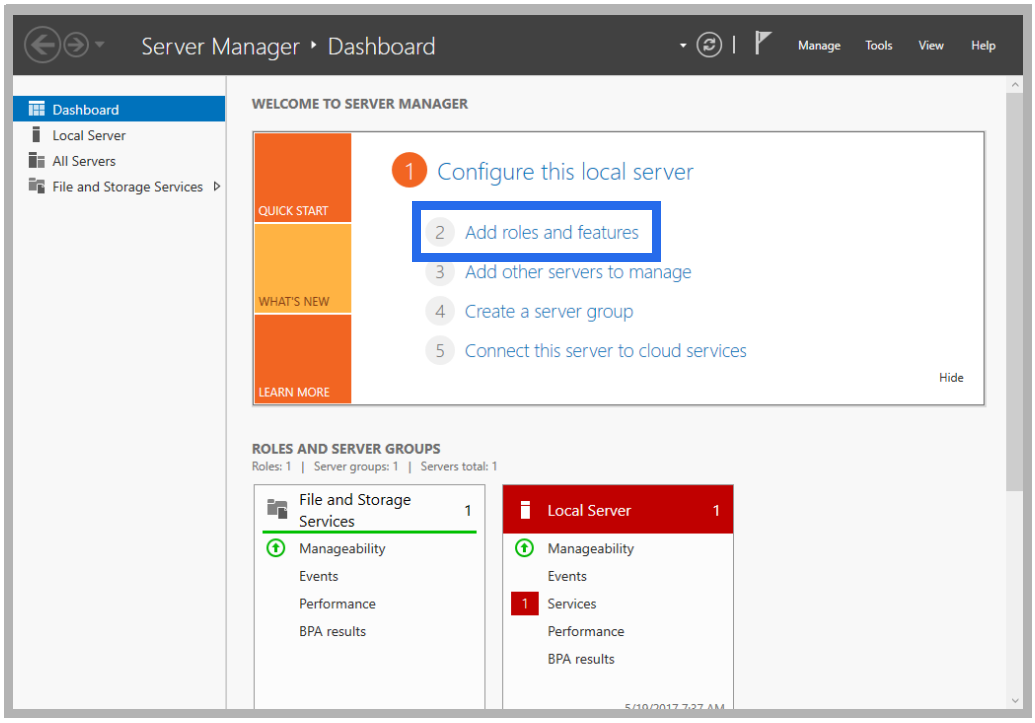
Avaya IX Messaging requires that signed digital certificates be installed on the voice server before attempting an installation.

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.

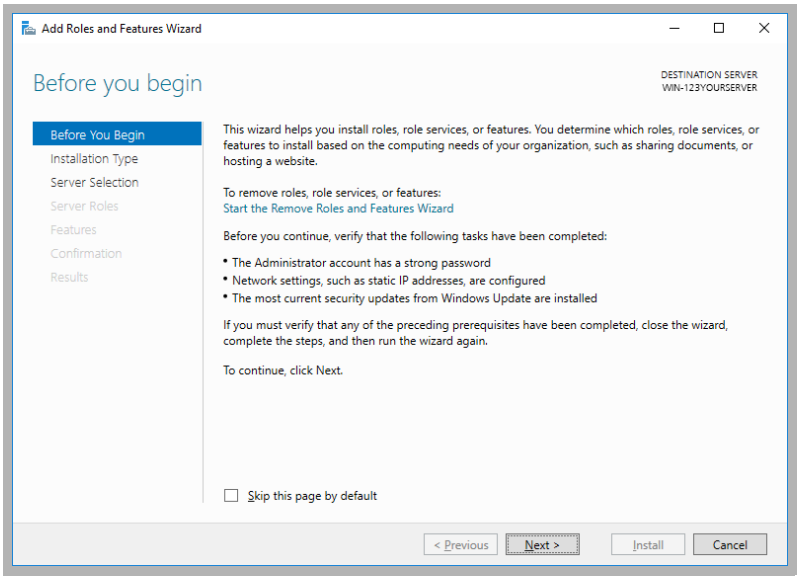
Server Roles and Features

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

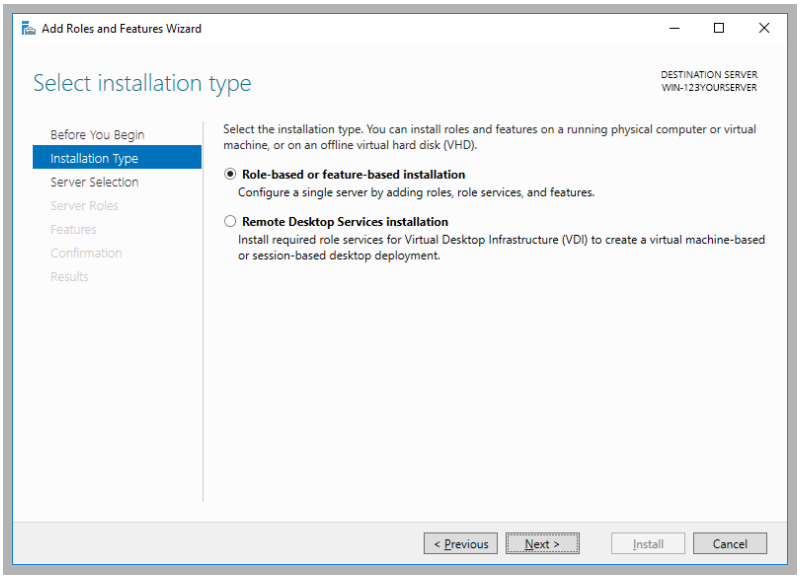


If this screen is hidden, go to **View** and select **Show Welcome Tile**.

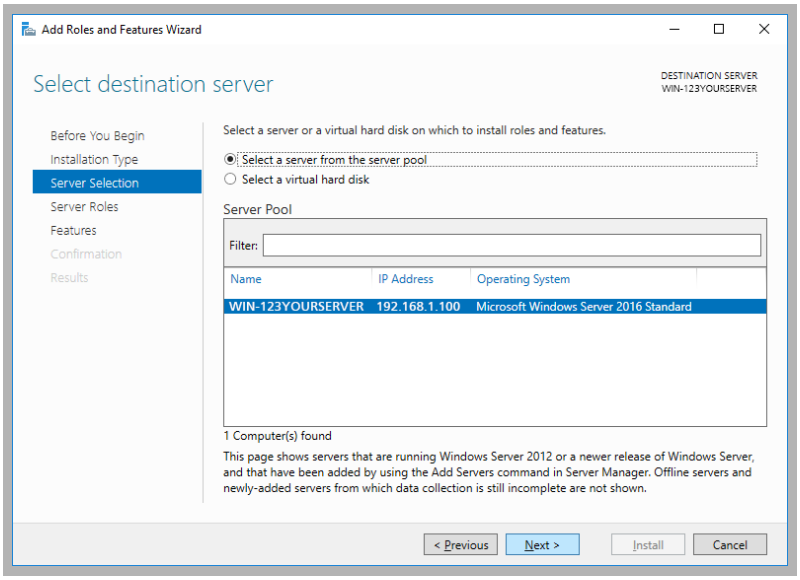
2. Click **Next**.



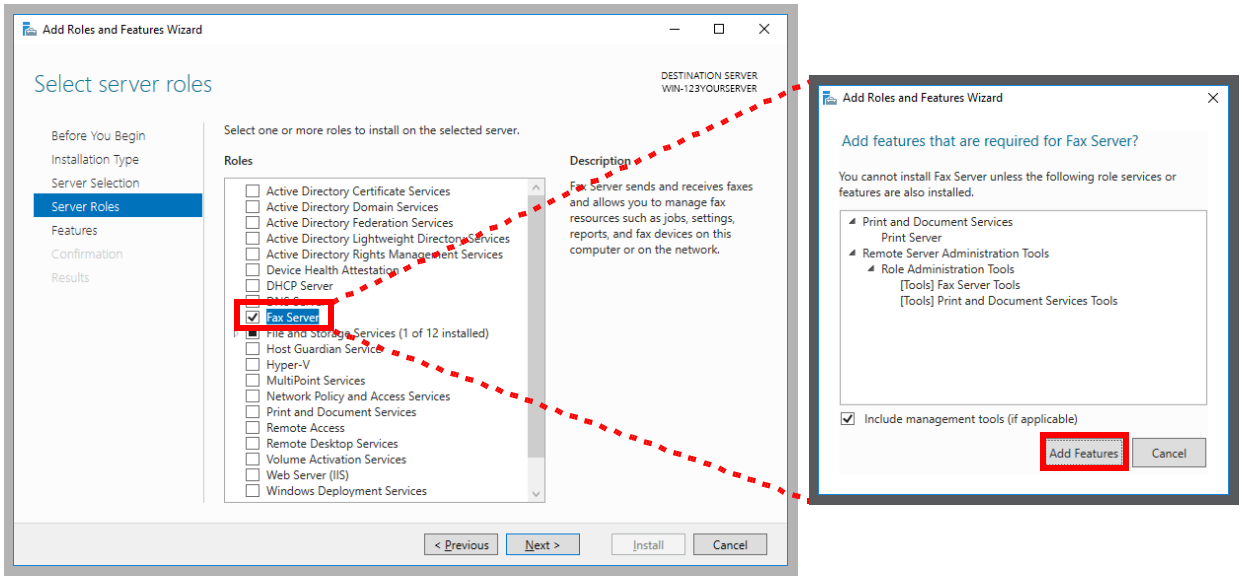
3. Leave the default settings as they are. Click **Next**.



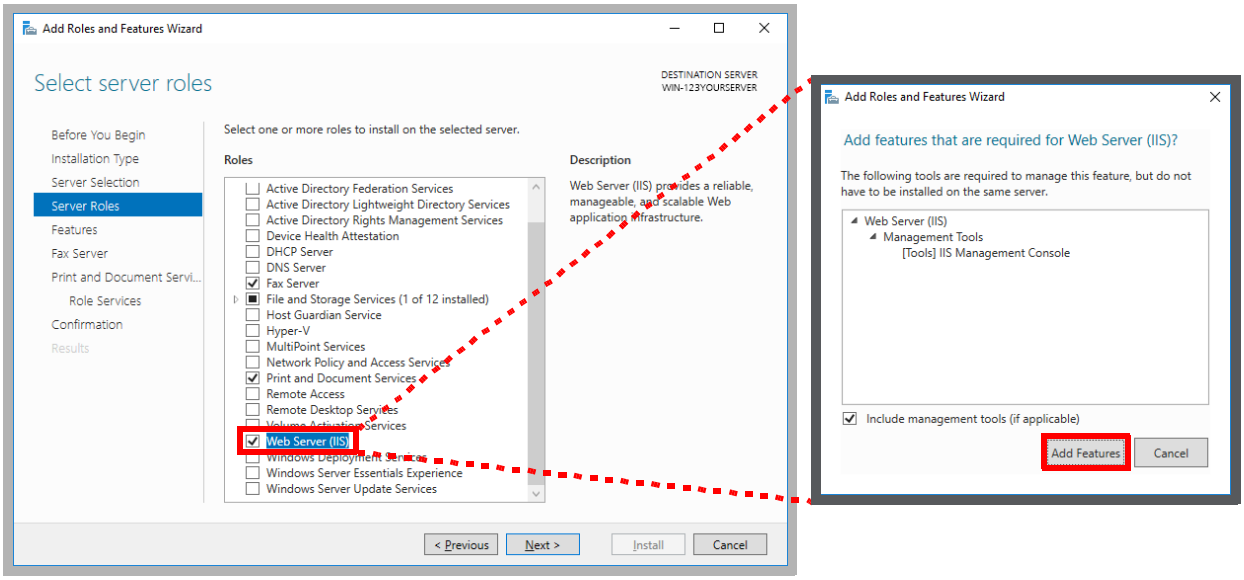
4. Leave the default settings as they are. Click **Next**.



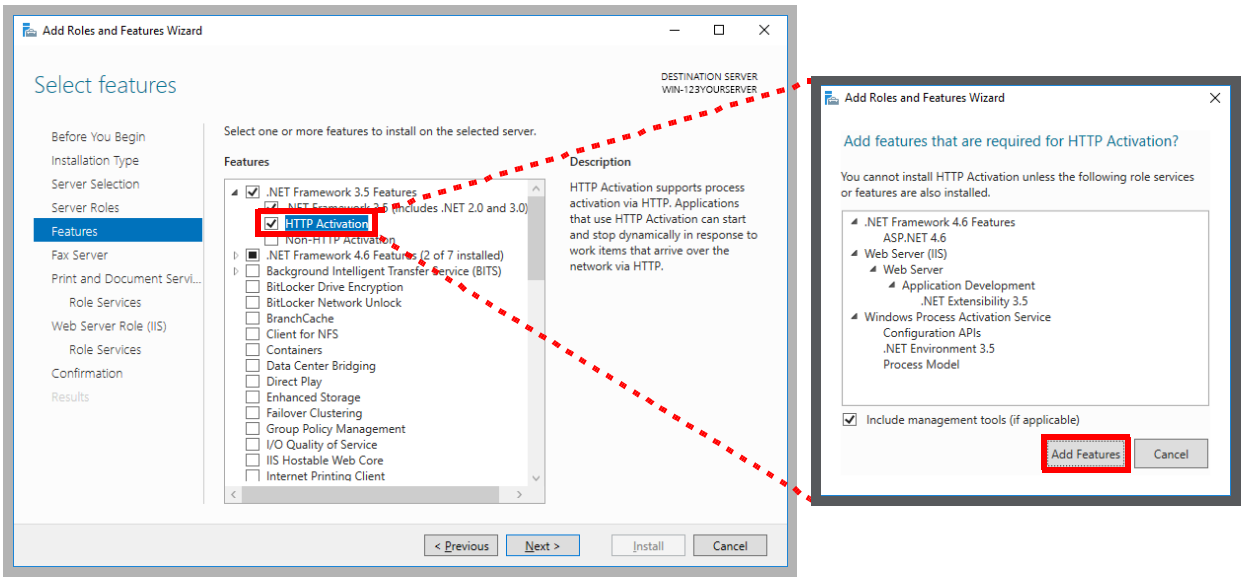
5. Enable **Fax Server**. When prompted, select **Add Features**.



6. Enable **Web Server (IIS)**. When prompted, select **Add Features.** Click **Next**.



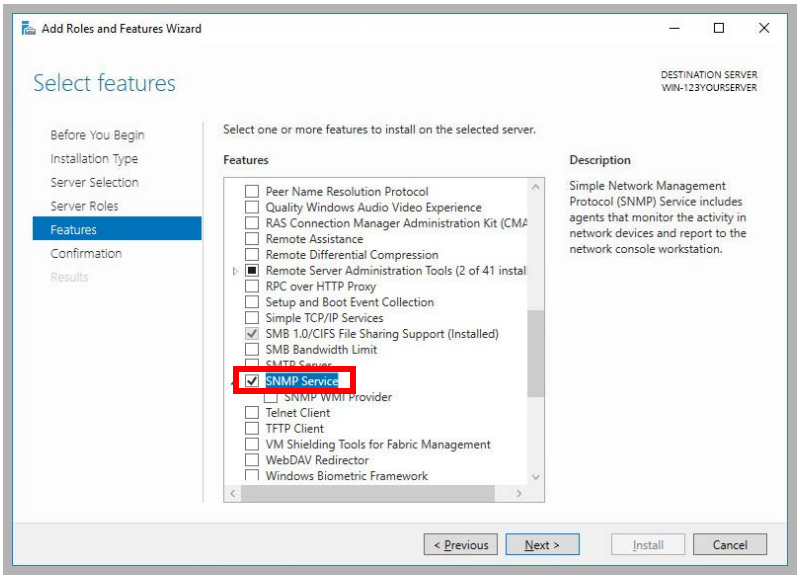
7. On the **Features** panel, open **.NET Framework 3.5 Features** and enable **HTTP Activation**. When prompted, select **Add Features**. Click **Next**.



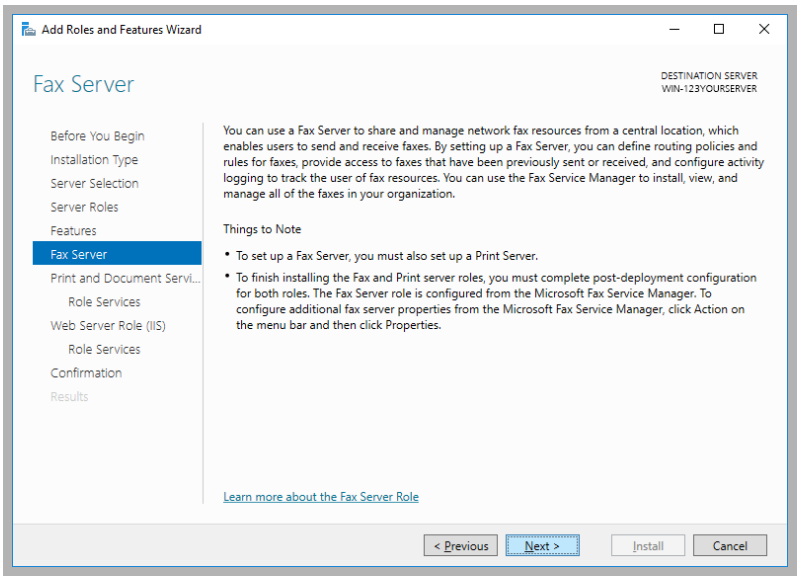
8. **Optional**: If you plan to use **SNMP Alarms** with Messaging, the **SNMP Service** must be added to Windows before the program can be installed.

   If SNMP Alarms are required, scroll down and enable SNMP Service.

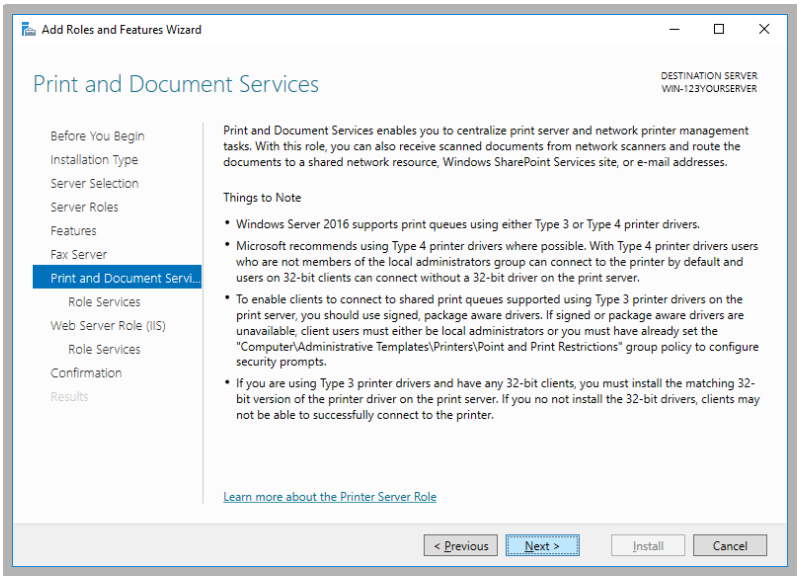
   If SNMP Alarms are not required, skip this step.



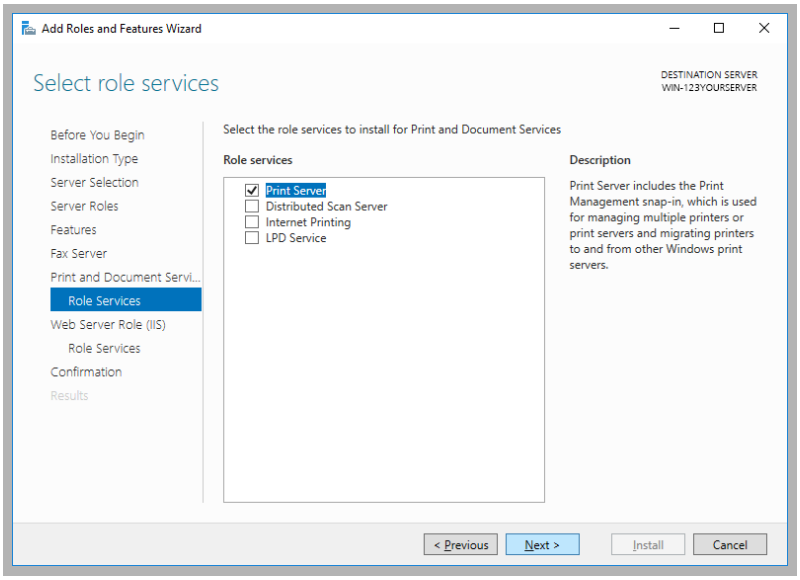
9. On the **Fax Server** screen, click **Next**.



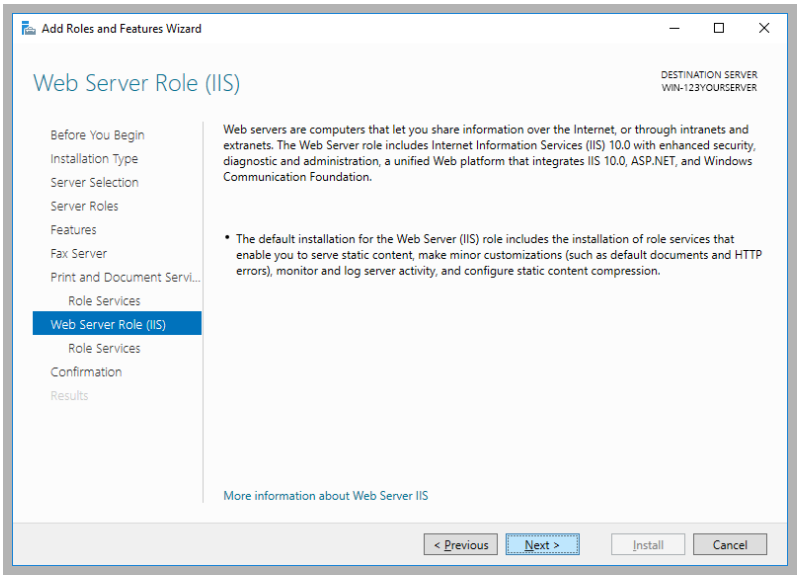
10. On the **Print and Document Services** screen, click **Next**.



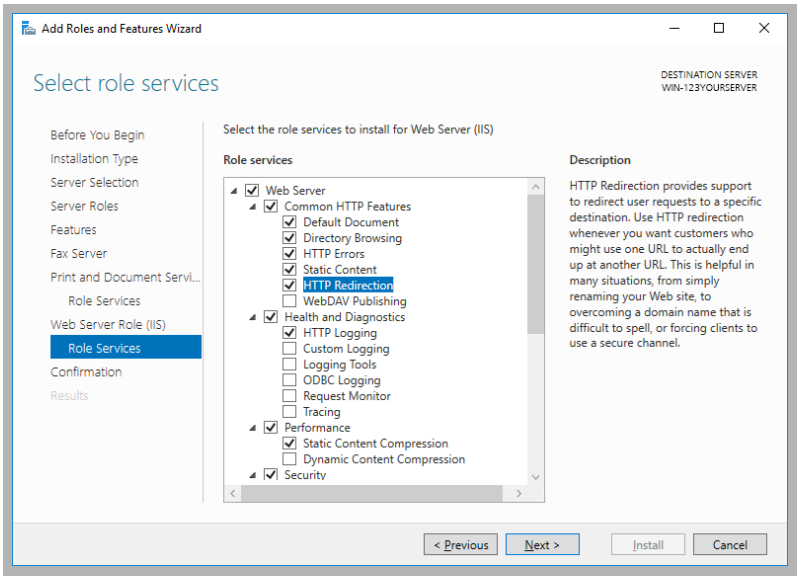
11. No changes are required here. Click **Next**.



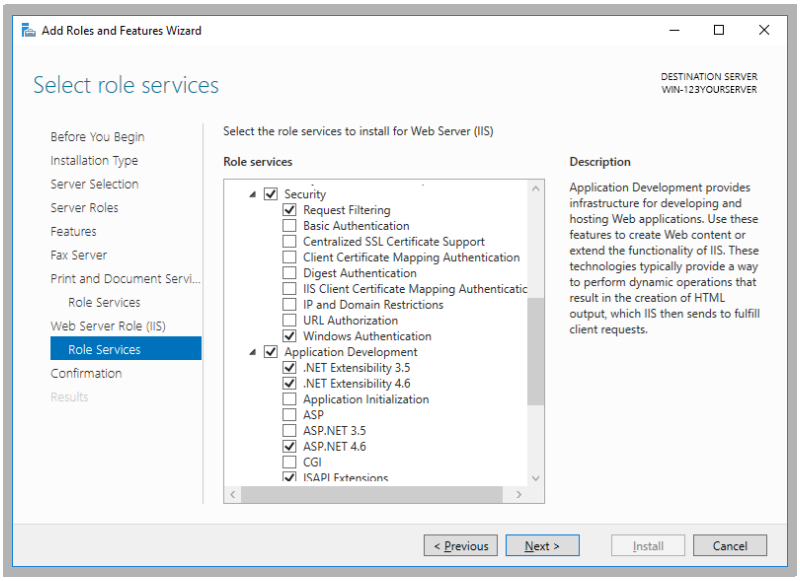
12. On the **Web Server Role (IIS)** screen, click **Next**.



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

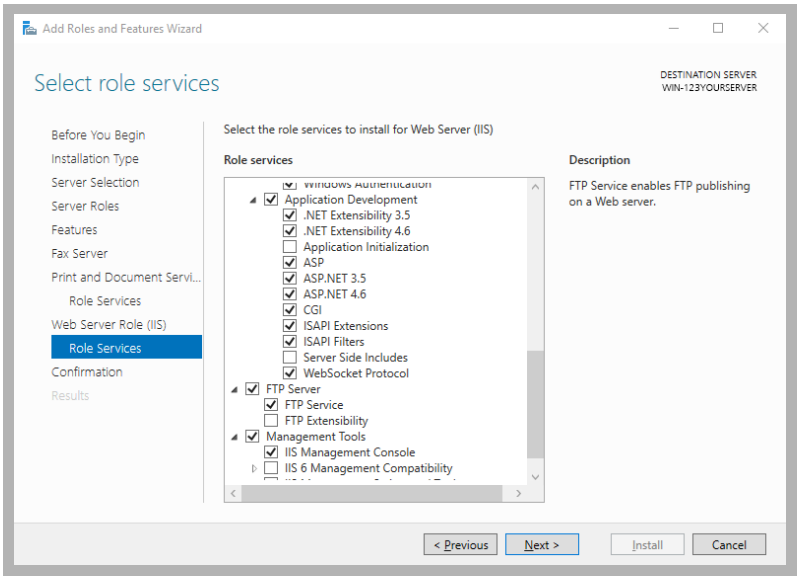


14. Under **Web Server > Security**, enable **Windows Authentication**.



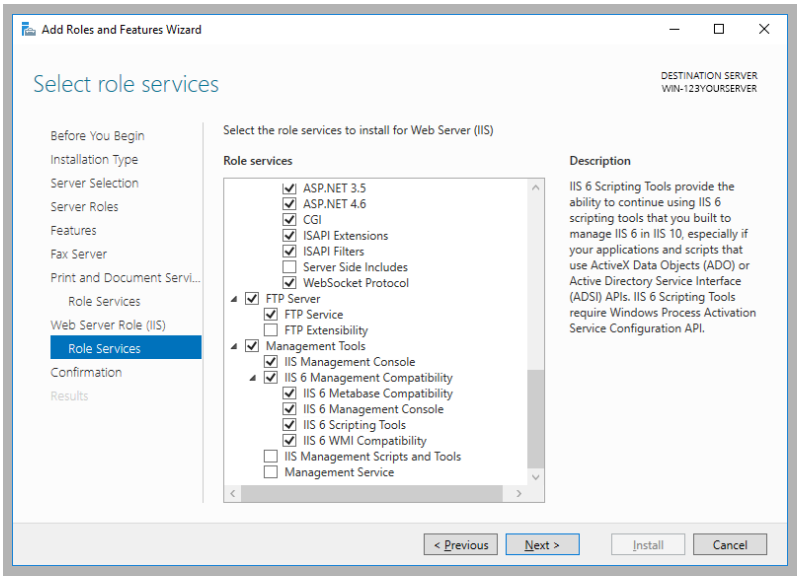
15. Under **Web Server > Application Development**, enable **.NET Extensibility 3.5**, **.NET Extensibility 4.6**, **ASP**, **ASP .NET 3.5**, **ASP .NET 4.6**, **CGI**, **ISAPI Extensions**, **ISAPI Filters** and **WebSocket Protocol**.

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

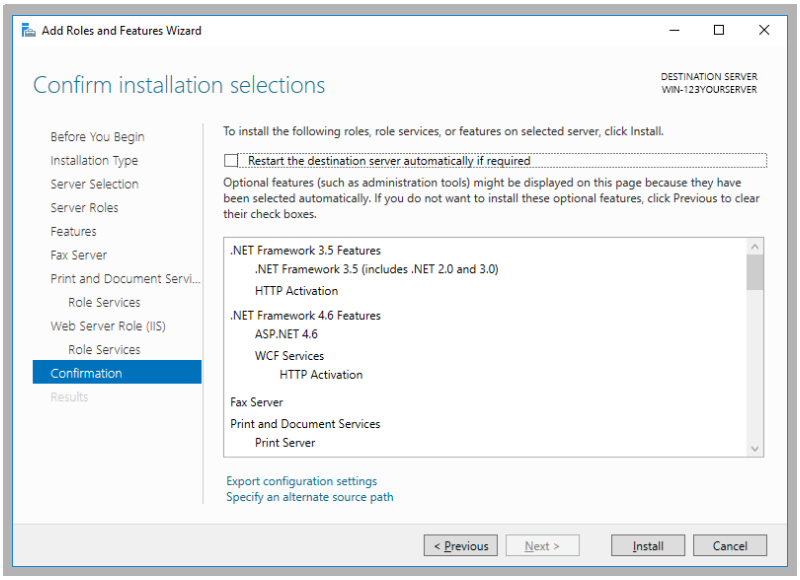


16. Under **Management Tools > IIS 6 Management Compatibility**, enable all items.

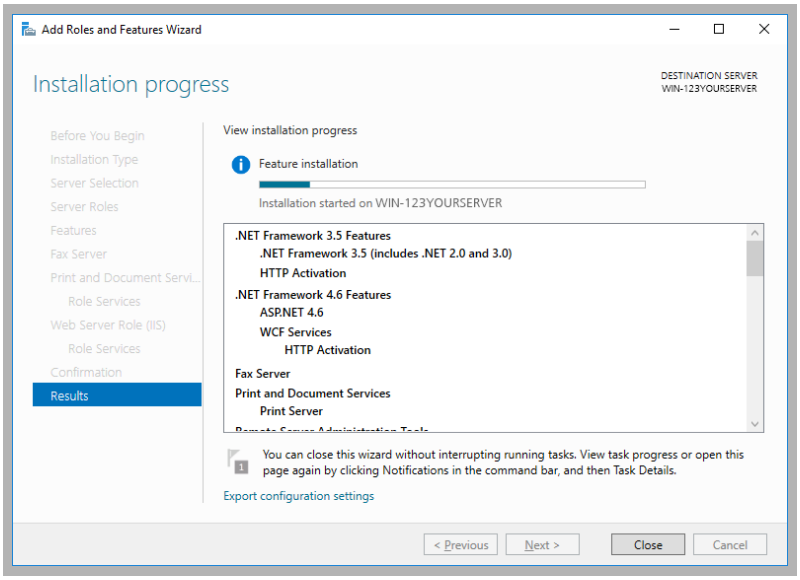
    Click **Next** when ready.



17. Review the selections here. When ready to proceed, click **Install**.



18. Windows will now start the installation process for the chosen items. This process may take a while.



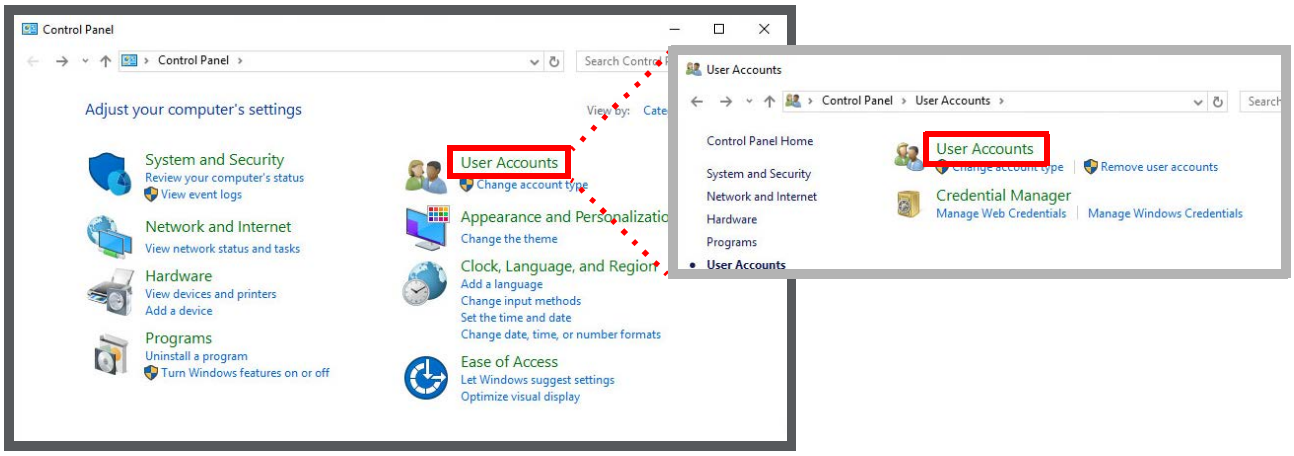
Note: This window can be closed without interrupting the installation procedure

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

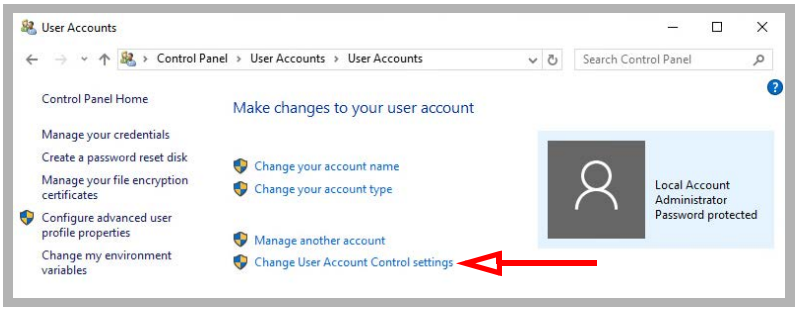
Disabling User Account Control Notification

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

   Again, click **User Accounts**.

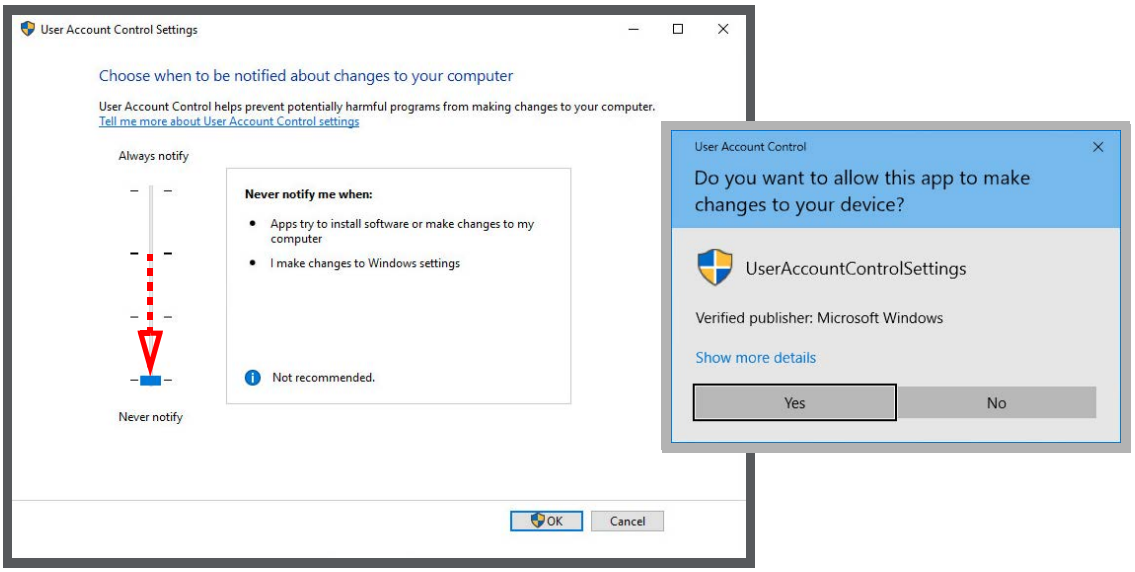


2. Select **Change User Account Control settings**.

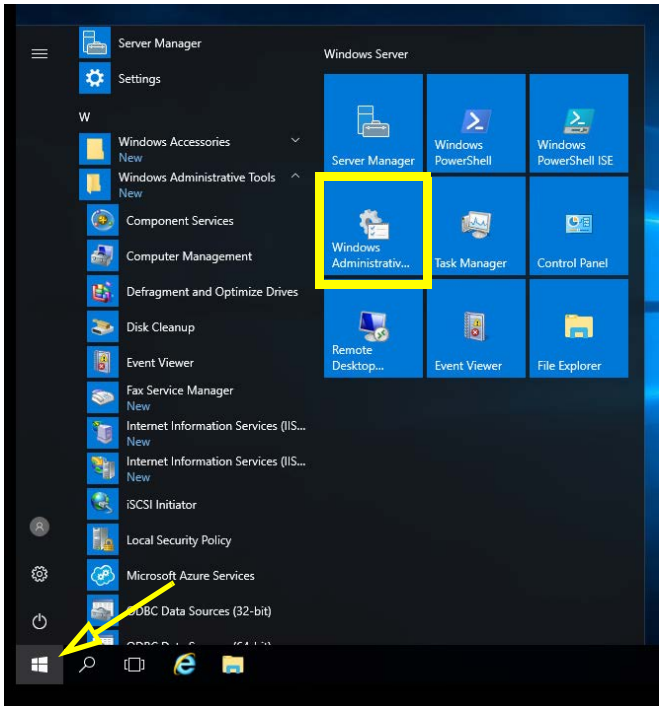


3. Click and drag the slider down to **Never Notify**.

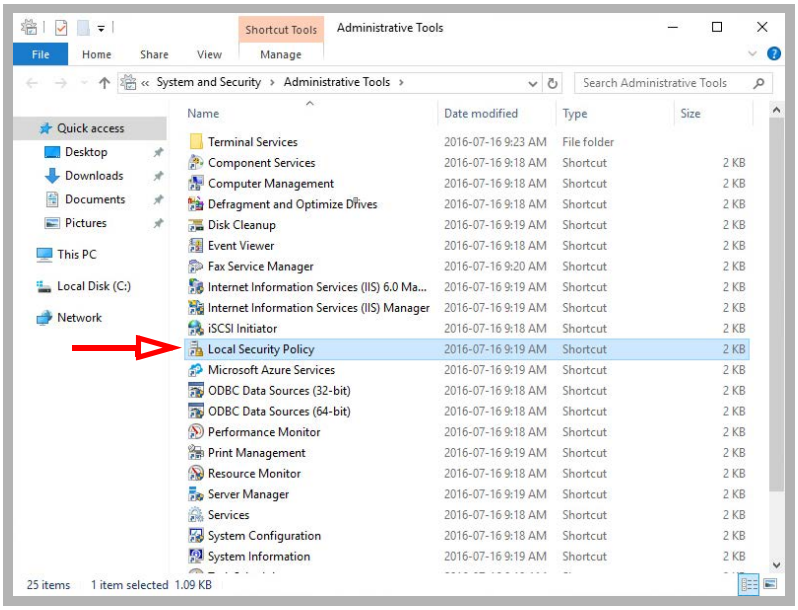
   Click **OK** and **Close**.



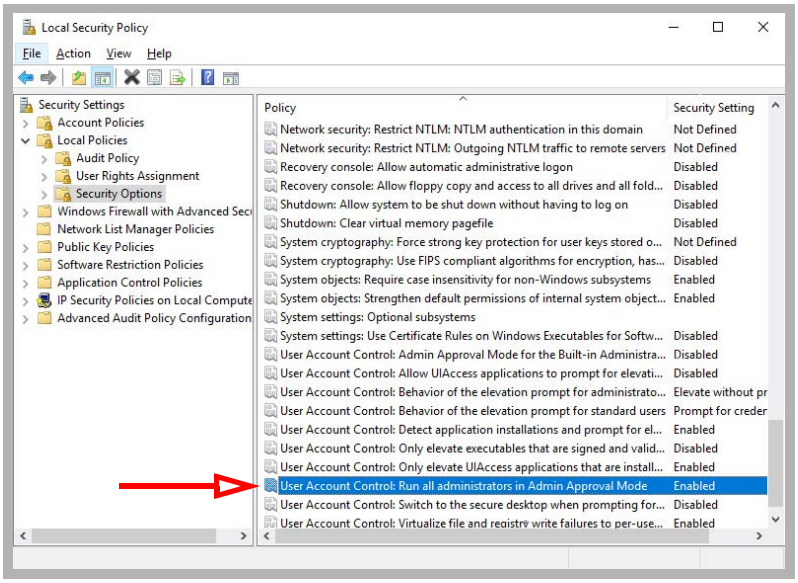
4. Open the **Start** menu and select **Windows Administrative Tools**.



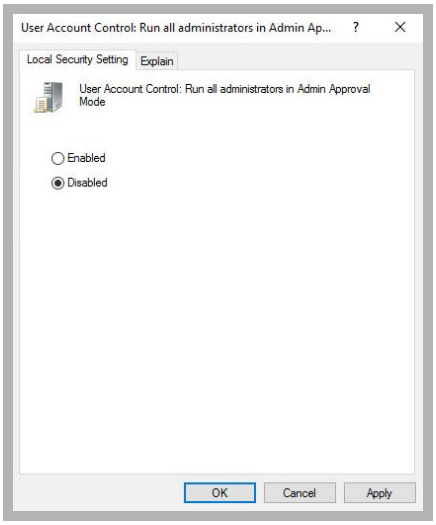
5. Double-click **Local Security Policy**.



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



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



8. Restart the computer to make the changes active.

Note: UAC Notifications can be restored after Messaging 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:

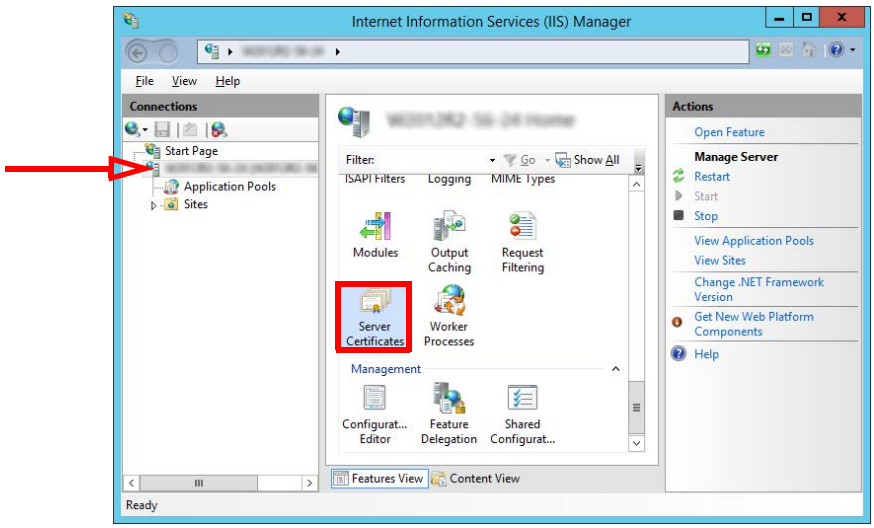
https://technet.microsoft.com/en-ca/library/cc753127(v=ws.10).aspx

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

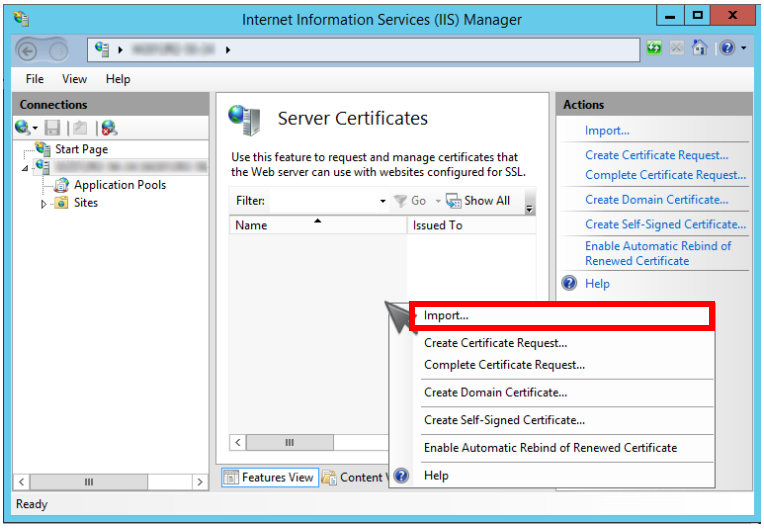
IIS Certificate Bindings

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

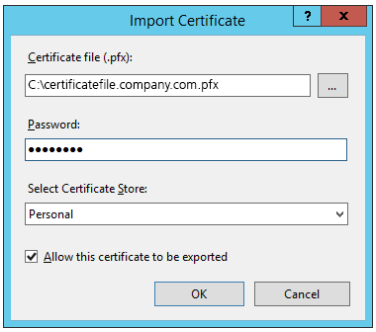
1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.



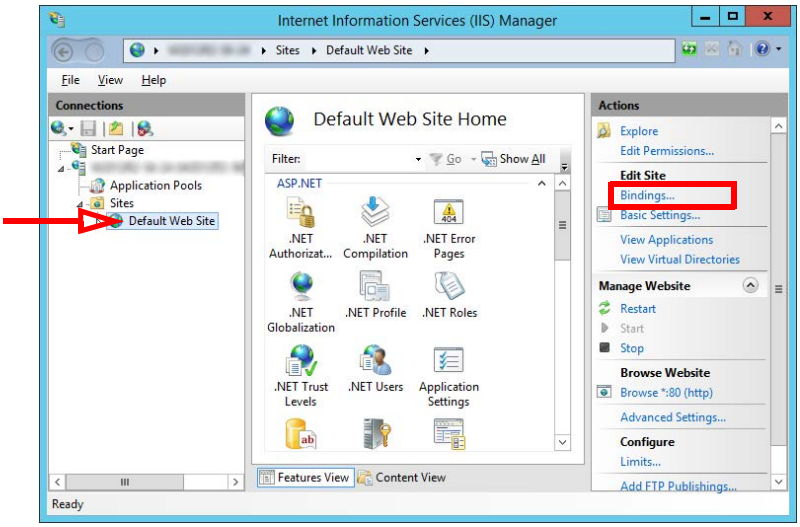
2. Right-click in the right-hand pane and choose Import from the pop-up menu.



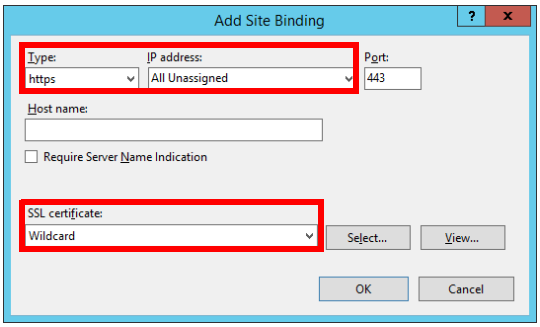
3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.



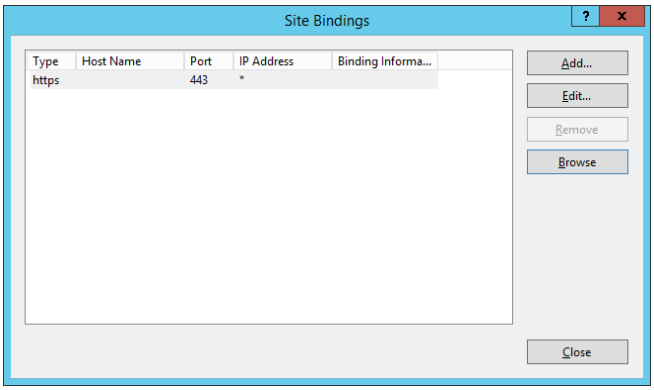
4. Go to **Sites > Default Web Site**.
Click **Bindings...**.



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**.



Install Microsoft .Net Framework 4.7.2

Avaya IX Messaging requires Microsoft .Net Framework version 4.7.2 to be installed to support various features within the program. If it has not already been installed, the administrator must download it and install it manually.

Note: .Net Framework 4.7.2 is not installed by default. It may be part of Windows updates, optional updates, or not provided at all. Follow these instruction is it is not installed on your system, or if you do not know if it has been installed.

1. Open a web browser and go to the Microsoft web site. Search for .Net Framework 4.7.2 and install the application on the server. For example:
   https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows .
2. Download the file to your server drive. When ready, run the program to install this feature.
3. When finished, restart the server.

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 IX Messaging has not logged in as the system administrator, that user must be given full rights to the root of the C drive.

About Passwords

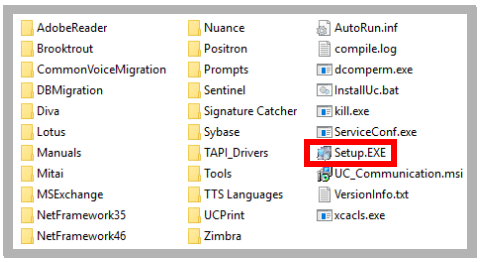
These rules are applied to all passwords created or used with Avaya Messaging, including those created during installation (Note: JITC installations have more stringent requirements). These include:

- **Length**: Passwords must be at least **14** characters long.
- **Class**: A password can contain upper and lower case characters, numbers and special characters. No minimum requirements for each character class are set by default, but this can be changed by the administrator.
- **Repeating Characters**: No character can be repeated more than 2 times consecutively (he**ll**o, world**!!**). This value can be modified by the administrator.
- **Repeating a Character Class**: No class of character can be repeated more than 4 times consecutively (ABCD, !@#$). This value can be modified by the administrator.
- **Reusing Passwords**: No new password can be the same as a previous password extending back 10 iterations. This value can be modified by the administrator.
- **Sharing Passwords**: Passwords must not be shared between users. Only one login per account is allowed at one time. Other users must login using different credentials.

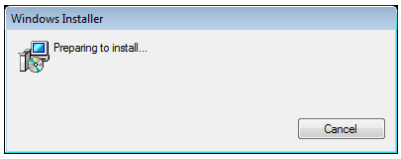
Note: Using an administrator account to perform routine functions leaves the servers open to malicious software attacks. Therefore, it is **strongly recommended** that each user with administrative privileges is also assigned a standard user account. To maintain security integrity, the administrator account should only be used when necessary, and should be immediately logged out afterwards.

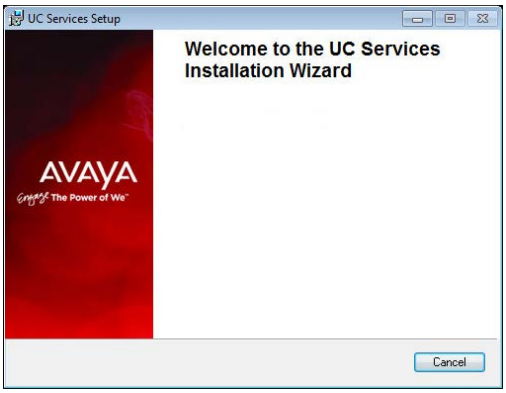
Procedure

1. Download the installation file (see chapter 4). 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 IX Messaging onto your voice server.





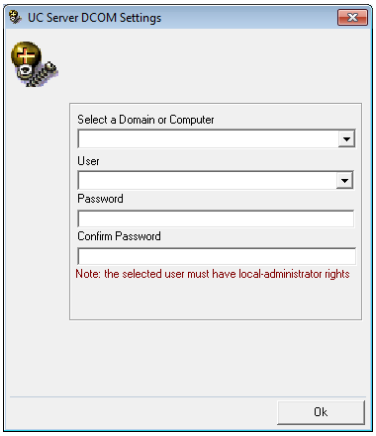
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging. They can also be downloaded from resources.zag.io in both PDF and HTML format.

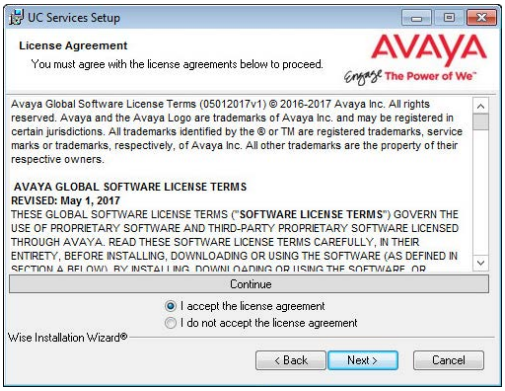
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.



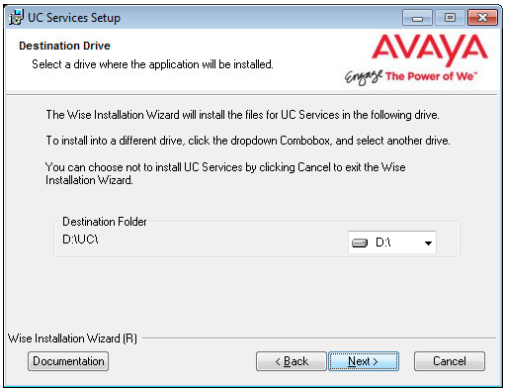
5. Review the license agreements and enable **I accept the license agreement**.

   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.

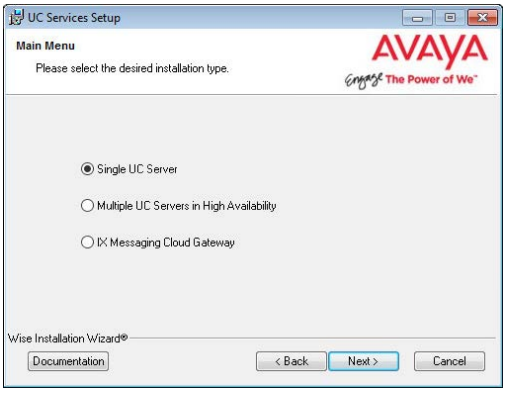
   Click **Next** to continue.



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**.

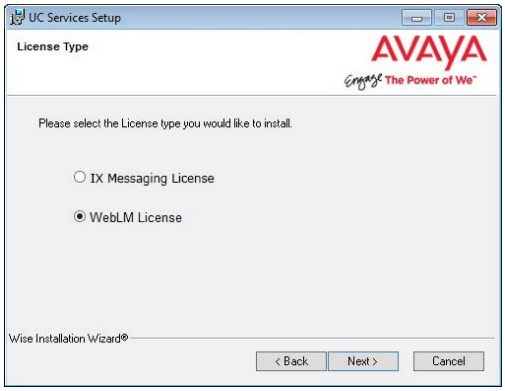


   Single UC Server: When operating Messaging on a single voice server computer.

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

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, 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.

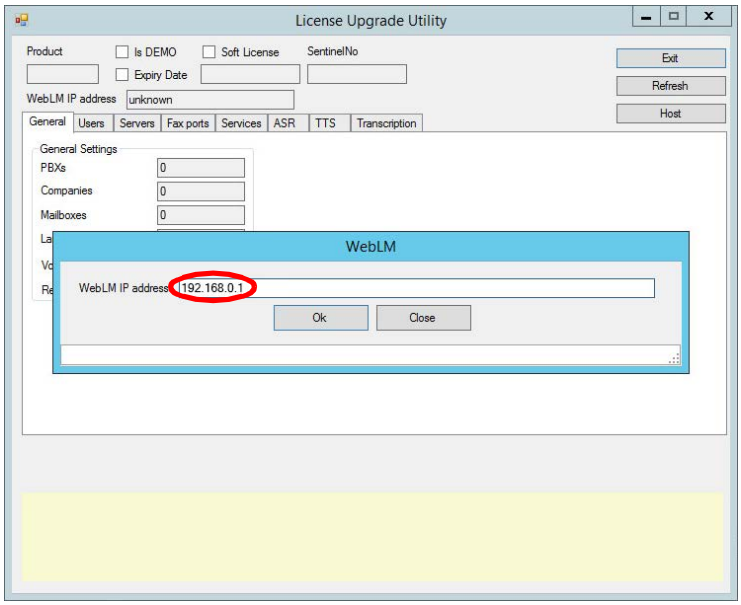


Note: If you select Messaging, go to **chapter 13, Installing the Messaging License**. When finished, return here and continue the installation from **step 11**. Skip step 9 through 10.

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.

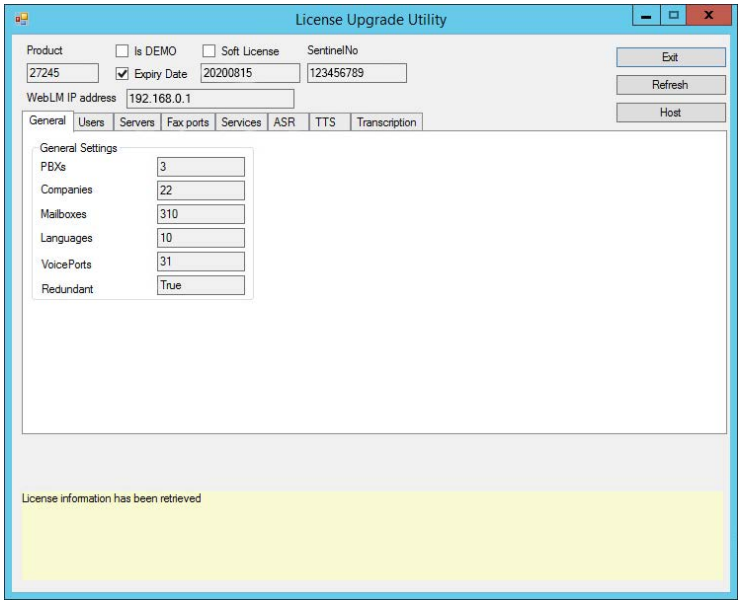
9. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   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 437.

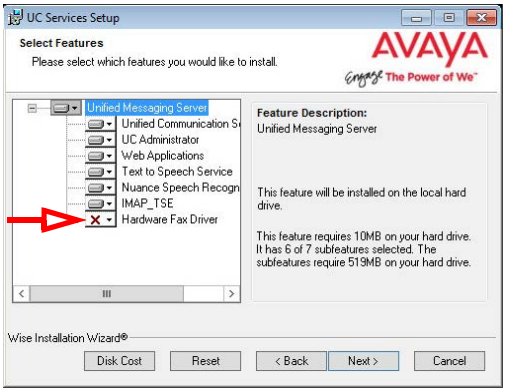
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.



Note: The number of voice ports is calculated based upon your license.
[(# Basic users + # Mainstream users) / 40] + Number of voice ports in license

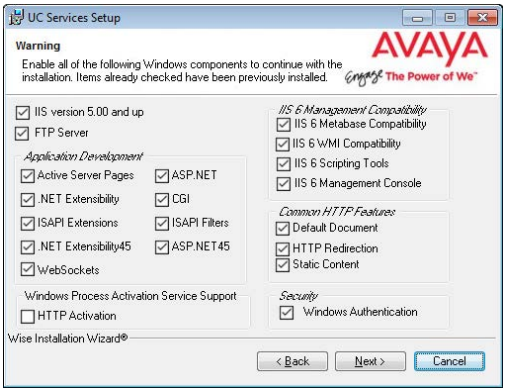
11. Select the **Components** required at your site. Disable any components that are not needed.

    Click **Next**.



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 Messaging requires to operate properly.



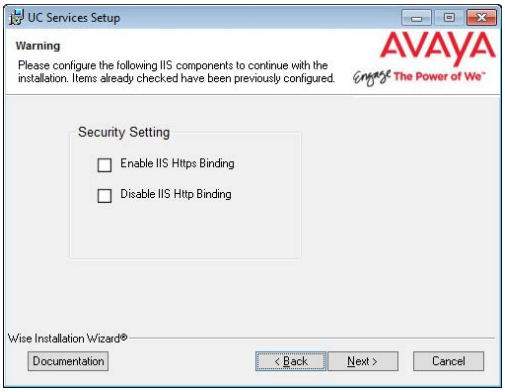
Note: This screen will only appear if one or more required components are **not** installed on the computer.

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 Messaging requires to operate.



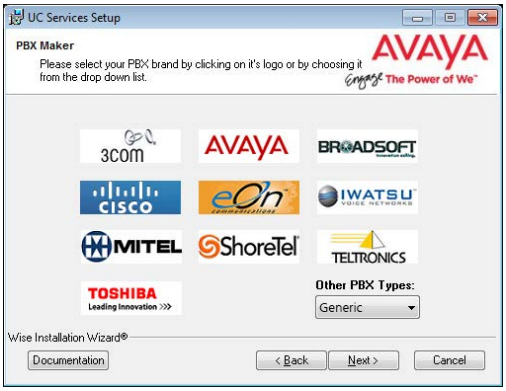
Note: This screen will only appear if one or more of the required settings has not been made on the computer.

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.

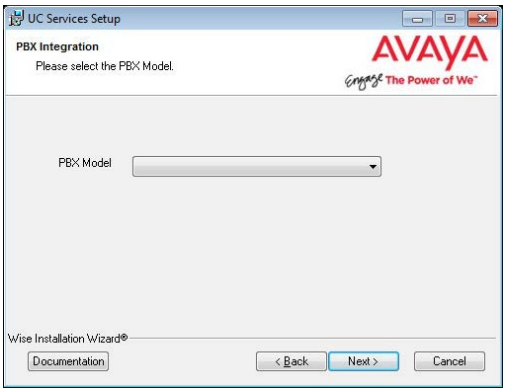
Note: The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

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



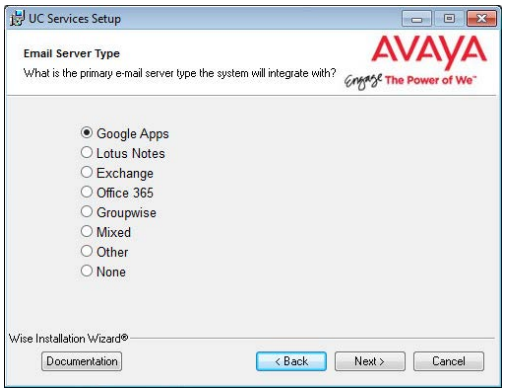
15. Select your PBX model from the dropdown menu.

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.

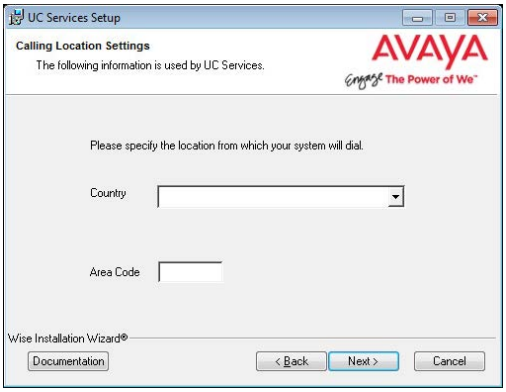
When ready, click **Next**.



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.

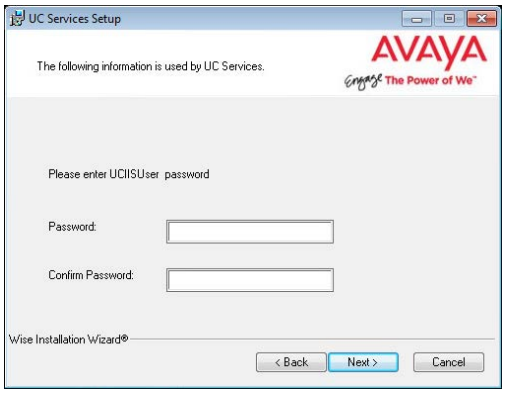
    Select the country from the dropdown menu, and enter the area code in the space provided.

    Click **Next** to continue.



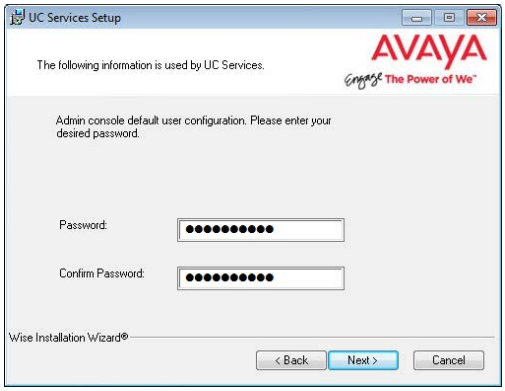
Note: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

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

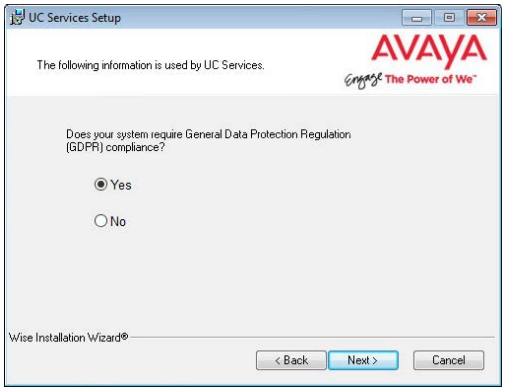


19. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of Avaya IX Messaging.

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.

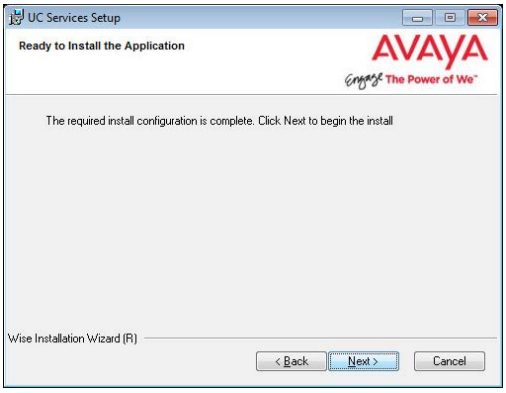


20. Choose either **Yes** or **No** to determine whether the system will apply General Data Protection Regulation (GDPR) compliance procedures to your data.
    With this option enabled, users and callers are notified that personal information will be collected. This information can also be completely removed from the system upon request.

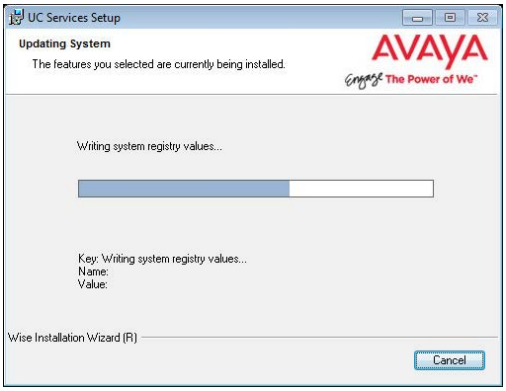


21. The preliminary information required for installation is now complete.

    Click **Next**.

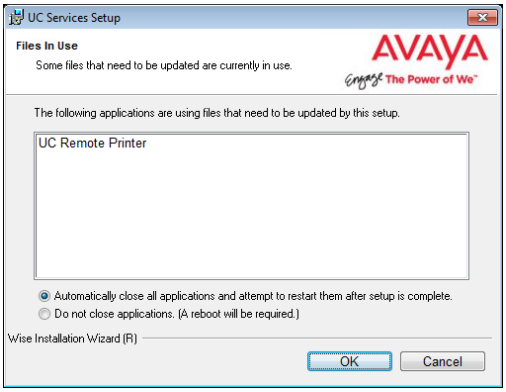


22. The selected components will now be installed. This process may take a while.



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

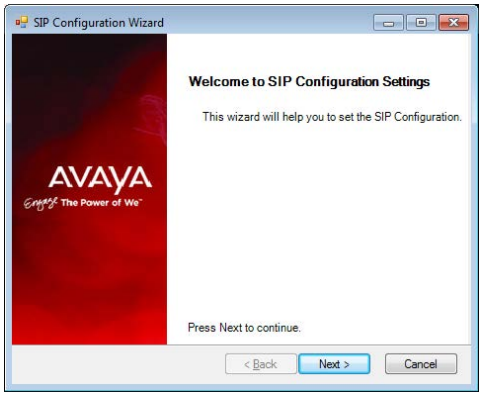
    Click **OK** when ready.



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

    Click **Next** to continue.

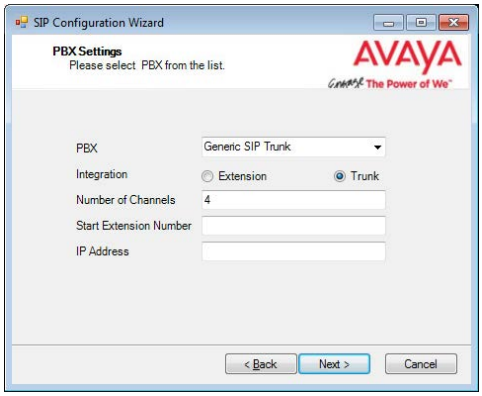


26. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.



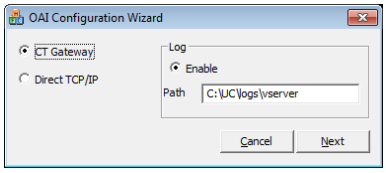
27. Confirm the information then click **Finish**.

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 Messaging programs folder after installation.

Note: This section is for installations where **Mitel 5000 (All)** was chosen at the PBX selection screen. Go directly to step 32 if this does not apply to your site.

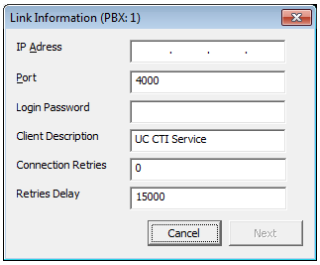
28. At the OAI Configuration Wizard screen:
    - Enable **Direct TCP/IP**.
    - **Set Number of Nodes = 1.**
    - **Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.**

    Click **Next**.



29. 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.

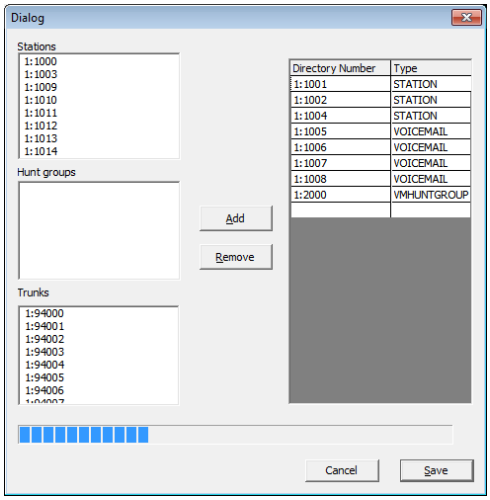
    Click **Next**.



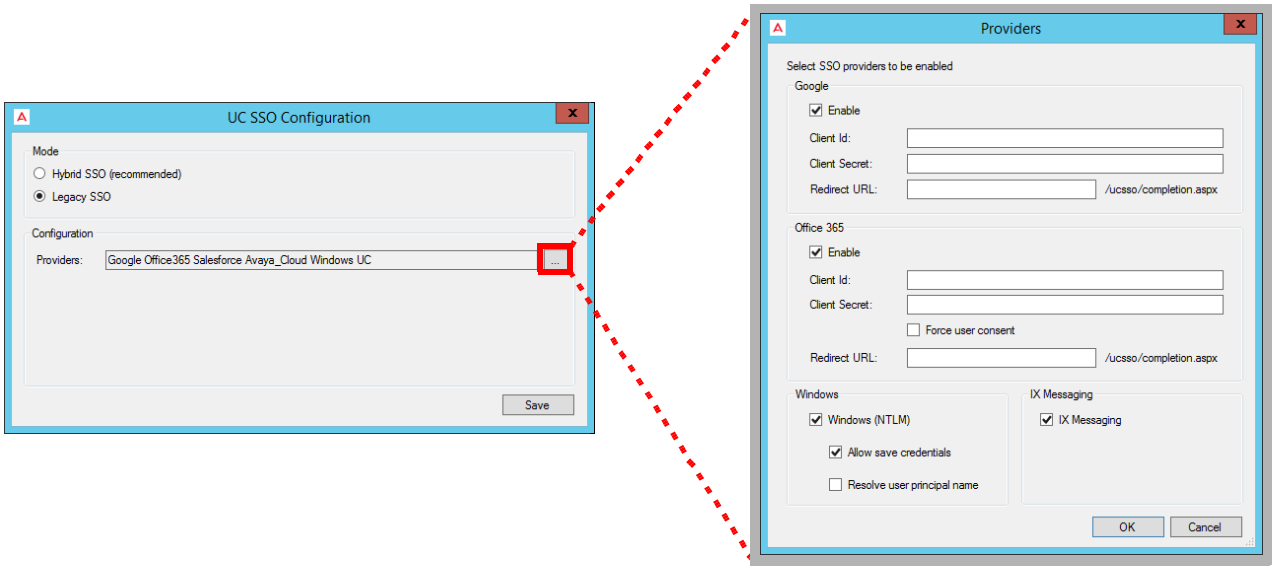
30. At the **Dialog** screen, from the lists on the left-hand side, choose the desired **Stations** (extensions and voicemail ports), **Hunt Groups** and **Trunks** to use with OAI.

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

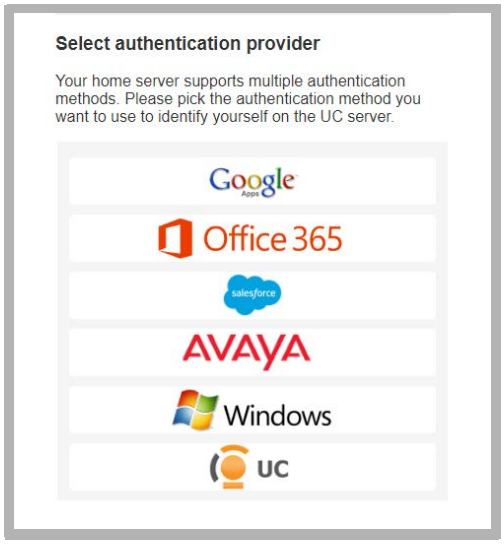
31. Click **Save** to finish the OAI setup and continue with the Messaging installation.

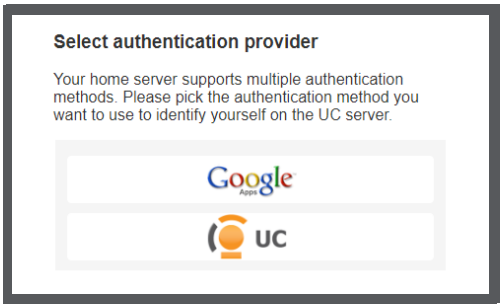


32. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



When clients / admins want access to these programs, they login using their credentials for one of the listed programs. They must have an account with that application before they can login.





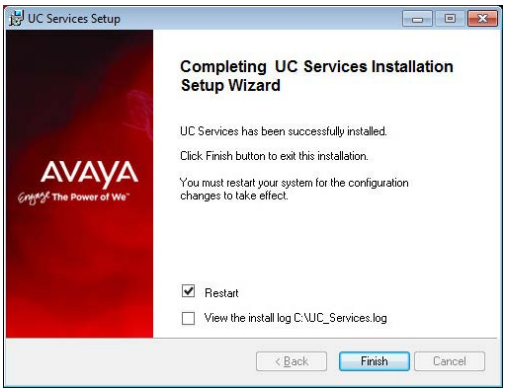
Enable all that apply, then click **OK**.

Click **Save** when finished.

Note: For complete details on using legacy and hybrid SSO, refer to chapter 25 of this document.

33. 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 Messaging installation is complete.

6 WINDOWS SERVER 2012 INSTALLATION (SIP)

In This Chapter:

Introduction

When installing Avaya IX Messaging version 10.8, 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

Requirements	Details
License	A Full License for 10.8.
Software	For details on Messaging 10.8 Hardware and Software requirements please consult the Technical Operating Guidelines.

Important: Microsoft Windows is not provided with any version of IX Messaging. The customer must install and fully update a suitable, licensed version of Windows onto the hardware platform before proceeding with the Avaya IX Messaging software installation.

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

Note: Avaya IX Messaging should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Messaging 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 Messaging voice server installation.

Installation Preparation

Deployment Configuration Considerations

- An Avaya IX Messaging 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 Messaging 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 Messaging. 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 Messaging installation.

Digital Certificates

Avaya IX Messaging 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.

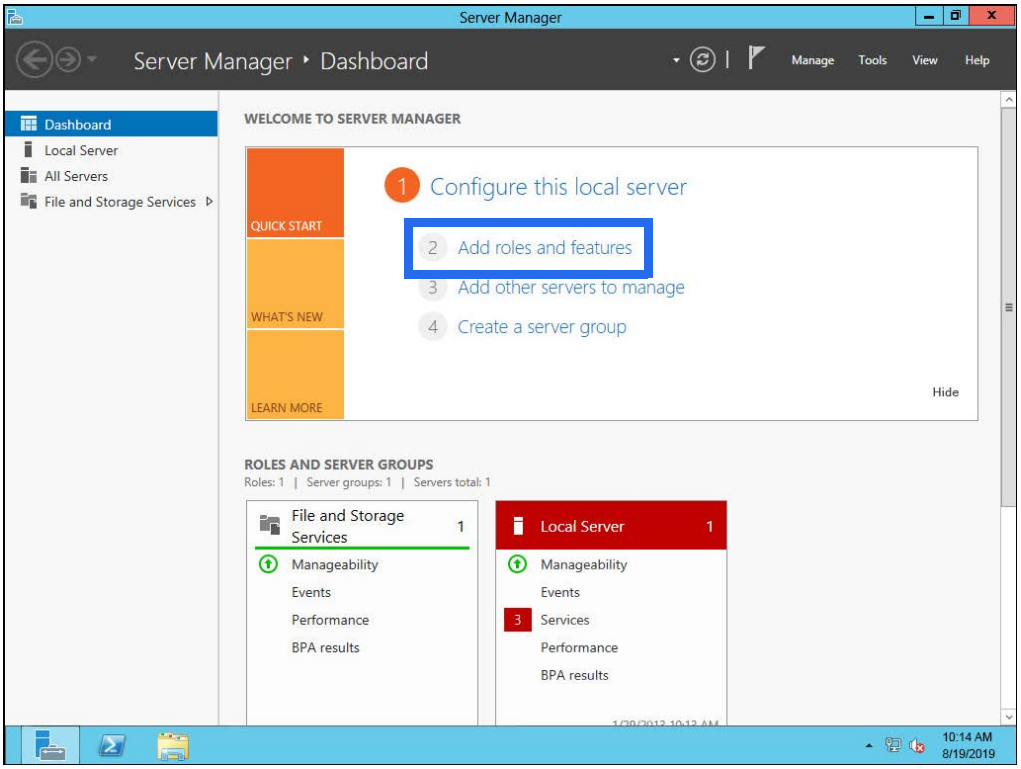
For High Availability installations, the certificates must be installed on the Consolidated server.

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.

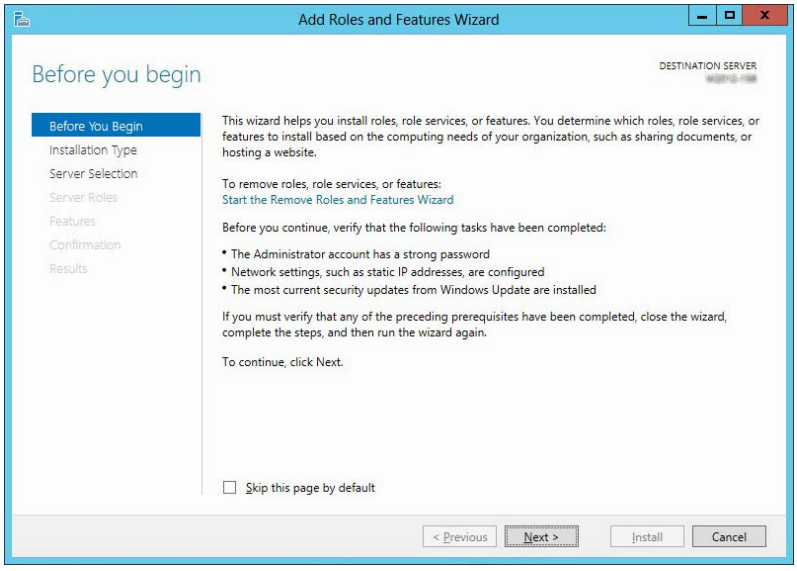
Server Roles and Features

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

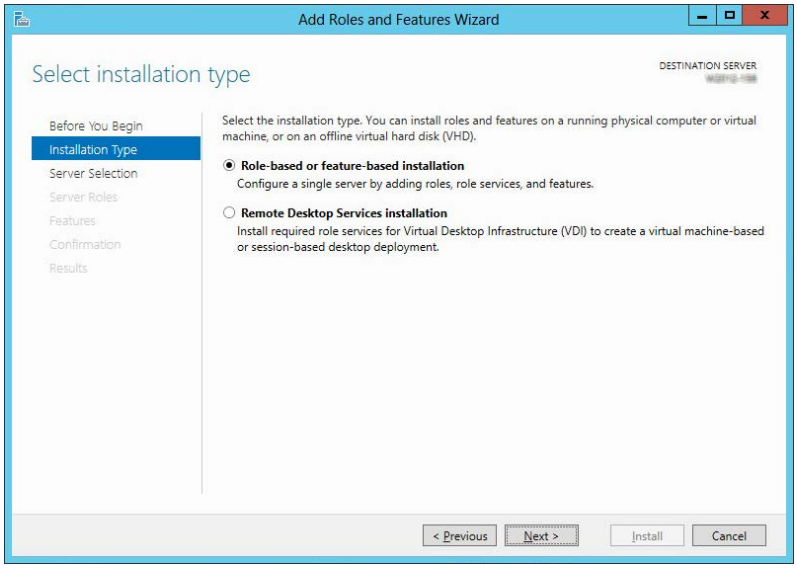


   If this screen is hidden, go to **View** and select **Show Welcome Tile**.

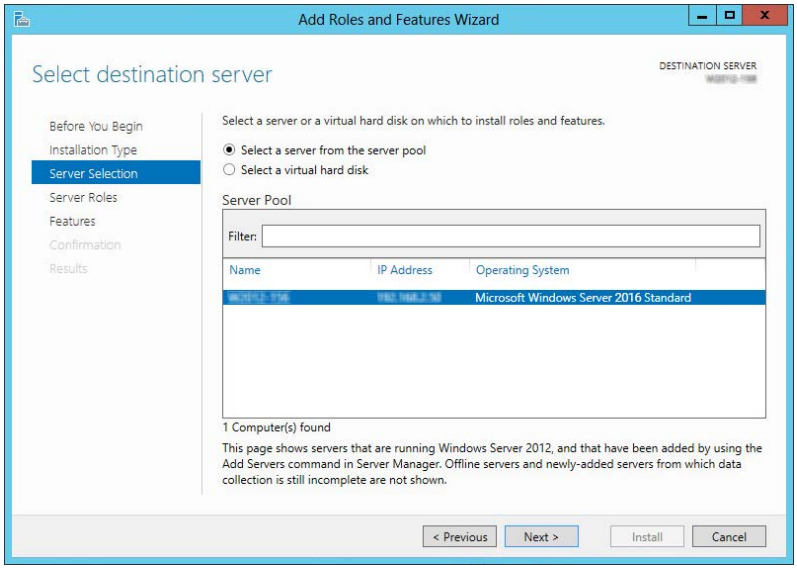
2. Click **Next**.



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

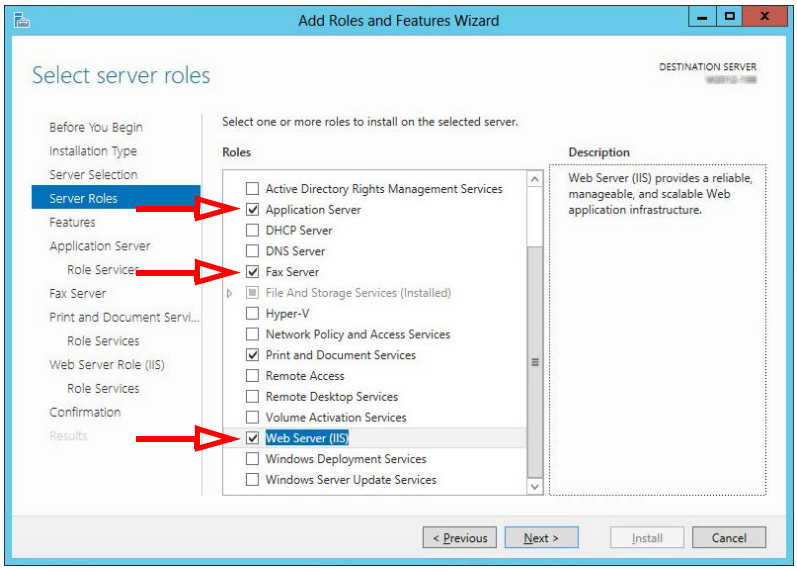


4. Leave the default settings as they are. Click **Next**.

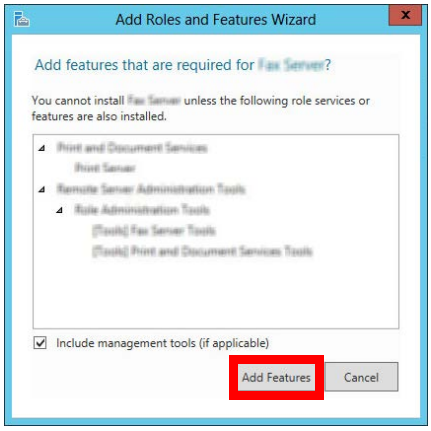


5. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes.

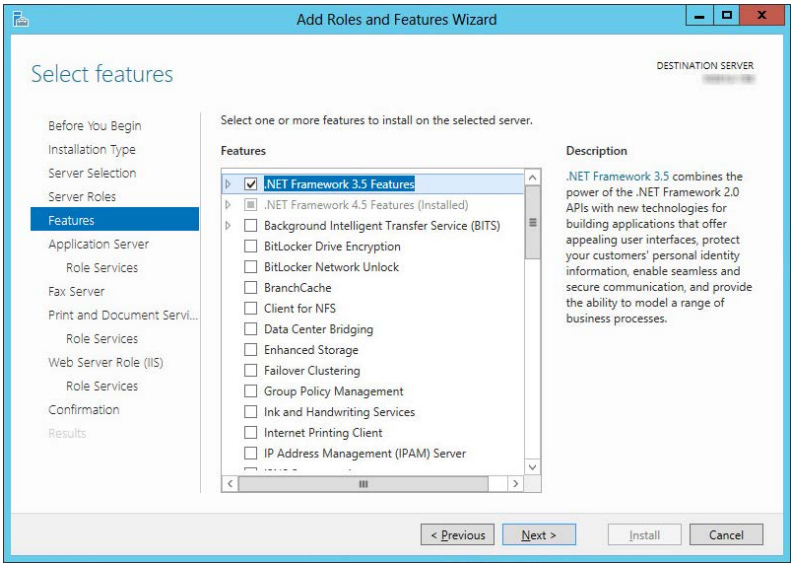
   Click **Next**.



Note: Throughout this installation, whenever you are prompted to confirm additions, always select **Add Features**.



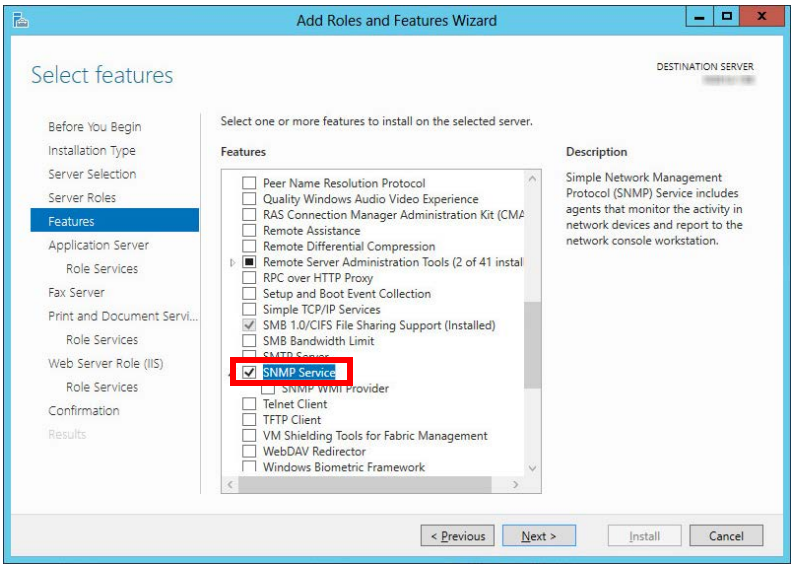
6. Enable the **.NET Framework 3.5 Features** checkbox.
   Expand .NET Framework 3.5 and ensure that **HTTP Activation** is enabled.
   Click **Next**.



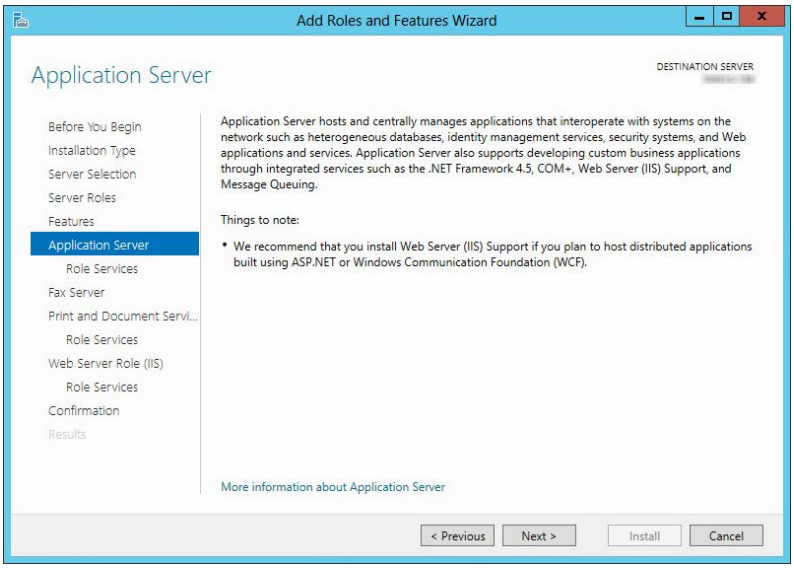
7. **Optional**: If you plan to use **SNMP Alarms** with Messaging, the **SNMP Service** must be added to Windows before the program can be installed.

   If SNMP Alarms are required, scroll down and enable SNMP Service.

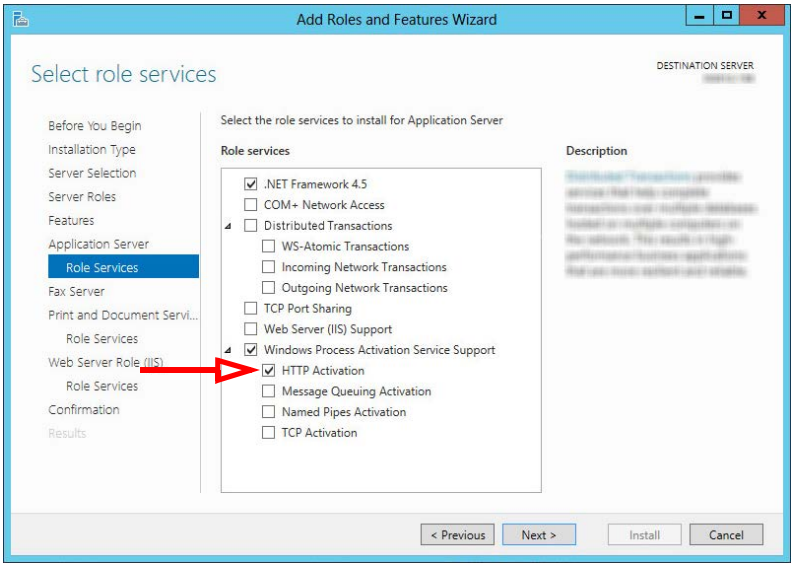
   If SNMP Alarms are not required, skip this step.



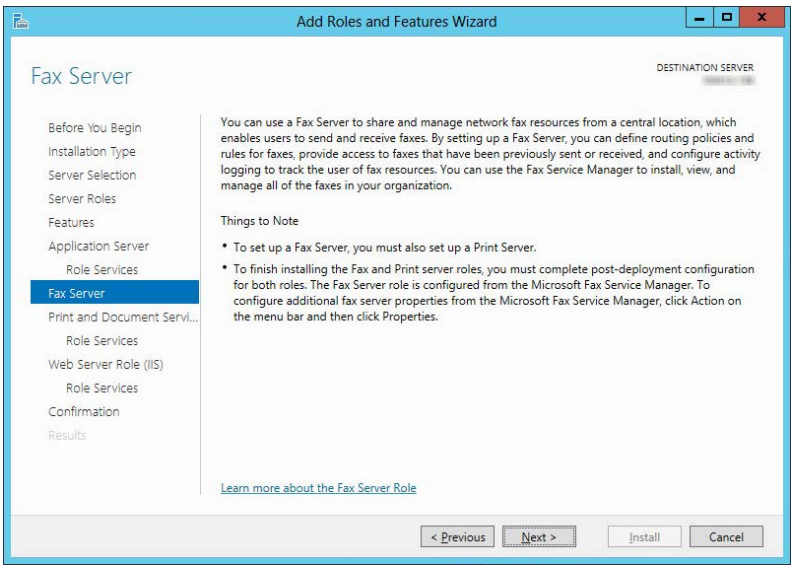
8. Review the information, then click **Next**.



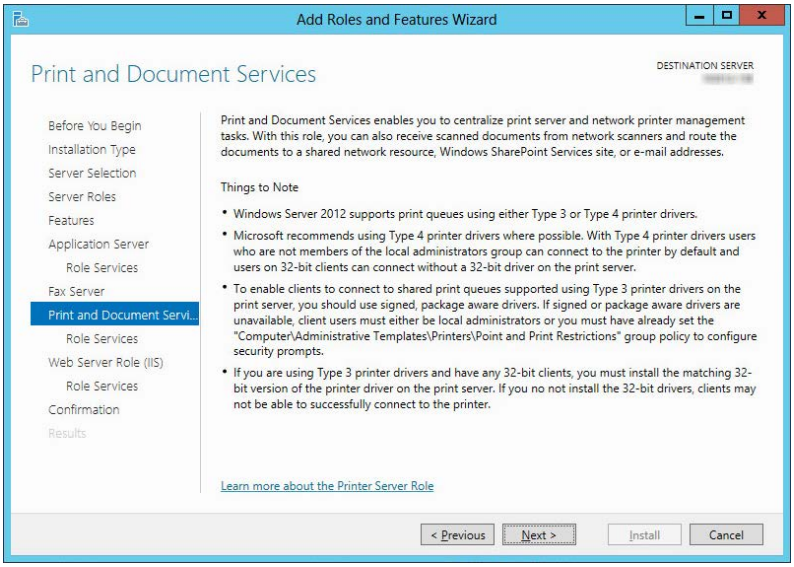
9. Ensure that **HTTP Activation**, under **Windows Process Activation Service Support** is enabled. Click **Next**.



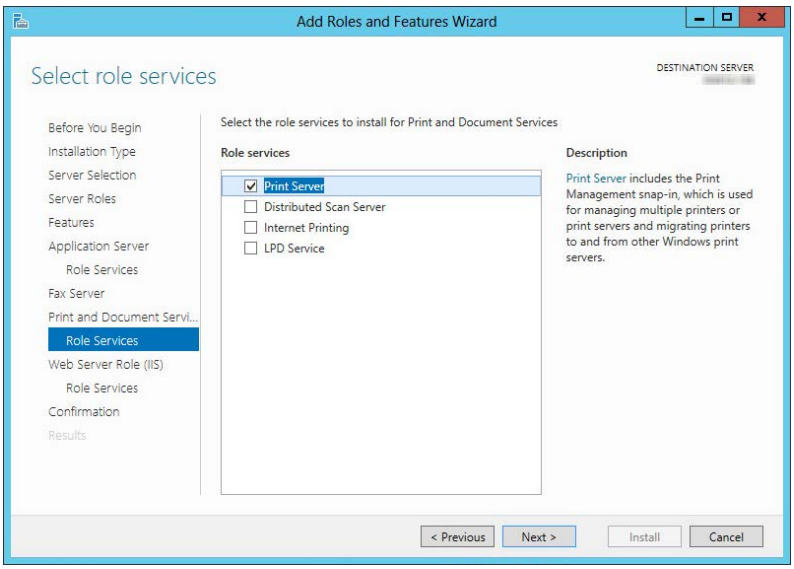
10. On the **Fax Server** screen, click **Next**.



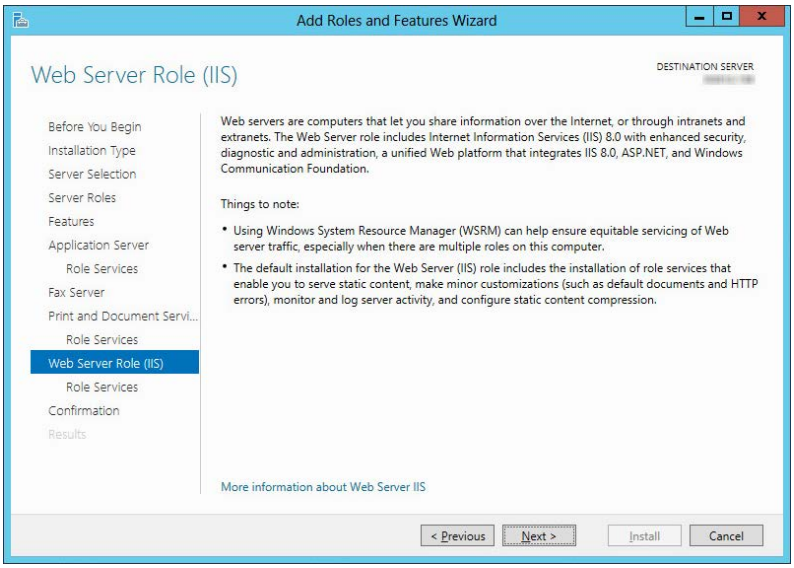
11. On the **Print and Document Services** screen, click **Next**.



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



13. On the **Web Server Role (IIS)** screen, click **Next**.



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

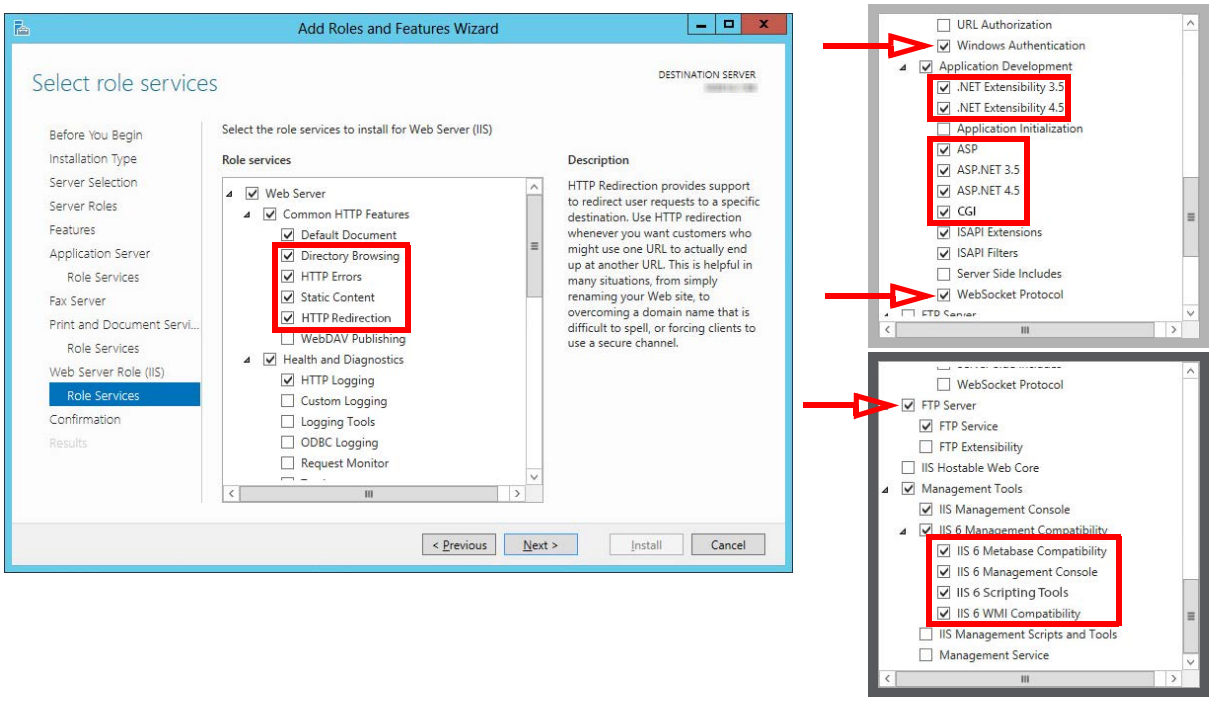
    Scroll down to **Security**, and enable **Windows Authentication**.

    Under **Application Development**, enable **.NET Extensibility 3.5**, **.NET Extensibility 4.5**, **ASP**, **ASP .NET 3.5**, **ASP .NET 4.5**, **CGI**, and **WebSocket Protocol**.

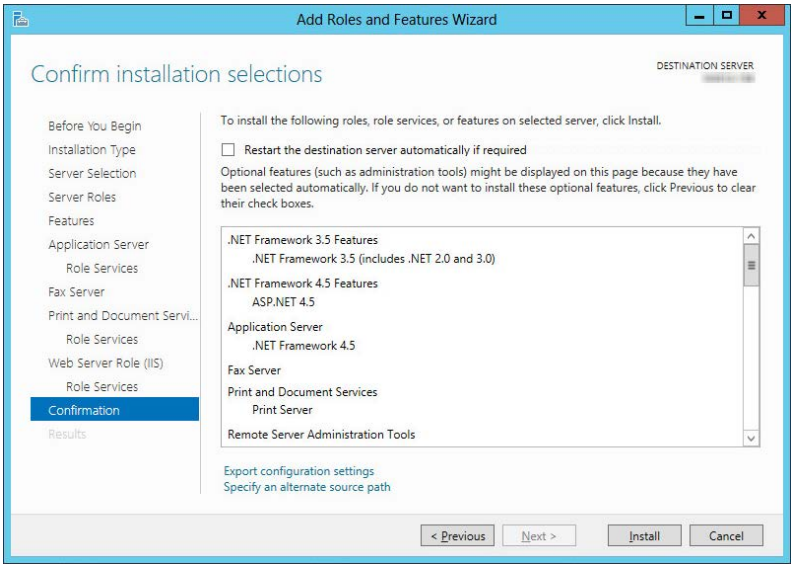
    Locate **FTP Server** and enable **FTP Service**.

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

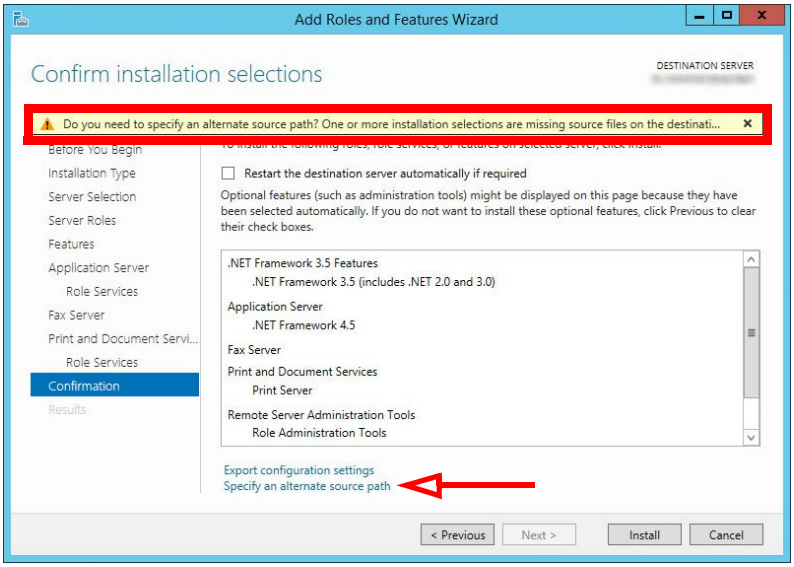
    Click **Next** when ready.



15. Review the selections here. When ready to proceed, click **Install**.

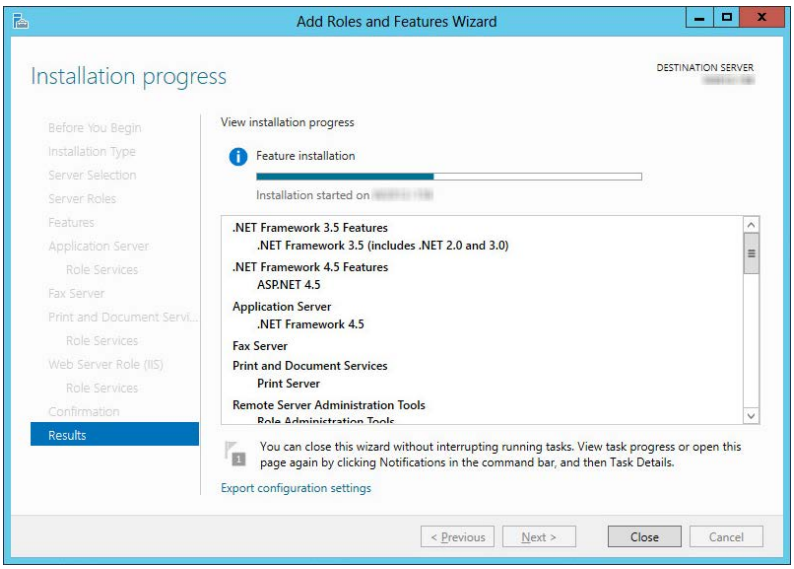


16. If prompted to provide the Windows disk to load the files, click **Specify an alternate source path** and direct it to the appropriate drive.



Hint: This is particularly important for virtual machine installations where there may not be a drive configured locally.

17. Windows will now start the installation process for the chosen items. This process may take a while.

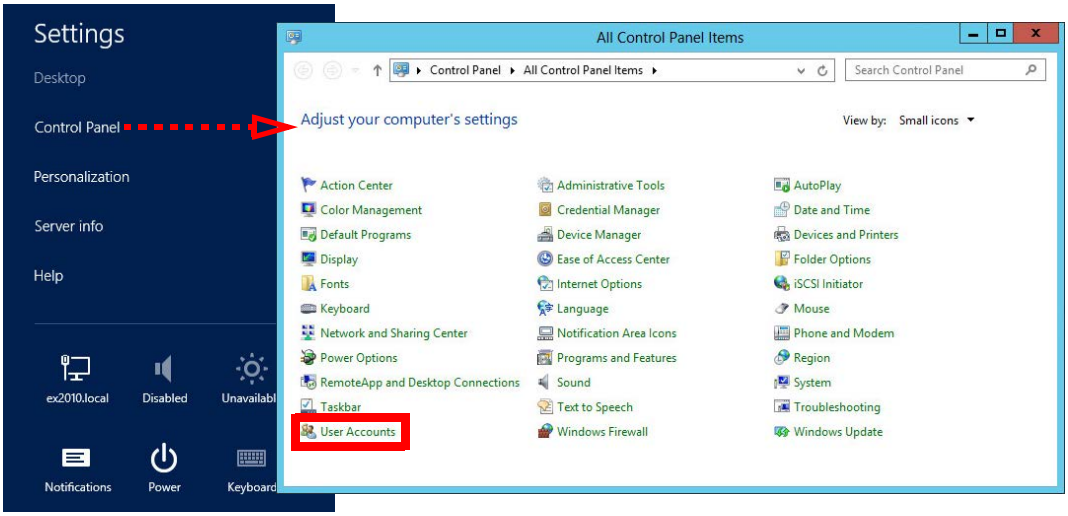


Note: This window can be closed without interrupting the installation procedure

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

Disabling User Account Control Notification

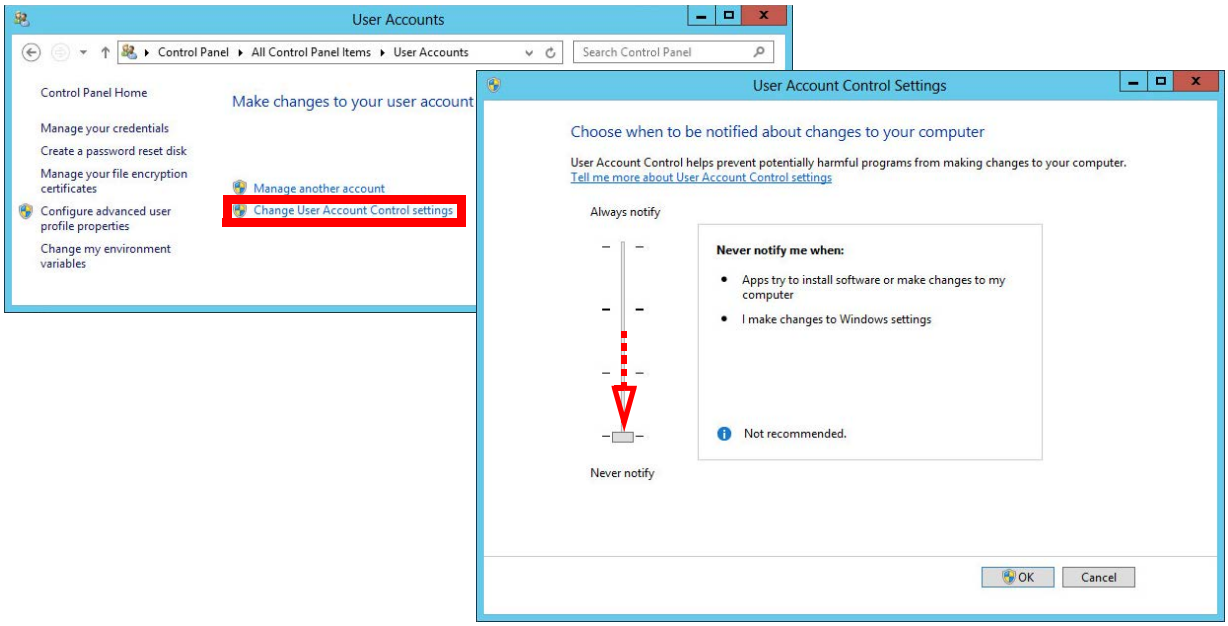
1. Go to **Settings > Control Panel**. Select **User Accounts**.



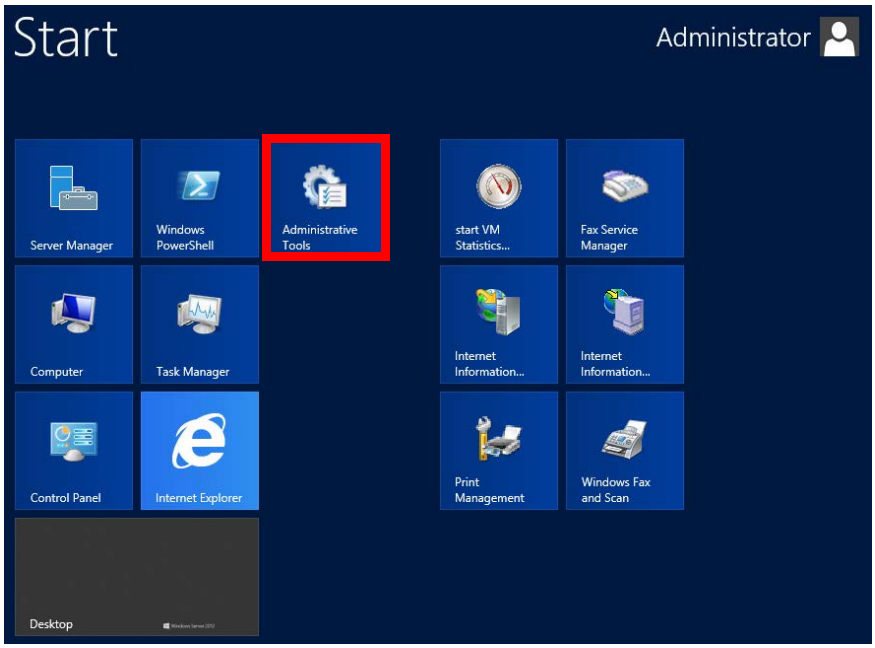
2. Select **Change Account Settings**.

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

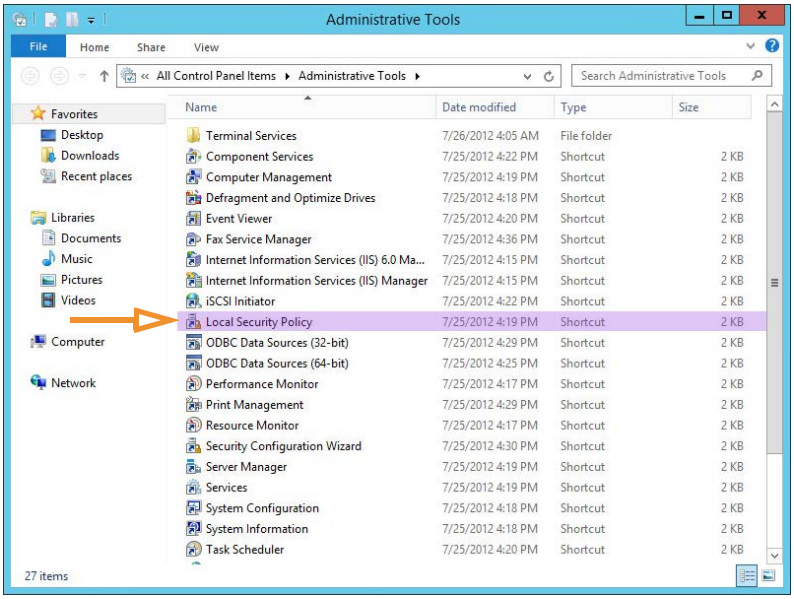
   Click **OK** and **Close**.



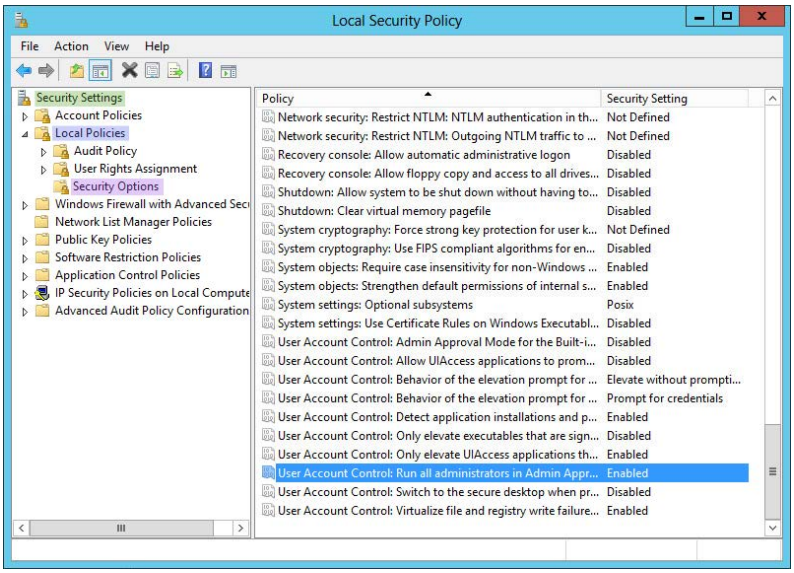
3. On the keyboard, click the **Start button**, and select **Administrative Tools**.



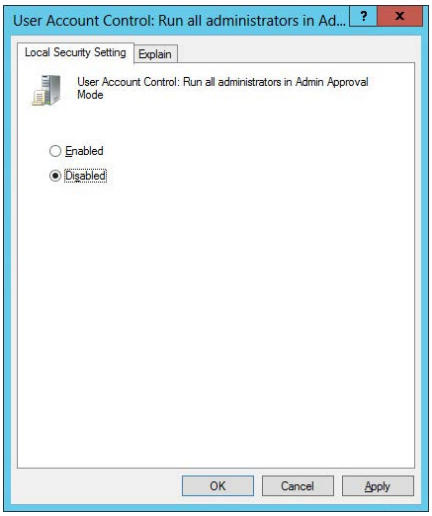
4. Double-click **Local Security Policy**.



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**.



Note: UAC Notifications can be restored after Messaging 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:

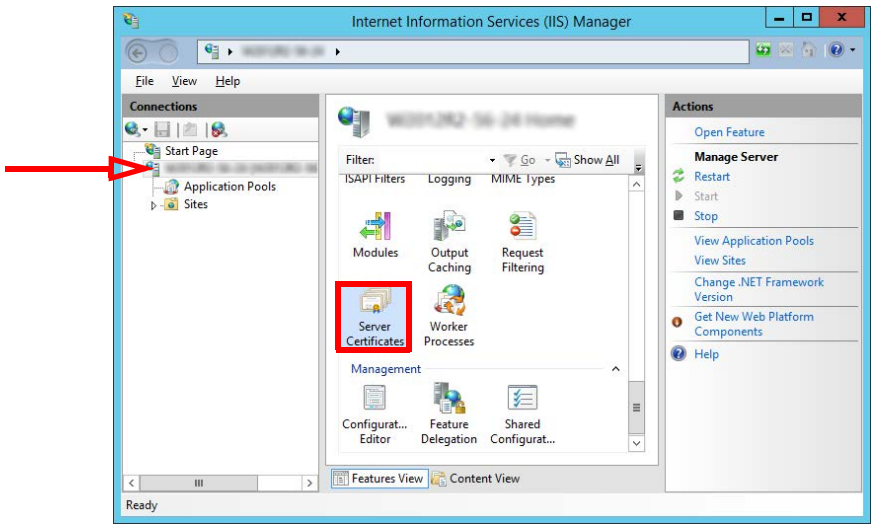
https://technet.microsoft.com/en-ca/library/cc753127(v=ws.10).aspx

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

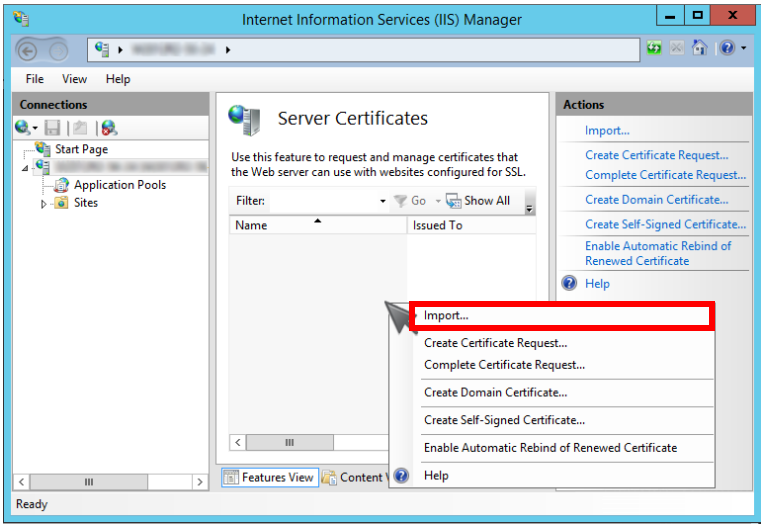
IIS Certificate Bindings

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

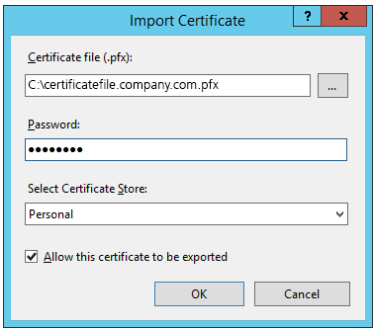
1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.



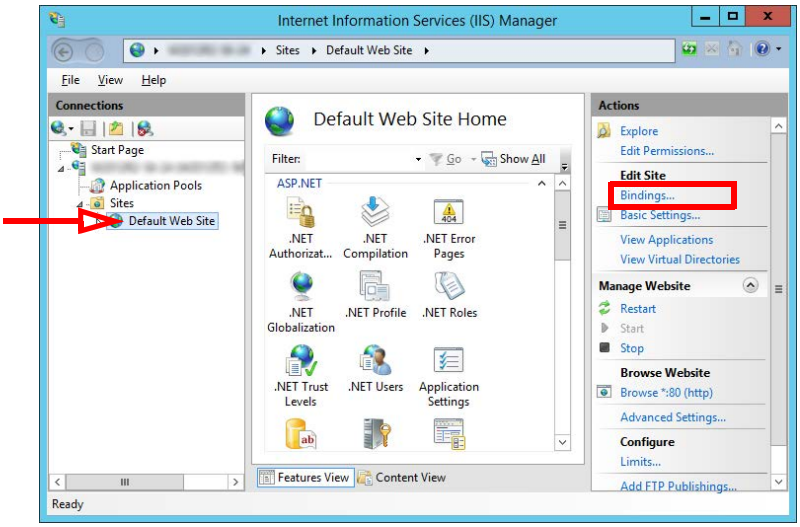
2. Right-click in the right-hand pane and choose Import from the pop-up menu.



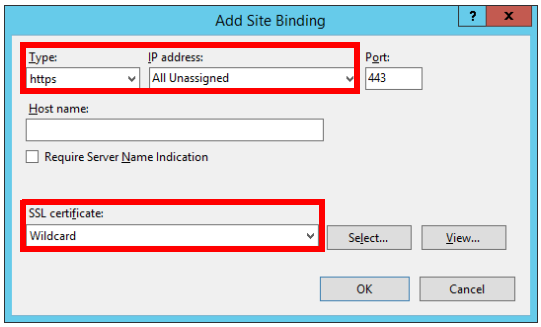
3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.



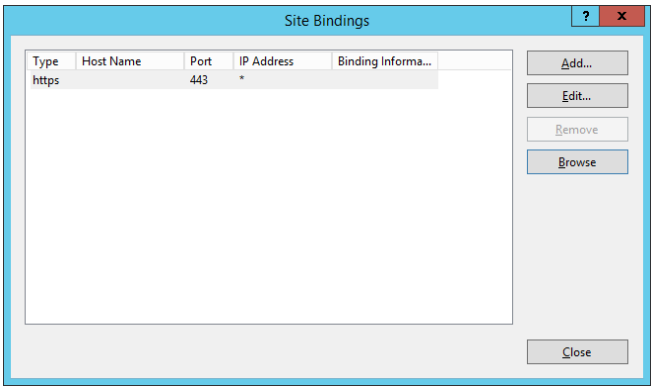
4. Go to **Sites > Default Web Site**.
Click **Bindings...**.



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**.



Install Microsoft .Net Framework 4.7.2

Avaya IX Messaging requires Microsoft .Net Framework version 4.7.2 to be installed to support various features within the program. If it has not already been installed, the administrator must download it and install it manually.

Note: .Net Framework 4.7.2 is not installed by default. It may be part of Windows updates, optional updates, or not provided at all. Follow these instruction is it is not installed on your system, or if you do not know if it has been installed.

1. Open a web browser and go to the Microsoft web site. Search for .Net Framework 4.7.2 and install the application on the server. For example:
   https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows .
2. Download the file to your server drive. When ready, run the program to install this feature.
3. When finished, restart the server.

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 IX Messaging has not logged in as the system administrator, that user must be given full rights to the root of the C drive.

About Passwords

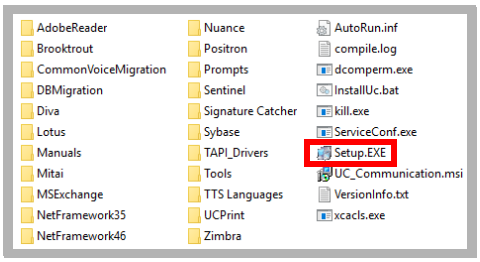
These rules are applied to all passwords created or used with Avaya Messaging, including those created during installation (Note: JITC installations have more stringent requirements). These include:

- **Length**: Passwords must be at least **14** characters long.
- **Class**: A password can contain upper and lower case characters, numbers and special characters. No minimum requirements for each character class are set by default, but this can be changed by the administrator.
- **Repeating Characters**: No character can be repeated more than 2 times consecutively (he**ll**o, world**!!**). This value can be modified by the administrator.
- **Repeating a Character Class**: No class of character can be repeated more than 4 times consecutively (ABCD, !@#$). This value can be modified by the administrator.
- **Reusing Passwords**: No new password can be the same as a previous password extending back 10 iterations. This value can be modified by the administrator.
- **Sharing Passwords**: Passwords must not be shared between users. Only one login per account is allowed at one time. Other users must login using different credentials.

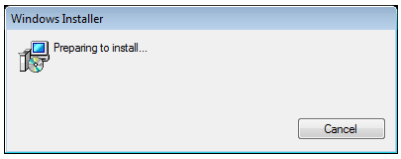
Note: Using an administrator account to perform routine functions leaves the servers open to malicious software attacks. Therefore, it is **strongly recommended** that each user with administrative privileges is also assigned a standard user account. To maintain security integrity, the administrator account should only be used when necessary, and should be immediately logged out afterwards.

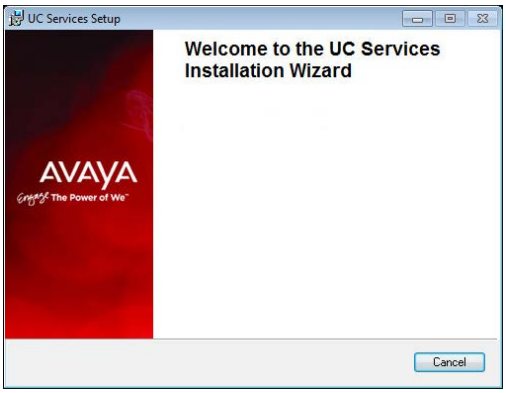
Procedure

1. Download the installation file (see chapter 4). 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 IX Messaging onto your voice server.





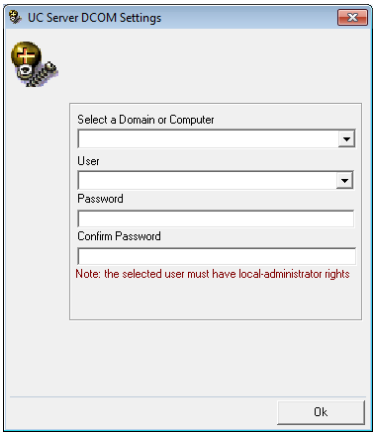
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging. They can also be downloaded from resources.zag.io in both PDF and HTML format.

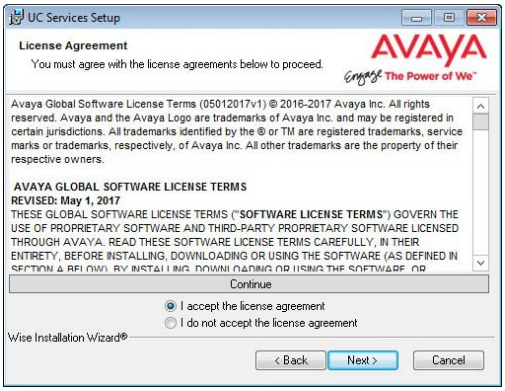
4. Enter the DCOM settings (local machine administrator login information). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.



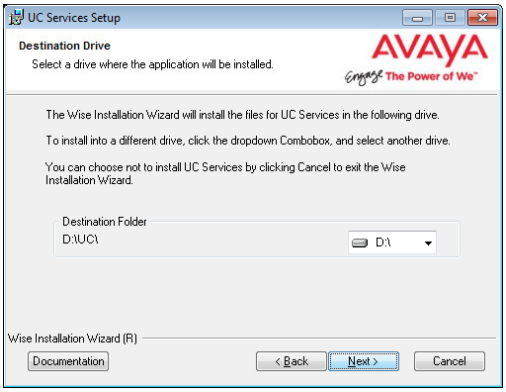
5. Review the license agreements and enable **I accept the license agreement**.

   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.

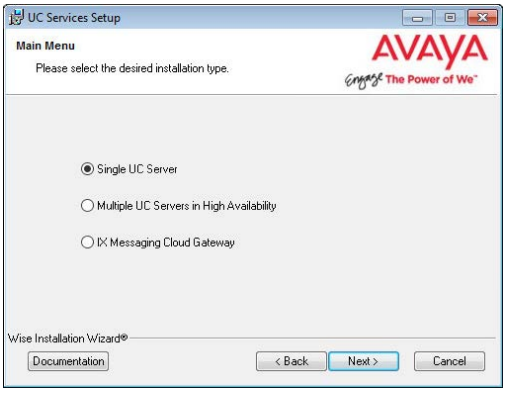
   Click **Next** to continue.



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**.

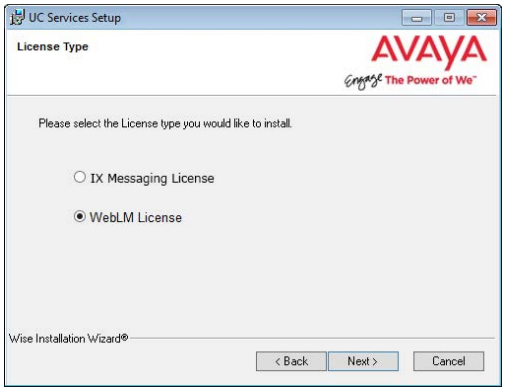


   Single UC Server: When operating Messaging on a single voice server computer.

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

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, 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.

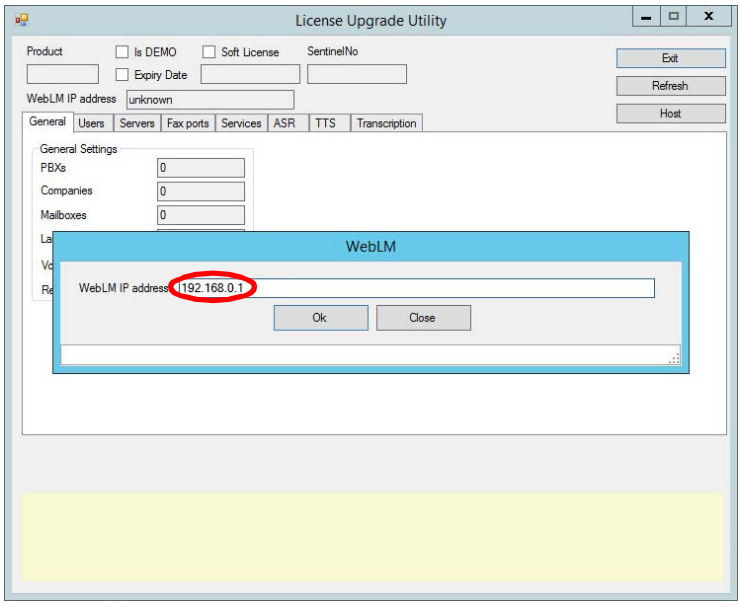


Note: If you select Messaging, go to **chapter 13, Installing the Messaging License**. When finished, return here and continue the installation from **step 11**. Skip step 9 through 10.

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.

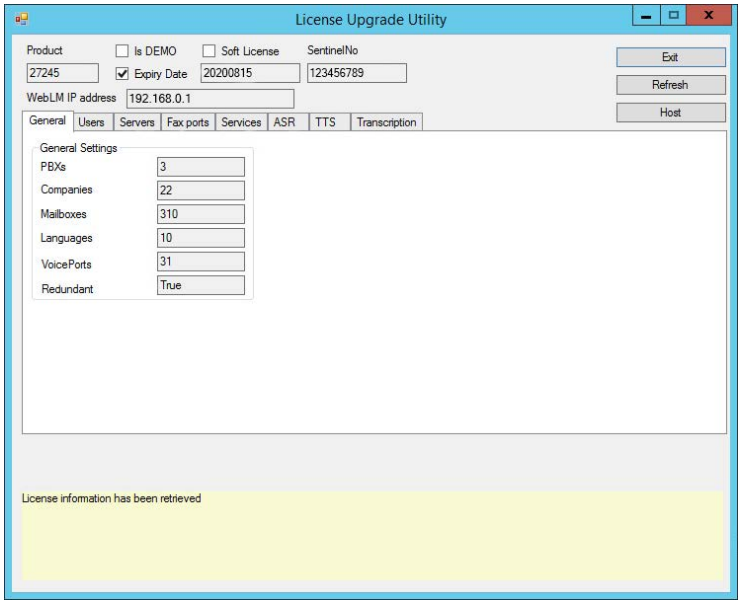
9. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   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 437.

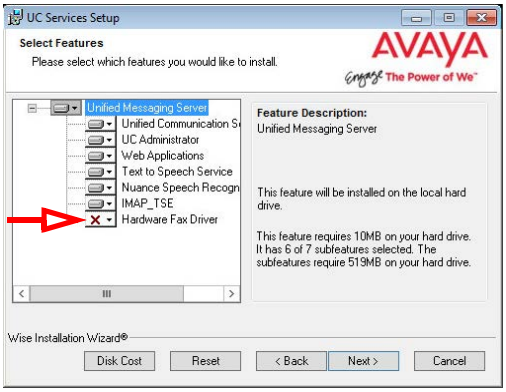
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.



Note: The number of voice ports is calculated based upon your license.
[(# Basic users + # Mainstream users) / 40] + Number of voice ports in license

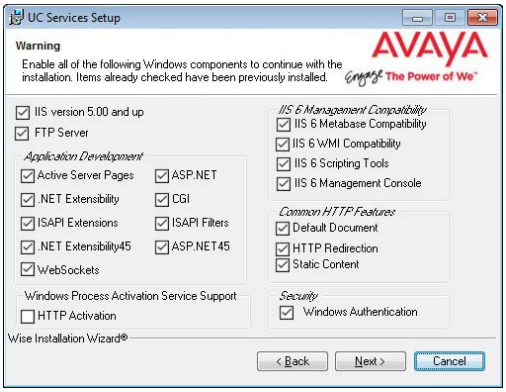
11. Select the **Components** required at your site. Disable any components that are not needed.

    Click **Next**.



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 Messaging requires to operate properly.



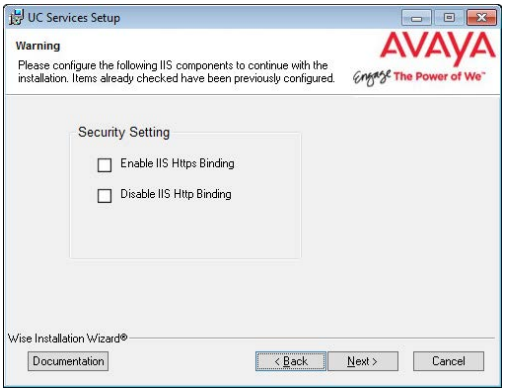
For all items that are not checked, return to Windows and add any missing pieces to the operating system.

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

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

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 Messaging requires to operate.



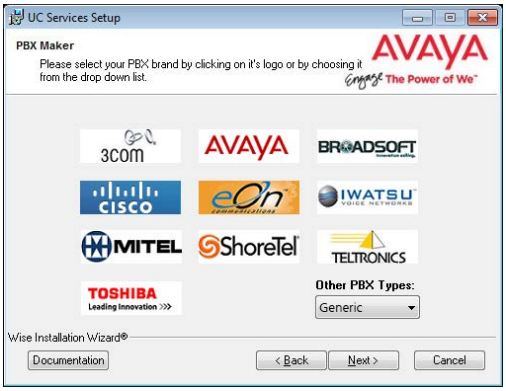
Note: This screen will only appear if one or more of the required settings has not been made on the computer.

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.

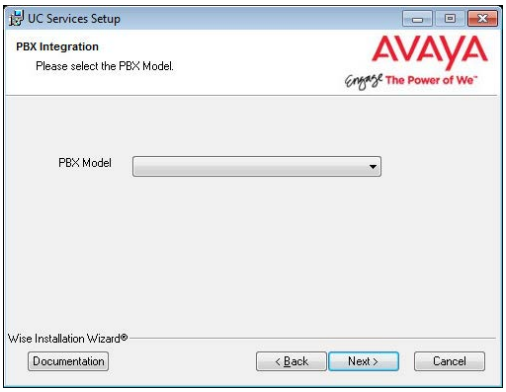
Note: The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

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



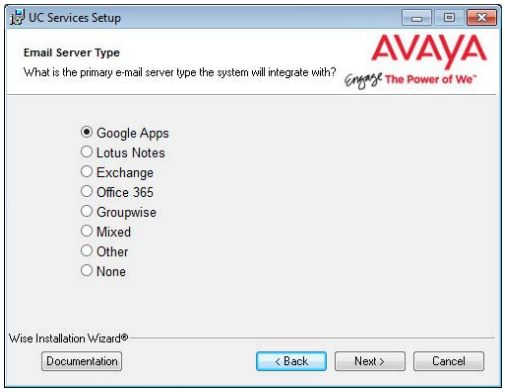
15. Select your PBX model from the dropdown menu.

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.

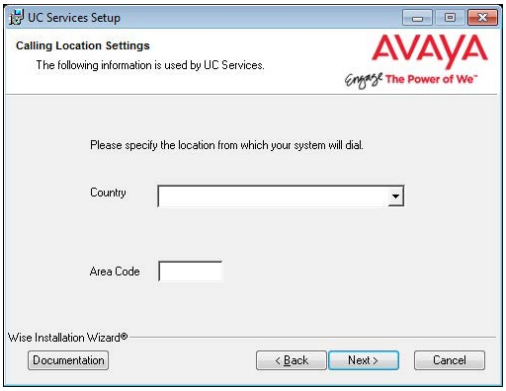
    When ready, click **Next**.



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.

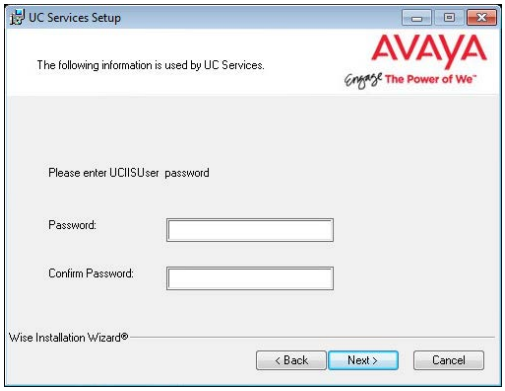
    Select the country from the dropdown menu, and enter the area code in the space provided.

    Click **Next** to continue.



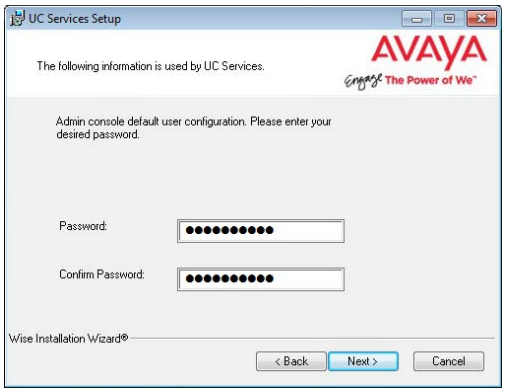
Note: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

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 IX Messaging.

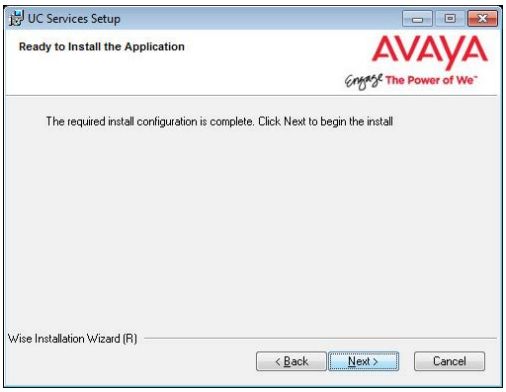
Hint: The password cannot be left blank. It must contain both letters and numbers (no special characters), and should be at least 6 characters long.



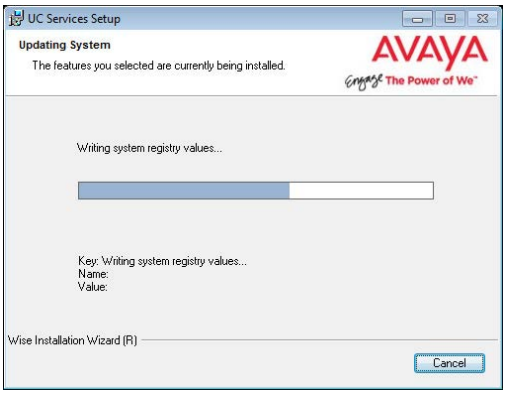
20. Choose either **Yes** or **No** to determine whether the system will apply General Data Protection Regulation (GDPR) compliance procedures to your data.
With this option enabled, users and callers are notified that personal information will be collected. This information can also be completely removed from the system upon request.

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

    Click **Next**.



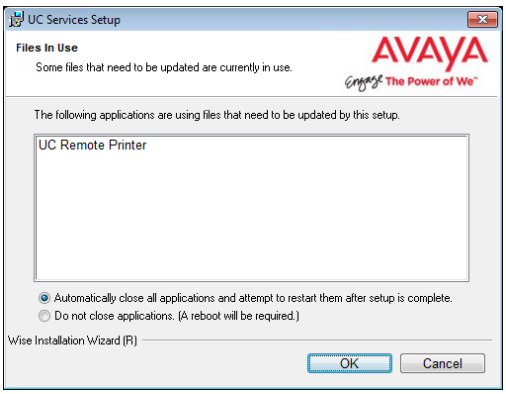
22. The selected components will now be installed. This process may take a while.



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

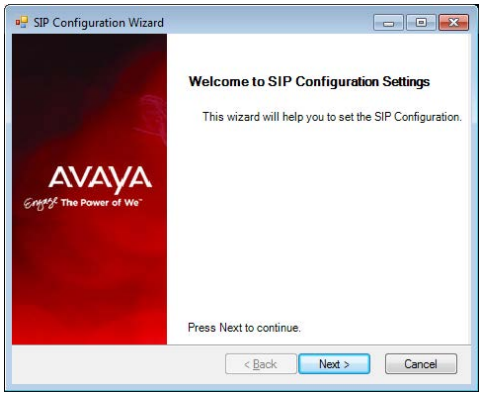
    Click **OK** when ready.

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

    Click **Next** to continue.

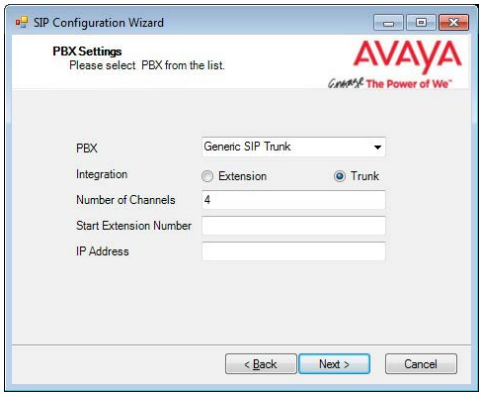


26. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.



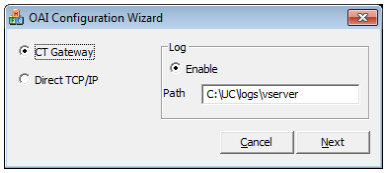
27. Confirm the information then click **Finish**.

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 Messaging programs folder after installation.

Note: This section is for installations where **Mitel 5000 (All)** was chosen at the PBX selection screen. Go directly to step 32 if this does not apply to your site.

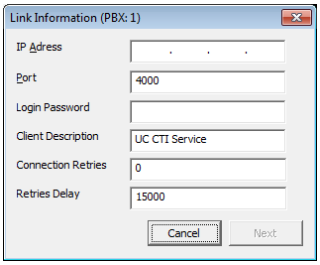
28. At the OAI Configuration Wizard screen:
    - Enable **Direct TCP/IP**.
    - **Set Number of Nodes = 1.**
    - **Activate the Enable logs radio button. The default path for the log files is shown. Enter a different path if the log file will be saved to another location.**

    Click **Next**.



29. 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.

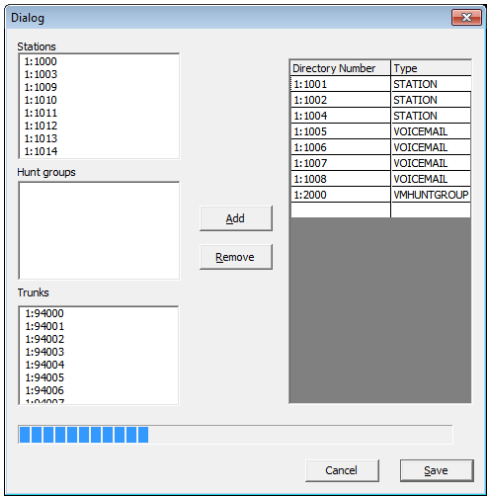
    Click **Next**.



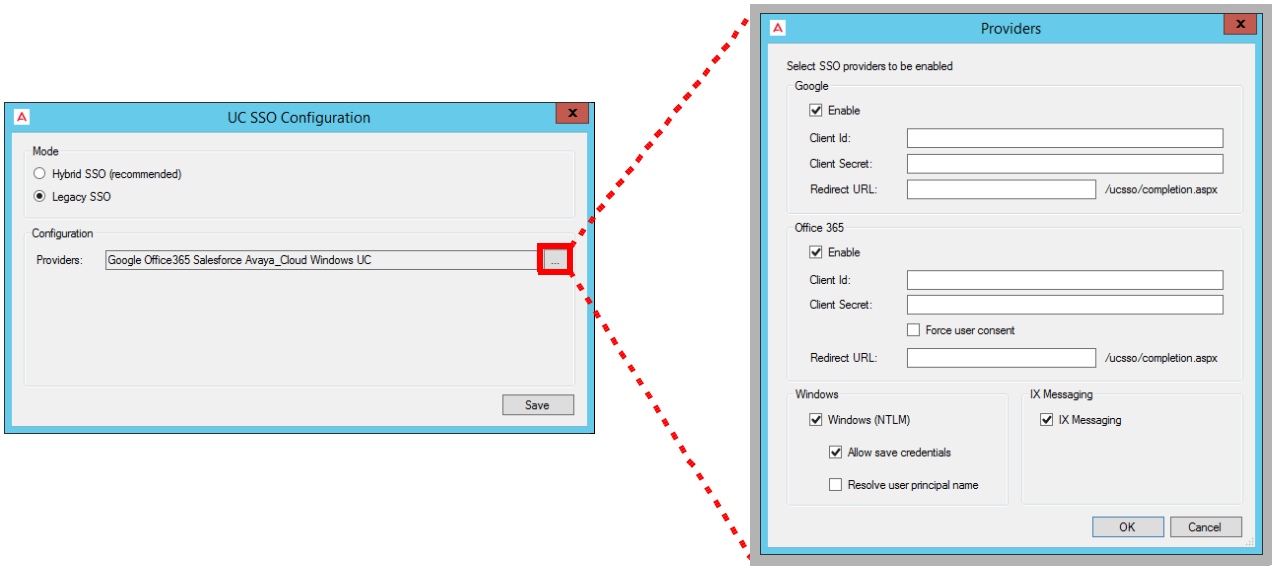
30. At the **Dialog** screen, from the lists on the left-hand side, choose the desired **Stations** (extensions and voicemail ports), **Hunt Groups** and **Trunks** to use with OAI.

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

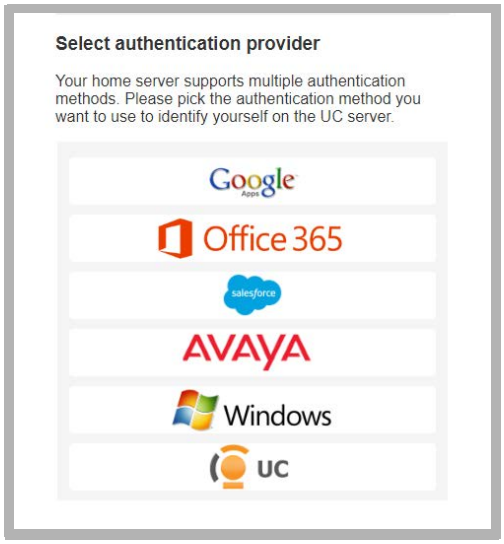
31. Click **Save** to finish the OAI setup and continue with the Messaging installation.

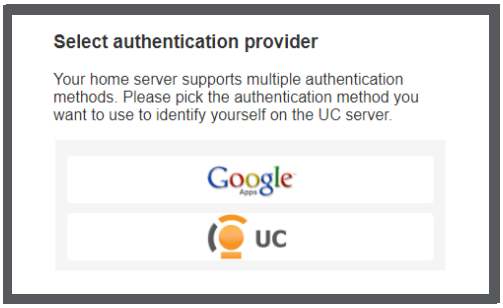


32. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



When clients / admins want access to these programs, they login using their credentials for one of the listed programs. They must have an account with that application before they can login.





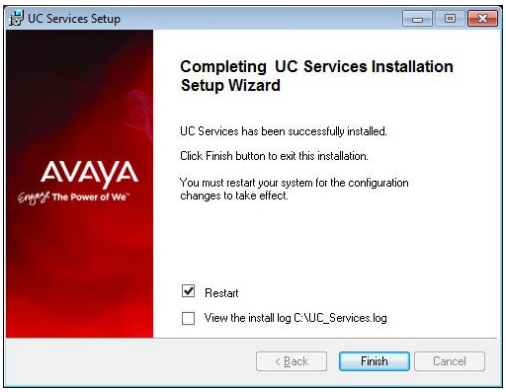
Enable all that apply, then click **OK**.

Click **Save** when finished.

Note: For complete details on using legacy and hybrid SSO, refer to chapter 25 of this document.

33. 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 Messaging installation is complete.

7 HIGH AVAILABILITY INSTALLATION

In This Chapter:

Introduction

Warning: Avaya IX Messaging High Availability **must** only be installed by trained and certified personnel.

This document provides the installation procedure for Avaya IX Messaging with a **High Availability Server (Primary, Secondary & Consolidated)**. The purpose of a High Availability Installation is operational continuity, in which the array of servers provides your organization with complete Messaging functionality in case of a voice server failure. The Consolidated server synchronizes the voice servers (Primary and all Secondaries) and maintains the database.

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 (Primary or Secondary) fails, traffic if routed away from that server to the still active ones.

- The license is maintained by the Primary 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

Requirements	Details
License	A Full License for 10.8 that includes HA.
Software	For details on Messaging 10.8 Hardware and Software requirements please consult the Technical Operating Guidelines.
Operating System	Windows Server 2012 or 2012 R2 Windows Server 2016 Windows Server 2019

Important: Microsoft Windows is not provided with any version of IX Messaging. The customer must install and fully update a suitable, licensed version of Windows onto the hardware platform before proceeding with the Avaya IX Messaging software installation.

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

A High Availability installation requires a minimum of 3 computers, each setup as a server. One server is defined as the Primary 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). A Secondary Consolidated Server can be included for additional failover security.

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

Note: Avaya IX Messaging 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, Primary and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the 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.

Time zones

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

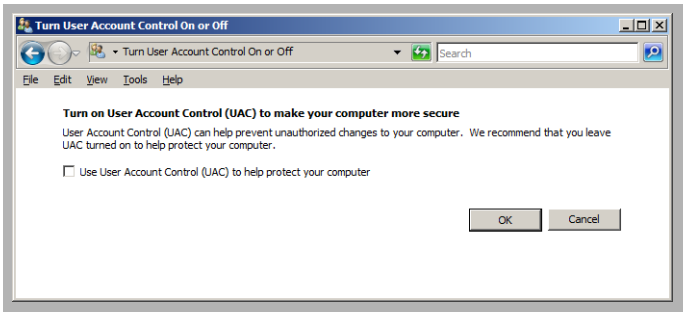
Disabling User Access Control Notification

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

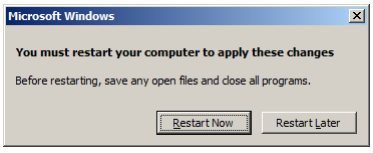
32-bit Windows:

1. Open **Control Panel > User Accounts**.
2. Click **Turn User Account Control on or off**.

3. Disable **Use User Account Control** then click **OK**.

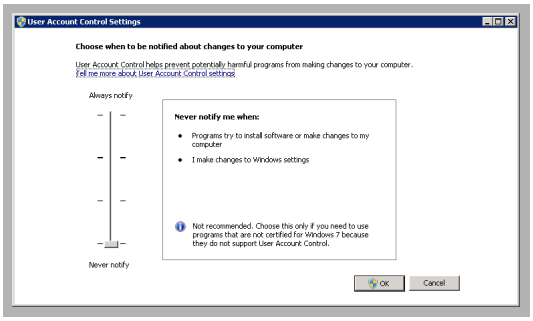


4. You will be prompted to restart your computer. Click **Restart Now** to restart the system.



64-bit Windows:

1. Open **Control Panel > User Accounts**.
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 Messaging installation.

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

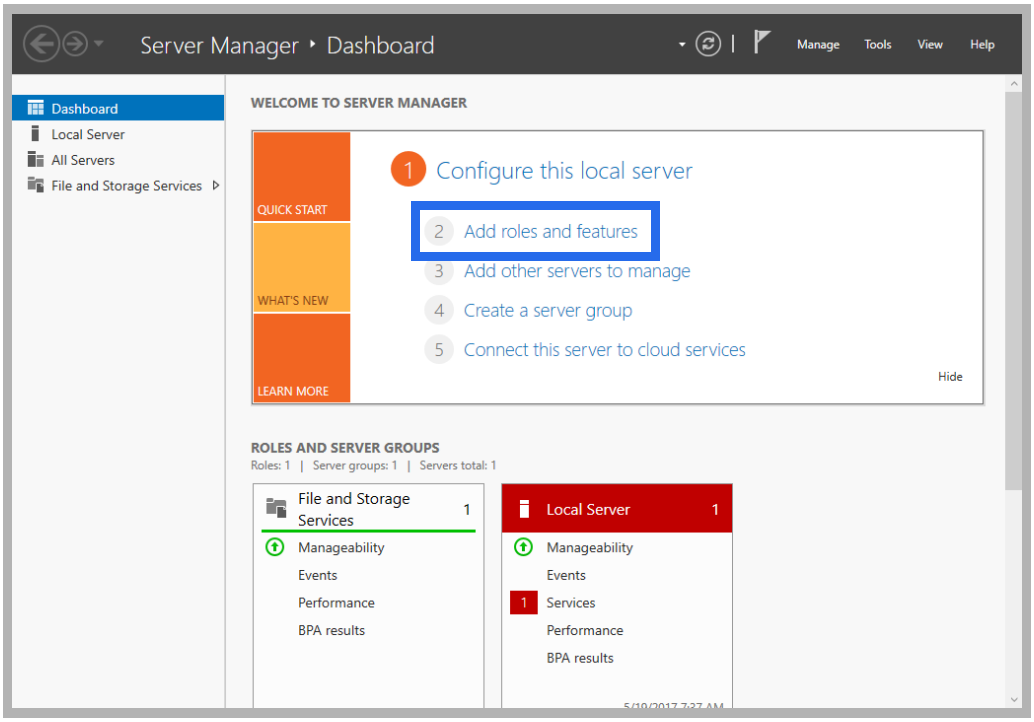
Server Manager Configuration: Win 2016/2019 (All Servers)

If your servers have Windows 2016 or 2019 installed, use this section. If they are using Windows 2012, go to page 183.
Perform the following steps on **ALL** servers; Primary, Consolidated, 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 Primary and Secondary Servers.

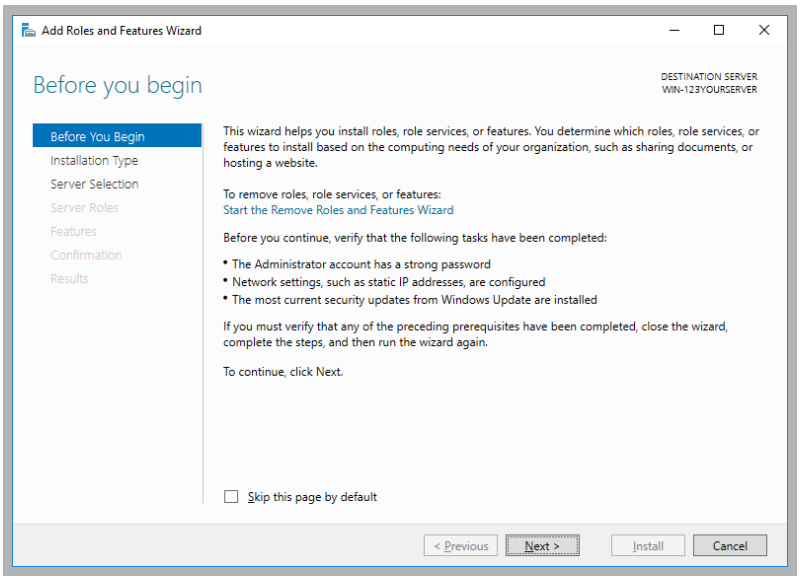
Note: Some of these steps may require additional files from the Windows disk or other storage location.

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

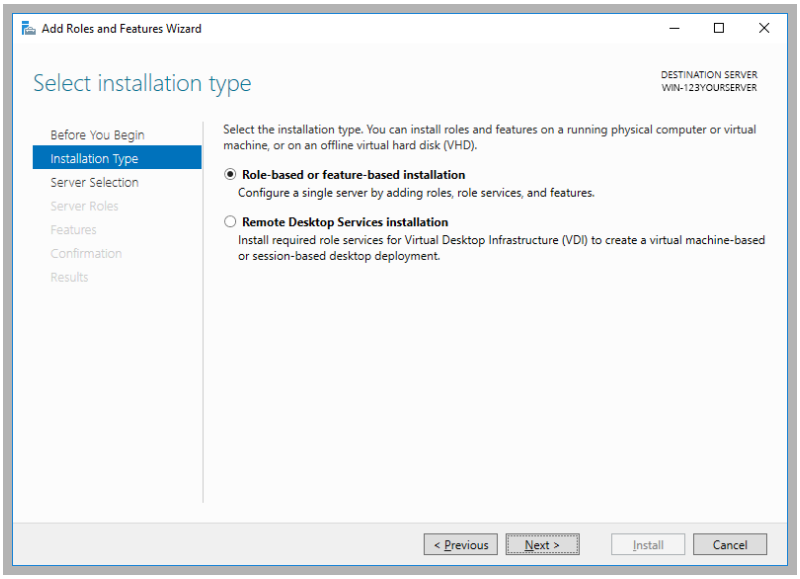


If this screen is hidden, go to **View** and select **Show Welcome Tile**.

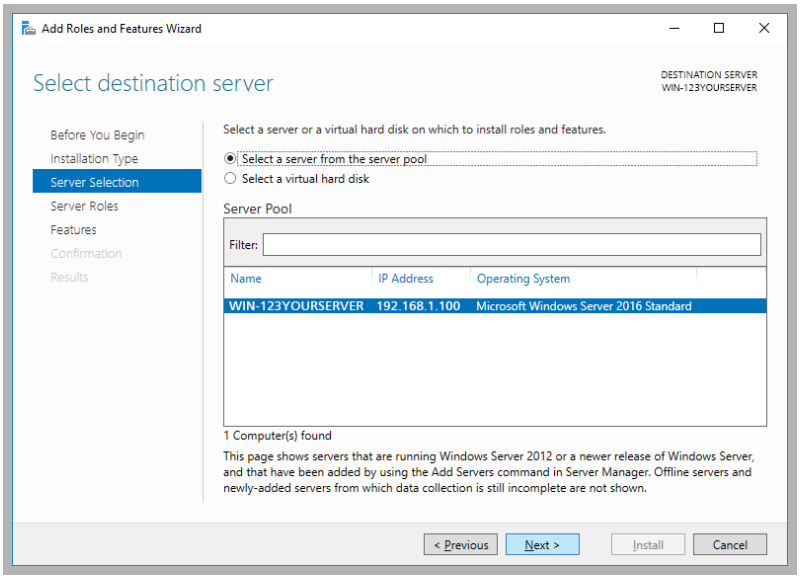
2. Click **Next**.



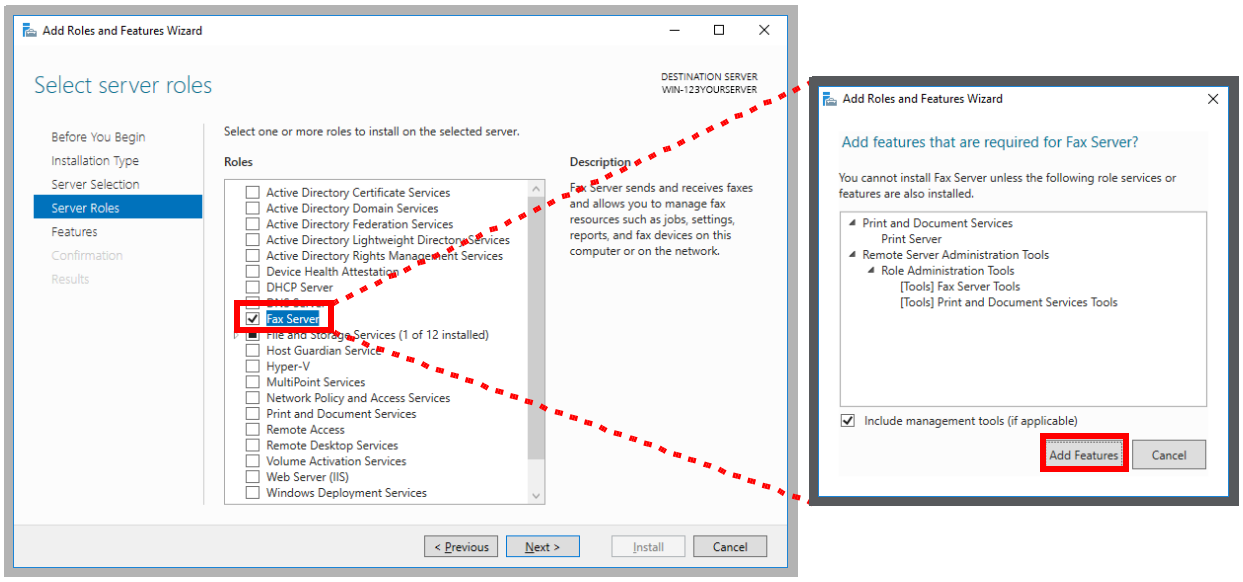
3. Leave the default settings as they are. Click **Next**.



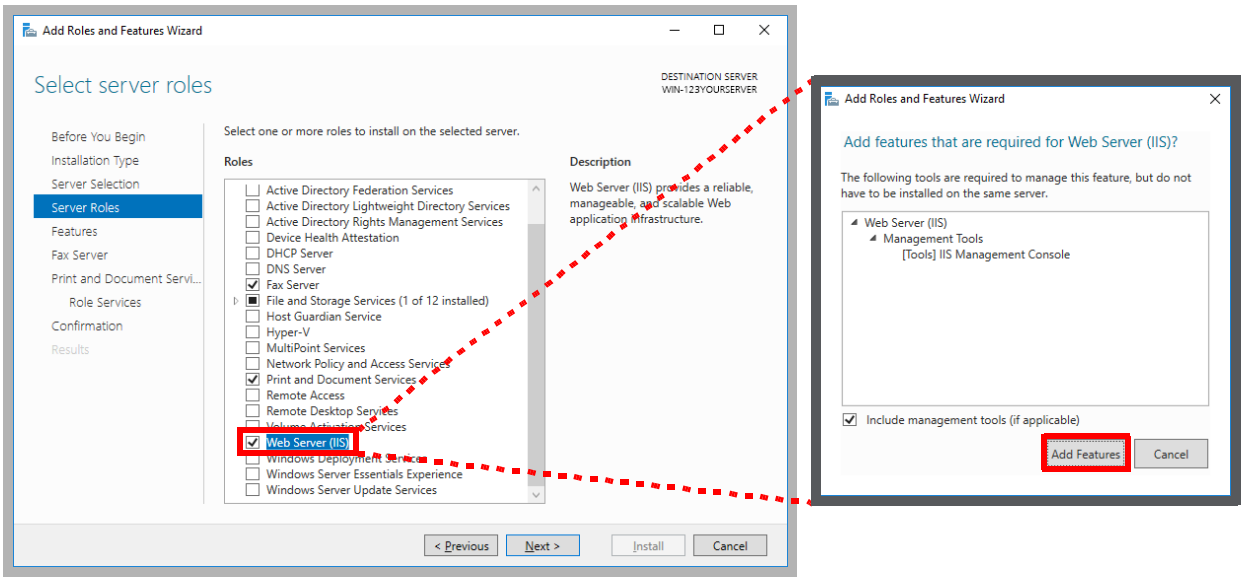
4. Leave the default settings as they are. Click **Next**.



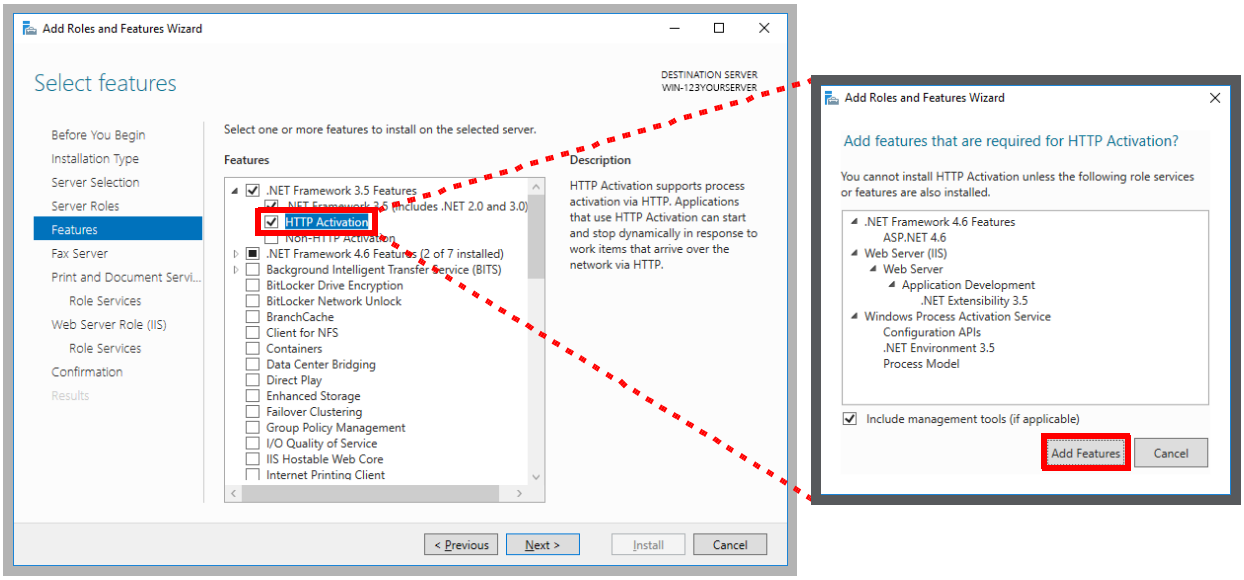
5. Enable **Fax Server**. When prompted, select **Add Features**.



6. Enable **Web Server (IIS)**. When prompted, select **Add Features.** Click **Next**.



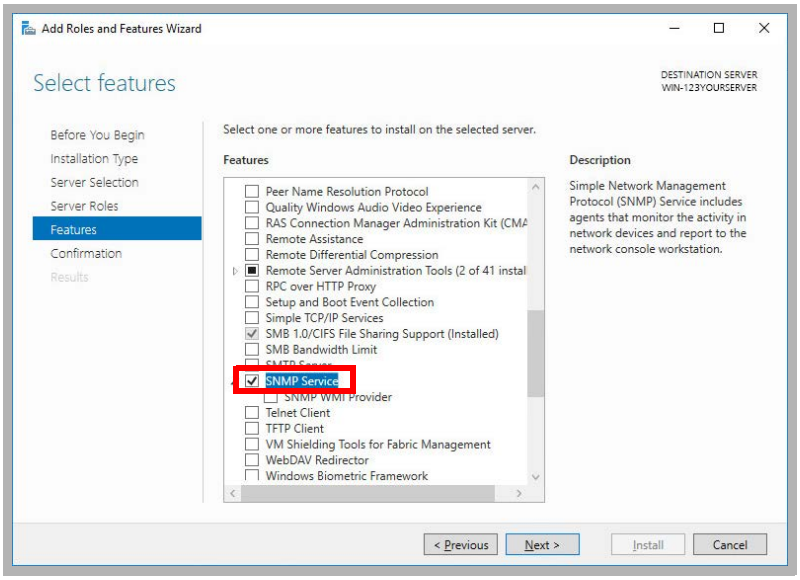
7. On the **Features** panel, open **.NET Framework 3.5 Features** and enable **HTTP Activation**. When prompted, select **Add Features**. Click **Next**.



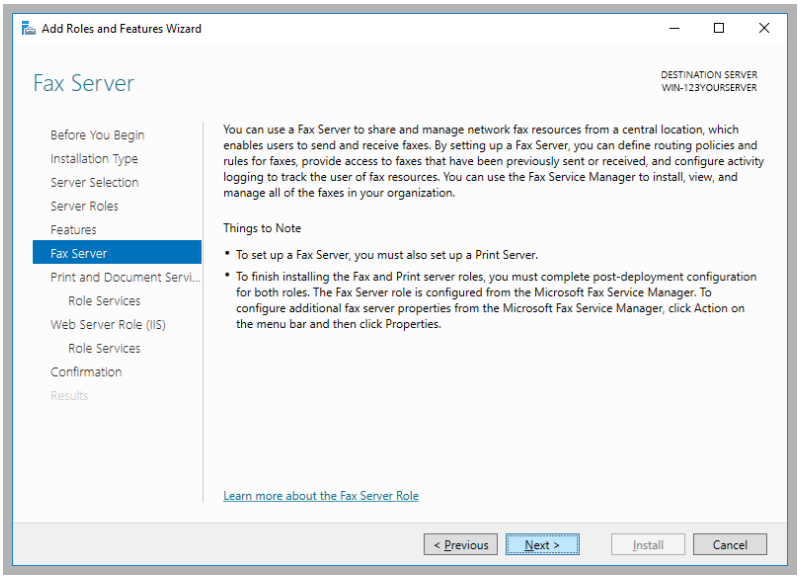
8. **Optional**: If you plan to use **SNMP Alarms** with Messaging, the **SNMP Service** must be added to Windows before the program can be installed.

   If SNMP Alarms are required, scroll down and enable SNMP Service.

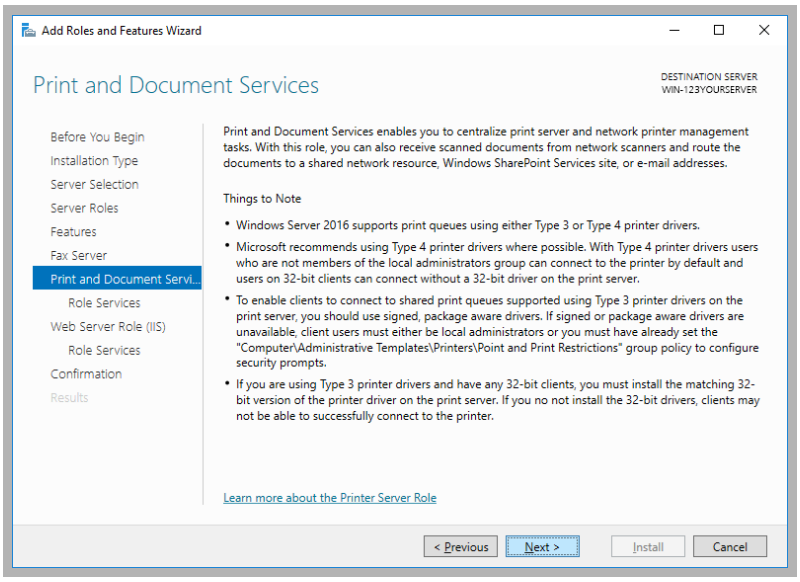
If SNMP Alarms are not required, skip this step.



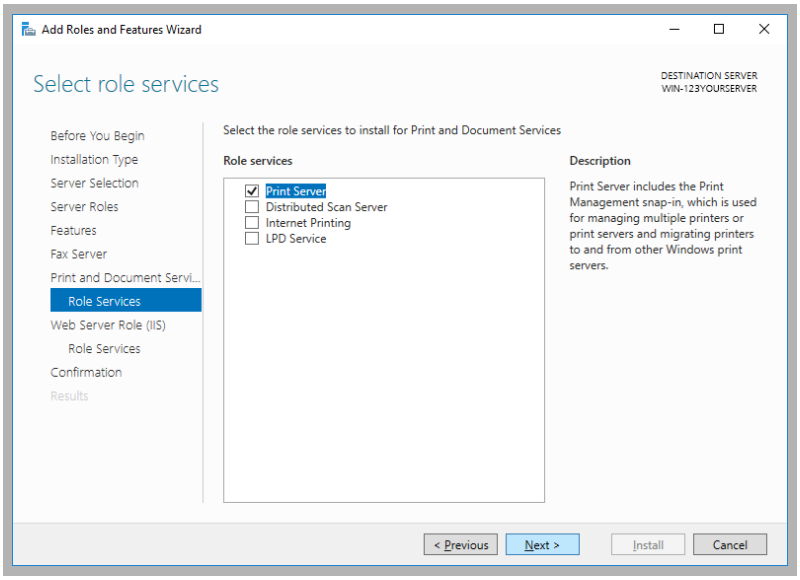
9. On the **Fax Server** screen, click **Next**.



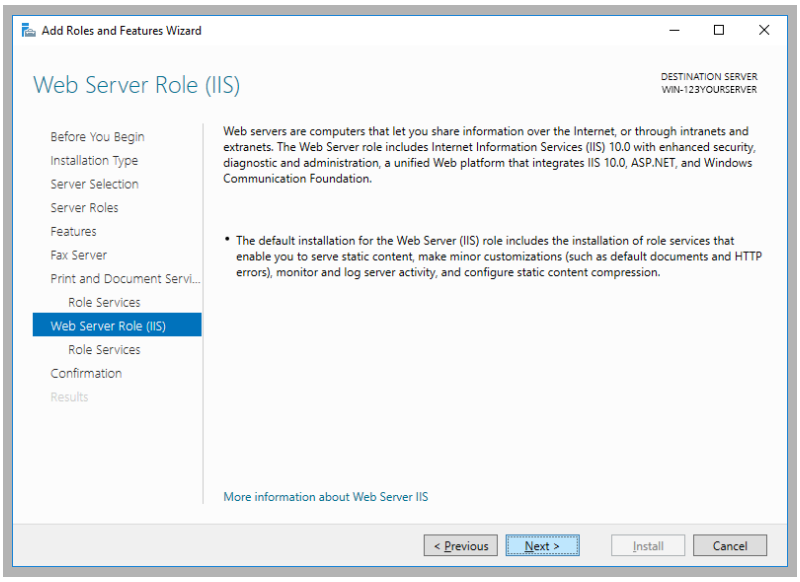
10. On the **Print and Document Services** screen, click **Next**.



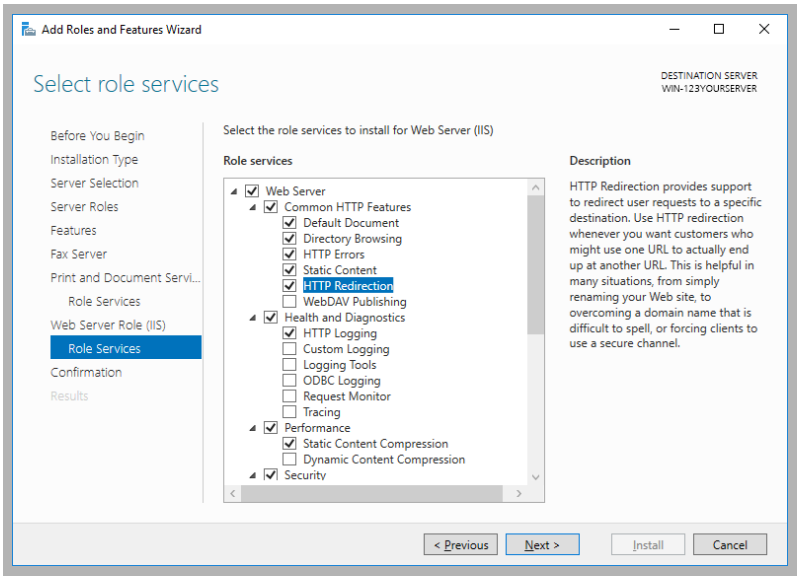
11. No changes are required here. Click **Next**.



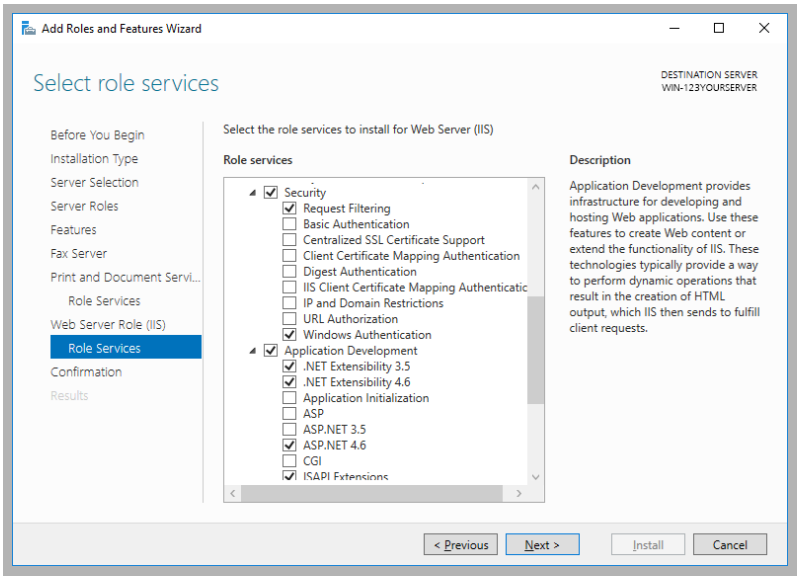
12. On the **Web Server Role (IIS)** screen, click **Next**.



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

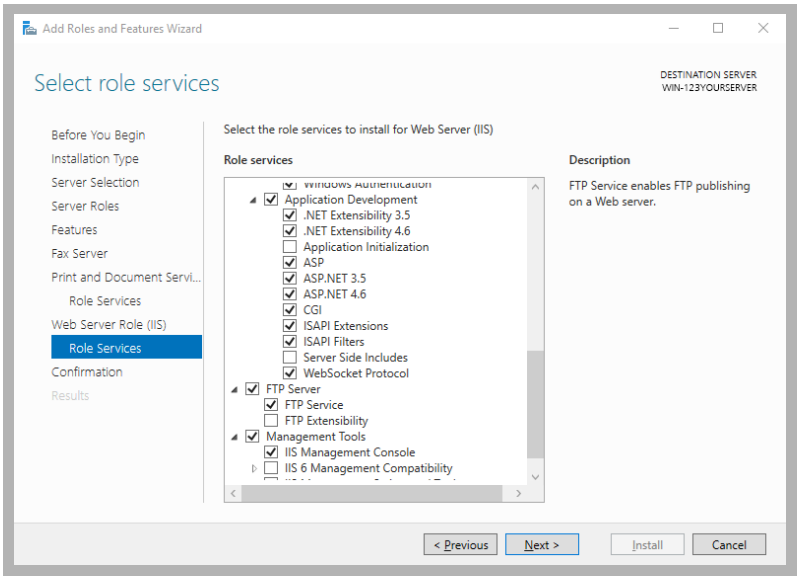


14. Under **Web Server > Security**, enable **Windows Authentication**.



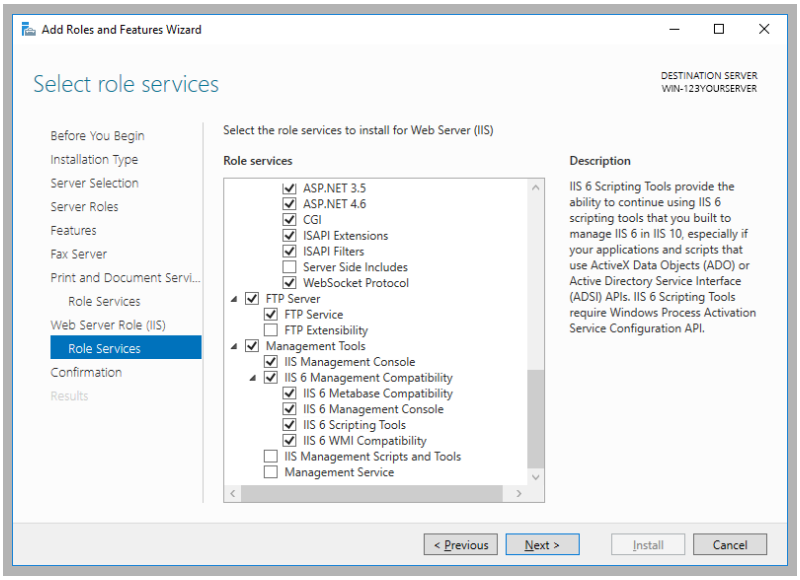
15. Under **Web Server > Application Development**, enable **.NET Extensibility 3.5**, **.NET Extensibility 4.6**, **ASP**, **ASP .NET 3.5**, **ASP .NET 4.6**, **CGI**, **ISAPI Extensions**, **ISAPI Filters** and **WebSocket Protocol**.

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

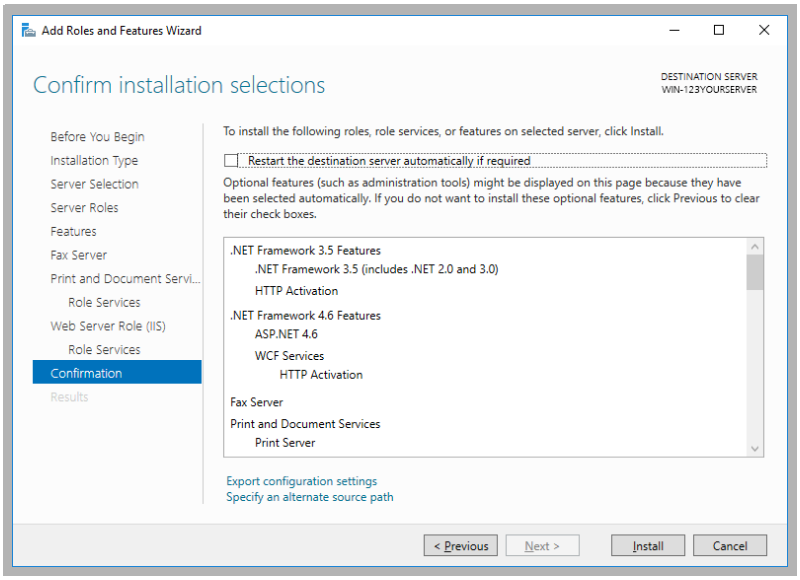


16. Under **Management Tools > IIS 6 Management Compatibility**, enable all items.

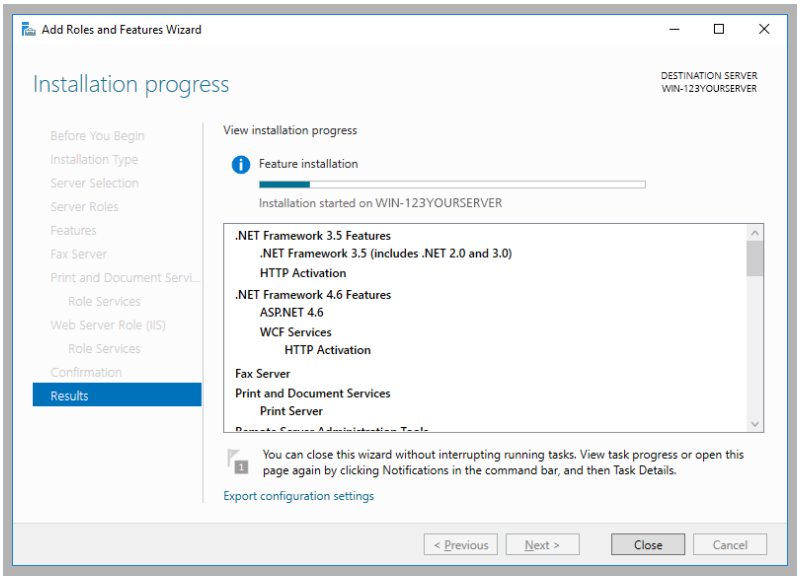
    Click **Next** when ready.



17. Review the selections here. When ready to proceed, click **Install**.



18. 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

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

The next section covers Roles and Services for Windows 2012. You can skip ahead to page 202, IIS Certificates (All Servers).

Server Manager Configuration: Win 2012 (All Servers)

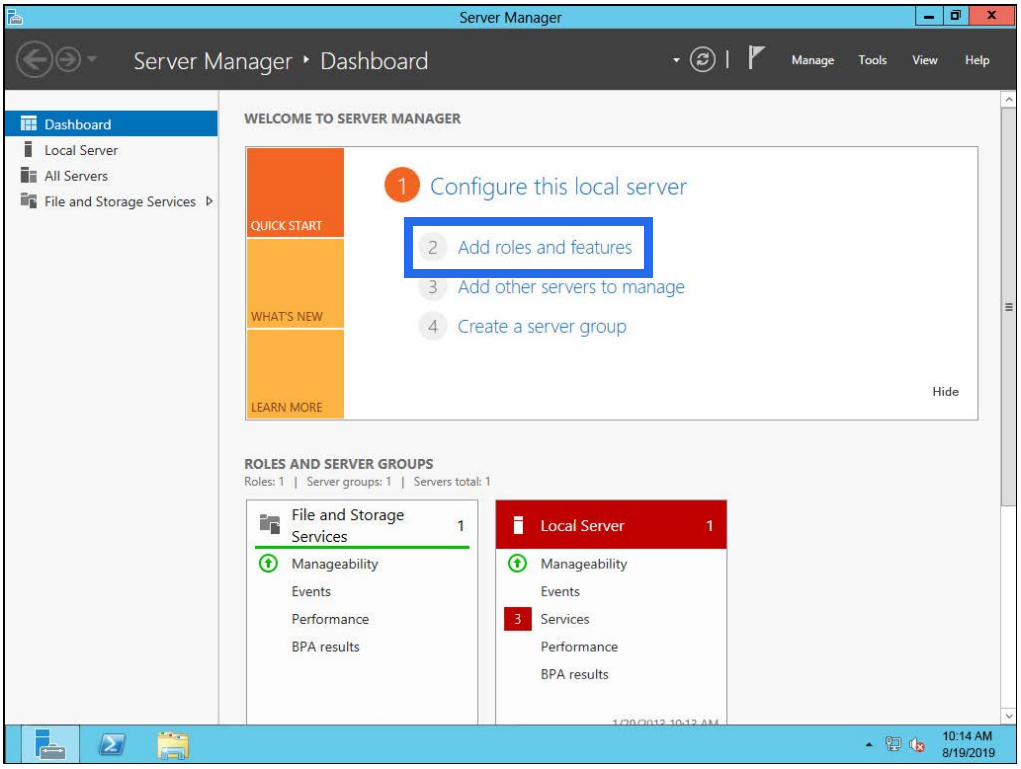
If your servers have Windows 2012 installed, use this section. If you are using Windows 2016 or 2019, go to page 165 instead.

Perform the following steps on **ALL** servers; Primary, Consolidated, 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 Primary and Secondary Servers.

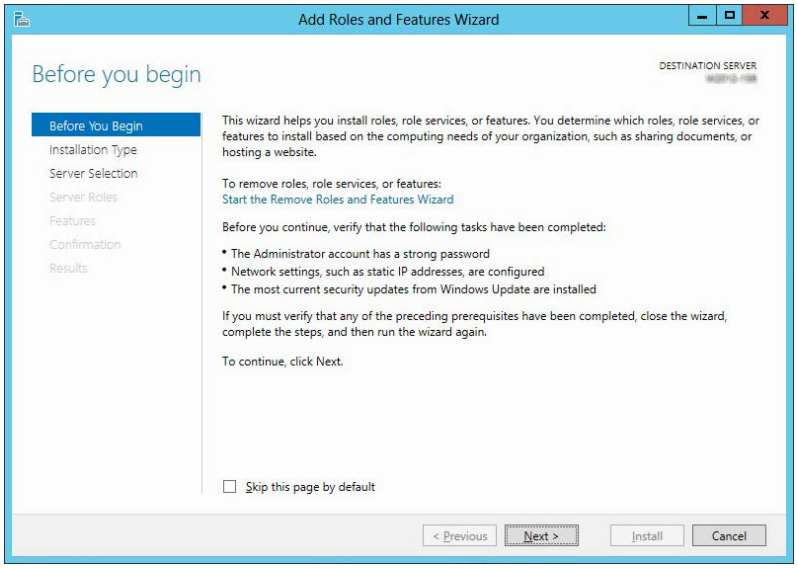
Note: Some of these steps may require additional files from the Windows disk or other storage location.

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

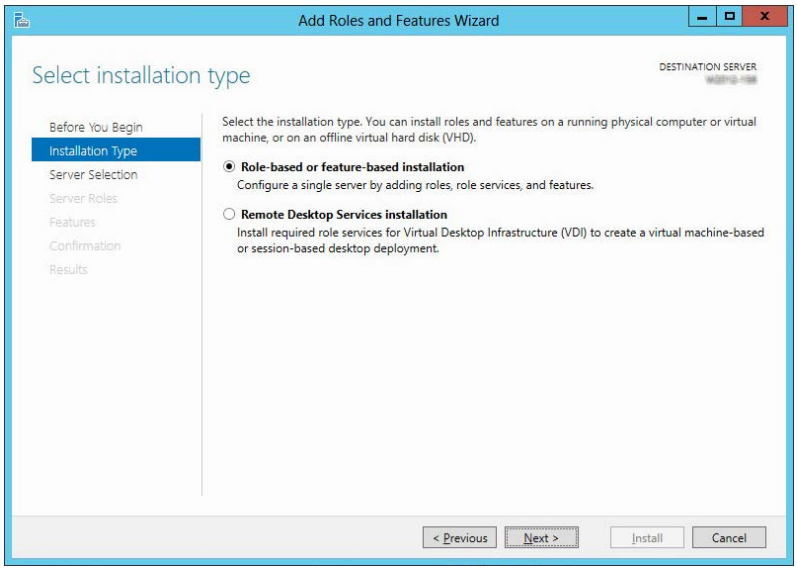


If this screen is hidden, go to **View** and select **Show Welcome Tile**.

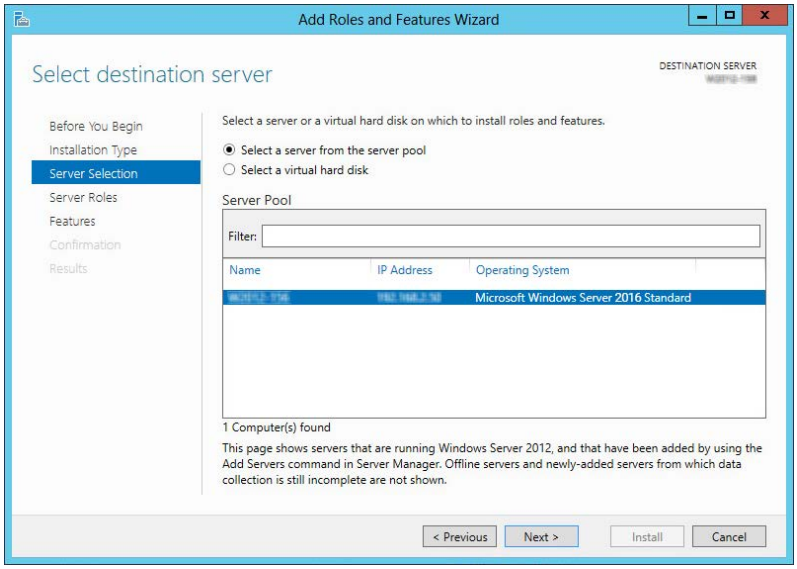
2. Click **Next**.



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

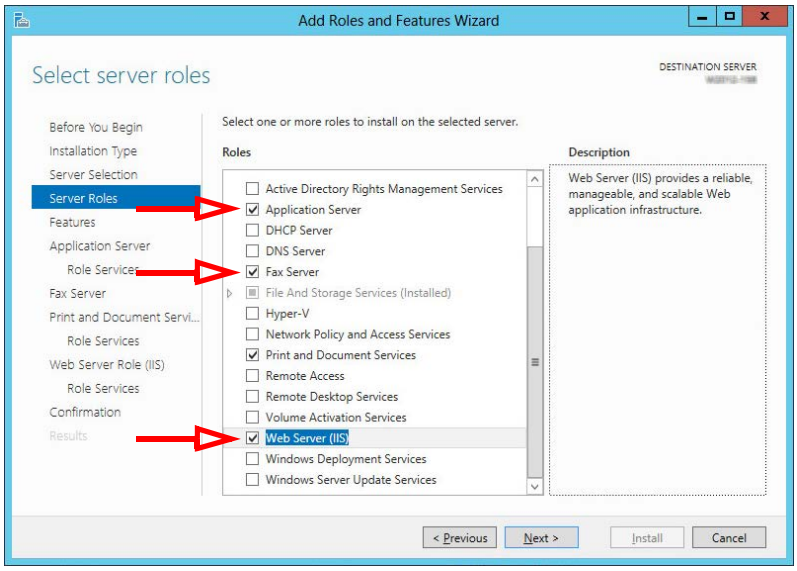


4. Leave the default settings as they are. Click **Next**.

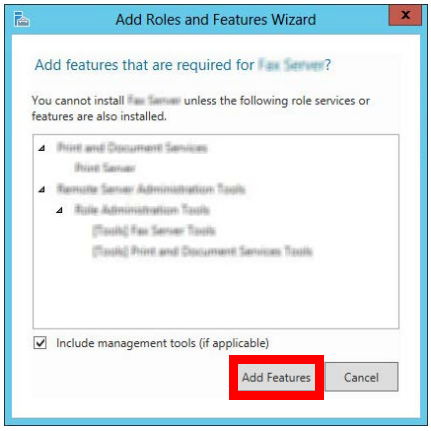


5. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes.

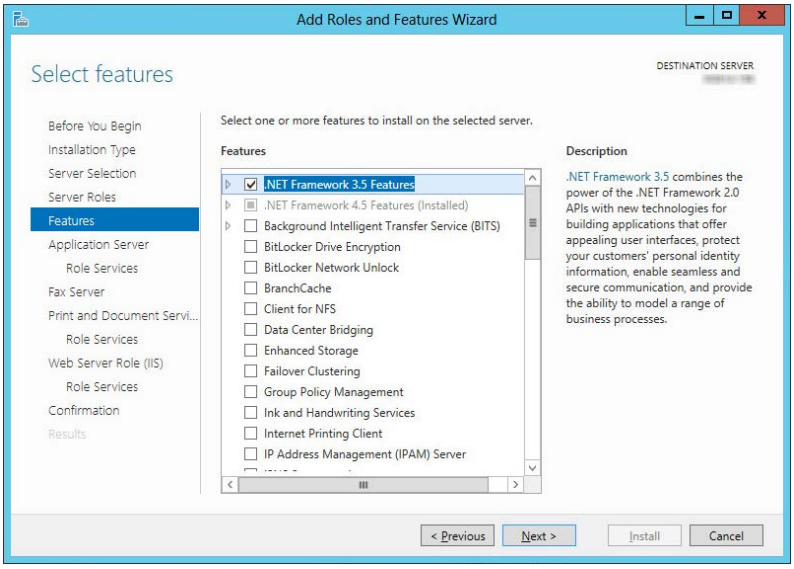
   Click **Next**.



Note: Throughout this installation, whenever you are prompted to confirm additions, always select **Add Features**.



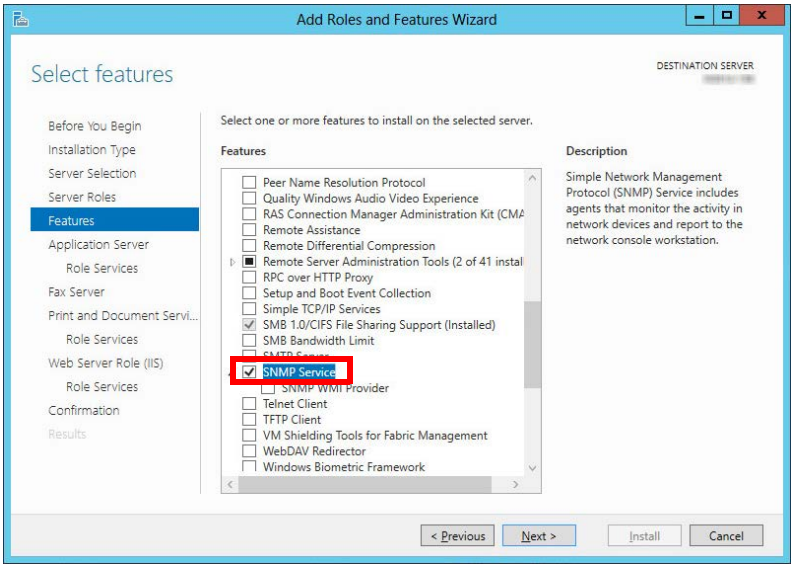
6. Enable the **.NET Framework 3.5 Features** checkbox. Click **Next**.



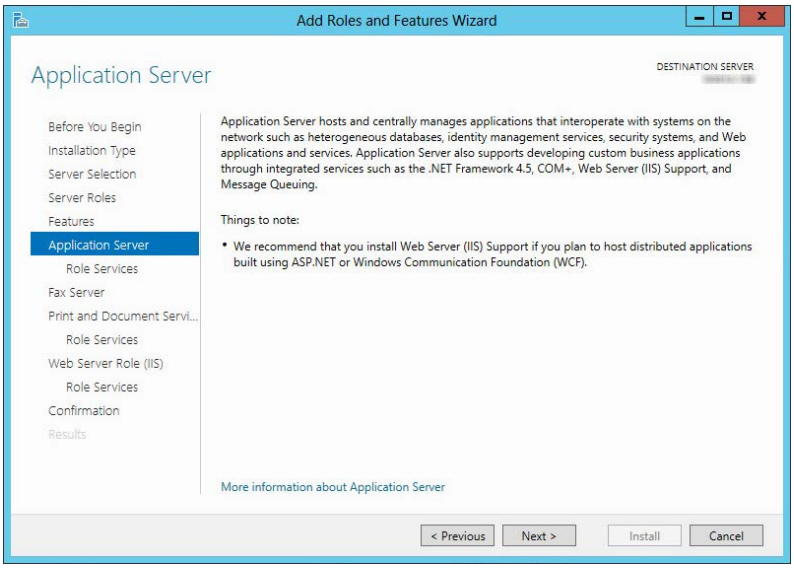
7. **Optional**: If you plan to use **SNMP Alarms** with Messaging, the **SNMP Service** must be added to Windows before the program can be installed.

   If SNMP Alarms are required, scroll down and enable SNMP Service.

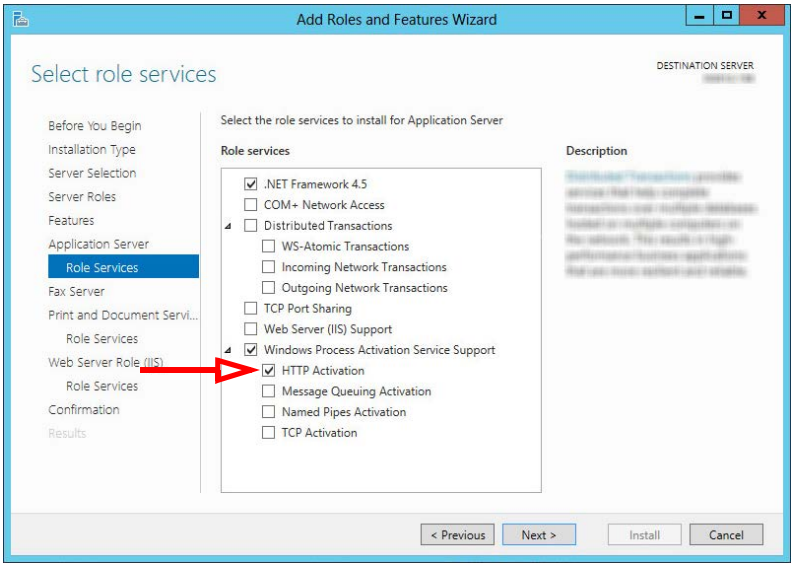
   If SNMP Alarms are not required, skip this step.



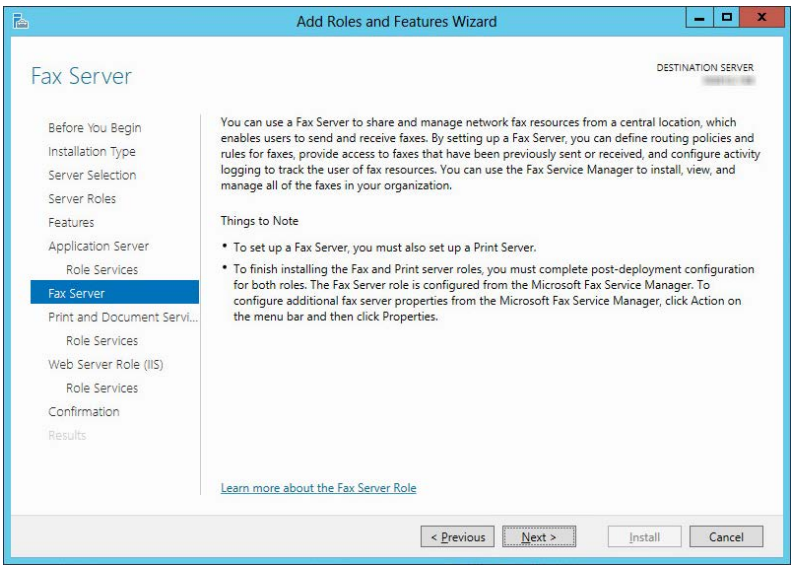
8. Review the information, then click **Next**.



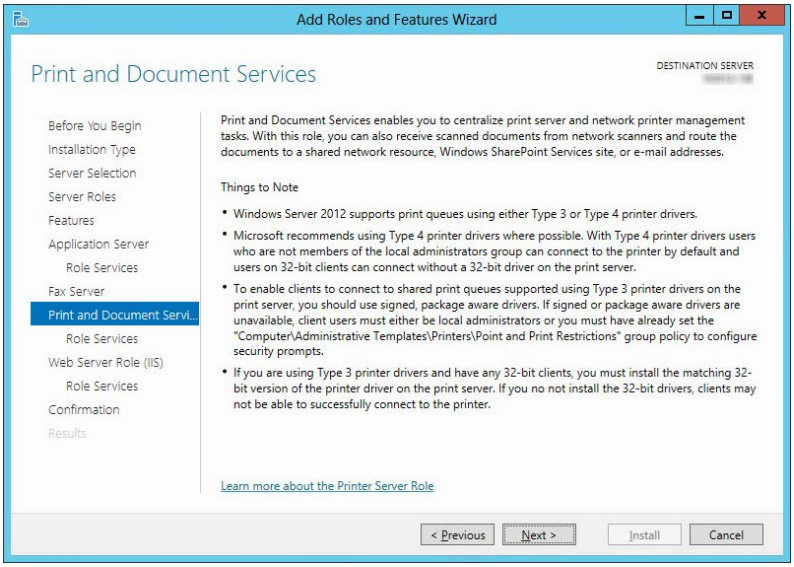
9. Ensure that **HTTP Activation**, under **Windows Process Activation Service Support** is enabled. Click **Next**.



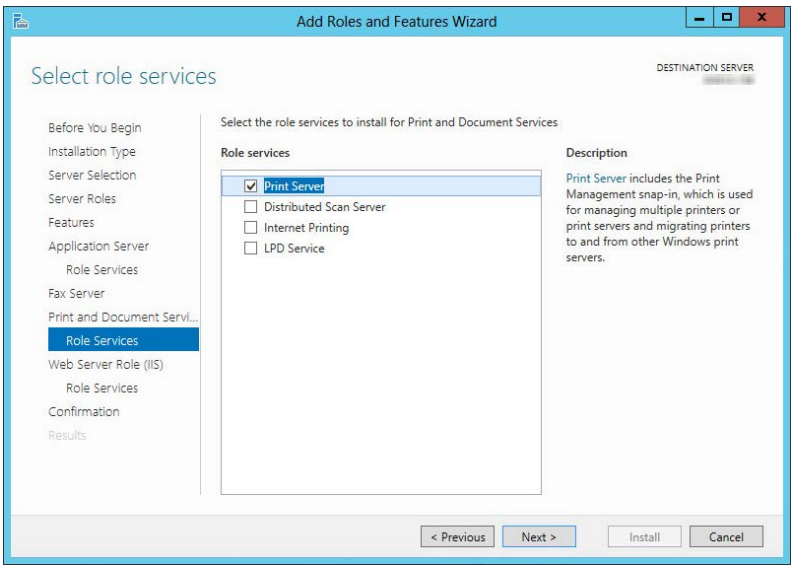
10. On the **Fax Server** screen, click **Next**.



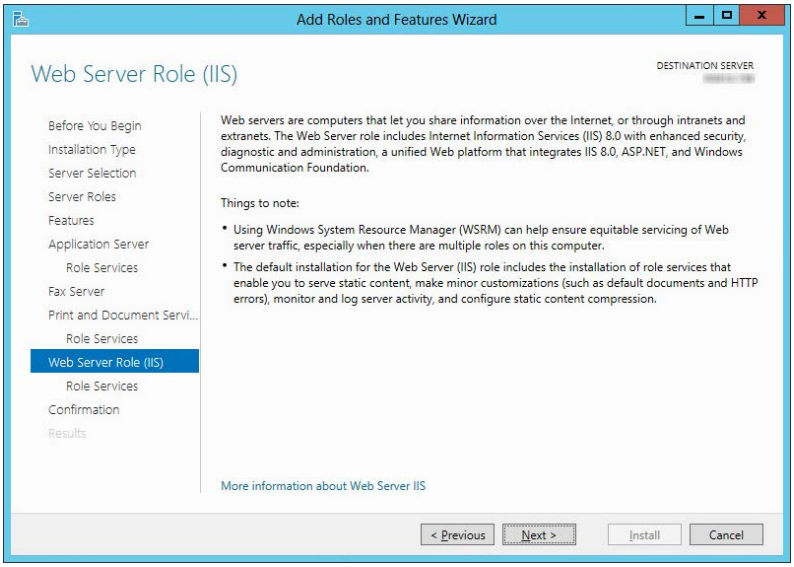
11. On the **Print and Document Services** screen, click **Next**.



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



13. On the **Web Server Role (IIS)** screen, click **Next**.



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

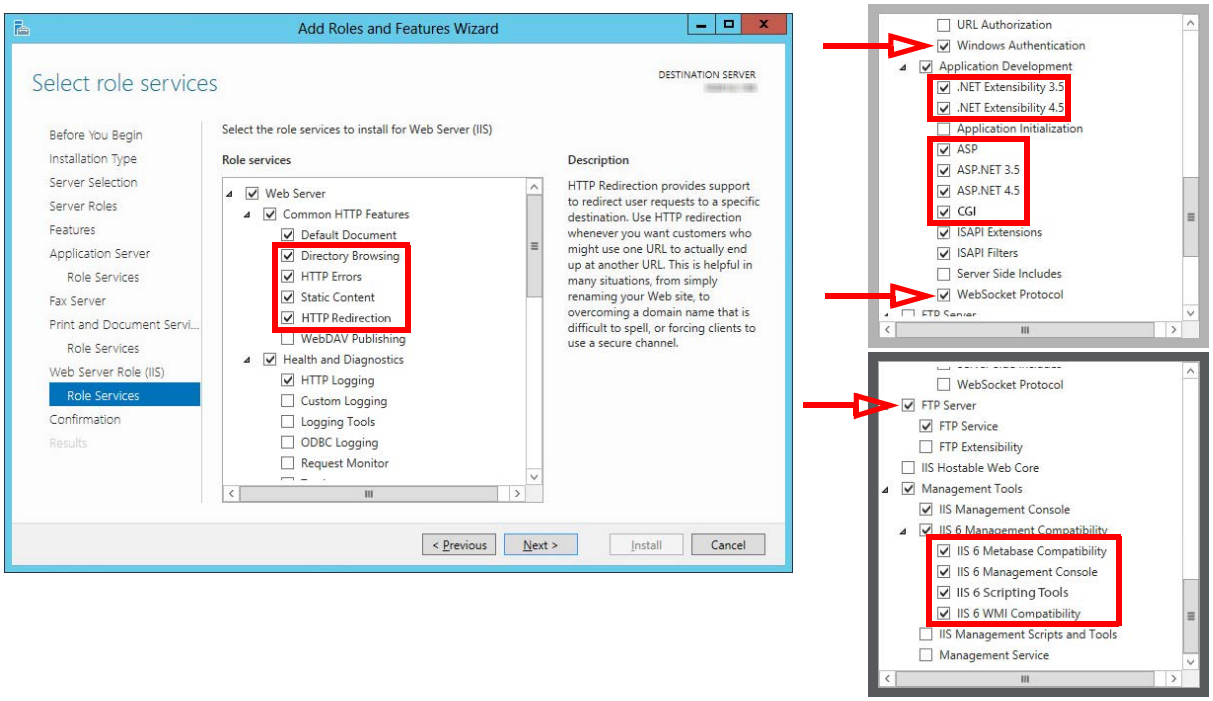
    Scroll down to **Security**, and enable **Windows Authentication**.

    Under **Application Development**, enable **.NET Extensibility 3.5**, **.NET Extensibility 4.5**, **ASP**, **ASP .NET 3.5**, **ASP .NET 4.5**, **CGI**, and **WebSocket Protocol**.

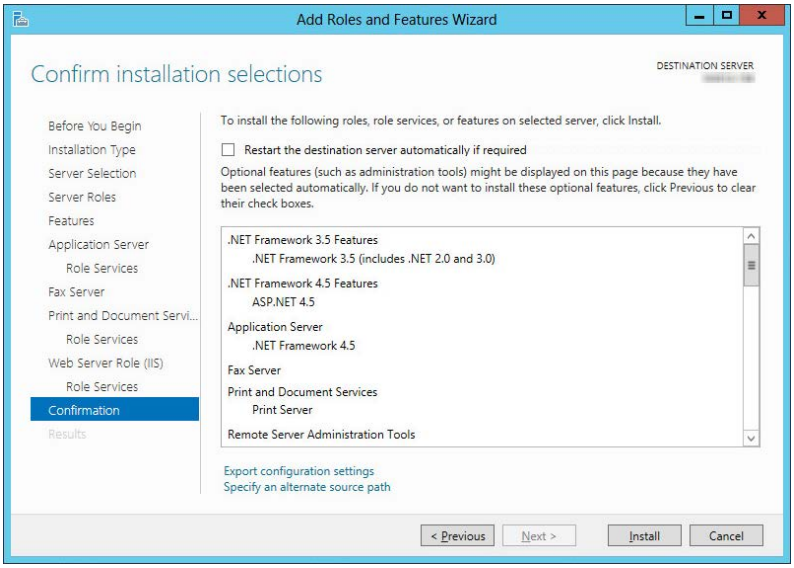
    Locate **FTP Server** and enable **FTP Service**.

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

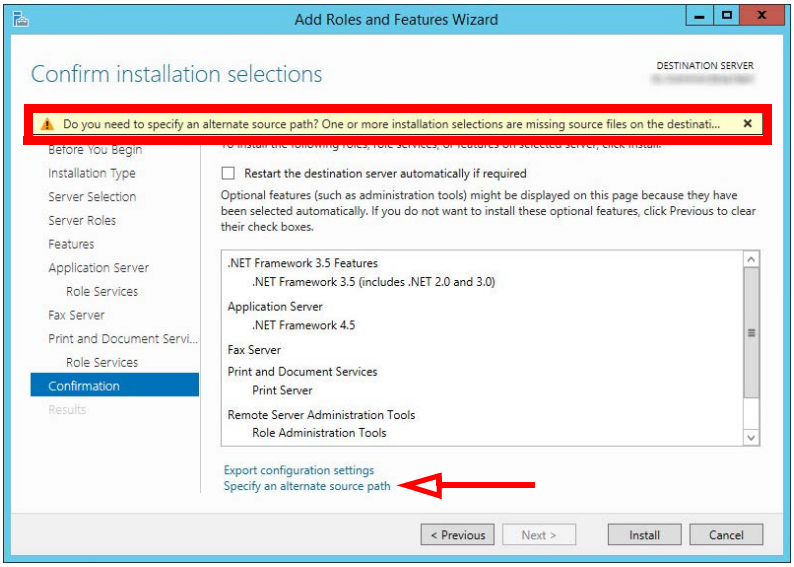
    Click **Next** when ready.



15. Review the selections here. When ready to proceed, click **Install**.

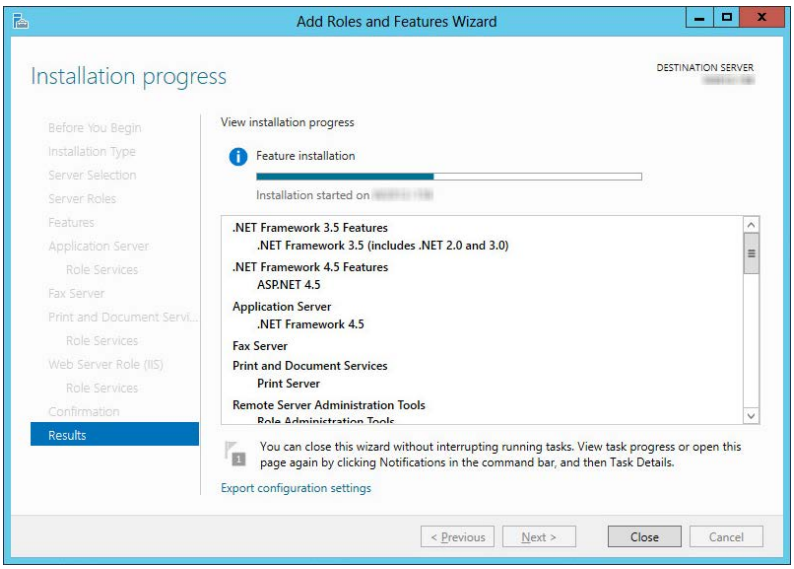


16. If prompted to provide the Windows disk to load the files, click **Specify an alternate source path** and direct it to the appropriate drive.



Hint: This is particularly important for virtual machine installations where there may not be a drive configured locally.

17. 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

18. Once all changes are complete, **Restart 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:

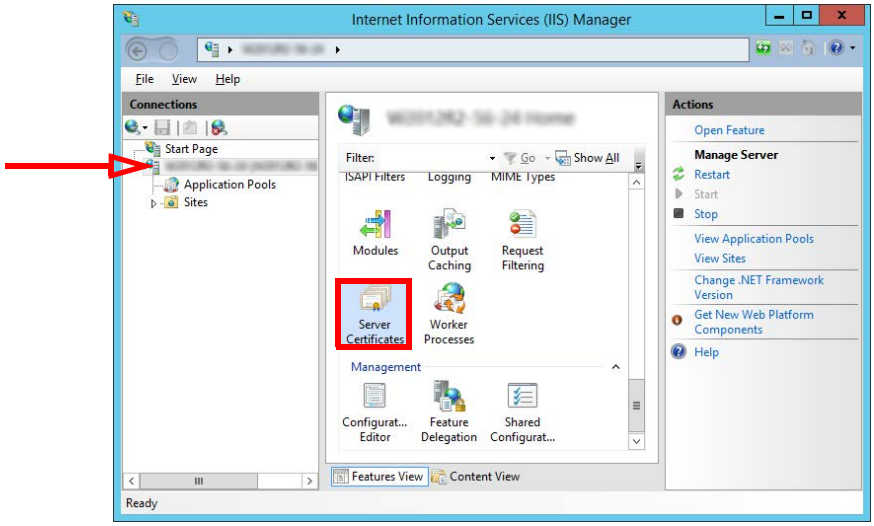
https://technet.microsoft.com/en-ca/library/cc753127(v=ws.10).aspx

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

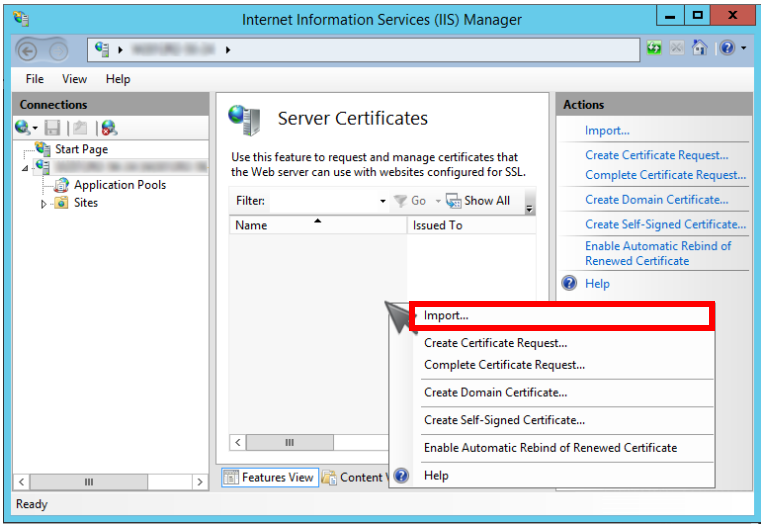
IIS Certificate Bindings

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

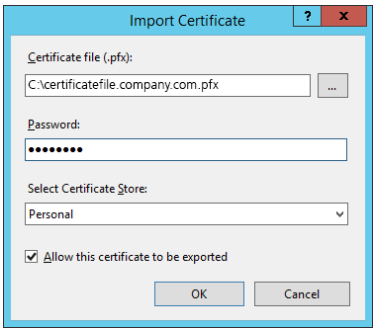
1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.



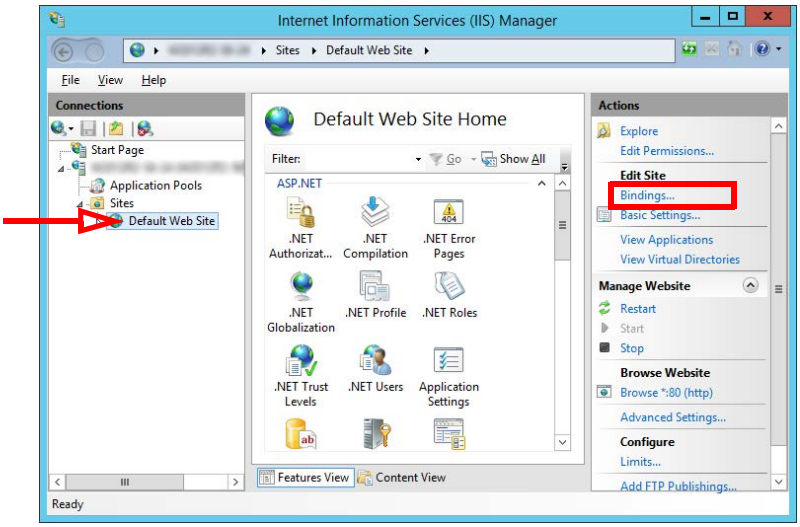
2. Right-click in the right-hand pane and choose Import from the pop-up menu.



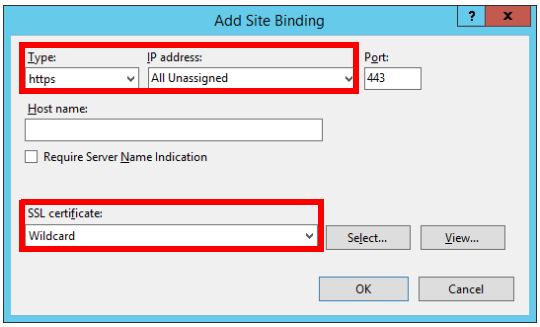
3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.



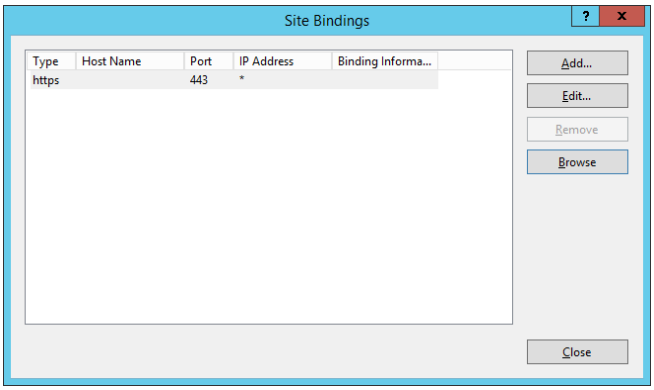
4. Go to **Sites > Default Web Site**.
Click **Bindings...**.



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**.



Install Microsoft .Net Framework 4.7.2

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

Avaya IX Messaging requires Microsoft .Net Framework version 4.7.2 to be installed to support various features within the program. If it has not already been installed, the administrator must download it and install it manually.

Note: .Net Framework 4.7.2 is not installed by default. It may be part of Windows updates, optional updates, or not provided at all. Follow these instruction is it is not installed on your system, or if you do not know if it has been installed.

1. Open a web browser and go to the Microsoft web site. Search for .Net Framework 4.7.2 and install the application on the server. For example:
   https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows .
2. Download the file to your server drive. When ready, run the program to install this feature.
3. When finished, restart the server.

Primary Voice Server

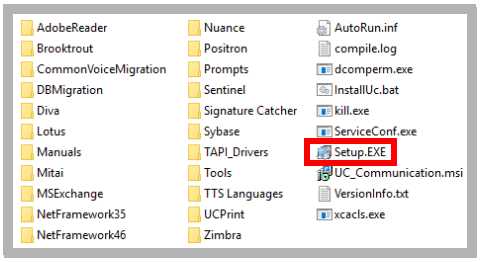
Important: The Primary Server **MUST** be the first server to be setup since the Primary holds the license for your site. The Consolidated Server should be next, and only when the database has synchronized between them should the Secondary Servers be installed. See Verifying File Sync on page 254.

Installation

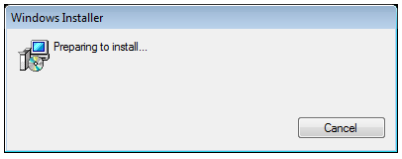
Important: In an HA installation, **all servers** must have the **same time zone** set under Windows Date / Time settings. If the servers are configured for different time zones, the timestamps will not play correctly.

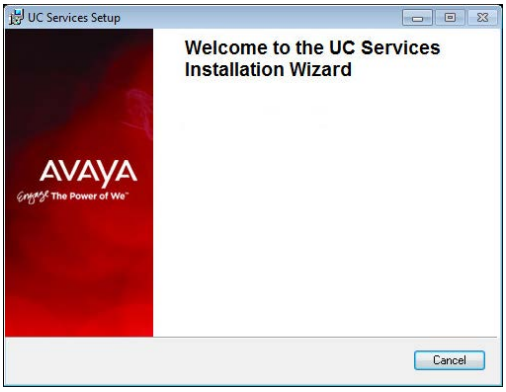
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update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

1. Download the installation file from (see chapter 4). 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 IX Messaging onto the Primary server.





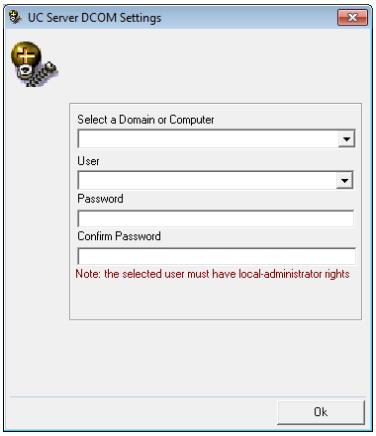
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging.

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.



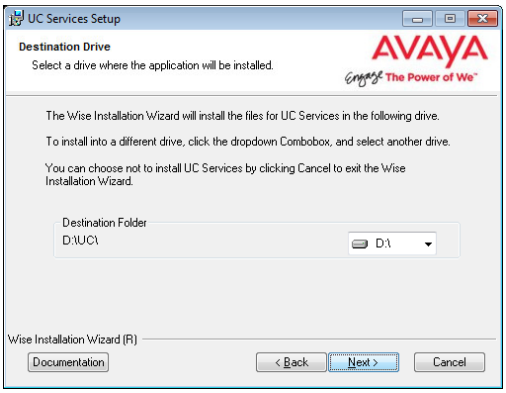
Hint: Wherever possible, this password should be setup with no expiration date. If the password does expire, then it must be changed on every computer that uses it. Many services will be unavailable until the change has been made everywhere.

5. Review all the license agreements, click **Continue**.
   When ready, 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.

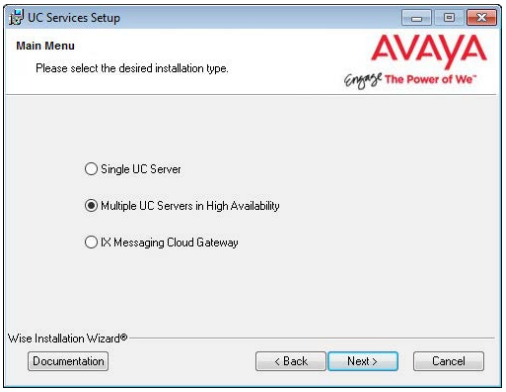
7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

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

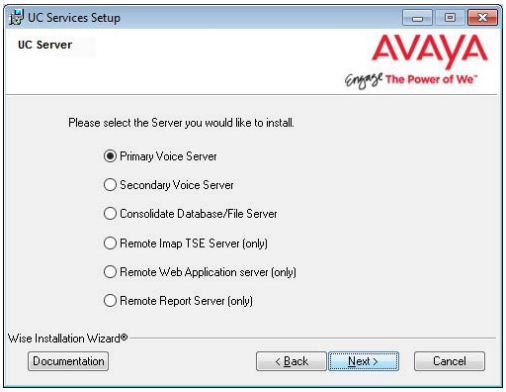
   Multiple UC Servers in High Availability: When running Messaging in High Availability mode for redundancy.

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, Install and Configure Cloud Gateway for complete details.

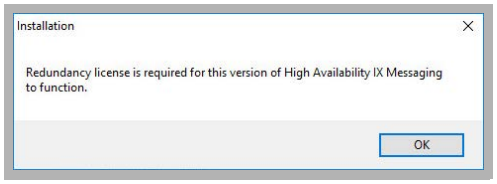


8. Select **Primary Voice Server**.

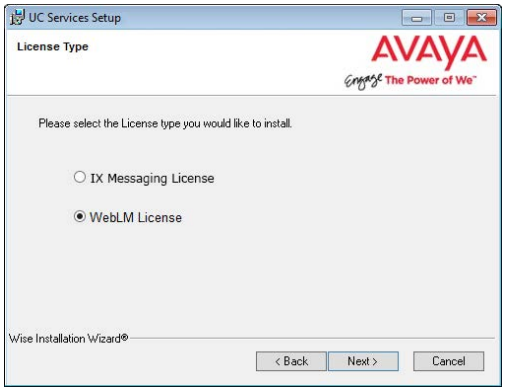
   Click **Next**.



9. This screen is a reminder that HA installations require an HA license. Click **OK**.



10. Select the license type you will using for this installation. Most sites will use the WebLM License option.

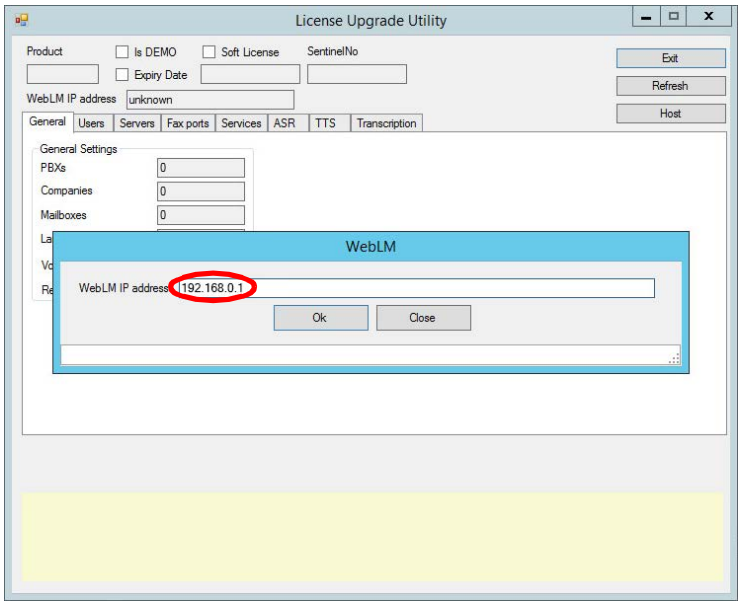


Note: If you select Messaging, go to **chapter 13, Installing the Messaging License**. When finished, return here and continue the installation from **step 13**. Skip step 11 through 12.

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.

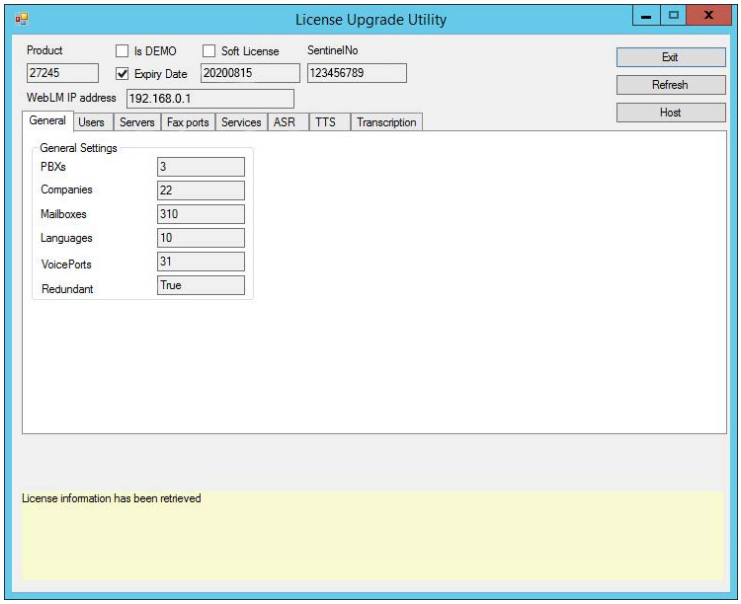
11. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

    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 437.

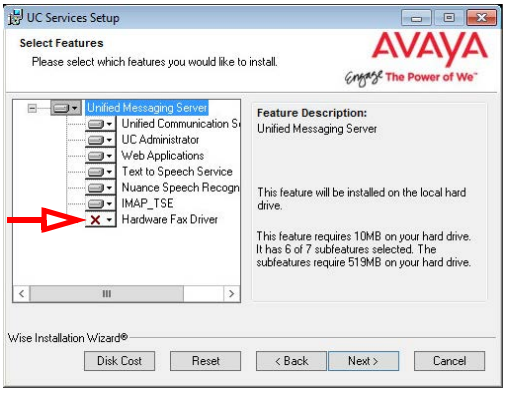
12. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.



Note: The number of voice ports is calculated based upon your license.
[(# Basic users + # Mainstream users) / 40] + Number of voice ports in license

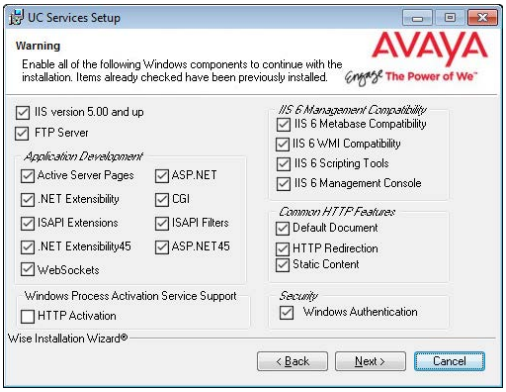
13. Select the **Components** required at your site.

    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.

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



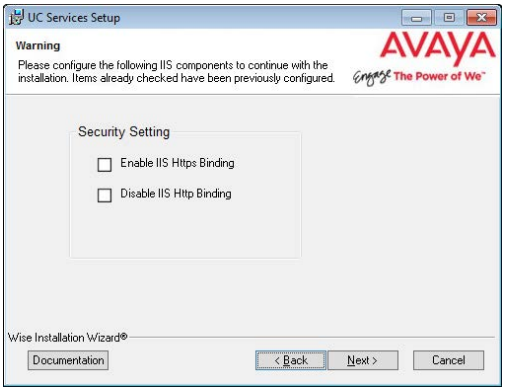
Note: This screen will only appear if one or more required components are **not** installed on the computer.

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 Messaging requires to operate properly.



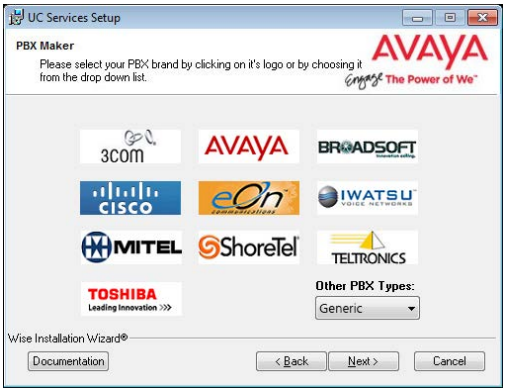
Note: This screen will only appear if one or more of the required settings has not been made on the computer.

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.

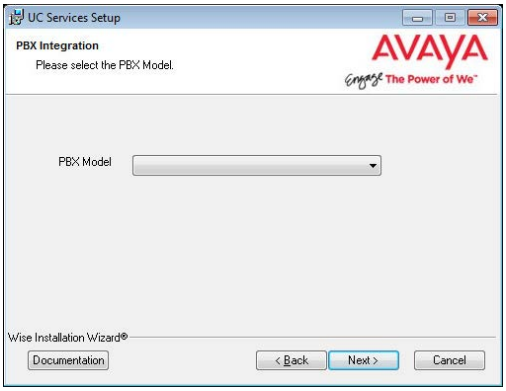
Note: The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

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



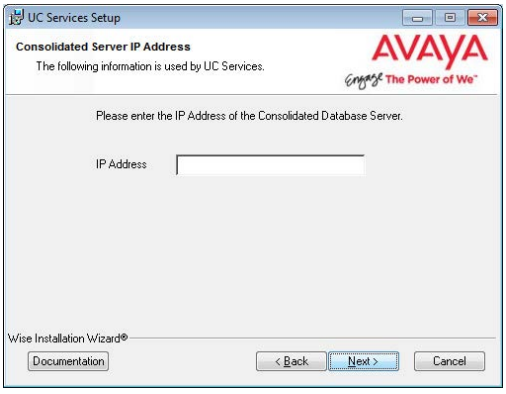
17. Select your PBX model from the dropdown menu.

    Click **Next**.



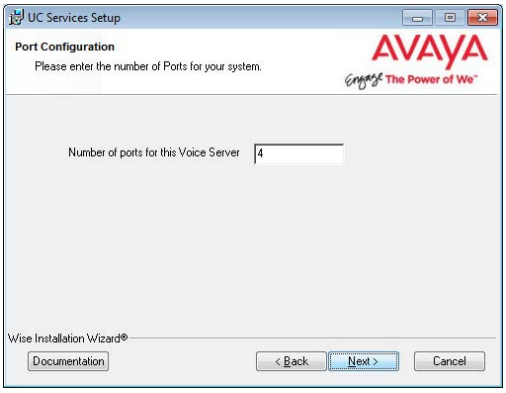
18. Enter the **IP Address** for the Consolidated Server.

    Click **Next**.



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

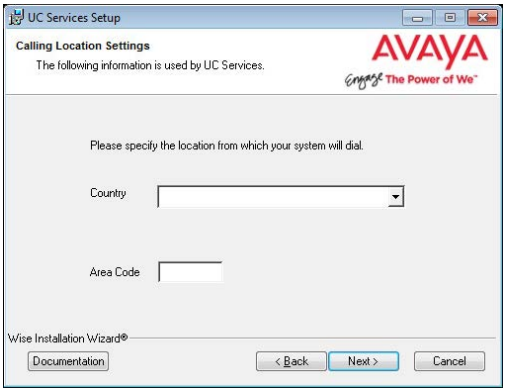
    Click **Next**.



20. 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.

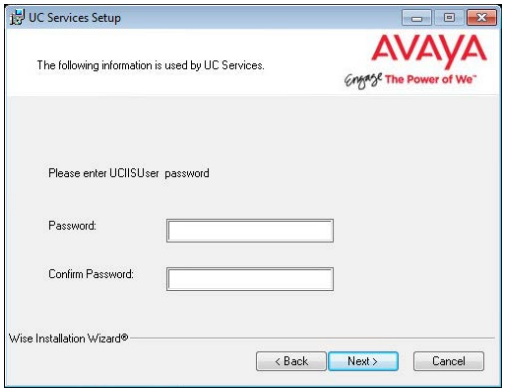
    Select the country from the dropdown menu, and enter the area code in the space provided.

    Click **Next** to continue.



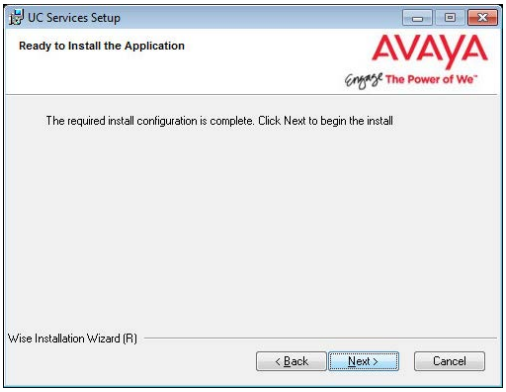
Note: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

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

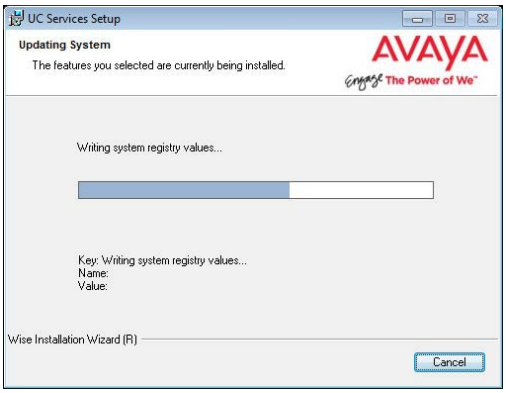


22. The preliminary information required for installation is now complete.

    Click **Next**.

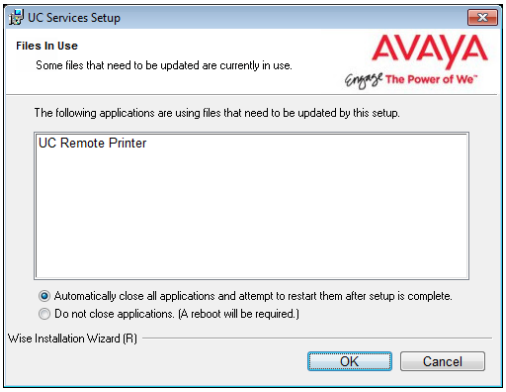


23. The selected components will now be installed. This process may take a while.



24. 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.

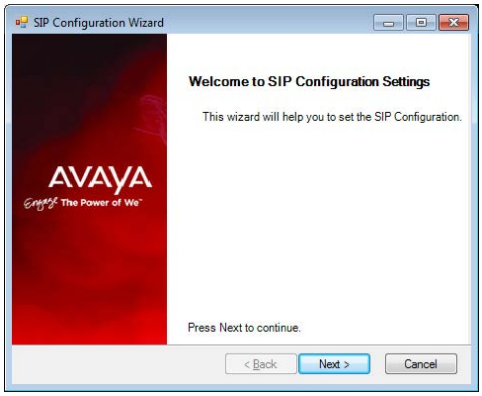
    Click **OK** when ready.



25. 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.

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

    Click **Next** to continue.

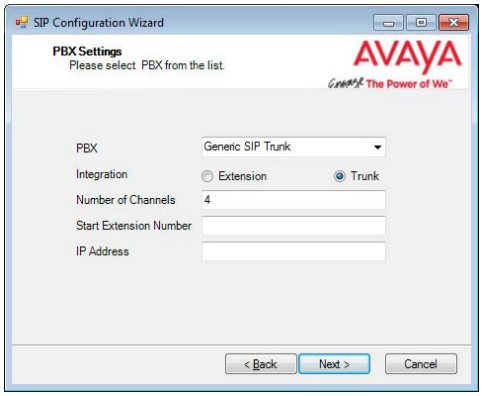


27. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.

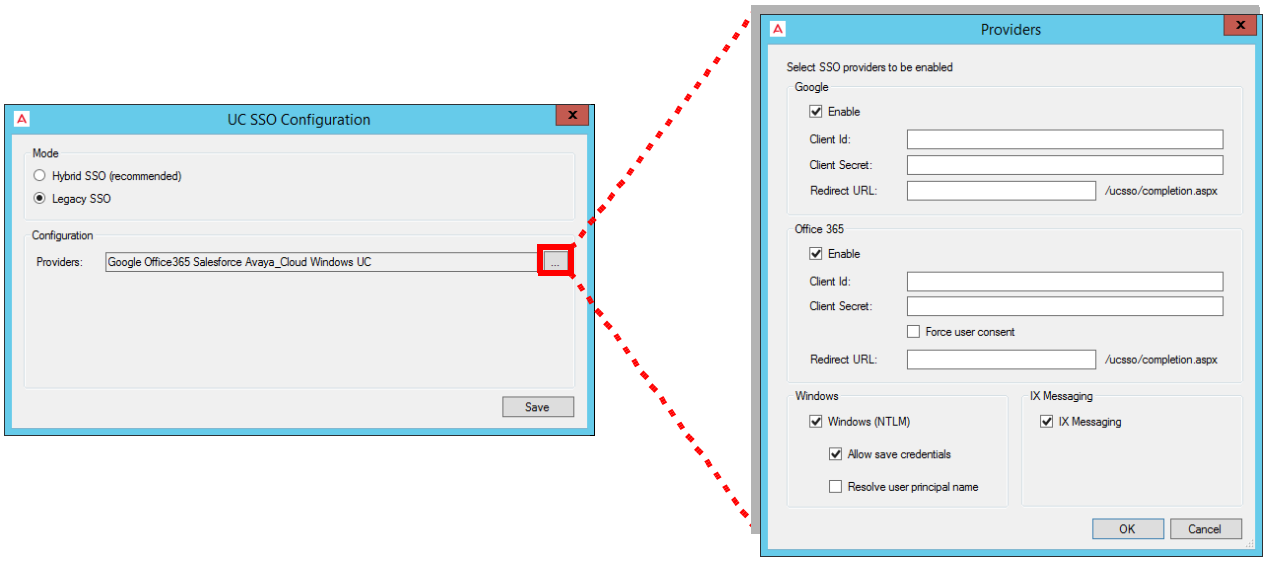


28. Confirm the information then click **Finish**.

> **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 Messaging programs folder after installation.

29. 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 as required.

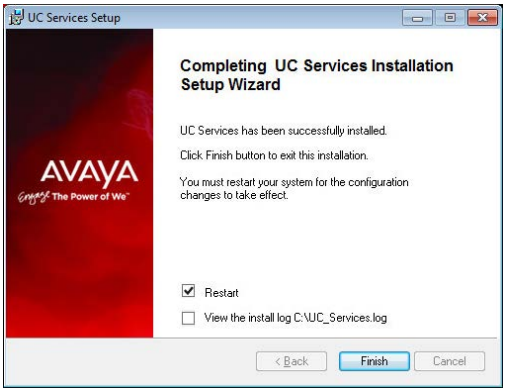
30. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



Note: For more information on the SSO Options, see chapter 25 on page 651: Single Sign-On (SSO).

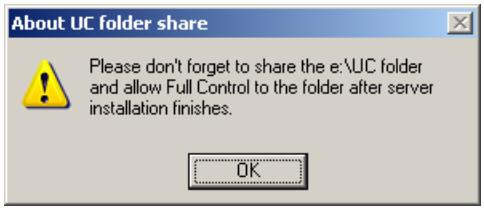
31. Click **Finish** to restart the server.

    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 256 for details).

    Click **OK** to restart the computer.



Warning: Once all of the HA servers (Primary, Consolidated, and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Primary 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

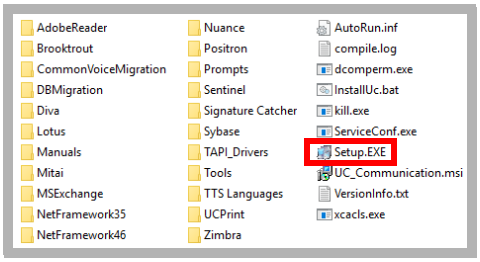
Important: The Primary Server **MUST** be the first server to be setup since the Primary holds the license for your site. The Consolidated Server should be next, and only when the database has synchronized between them should the Secondary Servers be installed. See Verifying File Sync on page 254.

Installation

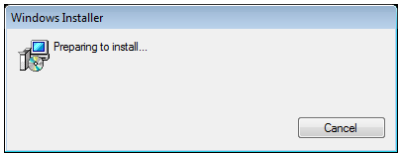
Important: In an HA installation, **all servers** must have the **same time zone** set under Windows Date / Time settings. If the servers are configured for different time zones, the timestamps will not play correctly.

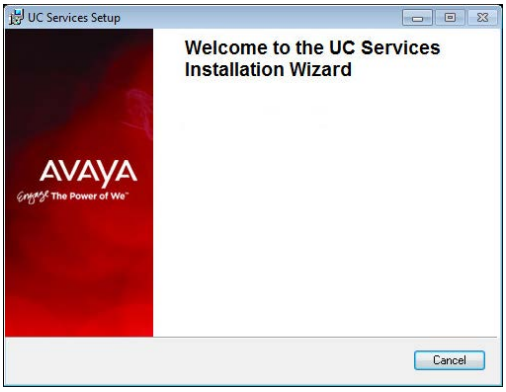
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update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

1. Download the installation file (see chapter 4). 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 IX Messaging onto your Consolidated server.





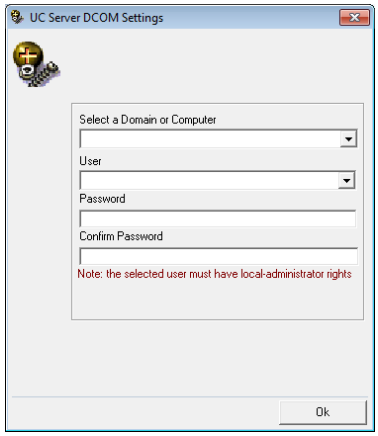
3. Once the Windows components have been verified, click **Next** to begin the installation procedure.

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 Messaging.

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.



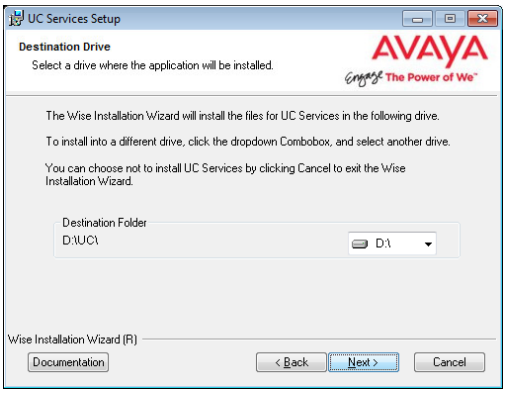
Hint: Wherever possible, this password should be setup with no expiration date. If the password does expire, then it must be changed on every computer that uses it. Many services will be unavailable until the change has been made everywhere.

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.

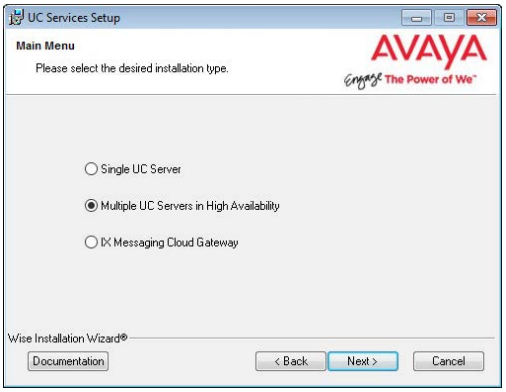
7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

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

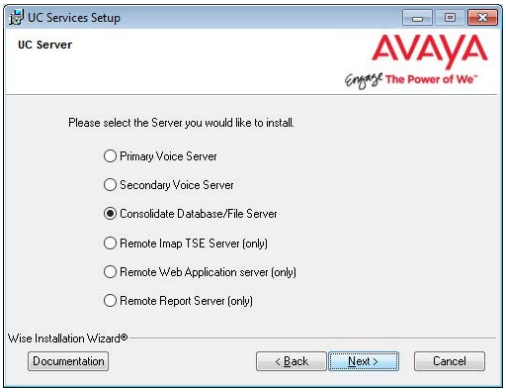
   Multiple UC Servers in High Availability: When running Messaging in High Availability mode for redundancy.

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, Install and Configure Cloud Gateway for complete details.

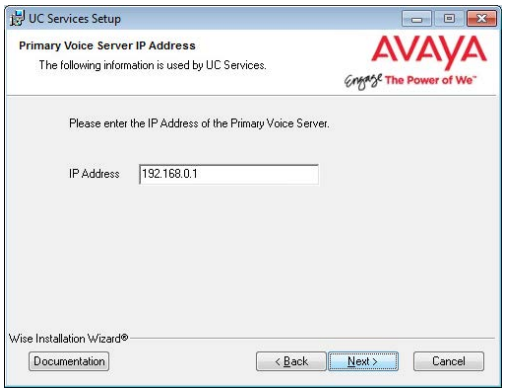


8. Select **Consolidated Database/File Server**.

   Click **Next**.

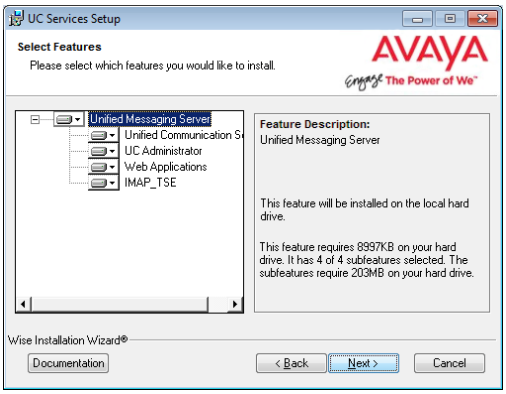


9. Enter the IP Address of the Primary Server, then click **Next**.

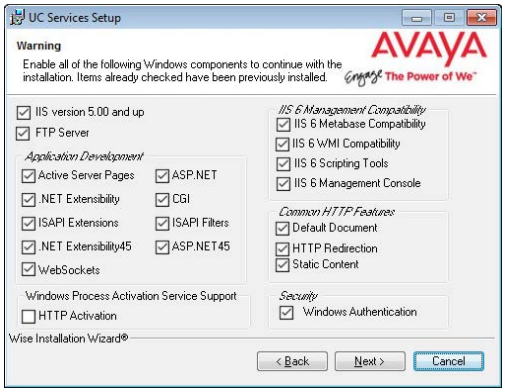


10. Select the **Components** required at your site.

    Click **Next**.



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



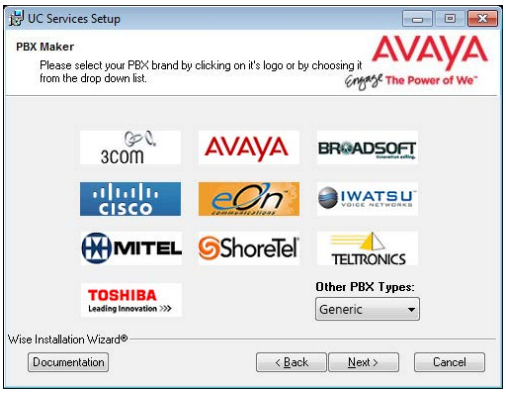
Note: This screen will only appear if one or more required components are not installed on the server.

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.

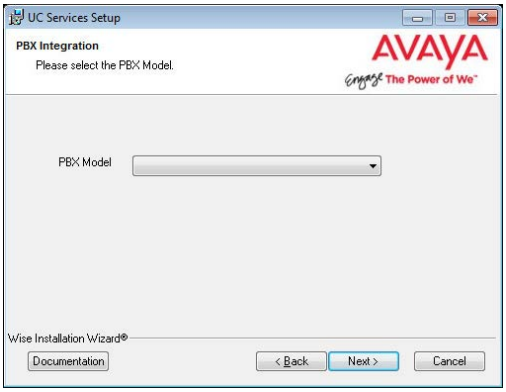
Note: The installation will not continue until all of the required components have been added to the server.
The screen does not refresh until you click **Next**.

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

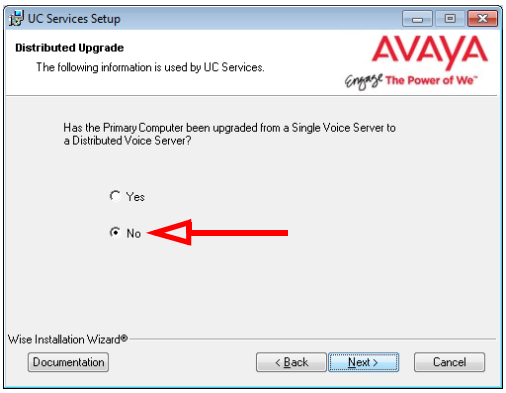


13. Select your PBX model from the dropdown menu.

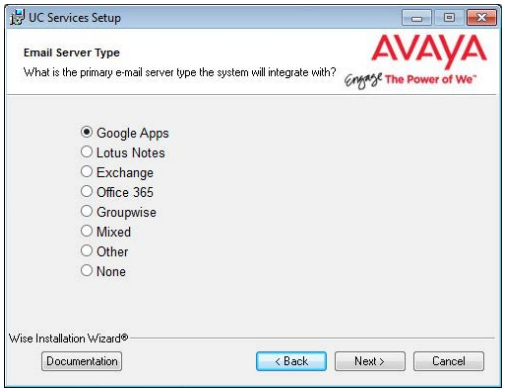
Click **Next**.



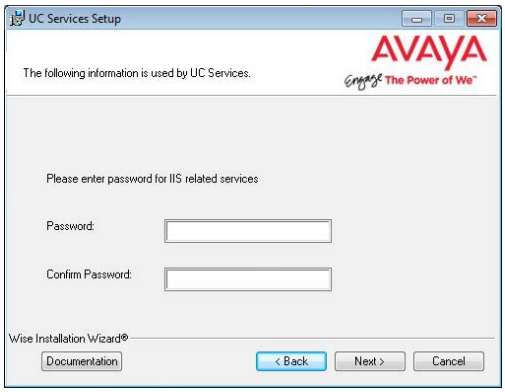
14. Unless the Primary Server has been upgraded from a Single Server installation, choose **No**.
Click **Next**.



15. 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.

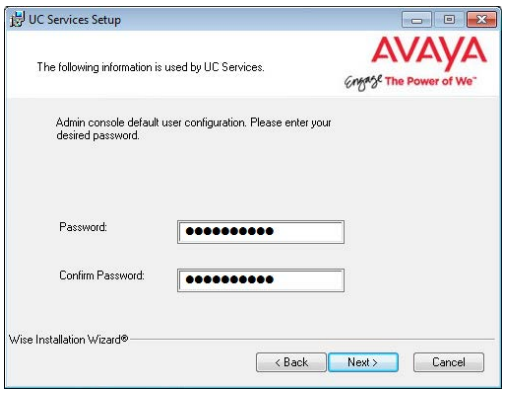


16. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.



17. 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.



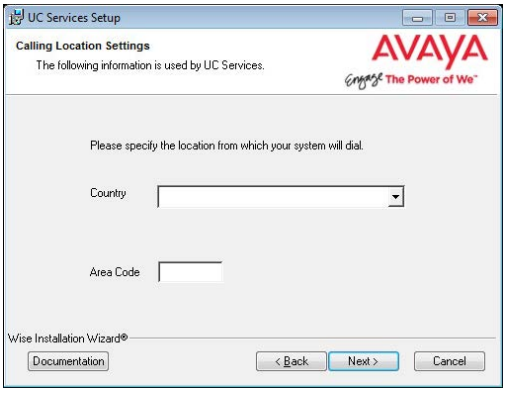
Warning: Once all of the HA servers (Consolidated, Primary and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Primary or Secondary servers before the synch is complete will corrupt the database preventing all logins on all servers.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

18. 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.

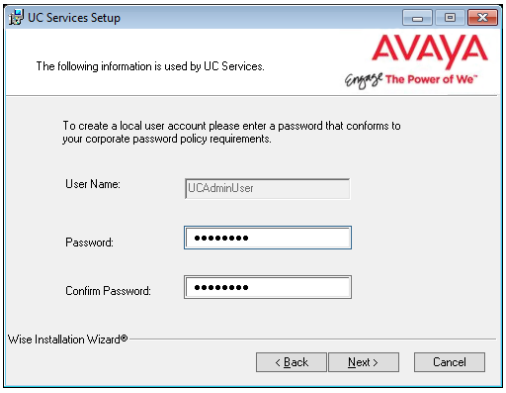
    Click **Next** to continue.

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.

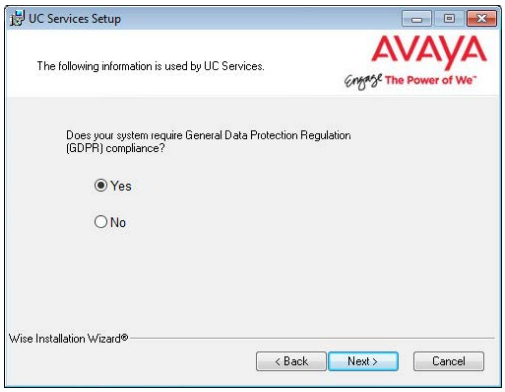


19. Create a new user administrator account on the local computer. Type and confirm a password for the new account.

    Click **Next** to continue.

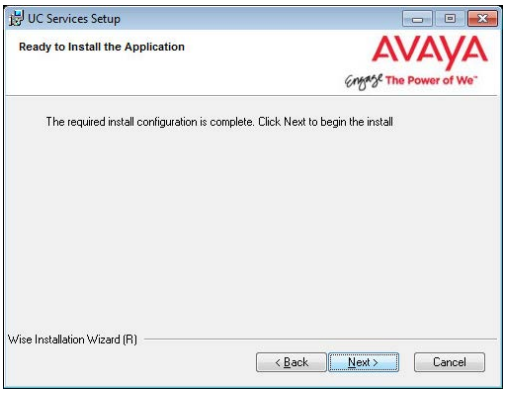


20. Choose either **Yes** or **No** to determine whether the system will apply General Data Protection Regulation (GDPR) compliance procedures to your data.
    With this option enabled, users and callers are notified that personal information will be collected. This information can also be completely removed from the system upon request.

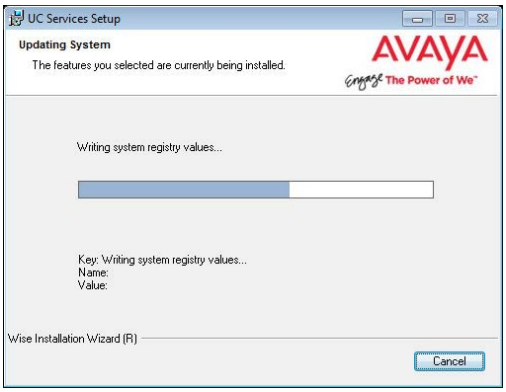


21. The preliminary information required for installation is now complete.

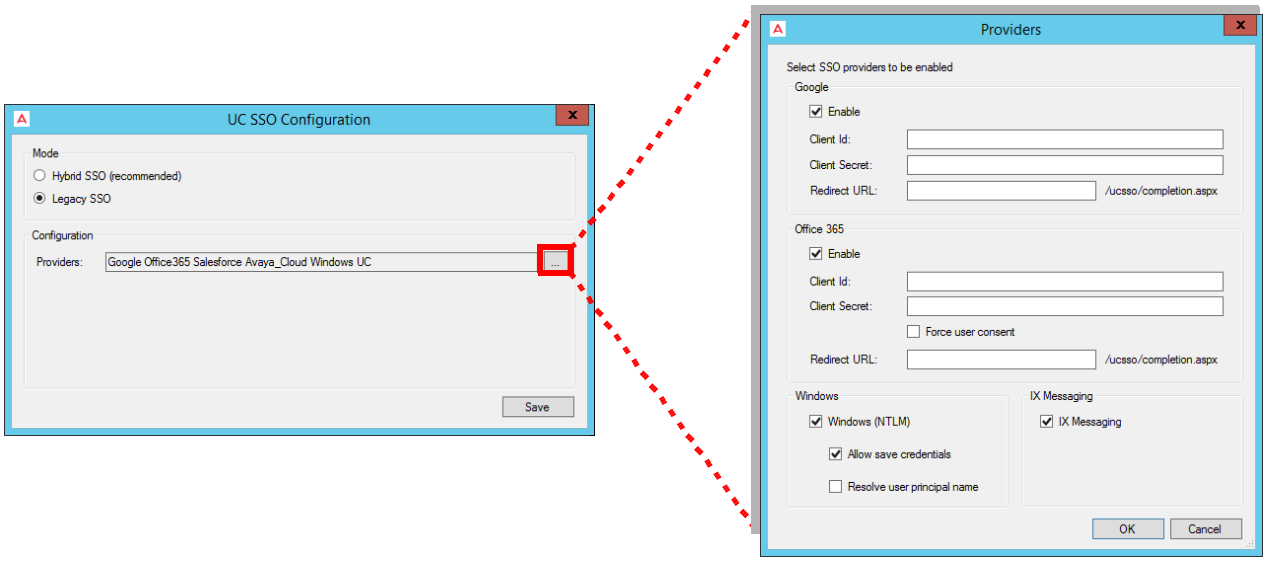
    Click **Next**.



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



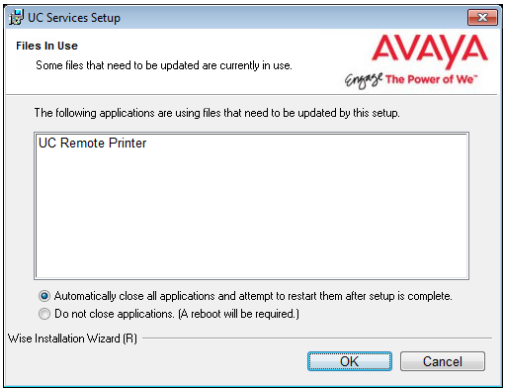
23. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



Note: For more information on the SSO Options, see chapter 25 on page 651: Single Sign-On (SSO).

24. 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.

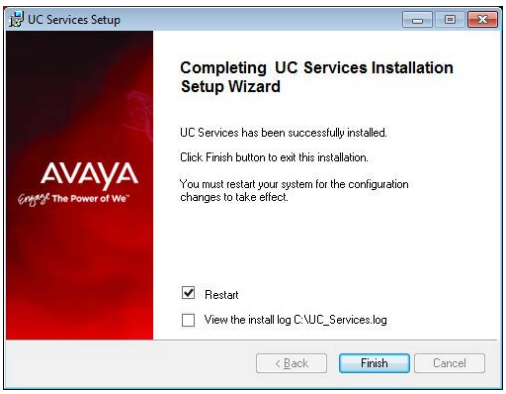
    Click **OK** when ready.



25. 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.

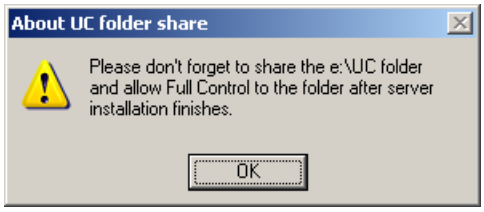
26. Click **Finish** to restart the server.

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



27. This alert is to remind you to properly share the UC installation folder (see for page 256 details).

    Click **OK** to restart the computer.



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

Secondary Voice Server

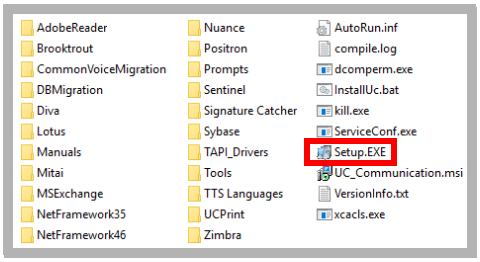
Important: The Primary Server **MUST** be the first server to be setup since the Primary holds the license for your site. The Consolidated Server should be next, and only when the database has synchronized between them should the Secondary Servers be installed. See Verifying File Sync on page 254.

Installation

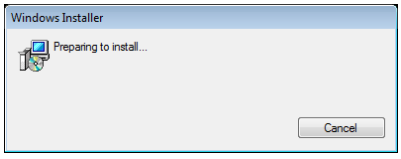
Important: In an HA installation, **all servers** must have the **same time zone** set under Windows Date / Time settings. If the servers are configured for different time zones, the timestamps will not play correctly.

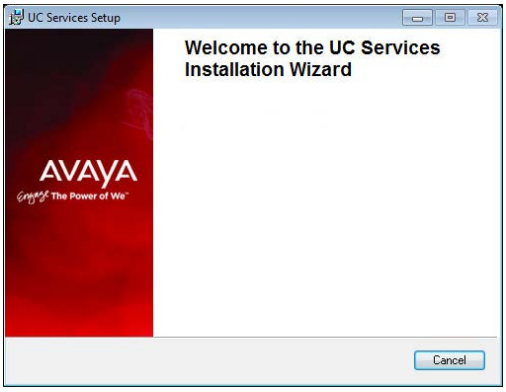
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update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

1. Download the installation file (see chapter 4). 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 IX Messaging onto all of your Secondary servers.





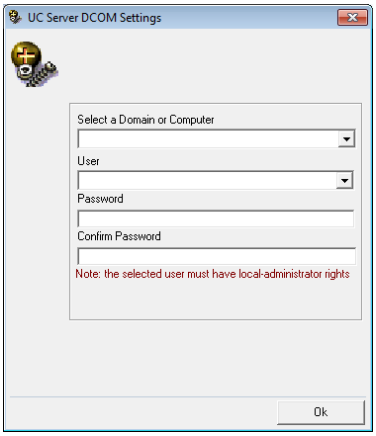
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging.

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.



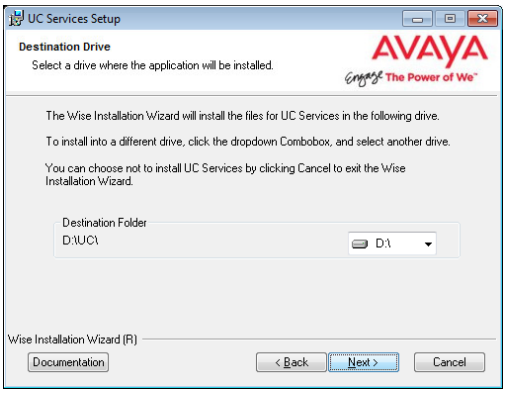
Hint: Wherever possible, this password should be setup with no expiration date. If the password does expire, then it must be changed on every computer that uses it. Many services will be unavailable until the change has been made everywhere.

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.

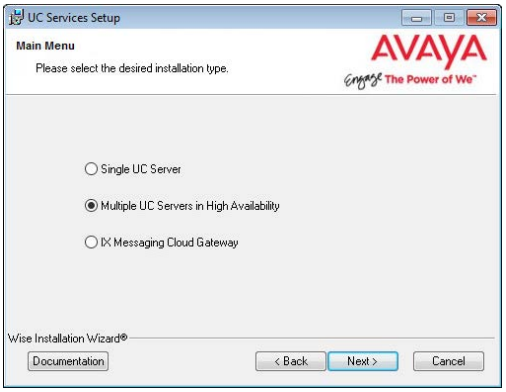
7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

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

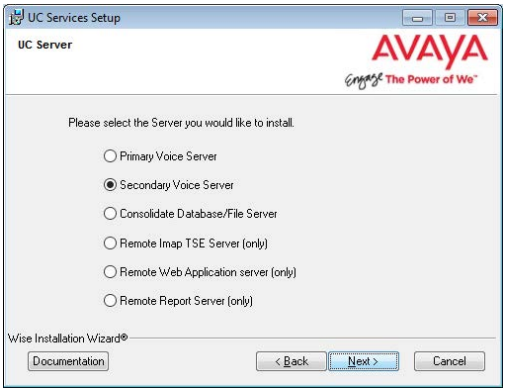
   Multiple UC Servers in High Availability: When running Messaging in High Availability mode for redundancy.

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, Install and Configure Cloud Gateway for complete details.



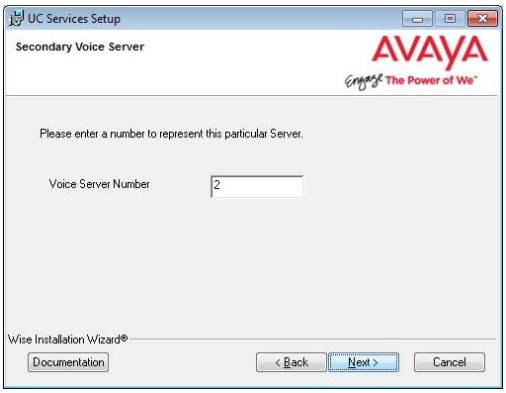
8. Select **Secondary Voice Server**.

   Click **Next**.



9. Enter the number for this Secondary Server. Each Secondary server must have a unique identifying number assigned **between 2 and 20**.

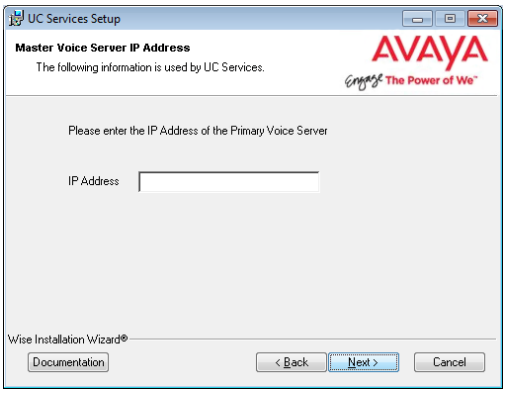
   Click **Next**.



> **Note**: The Primary Server is automatically assigned # 1.

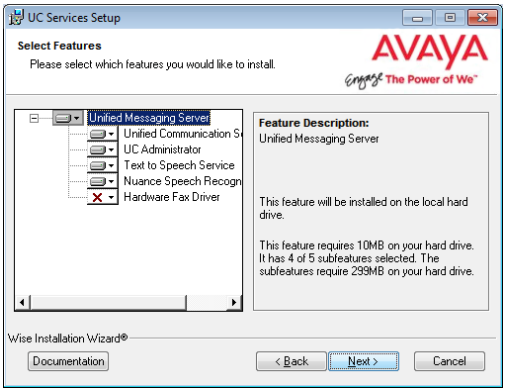
10. Enter the **IP Address** of the Primary Voice Server.

    Click **Next**.



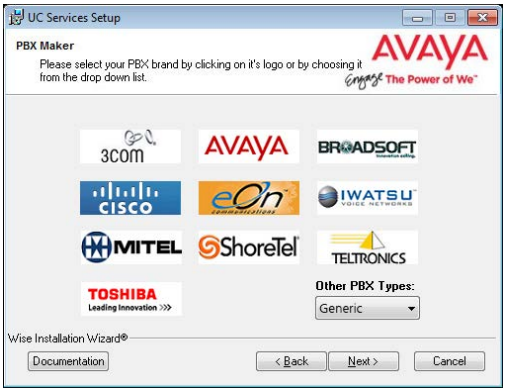
11. Select the **Components** required at your site.

    Click **Next**.



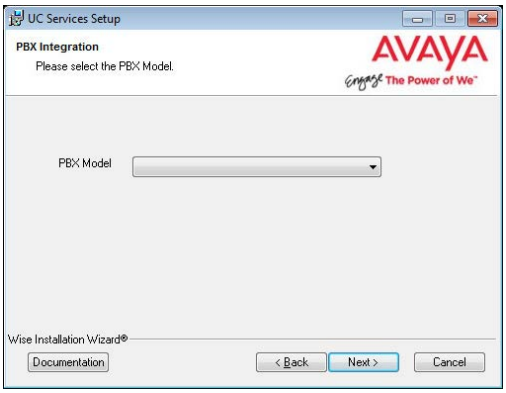
Note: If the Dialogic SR140 fax software will be used with this installation, ensure that the Hardware Fax Driver option is enabled here.

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



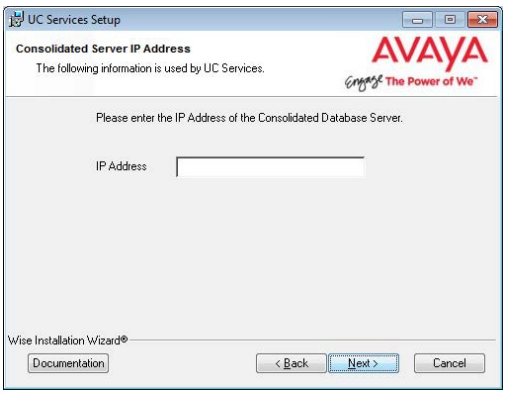
13. Select your PBX model from the dropdown menu.

    Click **Next**.



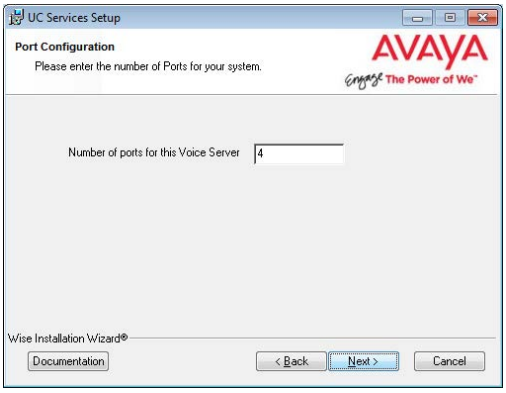
14. Enter the **IP Address** for the Consolidated Server.

    Click **Next**.

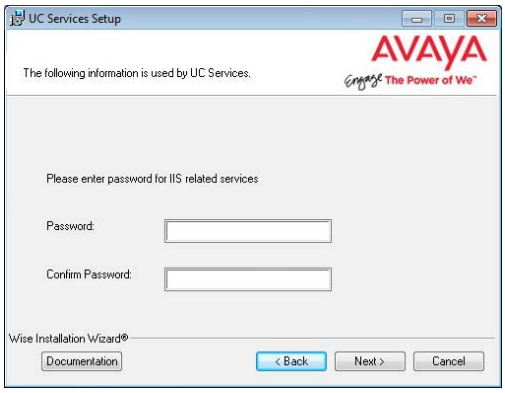


15. Enter the number of ports your system will use.

    Click **Next**.

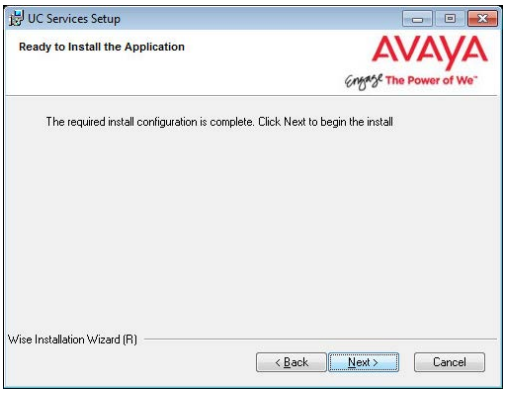


16. Create and verify a UC IIS User Password. This is used when logging into any associated web applications, such as Web Access.

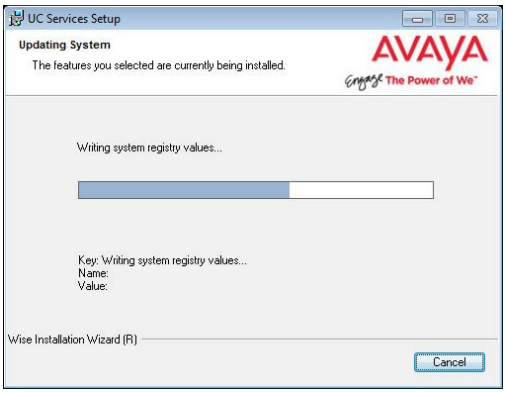


17. The preliminary information required for installation is now complete.

    Click **Next**.

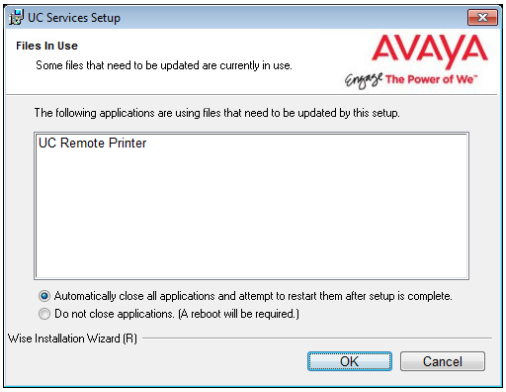


18. The selected components will now be installed. This process may take a while.



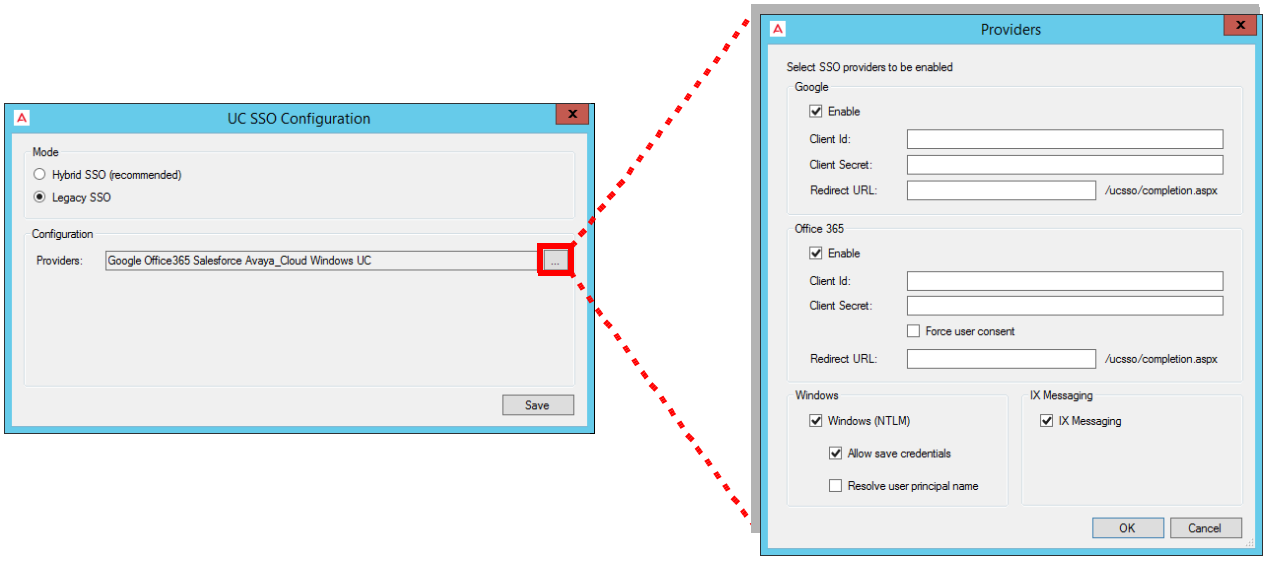
19. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.

    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.

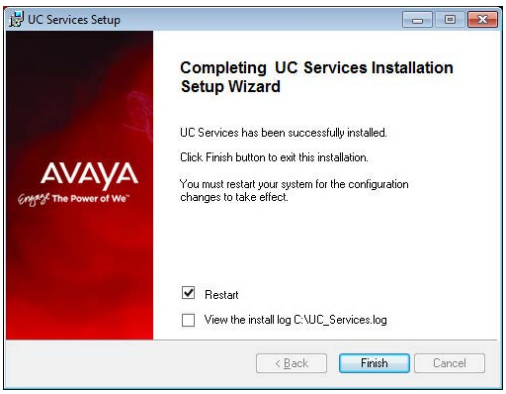
21. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



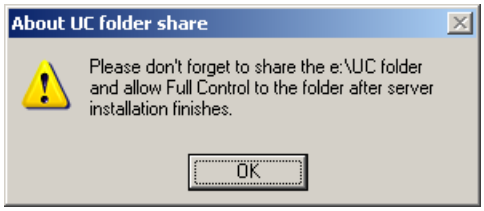
Note: For more information on the SSO Options, see chapter 25 on page 651: Single Sign-On (SSO).

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 page 256 for details).



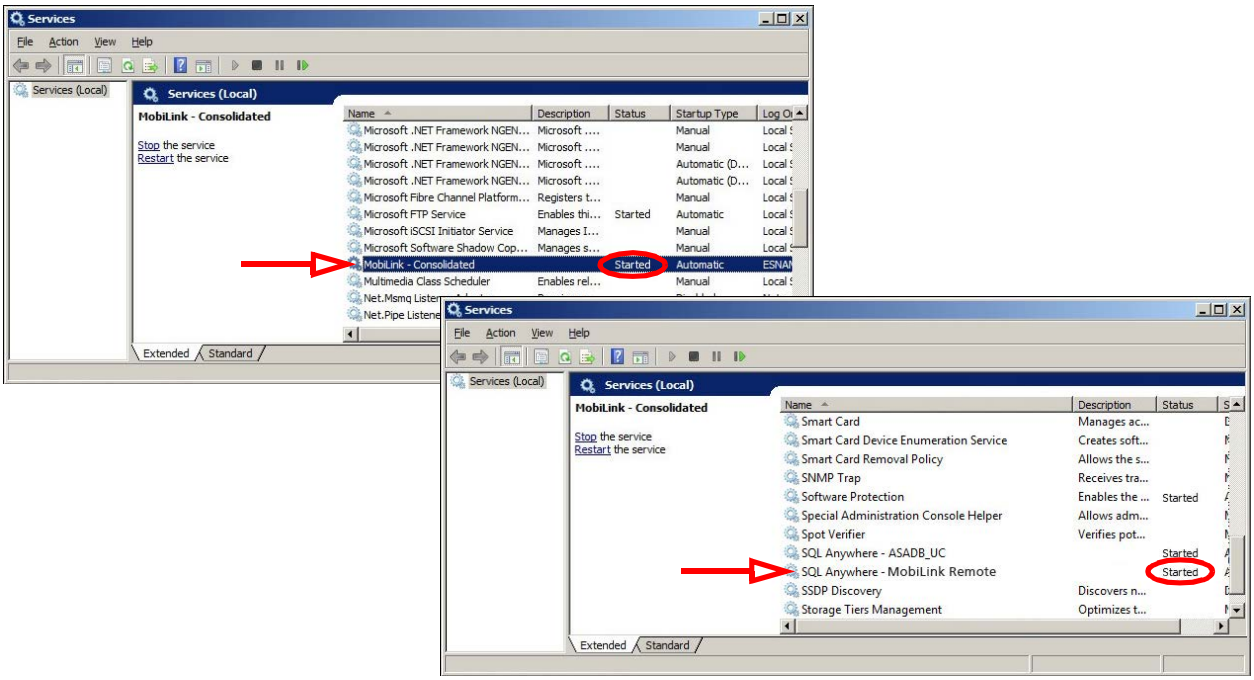
Click **OK** to restart the computer.

Warning: Once all of the HA servers (Consolidated, Primary and all Secondaries) have been installed, it is important to perform a full synch of all data. Attempting to login to the Primary 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

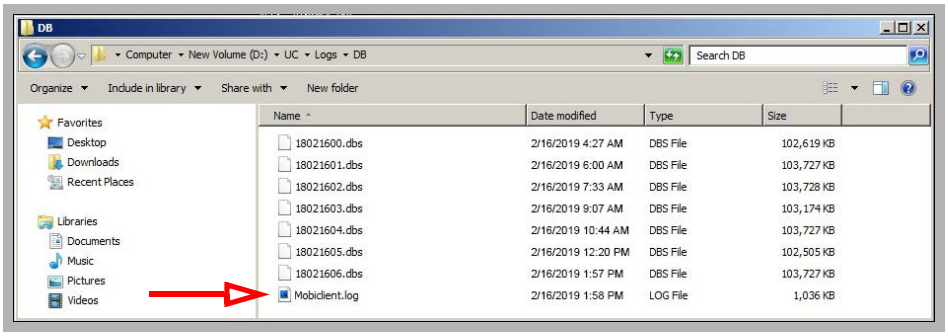
Once Primary and Consolidated servers have been installed, it is important to complete a full synch of all data before attempting to add any Secondary servers. Once a each Secondary has been attached, it too must be fully synchronized. Attempting to login to the Primary or Secondary servers before the 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 Primary and all Secondary servers, this service called **SQL Anywhere - MobiLink Remote**.

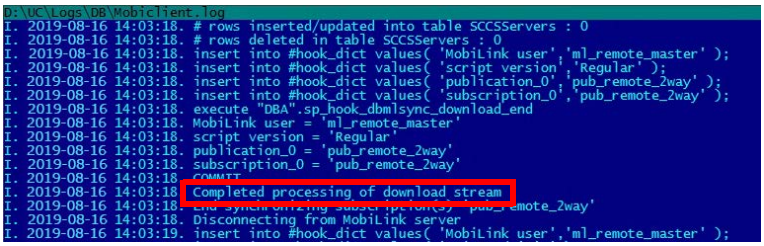


Open the services window and check that the named services are running on each server. If any are not active, then select it and press **Start**.

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.



Sharing the UC Folder

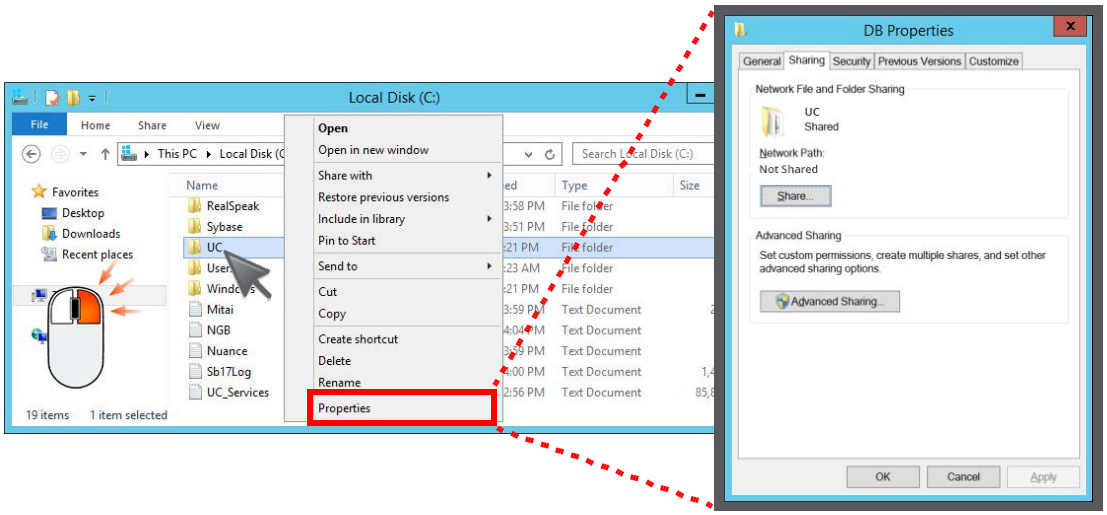
It is necessary to share the UC installation folder so that all of the programs and users have the required access. The following user accounts require full permissions to the UC folder:

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

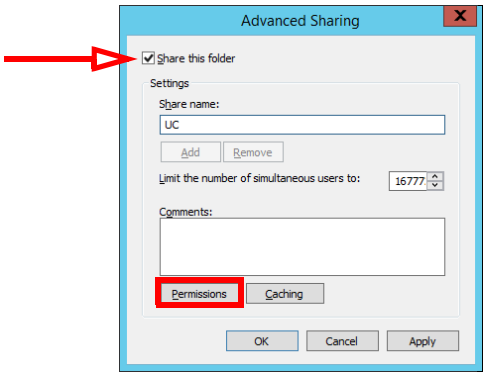
Follow this procedure on the Primary, the Consolidated, and on **each** Secondary server on the system.
Also share the folder if you are using a Remote Web Server.
If you are using Remote CSE Servers, the folder only needs to be shared with the DCOM user.

Procedure

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

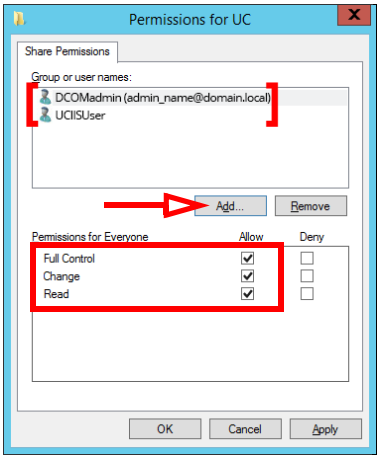


2. Click **Advanced Sharing**. Enable the **Share this folder** checkbox.



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.

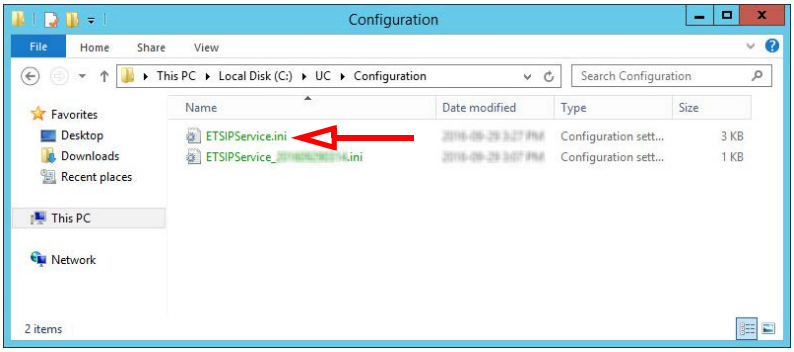
MWI Configuration

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.

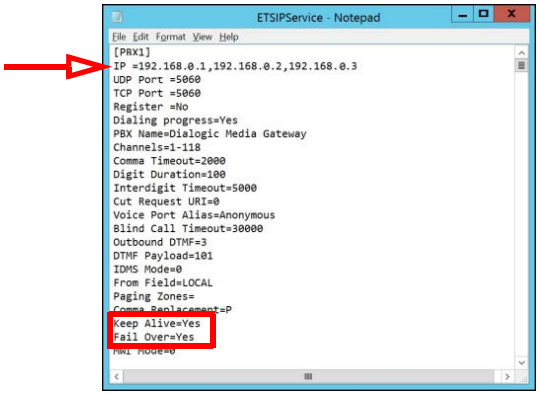
- Add a new line to the **ETSIPSERVICE.INI** file found in **/UC/Configuration** folder.



- 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 Primary and all Secondary servers) in the array.

Geo Redundancy

An Avaya IX Messaging HA installation can be spread across a geographically distributed network. Geo Redundancy allows a section of the network in one part of the world to go offline without affecting the remaining elements.

Installing Messaging with Geo Redundancy proceeds the same way as it does with any other HA install, but with some of the servers existing in other locations.

Geo Redundancy has the following network connection requirements to operate properly.

- All Messaging servers must be on the same network as the PBX.
- All servers must have a minimum 1Gbps connection to the network.
- The maximum round-trip latency for optimum performance is 10ms between servers, with an acceptable tolerance up to 60ms.
- The maximum round-trip latency between the voice servers and the PBX must be no more than 200 ms.
- Optimal round-trip latency is a maximum of 150 ms.
- The path of connectivity must have 20Mbps guaranteed bandwidth with no steady-state congestion.
- At all times, the LAN network connection must provide a min guaranteed 20Mbps upload / download speed.

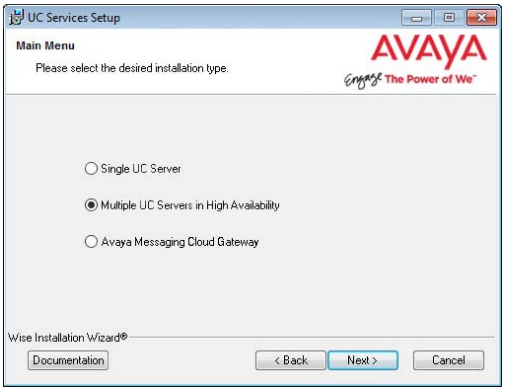
Contact your dealer if you have any further questions.

Adding Secondary Voice Servers

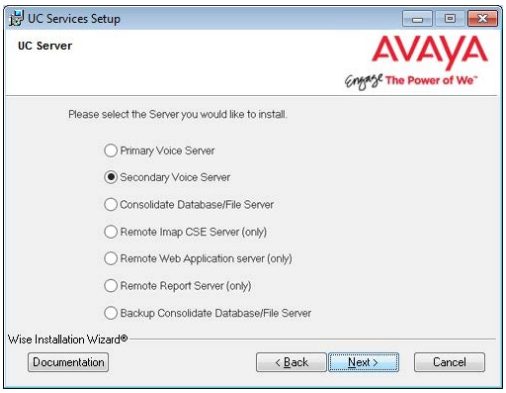
As your communication traffic expands, it may become necessary to add more Secondary Voice Servers to a High Availability environment to maintain adequate response times.

Note: The following procedure only applies to adding voice servers to the system. Only one Primary Voice Server can be installed.

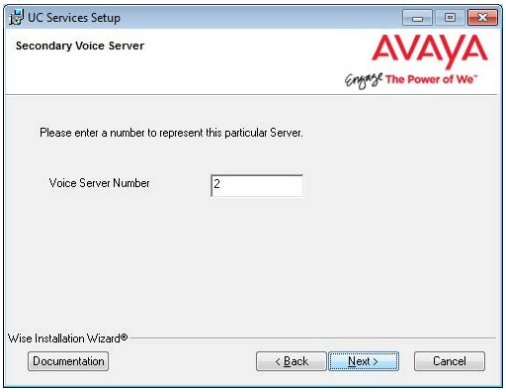
1. Create a new voice server (virtual or physical) with the same hardware parameters as the existing units.
2. Install and configure Windows (Roles and Features) as was done with the original voice servers.
3. Install Avaya IX Messaging on the new machine, selecting **Multiple UC Servers in High Availability** when prompted.



4. Continue with the installation and select **Secondary Voice Server** when prompted.



5. Continue with the installation. At the prompt, enter a number for the new server.
   Each Secondary server must have a unique identifying number assigned **between 2 and 20**.



Note: The Primary Server is automatically assigned # 1.

6. Complete the remaining steps of the Secondary Voice Server installation. When finished, reboot the new server.
7. When the new server has restarted, stop the **DBWatcher** service on both the new **Secondary Voice Server** and on the **Consolidated Server**. This will allow the new server to synchronize all data with the HA system.
8. When the synchronization has completed, restart the **DBWatcher** service on both the new **Secondary Voice Server** and on the **Consolidated Server**.

The new Secondary Voice Server has been added to the HA environment.

8 JITC INSTALLATIONS

In This Chapter:

Introduction

Avaya IX Messaging 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 IX Messaging can be purchased in a JITC certified format which encrypts the database files using FIPS approved encryption. Other security sensitive files and folders within Messaging 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.

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

When installing Avaya IX Messaging 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.

Requirements

Requirements	Details
License	JITC License for 10.8.
Software	For details on Messaging 10.8 Hardware and Software requirements please consult the Technical Operating Guidelines.

Important: Microsoft Windows is not provided with any version of IX Messaging. The customer must install and fully update a suitable, licensed version of Windows onto the hardware platform before proceeding with the Avaya IX Messaging software installation.

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

Note: Avaya IX Messaging should only be installed on a dedicated server specifically intended for the purpose. Sharing system resources with other applications may prevent Messaging 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 Messaging voice server installation.

Installation Preparation

Pre-requisites

- A JITC specific license for Avaya IX Messaging 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 Messaging installation.

Deployment Configuration Considerations

- An Avaya IX Messaging 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 Messaging 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 Messaging. While other configurations may be possible, Avaya cannot provide support in these areas.

Antivirus Applications

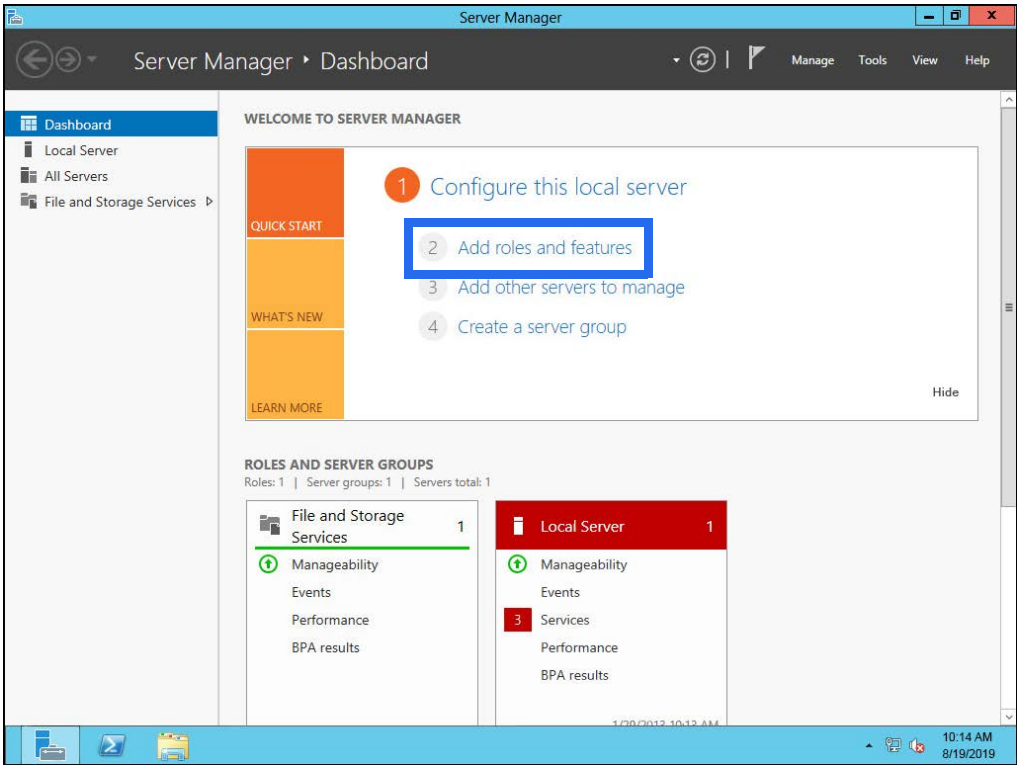
It is suggested that any antivirus applications currently active on the server computer be disabled during installation. Any other resource intensive applications or monitoring tools which may cause a conflict with the installation should also be disabled during the installation process.

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 Messaging installation.

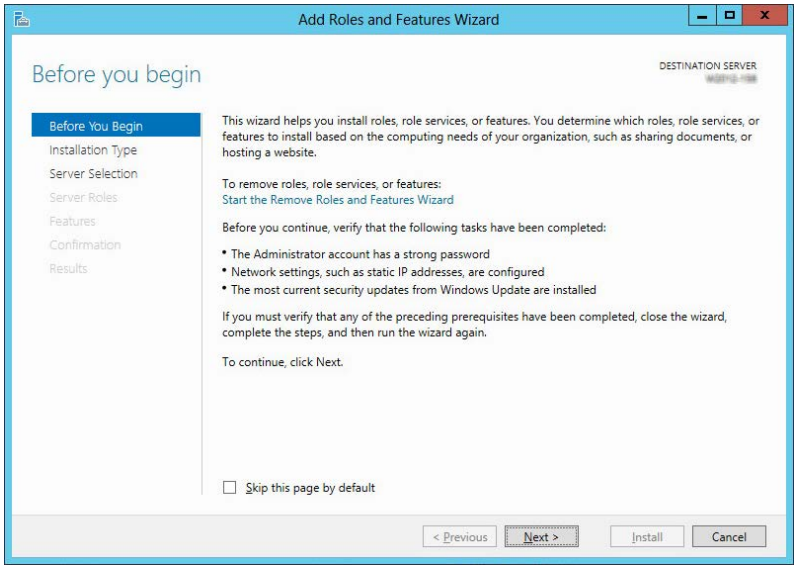
Server Roles and Features

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

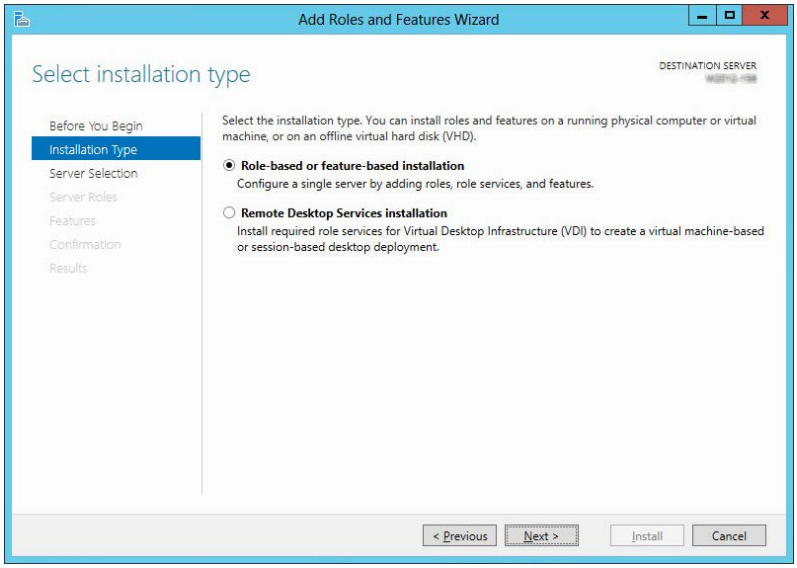


   If this screen is hidden, go to **View** and select **Show Welcome Tile**.

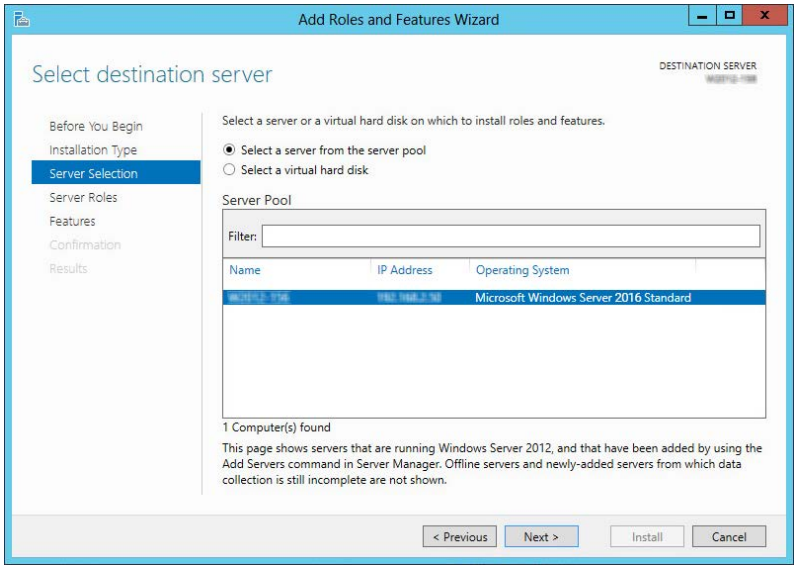
2. Click **Next**.



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

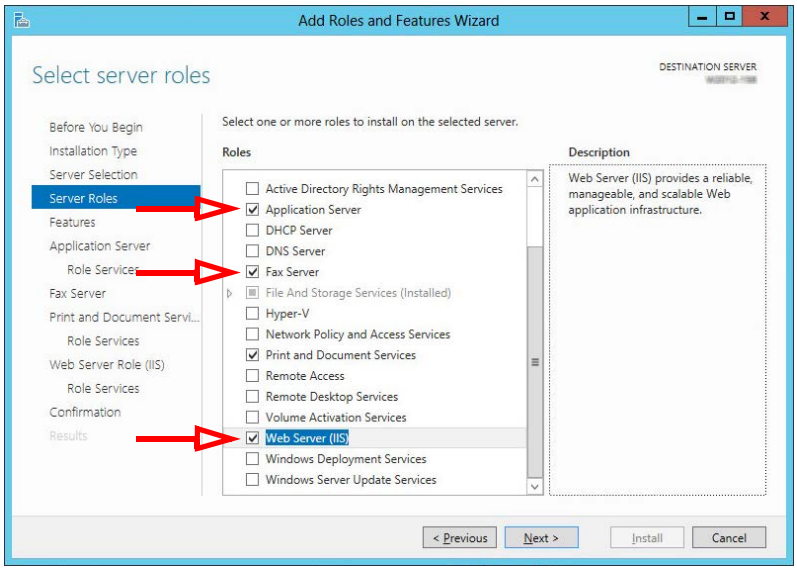


4. Leave the default settings as they are. Click **Next**.

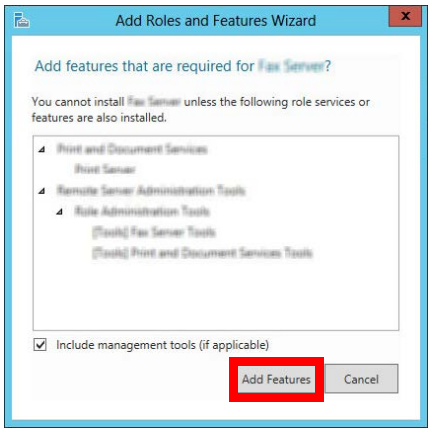


5. Enable the **Application Server**, **Fax Server** and **Web Server (IIS)** checkboxes.

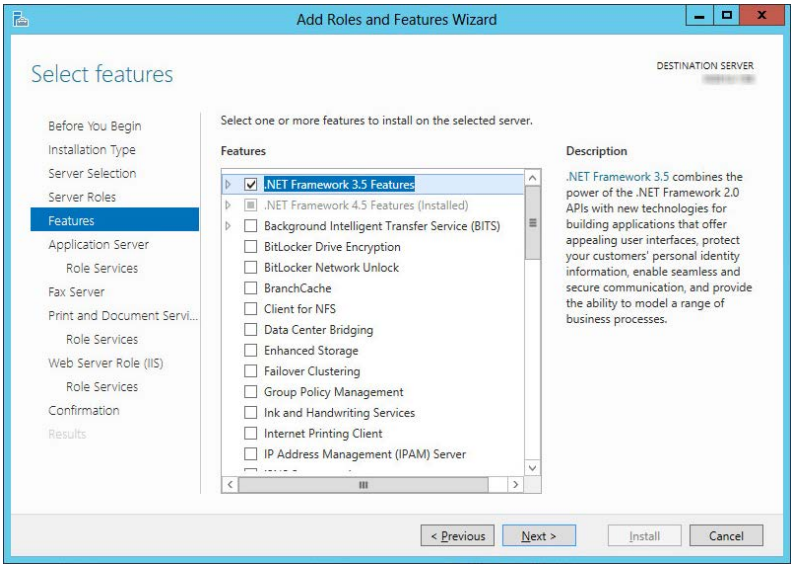
   Click **Next**.



Note: Throughout this installation, whenever you are prompted to confirm additions, always select **Add Features**.



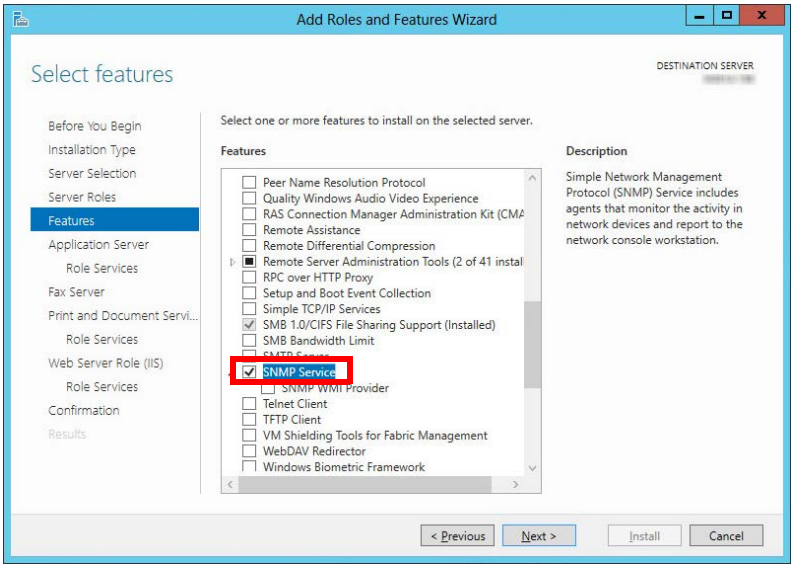
6. Enable the **.NET Framework 3.5 Features** checkbox. Click **Next**.



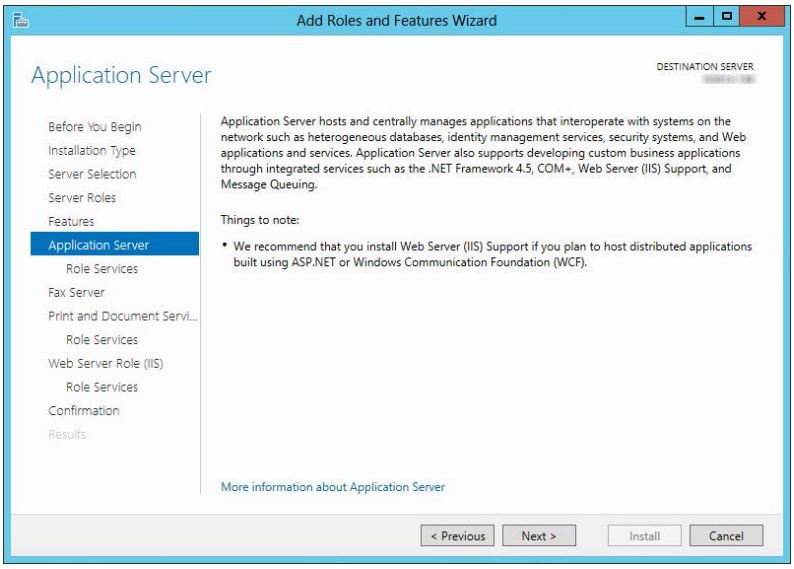
7. **Optional**: If you plan to use **SNMP Alarms** with Messaging, the **SNMP Service** must be added to Windows before the program can be installed.

   If SNMP Alarms are required, scroll down and enable SNMP Service.

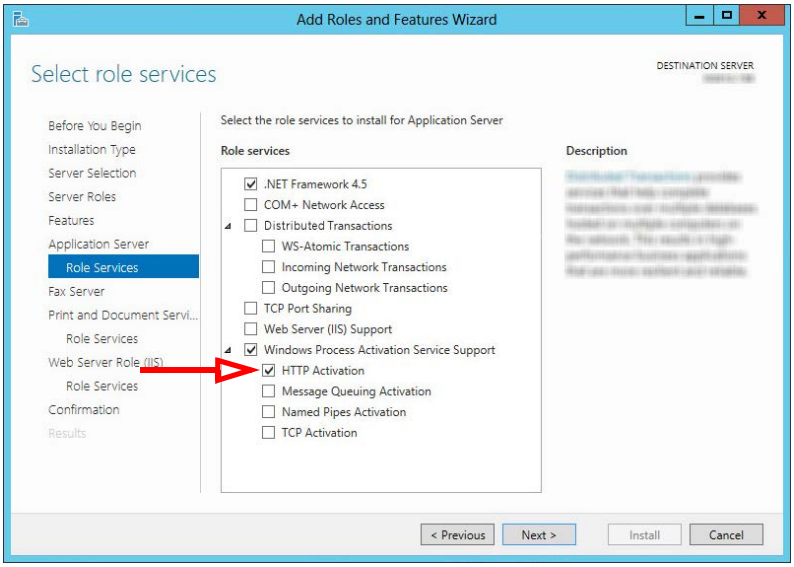
   If SNMP Alarms are not required, skip this step.



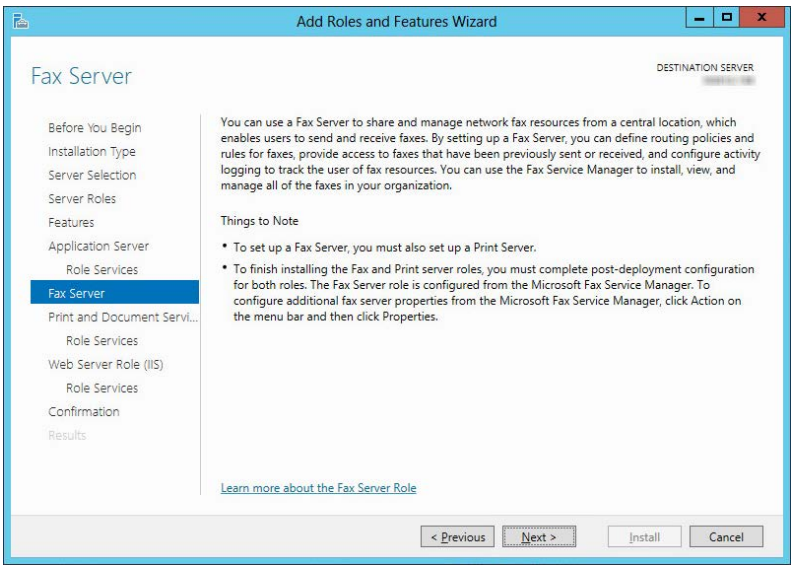
8. Review the information, then click **Next**.



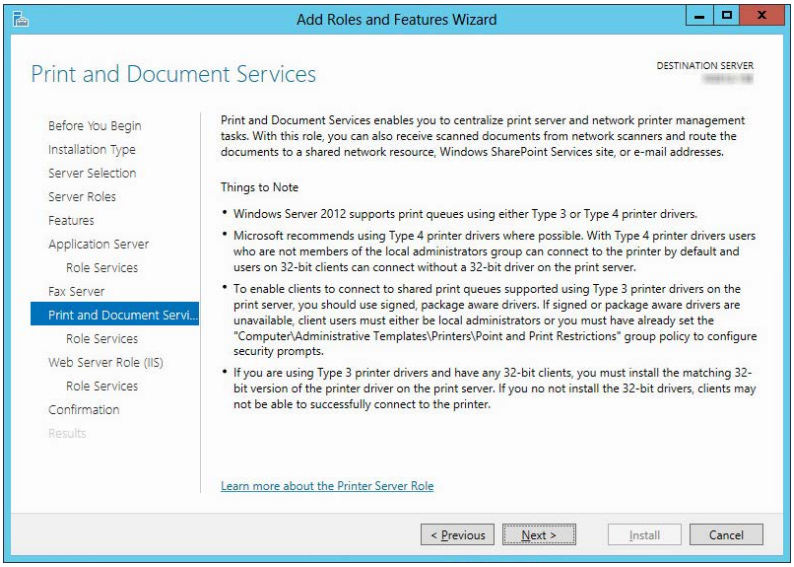
9. Ensure that **HTTP Activation**, under **Windows Process Activation Service Support** is enabled. Click **Next**.



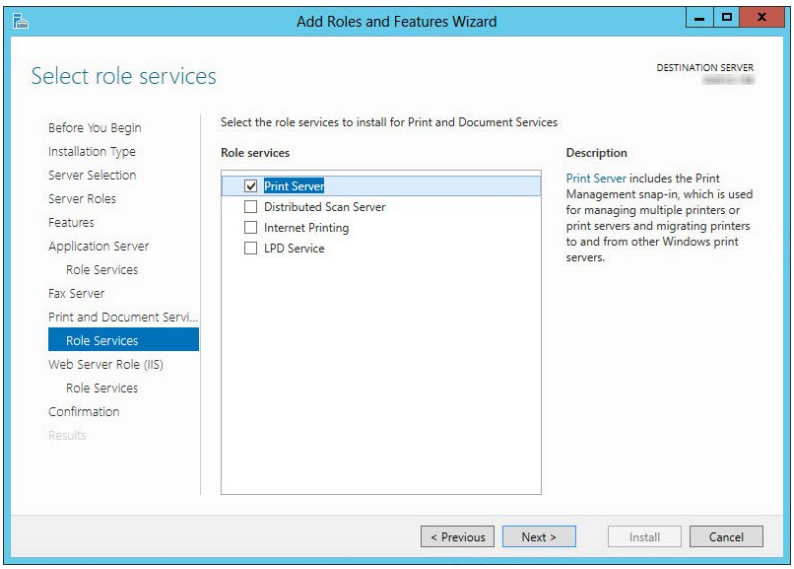
10. On the **Fax Server** screen, click **Next**.



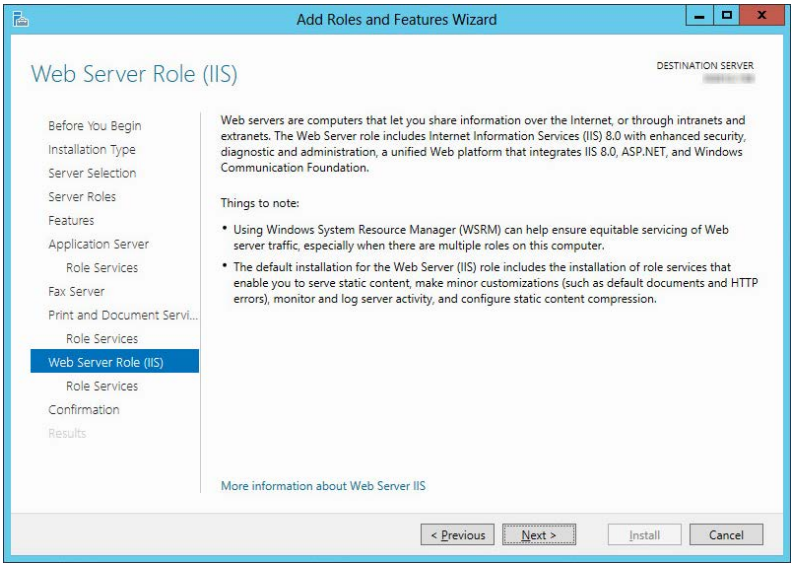
11. On the **Print and Document Services** screen, click **Next**.



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



13. On the **Web Server Role (IIS)** screen, click **Next**.



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

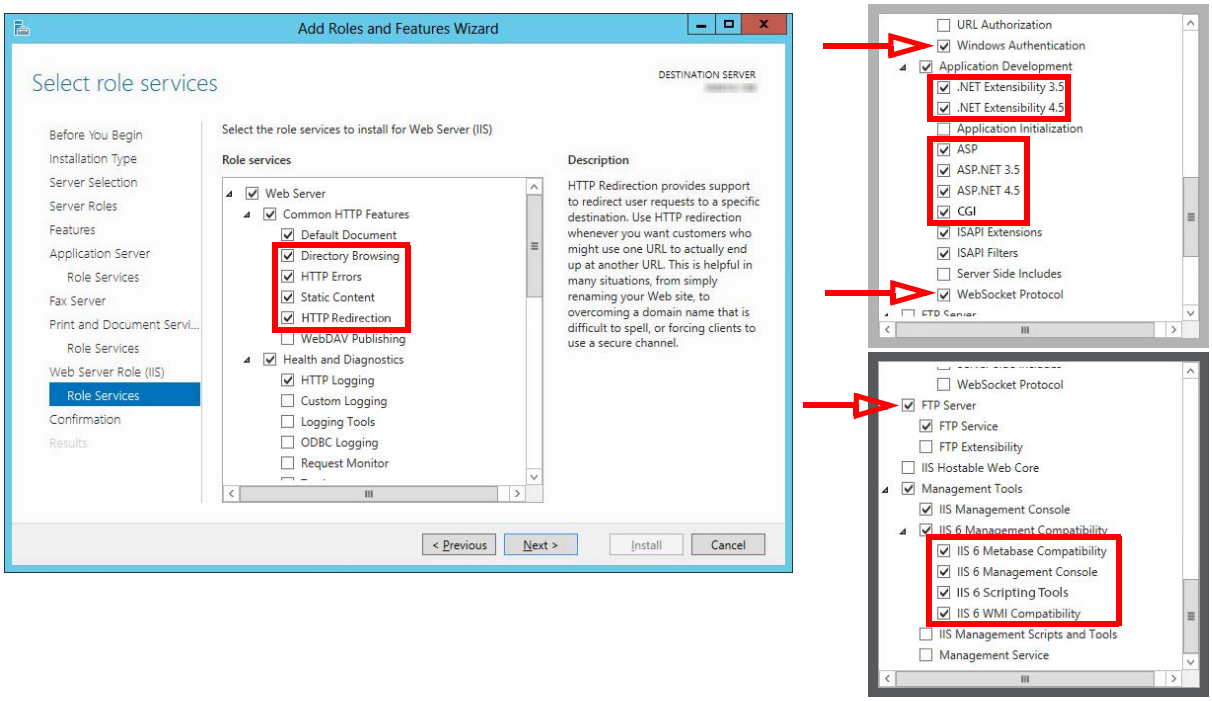
    Scroll down to **Security**, and enable **Windows Authentication**.

    Under **Application Development**, enable **.NET Extensibility 3.5**, **.NET Extensibility 4.5**, **ASP**, **ASP .NET 3.5**, **ASP .NET 4.5**, **CGI** and **WebSocket Protocol**.

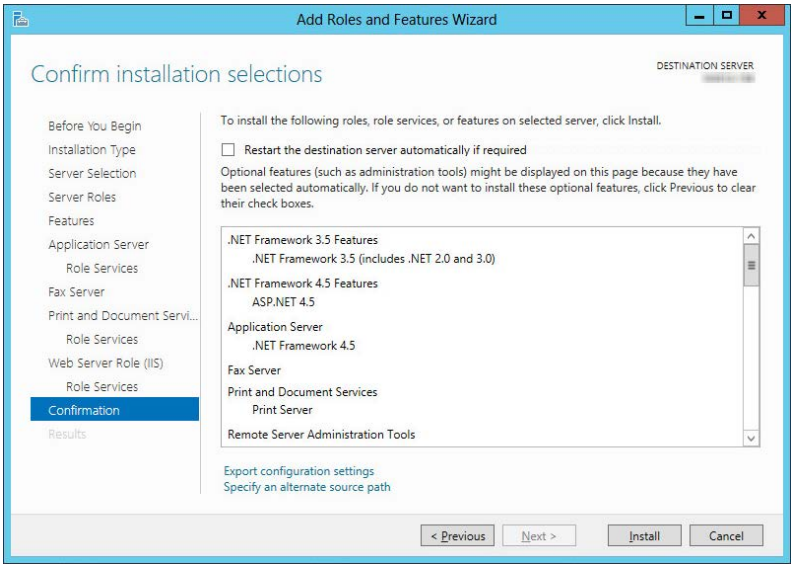
    Locate **FTP Server** and enable **FTP Service**.

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

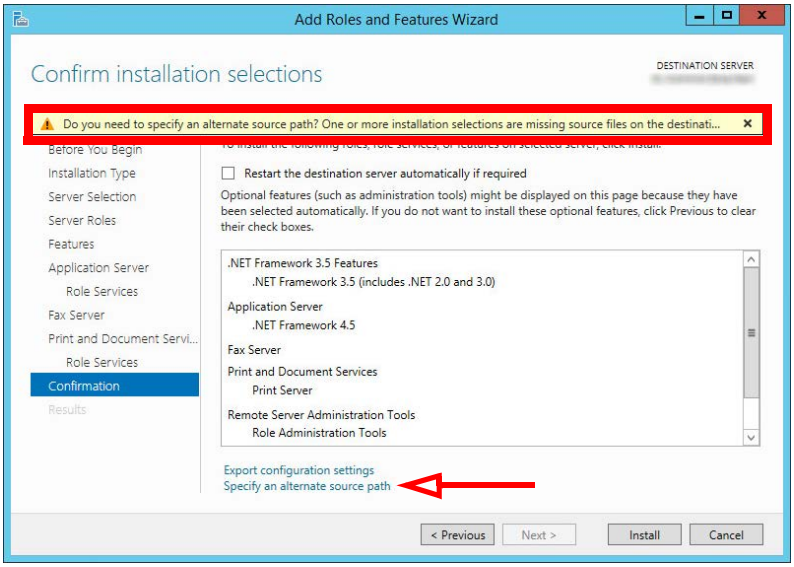
    Click **Next** when ready.



15. Review the selections here. When ready to proceed, click **Install**.

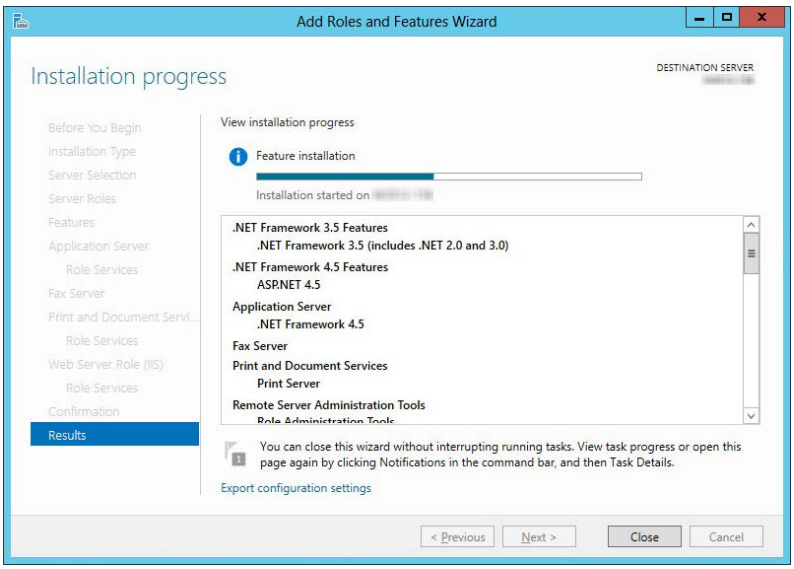


16. If prompted to provide the Windows disk to load the files, click **Specify an alternate source path** and direct it to the appropriate drive.



Hint: This is particularly important for virtual machine installations where there may not be a drive configured locally.

17. 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

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

Installing Microsoft .NET Framework 4.7.2

The Microsoft .NET Framework 4.7.2 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:

https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows

Follow the instructions provided to install .NET Framework 4.7.2 onto the server.

Certificates

Installing Certificates for Encrypted File System (EFS)

During installation, Avaya Messaging uses the Windows application **Cipher** to encrypt security sensitive files and folders. This uses the certificate installed in the Personal folder of the current user (the service/DCOM user created during installation). The certificate includes **Encrypting File System** under **Intended Purposes**.

Therefore, to ensure JITC compliance, you must to import the EFS certificate **before** installation.

Digital certificates can be purchased from a trusted Certificate Authority (CA), such as GoDaddy™ and Symantec™. A properly constructed certificate issued by your corporation's IT/Security team can also be used.

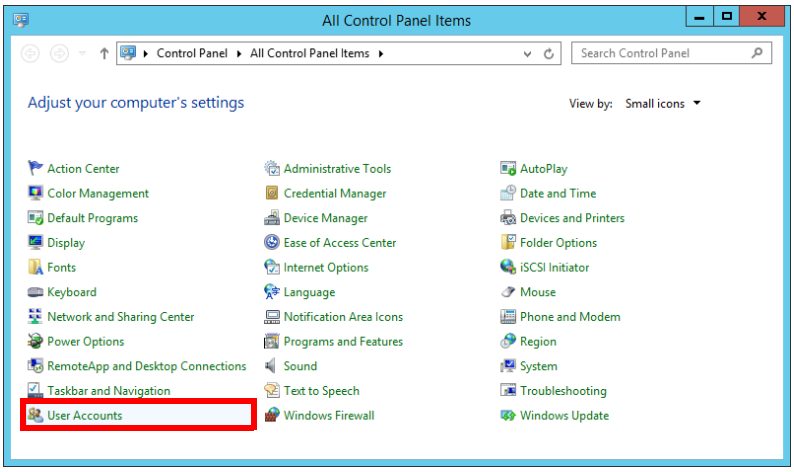
Important: Self-signed certificates are not permitted with JITC installations.

Installing a CA Signed Certificate

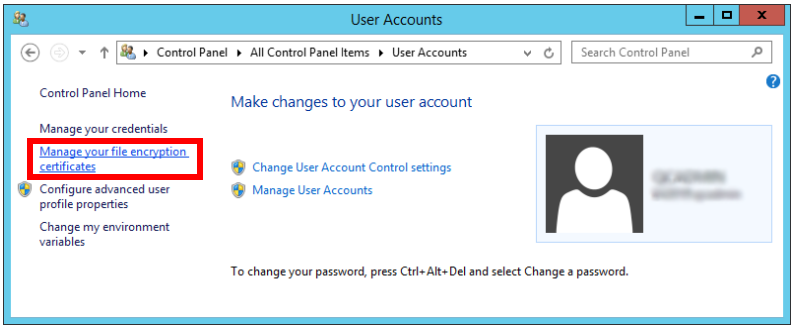
A Certifying Authority can issue a certificate to your company. They will provide a file containing the certificate and the password that opens it.

Save the file to a known location on the voice server hard drive.

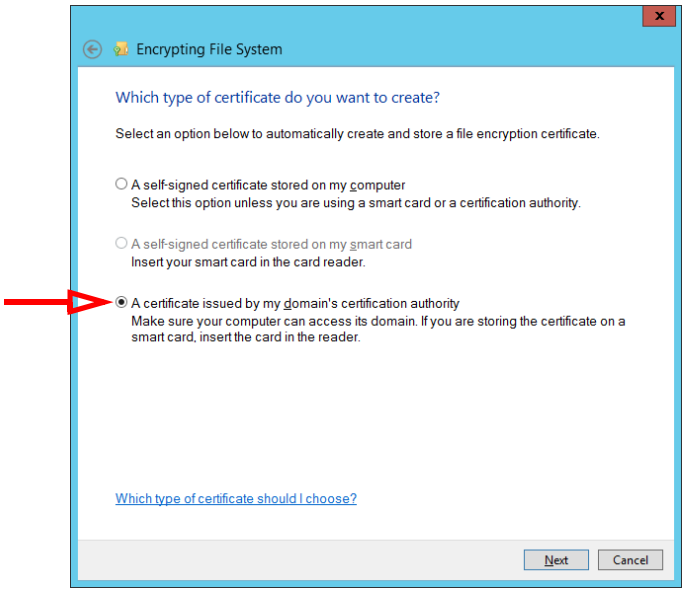
1. Open the Windows Control Panel and select **User Accounts**.



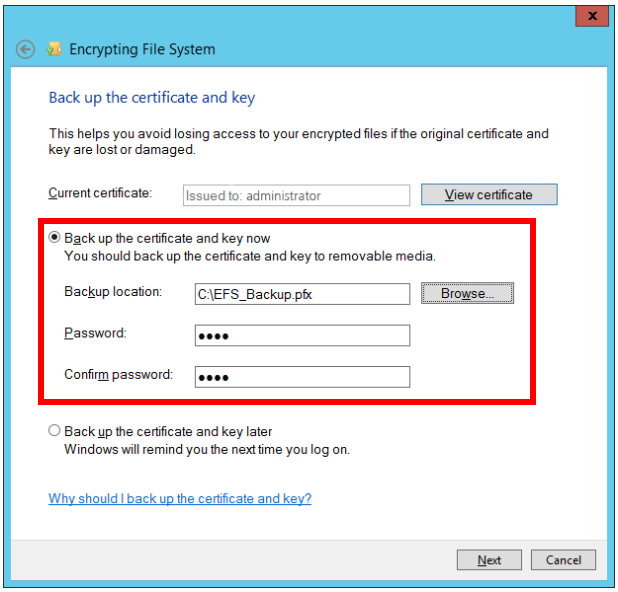
2. Click **Manage your file encryption certificates**.



3. Select **A certificate issued by my domain's certification authority**. Click **Next**.

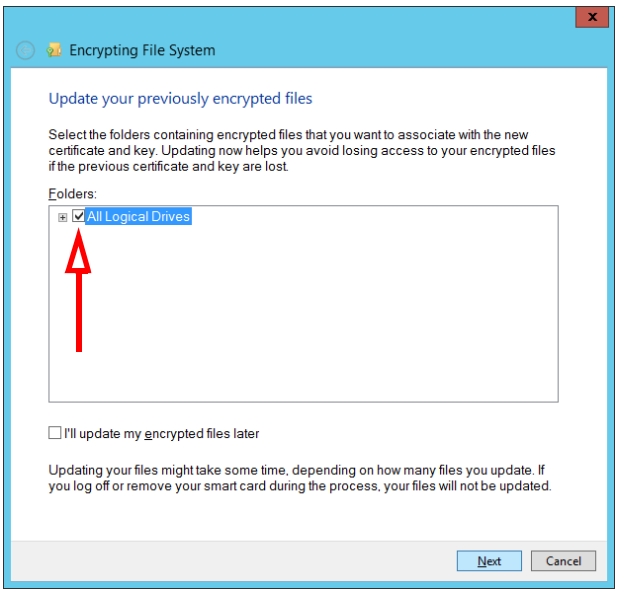


4. Enable **Backup the certificate and key now**, fill in the path to where the backup file will be saved, and give it a password. Click **Next**.

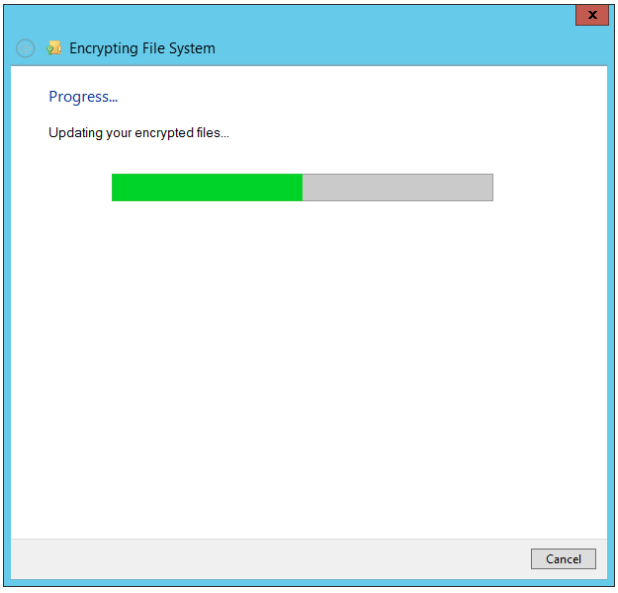


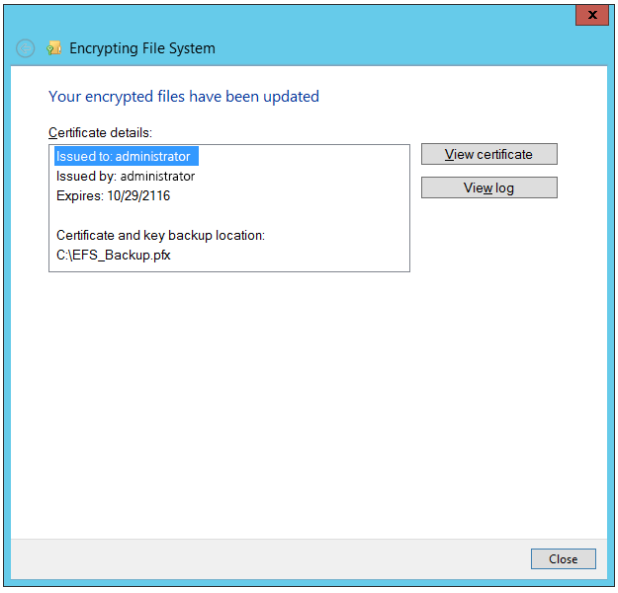
Important: If you are using a different certificate file, make sure to back it up once installation has finished. Instructions can be found in the **Backup and Restore the Certificate File** section.

5. Enable **All Logical Drives**, then click **Next**.

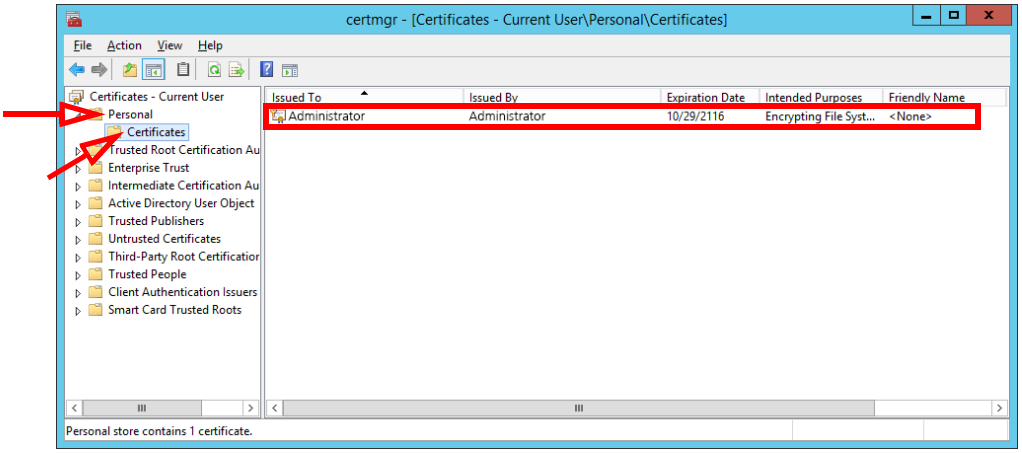


6. The files will be encrypted. When it is finished, a result summary will be displayed. Click **Close**.





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

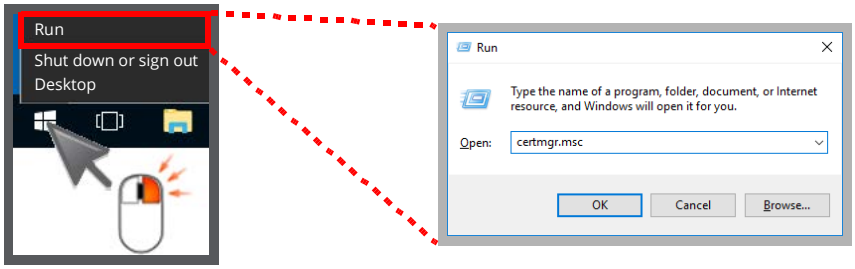
If you are using a certificate file from another source, or if you have not done so already, you should create a backup copy of the file. If the certificate becomes corrupt, none of your data will be accessible unless the certificate can be restored.

This section covers how to backup and restore the certificate file.

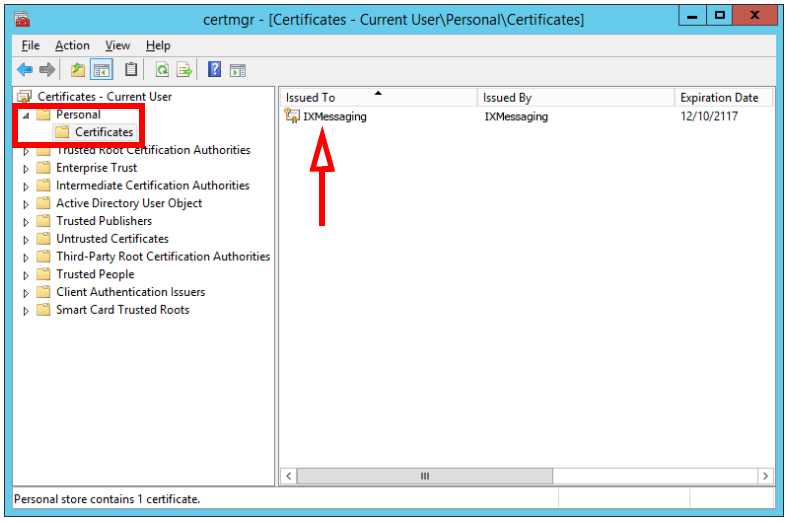
Backing-up the Certificate

To create a backup copy of the certificate file…

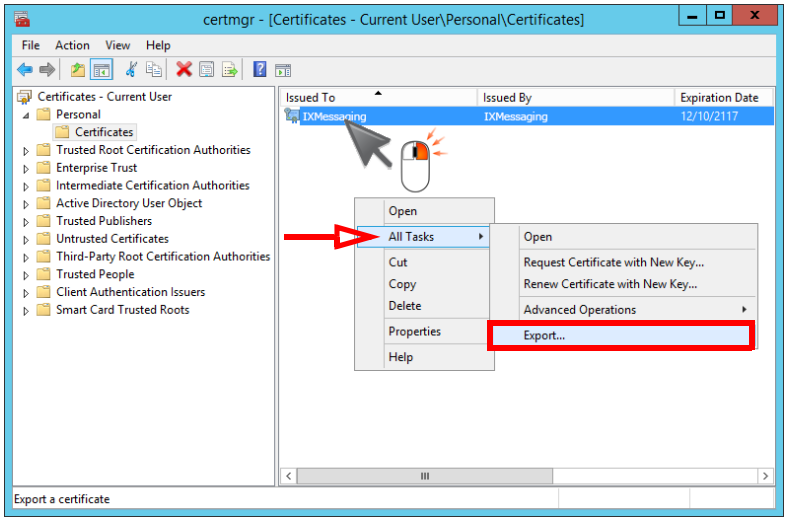
1. Launch the **Certificate Manager** console in Windows.
   Right-click the Windows icon and choose **Run**. Enter **certmgr.msc** and hit **OK**.



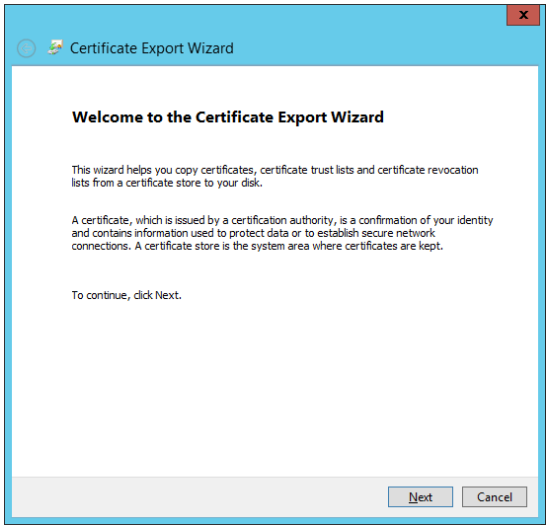
2. In the left-hand pane, open **Personal > Certificates**. Your certificate(s) will be displayed in the right-hand pane.



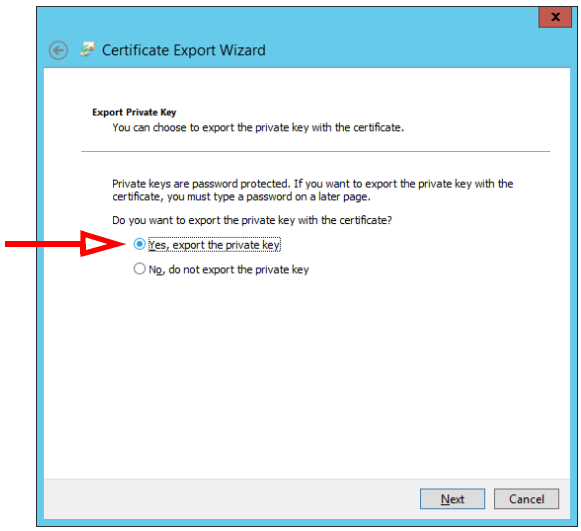
3. Right-click the certificate and select **All Tasks > Export**.



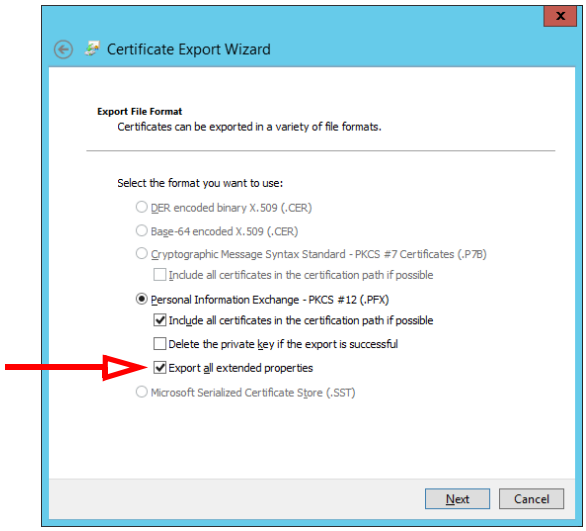
4. When the Certificate Export Wizard starts, click **Next**.



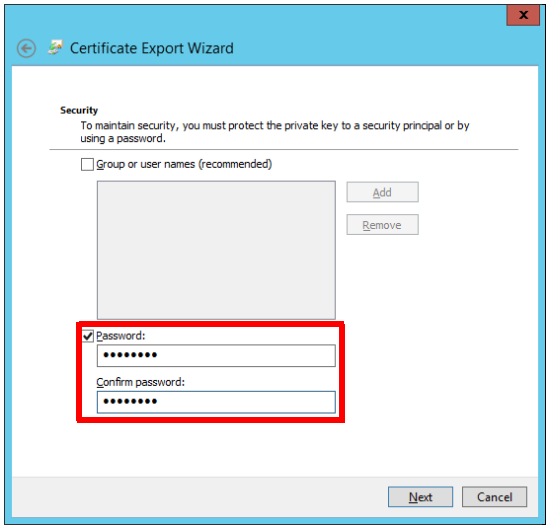
5. Enable **Yes, export the private key** and click **Next**.



6. Enable **Export all extended properties**. Choose **Next**.

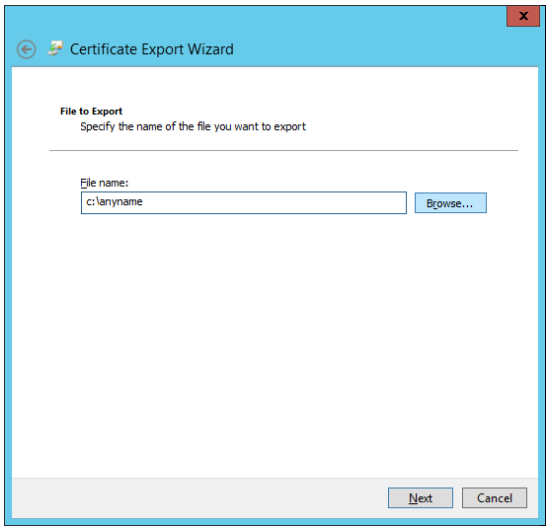


7. The backup copy of the certificate file requires a password for encryption.
Enable **Password**, then enter a password and re-enter to confirm. When ready, click **Next**.

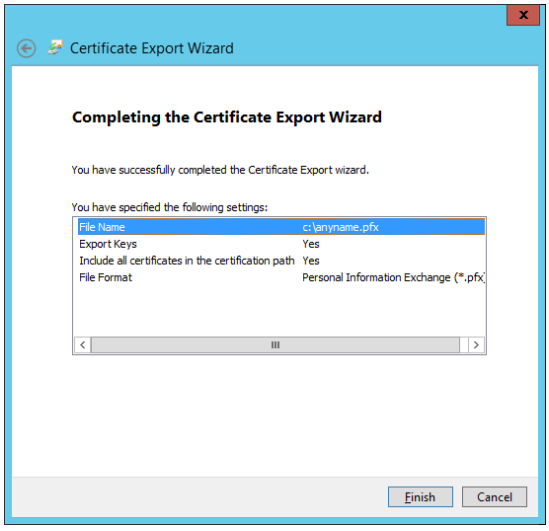


Important: Record this password and keep it in a safe location. **The loss of this password will lead to the complete and unrecoverable loss of data if you ever need to restore the certificate file.**

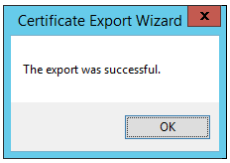
8. Save the file to your hard drive. Click **Next**.



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**.

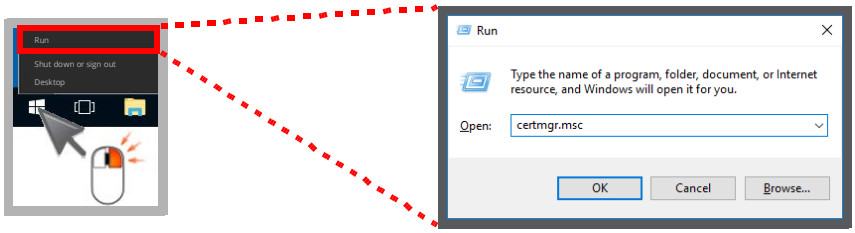


For maximum security, copy the file you just created to another drive (e.g. on another computer, network storage, on a thumb drive, etc.). If the original computer is completely inaccessible, saving the file to another location will still allow you regain access to the system.

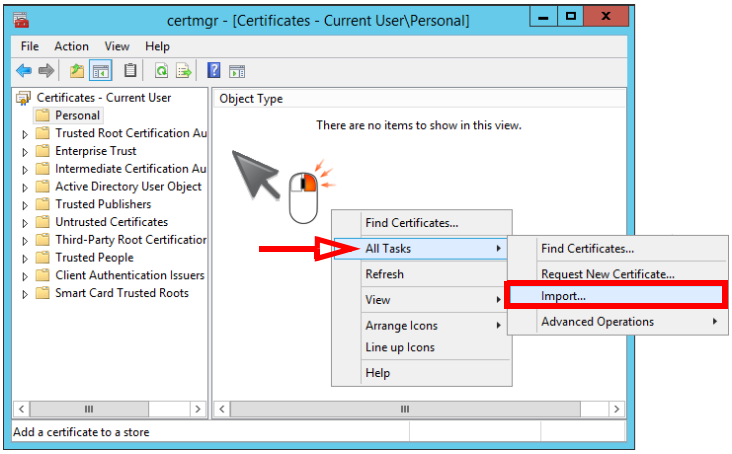
Restore the Certificate

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**.

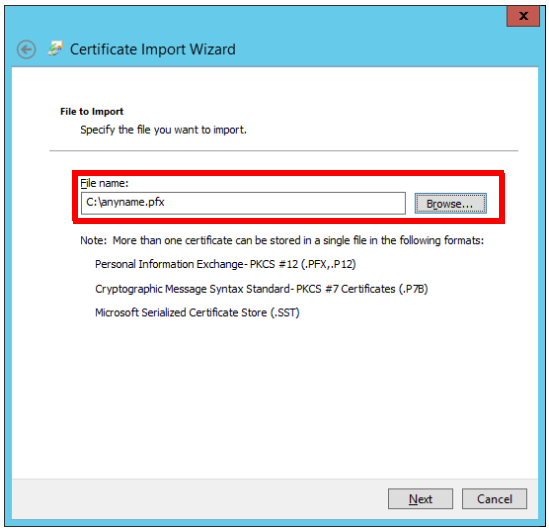


2. In the left-hand pane, the **Personal** folder will be empty. Right-click in the right-hand pane. Select **All Tasks > Import**.

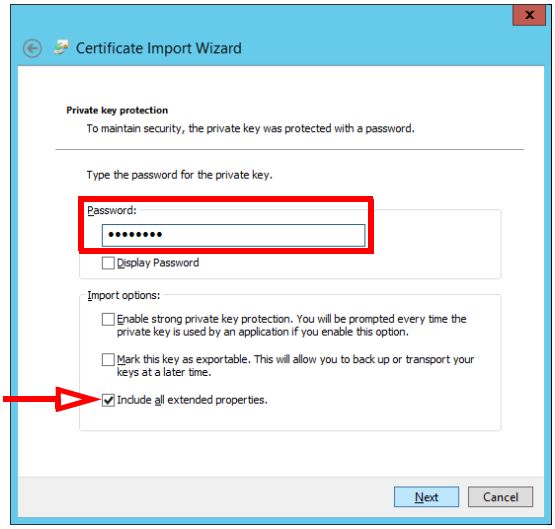


3. When the **Certificate Import Wizard** starts, click **Next**.

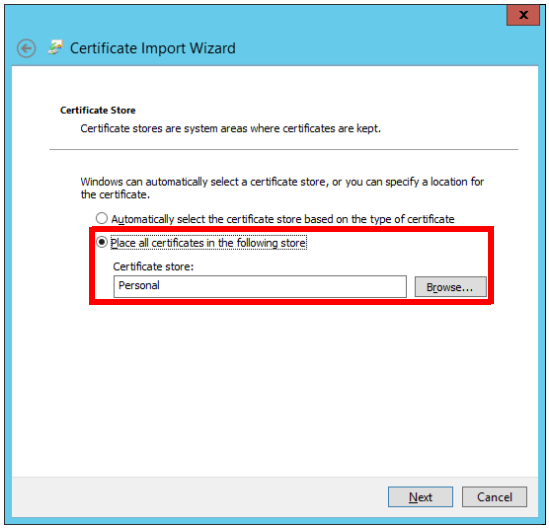
4. Locate the backup file and select **Next**.



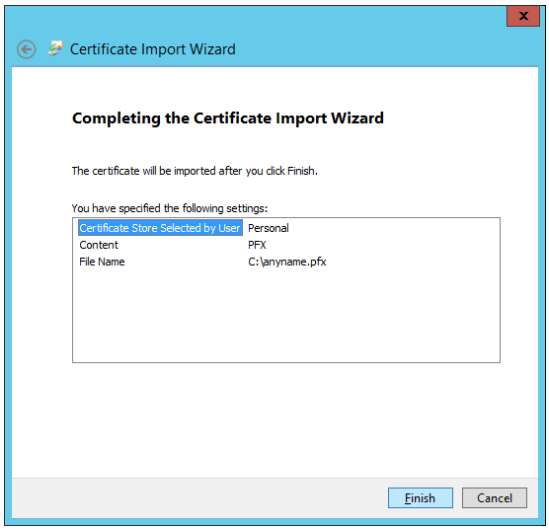
5. Enter the password that was used to secure the backup file. Enable **Include all extended properties**.



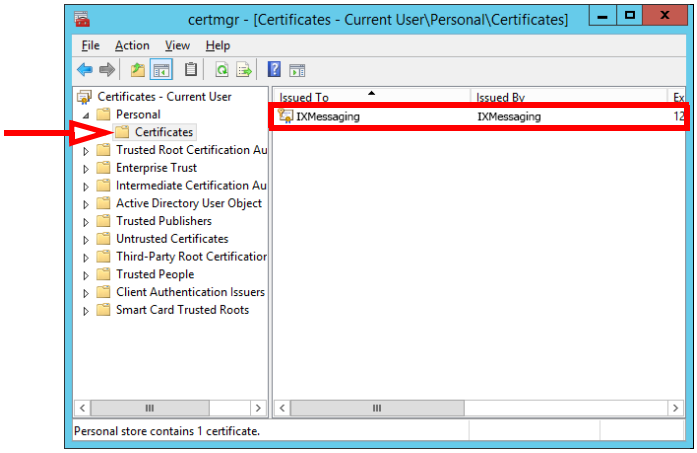
6. Ensure that the restored certificate will be copied to the **Personal** store and click **Next**.



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.

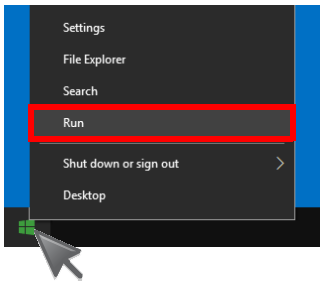
Reboot the server to have the changes take effect.

Import the Certificate on All Servers

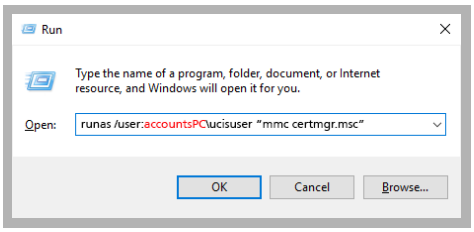
Important: The following procedure must be completed on all servers in a High Availability installation;

Primary, **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**.

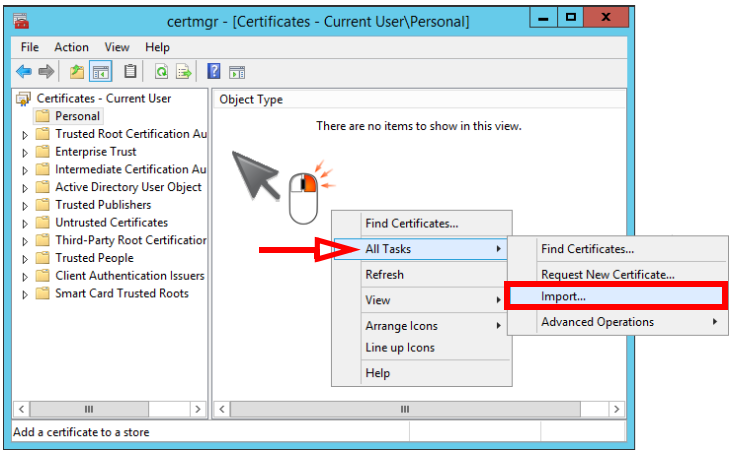


   When prompted at the command line, enter the password for the UCIISUser.
   The **Certificate Manager** console will open.

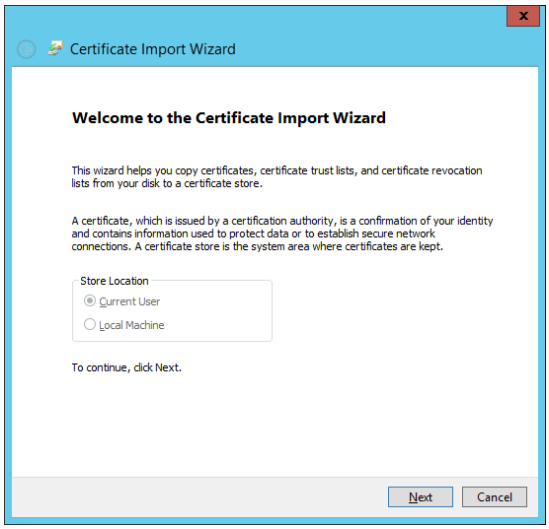
Important: The following command must also be run on the Consolidated server only.

runas /user:*computername*\ucAdminUser "mmc certmgr.msc"

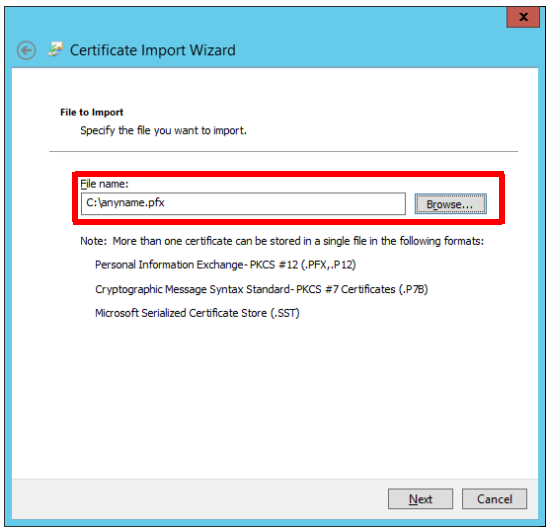
4. In the left-hand pane, the **Personal** folder will be empty.
   Right-click in the right-hand pane. Select **All Tasks > Import**.



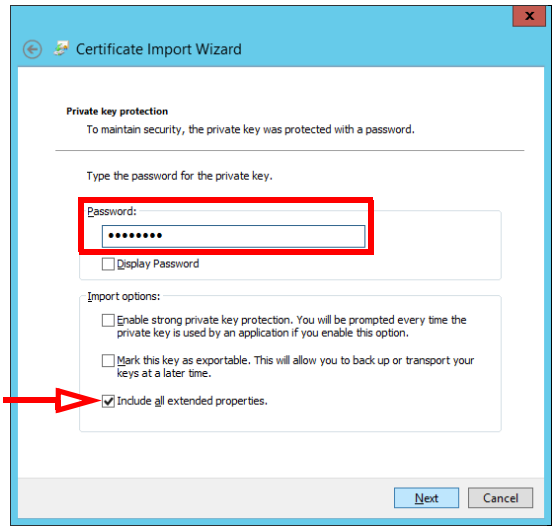
5. When the **Certificate Import Wizard** starts, click **Next**.



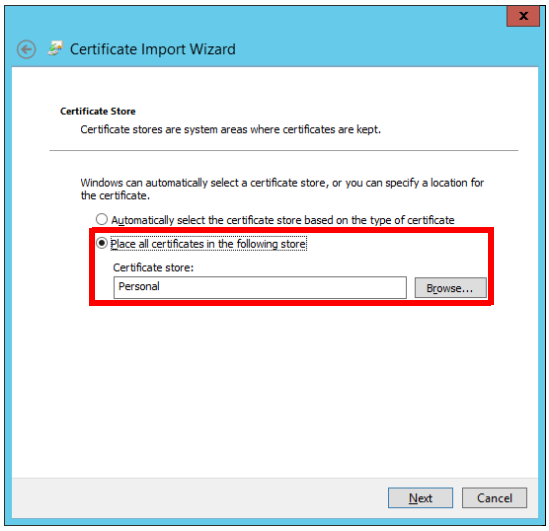
6. Locate the backup file and select **Next**.



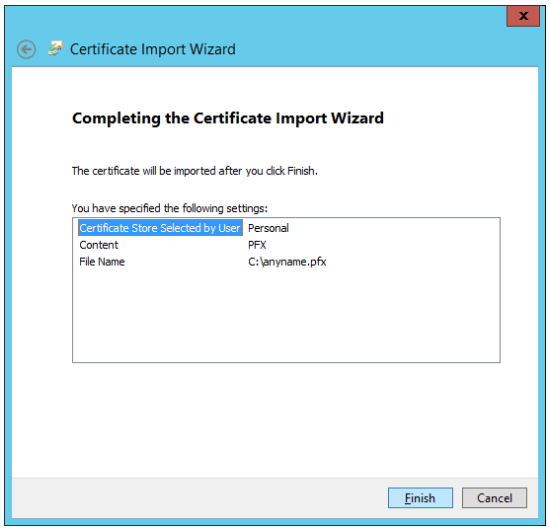
7. Enter the password that was used to secure the backup file. Enable **Include all extended properties**.



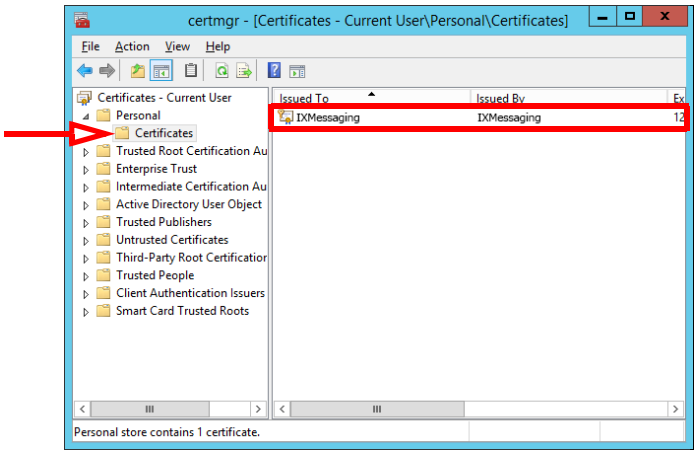
8. Ensure that the restored certificate will be copied to the **Personal** store and click **Next**.



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.



The certificate file has been successfully restored.

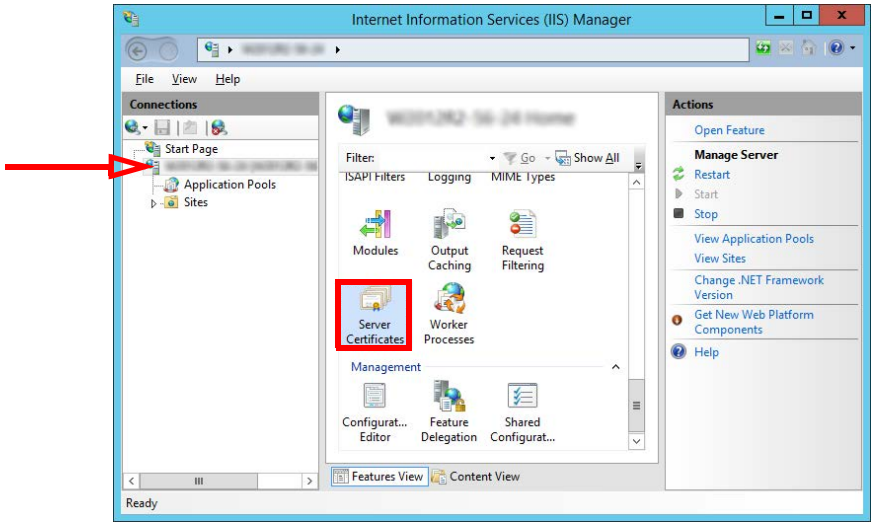
Reboot the server to have the changes take effect.

IIS Certificate Bindings

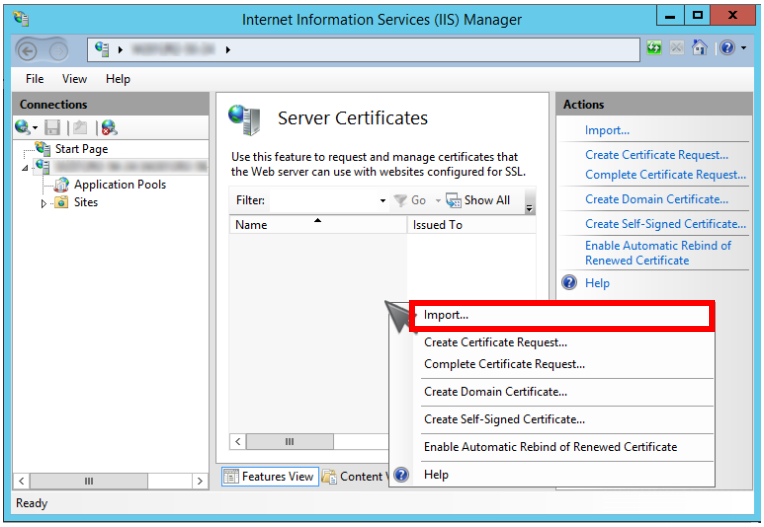
To enable an HTTPS connection, another certificate has to be installed in IIS. This certificate must be acquired from a certifying authority.

The HTTPS protocol must be enabled, and HTTP disabled.

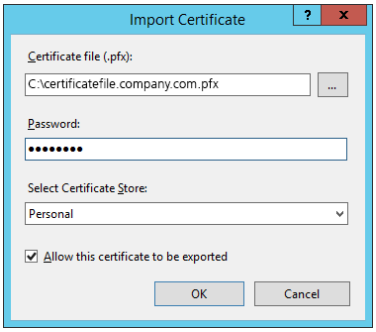
1. On the computer that functions as the web server, open the IIS Manager console. Select the local computer. Open **Server Certificates** in the right-hand pane.



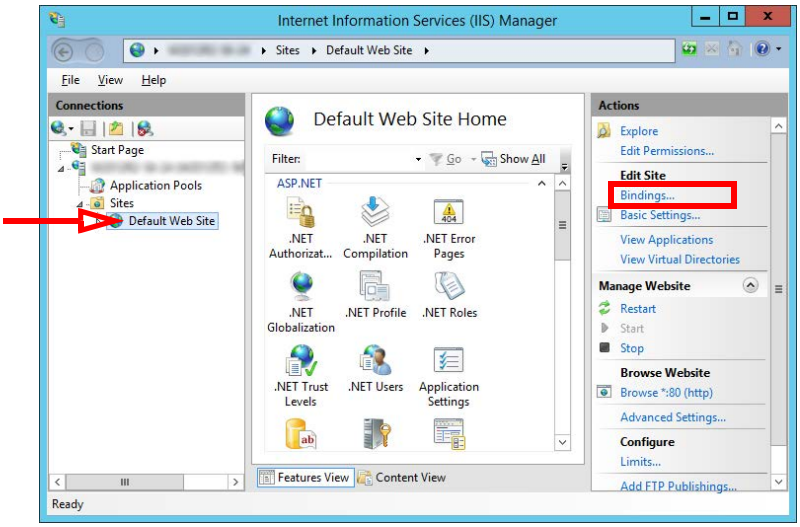
2. Right-click in the right-hand pane and choose Import from the pop-up menu.



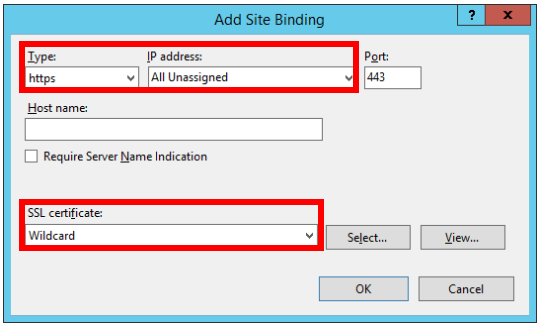
3. Enter the path to the certificate file and the password. Select **Personal** as the Certificate Store. Click **OK**.



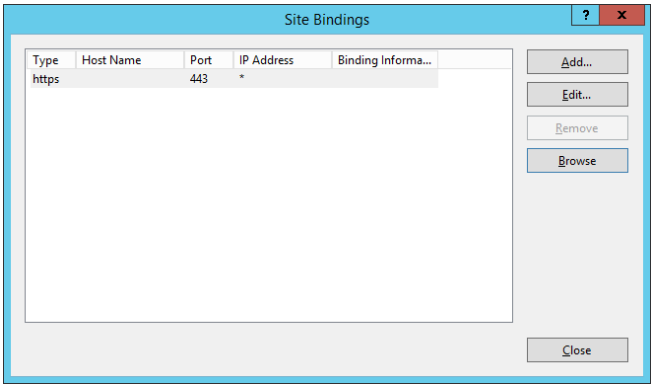
4. Go to **Sites > Default Web Site**.
Click **Bindings...**.



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**.

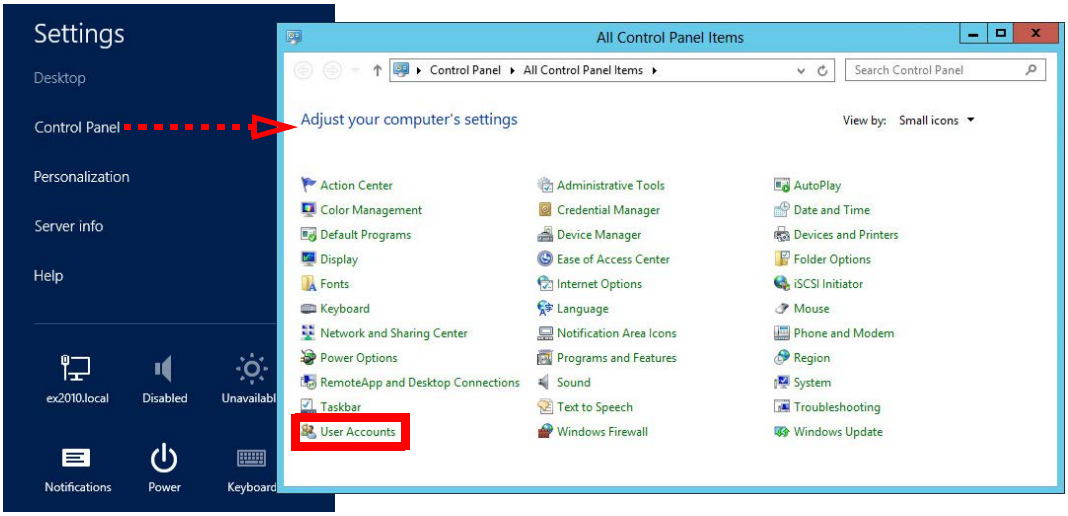


6. Remove HTTP from the list of bindings.
   Click **Close**.



Disabling User Account Control Notification

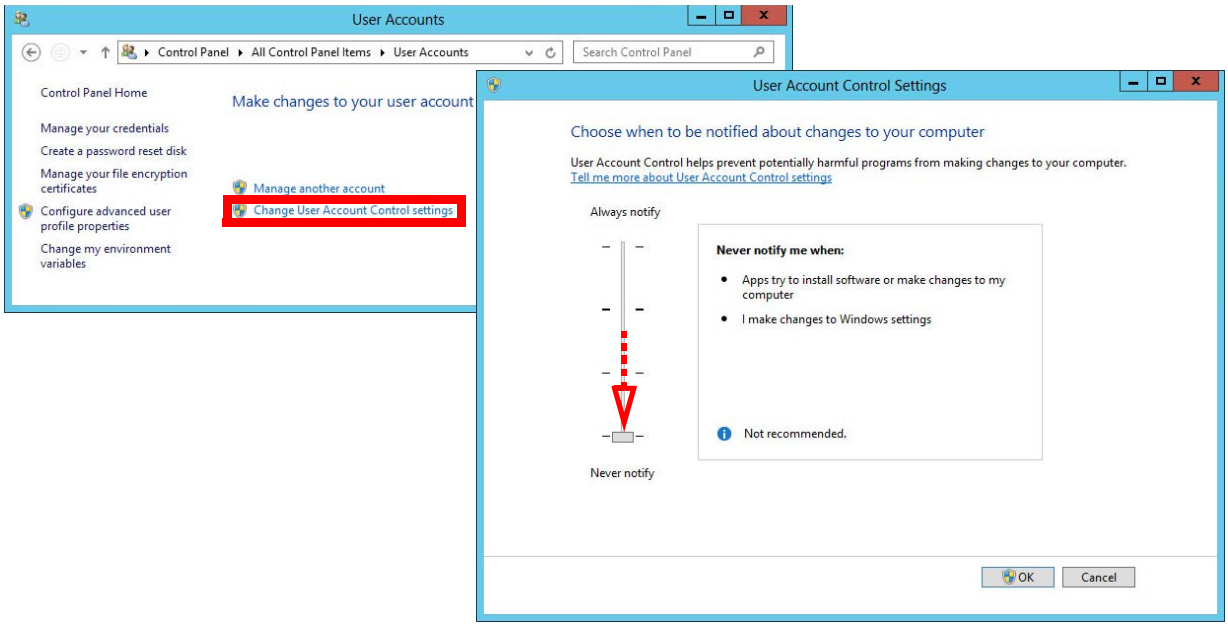
1. Go to **Settings > Control Panel**. Select **User Accounts**.



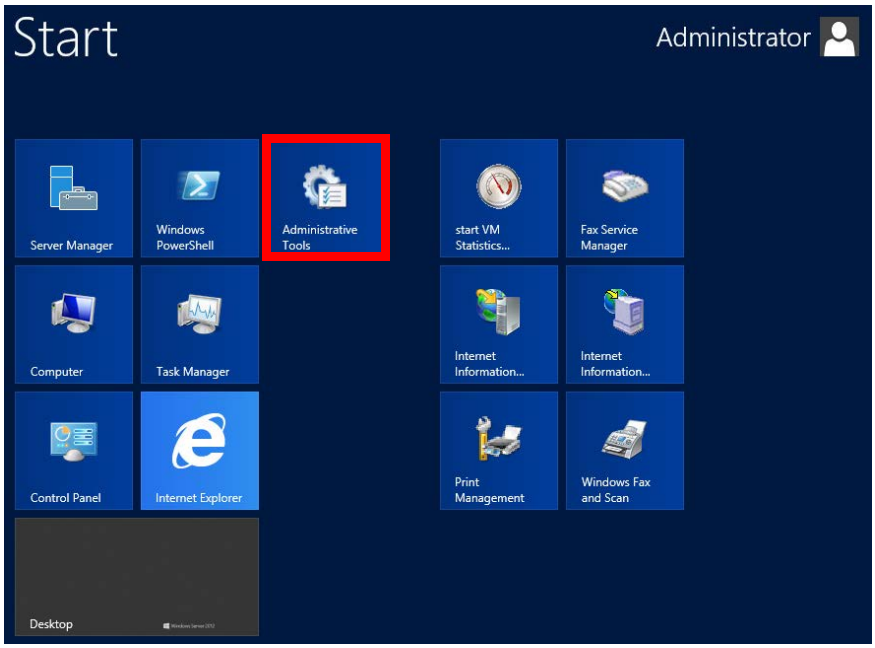
2. Select **Change Account Settings**.

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

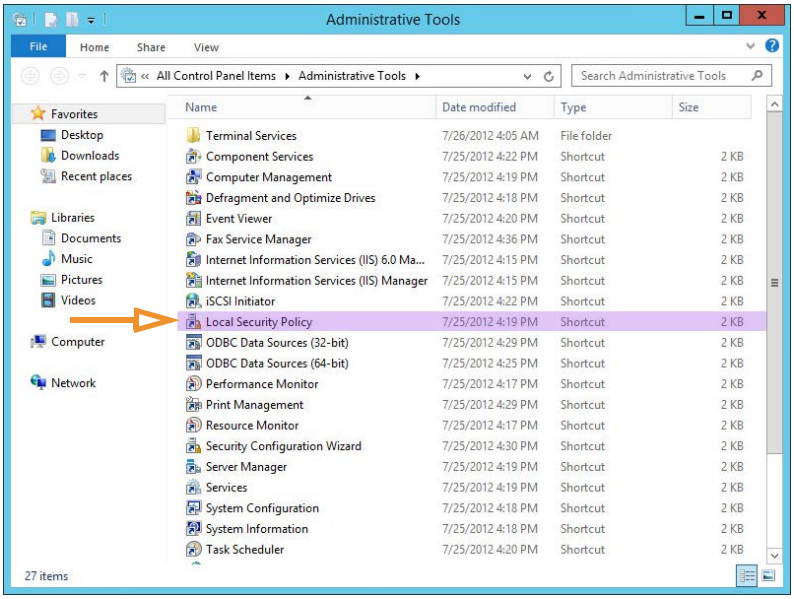
   Click **OK** and **Close**.



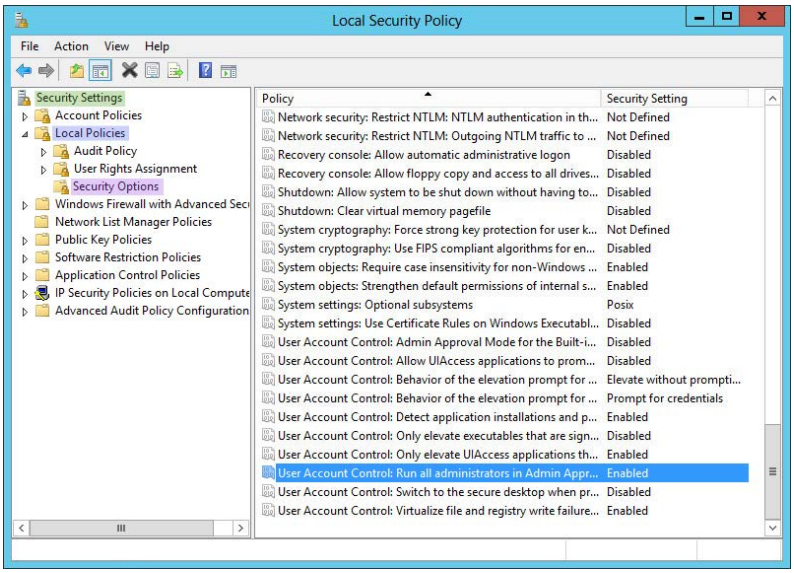
3. On the keyboard, click the **Start button**, and select **Administrative Tools**.



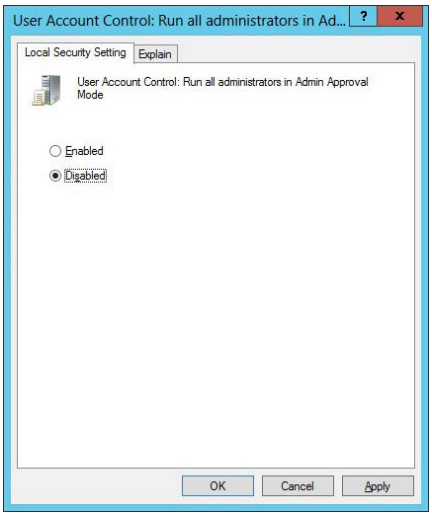
4. Double-click **Local Security Policy**.



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 Messaging has been installed.

Install Microsoft .Net Framework 4.7.2

Avaya IX Messaging requires Microsoft .Net Framework version 4.7.2 to be installed to support various features within the program. If it has not already been installed, the administrator must download it and install it manually.

Note: .Net Framework 4.7.2 is not installed by default. It may be part of Windows updates, optional updates, or not provided at all. Follow these instruction is it is not installed on your system, or if you do not know if it has been installed.

1. Open a web browser and go to the Microsoft web site. Search for .Net Framework 4.7.2 and install the application on the server. For example:
   https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows .
2. Download the file to your server drive. When ready, run the program to install this feature.

When finished, restart the server.

Installing Messaging for JITC on a Single Server

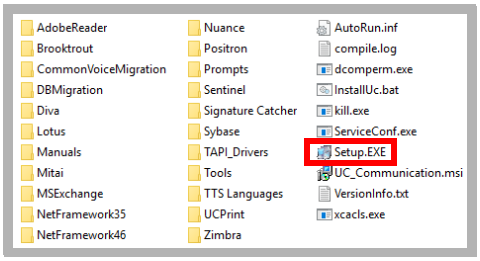
This section covers installing Messaging in Single Server configuration. If you are planning a High Availability installation, jump to page 336.

Continue with the Avaya IX Messaging 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.

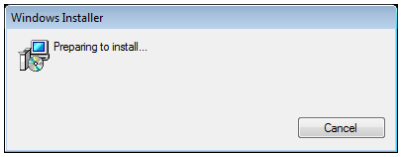
Installation

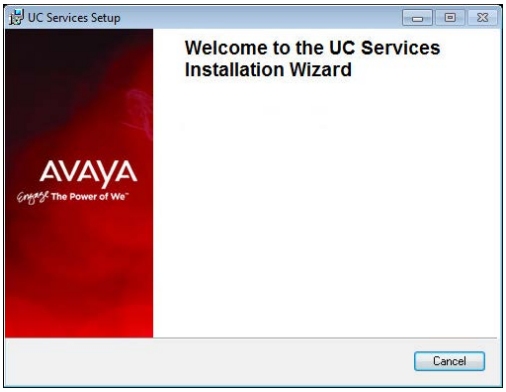
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic Update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

1. Download the installation file (see chapter 4). 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 IX Messaging onto your voice server.





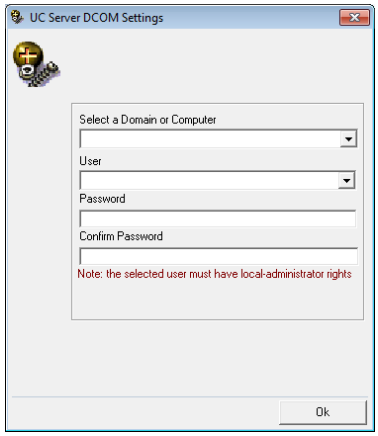
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging.

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.

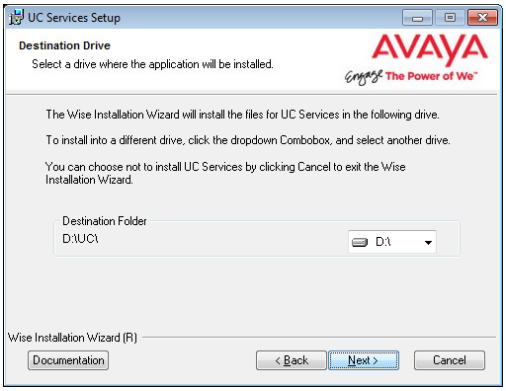


5. Review all the license agreements and select **I accept the license agreement**.

   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.

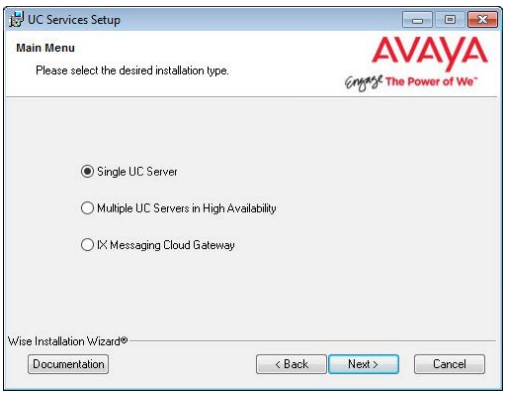
7. Enable **Single UC Server**.

   Click **Next**.

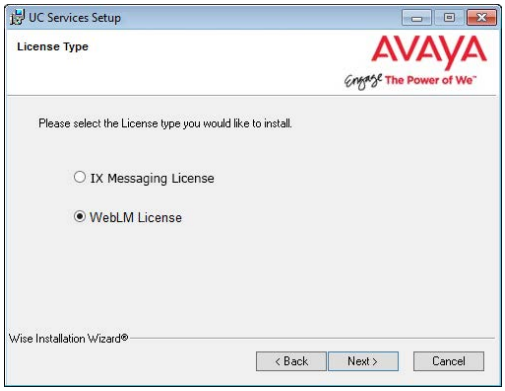
   Single UC Server: When operating Messaging on a single server computer.

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

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, 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.

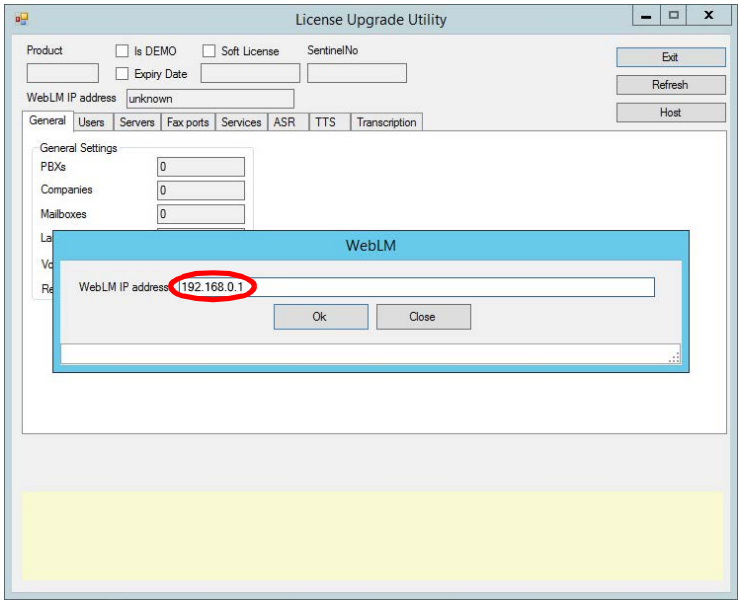


Note: If you select Messaging, go to **chapter 13, Installing the Messaging License**. When finished, return here and continue the installation from **step 11**. Skip step 9 through 10.

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.

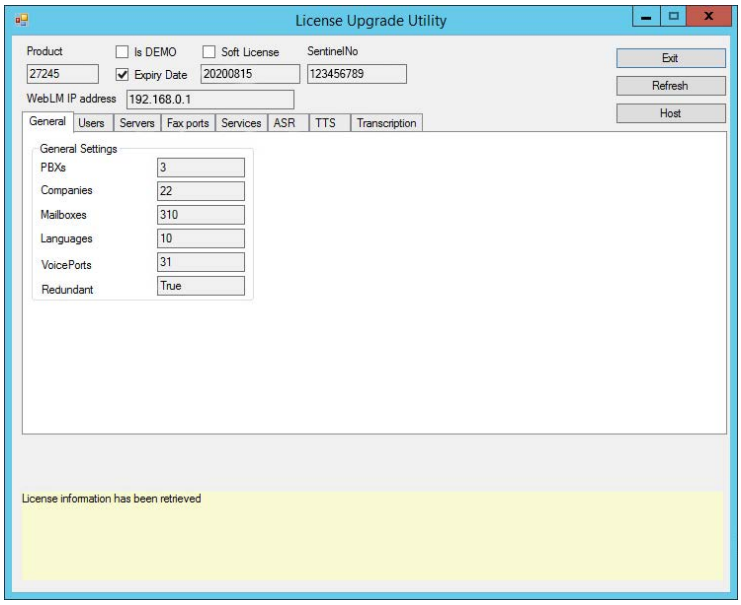
9. The **License Upgrade Utility** program opens and prompts you to enter the IP Address for the computer that houses the WebLM license engine.

   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 437.

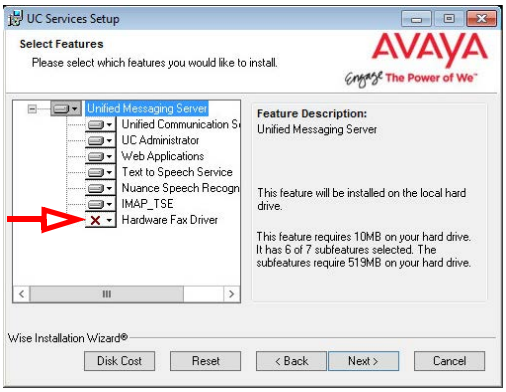
10. The utility will retrieve your license details from the server and display them here. Review the license details and click **Exit** when ready.



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



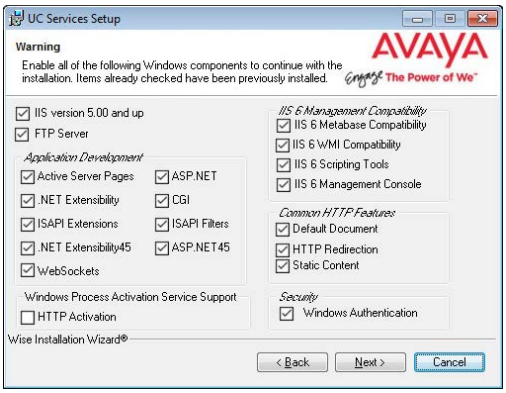
12. This screen shows all of the Windows roles and features that Messaging requires to operate properly.

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

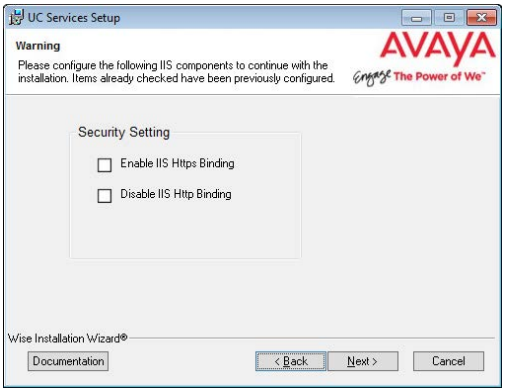
    For all items that are not checked, return to Windows and add any missing pieces to the operating system.

    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 Messaging requires to operate properly.



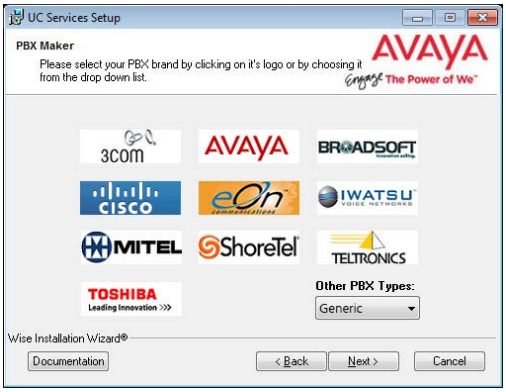
Note: This screen will only appear if one or more of the required settings has not been made on the computer.

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.

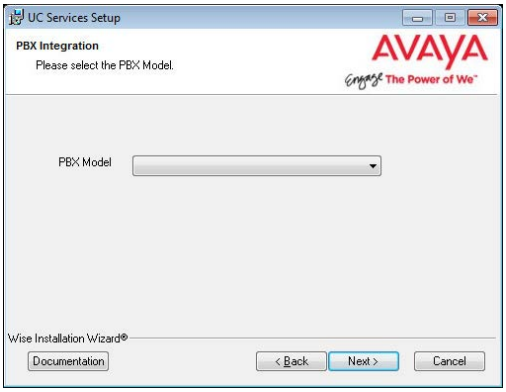
Note: The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

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



15. Select your PBX model from the dropdown menu.

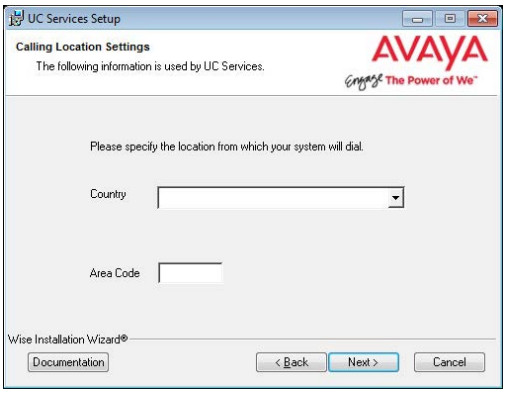
Click **Next**.



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.

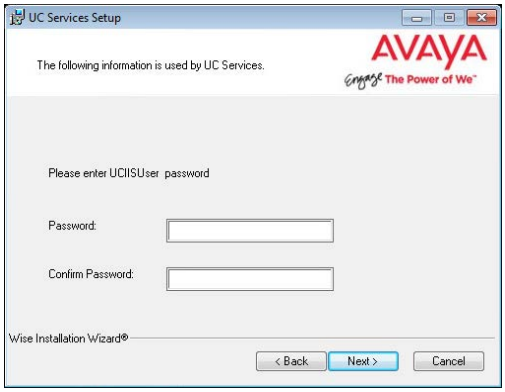
Select the country from the dropdown menu, and enter the area code in the space provided.

Click **Next** to continue.



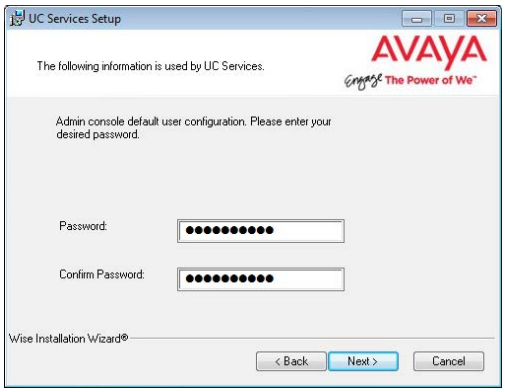
Note: If the Phone and Modem Settings under Windows Control Panel have already been configured, this step will not appear. The values entered there will be used automatically.

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

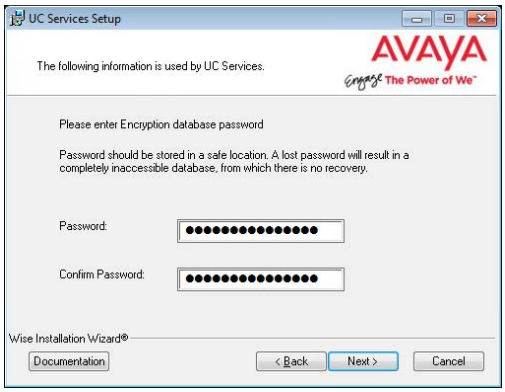


18. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of the system.

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 279 for a complete list of password requirements.

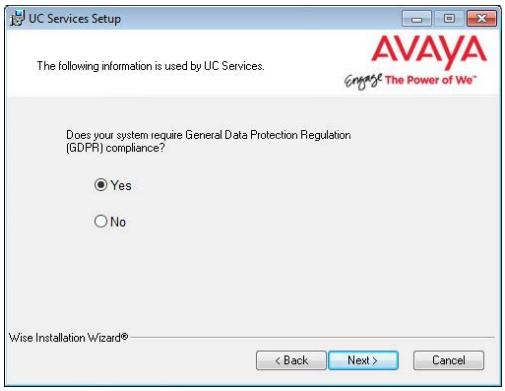


19. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.
This password must meet the requirements outlined **here**.



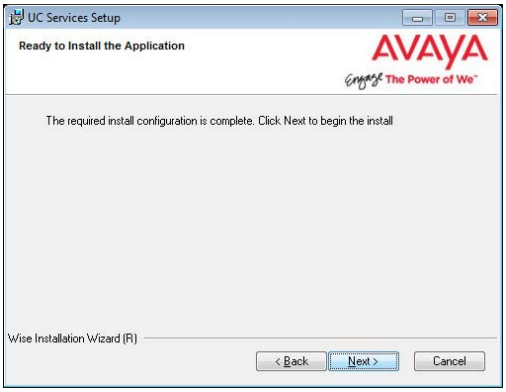
Important: Record this password and keep it in a safe location.
The loss of this password will lead to the complete and unrecoverable loss of data.

20. Choose either **Yes** or **No** to determine whether the system will apply General Data Protection Regulation (GDPR) compliance procedures to your data.
With this option enabled, users and callers are notified that personal information will be collected. This information can also be completely removed from the system upon request.

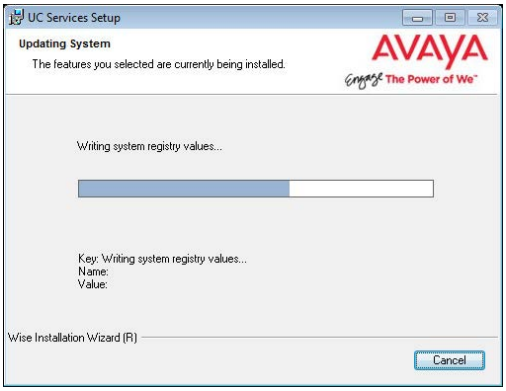


21. The preliminary information required for installation is now complete.

    Click **Next**.



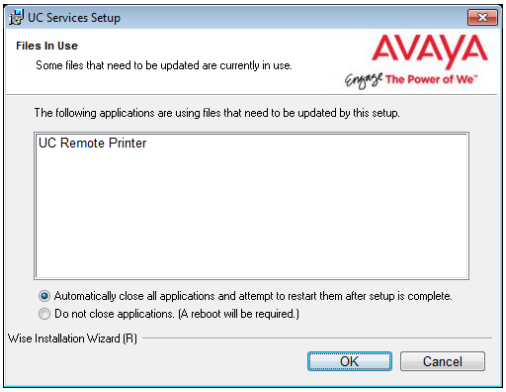
22. The selected components will now be installed. This process may take a while.



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

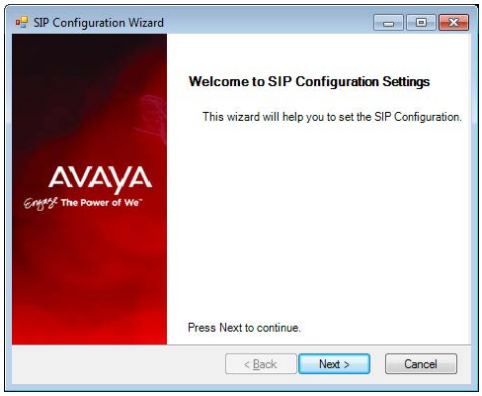
    Click **OK** when ready.

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

    Click **Next** to continue.

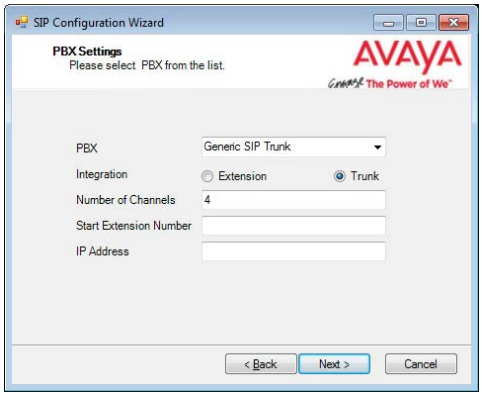


26. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.

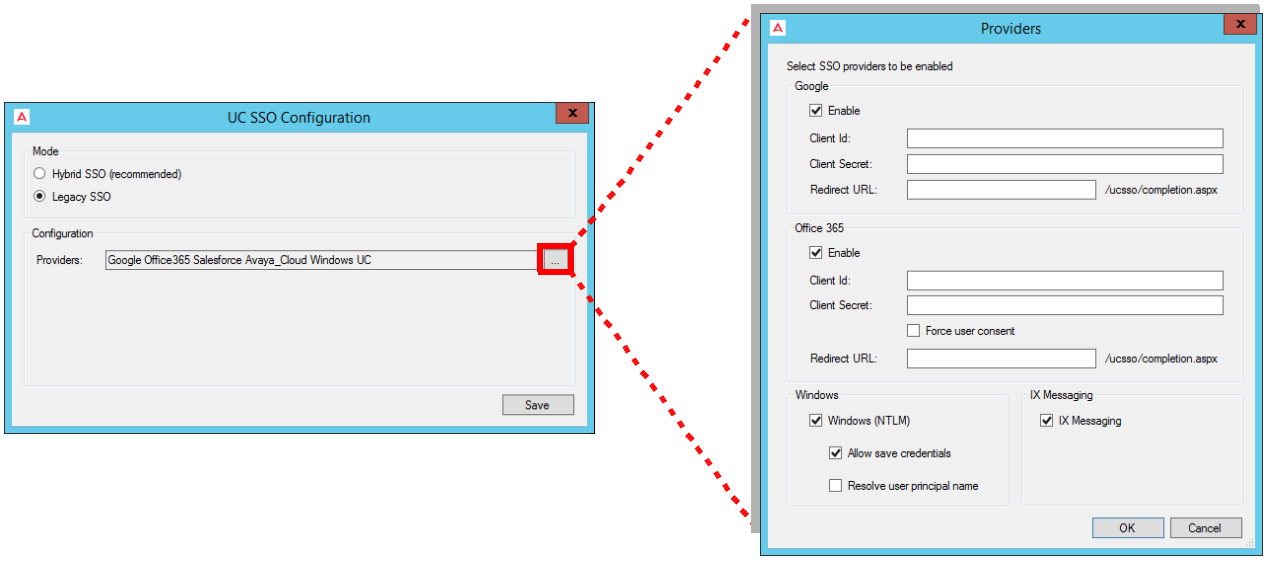
    Click **Next** when ready.



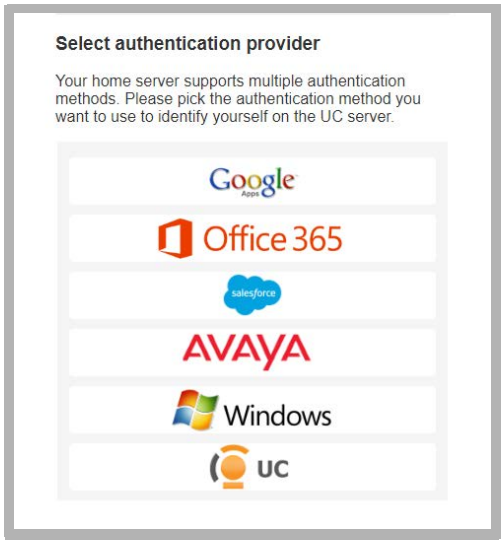
27. Confirm the information then click **Finish**.

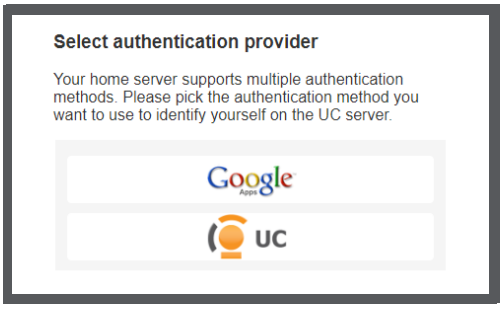
> **Note**: Depending on the type of SIP integration you'll be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Messaging programs folder after installation.

28. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



When clients / admins want access to these programs, they login using their credentials for one of the listed programs. They must have an account with that application before they can login.





Enable all that apply, then click **OK**.

Click **Save** when finished.

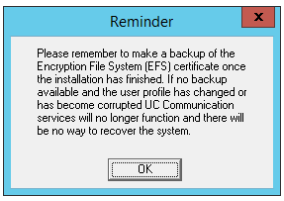
Important: The **Hybrid SSO** login procedure requires an active Internet connection. Only **Legacy SSO** can be used if Internet access is disabled / locked-down.

Note: For complete details on using legacy and hybrid SSO, refer to chapter 25 of this document.

29. 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**.

30. Verify that the Encryption File System (EFS) certificate has been saved to another secure location (see Backup and Restore the Certificate File on page 287). 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 Messaging for JITC with High Availability

This section covers installing Messaging for JITC in a High Availability (HA) configuration. If you are planning a Single Server installation, jump to page 318.

An HA installation involves up to 21 servers: 1 Primary 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 IX Messaging 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:

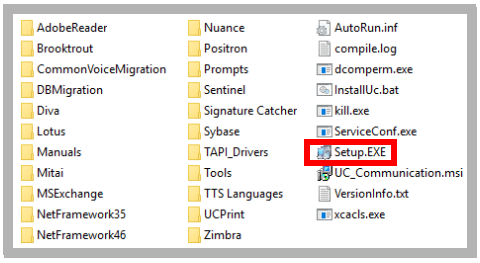
- **Primary Voice Server**
- **Consolidated Server**
- **Secondary Voice Servers**

Warning: It is important to login to the servers (Primary, Consolidated and all Secondaries) using a domain account that has full administrative rights on the local machine.

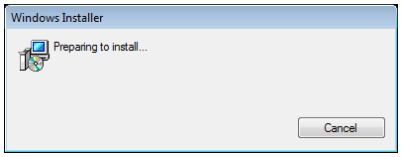
Primary Voice Server

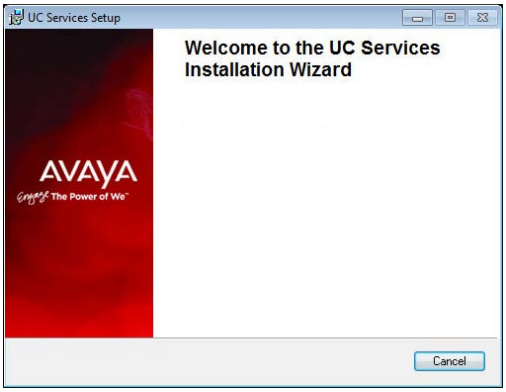
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic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

1. Download the installation file (see chapter 4). 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 IX Messaging onto the Primary server.





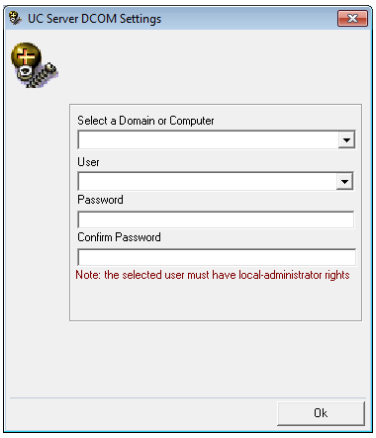
3. Once the Windows components have been verified, click **Next** to begin the installation.

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 Messaging.

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.

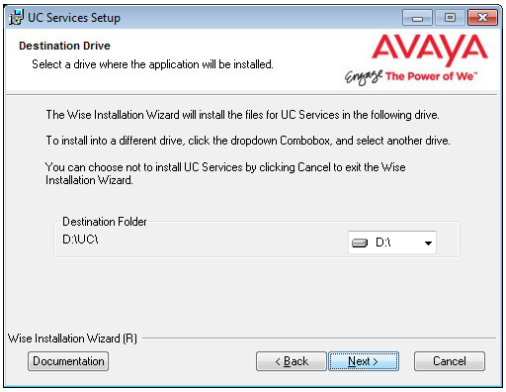


5. Review the license agreement and select **I accept the license agreement**.

   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.

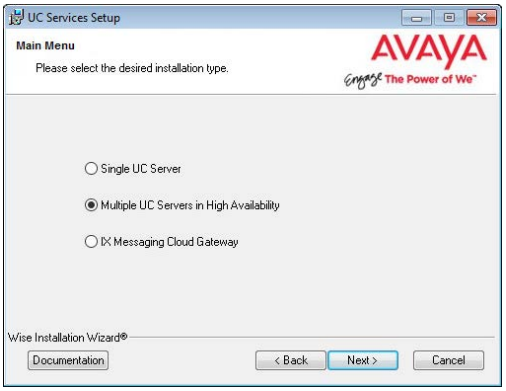
7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

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

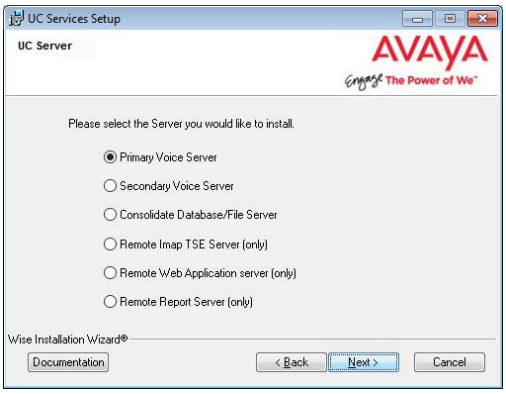
   Multiple UC Servers in High Availability: When running Messaging in High Availability mode for redundancy.

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, Install and Configure Cloud Gateway for complete details.

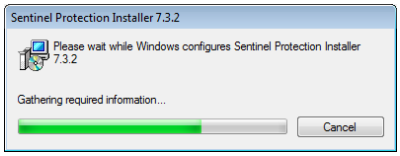


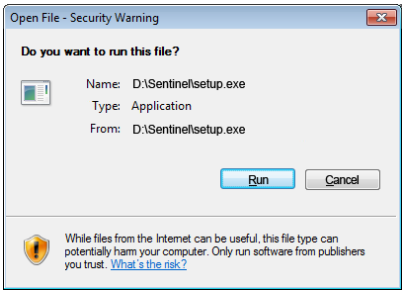
8. Select **Primary Voice Server**.

   Click **Next**.



9. When prompted, click **Run** to confirm the installation. The necessary files will be installed.

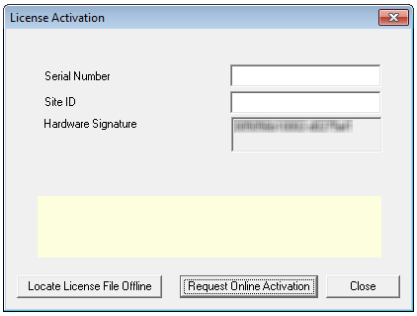




> **Note**: This screen may not appear, depending upon your system settings.

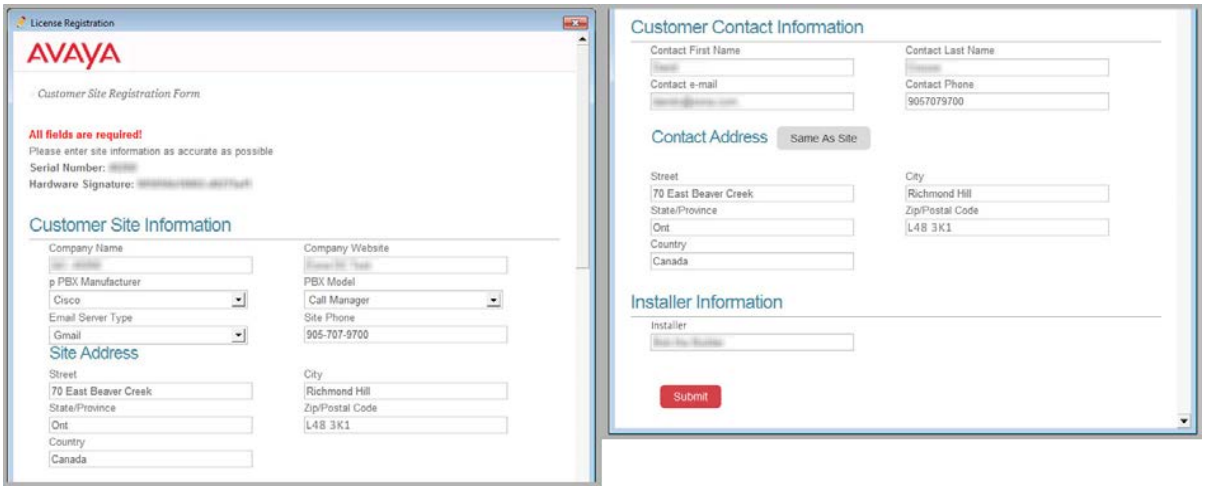
10. Once the process is complete the licensing screen will appear. It is recommended that you use Online Activation whenever possible. To do so, simply enter the **Serial Number** and **Site ID** .

    Click **Request Online Activation** when finished.

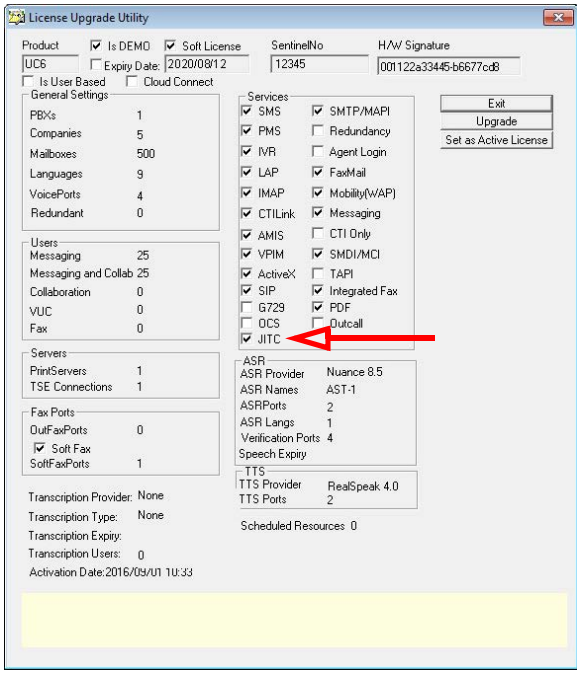


Warning: It is essential that the system/PC clock be properly set **before** activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

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**.

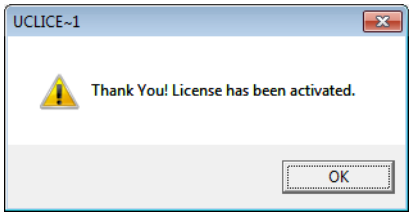


Caution: Verify that the JITC checkbox has been enabled. If it is empty, pause the installation immediately and contact your dealer. The license must be upgraded **before** you continue.

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**.



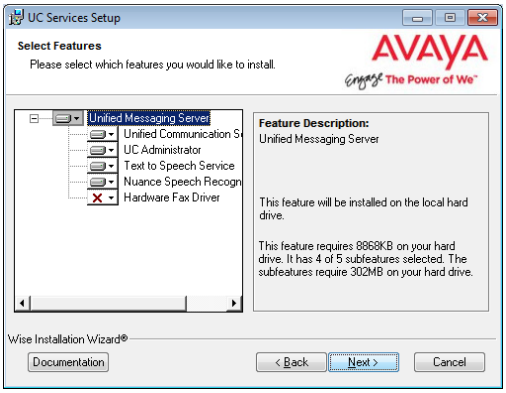
14. Click **Exit** to close the license window and continue with the installation.

15. This reminder may appear.

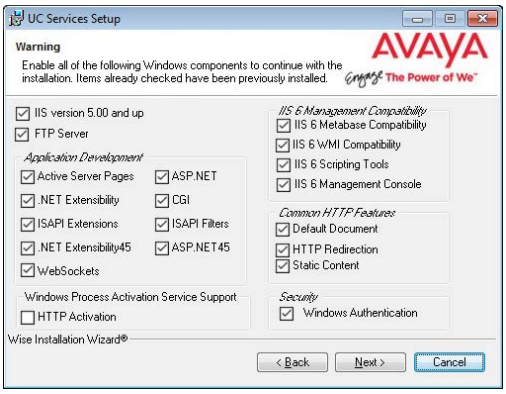
    Click **OK**.

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

    Click **Next**.



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



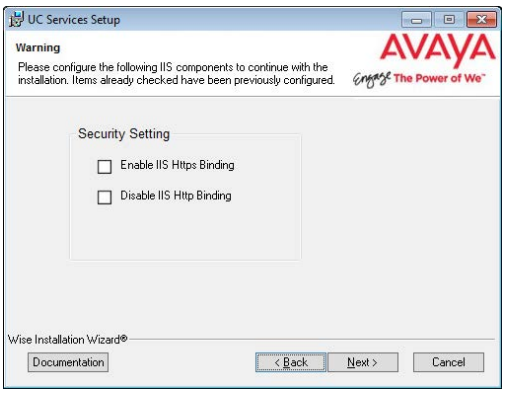
Note: This screen will only appear if one or more required components are **not** installed on the computer.

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 Messaging requires to operate properly.



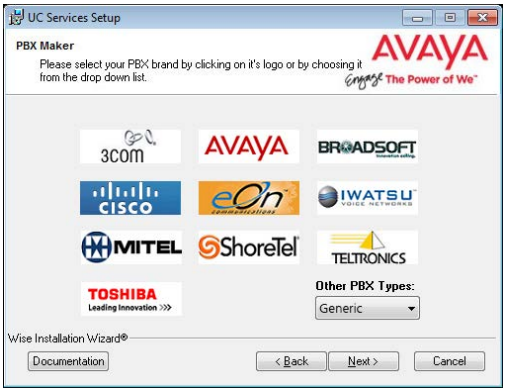
Note: This screen will only appear if one or more of the required settings has not been made on the computer.

For all items not checked, refer to **IIS Certificate Bindings** for configuration details.

Click **Next** when finished.

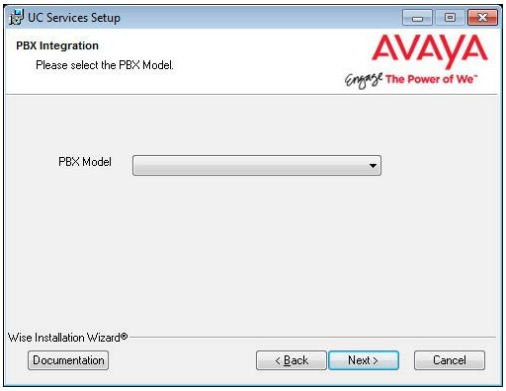
Note: The installation will not continue until all of the required IIS settings have been made.
This screen does not refresh until you click **Next**.

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



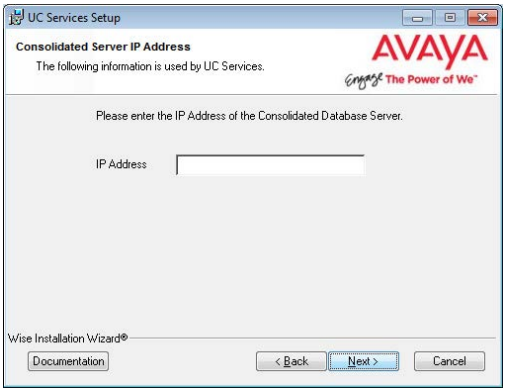
20. Select your PBX model from the dropdown menu.

    Click **Next**.



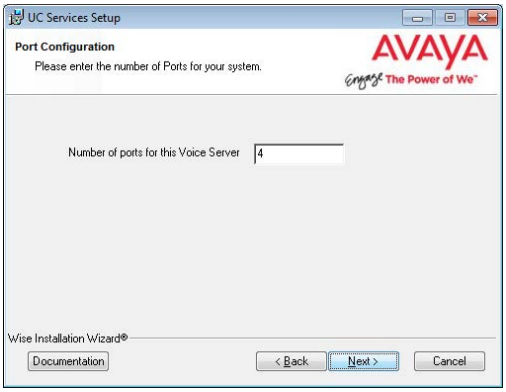
21. Enter the **IP Address** for the Consolidated Server.

    Click **Next**.



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

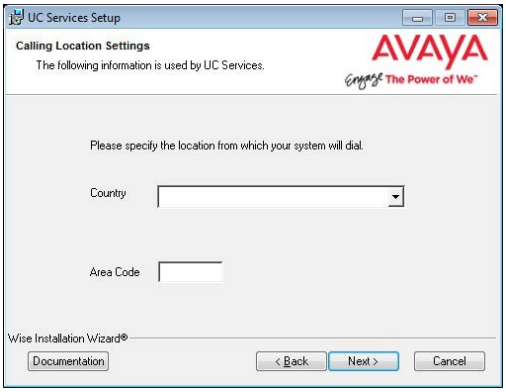
    Click **Next**.



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.

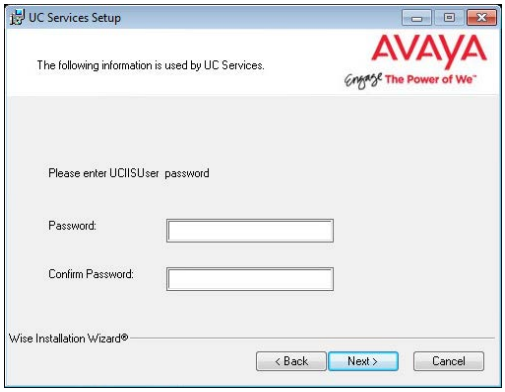
    Select the country from the dropdown menu, and enter the area code in the space provided.

    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.

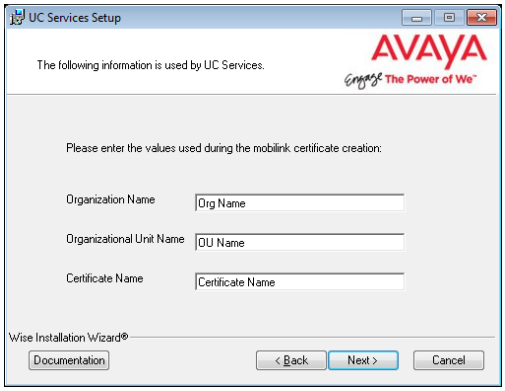


25. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.
    This password must meet the requirements outlined **here**.

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.

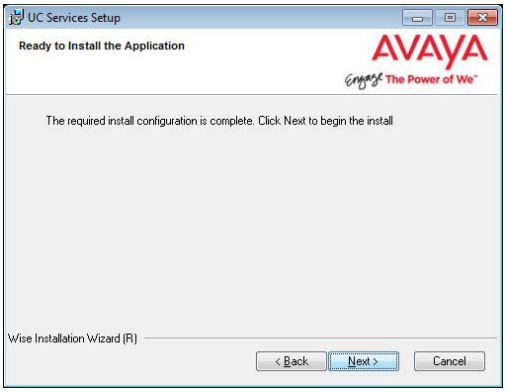
26. Enter the values in the spaces provided. These are provided with the certificate (either self-signed or a CA signed).

    These values are used when configuring the certificates on page 394.

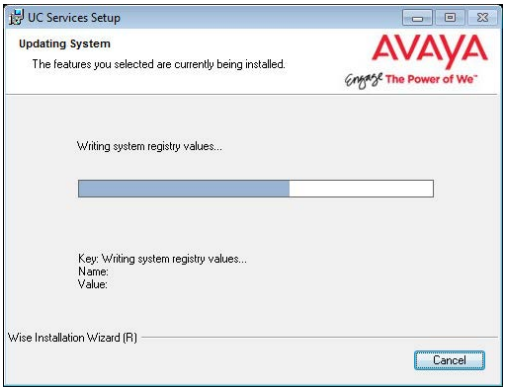


27. The preliminary information required for installation is now complete.

    Click **Next**.



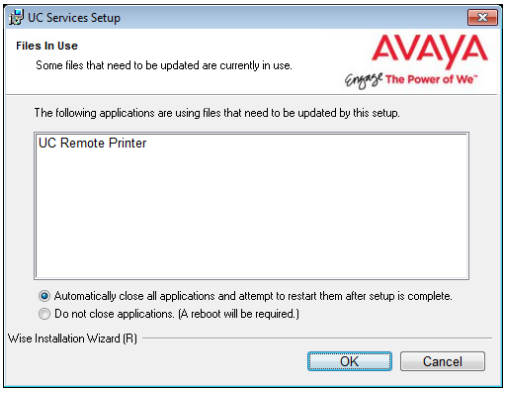
28. The selected components will now be installed. This process may take a while.



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.

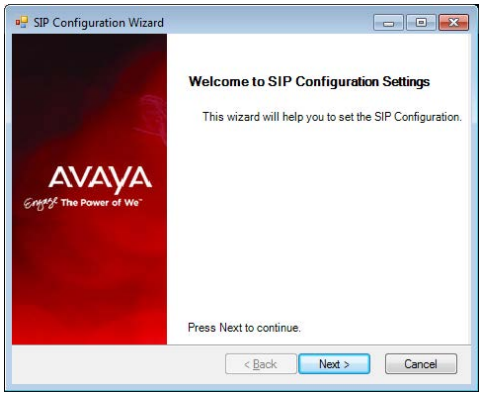
    Click **OK** when ready.

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.

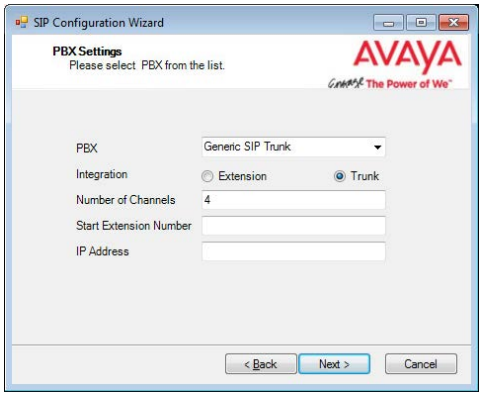


32. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.

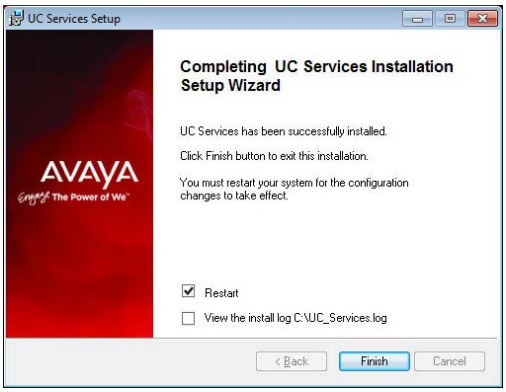


33. Confirm the information then click **Finish**.

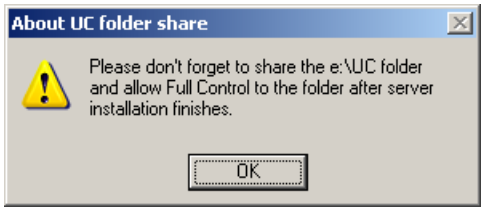
> **Note**: Depending on the type of SIP integration you'll be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Messaging programs folder after installation.

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**.

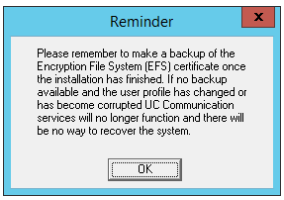


35. This alert is to remind you to properly share the UC installation folder (see page 256 for details).



> **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 287). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.

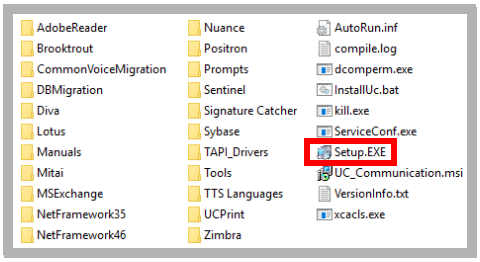


Click **OK** to restart the computer.

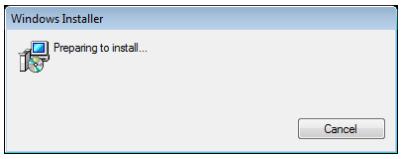
Consolidated Server

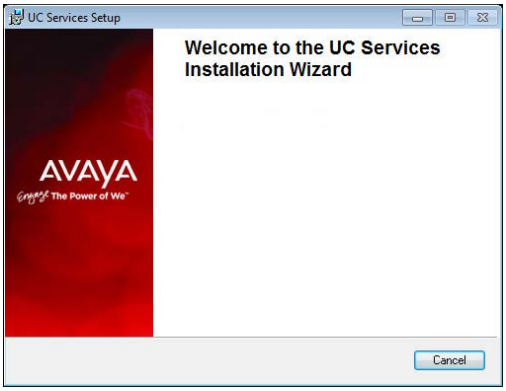
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic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

1. Download the installation file (see chapter 4). 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 IX Messaging onto your Consolidated server.





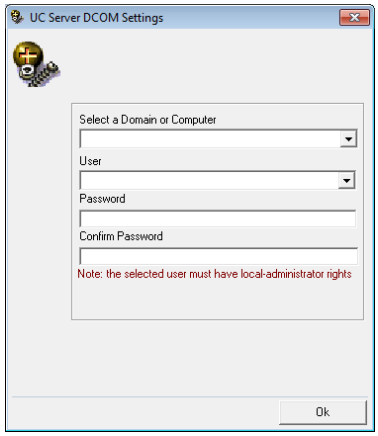
3. Once the Windows components have been verified, click **Next** to begin the installation procedure.

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 Messaging.

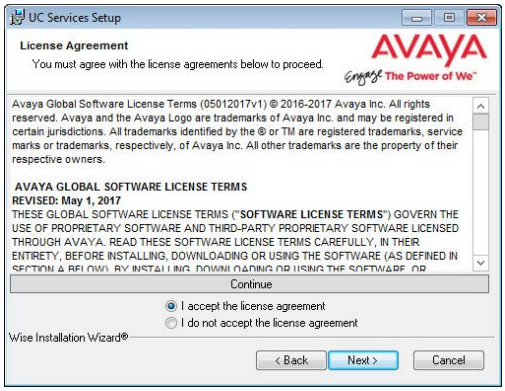
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

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



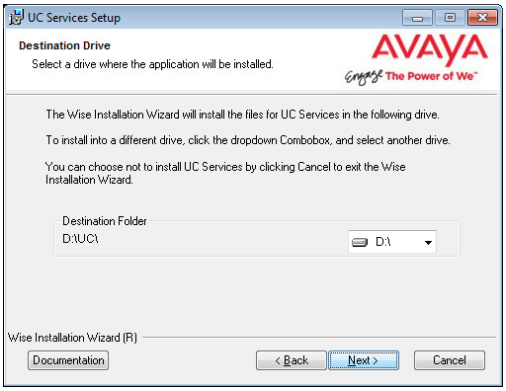
5. Review all the license agreements and select **I accept the license agreement**.

   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.

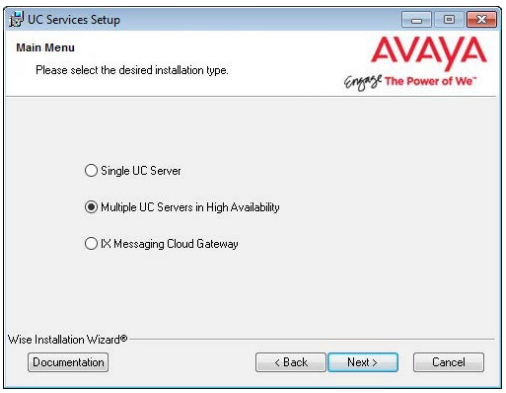
7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

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

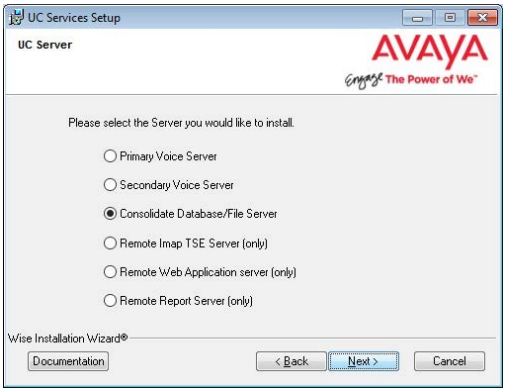
   Multiple UC Servers in High Availability: When running Messaging in High Availability mode for redundancy.

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, Install and Configure Cloud Gateway for complete details.



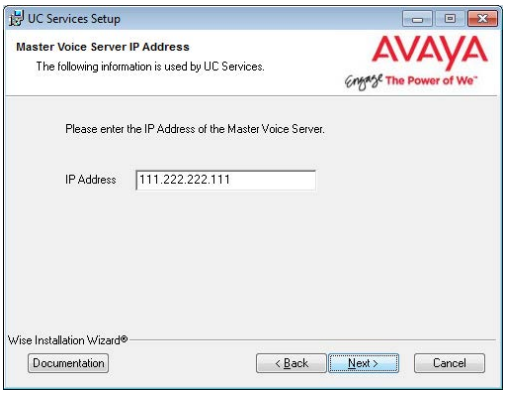
8. Select **Consolidated Database/File Server**.

   Click **Next**.



9. Enter the **IP address** for the Primary voice server.

   Click Next.

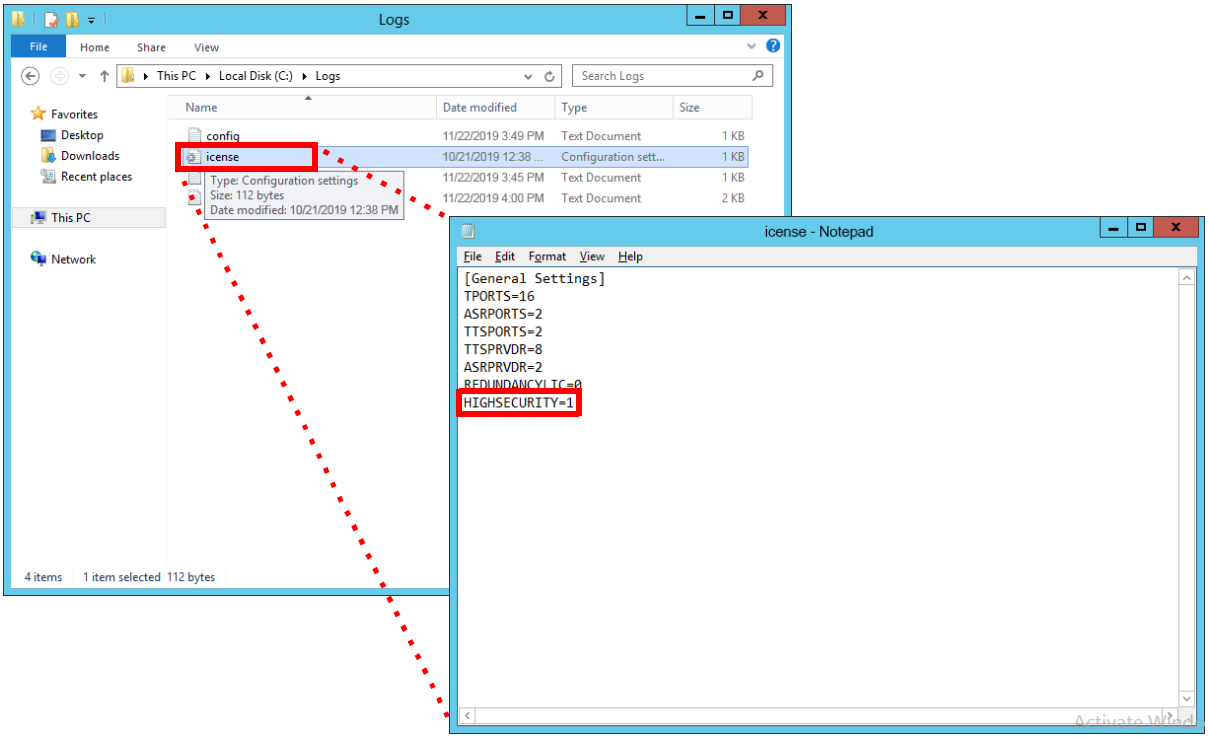


10. On the C drive, open the **Logs** folder.

    Open the file named **icense** using any text editor (e.g. Notepad).

    Verify **Highsecurity=1**. If it does not, verify that the same file (*IXM Installation drive*:\UC) on the Primary voice server does have this setting. If the setting is valid on the Primary, there is a connection or a sharing problem between the two machines. If the Primary is not correctly set, contact your reseller for an updated license.

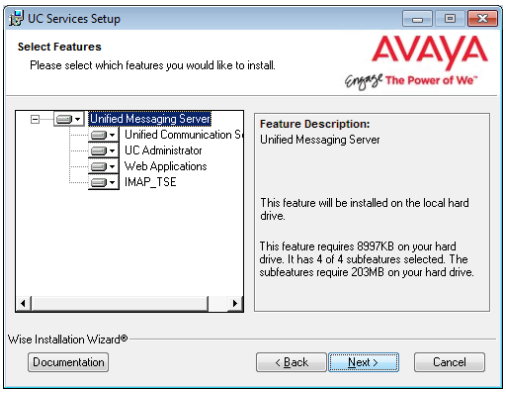
    Once any connection or sharing problems have been fixed, return to step 9 and check again for this file.



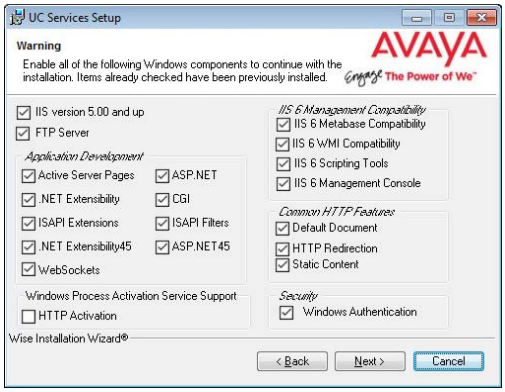
Caution: Do not continue the installation until this file has the Highsecurity setting equal to 1.

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.



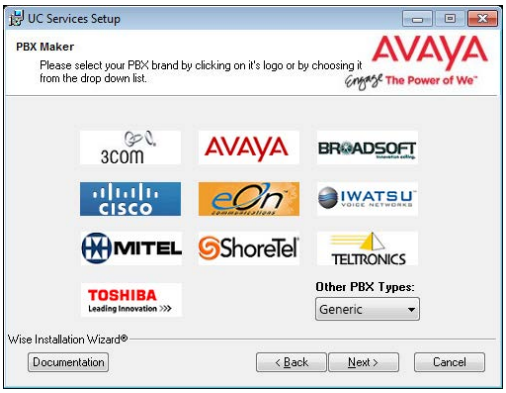
Note: This screen will only appear if one or more required components are not installed on the server.

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

Click **Next** when finished.

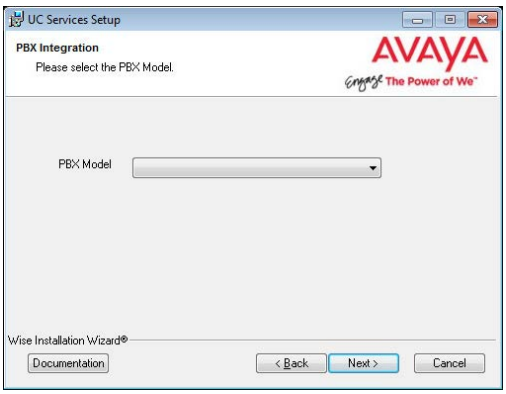
Note: The installation will not continue until all of the required components have been added to the server.
The screen does not refresh until you click **Next**.

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



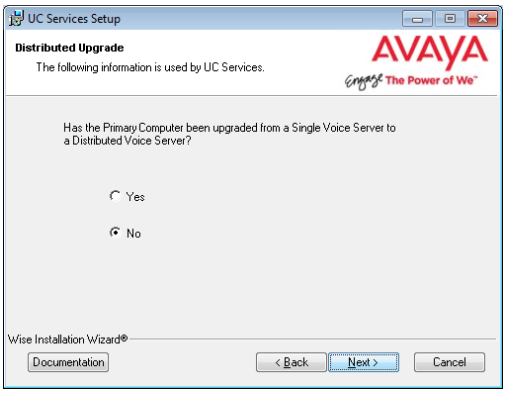
14. Select your PBX model from the dropdown menu.

Click **Next**.

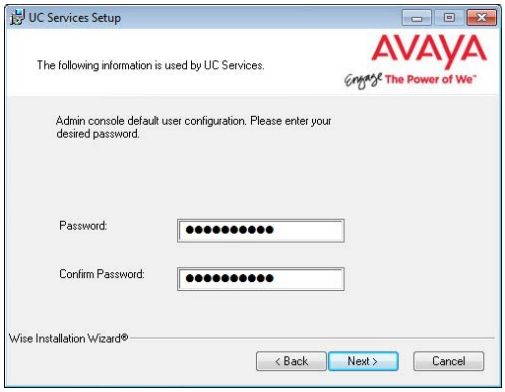


15. Unless the Primary Server has been upgraded, enable **No**.

Click **Next**.

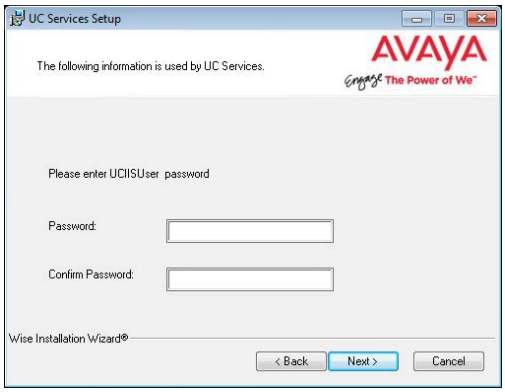


16. Enter a password to provide administrator only access to the system. This account password is used to configure the many elements of the system.

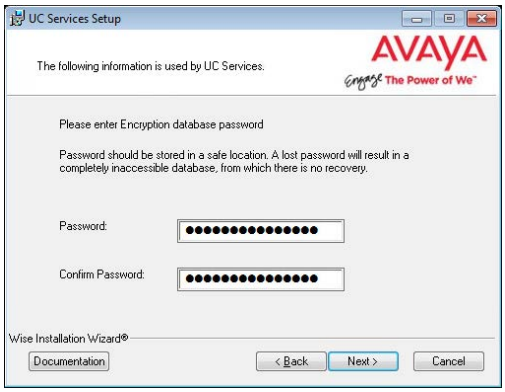


Hint: Passwords cannot be left blank. In a high-security installation, all passwords must contain letters, numbers and characters, and must be at least 15 characters long. See page 279 for a complete list of password requirements.

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

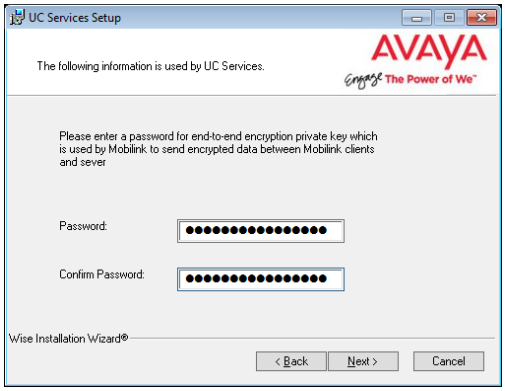


18. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.
This password must meet the requirements outlined **here**.



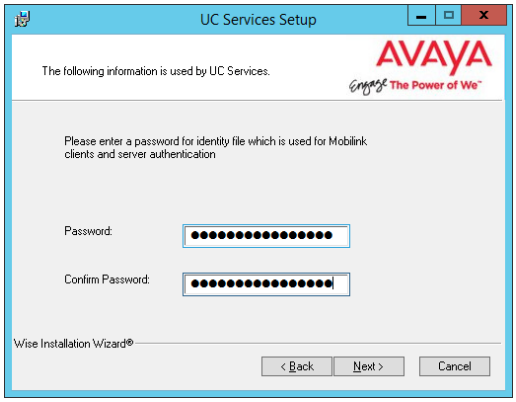
Important: Record this password and keep it in a safe location.
The loss of this password will lead to the complete and unrecoverable loss of data.

19. Enter an encryption password to protect Mobilink communications.



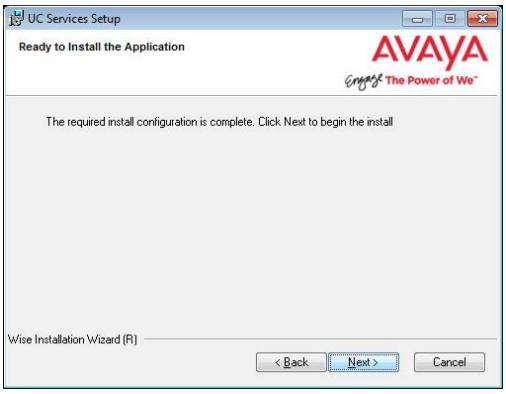
20. Enter a password for the Mobilink identity file.

    Click **Next**.

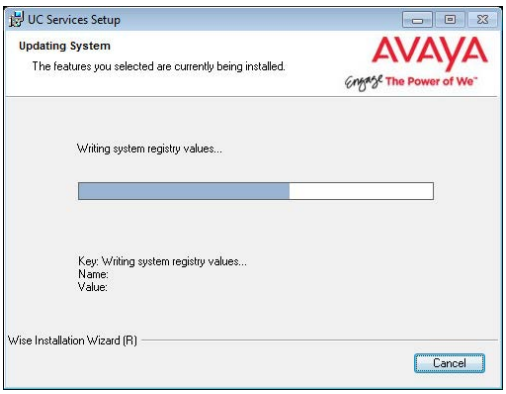


21. The preliminary information required for installation is now complete.

    Click **Next**.



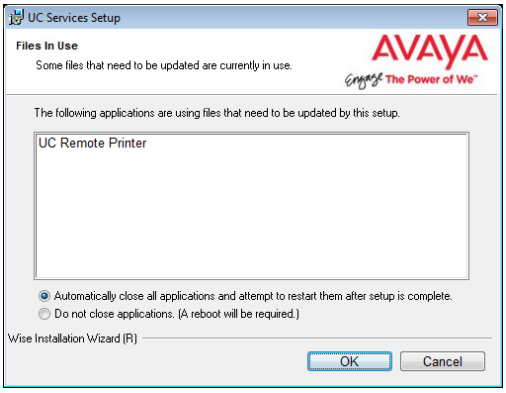
22. The selected components will now be installed. This process may take a while.



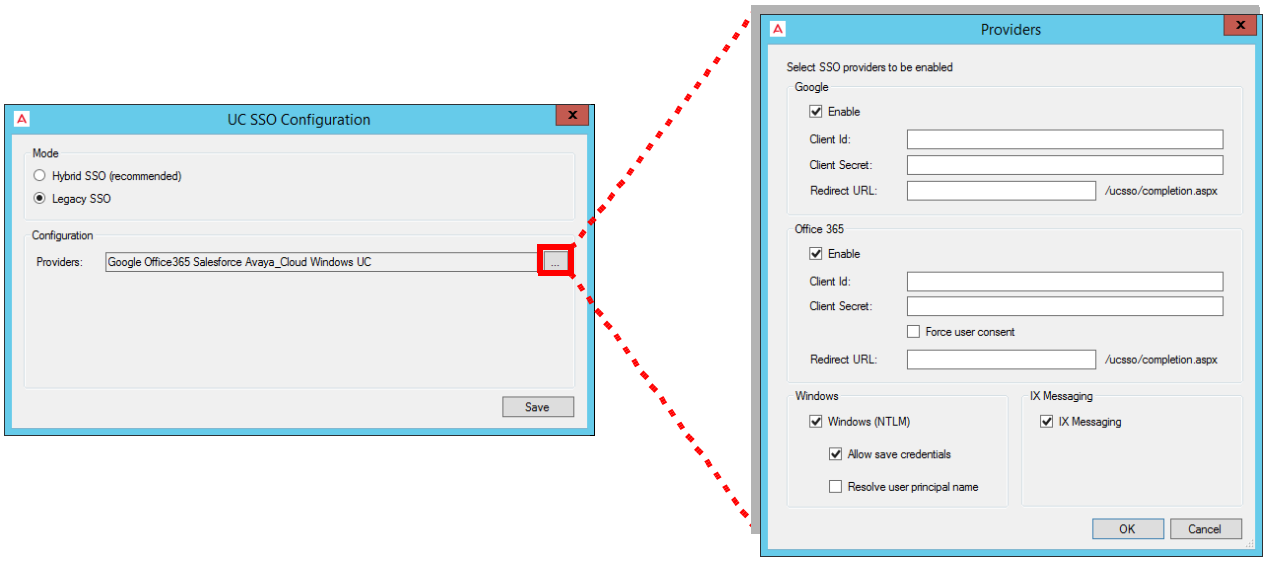
23. If you are warned about components being in use, either use the **Automatically Close** option or manually close the process which is interfering with the installation.

    Click **OK** when ready.

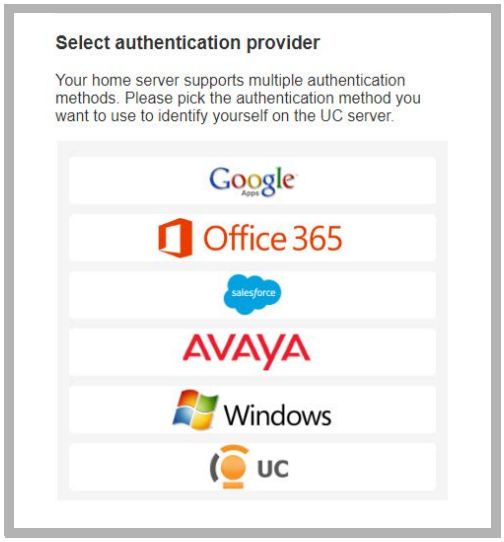
24. After all the components are copied, you may be asked to provide the settings for the **PBX** that you have chosen. Since this process varies greatly from system to system, please ensure that you configure your site's PBX exactly as required.

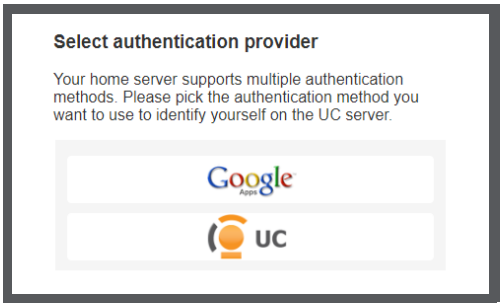


25. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



When clients / admins want access to these programs, they login using their credentials for one of the listed programs. They must have an account with that application before they can login.





Enable all that apply, then click **OK**.

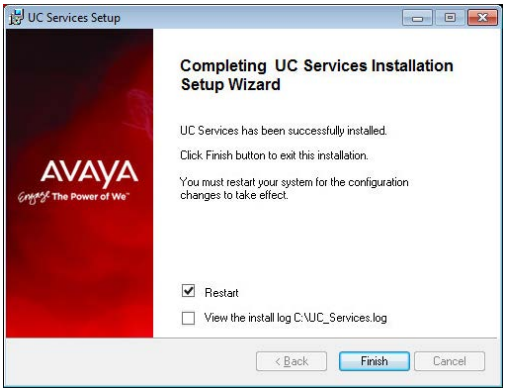
Click **Save** when finished.

Important: The **Hybrid SSO** login procedure requires an active Internet connection. Only **Legacy SSO** can be used if Internet access is disabled / locked-down.

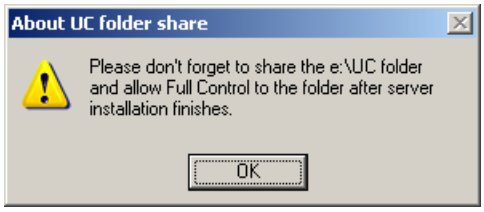
Note: For complete details on using legacy and hybrid SSO, refer to chapter 25 of this document.

26. 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**.

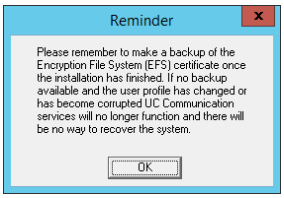


27. This alert is to remind you to properly share the UC installation folder (see page 256 for details).



Important: The installation folder **MUST** be shared before proceeding with the Consolidated and Secondary server installations.

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 287). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.



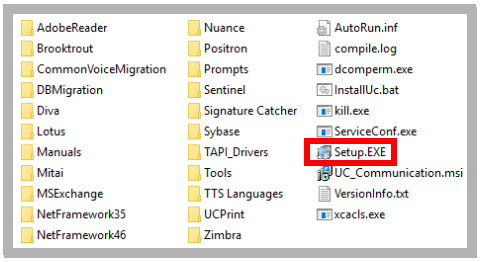
Click **OK** to restart the computer.

Secondary Voice Servers

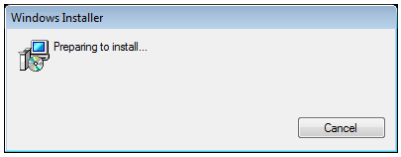
Up to 19 Secondary servers can be added to a High Availability environment. Each must be given its own, unique identification number (e.g. 2-20) which is assigned during installation.

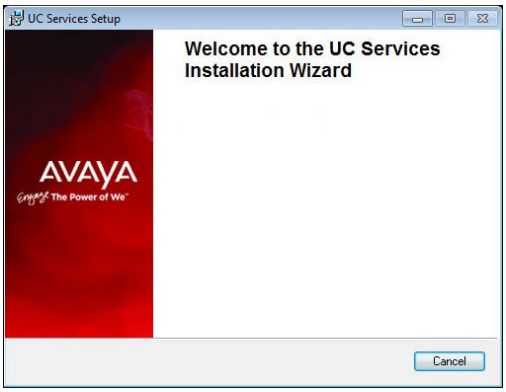
Note: Make sure that all of the necessary Services for your operating system have been installed before proceeding with the installation. Refer to the appropriate section of the Server Installation Guide for further details. Also make sure that **Windows Firewall is disabled**, and that **Windows Automatic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

1. Download the installation file (see chapter 4). 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 IX Messaging onto all of your Secondary servers.





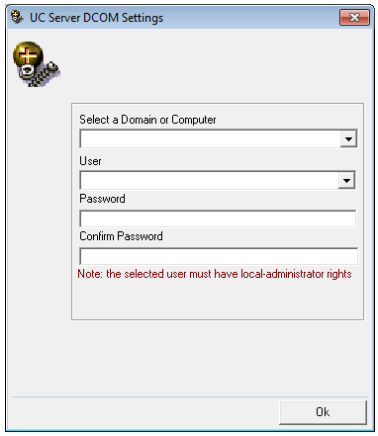
3. Once the Windows components have been verified, click **Next** to begin the installation procedure.

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 Messaging.

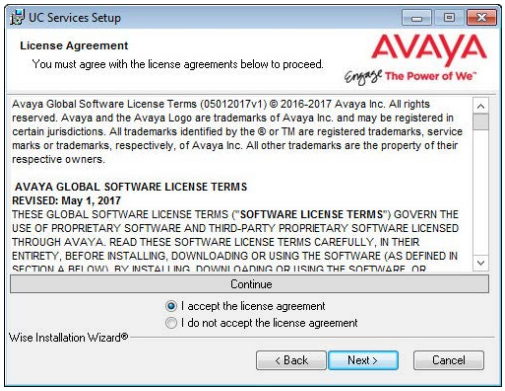
4. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

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



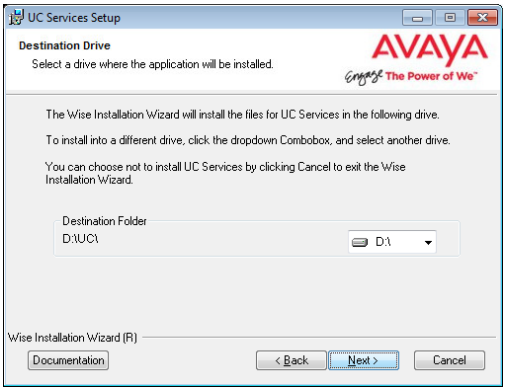
5. Review all the license agreements and select **I accept the license agreement**.

   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.

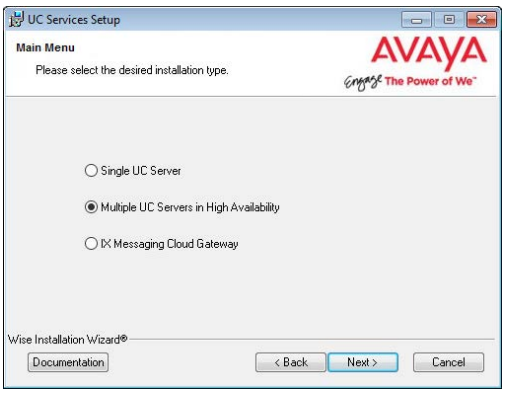
7. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.

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

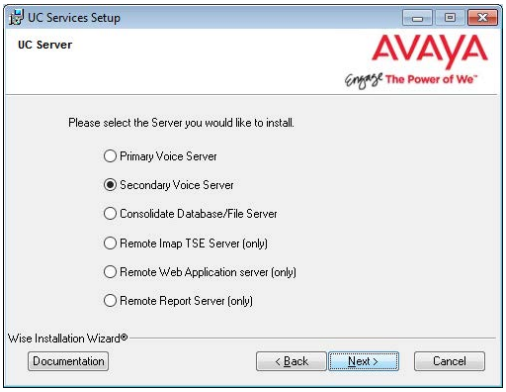
   Multiple UC Servers in High Availability: When running Messaging in High Availability mode for redundancy.

   IX Messaging Cloud Gateway: Gateway allows end-to-end synchronization between the Avaya Aura Messaging server and Google's Gmail using Avaya IX Messaging message sync and the CSE. Refer to chapter 15, Install and Configure Cloud Gateway for complete details.



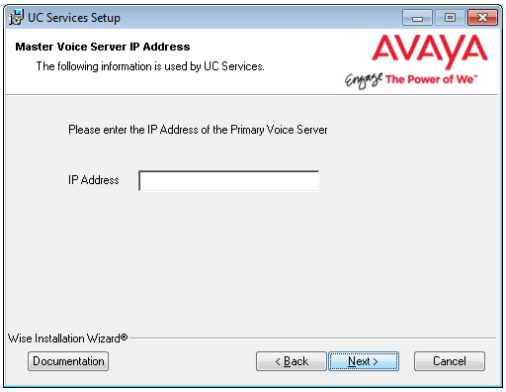
8. Select **Secondary Voice Server**.

   Click **Next**.



9. Select the **IP Address** of the Primary Voice Server.

   Click **Next**.

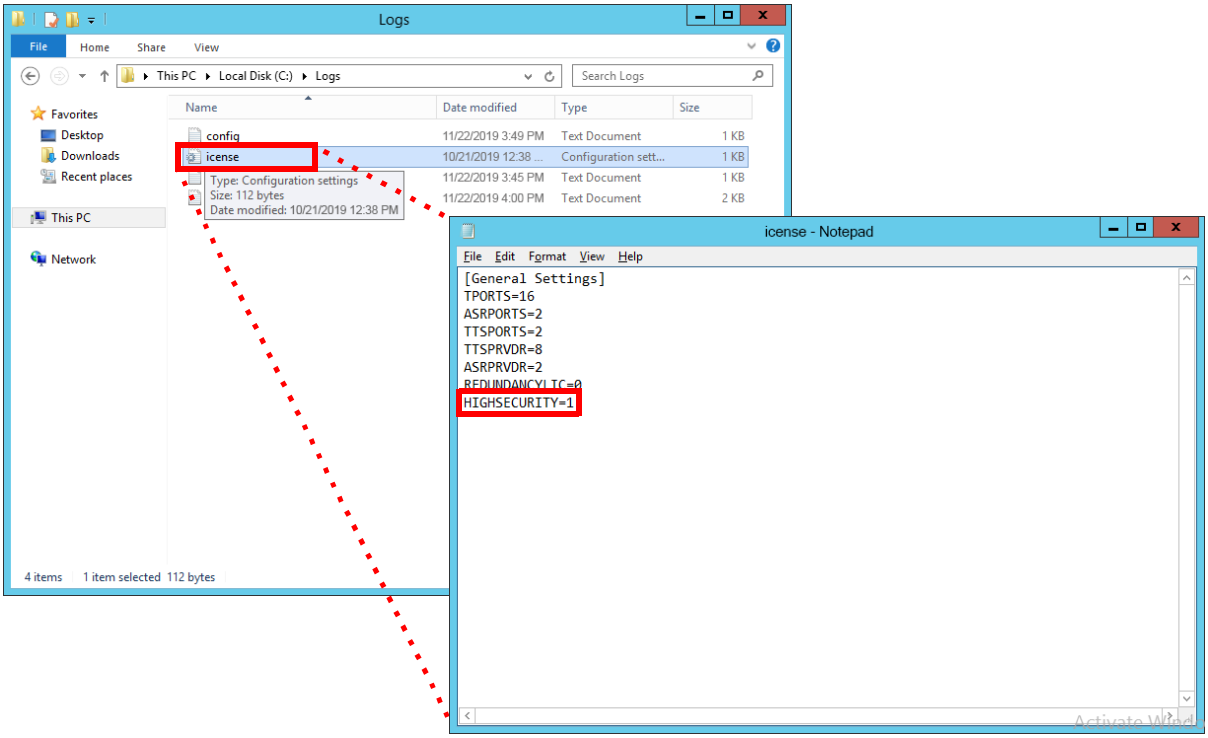


10. On the Messaging installation drive, open the **Logs** folder.

    Open the file named **license** using any text editor (e.g. Notepad).

    Verify **Highsecurity=1**. If it does not, verify that the same file (IXM Installation drive:\UC) on the Primary voice server does have this setting. If the setting is valid on the Primary, there is a connection or a sharing problem between the two machines. If the Primary is not correctly set, contact your reseller for an updated license.

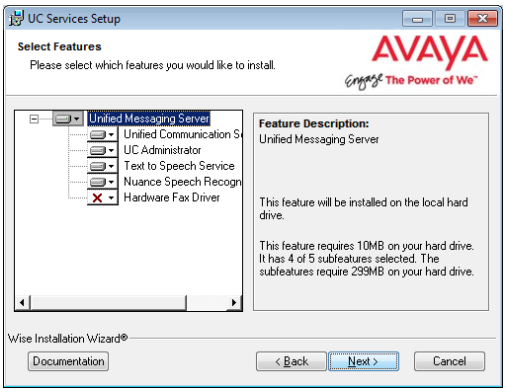
    Once any connection or sharing problems have been fixed, return to step 8 and check again for this file.



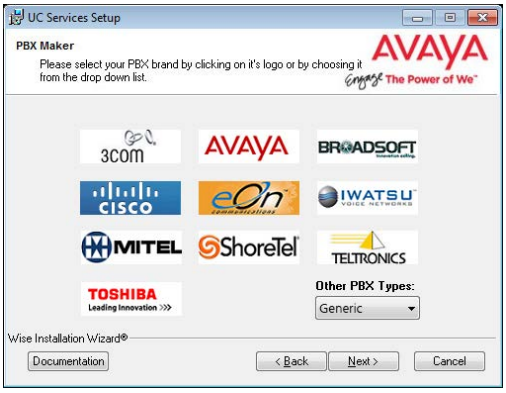
Caution: Do not continue the installation until this file has the **HIGHSECURITY** setting equal to **1**.

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

    Click **Next**.

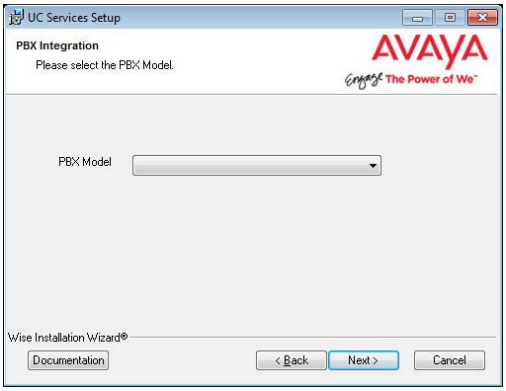


12. Select your PBX Brand then click **Next**.



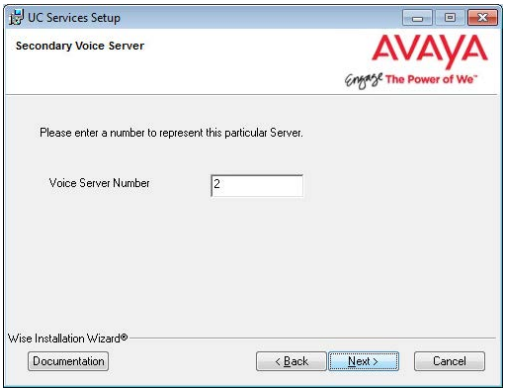
13. Select your PBX model from the dropdown menu.

    Click **Next**.



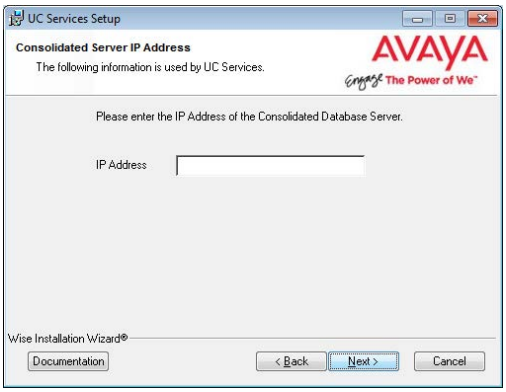
14. Enter the number for this Secondary Server. Each Secondary must have a unique number assigned between 2 and 20.

    Click **Next**.



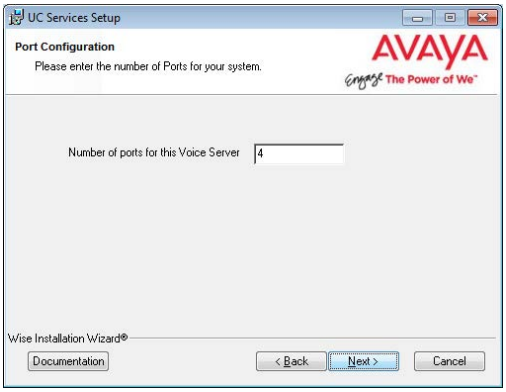
15. Enter the **IP Address** for the Consolidated Server.

    Click **Next**.

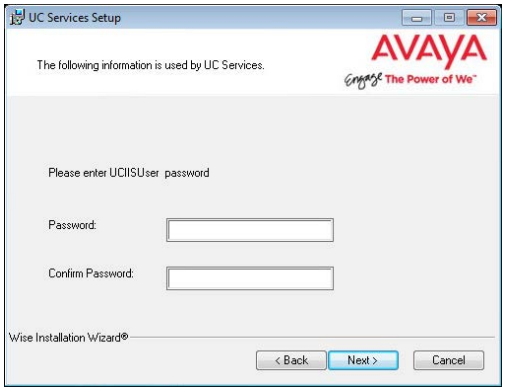


16. Enter the number of ports your system will use.

    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.

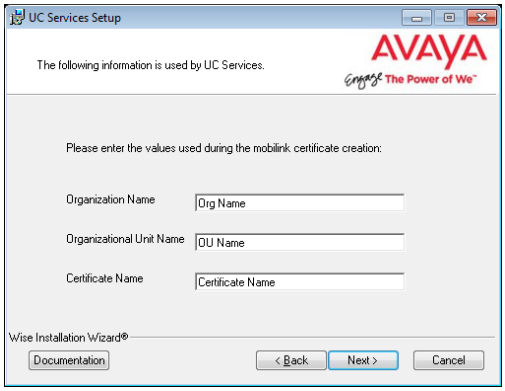


18. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.
    This password must meet the requirements outlined **here**.

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.

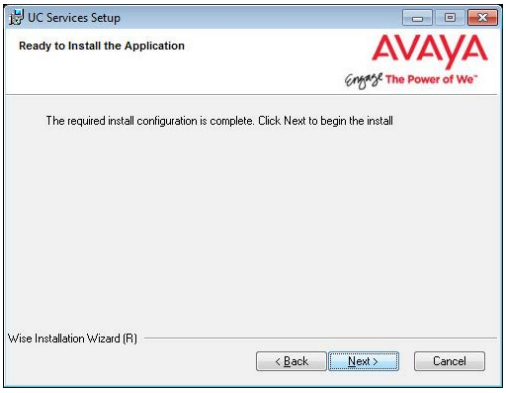
19. Enter the values in the spaces provided. These are provided with the certificate.

    These values must be the same as are used during the Primary voice server installation (step 26).

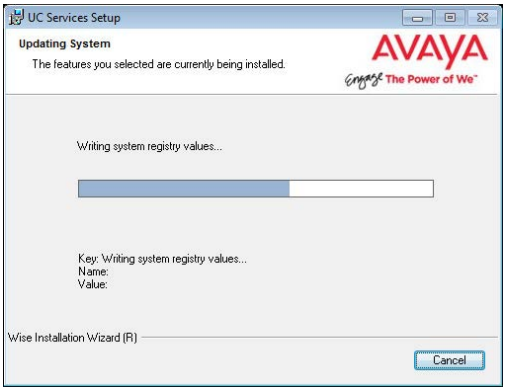


20. The preliminary information required for installation is now complete.

    Click **Next**.



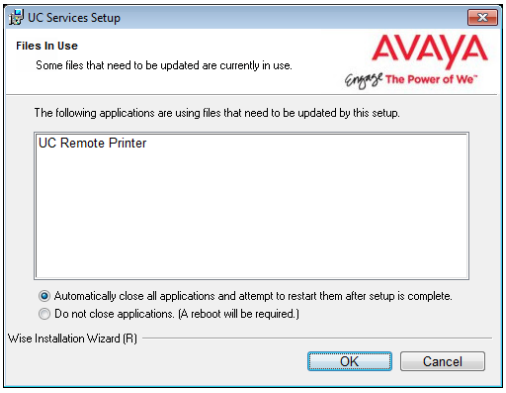
21. The selected components will now be installed. This process may take a while.



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.

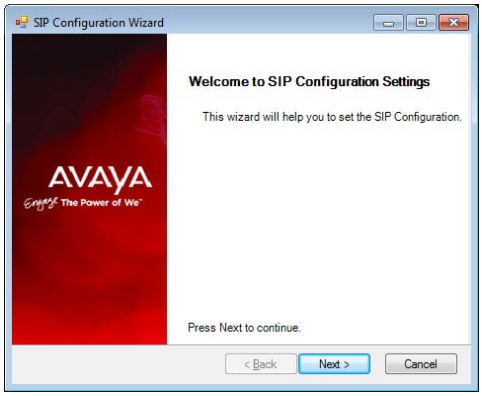
    Click **OK** when ready.

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.

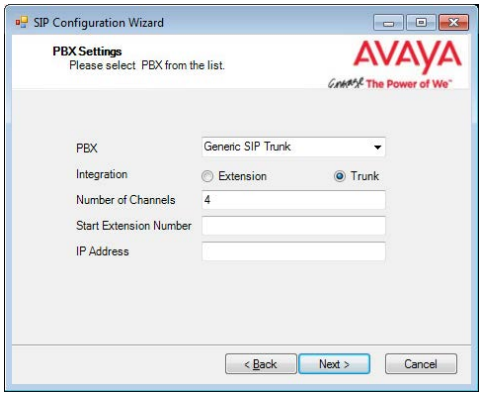


25. Fill out all required information. The **PBX** and the **Number of Channels** fields are automatically populated. Enter the **IP Address** of the PBX.

    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.

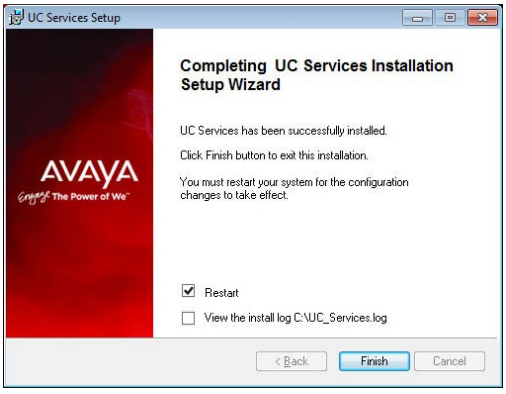


26. Confirm the information then click **Finish**.

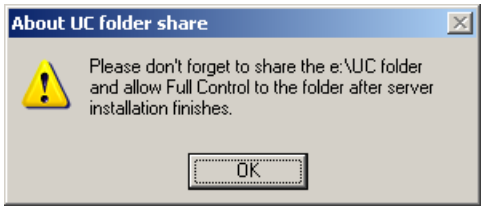
> **Note**: Depending on the type of SIP integration you will be using, you may have to fine tune the settings from the **SIP Configuration Tool** in order for the system to function properly. The SIP Configuration Tool can be found in the Messaging programs folder after installation.

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**.

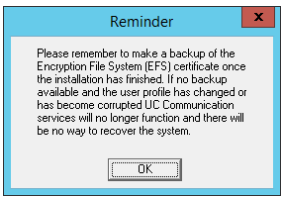


28. This alert is to remind you to properly share the UC installation folder (see page 256 for details).



> **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 287). If the certificate becomes corrupted, UC Communication will no longer function and are unrecoverable without this backup file.



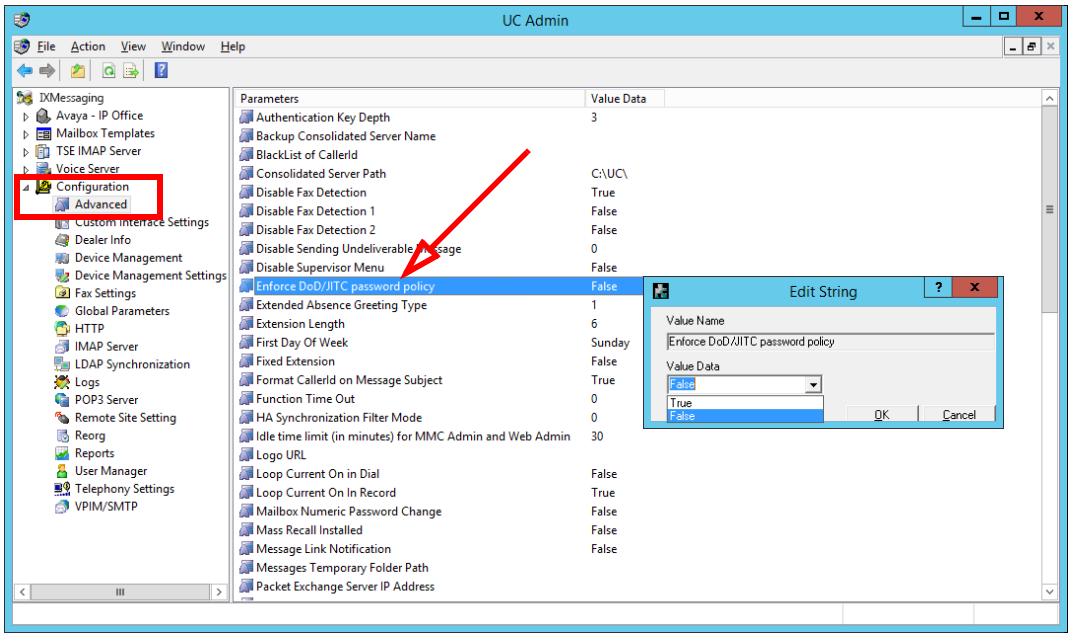
Click **OK** to restart the computer.

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 password 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, birthdays, etc.**

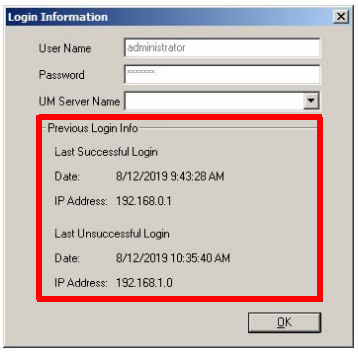
These rules are enabled by automatically when installing the JITC compliant edition of Avaya IX Messaging. They can also be manually enabled through the IXM Admin MMC under **Configuration > Advanced**.

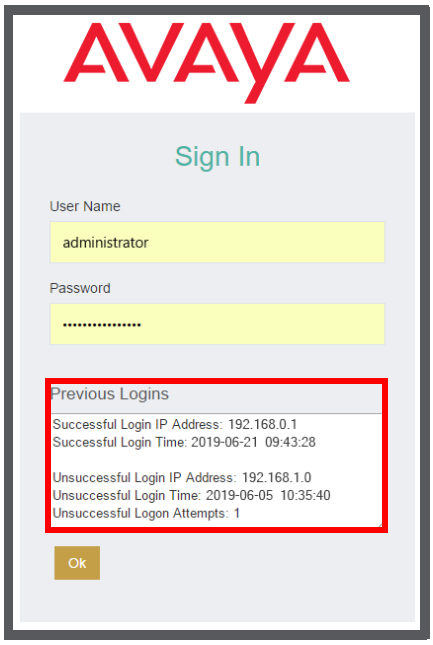


Logging In

When logging in to Avaya IX Messaging applications (i.e. IXM 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.

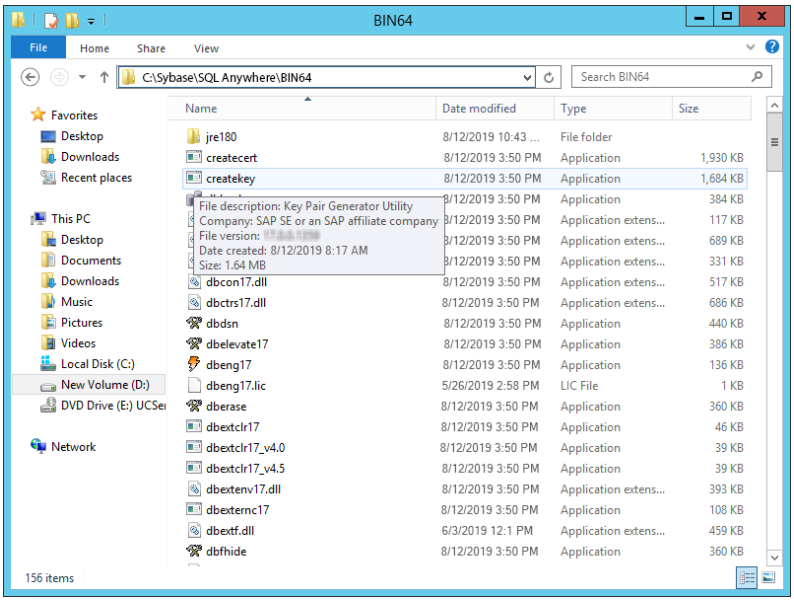




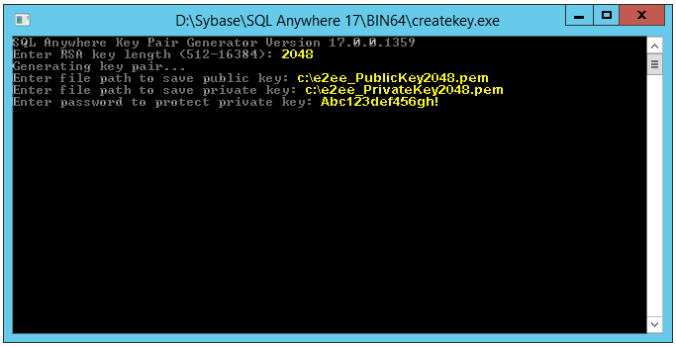
Creating Public and Private Keys

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 Primary computer, open the drive where Avaya IX Messaging 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 **Primary** voice server, and to all **Secondary** servers. Paste the file into the **UC\Certificates** folder on the drive where Avaya IX Messaging was installed.

   Copy the file generated for the **private** key to the same folder on the **Consolidated** server.

Certificates for Mobilink Connection: Self-Signed

Hint: If your site does not permit self-signed certificates, use the Certificates for Mobilink Connection: Not Self-Signed section on page 396 instead. Only one of these procedures is required.

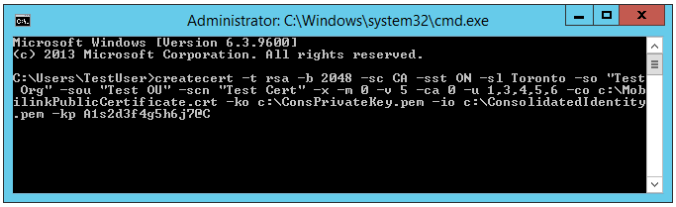
If you are using a self-signed certificate, run the following script from the command prompt to generate the Consolidated server identity and public certificates used by Mobilink services for authentication.

Change the highlighted sections so that they apply to your installation. Enter the same values that were used during the installation of the Primary voice server (step 26 on page 350).

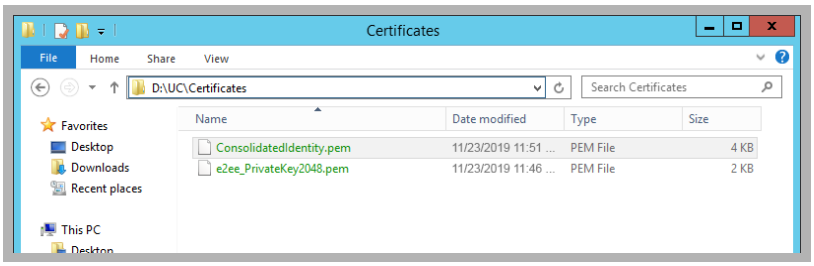
Enter the password you chose for the Consolidated server during installation (***Abc123def456gh!*** in this example).

All passwords must be JITC compliant (see page 390).

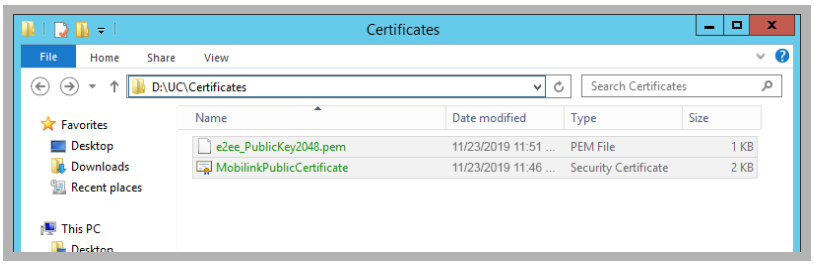
createcert -t rsa -b 2048 -sc CA -sst ON -sl Toronto -so "**Test Org**" -sou "**Test OU**" -scn "**Test Cert**" -x -m 0 -v 5 -ca 0 -u 1,3,4,5,6 -co c:\MobilinkPublicCertificate.crt -ko c:\ConsPrivateKey.pem -io c:\ConsolidatedIdentity.pem -kp ***Abc123def456gh!***



Copy the **ConsolidatedIdentity.pem** certificate file to the **UC\Certificates** folder on the Consolidated server to the drive where Avaya IX Messaging 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.



Copy the **MobilinkPublicCertificate.crt** certificate file to the **UC\Certificates** folder on the Primary and all Secondary servers to the drive where Avaya IX Messaging 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.



Certificates for Mobilink Connection: Not Self-Signed

Hint: If self-signed certificates are satisfactory, use the Certificates for Mobilink Connection: Self-Signed section on page 394 instead. Only one of these procedures is required.

If your site does not permit self-signed certificates, run the following scripts 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 that were used during the installation of the Primary voice server (step 26 on page 350).

Enter the password you chose for the Consolidated server during installation (***Abc123def456gh!*** in this example).

The Private certificate password (***Zyx987wvu654ts!*** in this example) is created here and must appear in the Public certificate command line.

All passwords must be JITC compliant (see page 390).

- **Private Certificate**: This certificate will reside on the Consolidated server.

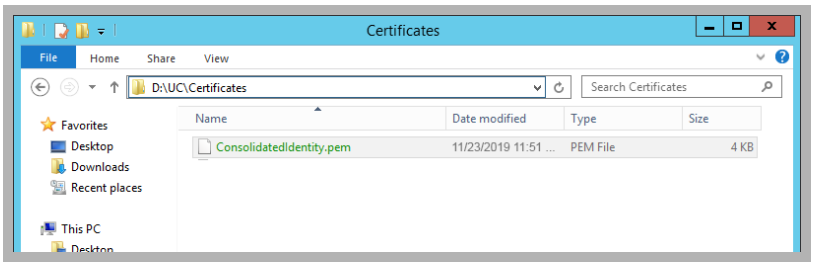
  createcert -t rsa -b 2048 -sc CA -sst ON -sl Toronto -so "**Test Org**" -sou "**Test OU**" -scn "**Test Cert**" -x -m 0 -v 5 -ca 1 -u 6,7 -co c:\MobilinkPublicCertificateCA.pem -ko c:\ConsPrivateKeyCA.pem -io c:\ConsolidatedIdentityCA.pem -kp "***Zyx987wvu654ts!***"

- **Public Certificate**: This certificate is used by Avaya IX Messaging to validate access using the private certificate. Copies must be made on the Primary and all Secondary voice servers.

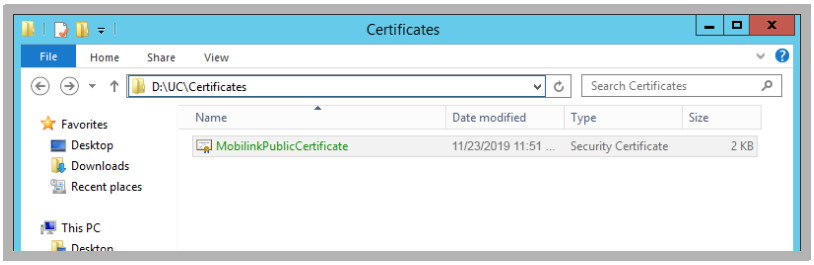
  createcert -t rsa -b 2048 -sc CA -sst ON -sl Toronto -so "**Test Org**" -sou "**Test OU**" -scn "**Test Cert**" -m 0 -v 5 -ca 0 -u 1,3,4,5,6 -c c:\MobilinkPublicCertificateCA.pem -ck c:\ConsPrivateKeyCA.pem -cp "***Zyx987wvu654ts!***" -co c:\MobilinkPublicCertificate.crt -ko c:\ConsPrivateKey.pem -io c:\ConsolidatedIdentity.pem -kp "***Abc123def456gh!***"

The certificate files are created in the root directory of the C:\ drive.

Copy the **ConsolidatedIdentity.pem** certificate file to the **UC\Certificates** folder on the Consolidated server drive where Avaya IX Messaging was installed.



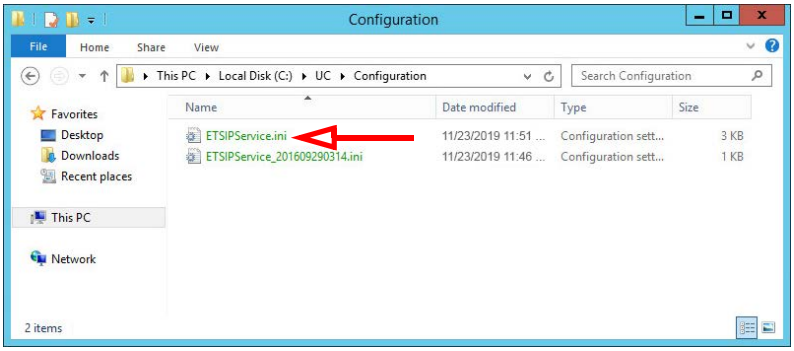
Copy the **MobilinkPublicCertificate.crt** certificate file to the **UC\Certificates** folder on the Primary and all Secondary servers to the drive where Avaya IX Messaging was installed.



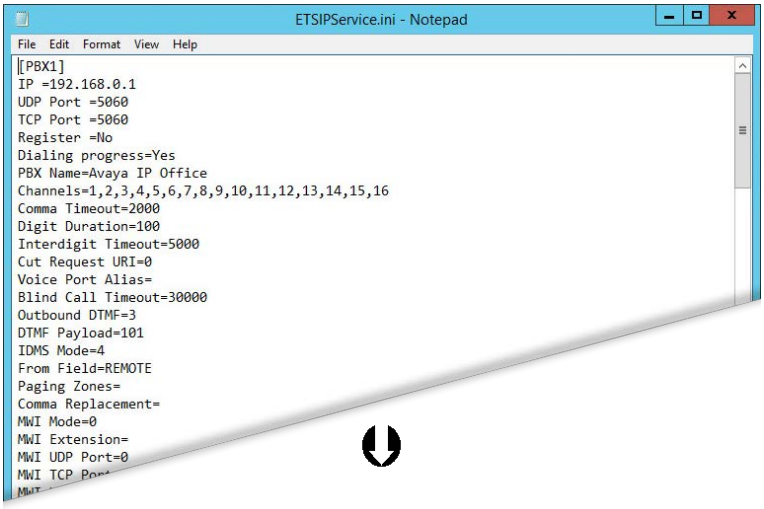
Configuring TLS with Messaging for SIP

After Avaya IX Messaging has been installed, modifications must be made to the **ETSIPService.ini** file. This will enable TLS security with the correct settings for use with Messaging.

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
MWI TCP Port = 5061
TCP Port = 5061

[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.

MWI TCP Port / TCP Port: Set both of these values to **5061**.

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 Messaging 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 Messaging certificates folder: entering **@sip.key** expands the path to **C:\UC\Certificates\sip.key** (where C is the drive where Messaging 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 Messaging certificates folder: entering **@sip.crt** expands the path to

C:\UC\Certificates\sip.crt (where C is the drive where Messaging 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 you installation requires an earlier version of TLS, change the value accordingly.

VALUE	VERSION
4	TLS 1.0
3	TLS 1.1
2	TLS 1.2
1	SSL 3.1

CA Certificates: Enter the full path to the PEM certificate file. Adding the prefix **@** will automatically include the path to the Messaging 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 Messaging 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.

VALUE	VERSION
4	TLS 1.0
3	TLS 1.1
2	TLS 1.2
1	SSL 3.1

Note: Some sites may require **Mutual Certification** between the Messaging 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
```

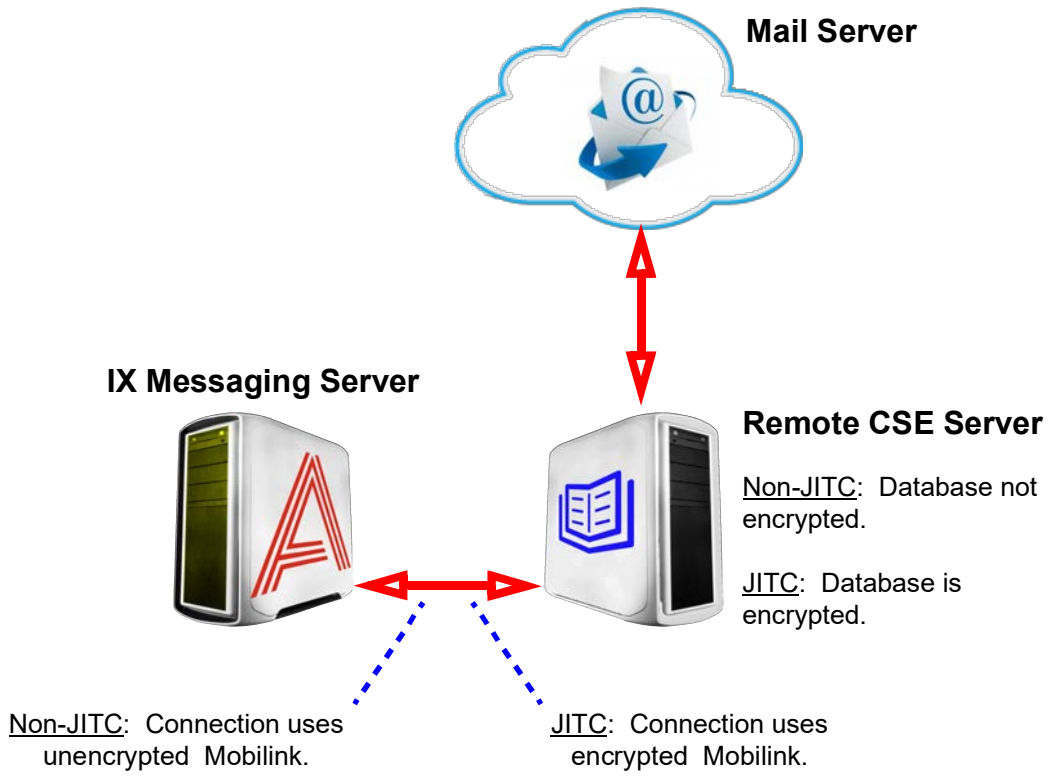
Installing Remote CSE Under JITC

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 Messaging 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.

Note: Each Remote CSE Server supports a **single** email type (e.g. Exchange, Office 365, Gmail, etc.). If more than one email type is required, the Consolidated Server cannot be used for synchonization.



Traffic Flow through a Remote CSE Server

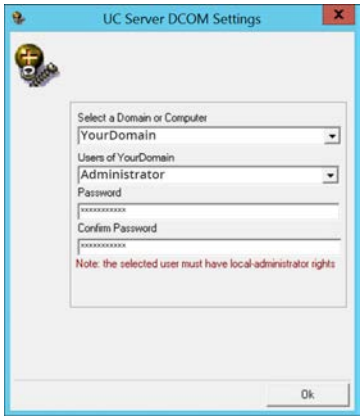
Installation Procedure

1. On the computer designated as the Remote CSE Server, open the Avaya IX Messaging folder on your server hard drive and run **Setup.exe** as administrator to launch the installer.

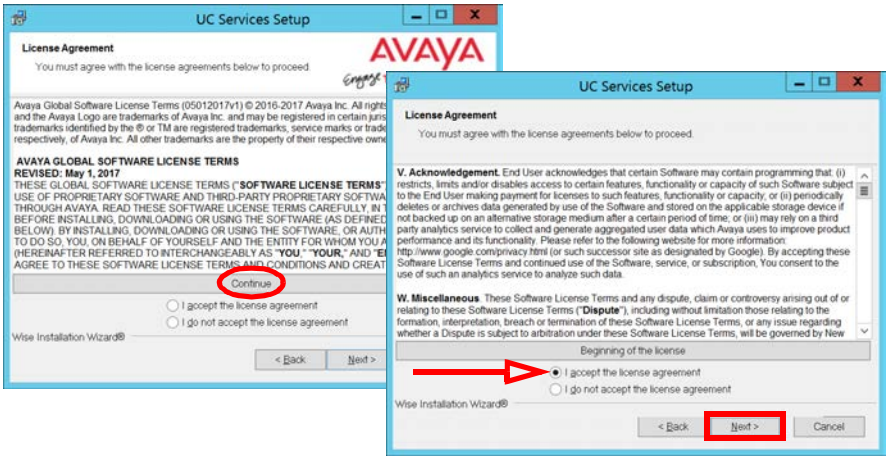
   When prompted, click **Next**.

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.

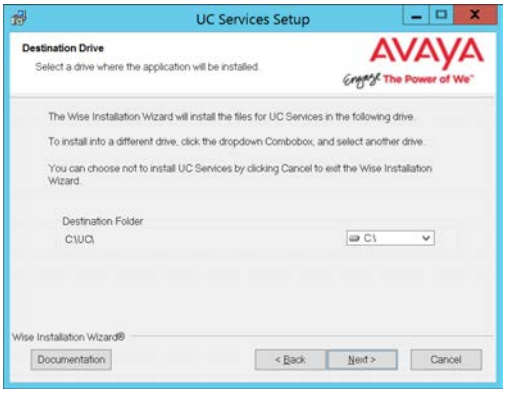


3. Review the license agreement. Click **Continue**, enable the **I accept the license agreement** checkbox, then click **Next**.



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.

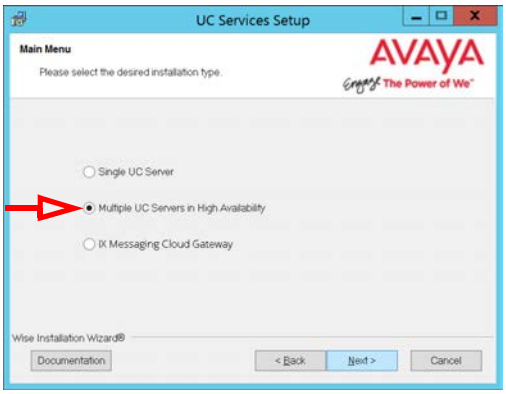
   Click **Next** to continue.



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

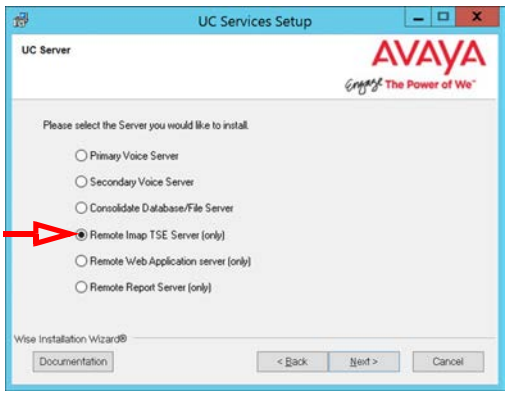
5. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.



6. Select **Remote Imap TSE Server (only)**.

   Click **Next**.

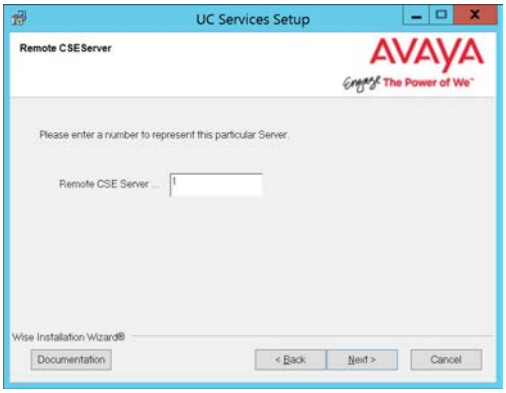


7. Enter a number between 1-25 for this server.

   If you configure multiple CSE servers, each must be given a unique number; no two servers can share the same number.

   Avaya IX Messaging supports up to 25 CSE servers.

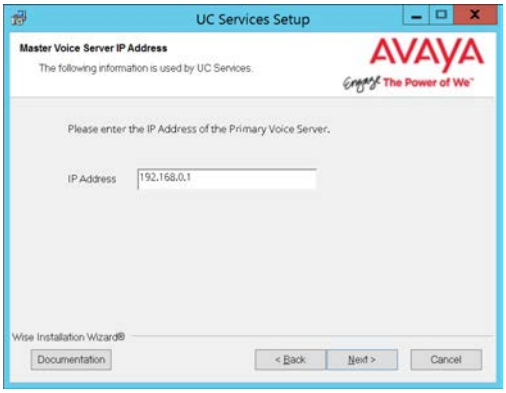
   Click **Next**.



Note: Each CSE server can support up to 5000 users.

8. Enter the IP Address of the **Primary** server.

   Click **Next**.

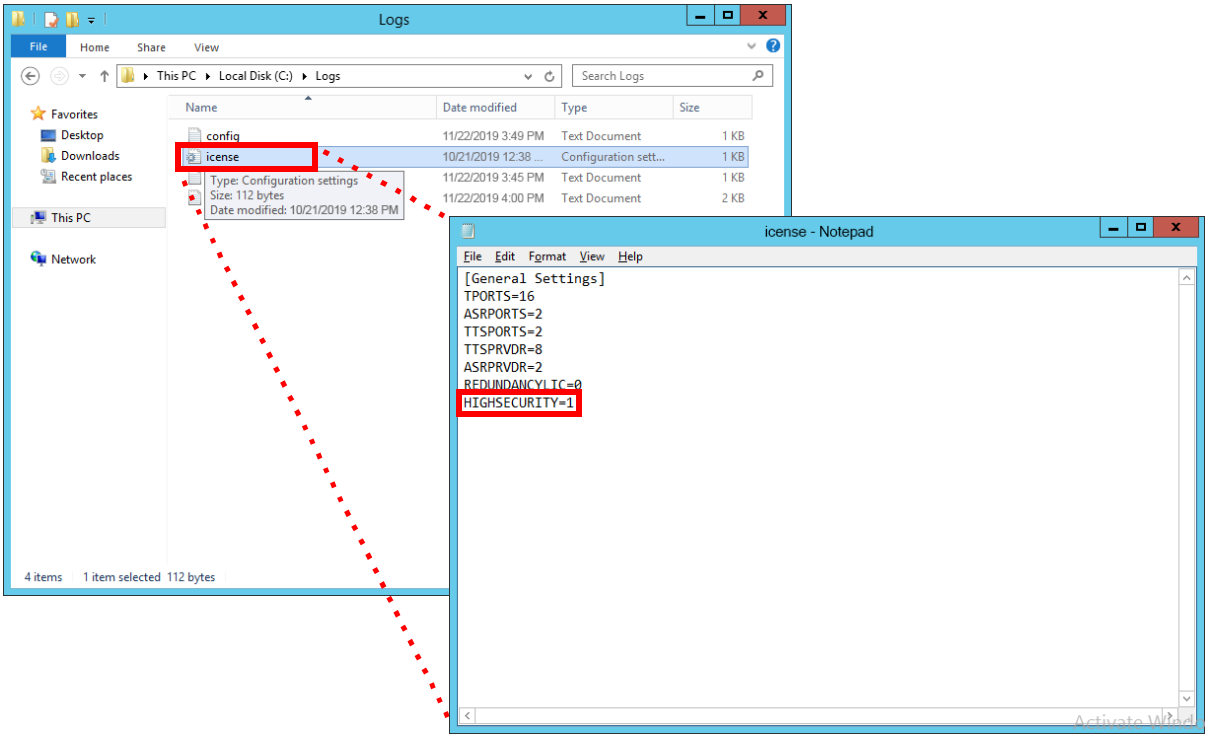


9. On the C drive, open the **Logs** folder.

   Open the file named **license** using any text editor (e.g. Notepad).

   Verify **Highsecurity=1**. If it does not, verify that the same file (*IXM Installation drive*:\UC) on the Primary voice server does have this setting. If the setting is valid on the Primary, there is a connection or a sharing problem between the two machines. If the Primary is not correctly set, contact your reseller for an updated license.

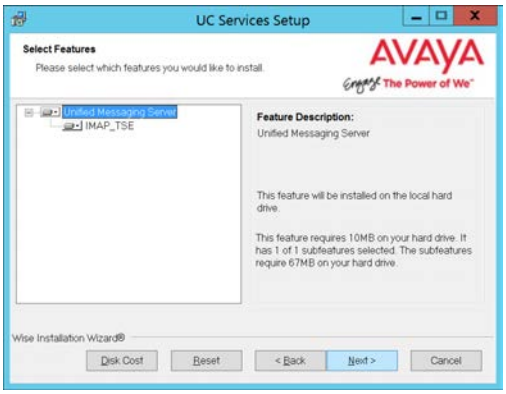
   Once any connection or sharing problems have been fixed, return to step 9 and check again for this file.



Caution: Do not continue the installation until this file has the Highsecurity setting equal to 1.

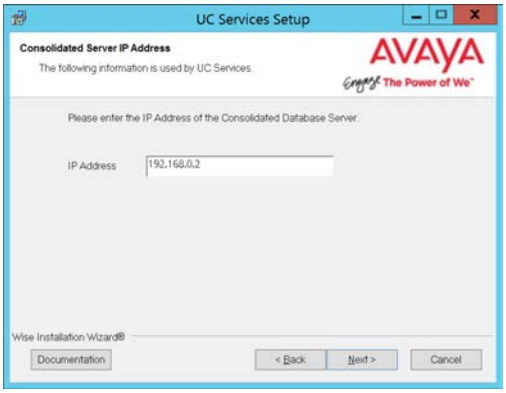
10. Select the **Components** required at your site. Disable any components that are not needed.

    Click **Next.**



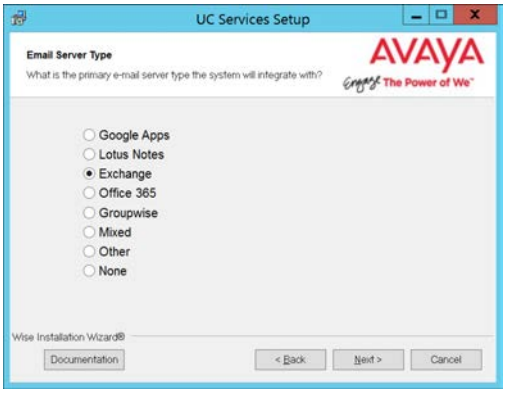
11. Enter the IP Address for the **Consolidated** server.

    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.

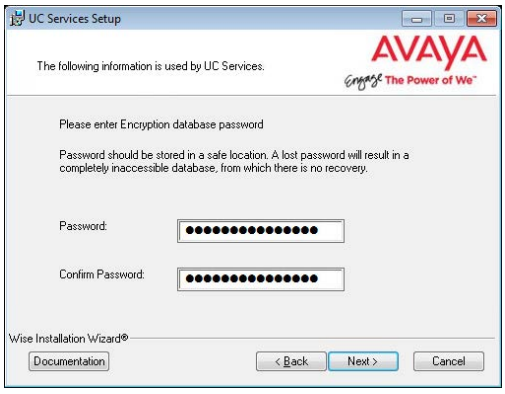
    When ready, click **Next**.



Note: Each Remote CSE Server supports a **single** email type (e.g. Exchange, Office 365, Gmail, etc.). If more than one email type is required, the Consolidated Server cannot be used for synchonization.

13. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.

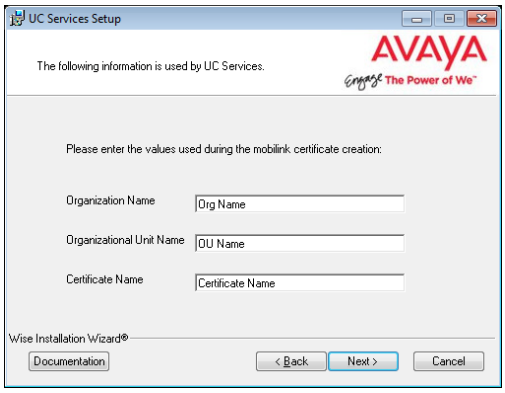
    This password must meet the requirements outlined **here**.



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.

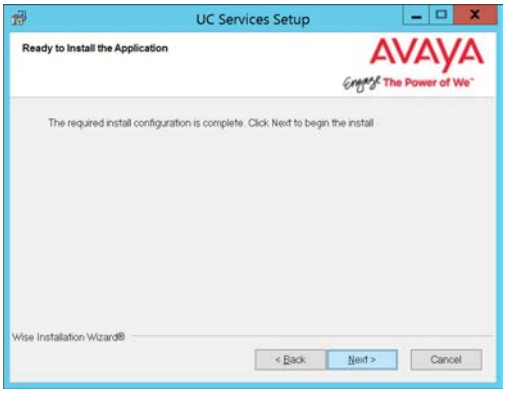
14. Enter the values in the spaces provided. These are provided with the certificate.

    These values must be the same as are used during the Primary voice server installation (step 26).

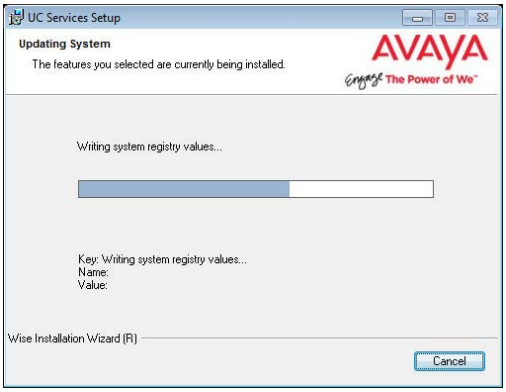


15. The preliminary information required for installation is now complete.

    Click **Next**.

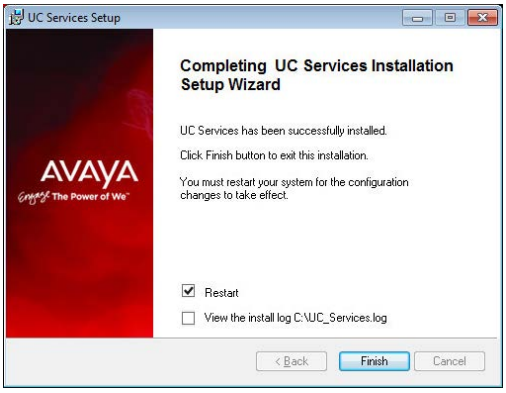


16. The selected components will now be installed. This process may take a while.

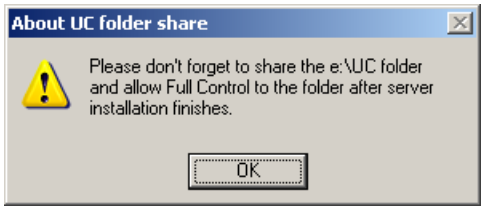


17. Click **Finish** to restart the server.

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

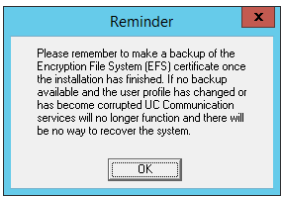


18. This alert is to remind you to properly share the UC installation folder (see page 256 for details).



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 287). 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 Messaging 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

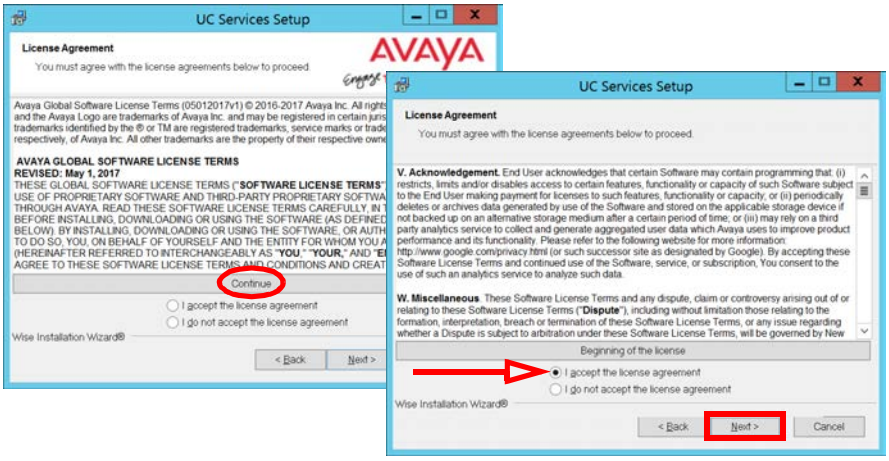
1. On the computer designated as the Remote Web Server, open the Avaya IX Messaging folder on your server hard drive and run **Setup.exe** as administrator to launch the installer.

   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.

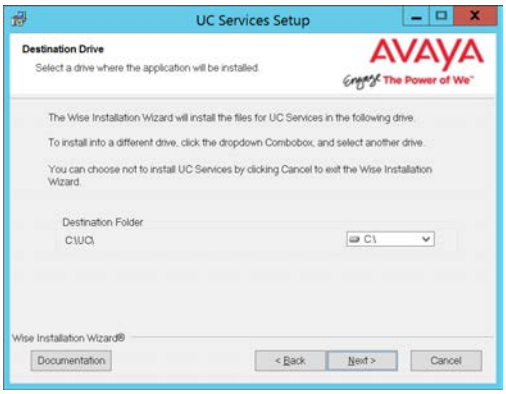
   Click **OK** after entering the credentials.

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.

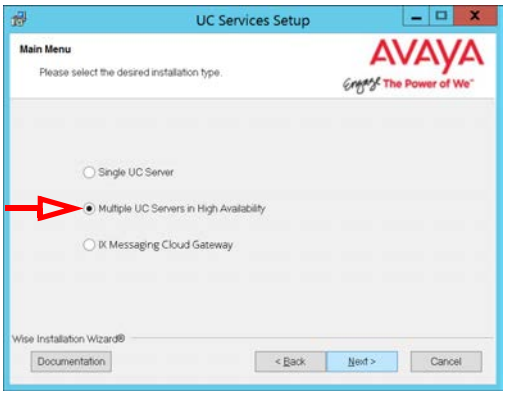
   Click **Next** to continue.



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

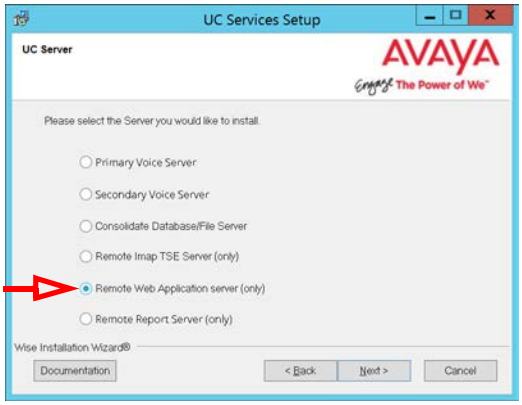
5. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.



6. Select **Remote Web Application server (only)**.

   Click **Next**.

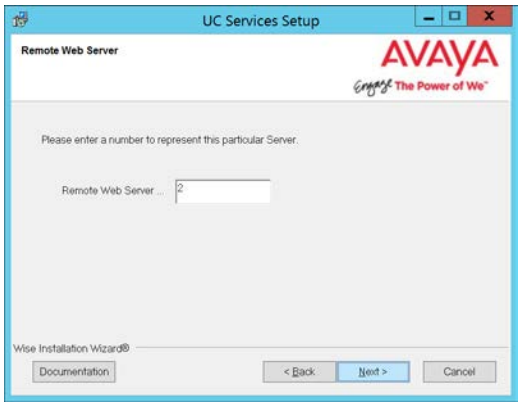


7. Enter a number between 1-14 for this server.

   If you configure multiple Web servers, each must be given a unique number; no two servers can share the same number.

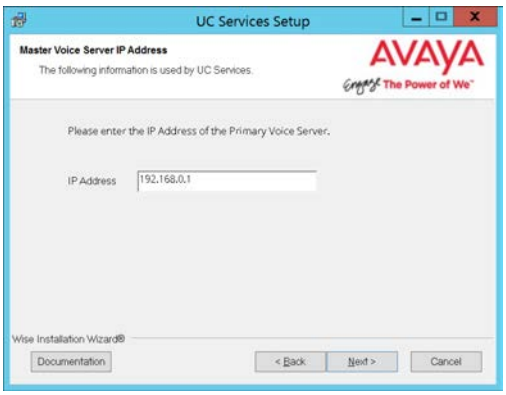
   Avaya IX Messaging supports up to 14 Web servers.

   Click **Next**.



8. Enter the IP Address of the **Primary** server.

   Click **Next**.

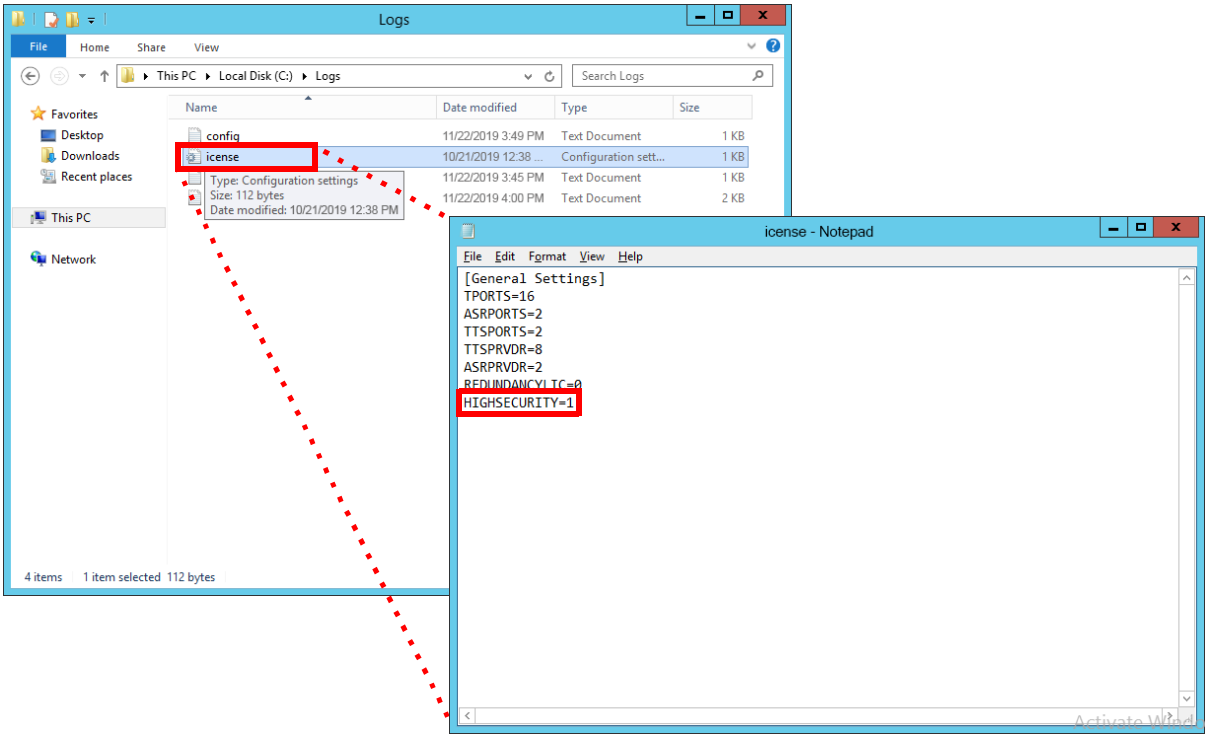


9. On the C drive, open the **Logs** folder.

   Open the file named **icense** using any text editor (e.g. Notepad).

   Verify **Highsecurity=1**. If it does not, verify that the same file (*IXM Installation drive*:\UC) on the Primary voice server does have this setting. If the setting is valid on the Primary, there is a connection or a sharing problem between the two machines. If the Primary is not correctly set, contact your reseller for an updated license.

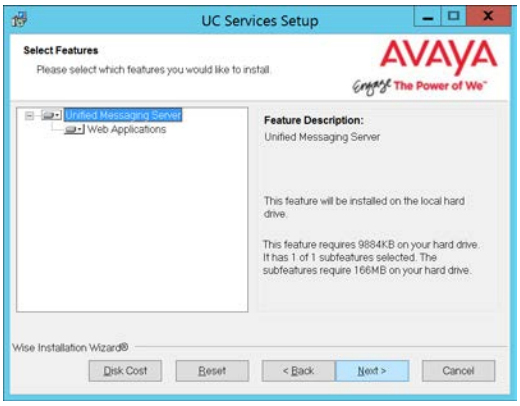
   Once any connection or sharing problems have been fixed, return to step 9 and check again for this file.



Caution: Do not continue the installation until this file has the Highsecurity setting equal to 1.

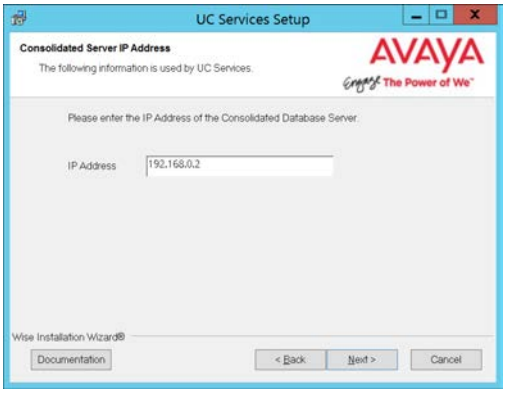
10. Select the **Components** required at your site. Disable any components that are not needed.

    Click **Next.**

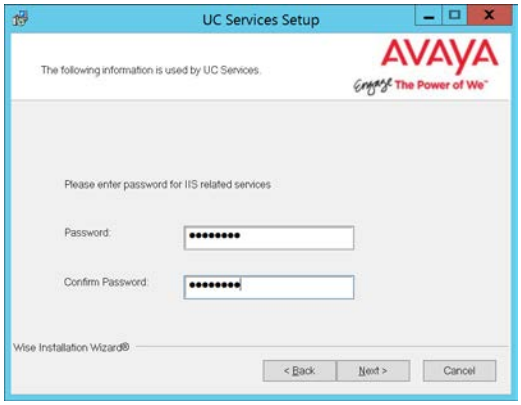


11. Enter the IP Address for the **Consolidated** server.

    Click **Next**.

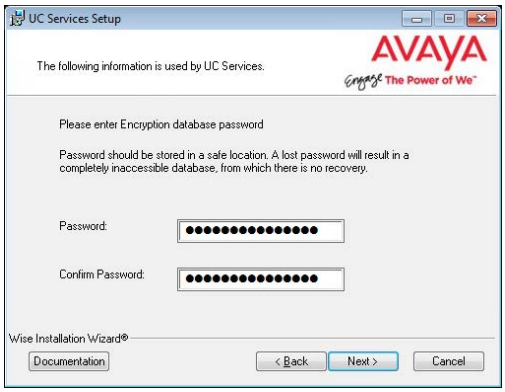


12. Enter and confirm the password for the UCIIS user. This must be the same UCIIS password that was created on the other servers.



13. Enter the database encryption password. The database files will be encrypted with this password using the FIPS 140-2 certified security algorithms.

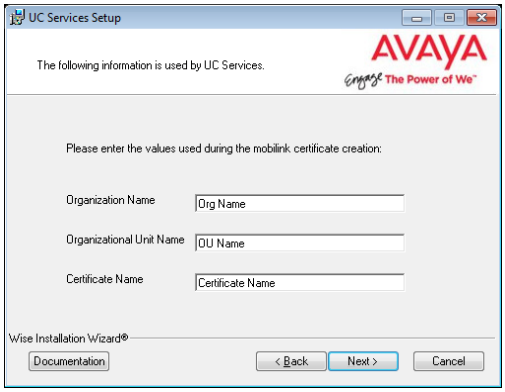
    This password must meet the requirements outlined **here**.



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.

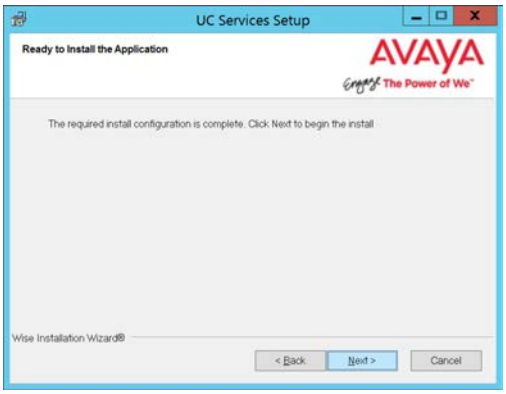
14. Enter the values in the spaces provided. These are provided with the certificate.

    These values must be the same as are used during the Primary voice server installation.

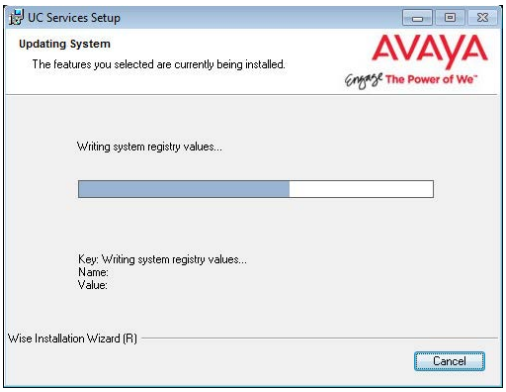


15. The preliminary information required for installation is now complete.

    Click **Next**.

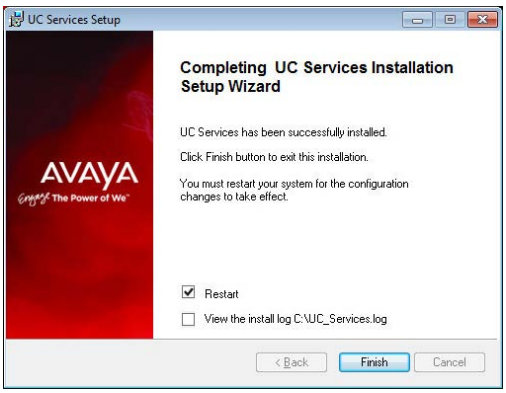


16. The selected components will now be installed. This process may take a while.

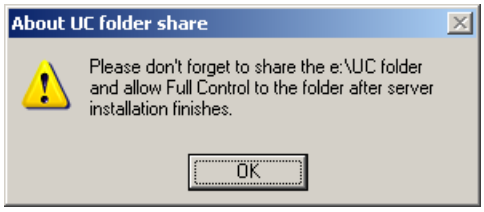


17. Click **Finish** to restart the server.

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

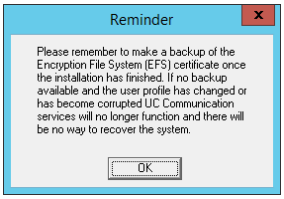


18. This alert is to remind you to properly share the UC installation folder (see page 256 for details).



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 287). 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.

9 GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE

In This Chapter:

Introduction

By default, certain information is collected on all incoming calls through Avaya IX Messaging. This data is collected so that site administrators can generate reports that show traffic flows, system capacity and other usage data. This information includes calling number, caller ID, date and time and length of the call, and so on. Conversations can also be recorded and stored by the system.

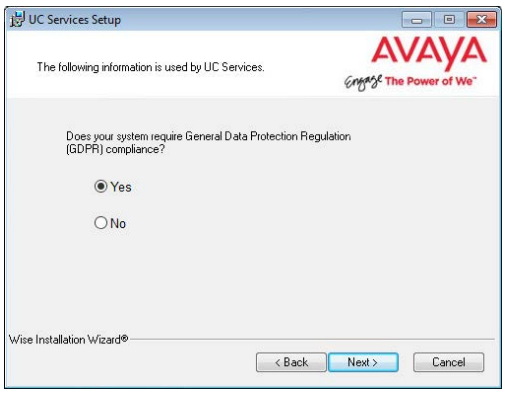
Avaya IX Messaging complies with the General Data Protection Regulation (GDPR) standard, allowing site administrators to delete this information from the database after a request from the caller, maximizing personal data security.

Prompts can be setup to be played before each call starts, alerting the caller that the information is being collected. They then have the option to terminate the call, or to request that the details be removed from the database afterwards if security is an issue.

Installation

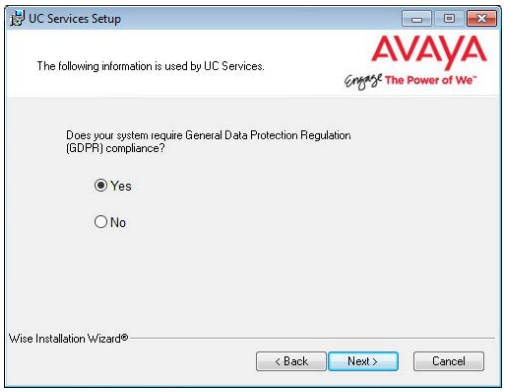
Adding GDPR to Avaya IX Messaging is typically done during the initial program installation procedure, although it can be added afterwards (see Enable / Disable GDPR).

During installation, at the screen where you are asked whether or not you want to include GDPR with the product, enable **Yes**. This will cause the installer to make the necessary adjustments to the database to accommodate GDPR. It also installs the utility that allows the administrator to remove a caller's details from the database.



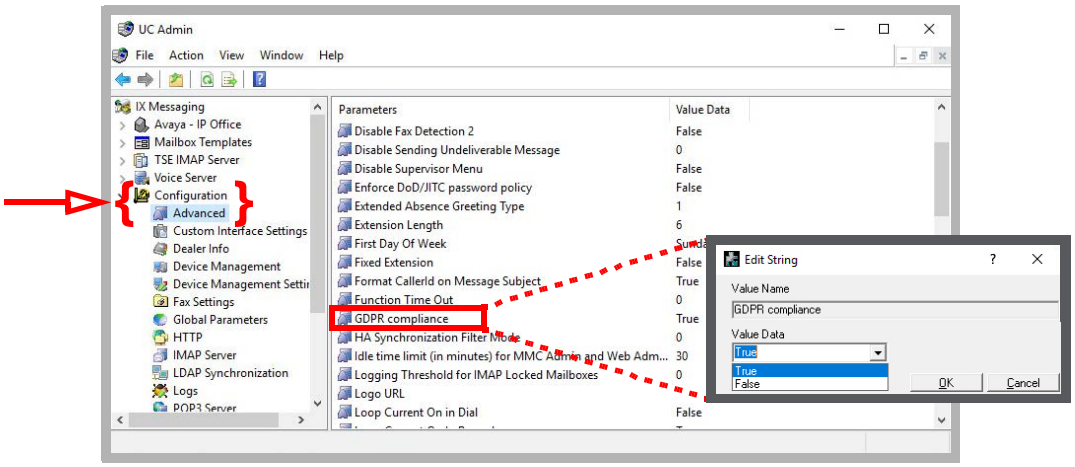
Enable / Disable GDPR

Typically, enabling or disabling GDPR is configured during the initial installation of Avaya IX Messaging.



It can always be turned on or off at any time thereafter as required.

1. Open Messaging Admin on the voice server.
2. Open **Configuration > Advanced**.
3. In the right-hand pane, double-click **GDPR compliance** and set the Value Data field to **True** (to enable) or **False** (to disable) this feature.

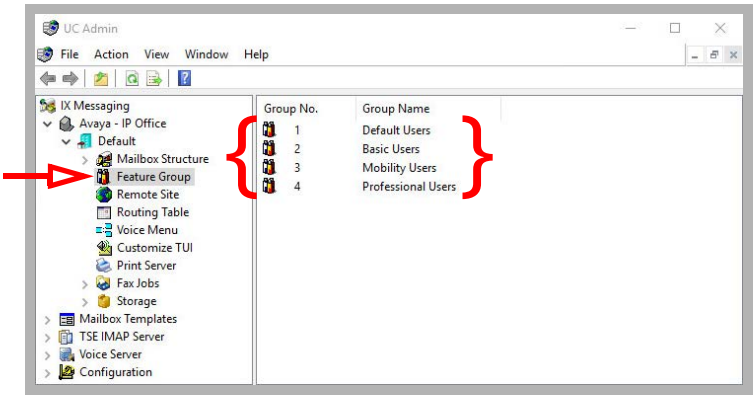


Enabling and Customizing Collection Notification Alerts

An audio alert can be played before an incoming call to notify the caller that their personal information will be collected or that the conversation is being recorded. They have the option to request that this information be deleted.

A standard, generic, system prompt can be used for each case, or you can record custom prompts.

1. Open Messaging Admin on the voice server.
2. Open **Company > Default > Feature Group**. Select a Feature Group to apply GDPR notifications to and double-click.

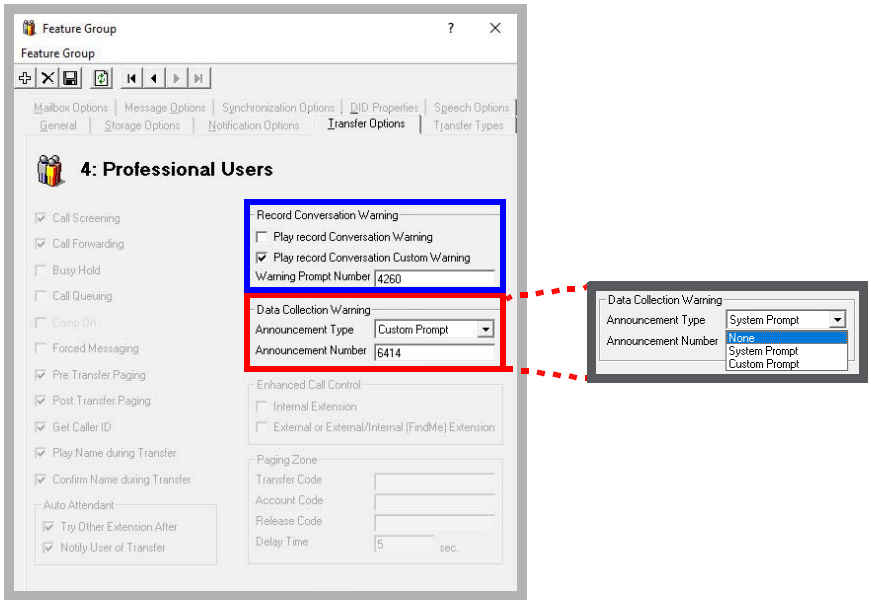


3. Go to the **Transfer Options** tab.
4. In the section for **Record Conversation Warning**, enable **Play record Conversation Warning** to play the system prompt for the incoming caller whenever the call will be recorded.
   If you have recorded a customized greeting for this event, enable **Play record Conversation Custom Warning** instead and enter the 4-digit SAL number (digits only) for the custom recording (see Recording a Custom Greeting).
   If you do not wish to play a warning when recording a call, disable both options.
5. In the section for **Data Collection Warning**, select an **Announcement Type**.

   None: This option will disable the warning for data collection.

   System Prompt: Plays the system prompt when an incoming caller leaves a message in voicemail.

   Custom Prompt: Plays the custom prompt that you recorded when an incoming caller leaves a message in voicemail. Enter the 4-digit SAL number (digits only) for the custom recording (see Recording a Custom Greeting).

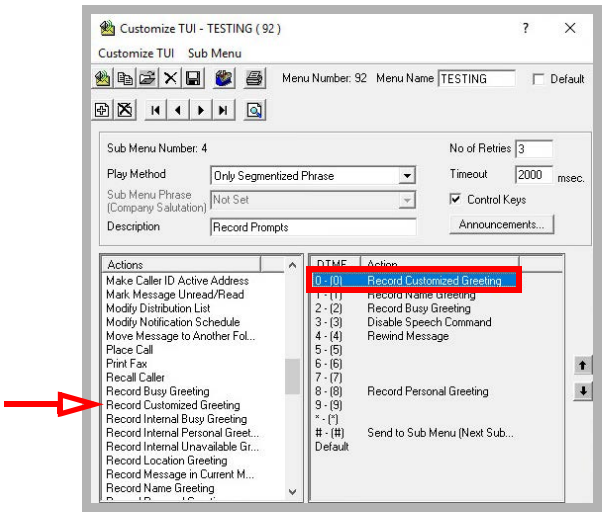


Recording a Custom Greeting

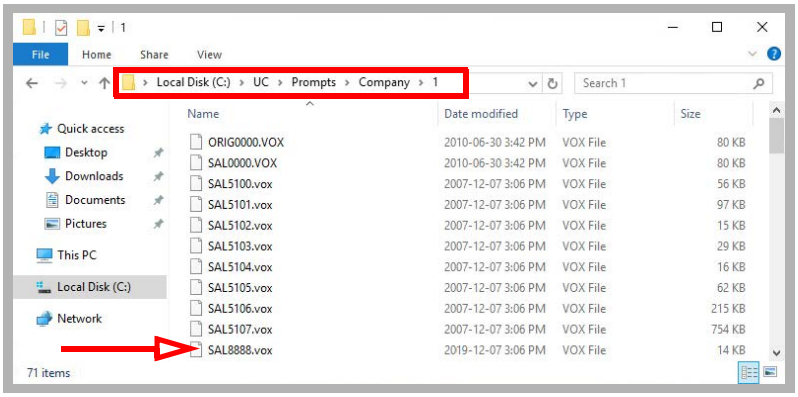
Custom greetings are recorded using a desktop telephone.

1. On a desktop telephone, connect to the system and navigate to the **Record Custom Greeting** prompt in your telephone menus.

   How to reach this menu item depends upon how your **Telephone User Interface (TUI)** is configured. If necessary, add the **Record Custom Greeting** item to one of the telephone menus.



2. When prompted, enter a 4-digit number to identify the file. The recording will be stored in the voice server **Prompts** folder with the format **SALnnnn.vox** where nnnn is the number you entered.
   Copy this file into the **\UC\Prompts\Company\1** folder if it is not there already.



Note: The number 1 used in this example is the company number. If your site hosts more than one company on a single voice server, then enter the appropriate number for that company instead.

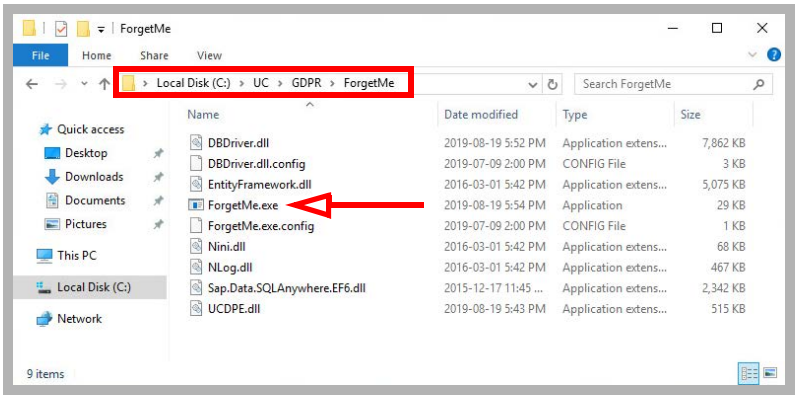
Important: Make sure that the number you assign to the custom prompt is unique. It must not be the same as any other prompt or the original prompt will be overwritten by the new one.

This 4-digit number is used when configuring the prompt to play when a recording a meeting, or when a caller chooses to leave a message in a voice mailbox.

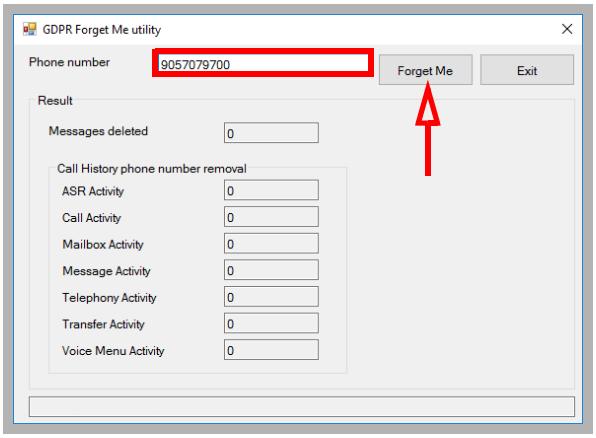
Removing a Caller's Details from the Database

To remove a caller's collected information from the database, run the ForgetMe tool found in the UC directory.

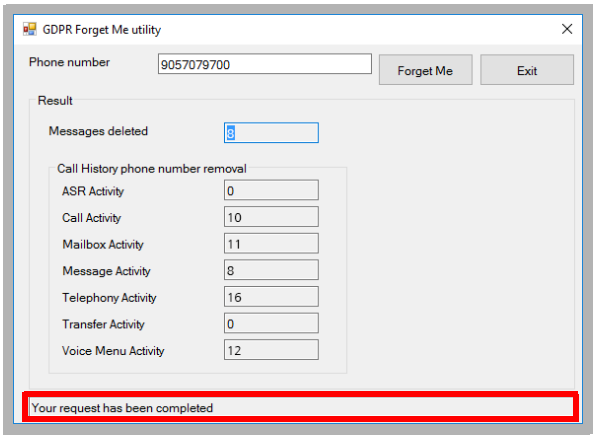
1. In the install directory for Avaya IX Messaging, open the **UC > GDPR > ForgetMe** folder. Run (double-click) the **ForgetMe.exe** application.



2. Enter the telephone number of the caller to be removed from the database, then click **Forget Me**.



3. The utility will remove all references from the database associated with that number. The entries removed are tallied and displayed in the appropriate spaces on the screen.



4. Enter another number to delete, or click **Exit** when finished.

10 UPDATING THE WINDOWS OPERATING SYSTEM

Introduction

Once Avaya IX Messaging program is operational, there will be occasions when the Windows operating system on the servers must be updated. In order to safely perform the required updates, it is necessary that several services for Messaging be stopped. If Windows is updated without first stopping these services, the database may be damaged.

It is advisable to make a backup of your system, or take a snapshot of its current state, before proceeding with the update.

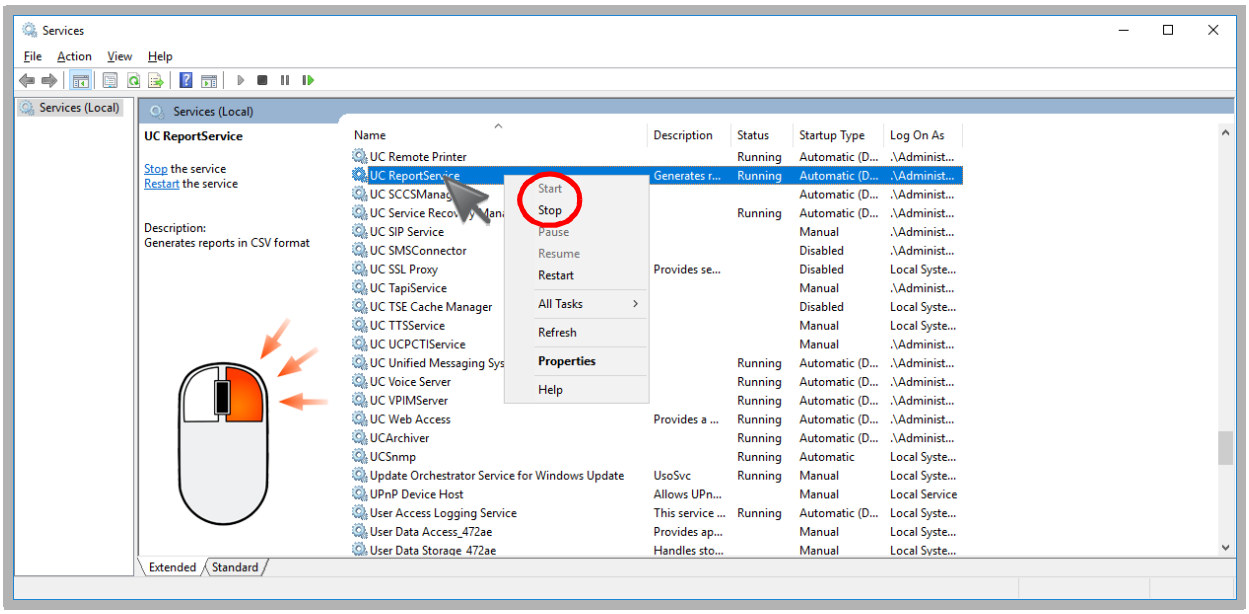
Stop all of the following services on each server. In an HA environment, this includes the Primary, all Secondaries, and the Consolidated servers. Any additional servers, such as Remote CSE, must also be processed this way.

SERVICES TO STOP	SERVER AFFECTED
UC Service Recovery Manager	Single Server, Consolidated [1]
UC Web Access	Single Server, Consolidated
UC ReportService	Single Server, Consolidated
UC Background File Organizer	All
UC CSE PIM Synchronization Engine	Single Server, Consolidated
UC Content Synchronization Engine	Single Server, Consolidated
UC Business Layer Service	All
UC Background Task Manager	All
UC VPIMServer	Single Server, Consolidated
UC Unified Messaging System Tasks Service	Single Server, Consolidated
Mobilink Consolidated	Consolidated
DBWatcher	All
UC Voice Server	Single Server, Primary, Secondaries
UC MRCP Watcher	Single Server, Primary, Secondaries
Nuance Recognition Service	Single Server, Primary, Secondaries
SQLAnywhere Mobilink Remote	Primary, Secondaries
SQL Anywhere - USADB_UC	All

1 - The UC Service Recovery Manager service must be the first one stopped since its role is to restart the other services should they fail and bring the system down.

Note: If prompted to stop other services in addition to the ones shown, always choose **YES**. Some services are dependent upon others and must all be stopped together.

In the Windows Service Manager, right-click a service, and choose Stop from the dropdown list.



When the Windows update is complete, reboot the server.

Once the server is operating, verify that all of the services are running. If any are still stopped, manually start them from the Services window.

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 Messaging 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 Messaging will revert to demo mode after a grace period (see page 444).

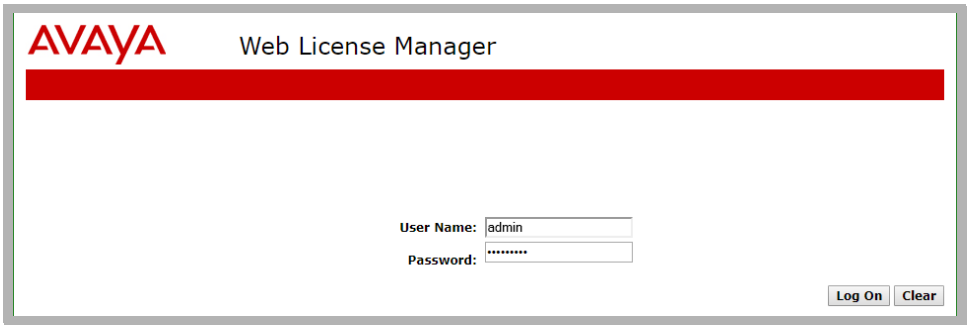
Before installing Avaya IX Messaging onto the voice server, the site administrator must designate another computer to act as the license server, and then load the Web License Manager software onto that machine.

Server Specifications

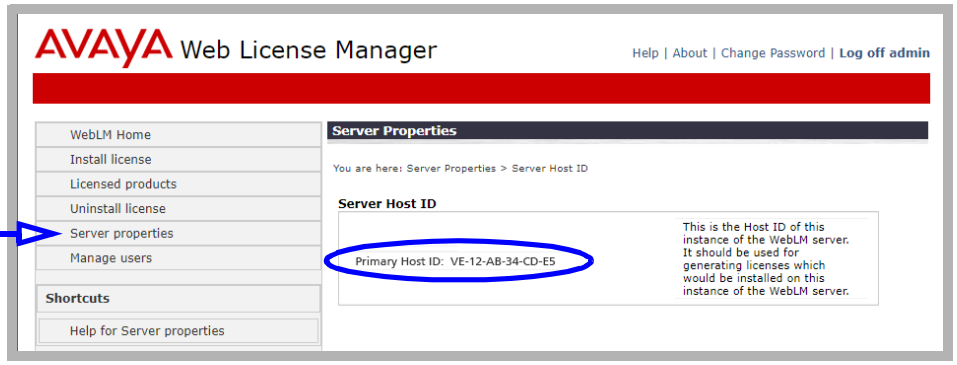
Refer to the Avaya WebLM documentation for the latest server specifications.

Configuring Web License Manager

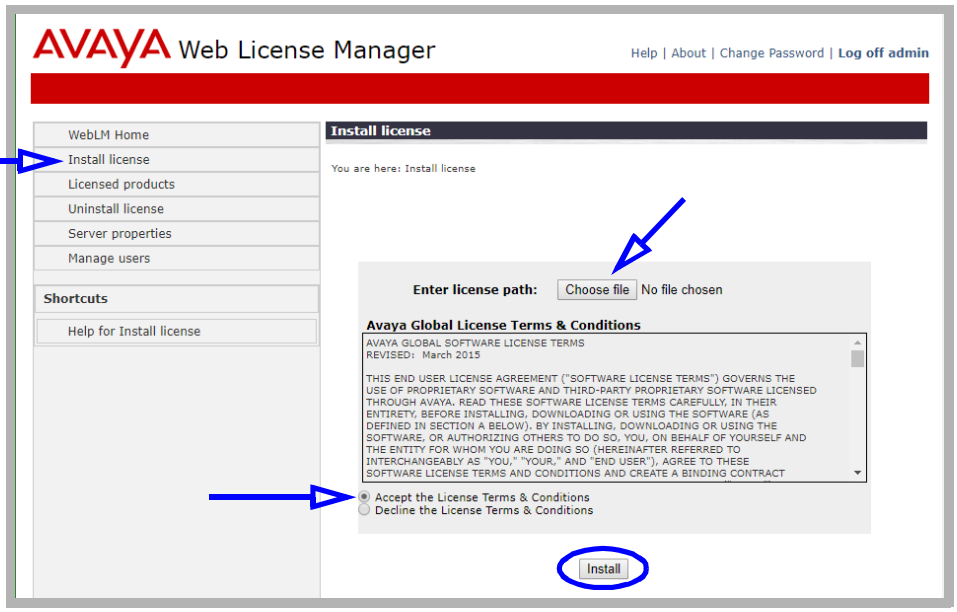
1. On the computer designated as the license server, install the WebLM program according to the Avaya documentation.
2. When finished, launch the Web License Manager and login using administrator credentials.



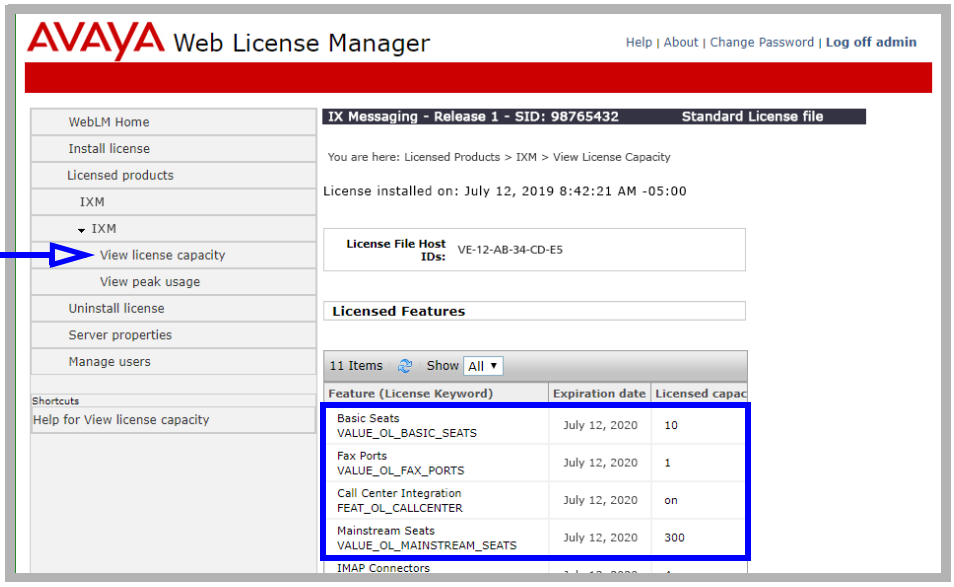
3. Go to the **Server properties** tab and record the **Primary Host ID**. This is used to generate an XML license file specific to this machine.



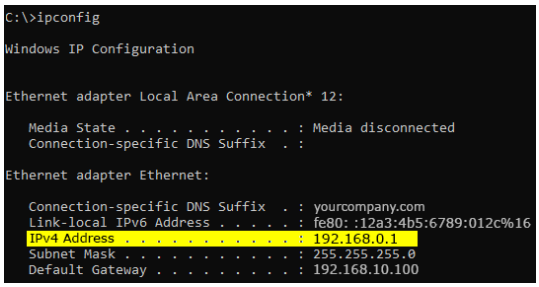
4. Send the Host ID to your vendor, and they will provide the license XML file for your program.
5. Return to WebLM and go to the **Install License** tab.
   Enable the Accept License Agreement button.
   Select **Choose file**, locate the license XML file on your computer and click **Install**.



6. Once the license has been installed, you can verify the details of your license from the **Licensed products > IXM > IXM > View License Capacity** tab.



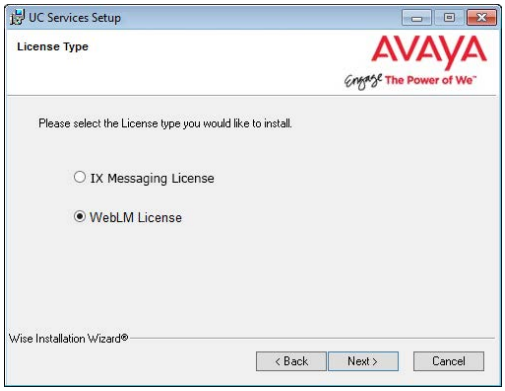
7. Record the IP Address for this machine. This is used when installing the license in Messaging.



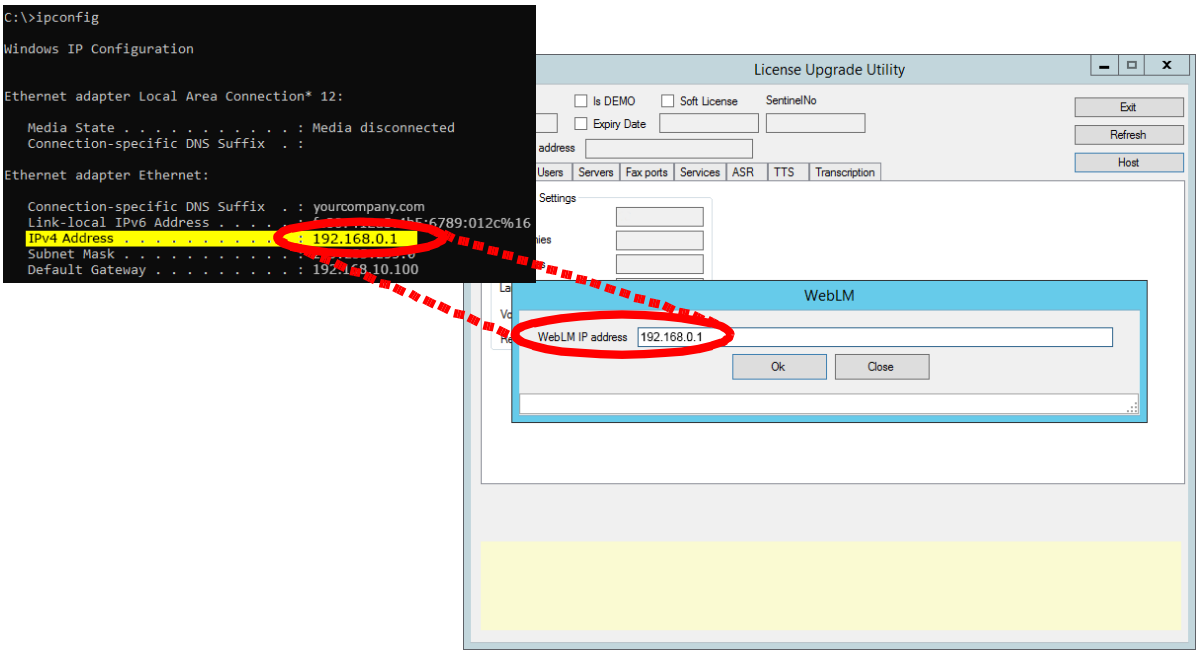
Installing the Messaging License

During the standard installation procedure, when you reach the License Type selection screen:

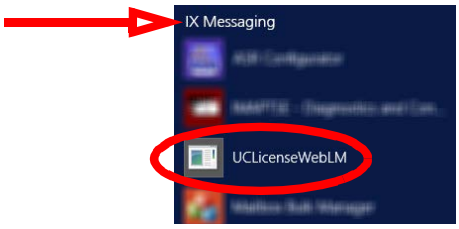
1. Choose Web LM as the license type.



2. At the prompt, enter the IP address for the server configured in step 7 above. When ready, click **OK**.

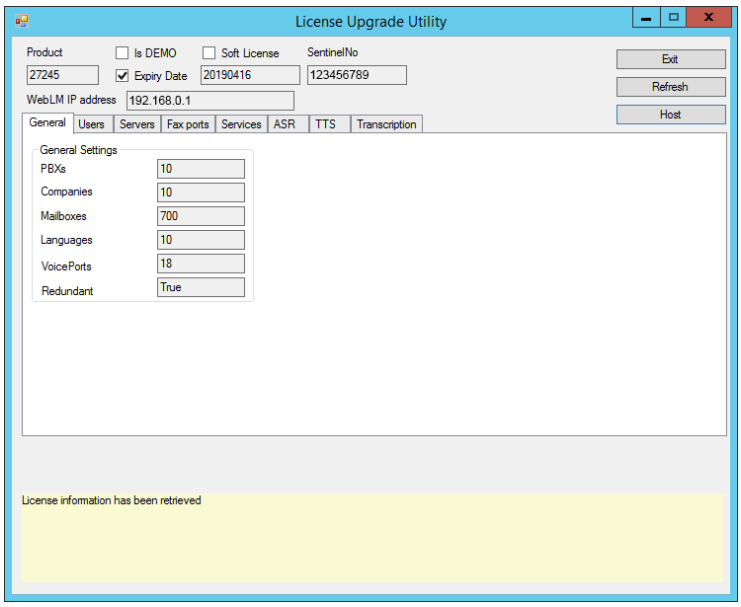


Hint: You can close and exit the installation at any time, although the program will operate in demo mode until a license is applied. To add the license information at a later time, or to modify your license with new features, go to **Start > IX Messaging > UCLicenseWebLM** and enter the details.



This menu item will only appear if you are using the WebLM license option.

3. The license screen will be populated by the details shown is step 6.



4. Return to the appropriate installation chapter and step to complete the installation.

Licensing

Soft License

Avaya IX Messaging program authorization is managed through a “soft” license. Activation of the program features and capacity (mailboxes) requires an connection to the license server. Messaging 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), Messaging will immediately revert to Demo Mode. Contact customer service to reactivate the license.

Normal Operation

Once Messaging 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 Messaging with details of the problem.

If the program detects that the license details are different between the Messaging 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 Messaging 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 Primary connects to the license server. The Consolidated Server and all Secondary Servers get their licensing information from the Primary. Therefore, it is imperative that the Primary 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 Primary.

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 reduce to a single port with 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Messaging 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

Time Before Expiration	Action Taken
+90 days	eMail Administrator
+60 days	eMail Administrator
+30 days	eMail Administrator
+15 days to 0 days	daily eMails to Administrator
License Expires	
-1 day to -60 days	Program capacity reduced to 25%
-61 days and over	Demo Mode

Licensing Grace Periods and Actions

Condition	Grace Period	Action Taken after Grace Period
Failure to authenticate license	28 days	Demo Mode
Upgraded license not activated	28 days	Demo Mode
Hardware changes	-	Demo Mode
License Mismatch (not an upgrade)	-	Demo Mode

HA Licensing

In an HA installation, if the Primary server stops synchronizing with the Consolidated and Secondary servers (i.e. the Primary has gone offline or crashed), the connection must be re-established within 10 days before the system reverts to demo mode. If the Primary server remains connected to the Consolidated and Secondary servers, but cannot connect to the license server, then the **Failure to authenticate license** milestone is used (i.e. demo after 28 days).

Condition	Grace Period	Action Taken after Grace Period
Primary Server fails to synch license with Consolidated and Secondary servers	10 days	Demo Mode
Primary Server cannot connect to the license server.	28 days	Demo Mode

MessagingMessagingMessaging

12 INSTALLING THE MESSAGING LICENSE

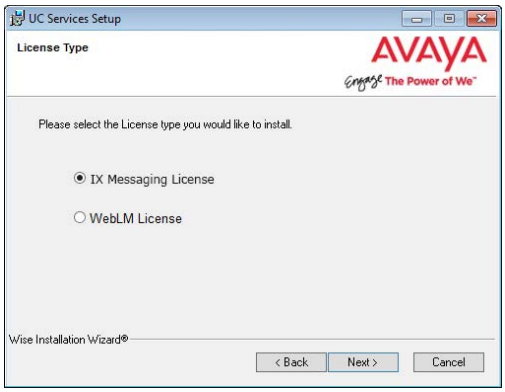
Introduction

As an alternative to the Avaya WebLM license, Messaging 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 Messaging license server.

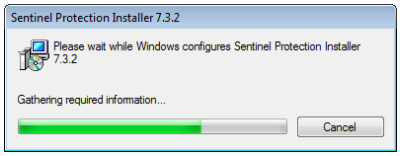
Installing the Messaging License

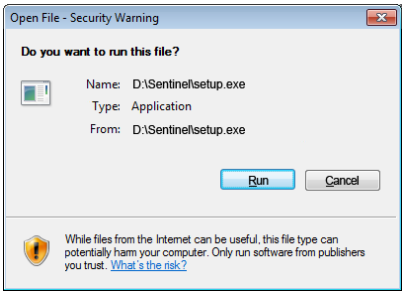
During the standard installation procedure, when you reach the License Type selection screen:

1. Choose **Messaging** as the license type instead of Web LM.



2. When prompted, click **Run** to confirm the installation. The necessary files will be installed.

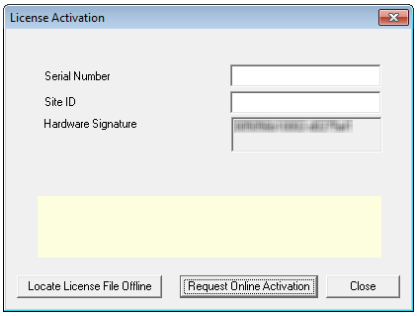




Note: This screen may not appear, depending upon your Windows operating system and settings.

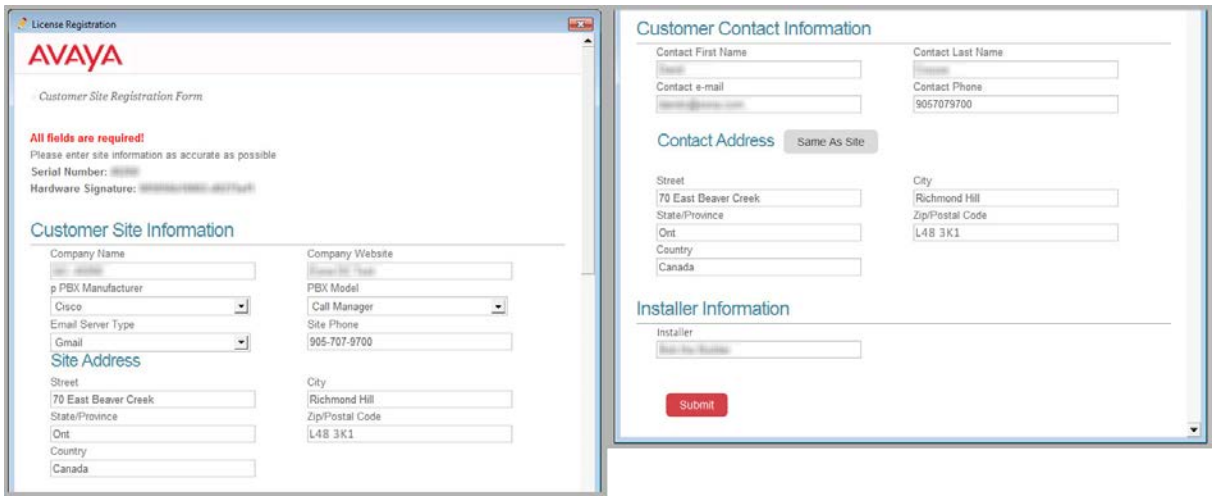
3. Once the process is complete the licensing screen will appear. It is recommended that you use Online Activation whenever possible. To do so, simply enter the **Serial Number** and **Site ID**.

   Click **Request Online Activation** when finished.

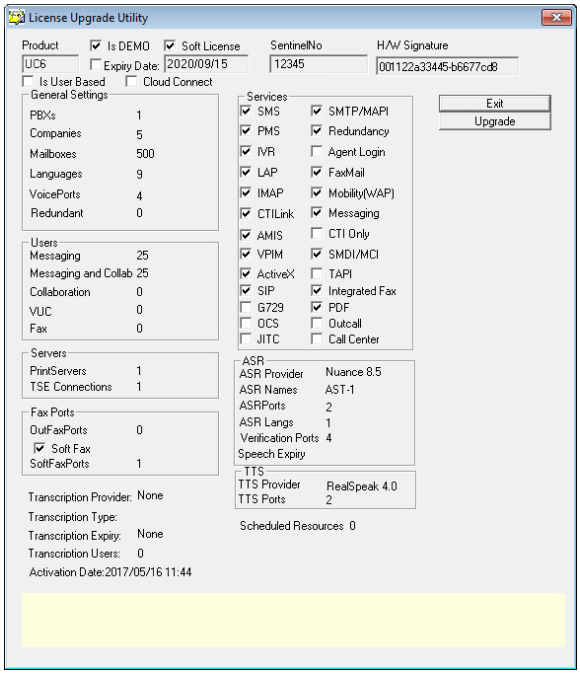


Warning: It is essential that the system/PC clock be properly set **before** activating the license. Any subsequent changes to the clock can adversely affect or terminate the license.

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**.

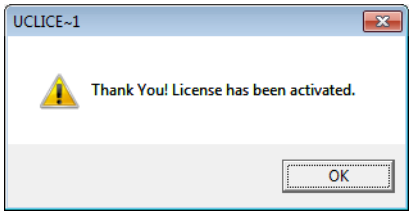


5. Confirm the contents of your license then click on the **Set as Active License button**.



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 IX Messaging 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. Messaging 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), Messaging 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 Messaging 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 Messaging with details of the problem.

If the program detects that the license details are different between the Messaging 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 Messaging 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, Messaging 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 Messaging 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 Primary connects to the license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Primary. Therefore, it is imperative that the Primary 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 Primary.

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 reduce to a single port with 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Messaging 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

Time Before Expiration	Action Taken
+90 days	eMail Administrator
+60 days	eMail Administrator
+30 days	eMail Administrator
+15 days to 0 days	daily eMails to Administrator
License Expires	
-1 day to -60 days	Program capacity reduced to 25%
-61 days and over	Demo Mode

Licensing Grace Periods and Actions

Condition	Grace Period	Action Taken after Grace Period
Failure to authenticate license	28 days	Demo Mode
Upgraded license not activated	28 days	Demo Mode
1st Hardware change	-	Refresh license to continue
2nd Hardware change	-	Demo Mode
License Mismatch (not an upgrade)	-	Demo Mode

HA Licensing

In an HA installation, if the Primary server stops synchronizing with the Consolidated and Secondary servers (i.e. the Primary has gone offline or crashed), the connection must be re-established within 10 days before the system reverts to demo mode. If the Primary server remains connected to the Consolidated and Secondary servers, but cannot connect to the license server, then the **Failure to authenticate license** milestone is used (i.e. demo after 28 days).

Condition	Grace Period	Action Taken after Grace Period
Primary Server fails to synch license with Consolidated and Secondary servers	10 days	Demo Mode
Primary Server cannot connect to the license server.	28 days	Demo Mode

13 SECURING MESSAGING COMMUNICATIONS USING TLS

Introduction

Note: Configuring a site to use TLS communications is optional. It is not required for normal operations.

By default, Avaya IX Messaging communicates with the PBX using UDP (User Defined Protocol). This can be enhanced by activating TLS (Transport Layer Security) if the added security it provides is desirable.

Note: The PBX can be either a physical device, or a UC management software program (such as Avaya Aura Communication Manager).

This is part of all JITC installations, but is also available to all sites where required.

Architecture

TLS communications are established between the Messaging 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 Messaging server to use TLS.

For High Availability Installations

Configure the **Primary** 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.

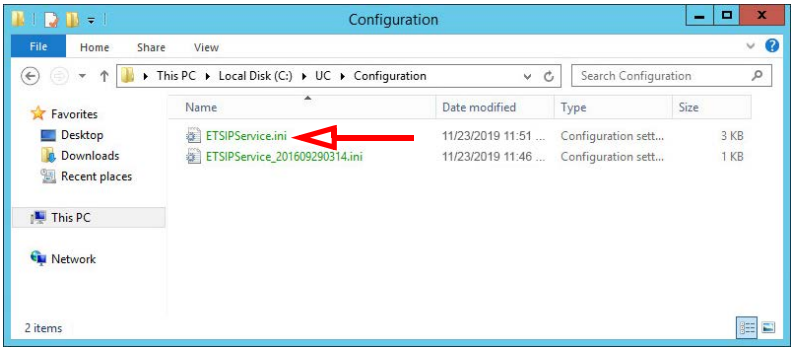
Configuring TLS on the PBX / UC Manager

Refer to the specific product documentation for details on configuring your PBX / system to use TLS.

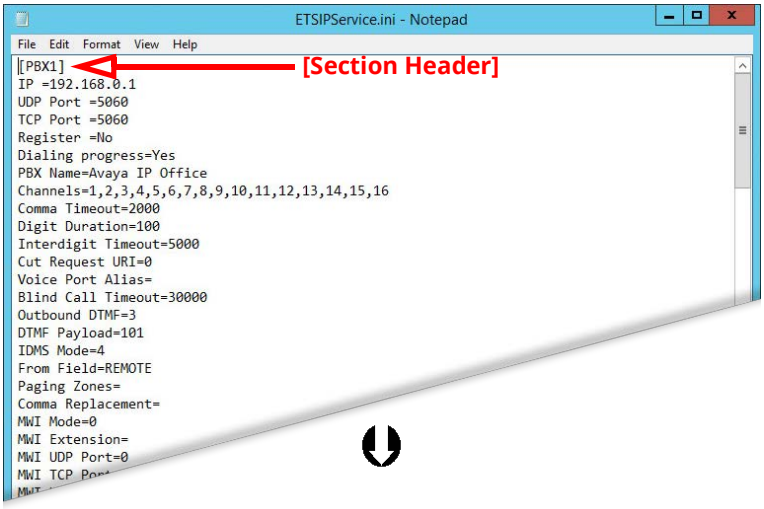
Configuring TLS with Messaging for SIP

After Avaya IX Messaging has been installed, modifications must be made to the **ETSIPService.ini** file. This will enable TLS security with the correct settings for use with Messaging.

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
MWI TCP Port = 5061
TCP Port = 5061

[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.

MWI TCP Port / TCP Port: Set both of these values to **5061**.

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 Messaging 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 Messaging certificates folder: entering **@sip.key** expands the path to **C:\UC\Certificates\sip.key** (where C is the drive where Messaging 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 Messaging certificates folder: entering **@sip.crt** expands the path to **C:\UC\Certificates\sip.crt** (where C is the drive where Messaging 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.

VALUE	VERSION
4	TLS 1.0
3	TLS 1.1
2	TLS 1.2
1	SSL 3.1

CA Certificates: Enter the full path to the PEM certificate file. Adding the prefix **@** will automatically include the path to the Messaging 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 Messaging 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.

VALUE	VERSION
4	TLS 1.0
3	TLS 1.1
2	TLS 1.2
1	SSL 3.1

Note: Some sites may require **Mutual Certification** between the Messaging voice server and the PBX / UC Manager. To configure this item, copy the **Private Key** and **Certificate** elements from TLS Server into the TLS Client section.

```
[TLS Client]
CA Certificates=@CertificateName.pem;
Intermediate Certificates=@CertificateName-G2.pem
Certificate Depth=5
Method=2
Private Key=@sip.key
Certificate=@sip.crt
```

14 AVAYA IX MESSAGING 9.X+ TO 10.8 UPGRADE (SIP)

In This Chapter:

Introduction

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 relying fully on this manual.

Requirements

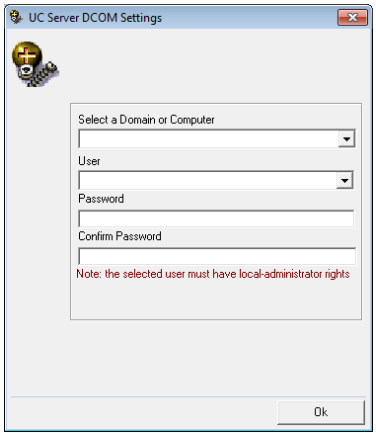
Requirements	Details
License	Existing Officelinx 9.x - 10.7 license
Software	Avaya IX Messaging 10.8 Hardware and Software requirements differ from previous versions. Please consult the Technical Operating Guidelines for detailed information.

Important Notification

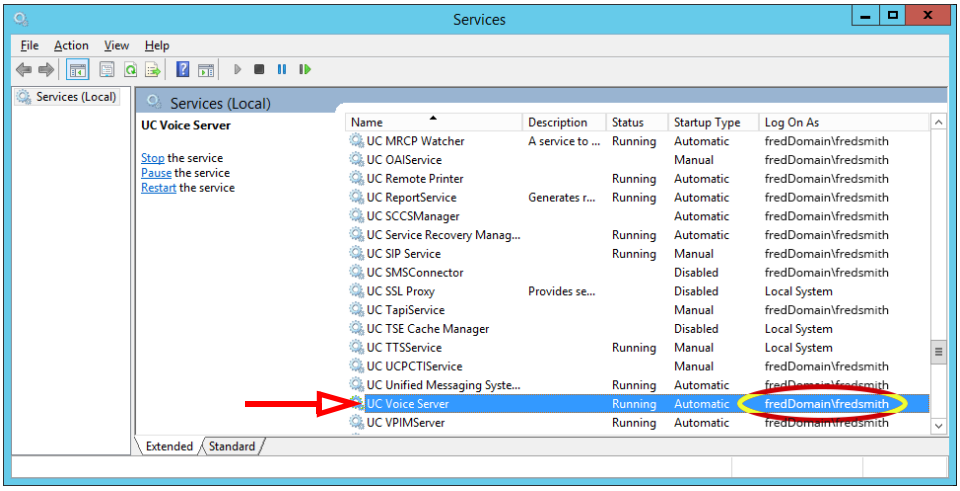
It is vital that the operator login to the voice server(s) being upgraded using the **same username and domain / local administrator** credentials that were provided during the initial program installation (DCOM settings). If different credentials are used, the database may become corrupted and it will be unrecoverable.

(See Backup on page 464 to safeguard your files before proceeding with any upgrade.)

During the upgrade procedure, when prompted for the DCOM settings, enter the same credentials that were used in the initial installation.



To determine which account was used, review Windows Services to see which credentials ("Log On as") are attached to the UC Voice Server service.



Upgrade Preparation

Backup

It is suggested that the User back up certain files in the **\UC** folder on the system before beginning the upgrade.

The following folders must be backed up:

- **\UC\DB**
- **\UC\Messages**
- **\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).

Upgrade Paths

The upgrade path to use depends upon the operating system of your existing installation.

Windows Server 2012 or 2016

- Install Avaya IX Messaging 10.8 over the existing installation (see page 465).

All Other Versions of Windows

- Avaya IX Messaging 10.8 is not supported on other versions of Windows. On a new server, install and configure Windows Server 2012 or 2016.
- Install Avaya IX Messaging 10.8 onto the new server.
- Use the Database Migration tool to move and install the old data files on the new machine.
  Refer to the Database Migration Tool chapter on page 487 for complete details on enabling this upgrade.

Upgrading from Officelinx 9.x and Earlier

Older versions of Officelinx / IX Messaging require a two-step upgrade procedure. Earlier versions must first be upgraded to 10.1, before proceeding to upgrade to Avaya Messaging 11.0.

FROM RELEASE	UPGRADE STEPS
R 9.x and Earlier	Two Steps -- Your Current Version to 10.1 then 10.1 Release to 10.8
R 10.0 and Later	Single Step -- Your Current Version (≥10.x) to 10.8

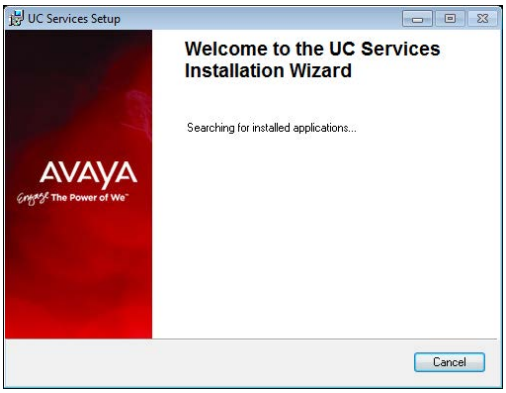
Upgrading 10.8 on Windows Server 2012 / 2016

The upgrade program can be downloaded from support.avaya.com or through your normal PLDS channel.

The downloaded file is a compressed zip formatted document . Once it has finished downloading, double-click the zip file to unpack the contents to your computer.

Double-click the executable file (exe) to launch the installer.

1. Run **Setup.exe** from your original disk or downloaded file.



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.

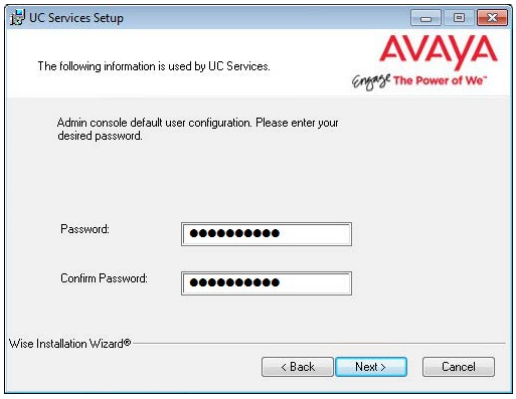
2. Once the Windows components have been verified, the following screen will appear.

   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 IX Messaging.

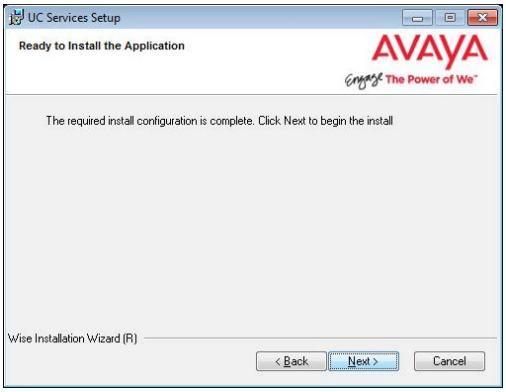
3. If the installer determines that the administrator password is not sufficiently secure (e.g. **1111**), this screen will appear requiring it to be changed.

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

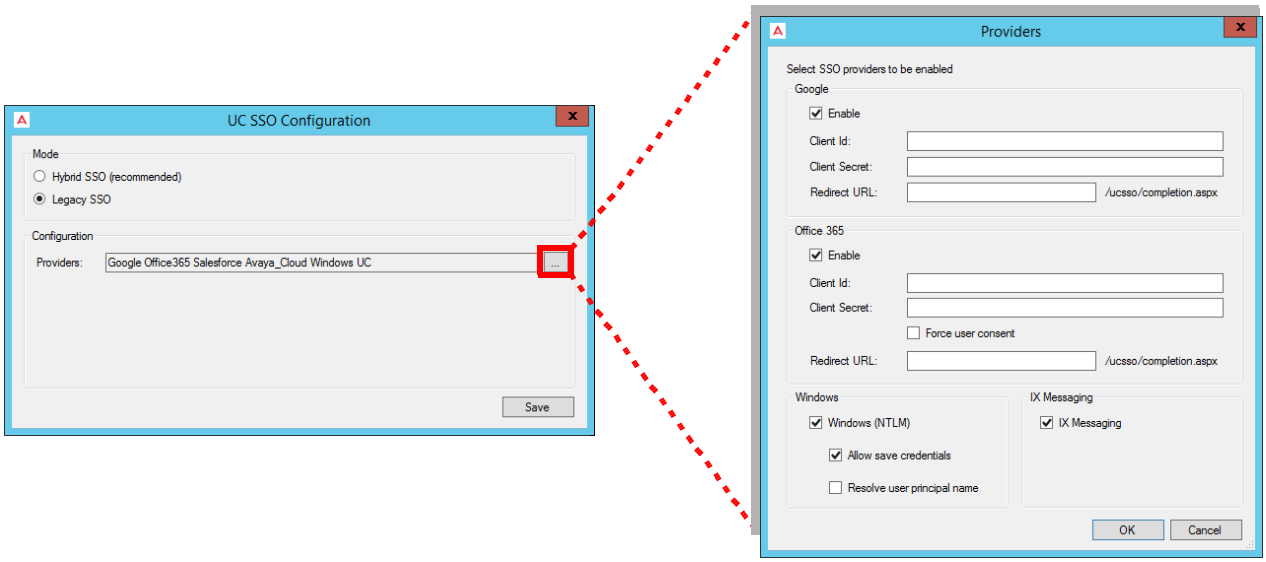


4. The preliminary information required for installation is now complete.

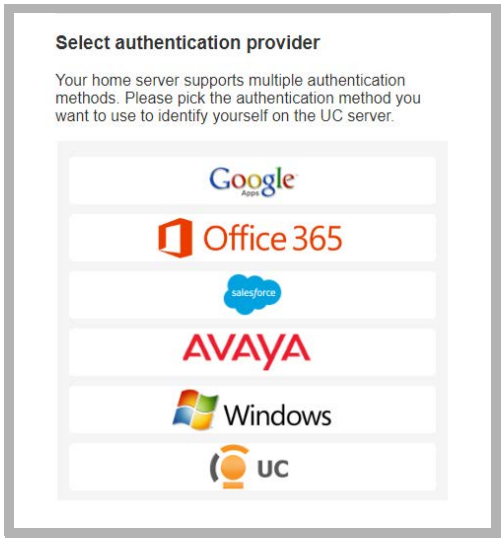
   Click **Next**.

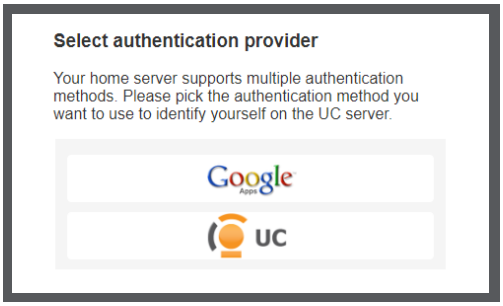


5. On the SSO Configuration screen, enable **Legacy SSO**. From the dropdown menu, enable the Providers that you want your clients to be able to use to access **Web Admin**, **Messaging Admin**, **Web Access**, and **Web Reports**. Items that are disabled will not appear during client login.



When clients / admins want access to these programs, they login using their credentials for one of the listed programs. They must have an account with that application before they can login.





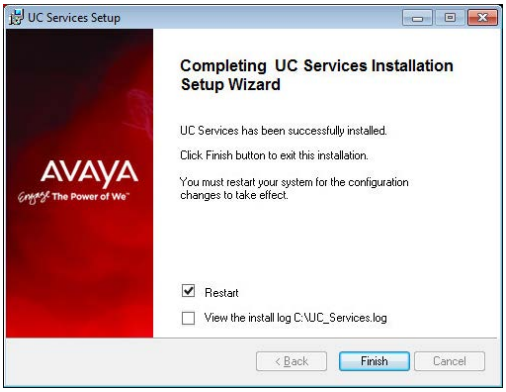
Enable all that apply, then click **OK**.

Click **Save** when finished.

Note: For complete details on using legacy and hybrid SSO, refer to chapter 25 of this document.

6. When the migration and other related configurations are complete, you will see the following screen.

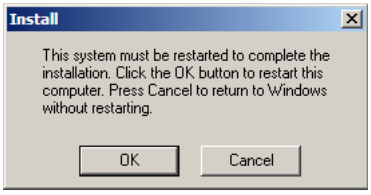
   Click **Finish** to complete the installation.



7. 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**.



Note: For Windows operating systems other than Windows Server 2012 or Windows Server 2016, use the Database Migration Tool chapter on page 461 for complete details on upgrading your system.

15 UPGRADING AVAYA IX MESSAGING HIGH AVAILABILITY INSTALLATION

In This Chapter:

Upgrading an Existing HA Installation

Use this section to upgrade an earlier HA version to Messaging 10.8 HA. Please make sure that your license has also been properly upgraded.

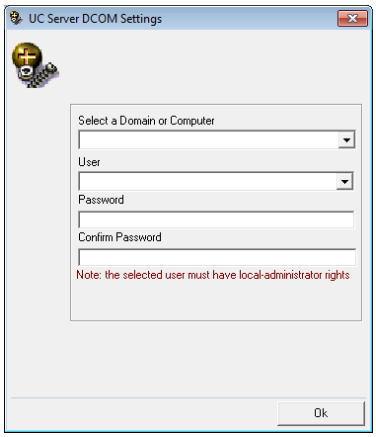
Note: Click here to learn about updating from a **non-HA** installation **to full HA**.

Important Notification

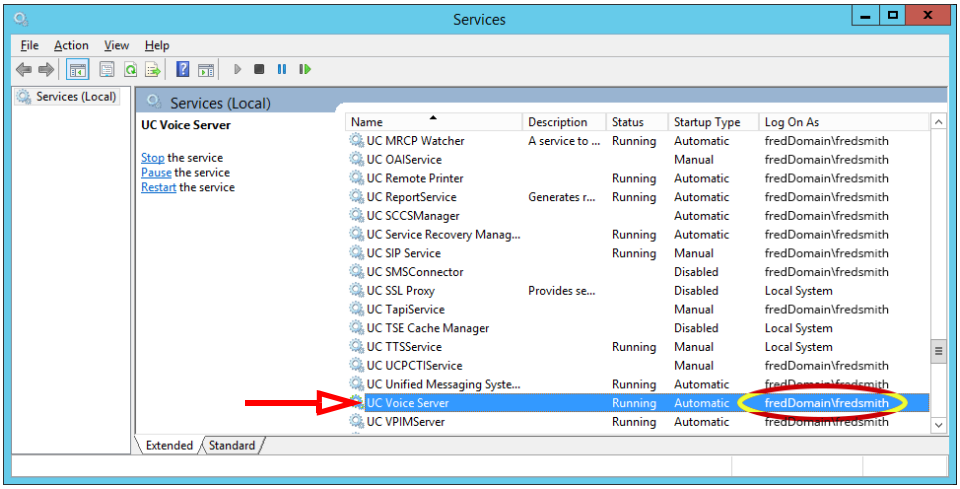
It is vital that the operator login to the voice server(s) being upgraded using the **same username and domain / local administrator** credentials that were provided during the initial program installation (DCOM settings). If different credentials are used, the database may become corrupted and it will be unrecoverable.

(See Backup on page 464 to safeguard your files before proceeding with any upgrade.)

During the upgrade procedure, when prompted for the DCOM settings, enter the same credentials that were used in the initial installation.



To determine which account was used, review Windows Services to see which credentials ("Log On as") are attached to the UC Voice Server service.



Download the Upgrade

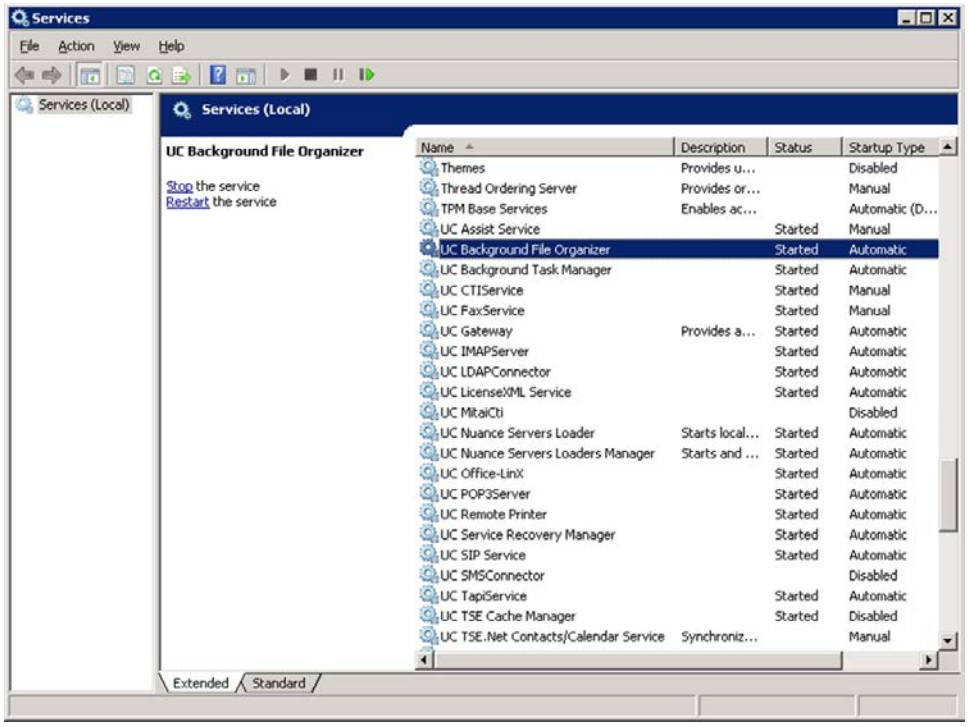
The upgrade program can be downloaded from support.avaya.com or through your normal PLDS channel.

The downloaded file is a compressed zip formatted document . Once it has finished downloading, double-click the zip file to unpack the contents to your computer.

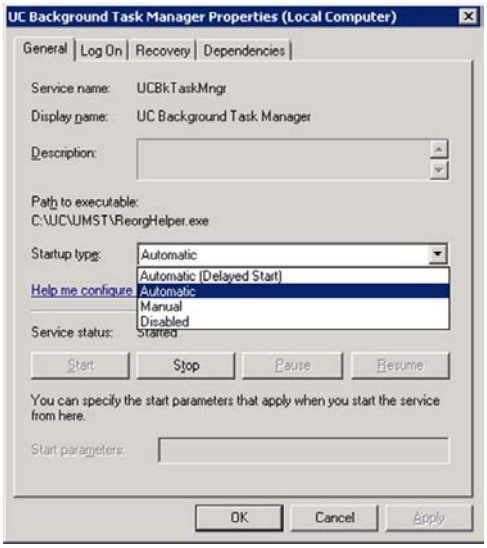
Double-click the executable file (exe) to launch the installer.

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 (see page 476 for a list). 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 (Primary, Consolidated, Secondary) is being used at all times.

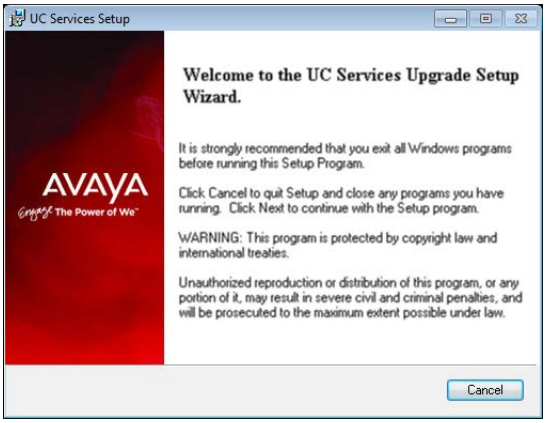
Hint: For safety, copy the DB, Messages and Prompts folders from the UC directory to the computer desktop. Record the **Startup Type** of all services (Manual or Automatic) before proceeding so you can properly reset them afterwards.

1. On the **Consolidated** server, stop and disable the **UC Service Recovery Manager** service.
2. On the **Primary** 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 **Primary**, stop and disable **SQL Anywhere-MobiLink Remote_<computer name>** (Mobilink).
5. Backup the database on the **Primary** server.
6. Gracefully stop and then start **SQL Anywhere-ASADB_UC** (database) on the **Primary** server.
7. Upgrade the **Primary** server to the current release of Messaging as per **Installing the Upgrade on page 477**.
8. Check that the **SQL Anywhere-MobiLink Remote_<computer name>** service is still disabled then restart the **Primary** server.
9. Once the **Primary** server has rebooted, start the **UC Voice Server** service and check that the **Primary** 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 CSE** servers, stop and disable the **UC TSE Cache Manager** service.
14. On the **Remote Admin** servers, close all remote admin connections.
15. On the **Consolidated**, stop and disable these services: **DBWatcher, MobliLink_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 Messaging as per **Installing the Upgrade on page 477**.
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 Messaging as per **Installing the Upgrade on page 477**.
22. After the upgrade to the **Consolidated** server has completed, cofirm that the **UC Service Recovery Manager** service is disabled and restart the server.
23. On both the **Consolidated** and the **Primary** servers, stop and disable **DBWatcher**. Then start **Mobilink - Consolidated** on the Consolidated server, and **SQL Anywhere - MobilinkRemote** on the Primary server.
24. Wait until the **Primary** 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**, **Primary**, and all **Secondaries** start all UC Services except **UC Service Recovery Manager**.
28. Upgrade all **Remote CSE** servers to the current release of Messaging as per **Installing the Upgrade on page 477**.
29. Start the **Remote CSE** 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 Messaging as per **Installing the Upgrade on page 477**.
32. Return all services to their original Startup Type and restart.

Installing the Upgrade

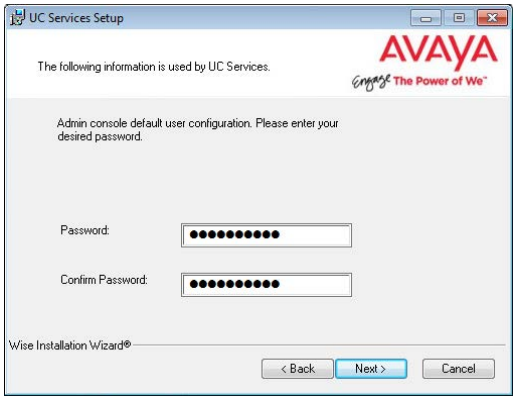
1. Run the update program. The following screen appears.

   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.

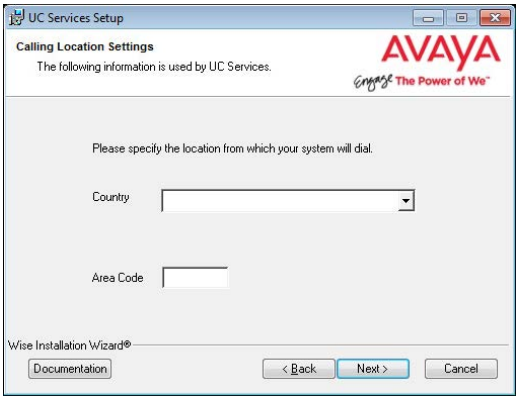
   The password cannot be left blank, it must contain both letters and numbers, and should be at least 6 characters long.



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.

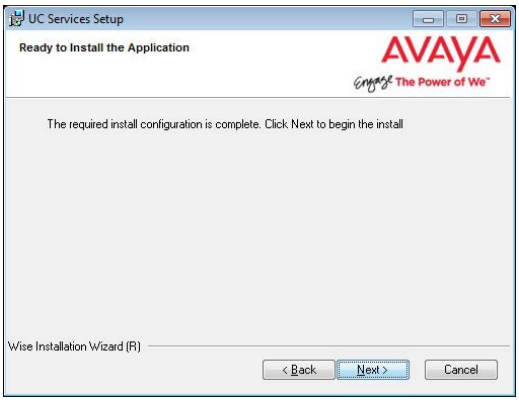
   Click **Next** to continue.



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.

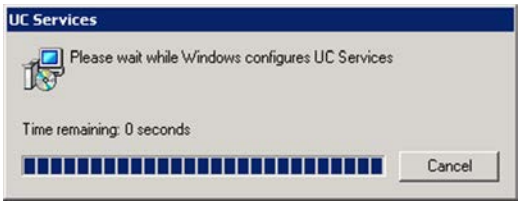
4. The preliminary information required for installation is now complete.

   Click **Next**.

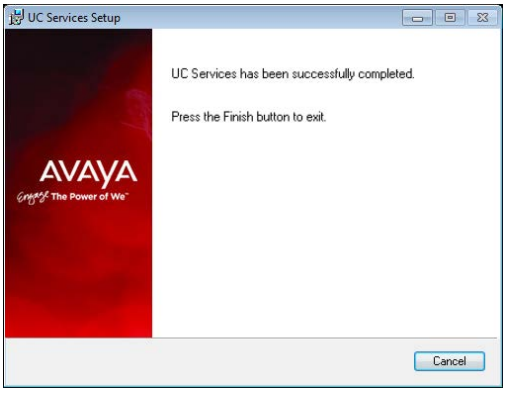


5. Applicable services will be stopped by the program.

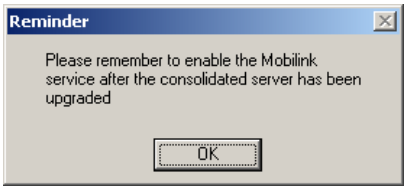
6. The wizard will continue with the upgrade.



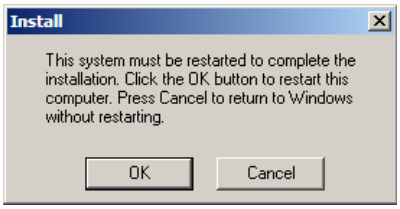
7. When finished, the following screen will appear. Click **Finish** to complete the upgrade.



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 476 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 IX Messaging installation that you want to upgrade to High Availability. Please make sure that your license has also been properly upgraded.

Note: Click here to learn about updating a **full HA** to the latest version.

Caution: It is **strongly** recommended that the Messaging 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 10.8

Before installing High Availability, Avaya IX Messaging must first be updated to the latest 10.8 release. See the appropriate sections of this manual for detailed information on updating Messaging.

- Avaya IX Messaging 9.X+ to 10.8 Upgrade (SIP) on page 461.

Upgrade to HA

Once Avaya IX Messaging has been updated to 10.8, High Availability can be installed.

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

Primary Voice Server

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

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

1. On the Single Server computer, launch the Messaging installation wizard.
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 Primary Voice Server installation procedure.

Consolidated Server

Once the Primary Voice Server is running, the Consolidated Server can be installed.

On the Consolidated Server computer, launch the installation wizard and follow the setup process.

Secondary Voice Servers

After the Primary and the Consolidated Servers are ready, all of the Secondary Voice Servers can be installed.

On all of the Secondary Voice Server machines, launch the installation wizard and follow the setup process.

Sharing the UC Folder

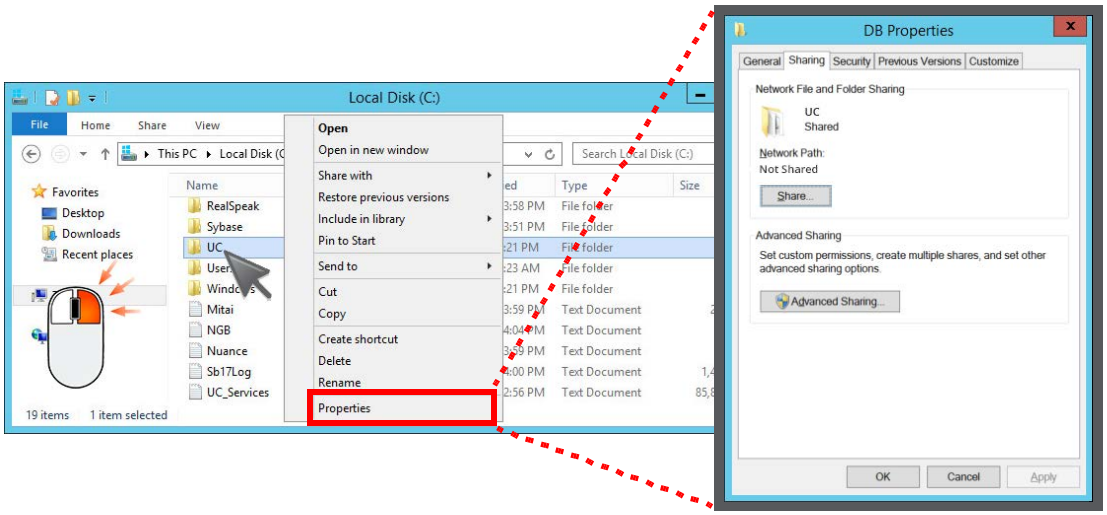
It is necessary to share the UC installation folder so that all of the programs and users have the required access. The following user accounts require full permissions to the UC folder:

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

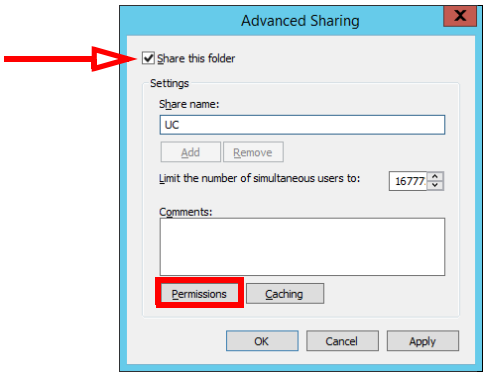
Follow this procedure on the Primary, the Consolidated, and on **each** Secondary server on the system. Also share the folder if you are using a Remote Web Server.
If you are using Remote CSE Servers, the folder only needs to be shared with the DCOM user.

Procedure

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

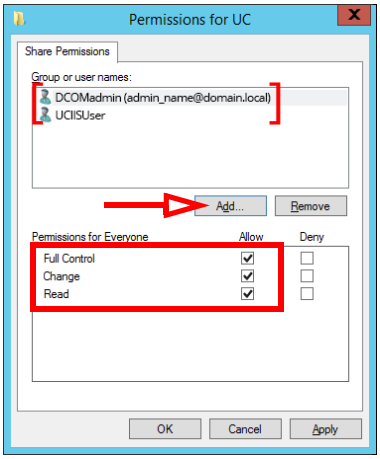


2. Click **Advanced Sharing**. Enable the **Share this folder** checkbox.



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.

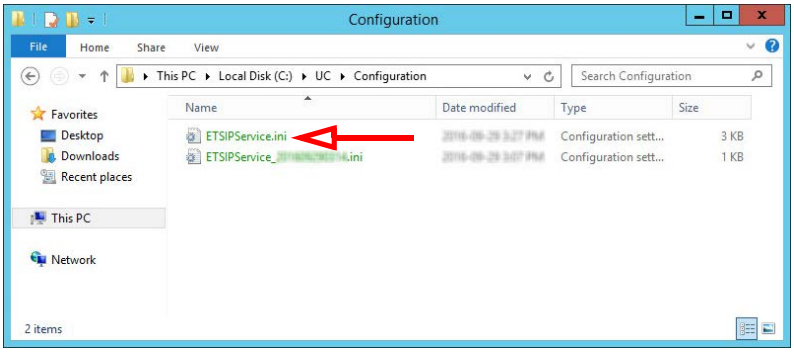
MWI Configuration

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.

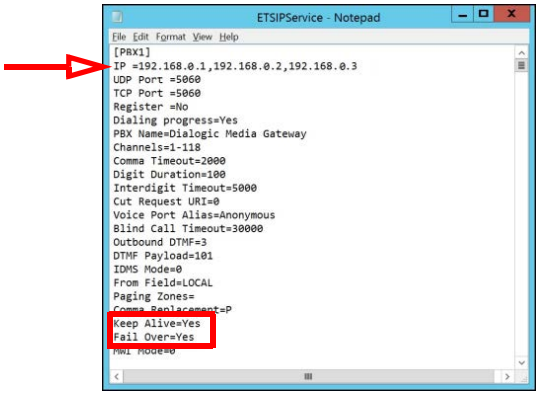
- Add a new line to the **ETSIPSERVICE.INI** file found in **/UC/Configuration** folder.



- 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 Primary and all Secondary servers) in the array.

16 DATABASE MIGRATION TOOL

In This Chapter:

Introduction

Many users of Messaging may opt to upgrade their hardware while upgrading the software. Unlike a simple upgrade, a migration also involves moving the Messaging server to a different computer in addition to updating the software. To support these customers, a database migration tool is included with the Messaging installation package.

Regardless of what version of Avaya IX Messaging you are starting from, the migration procedure is largely the same. Extra steps specific to a certain version are added where indicated.

Single Server (SS)
Current version 9.x and later (SS) updating to 10.8 (SS)
High Availability (HA)
Current version 9.x and later (HA) updating to 10.8 (HA)
Current version 9.x and later (SS) updating to 10.8 (HA)

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

Requirements	Details
License	---
Software	Existing Officelinx 9.x and later system with proper database and Avaya IX Messaging 10.8 software and license
Operating System	Windows Server 2012 Windows Server 2016

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. IXM Admin, UM Monitor).

Messaging Installation

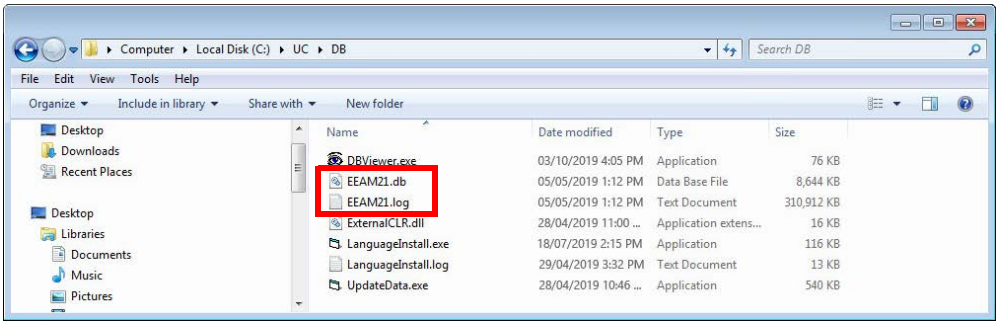
Before migrating the data from the old server, Messaging must be installed on the new server(s). For more information on installing Messaging, consult the appropriate chapters in this guide.

- Windows Server 2012 on page 105.
- Windows Server 2016 on page 51.
- High Availability on page 159.

Migration Procedure (SIP)

Once all of the preparations have been made, proceed with the migration of the data files to the new Avaya IX Messaging 10.8 server.

1. On the new server, stop all Messaging 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 10.8 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.
   On the old server, Messages will be stored in \UC\Messages, Greetings will be stored in UC\Prompts\Personal\, and Company Salutations are stored in the UC\Prompts\Company folders.
   Messages should be copied to the new 10.8 system's Messages folder (\uc\messages\), personal prompts to the prompts folder (\uc\prompts\) and so on.

Note: For Company Salutations, the name of the file must be unique since the new 10.8 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 10.8 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. Copy a **DSNConn.cfg** file from a **\UC\DBbackup*X*** folder, where ***X*** is the number of the day of the week the backup was taken. Copy the file from any one of these folders and paste it into the **\UC\DB** folder on the new server.
4. From the original installation files, copy the **Migration_Utility.exe** file to the **\UC\DB** folder on the new server.

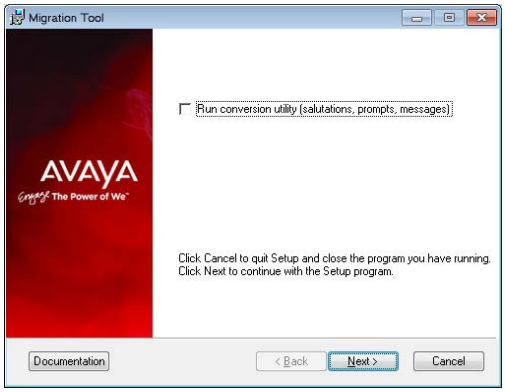
Note: In an HA environment, the server migrated using this utility will become the Primary server on the new HA system. The Consolidated and Secondary servers must all be fresh installs; no migration is required.

5. Run (double-click) the application that you have just copied. The Migration Utility Wizard will start.

   Click **Next** to continue.

6. Ensure that the **Run conversion utility...** checkbox is disabled.

   Click **Next**.

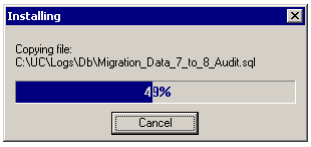


7. The application will stop the necessary services before proceeding.

8. 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.

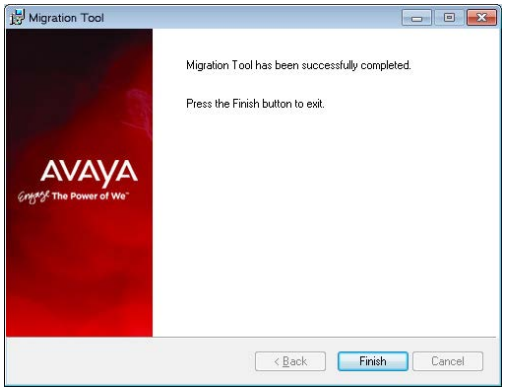
9. Once the unload process is complete, the application will migrate the database. This process may take a while depending on the size of your database. Please be patient.

10. Files will be moved and replaced accordingly.

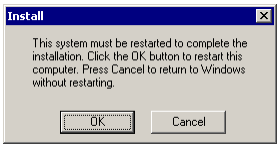


11. You will see this screen when the process has completed.

    Click **Finish** to exit the Migration Wizard.



12. When prompted, click **OK** to restart your computer.



The old database is now ready to be used with the new 10.8 system.

17 DEDICATED CSE SERVER INSTALLATION

In This Chapter:

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 CSE server to your system please follow the instructions in this document accurately.

Requirements

Requirements	Details
License	---
Software	Existing Avaya IX Messaging system to integrate with.

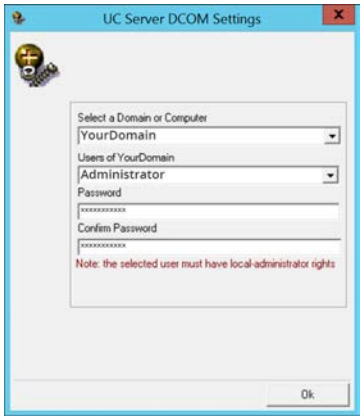
Dedicated CSE Server Installation

1. On the computer designated as the Remote CSE Server, open the Avaya IX Messaging folder on your server hard drive and run **Setup.exe** to launch the installer.

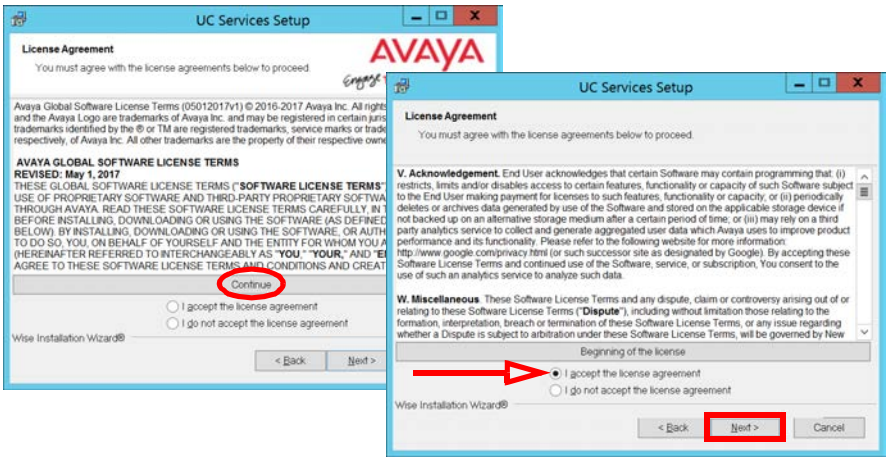
   When prompted, click **Next**.

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.

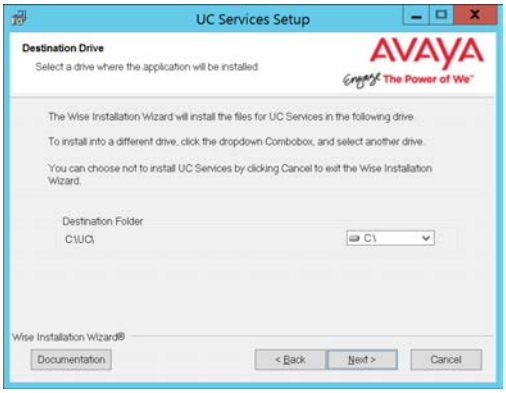


3. Review the license agreement. Click **Continue**, enable the **I accept the license agreement** checkbox, then click **Next**.



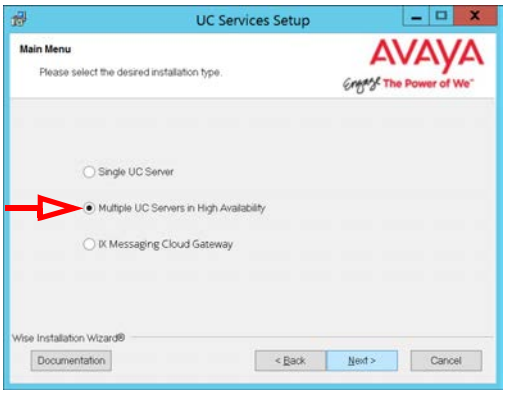
4. You will be asked to select the destination directory for the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a **UC** folder on the C drive.

   Click **Next** to continue.



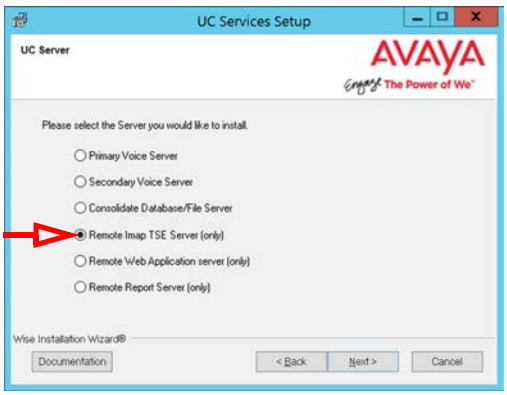
5. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.



6. Select **Remote CSE Server (only)** (formerly the Imap TSE server).

   Click **Next**.

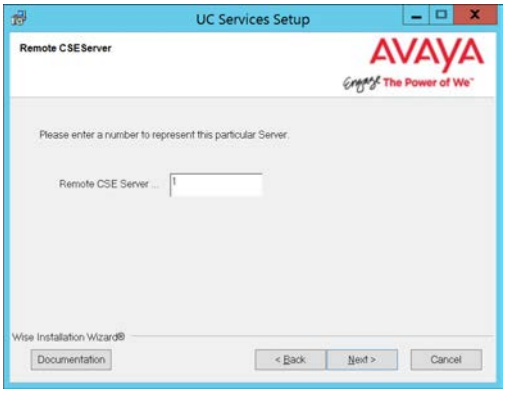


7. Enter a number between 1-25 for this server.

   If you configure multiple CSE servers, each must be given a unique number; no two servers can share the same number.

   Avaya IX Messaging supports up to 4 CSE servers.

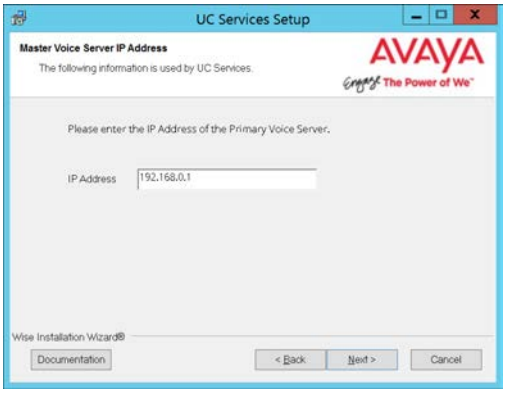
   Click **Next**.



Note: Each CSE server can support up to 5000 users.

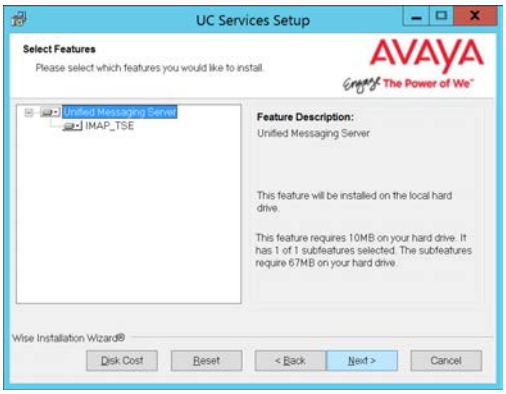
8. Enter the IP Address of the **Primary** server.

   Click **Next**.



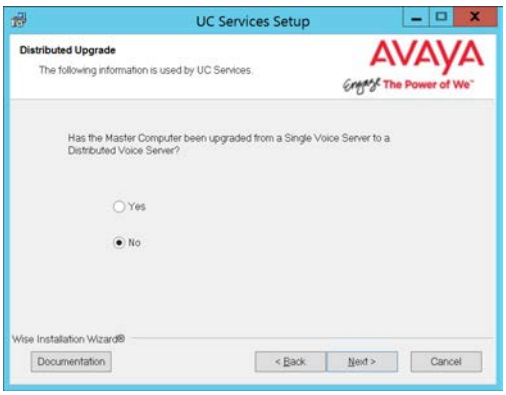
9. Select the **Components** required at your site. Disable any components that are not needed.

   Click **Next.**



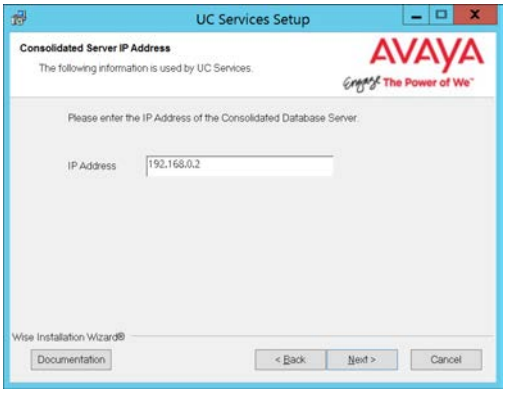
10. Unless the Primary Server has been upgraded from a Single Server configuration, choose **No**.

    Click **Next**.



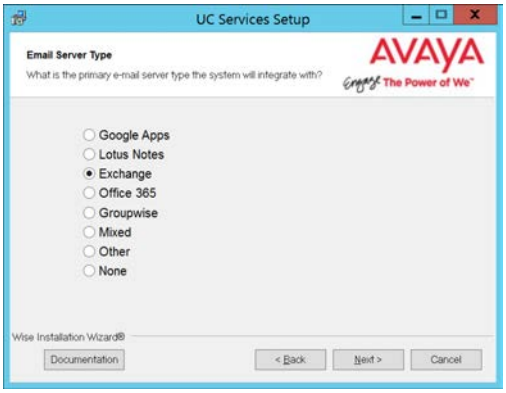
11. Enter the IP Address for the **Consolidated** server.

    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.

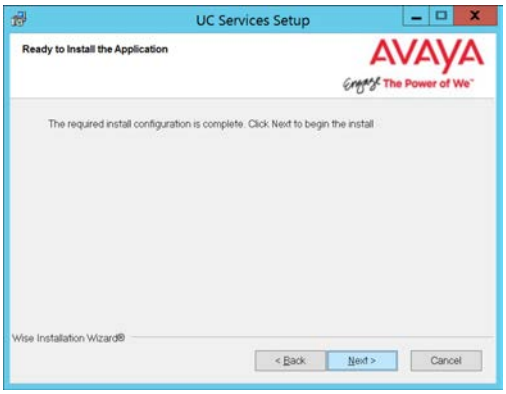
    When ready, click **Next**.



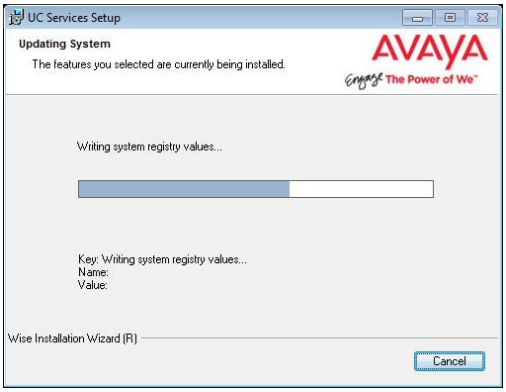
> **Note**: Each Remote CSE Server supports a **single** email type (e.g. Exchange, Office 365, Gmail, etc.). If more than one email type is required, the Consolidated Server cannot be used for synchonization.

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

    Click **Next**.

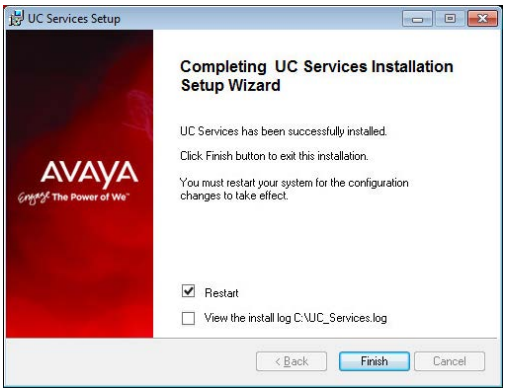


14. The selected components will now be installed. This process may take a while.



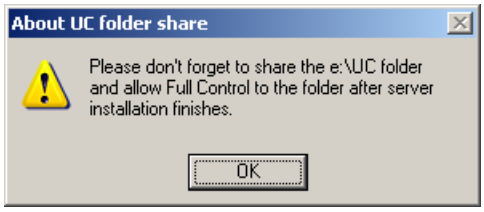
15. Click **Finish** to restart the server.

    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 256 for details).



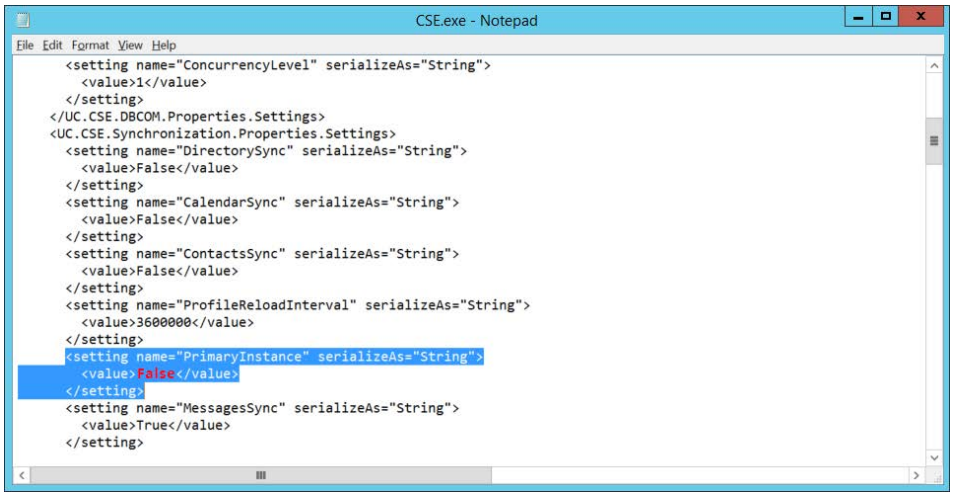
The Remote CSE server installation is complete.

Configuration For Remote CSE server installations

Once you have finished configuring the dedicated CSE server, you must configure your voice server to finalize the changes.

1. On the **Consolidated** and the **Remote CSE** 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.



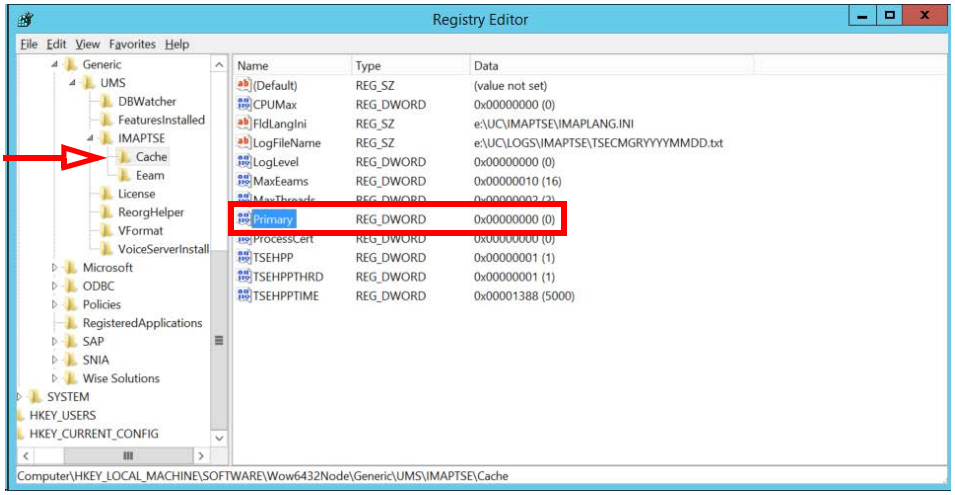
2. On both of the Consolidated and the Remote CSE servers, open the Registry.

   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**.

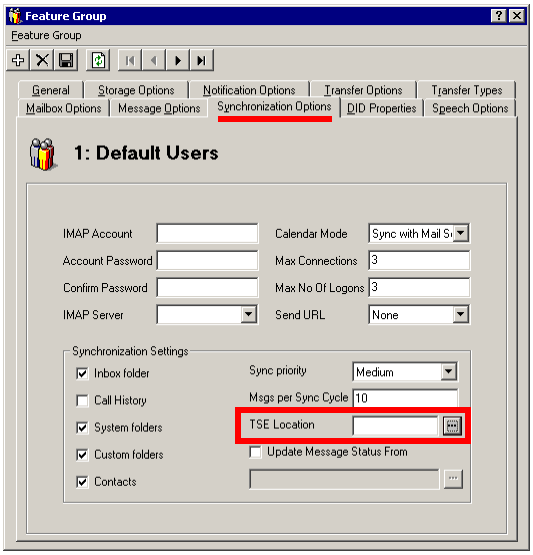
   On 32-bit operating systems, scroll down to **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Generic\UMS\IMAPTSE\Cache**.

   Verify that the value for **Primary** is **0**.

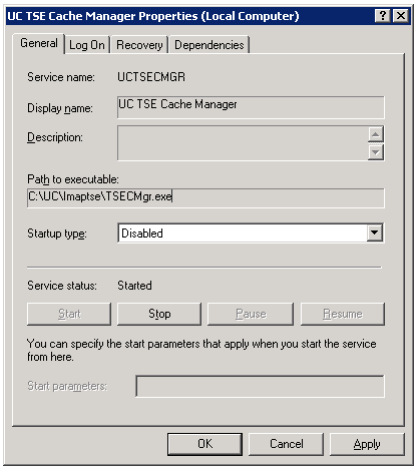


3. Restart the server to complete the configuration changes.

4. Open a **Feature Group** in the **IXM 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 Cache 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.



18 DEDICATED WEB SERVER INSTALLATION

In This Chapter:

520 The Remote Web server installation is complete.

Introduction

The Dedicated Web Server allows you to separate web portions of Avaya IX Messaging from the voice server so that you to balance the work load on each system and facilitate a customized network environment. Most web related Messaging 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

Requirements	Details
License	---
Software	Existing Avaya IX Messaging system to integrate with IIS installed on the OS.

Dedicated Web Server Installation

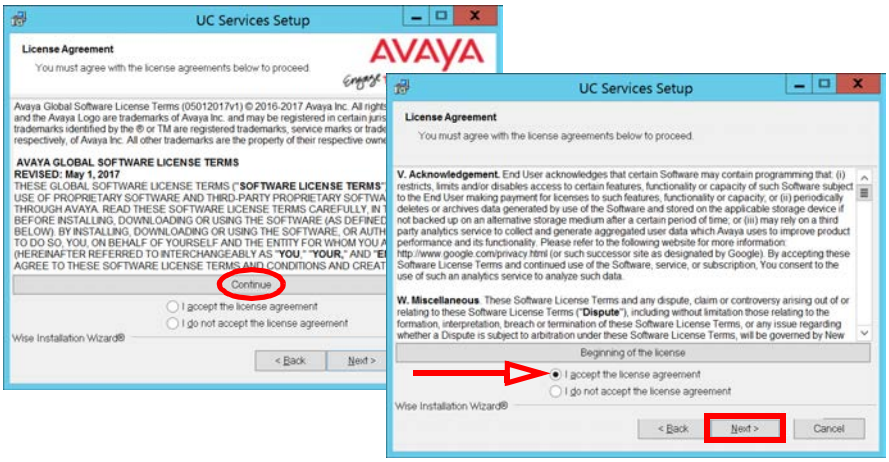
1. On the computer designated as the Remote Web Server, open the Avaya IX Messaging folder on your server hard drive and run **Setup.exe** to launch the installer.

   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.

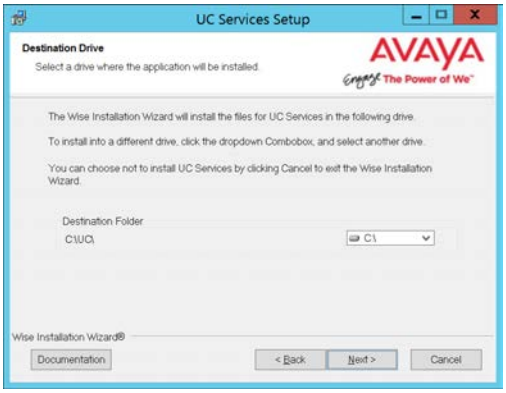
   Click **OK** after entering the credentials.

3. Review the license agreement. Click **Continue**, enable the **I accept the license agreement** checkbox, then click **Next**.



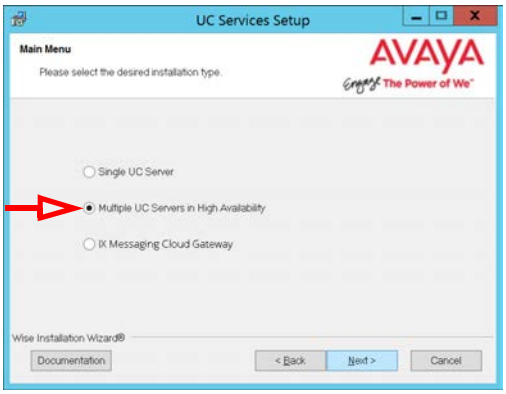
4. You will be asked to select the destination directory for the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a **UC** folder on the C drive.

   Click **Next** to continue.



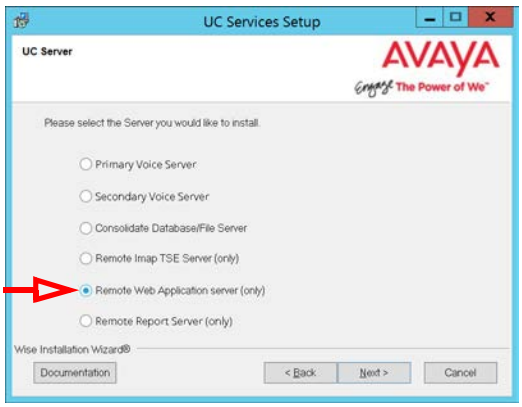
5. Enable **Multiple UC Servers in High Availability**.

   Click **Next**.



6. Select **Remote Web Application server (only)**.

   Click **Next**.

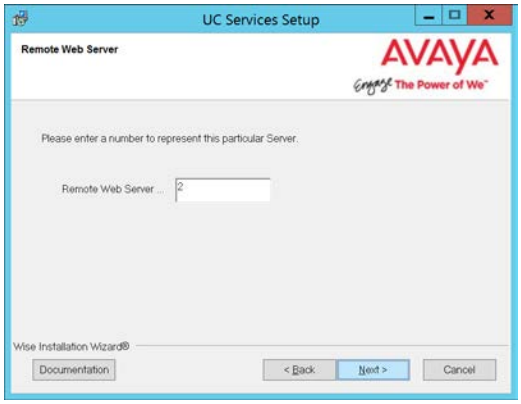


7. Enter a number between 1-14 for this server.

   If you configure multiple Web servers, each must be given a unique number; no two servers can share the same number.

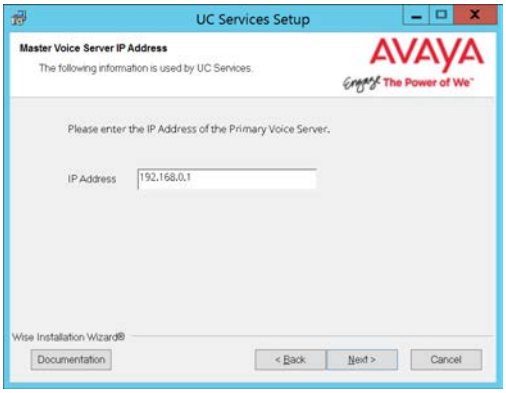
   Avaya IX Messaging supports up to 14 Web servers.

   Click **Next**.



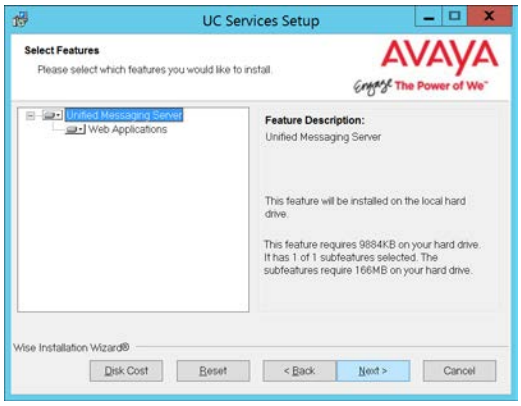
8. Enter the IP Address of the **Primary** server.

   Click **Next**.



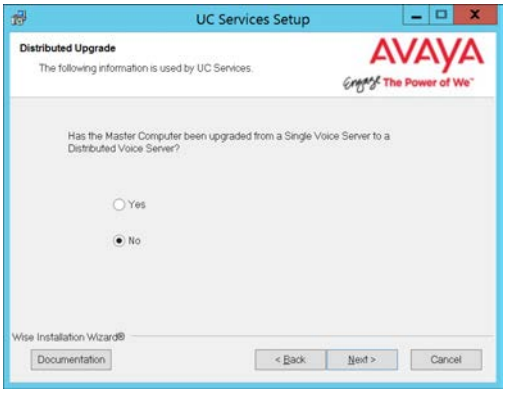
9. Select the **Components** required at your site. Disable any components that are not needed.

   Click **Next.**



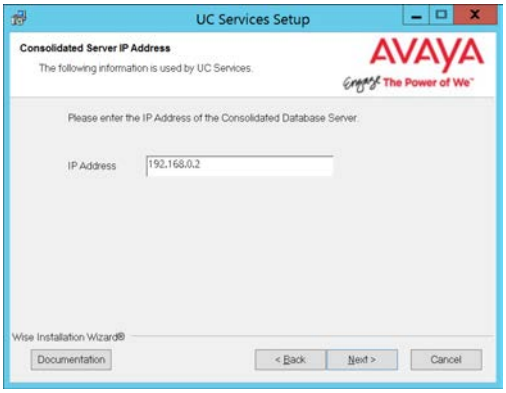
10. Unless the Primary Server has been upgraded from a Single Server configuration, choose **No**.

    Click **Next**.



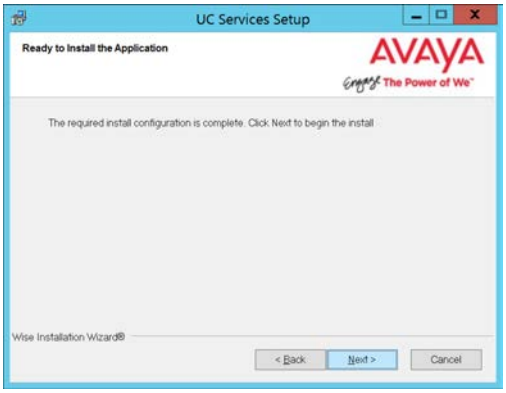
11. Enter the IP Address for the **Consolidated** server.

    Click **Next**.

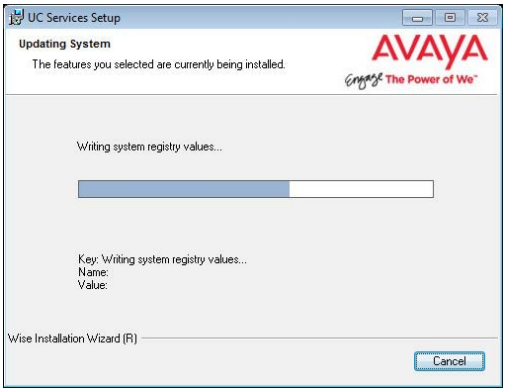


12. The preliminary information required for installation is now complete.

    Click **Next**.

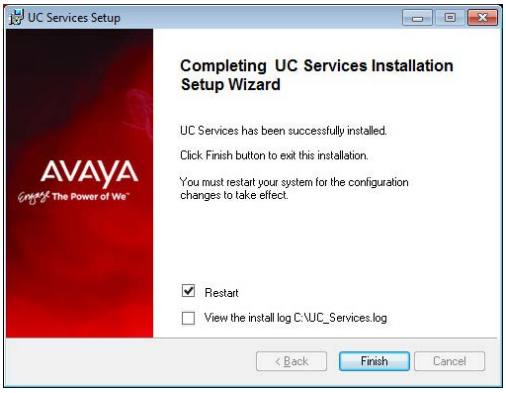


13. The selected components will now be installed. This process may take a while.



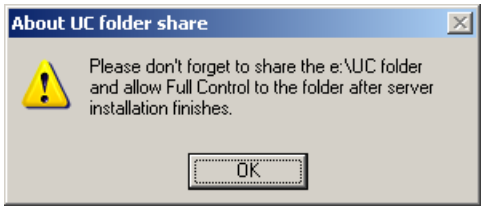
14. Click **Finish** to restart the server.

    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 256 for details).



The Remote Web server installation is complete.

19 LANGUAGE PACK INSTALLATION

In This Chapter:

Introduction

By installing a language onto an existing Messaging system, you will be able to address the needs of specific regions and audiences. This transforms the Messaging 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 installation package.

The following table lists the languages available.

English	English TTY	German	Spanish
English UK	French	Italian	Spanish EU
	French EU	Portuguese BR	

This table shows the languages available for use with the Text-to-Speech Engine (TTS), and Automatic Speech Recognition (ASR).

Language	Regional Variation (if any)
English	**(program default)**
English AU	Australia
English UK	United Kingdom
French	North America
French EU	Europe
German	
Italian	
Portuguese BR	Brazil
Spanish	Americas
Spanish EU	Europe

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**

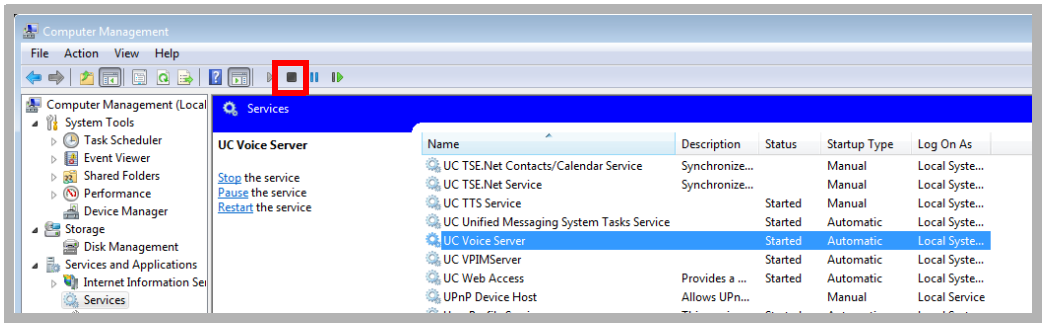
Note: Take care to refer to Internet Information Services (IIS) on your PC and ensure that the FTP server is installed and running. Close all Server-related programs (i.e. UM Admin, UM Monitor).

Stop Messaging 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 IX Messaging installation package. All other languages are available for download from Avaya Inc. Contact your reseller for more details.

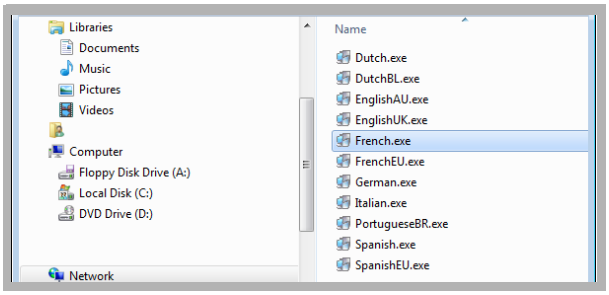
The downloaded files are in executable (EXE) format, and there is a single file for each available language. Download the file to a local drive and double-click to install the chosen language onto the voice server.

Note: Once installed on the server, the language must be selected through IXM Admin before it will be available.

Language Pack Installation

Note: The Messaging 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.

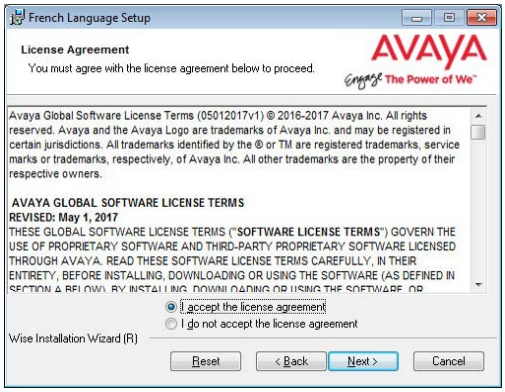


3. The program will begin preparing to install the language pack.

4. At the Welcome screen, click **Next** to continue.

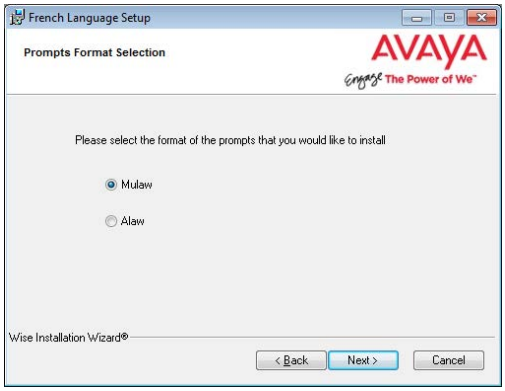
5. When prompted with the **End User License Agreement**, enable **I accept the license agreement**.

   Click **Next** to continue.



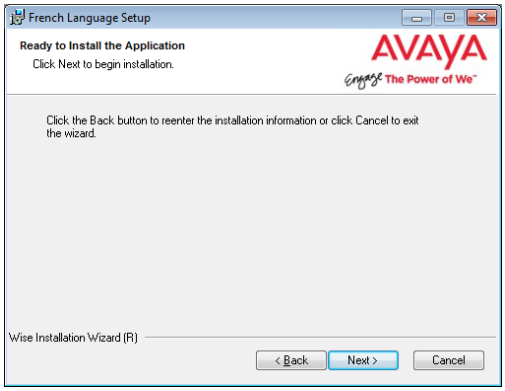
6. Select the appropriate format for voice prompts (**Mulaw** or **Alaw**).

   Click **Next**.



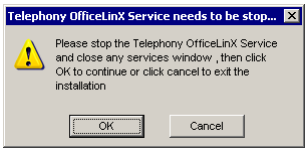
7. The wizard is ready to install the language pack.

   Click **Next** to begin the installation.

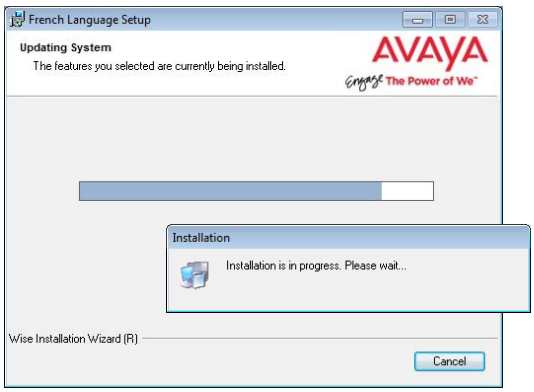


8. If you have not stopped all the necessary services, you will be prompted to do so at this point.

   Stop the services then click **OK** to continue.



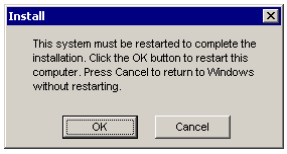
9. Installation will begin and all of the components for the selected language will be copied to the server.



10. You will be notified when the installation is complete.

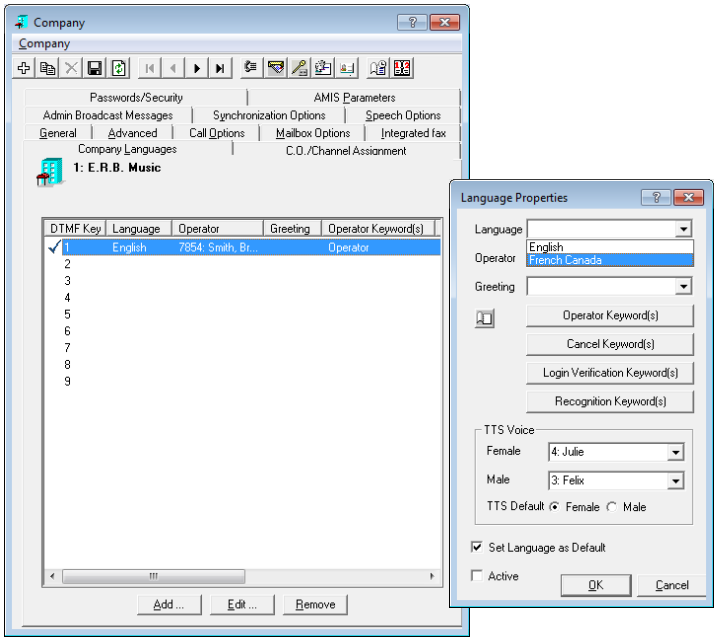
    Click **Finish**.

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 **IXM 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.

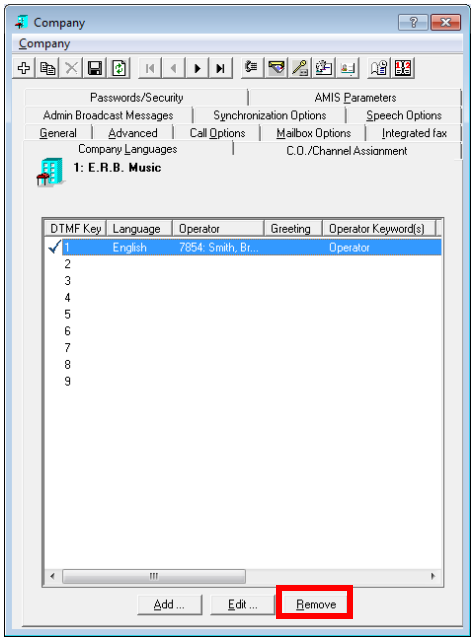
Set Language as Default: Enable this option to set the current language as the first one that callers will hear when connecting to the system.

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.

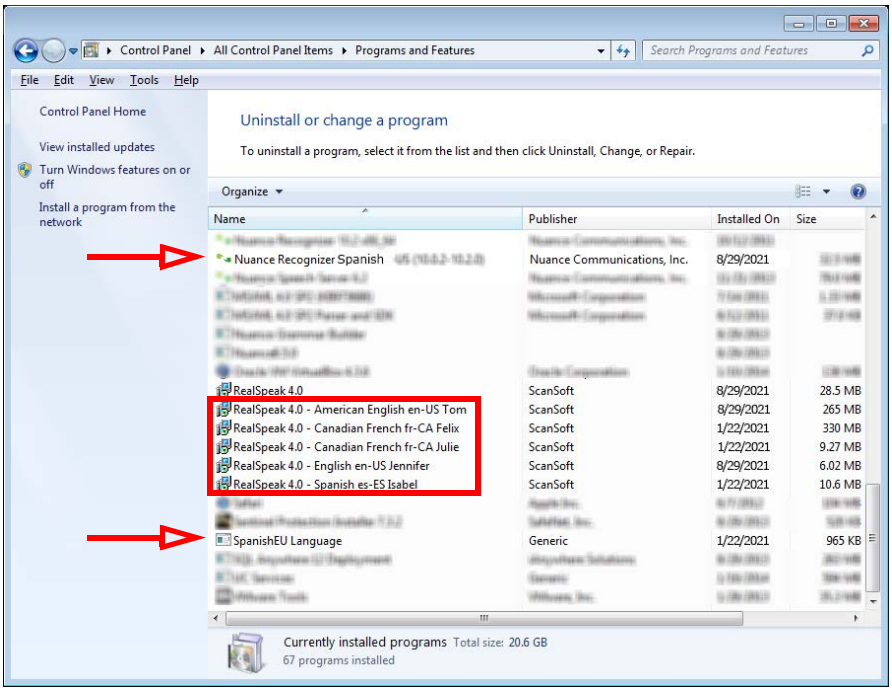
Deleting Languages from the Server

1. To remove the language pack and files from the voice server, begin by Removing the language from the system in IXM 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.
4. Delete the **Nuance Recognizer** entry for the language you want to remove.

   The server must be restarted after the files have been removed.



5. After the server has rebooted, delete the language file from the Programs and Features window.

20 SERVER BACKUP USING CARBONITE AVAILABILITY

In This Chapter:

Introduction

Warning: Carbonite Availability **CANNOT** be used in a high-security (JITC) installation.

An Avaya IX Messaging High Availability installation provides the means to maintain operations through failures in the Primary 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.

Important: Carbonite Availability can be used **ONLY** with the HA Consolidated server. It cannot be applied to the Primary or Secondary servers, Remote CSE or Admin, Single Server machines, etc.

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. This license must be renewed annually.

Before proceeding, the Messaging 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 Consolidated server and the backup machines (a server pair) must be using the same operating system with identical hardware.

REQUIREMENTS	DETAILS
Carbonite Availability	v. 8.2
Operating System	Windows Server 2012 or 2012 R2 Windows Server 2016
Network Cards	2 NICs are required in both the Consolidated and Backup servers

Terminology

Carbonite Availability uses the terms Source and Target to describe the two servers in each pairing. The computer that manages the process is known as the client.

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 (the Consolidated server).

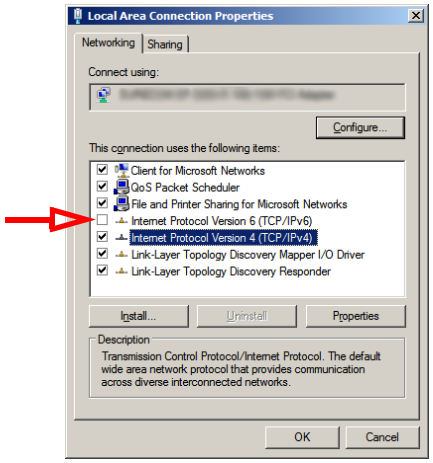
Target: This is the backup server. The Target is a real-time mirror of the Source, but does not itself handle live traffic.

Client: This can be any other computer that has network access to the Source and Target servers. It can be installed on either the Source or Target servers, or one or more other computers on the network. The 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.

Configuring the Network Cards

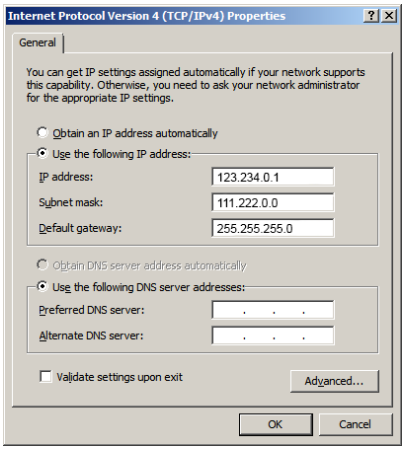
Both servers (source and target) in each pair must have **2 NIC**s installed. On each machine, designate one to be the primary and the other as the secondary NIC. Perform the following procedure on both the Source and Target servers.

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.



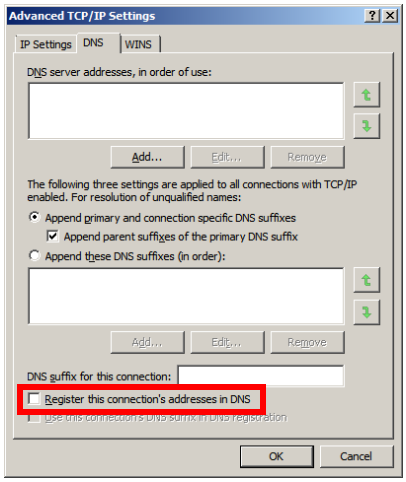
3. Enter the IP Address that the secondary NIC is to use.

   Leave the DNS server details empty.

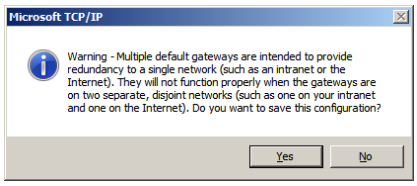


4. Click **Advanced** and open the **DNS** tab.

   Disable the option to **Register this connection's addresses in DNS**.



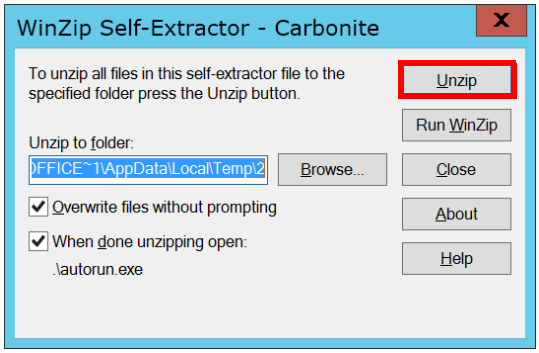
5. Click **OK** to save the configuration. If prompted, click **Yes** to continue passed the warning.



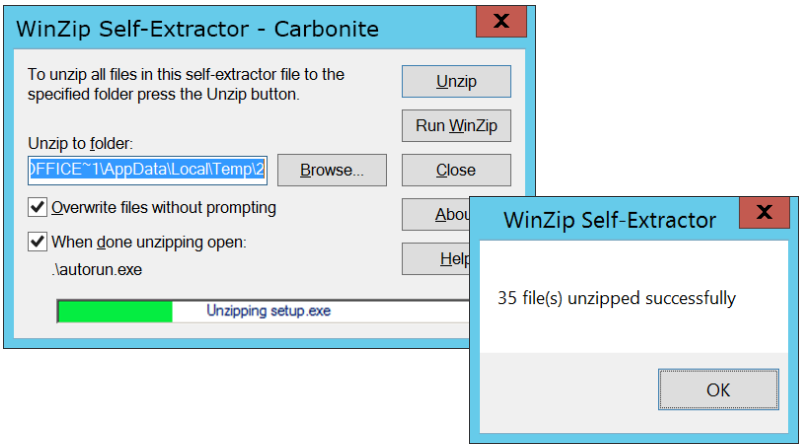
Installing Carbonite Availability on the Servers

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).

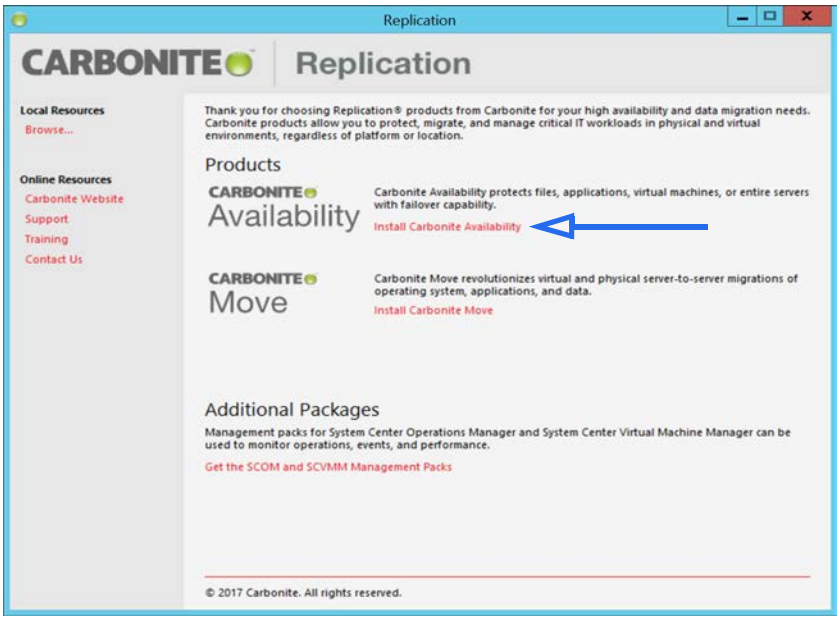
1. Double-click the program to start the installation.
2. Specify the location on your hard drive where the compressed files should be extracted to.
   Click **Unzip**.



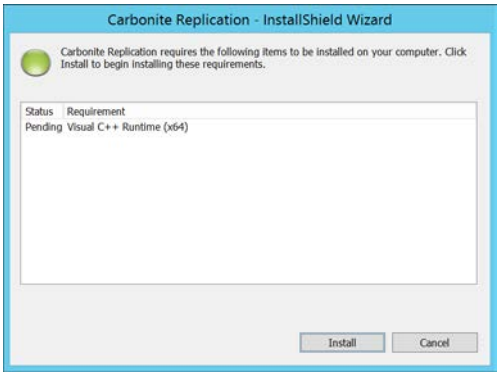
3. The files will be unpacked onto your drive. When finished, click **OK** to continue.



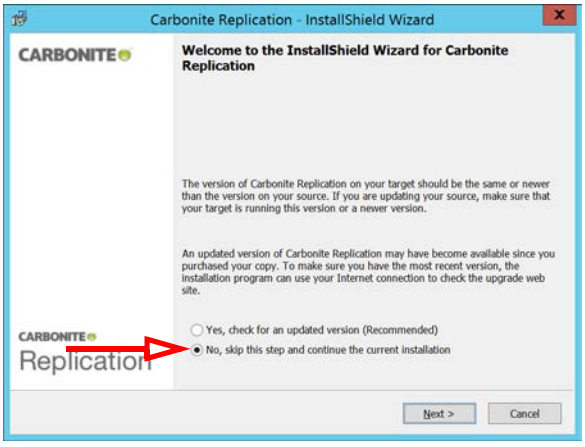
4. From the main screen, select **Install Carbonite Availability**.



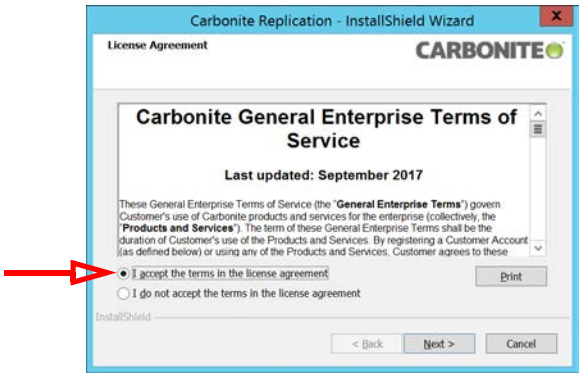
5. Any required applications that are not installed on your system will be added now. Click **Install** to continue.



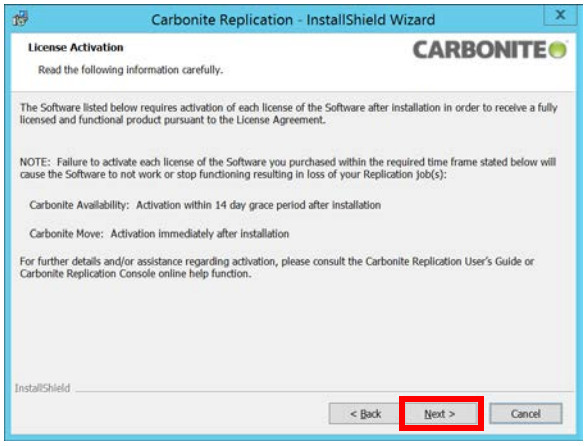
6. When prompted to check for the latest installation, select **No** and click **Next** to continue.



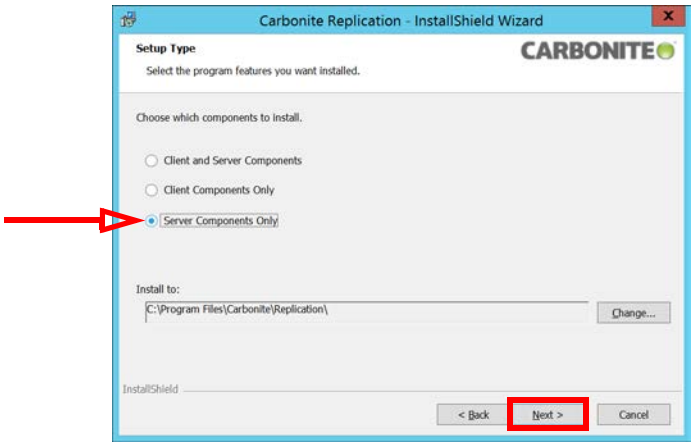
7. Accept the terms of the license agreement and click **Next** to continue.



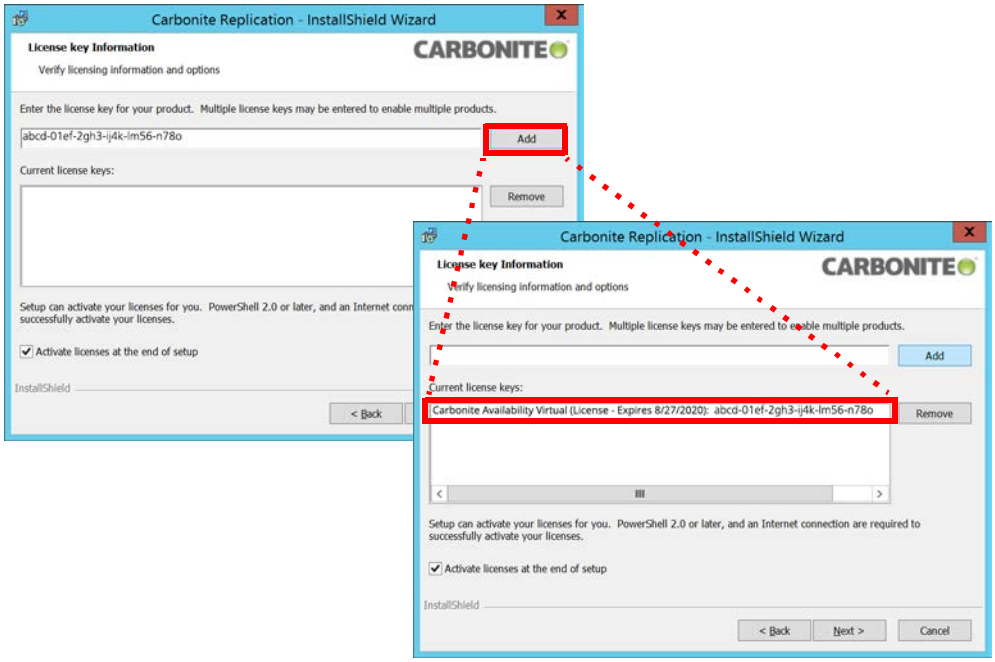
8. Click **Next** to activate the license.



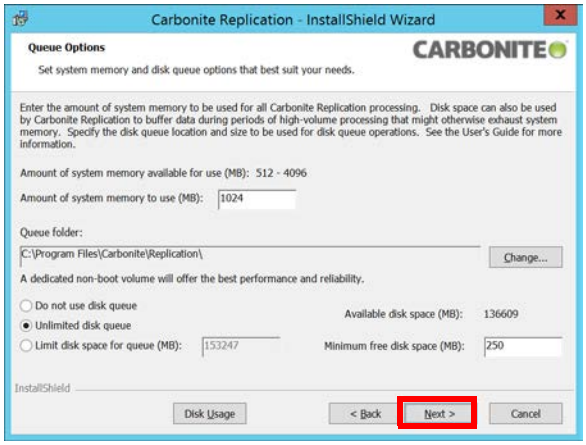
9. Enable **Server Components Only**, then click **Next**.



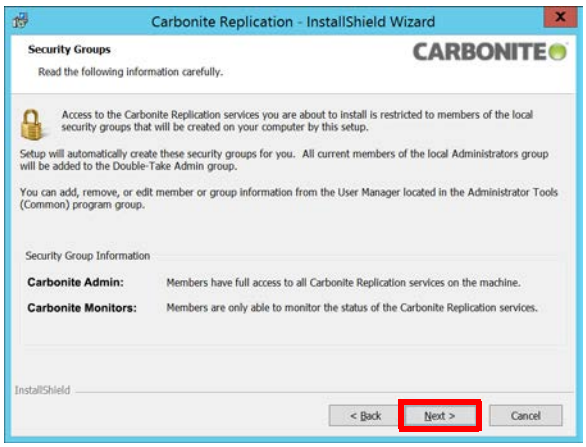
10. Enter the license key that came with the program into the space provided. Click **Add** to install the license onto the computer. Click **Next** to continue.



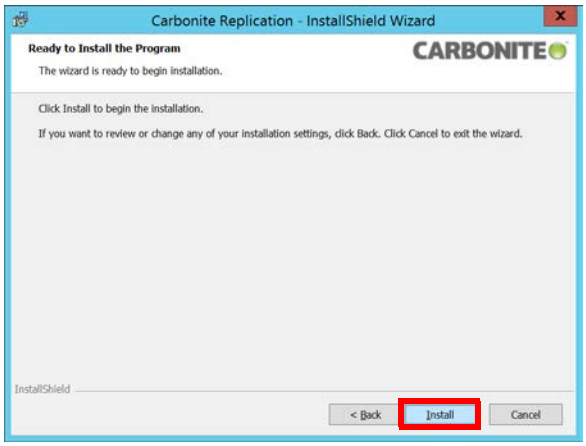
11. Leave all settings at their defaults. Click **Next** to continue.



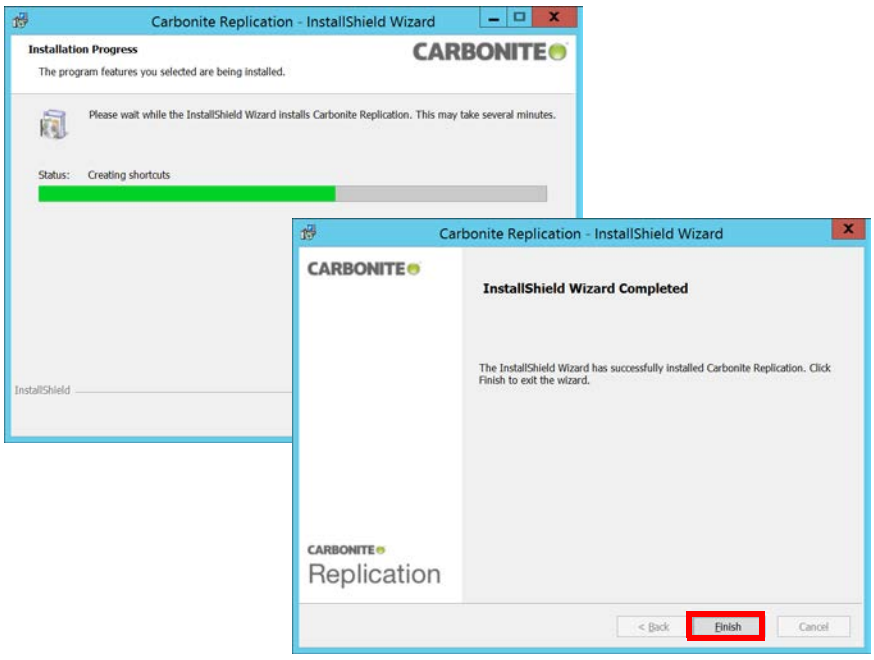
12. Click **Next** at the **Security Groups** screen.



13. Click **Install** to begin adding the program to the server.



14. The program will be installed. Click **Finish** when prompted.

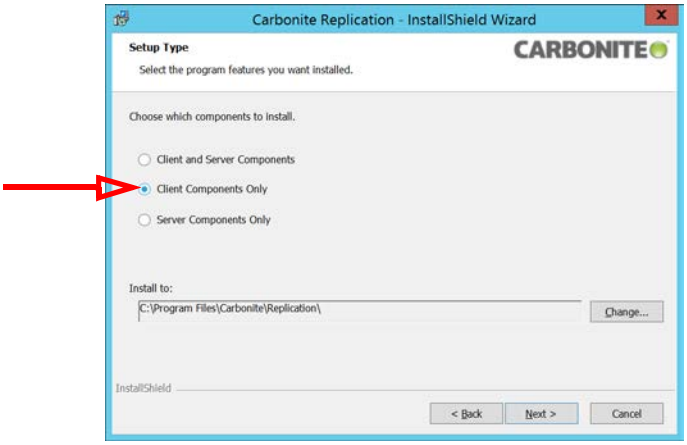


Installing Carbonite Availability on the Client

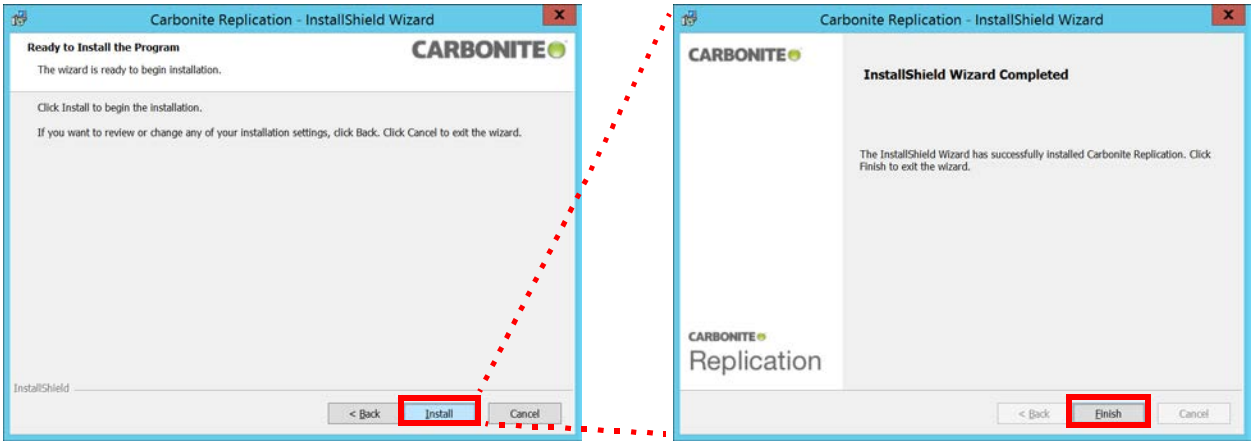
A computer is required to act as the client/manager for the servers. This machine can be any that has network access to the Source and Target servers. It can be installed on either the Source or Target servers, or one or more other computers on the network. The client can be installed on any computer 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.

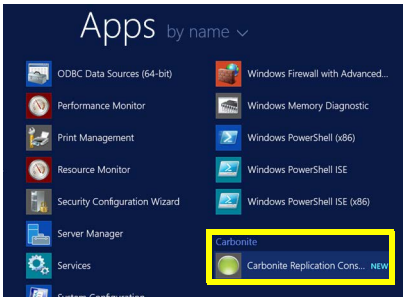
1. Install the software on the client computer as shown above, but when step 9 is reached, choose **Client Components Only** instead and continue.



2. Complete the installation.



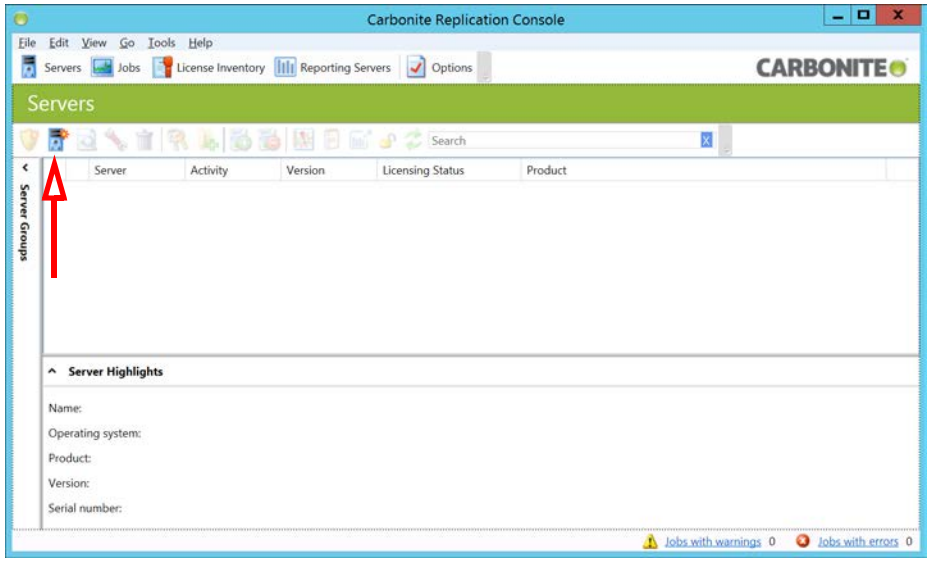
3. The Carbonite Replication console will be installed onto the client machine. Use this application to configure the disaster recovery and failover details for the 2 servers.



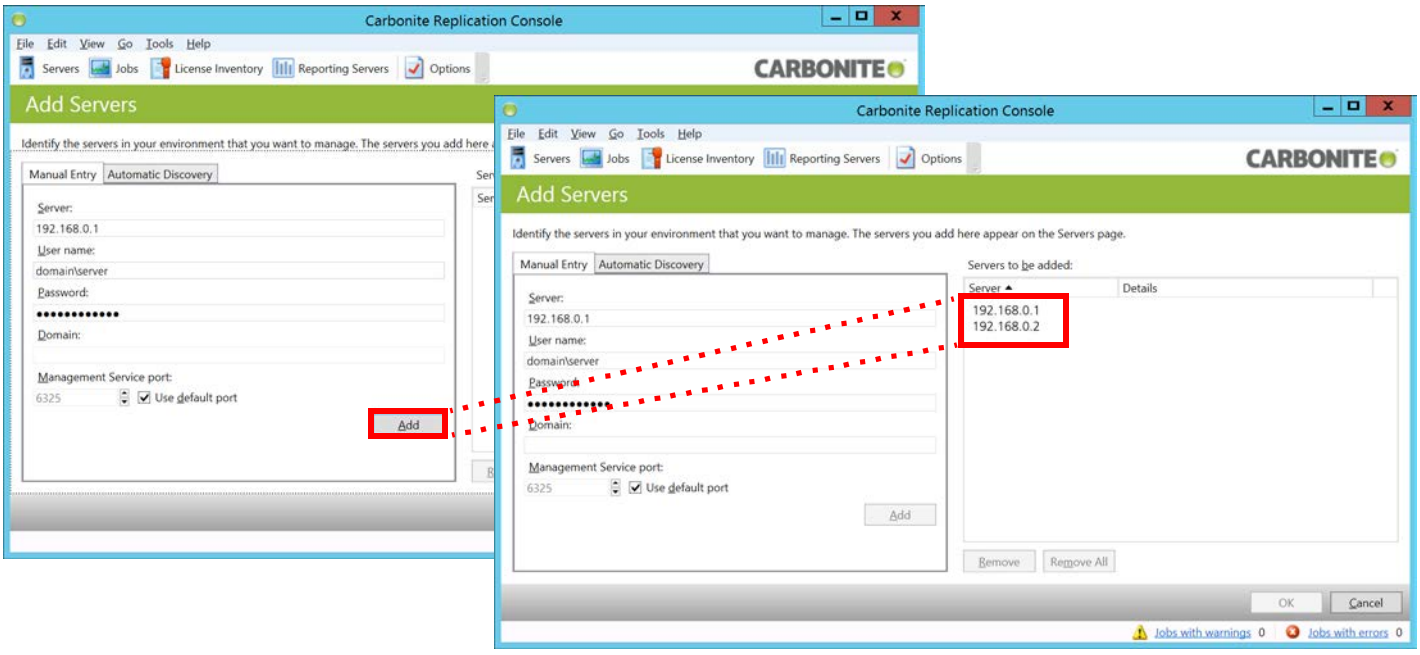
Configuring Failover

Setting up the details of the failover is done from the client computer using the **Carbonite Replication Console**.

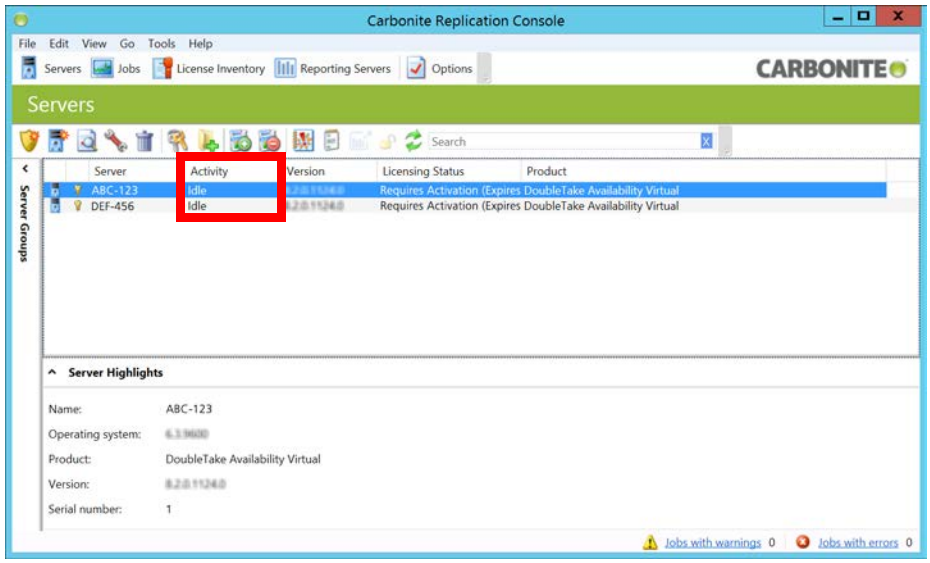
1. Double-click the console icon on the **Client** computer to start the console.
2. From the main screen, click the **Add servers** icon.



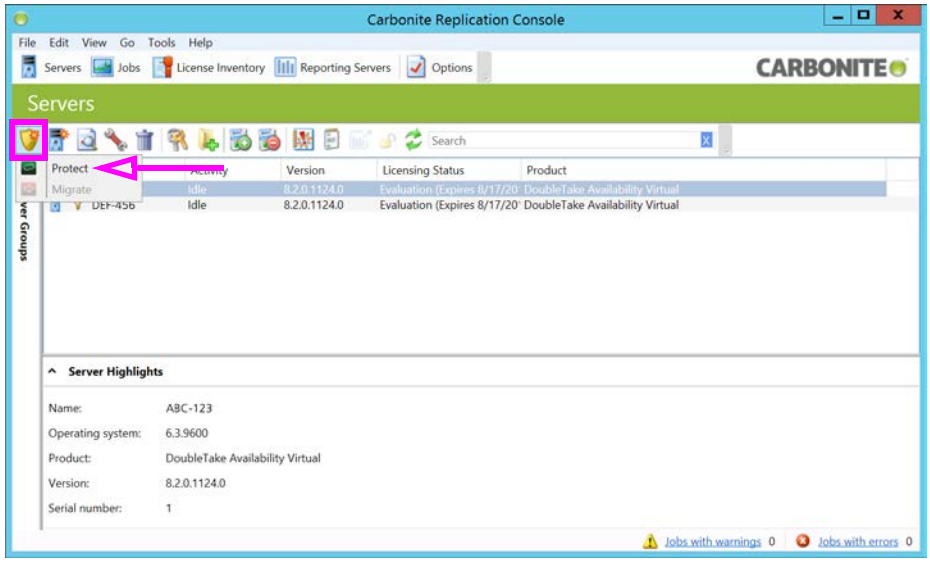
3. On the **Manual Entry** tab, enter the required details for the Primary NIC on one of the Source servers. Click **Add** when ready.
   Repeat for the Primary NIC on the other server.
   Click **OK** when finished to add both servers to the console.



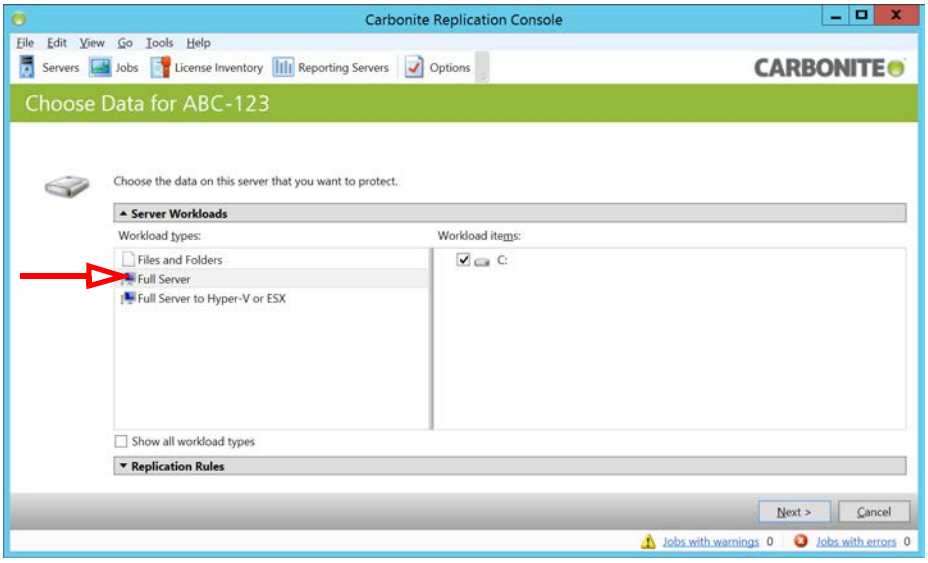
4. The Secondary NICs for both servers appear on the main screen of the console.
Under the **Activity** column, anything other than **Idle** means that an error has occurred. In this case, delete the server and repeat step 1 to 3.



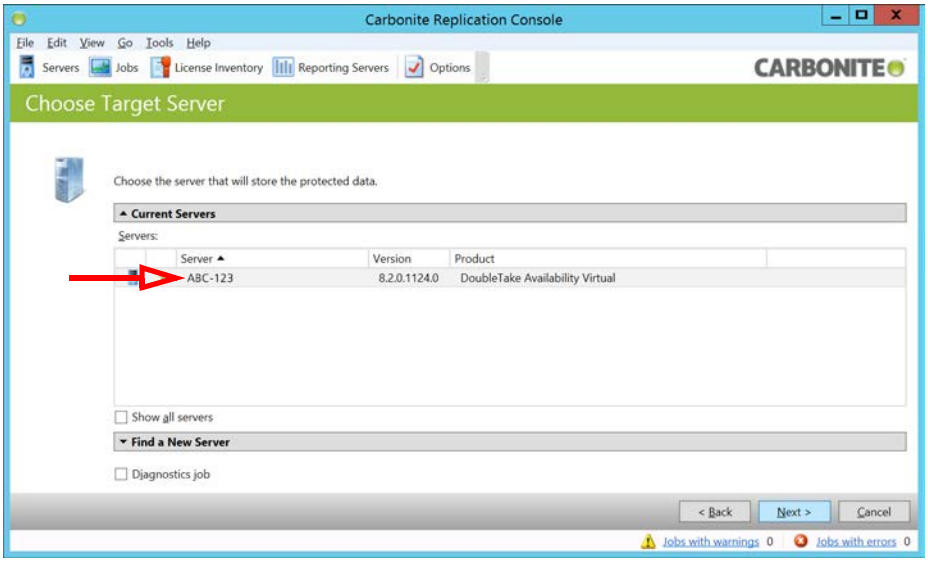
5. Select the **Source** server. Click the **Create New Job** icon and choose **Protect** from the dropdown menu.



6. Choose **Full Server** and click **Next**.



7. Choose the **Target** machine to mirror the Source files onto, and click **Next**.



8. Configure the settings for the failover monitor. Scroll down to reveal additional options.

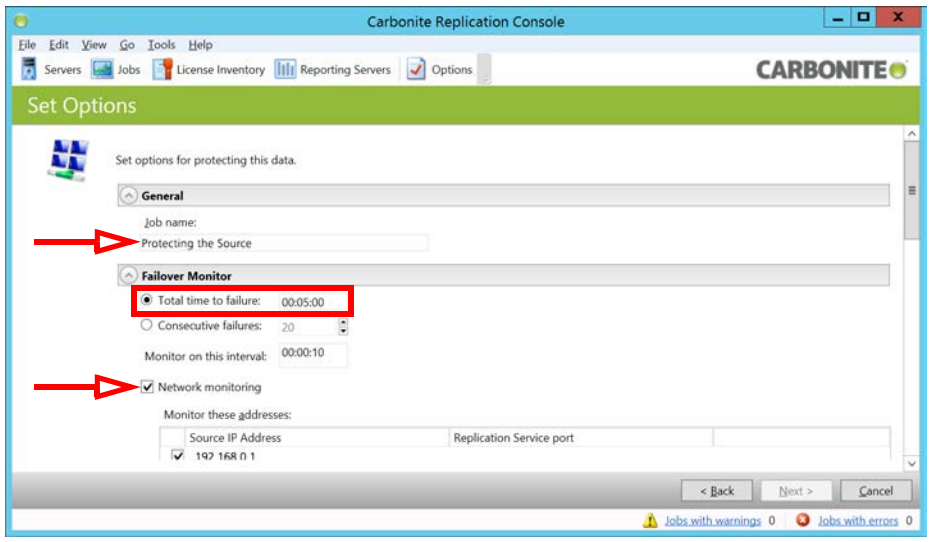
General

- **Job name** can be anything. Make it user friendly to make the job easier to manage.

Failover Monitor

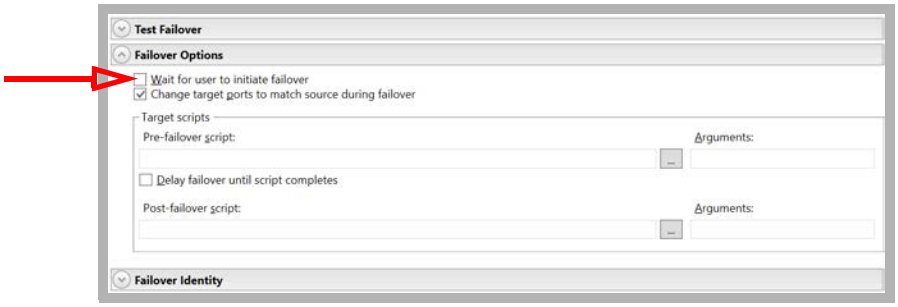
- Enable **Total time to failure** and enter the maximum time that the Source can be unresponsive before initiating the failover. Entering a value that is too small may trigger failovers during a scheduled reboot of the Source. The Target server monitors this connection as it continuously mirrors data, 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**.**



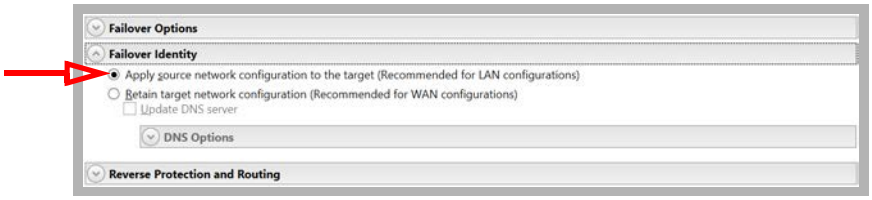
Failover Options

- Disable **Wait for user to initiate failover** to make the process automatic.



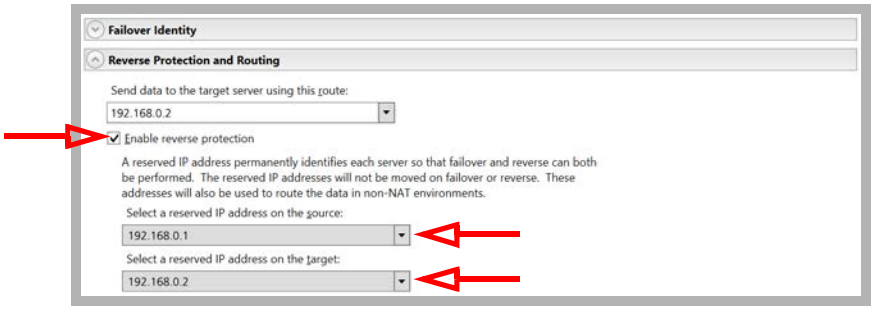
Failover Identity

- 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.



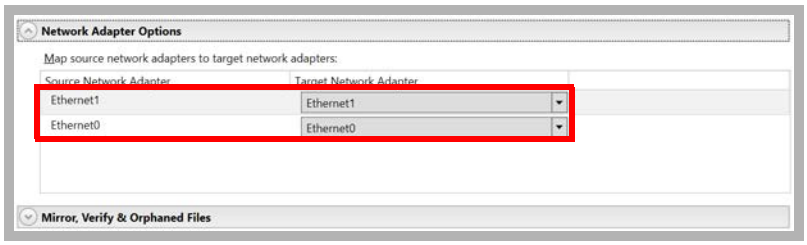
Reverse Protection and Routing

- 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

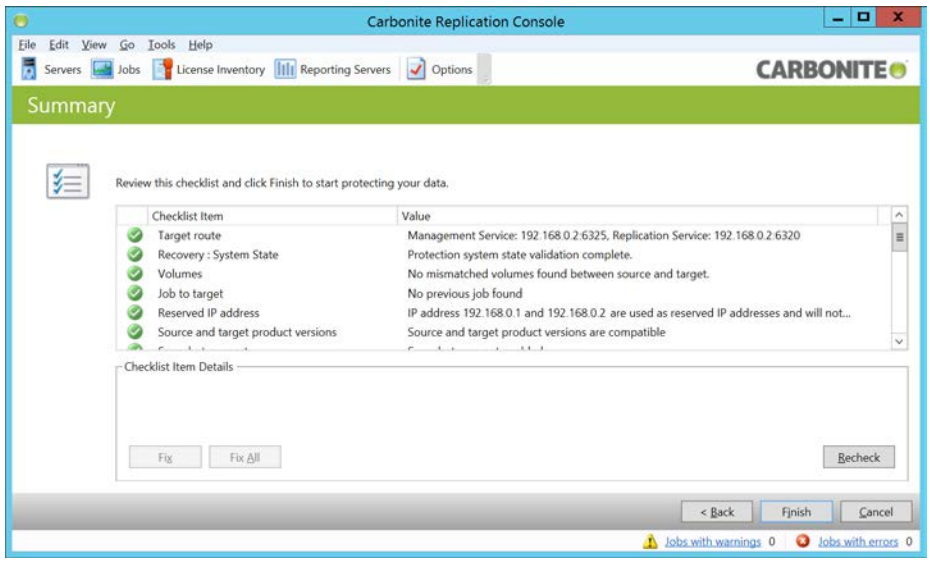
- Under **Map source network adapters to target network adapters**, use the dropdown menus to match the Primary NIC on the Source server with the Primary NIC on the Target server. Do the same for the Secondary cards.



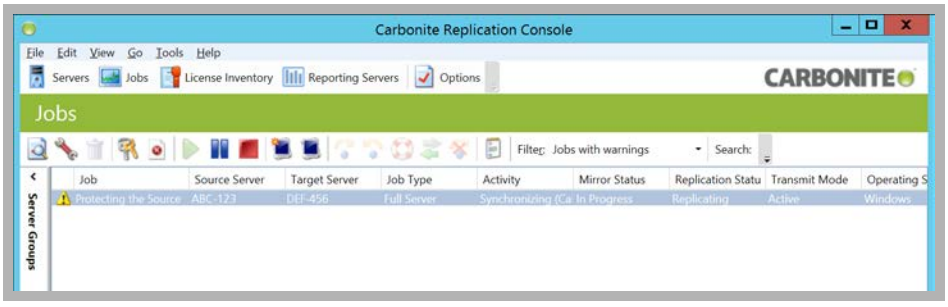
Leave all other settings at their default values.

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 Messaging 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.

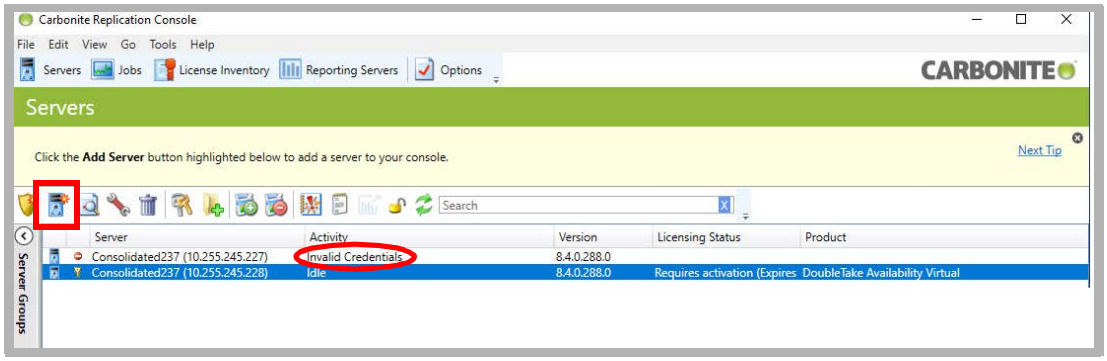
Drives Damaged/Formatted/Replaced

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.

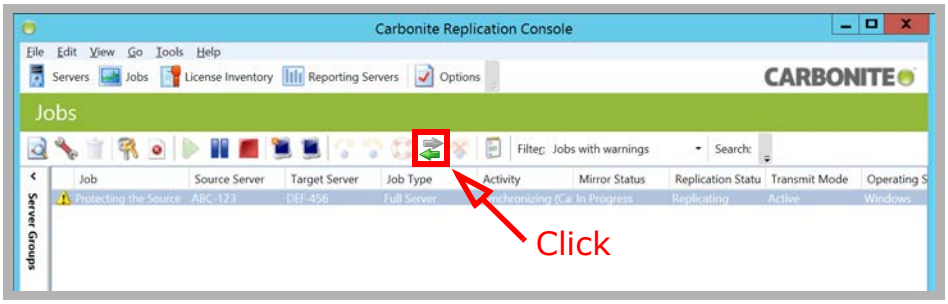
Running Recovery

When the server comes back online, Carbonite will require the credentials for that machine to be entered before the system recovery can start.



Enter the credentials.

After logging in, the restored server must have Carbonite's **Reverse Protection** enabled manually.



Once **Reverse Protection** has been enabled, the system recovery will begin.

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.

REQUIREMENTS	DETAILS
Carbonite Availability	v. 8.2
Operating System	Windows Server 2012 or 2012 R2 Windows Server 2016
Network Cards*	1 NIC is required in both the Consolidated and Backup servers

* - 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 Messaging 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. The computer that manages the process is known as the client.

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.

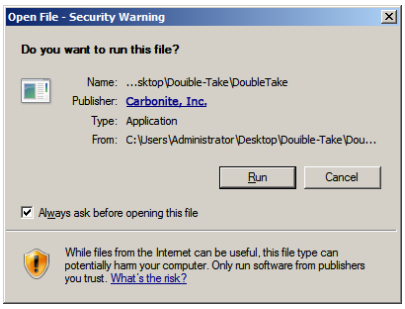
Target: This is the backup server. The Target is a real-time mirror of the Source machine, but does not itself handle any live traffic.

Client: This can be any other computer that has network access to the Source and Target servers. It can be installed on either the Source or Target servers, or one or more other computers on the network. The 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.

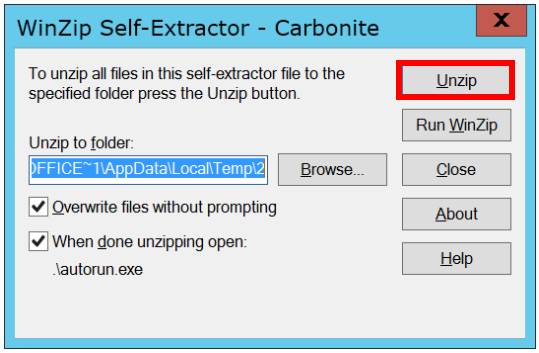
Installing Carbonite Availability on the Servers (WAN)

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.

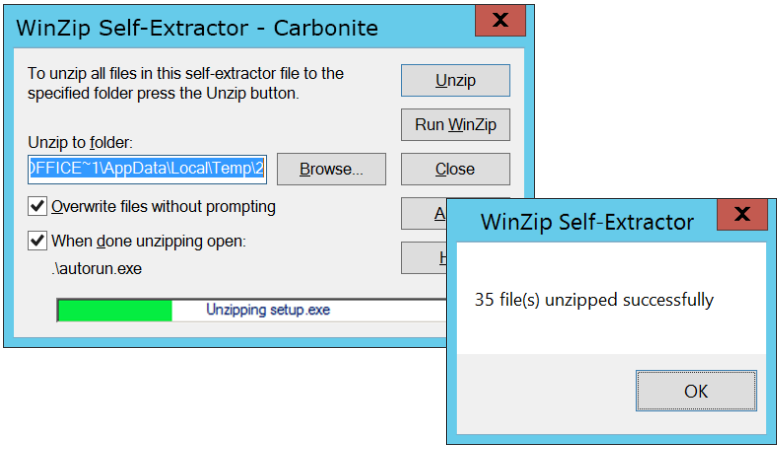
1. Double-click the program to start the installation.
   Click **Run** to continue.



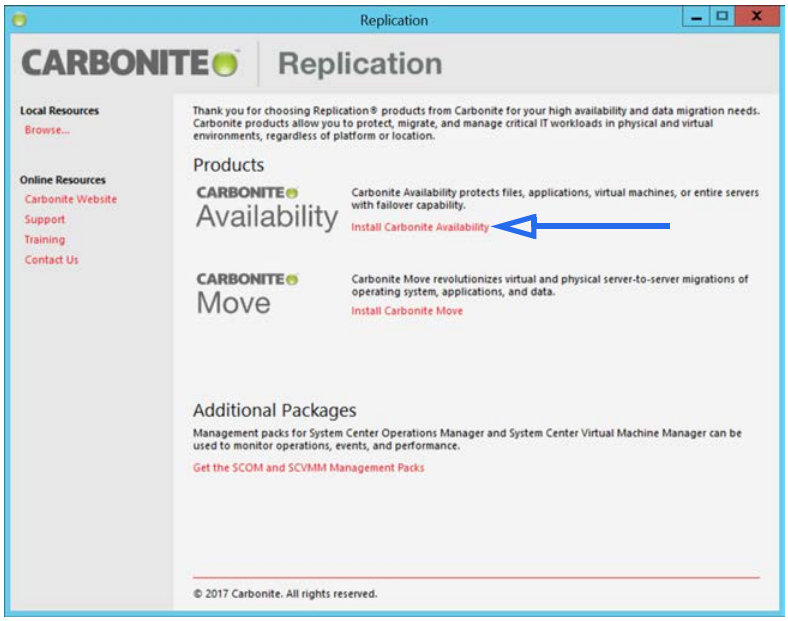
2. Specify the location on your hard drive where the compressed files should be extracted to.
   Click **Unzip**.



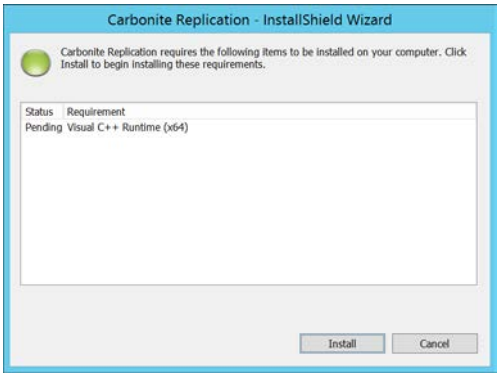
3. The files will be unpacked onto your drive. When finished, click **OK** to continue.



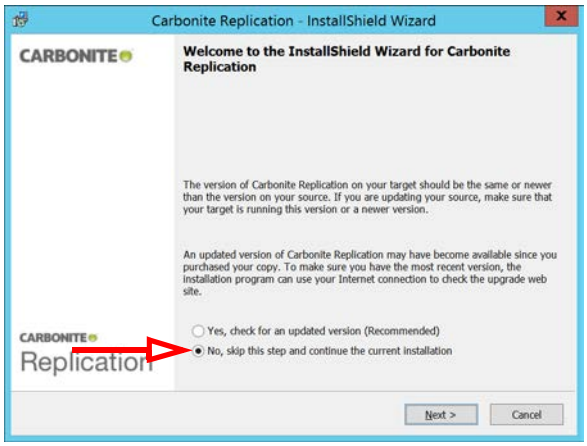
4. From the main screen, select **Install Carbonite Availability**.



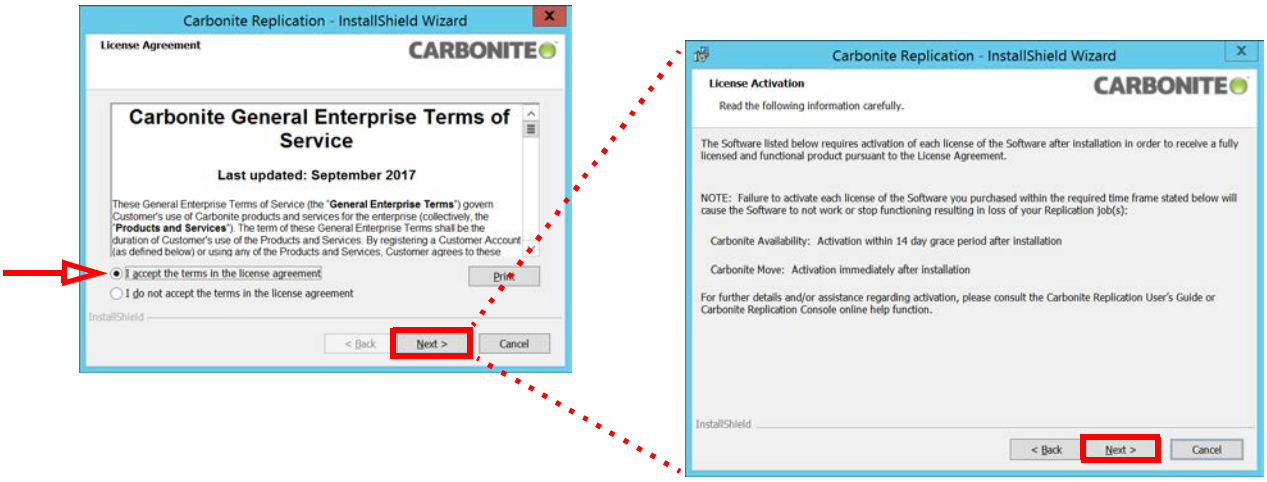
5. Any required applications that are not installed on your system will be added now. Click **Install** to continue.



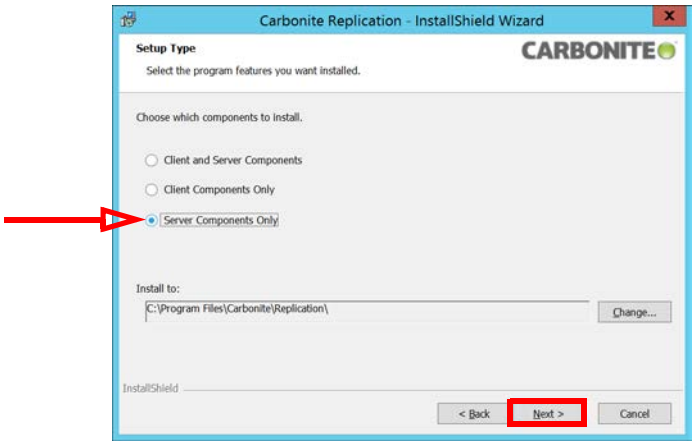
6. When prompted to check for the latest installation, select **No** and click **Next** to continue.



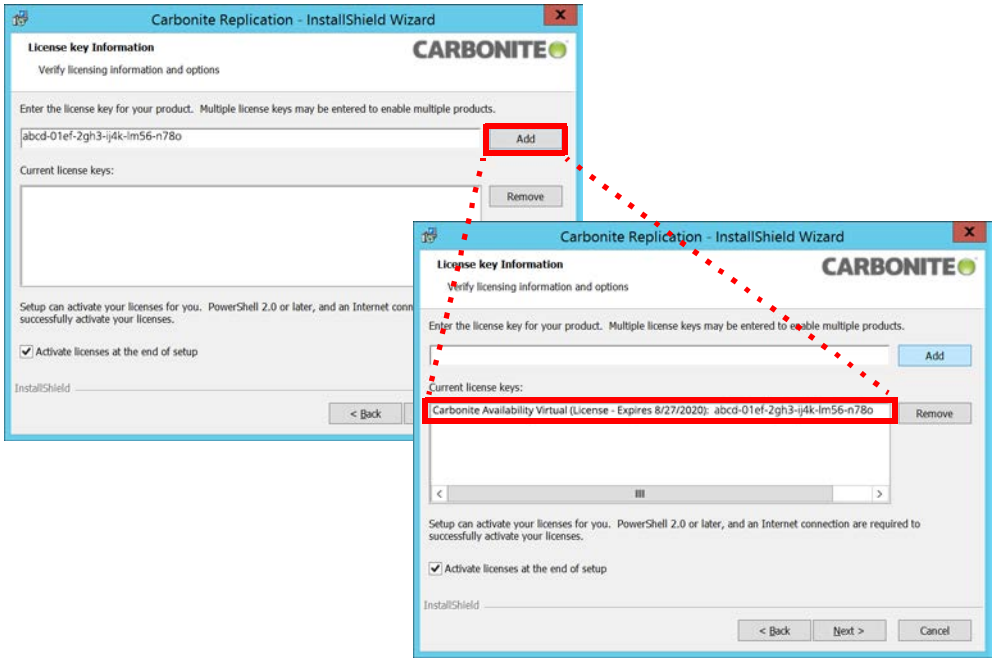
7. Accept the terms of the license agreement and click **Next** to continue, then click **Next** to activate the license.



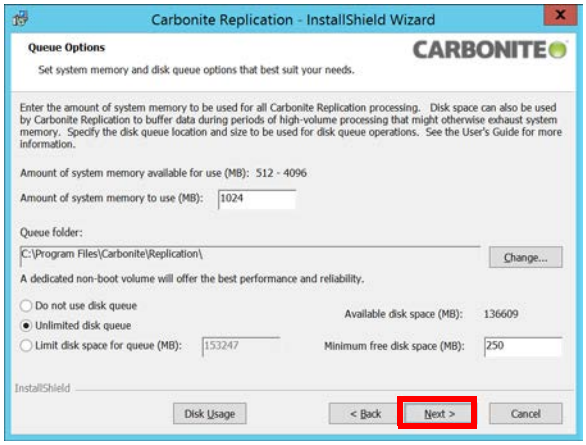
8. Enable **Server Components Only**, then click **Next**.



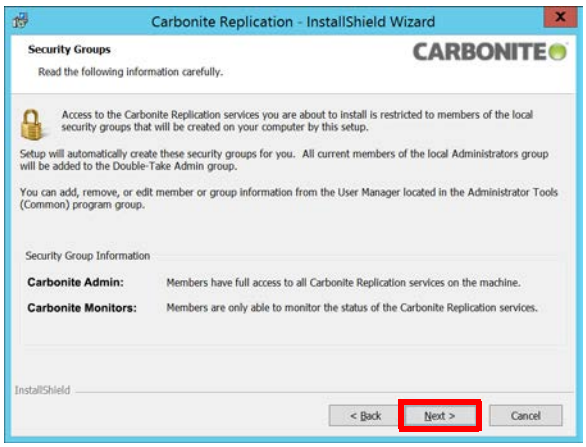
9. Enter the license key that came with Carbonite Availability into the space provided. Click **Add** to install the license onto the computer. Click **Next** to continue.



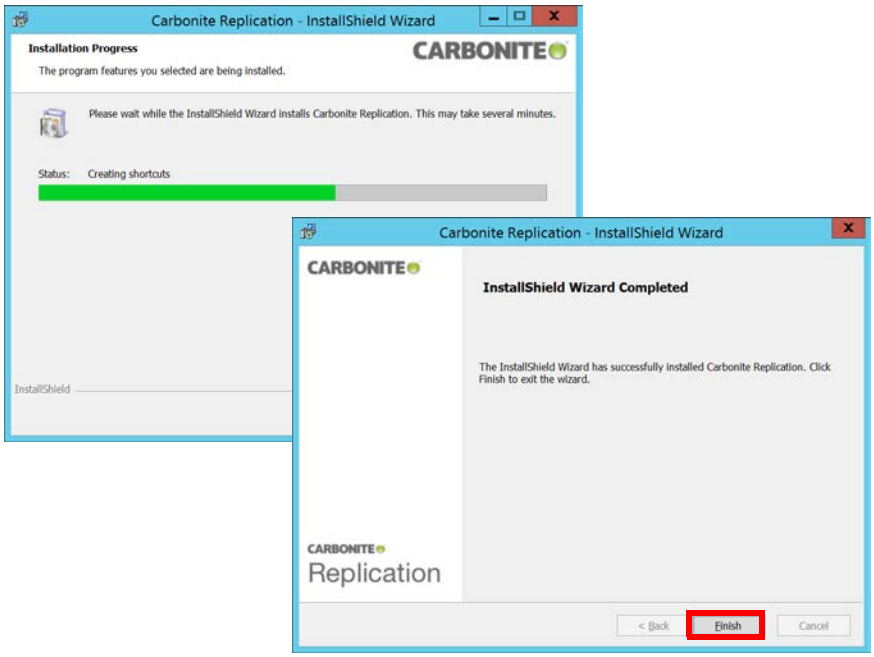
10. Leave all settings at their defaults. Click **Next** to continue.



11. Click **Next** at the **Security Groups** screen. Click **Install** to begin adding the program to the server.



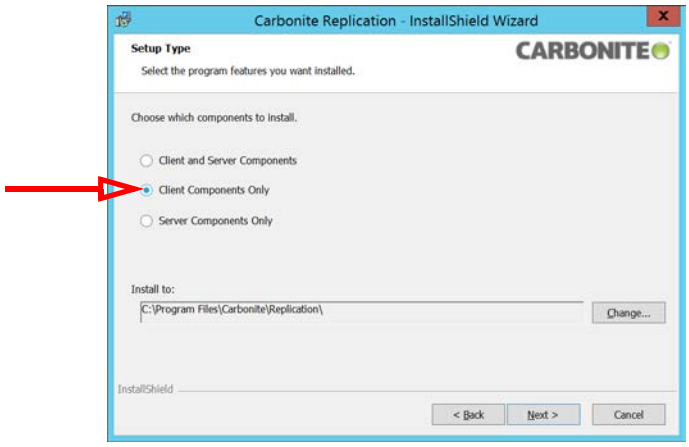
12. The program will be installed. Click **Finish** when prompted.



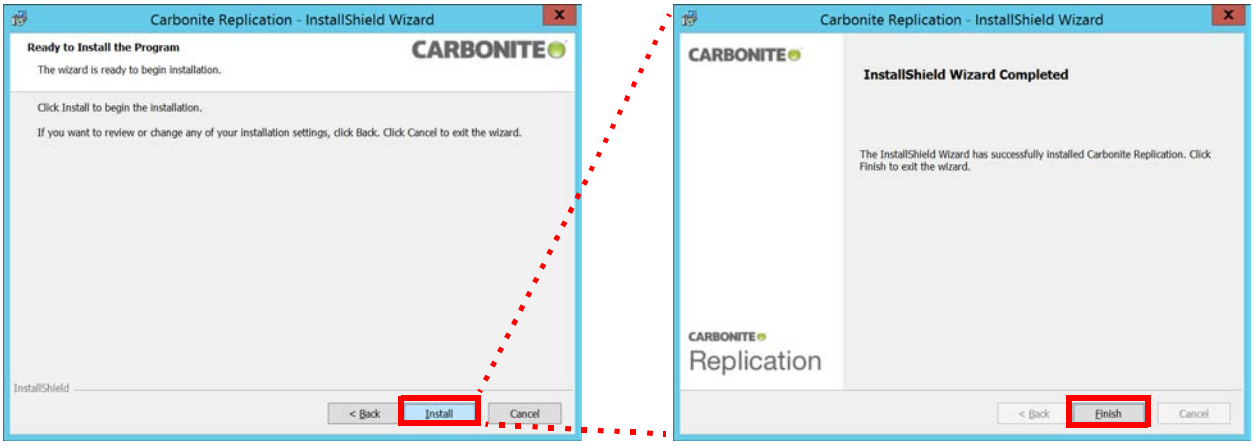
Installing Carbonite Console on the Client (WAN)

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.

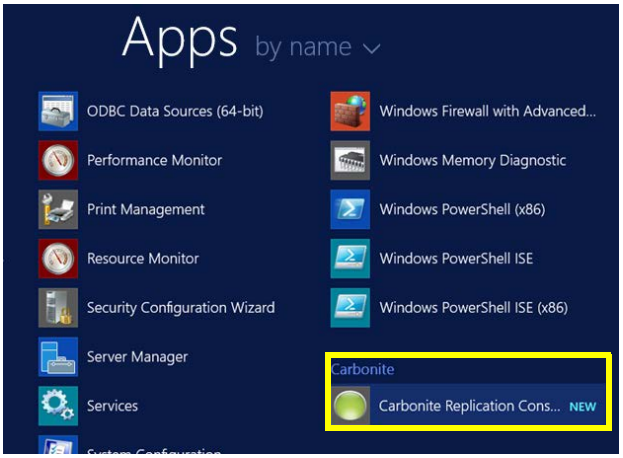
1. Install the software on the client computer as shown above, but when step 9 is reached, choose **Client Components Only** instead and continue.



2. Complete the installation.



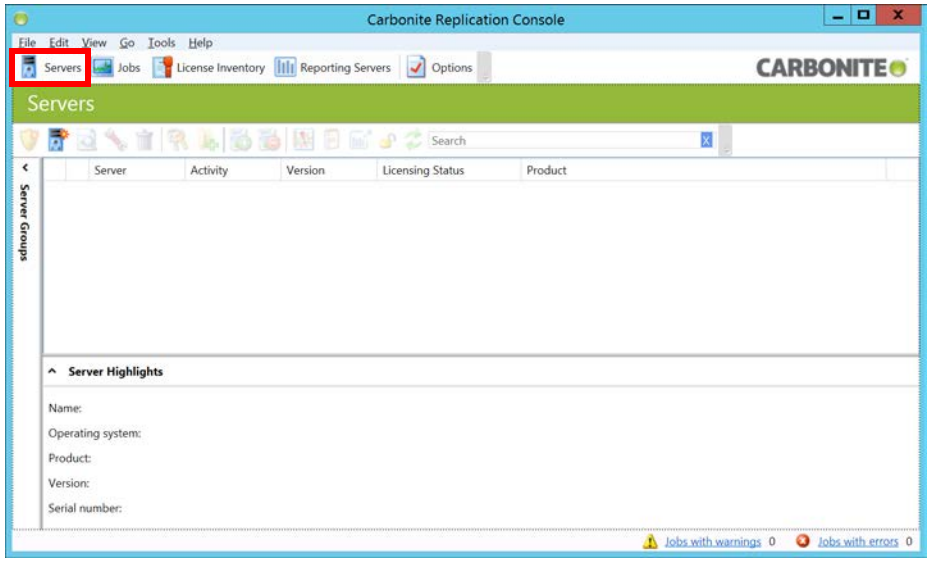
3. The Carbonite Availability console will be installed onto the client machine. Use this application to configure the disaster recovery and failover details for the servers.



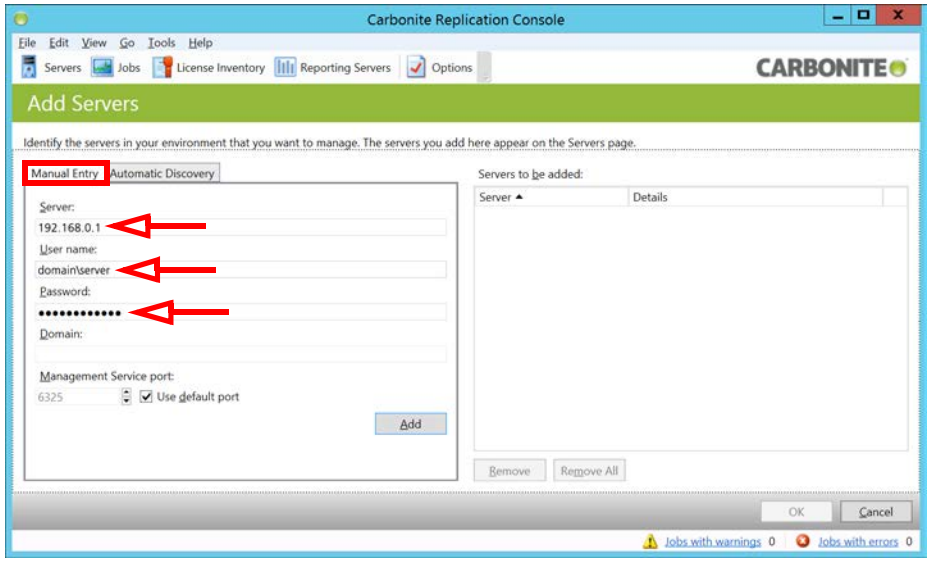
Configuring Failover (WAN)

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.



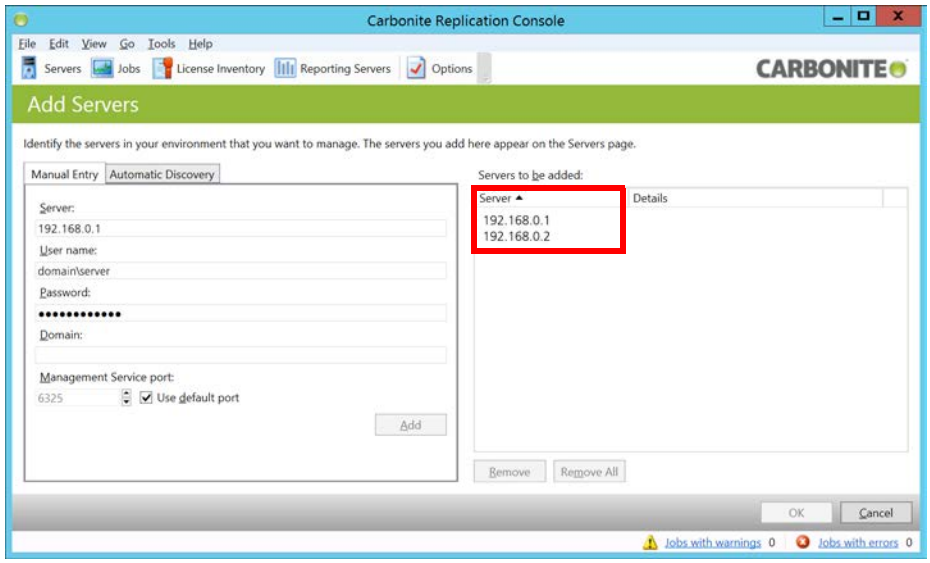
Server: Enter the IP address for the Carbonite server.

User name: Type in the domain, forward slash, and the administrator username in this space. For example, **domain/username**.

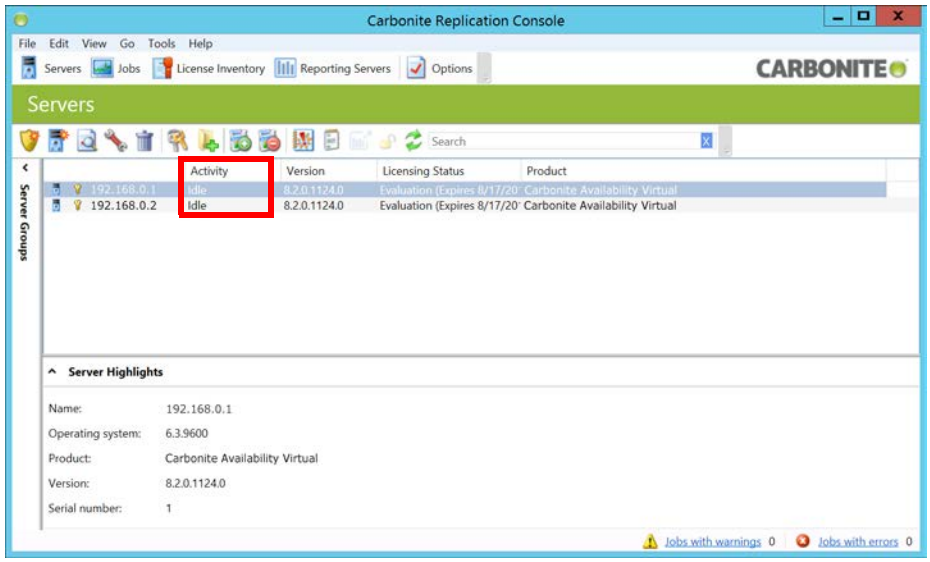
Password: Add the password for the administrator account here.

When ready, click **Add**.

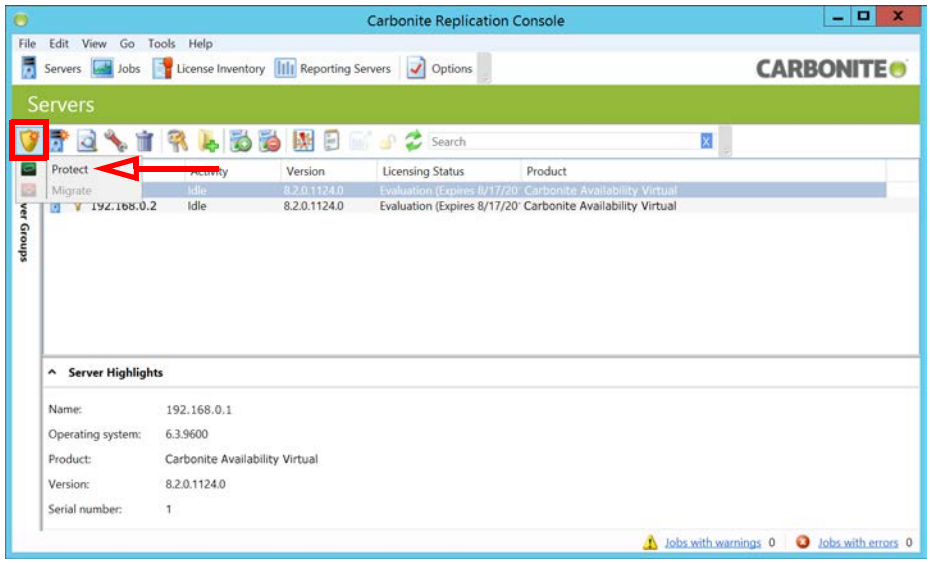
4. Repeat step 3, adding the details for the other Carbonite server.
Both servers will appear in the right hand window of this screen.



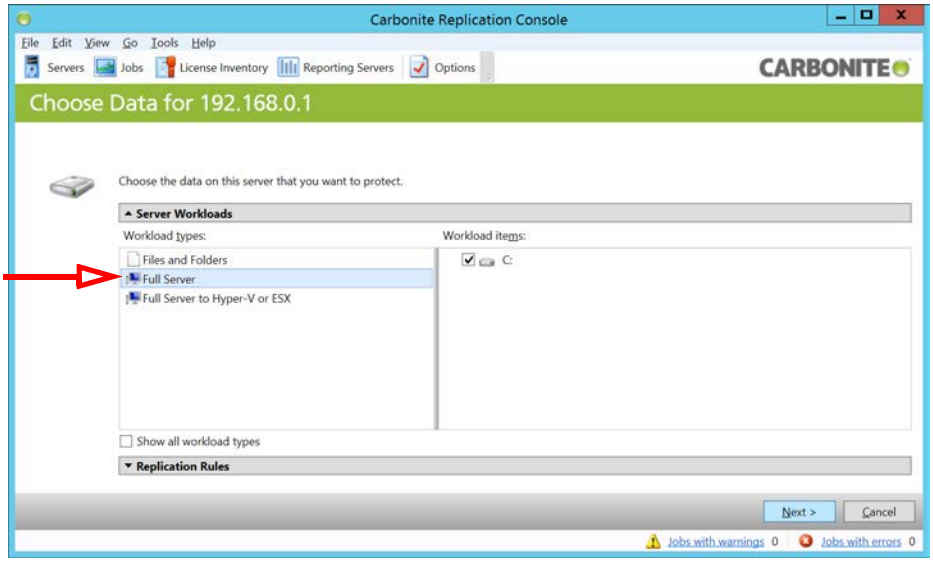
5. Under the **Activity** column, anything other than **Idle** means that an error has occurred. Delete the server and repeat step 1 to 3 for the affected server.



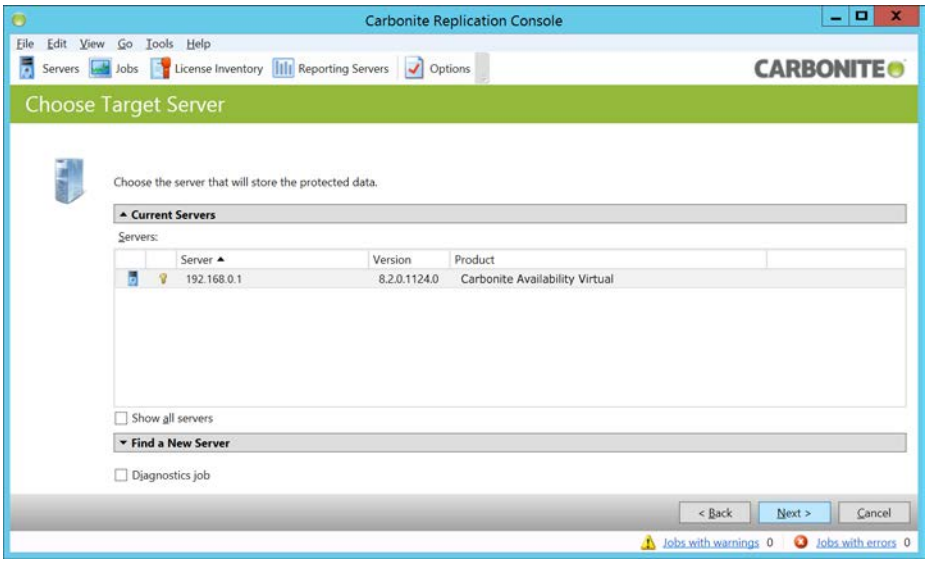
6. Select a server, click the **Create Job** icon, and select **Protect**.



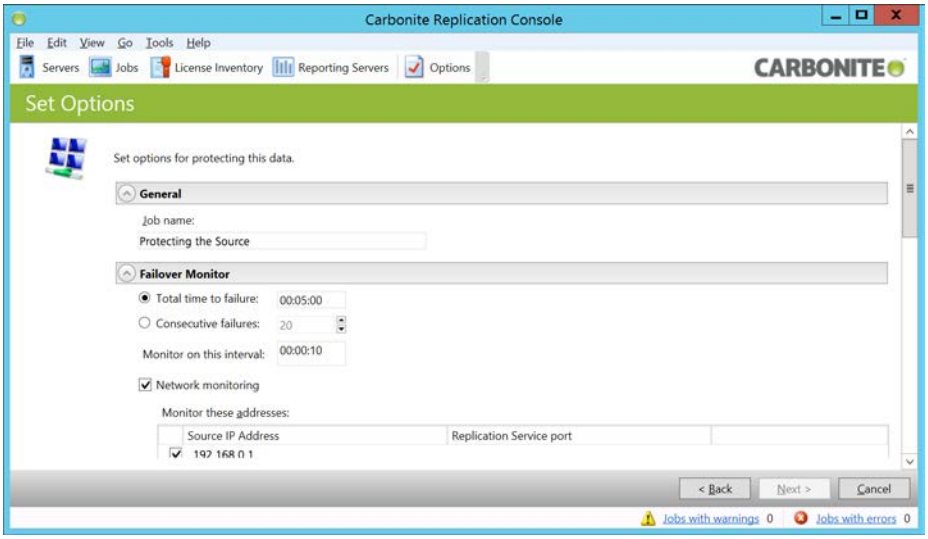
7. On the Choose Data screen, select **Full Server** and click **Next**.



8. Select the server where the protected data will be stored, then click **Next**.

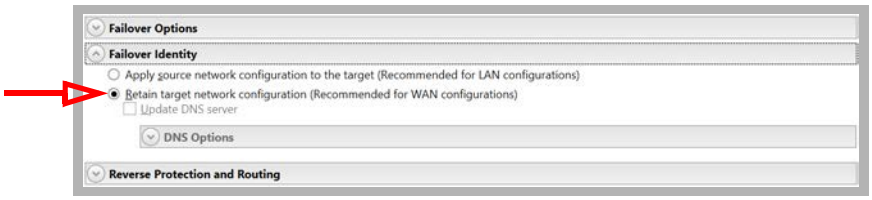


Make the following changes to **Set Options**.

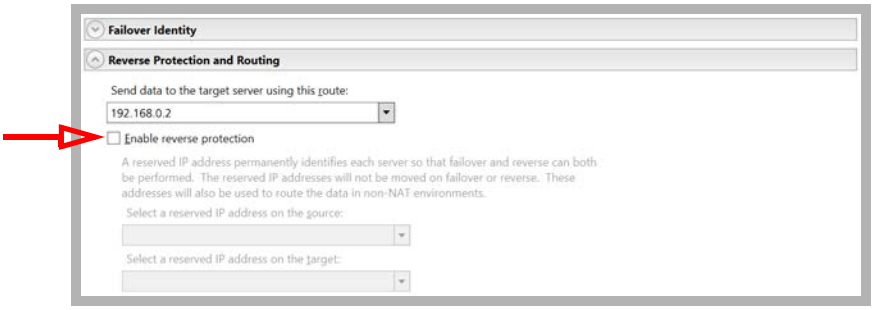


9. Scroll down and expand **Failover Options**. Enable **Wait for user to initiate failover**.

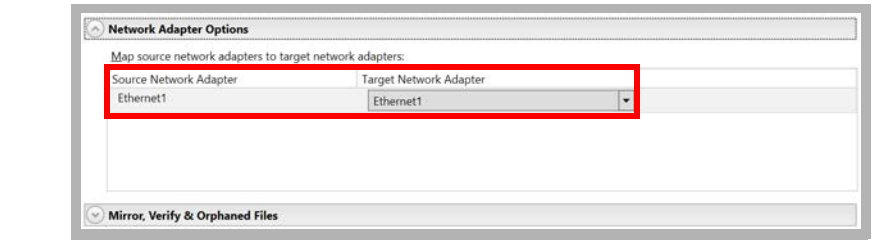
10. Scroll down and expand **Failover Identity**. Enable **Retain target network configuration**.



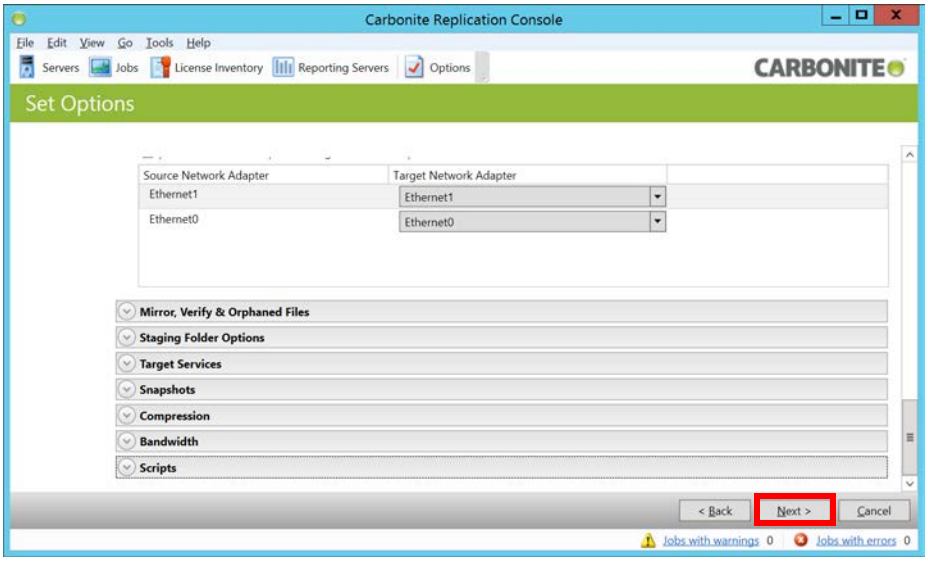
11. Scroll down and expand **Reverse Protection**. Turn off **Enable reverse protection**.



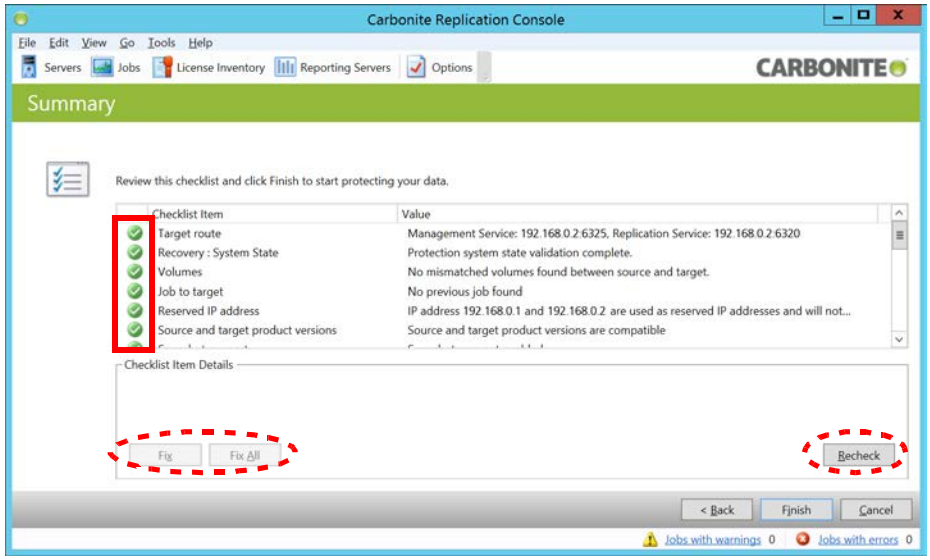
12. Scroll down and expand Network Adapter Options. Map the network interface adapter card on the Target server to the card on the Source.



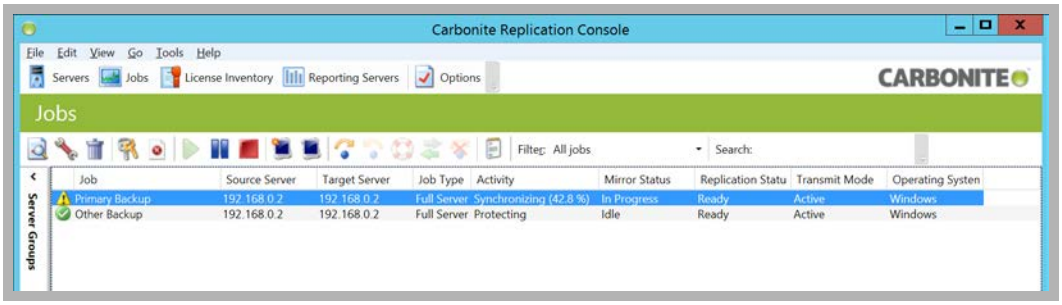
13. Leave all other settings at their default values and click **Next**.



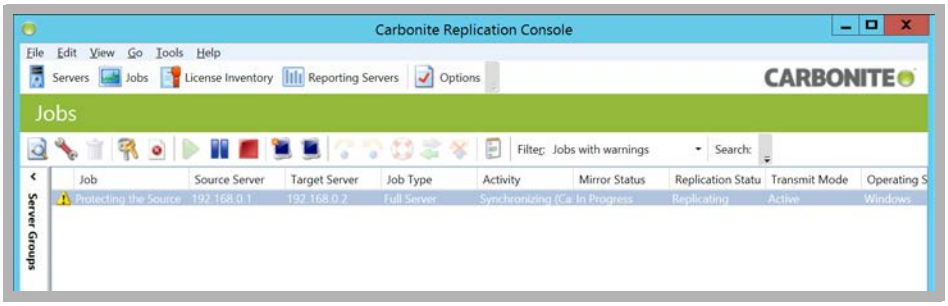
14. The program will make the specified changes and verify all connections. Fix and Recheck any items that failed during testing. When all items appear green, click **Finish**.



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.



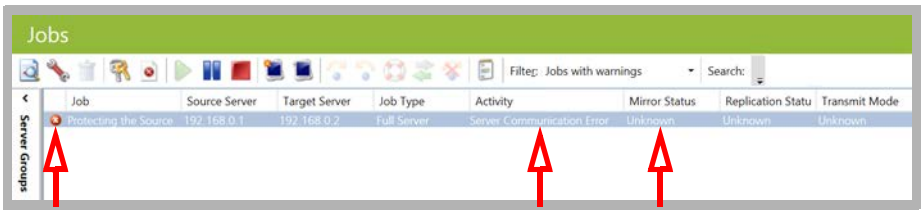
Triggering Failover (WAN)

In a WAN configuration, the failover is not automatic and requires administrator intervention.

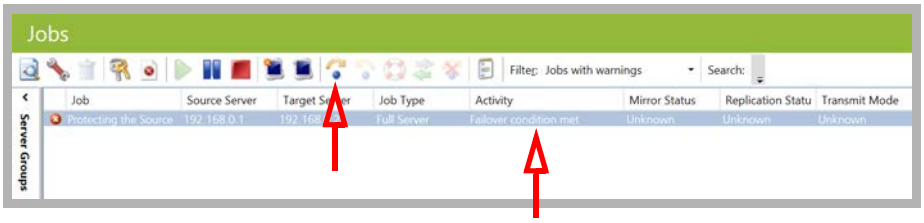
Under normal conditions, the Source will manage the Messaging traffic, while the Target continuously mirrors the data.

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**.

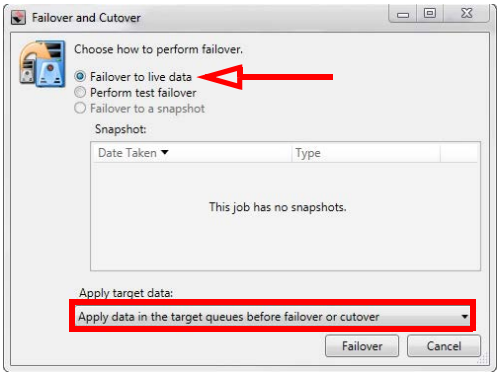


2. The failover procedure is triggered by selecting the job, then clicking the failover icon .



3. Enable **Failover to live data**.
   From the **Apply target data** menu, select **Apply data in the target queues before failover or cutover**.

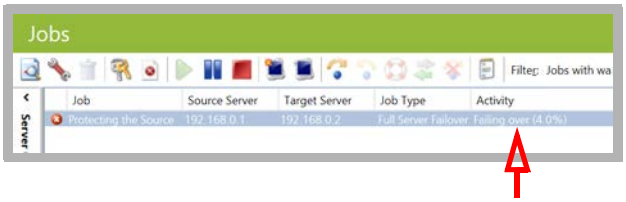
   Click **Failover** when ready to begin Data Recovery.



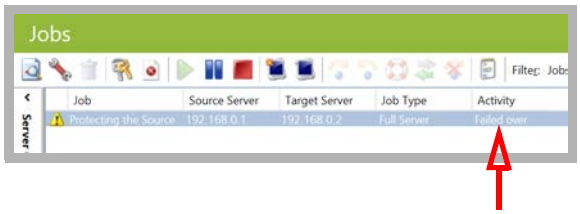
While the servers are in failure mode, there will be no services.

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

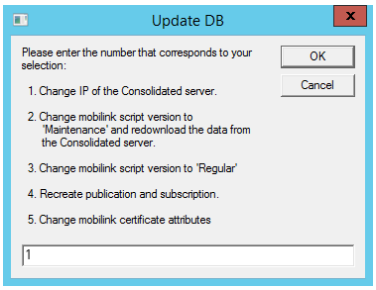
Once failover is complete and the Target is active as the new Source, the voice servers must re-establish communication before voicemail functions will start working.

Enabling Voicemail Functions on HA Servers

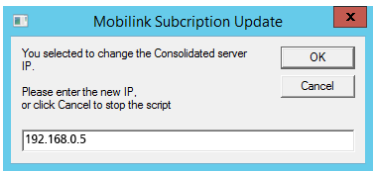
For Consolidated Server

After a failover, the IP addresses of the live servers have changed. Update Messaging to re-establish voicemail functions.

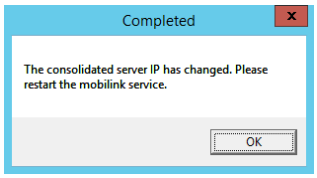
1. Stop and disable the **SQL Mobilink Service** on the Primary and all Secondary servers.
2. Change the IP address of the Consolidated server on the Primary and Secondary servers only. This is the Mobilink connection that allows the servers to sync the database. Run the **UpdateDBHA_64.exe** utility 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**.



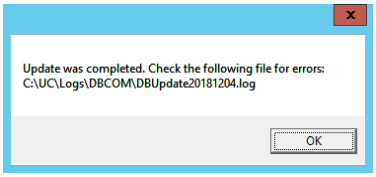
4. Enter the new IP address of the backup Consolidated server, then click **OK**.



5. The IP Address for the Consolidated server will be changed. Click **OK**.



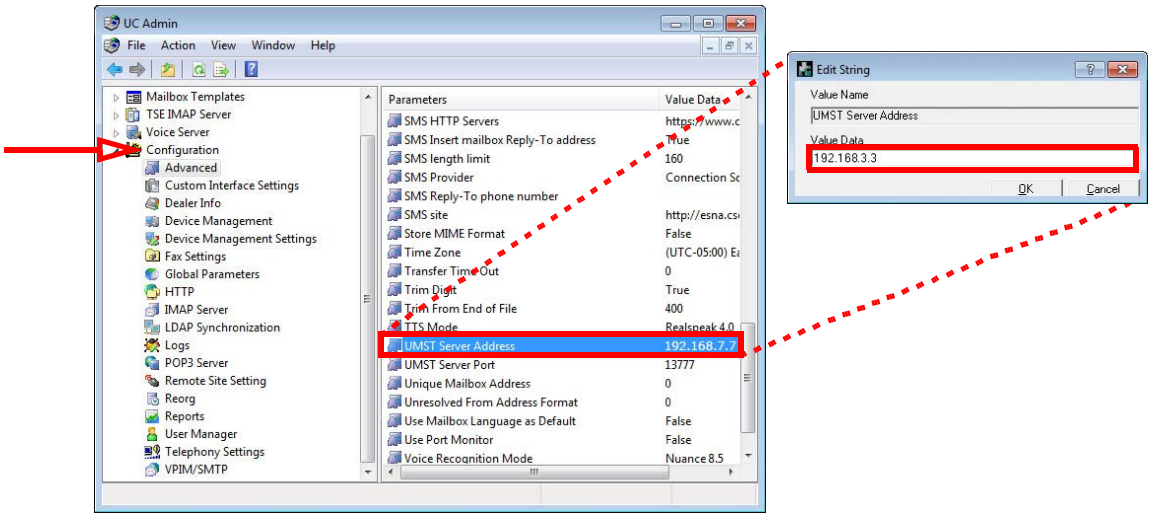
6. Any errors can be viewed in the log file. When finished, click **OK** to complete the change.



Start the **SQL Mobilink** service on all servers in the HA environment.

7. Change the IP address of the UMST (Consolidated) server to the IP address the server attained during failover. Open IXM Admin, and go to **Configuration > Advanced**.

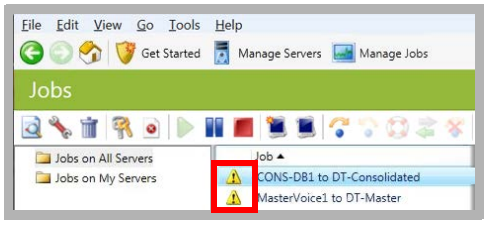
8. Double-click **UMST Server Address** in the right-hand pane and enter the updated IP address for the UMST server.



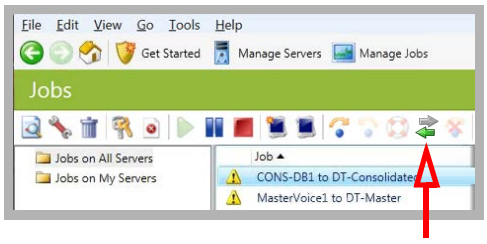
Reversing Protection After Failover

After failover, the old Target server has become the new Source server. Once the cause of the failure has been corrected, the original Source can become the new Target, thereby restoring failover protection to the system.

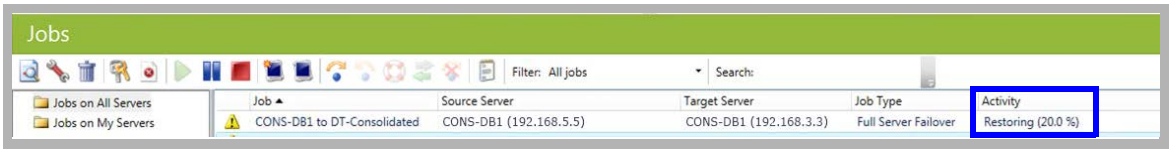
1. Open the Carbonite Availability monitor. Failover protection is no longer active.



2. To initiate Reverse Protection, click the **Reverse** button in the toolbar.

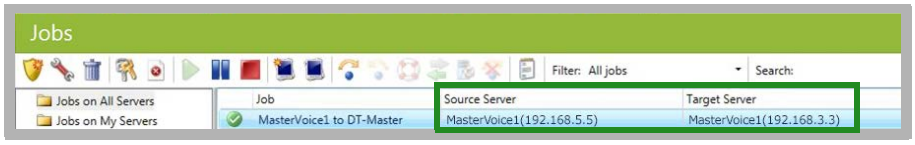


This initiates a synchronization of the servers, with the original Target as the new Source, and the original Source now the Target. The monitor displays the progress of the synchronization.

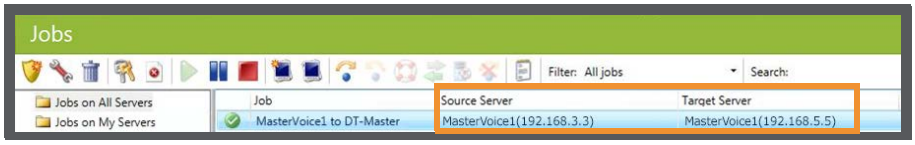


When the synchronization is complete, the system is again safe with failover protection.

Compare the configuration from before and after the failover. The two servers have traded positions.



Before



After

Reverse protection has been enabled successfully.

21 CSE SERVER BACKUP

In This Chapter:

Introduction

In a High Availability environment, server failover is handled automatically for all voice servers (Primary and all Secondaries). The Consolidated server can be backed up using Carbonite Availability. However, Remote CSE servers require a different solution.

Apply the following procedure to all of the Remote CSE servers on your system. One additional server is required to be available as part of the system to take over when an active server fails. This server does not process any traffic, but it must be active to keep its database and other files current with the rest of the system.

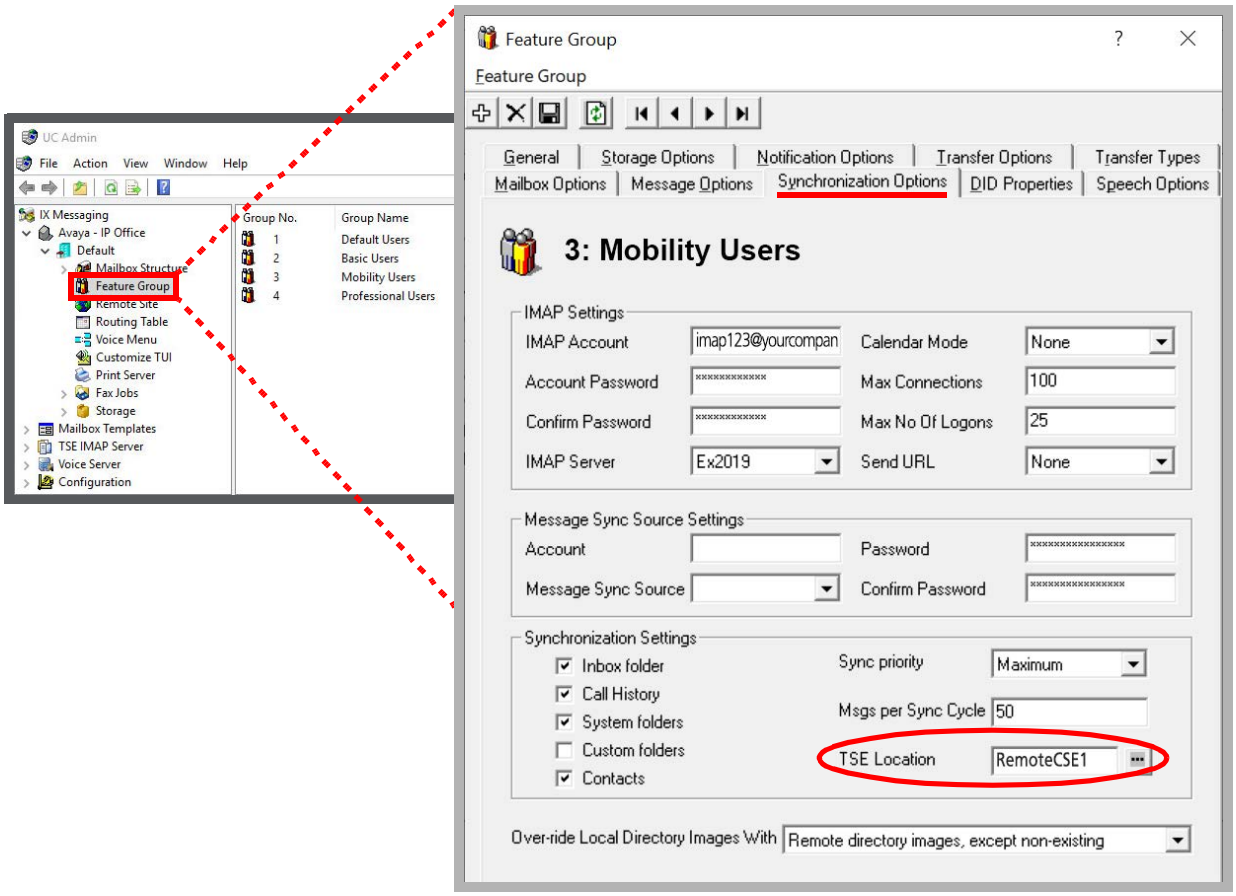
This procedure does not provide automatic, unattended failover as some action is required by the administrator.

Setup

When setting up multiple Remote CSE servers on a system, configure the Feature Groups on the Consolidated Server to use the appropriate Remote CSE for each group.

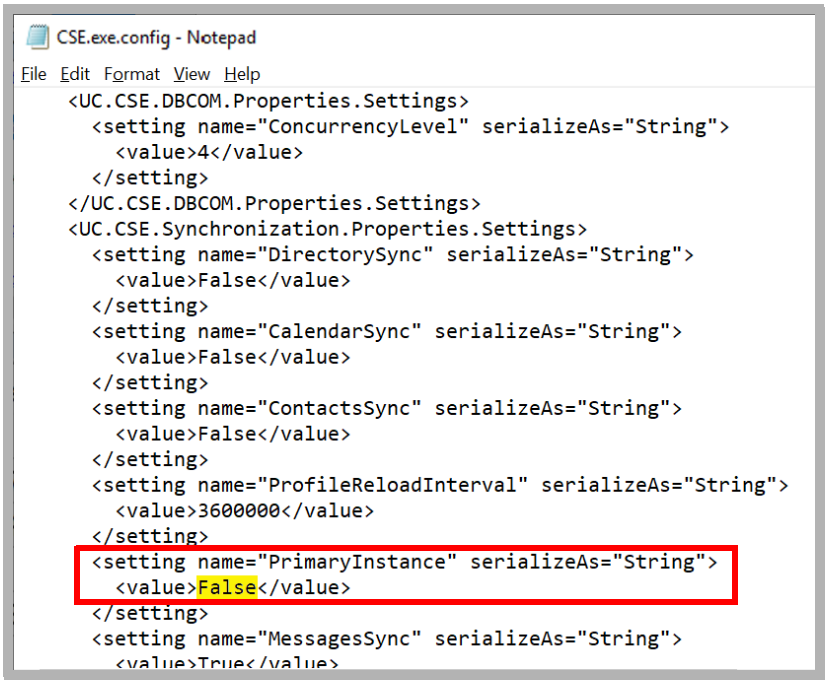
Consolidated Server

1. On the Consolidated server, open **UC Admin > Feature Group > Synchronization Options**.
2. Set the **TSE Location** field for each Feature Group to the desired Remote CSE server.



All Remote CSE Servers

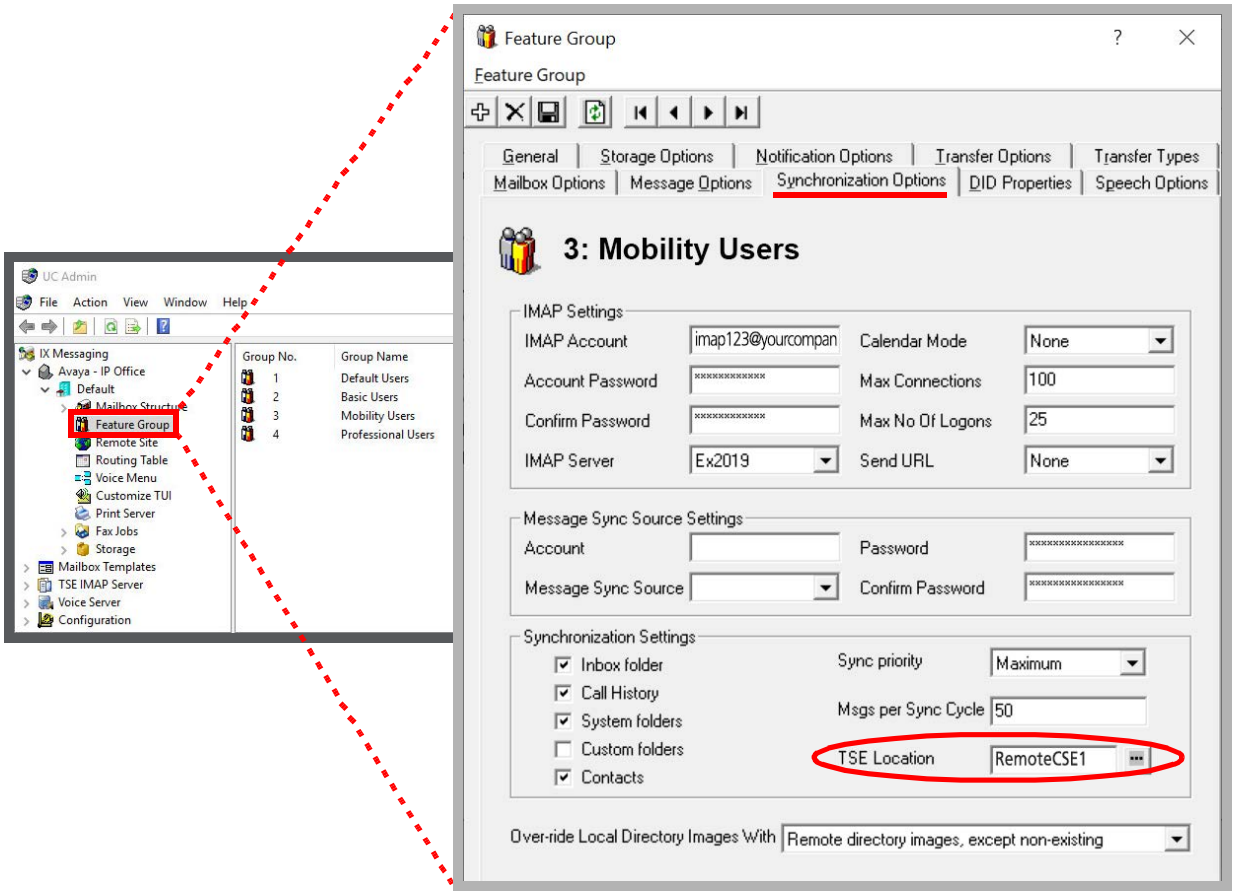
3. On each of the Remote CSE servers, including the spare, go to the Avaya IX Messaging installation location, and open the **\UC\UCCSE** folder. Double-click the **CSE.exe.config** file to open it in Notepad.
4. Change the **Primary Instance** value to **False**. Save the file.



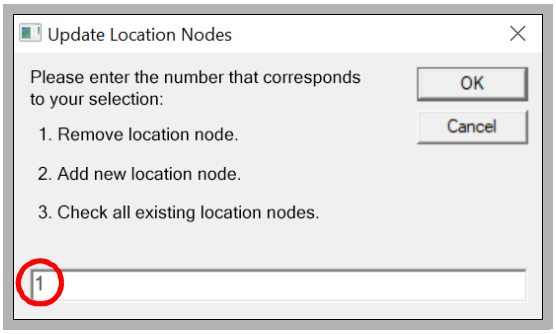
Failover Procedure

When a Remote CSE server fails, the spare machine must be brought into service and the broken one removed for repair.

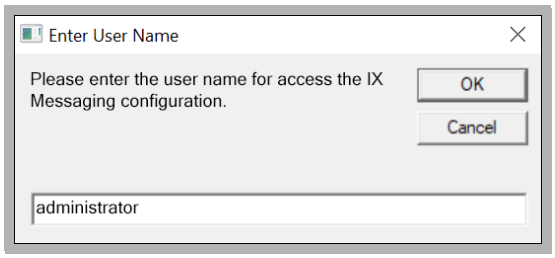
1. On the Consolidated server, open **UC Admin > Feature Group > Synchronization Options**.
2. For each Feature Group that used the broken Remote CSE server, change the **TSE Location** field. Enter the PC name of the spare machine in this field. Click **Save** when finished each Feature Group.



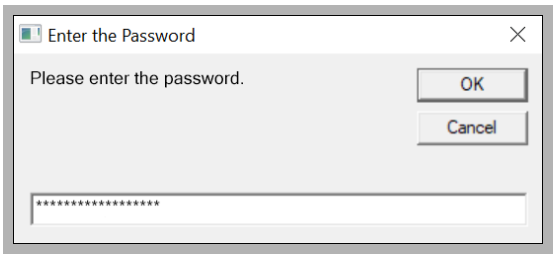
3. On the Consolidated server, open the \UC\DB folder and double-click the **UpdateLocationNodes** application.
4. Enter **1** in the space provided to **Remove location node**. Click **OK**.



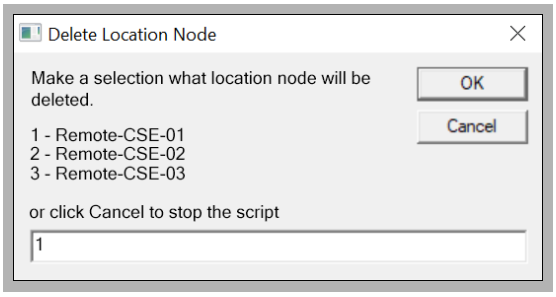
5. Enter the username of the administrator account for Avaya IX Messaging. Click **OK**.



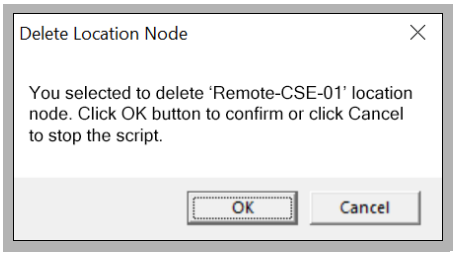
6. Type in the administrator password. Click **OK**.



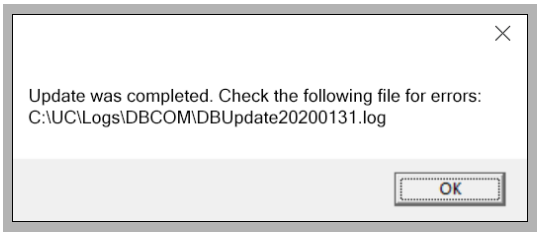
7. Enter the number which corresponds to the failed Remote CSE server. Click **OK**.



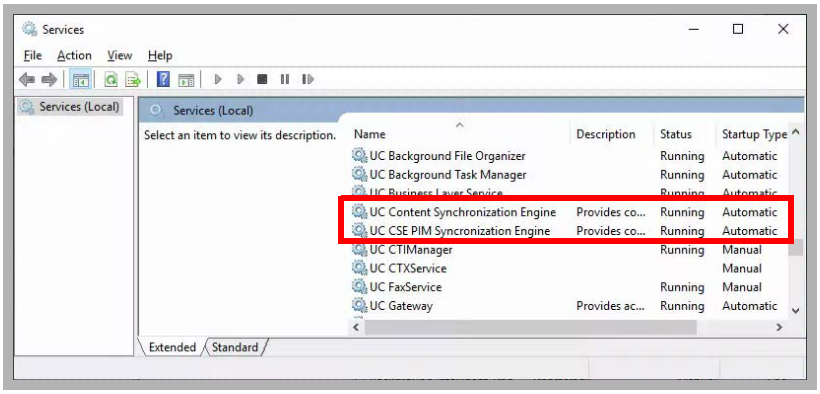
8. You are prompted to confirm the deletion of the server. Click **OK** to confirm. This will remove the failed server from the list of remote CSE servers in the database.



9. The broken server has been removed.



10. Restart these 2 services on the spare server: **UC Content Synchronization Engine**, **UC CSE PIM Synchronization Engine**.



11. The Remote CSE server has been successfully replaced with the spare.

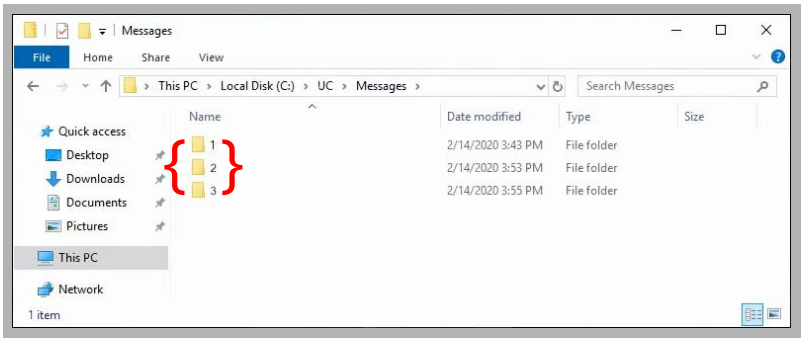
Restoring After a Failover

After a failover, once the broken server has been repaired or replaced, it can be put back into service either as the new spare server, or to take over as the active server again.

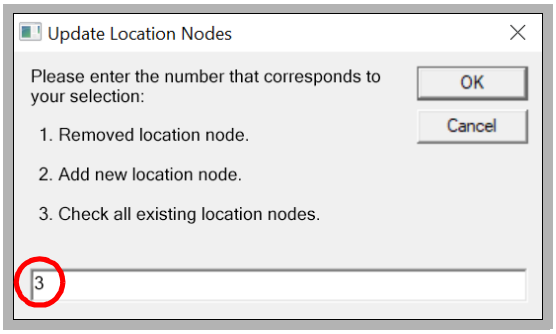
Returning the Original Server

If you are returning the broken machine to service, do the following.

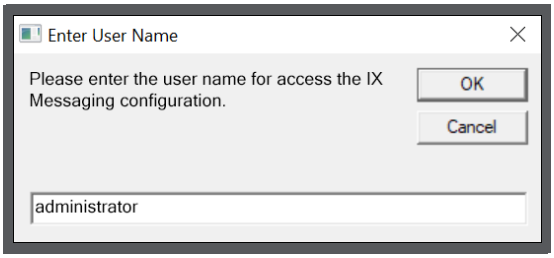
1. Reconnect the repaired computer to the network.
2. From any of the other servers, copy the contents of the Messages folder (\UC\Messages\ ) to the same folder on the repaired server. This will ensure that the new machine has the latest files.
   If you have more than one company installed on the system, select the number for the company you want to restore.

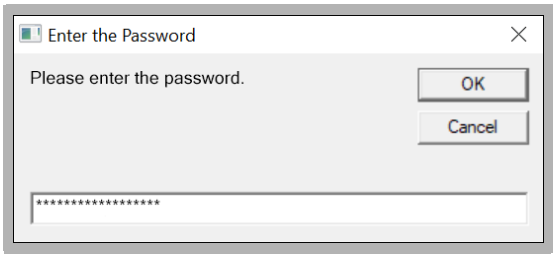


3. Run the **UpdateNodesLocation** application and enter **3** to **Check all existing location nodes**.

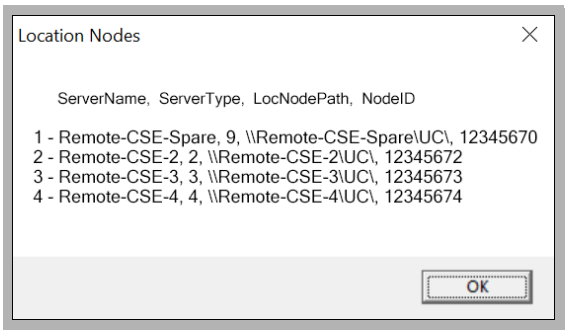


4. Enter the username and password of the administrator account for Avaya IX Messaging.



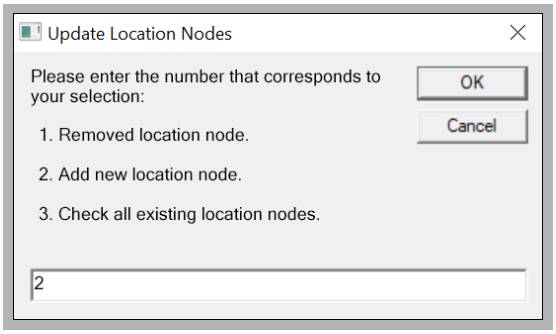


5. Verify that the server you are returning to service does not appear on the list.

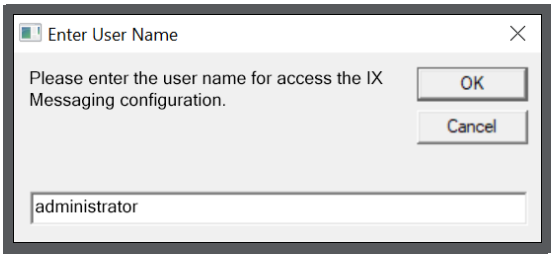


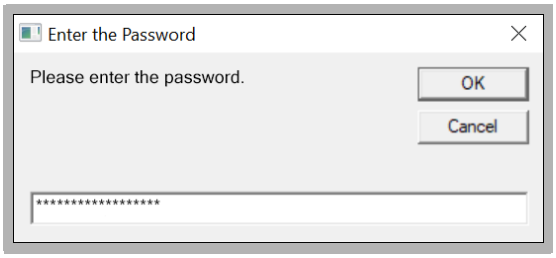
If the restored computer is in the list, no further action is required.

6. If the new machine is not on the list, it must be added to the nodes. On the Consolidated server, run the **UpdateNodesLocation** application again and select **2** to add a new node.

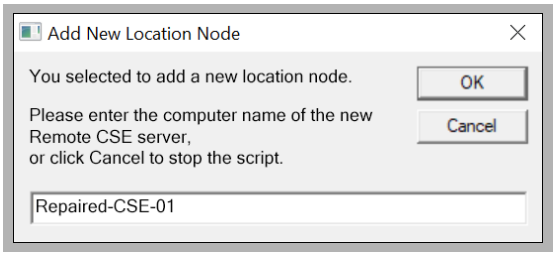


7. Enter the username and password of the administrator account for Avaya IX Messaging.

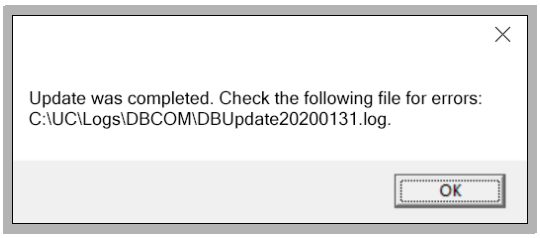




8. Enter the computer name of the node being added to the list. Click **OK** when finished.



9. The repaired computer has been added to the list of Remote CSE servers in the database.

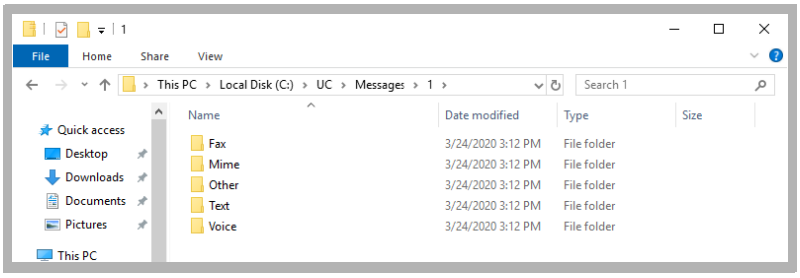


Installing a New Server

Follow the steps in **chapter 17 - Dedicated CSE Server Installation** to install the new Remote CSE Server. It is not necessary to use the UpdateNodesLocation application to add the new node. The new computer will be added to the list of remote CSE servers in the database during mobilink synchronization. However, the Messages folder must still be copied to ensure that it's files are up-to-date.

Messages Folder

It is only necessary to copy the folders for the message types you are using.



22 VMWARE SUPPORT

In This Chapter:

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 IX Messaging 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

Software	Version
VM Software	VMware ESXi 4.x / 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 6.7 Hyper-V Server 2012 Windows Terminal Services[1]
OS for Messaging	Server 2012 or 2012 R2 Server 2016 Server 2019

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.

Hardware	
CPU	Requires Intel® CPU which meets or exceeds the requirements of ESXi 4+

1 - Windows Terminal Services only supports the installation of the client software. The Messaging server cannot be installed here.

Virtual Environment Limitations

Migrating data from a virtual machine environment is not supported.

Migrating data to a virtual machine from an existing physical environment is supported, but only if AM is installed first. Move an existing server onto a virtual machine by migrating the database using the utilities provided with the Messaging installation package. You can transfer both 7.x and 8.x systems to an 10.8 virtual environment. Messaging must be installed on a new virtual machine with a clean operating system.

Warning: Importing an existing Avaya IX Messaging environment to a virtual image is not supported.

Messaging installed on a virtual environment requires the same hardware resource as non-virtual machine environments.

Note: The fax capability of Messaging within a virtual environment is limited to **24 ports**.

Warning: **Do Not take snapshots** while the servers are in operation as this can lead to serious corruption in the database. System performance may also be heavily compromised. To take a snapshot, shutdown the server first, then take the snapshot while the system is down.

This table shows the list of VMWare features supported.

FEATURE	AVAYA MESSAGING 10.8	AVAYA MESSAGING 11.0
Support for ESXi 6.0	Yes	No
Support for ESXi 6.5	Yes	Yes
Support for ESXi 6.7	Yes	Yes
Support for ESXi 7.0	No	Yes
VMware vMotion	No	No
VMware Snapshot	No	No (Only temporary snapshots prior to upgrade can be created and should be removed after upgrade)
VMware HA	Yes	Yes
VMware DRS	No	No
VMware FT	No	No
vSphere Standard Switch	Yes	Yes
vSphere Distributed Switch	Yes	Yes
Reservation Required	No	No
VSAN Support	Yes	Yes
Thin Provisioning	No	No

Virtual Machine Environment Hardware Requirements

The hardware requirements for setting up Messaging within a virtual environment are the same as for a physical machine. See the System Requirements and Capacity chapter of this guide for more information.

The configuration of the virtual environment does create other considerations for server installation.

For further details on Hardware Requirements, see page 39.

VMware Technology Guidelines

VMware offers 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 Messaging server application and how to utilize VMware solutions with Messaging in mind.

- **High Availability**: VMware also offers its own High Availability solution, which should not be confused with Messaging 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. Messaging 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, Messaging 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 Messaging 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 of 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 Messaging Voice Server's minimum hardware requirements, so Messaging will remain incompatible with FT until the algorithm is changed to support the resources required.

VM Environment Feature Comparison Chart

	HA	DRS	FT
Active Migration	N	N	N
Recovery from Hardware Crash	Y	Y	Y
Recovery from Software Crash	Y	Y	Y
0 Down Time during Crash	N	N	Y
Smart Allocation of Hardware Resources	N	Y	N
Messaging Support	Y	Y	N*
Known Behaviors:			
Voice Traffic	Interrupted until HA recovers	Interrupted until HA recovers	N/A*
iLink Pro Desktop	Interrupted until HA recovers	Interrupted until HA recovers	N/A*
Messaging	Interrupted until HA recovers	Interrupted until HA recovers	N/A*
CTI	Interrupted until HA recovers	Interrupted until HA recovers	N/A*

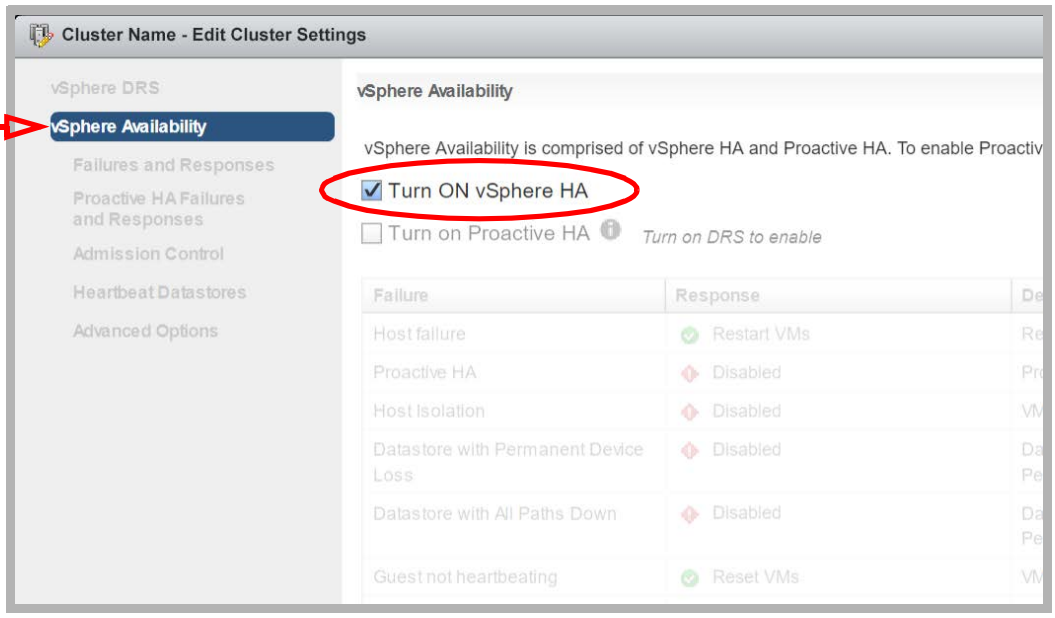
* Due to the way in which Fault Tolerance is designed, Avaya IX Messaging cannot function within the FT model. FT is limited with regard to computer resources (e.g. single core processor) while Messaging has specific minimum resource requirements to function properly. Until VMware upgrades the FT system to support higher amounts of resources, Messaging cannot be deployed under the FT model.

VMware: HA for the Consolidated Server

In a High Availability environment, the Primary 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. Both the Consolidated and Primary voice servers can backed up this way. The Secondary voice servers cannot.

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.

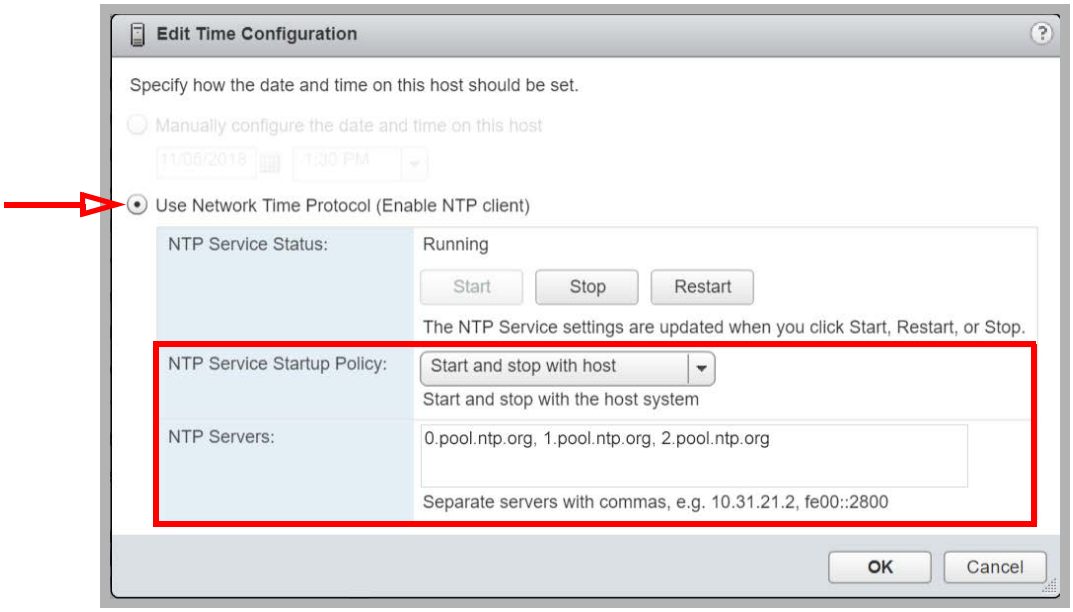


3. Add 2 or more Hosts within the Cluster. One Host contains the virtual machine that houses the Consolidated server, while the others are available should the active Host fail.

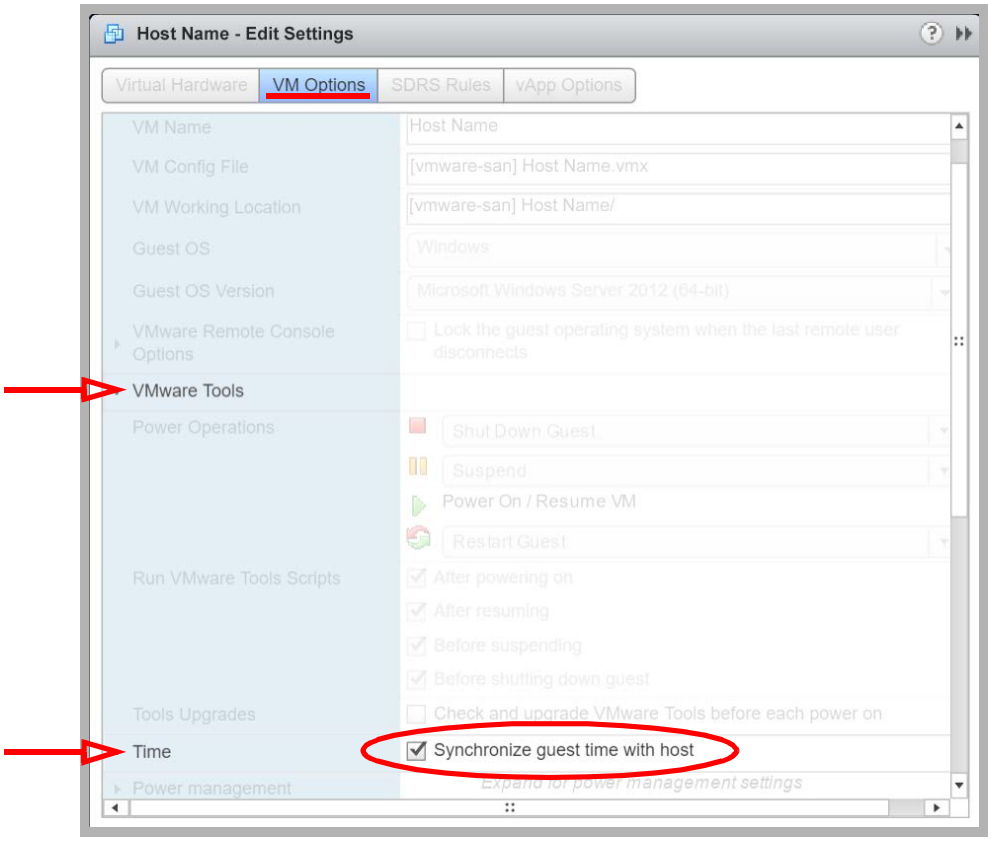
Important: It is essential that all of the Host servers (Consolidated, Primary, and backups) have their clocks synchronized. Certain critical functions within Messaging are time sensitive and will fail if the Hosts are not coordinated.

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 Avaya IX Messaging 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.

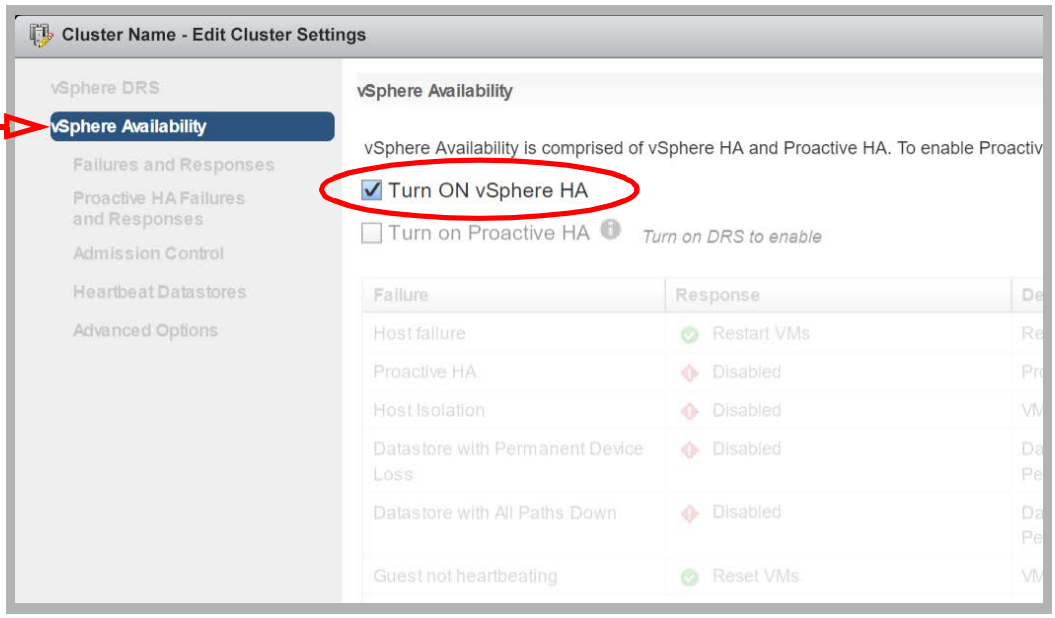
Important: The Messaging system will be unavailable during the changeover and reboot process.

VMware: HA for the Primary Voice Server

In a High Availability environment, the Primary 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.

VMware includes an HA option for its Hosts, providing failover support for the Primary voice server. Both the Consolidated and Primary voice servers can backed up this way. The Secondary voice servers cannot.

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.

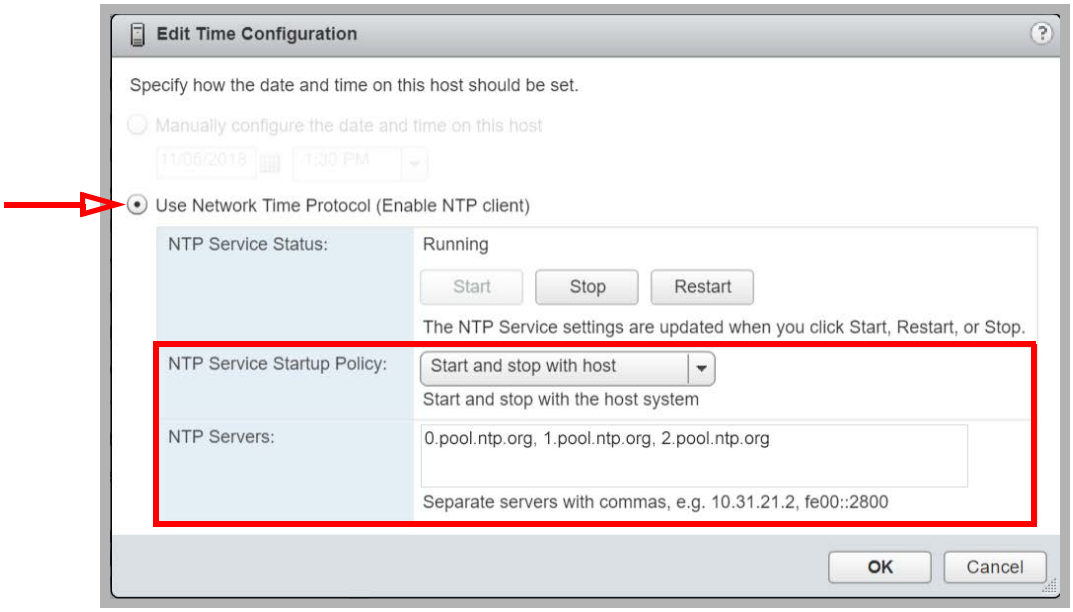


3. Add 2 or more Hosts within the Cluster. One Host contains the virtual machine that houses the Primary voice server, while the others are available should the active Host fail.

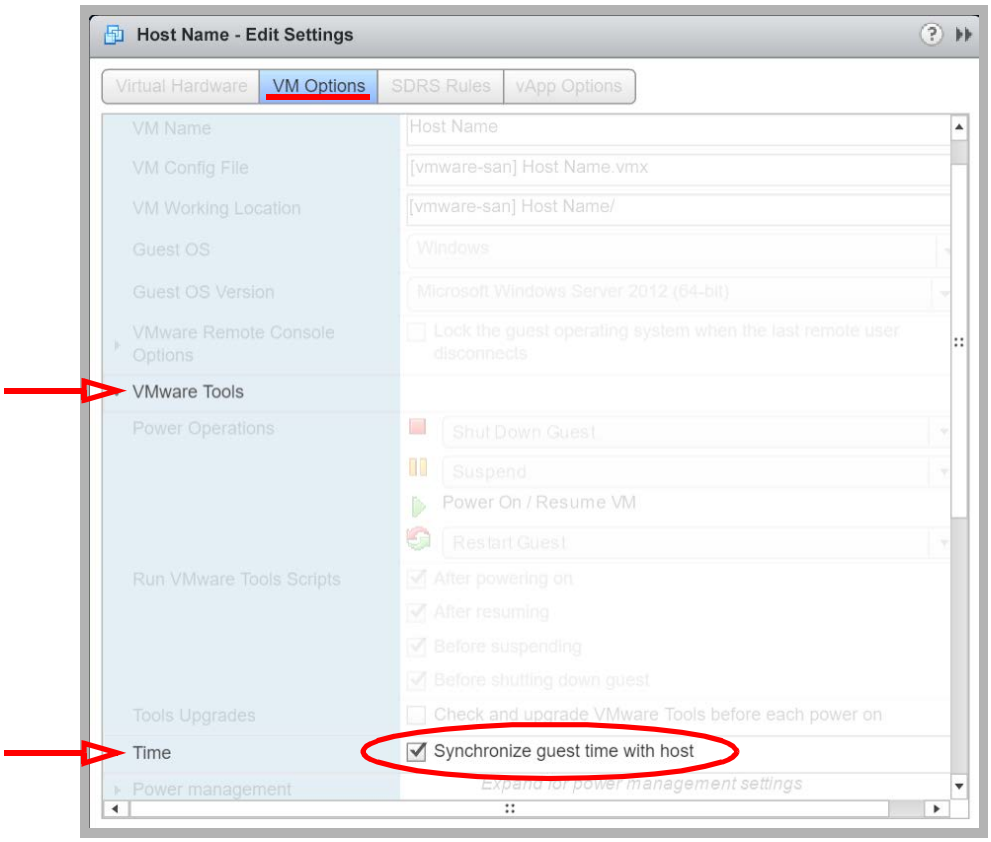
Important: It is essential that all of the Host servers (Consolidated, Primary, and backups) have their clocks synchronized. Certain critical functions within Messaging are time sensitive and will fail if the Hosts are not coordinated.

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 Avaya IX Messaging Primary voice server onto one of the virtual machines.

If the Host with the virtual machine running the Primary voice server fails, VMware will automatically move the server to another Host within the Cluster and restart the virtual machine.

Important: The Messaging system will be unavailable during the changeover and reboot process.

Additional Considerations for AACC Users

There are additional conditions for sites that are integrating with Avaya Aura Contact Center.

- The IX Messaging virtual machine must use the same network interface card (NIC) for both ELAN and CLAN
- On the CS1000, configure the parameter **Set Type = 2008** for the DMG ports.
- Configure the following 2 services for **Automatic (Delayed Start)**:
  UC Voice Server
  UC Service Recovery Manager (found on the Consolidated Server)

Virtual Environment Deployment Example

The following are performance results from a virtualized Avaya IX Messaging 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 Messaging's behavior under virtual environments.

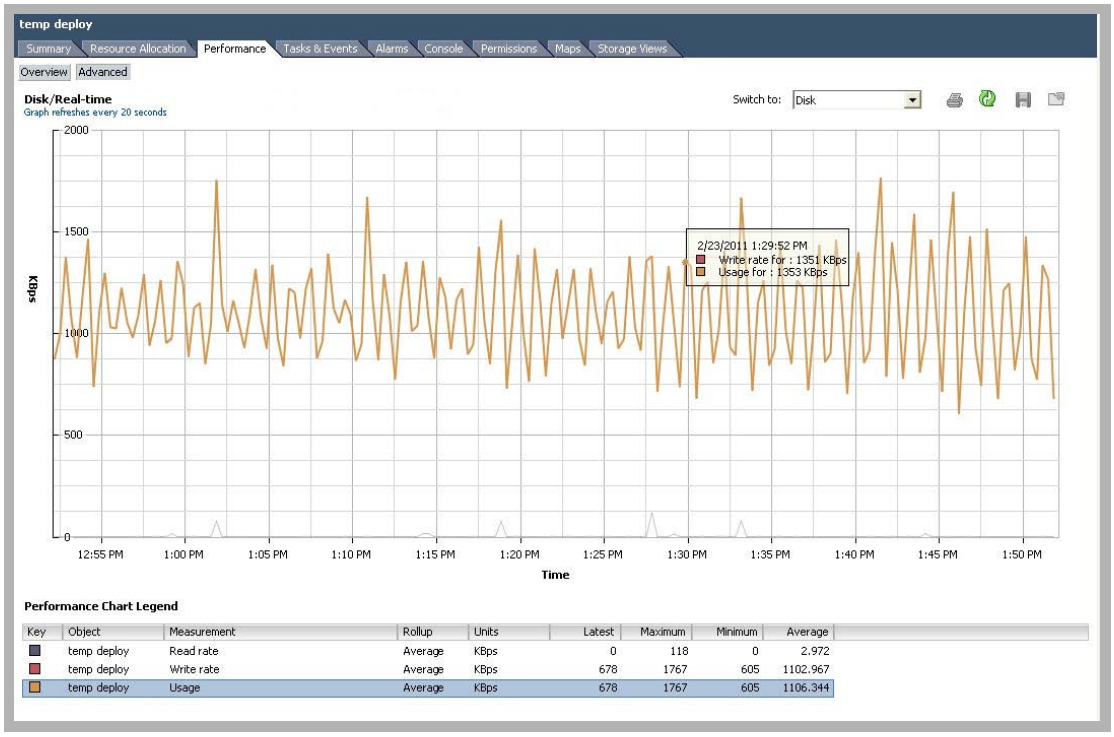
CPU Usage

Avaya IX Messaging 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 Messaging will guarantee a consistent level of performance.

Datastore Latency

Avaya IX Messaging achieved a low average latency of 5.356ms for reading and 2.378ms for writing.

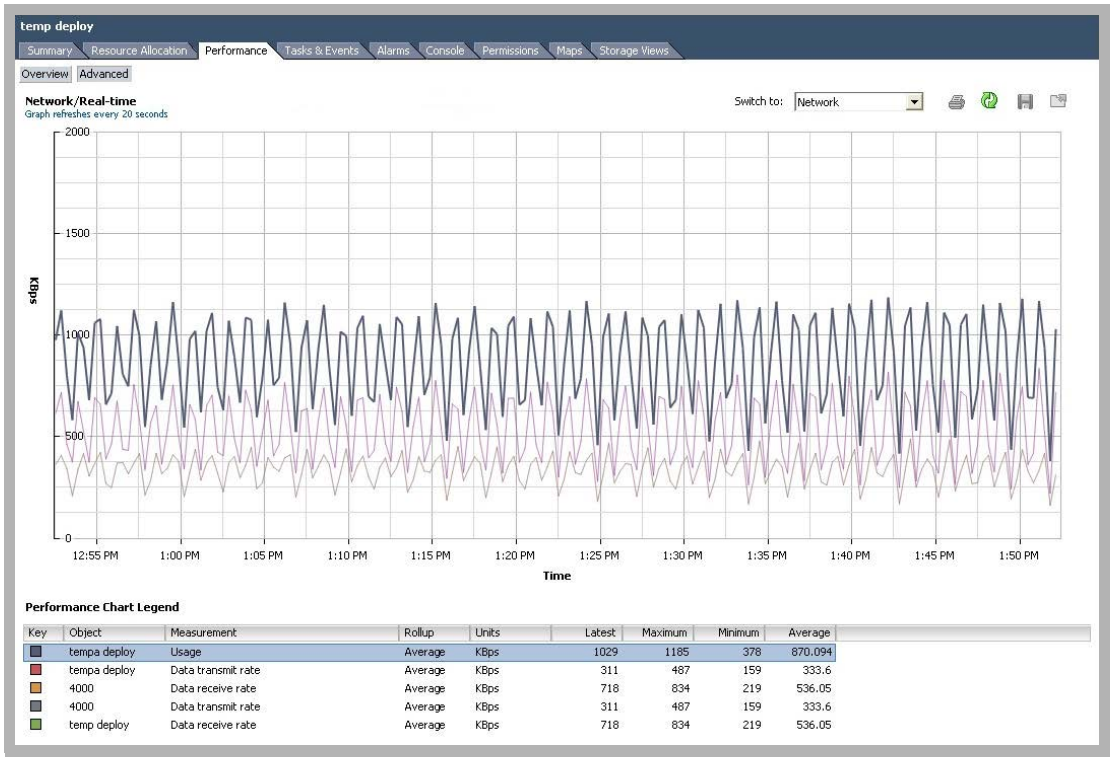
Disk Usage Rate



Avaya IX Messaging 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 Messaging will guarantee a consistent level of performance.

Network Usage Rate



Avaya IX Messaging 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 Messaging will guarantee a consistent level of performance.

Conclusion

Since Avaya IX Messaging is designed to be the sole application running on a given Virtual Machine, it is easy to assign the necessary resources for Messaging. By ensuring that Messaging always has access to the required resources, you will be able to guarantee the level of performance required by your site.

23 VIRTUALIZED ENVIRONMENT: MICROSOFT HYPER-V

In This Chapter:

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 IX Messaging 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 IX Messaging 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

Software	Version
Hyper-V	Windows Server 2012 or 2012 R2 Hyper-V Server 2012*
OS for Messaging	Windows Server 2012 or 2012 R2 Windows Server 2016

* - 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 645 for more details on using Hyper-V Server 2012.

Virtual Environment Limitations

You cannot directly upgrade an existing Messaging server to a virtual environment. However, you can move an existing server onto a virtual machine by migrating the database using the utilities provided with the Messaging installation package. You can transfer both 7.x and 8.x systems to an 9.0 virtual environment. Messaging must be installed on a new virtual machine with a clean operating system.

Messaging installed on a virtual environment requires the same hardware resources as non-virtual machine installations.

Warning: Moving an existing Messaging environment to a virtual image is not supported. However, after installing Messaging onto the virtual machine, the data files can be migrated to the new location.

Note: The fax capability of Avaya IX Messaging within a virtual environment is limited to 8 ports.

Warning: **Do Not create checkpoints** while the servers are in operation as this can lead to serious corruption in the database. System performance may also be heavily compromised. To create a checkpoint, shutdown the server first, then create the checkpoint while the system is down.

Adding Hyper-V to the Host

Before installing Avaya IX Messaging 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

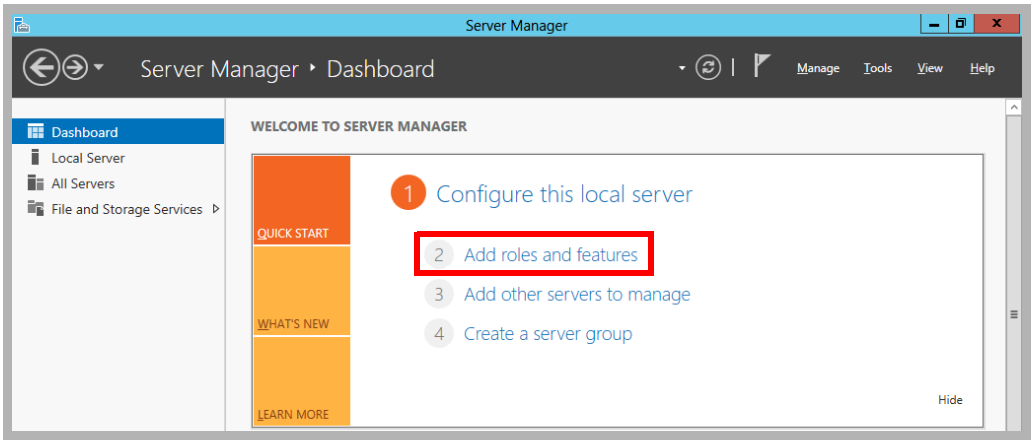
The environment created (**Guest**) on the host must have its own licensed copy of Windows installed, configured and fully patched. The version of Windows required must be one supported by Messaging.

Adding the Hyper-V Role

> **Note**: These steps are performed on Windows Server 2012, not Hyper-V Server 2012. See page 645 for details on using Hyper-V Server.

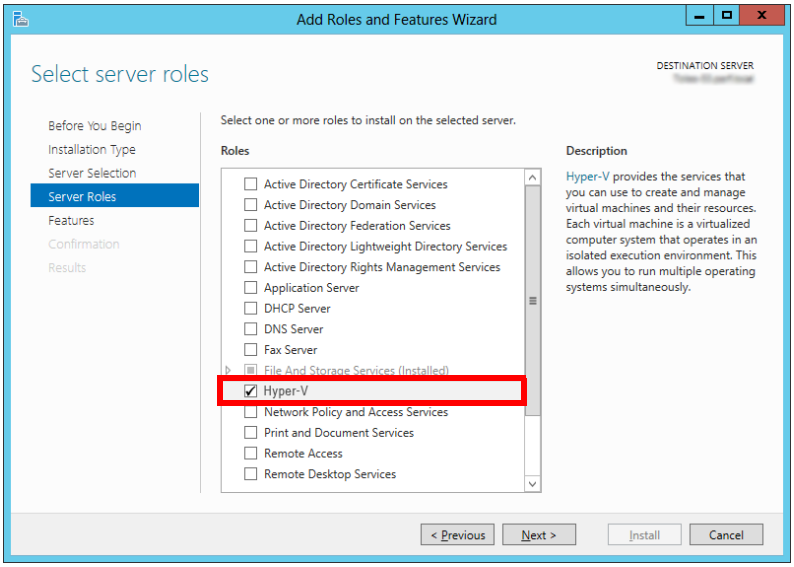
Once the **Host** has had Windows Server 2012 installed and patched, follow the directions below to add the Hyper-V role.

1. On the **Host** computer, open the **Server Manager** utility and add a new role.

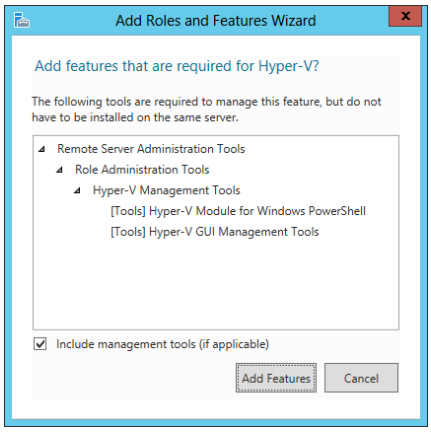


2. Proceed through the screens. At the **Select server roles** pane, enable **Hyper-V** from the available options.

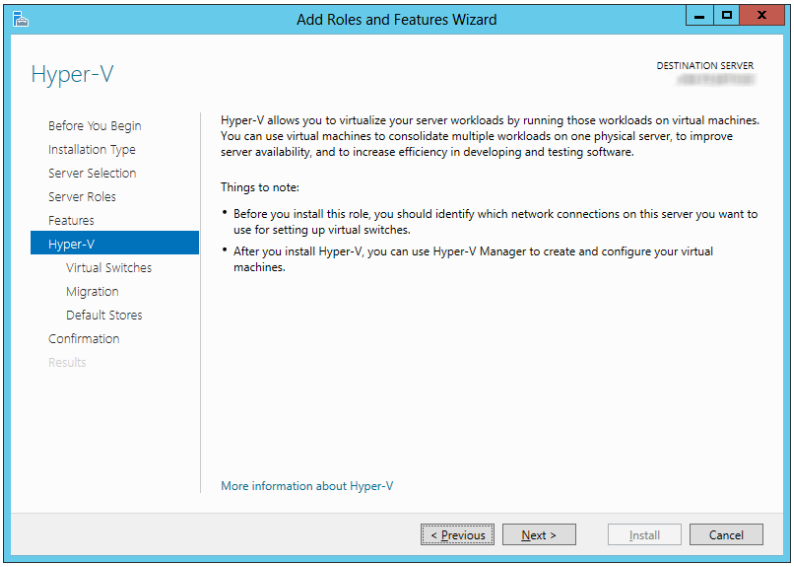
   Click **Next**.



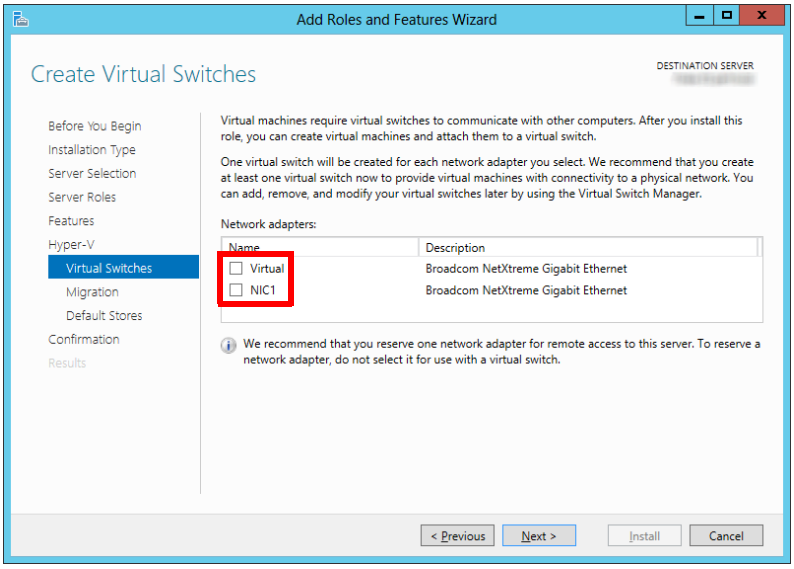
3. At the prompt, confirm the selection by clicking **Add Features**.



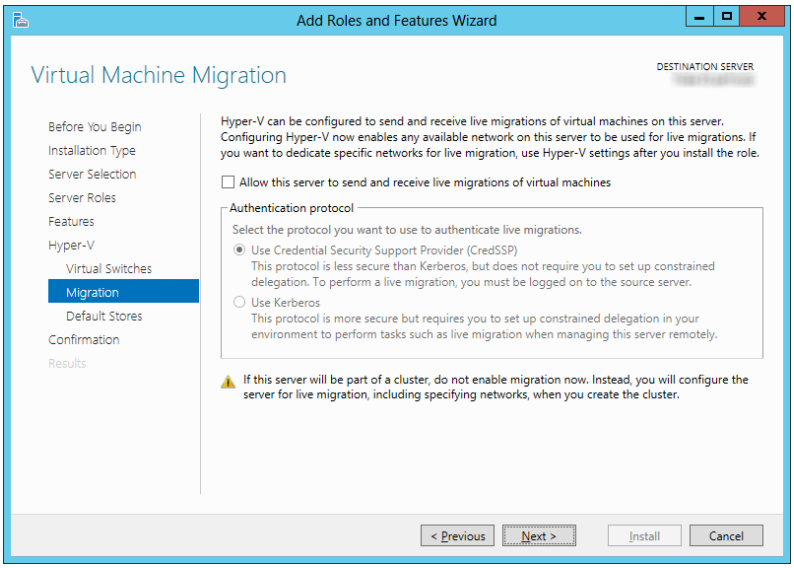
4. Continue until you reach the Hyper-V setup screen. Click **Next**.



5. Disable all of the virtual switches on the **Host**, then click **Next**.

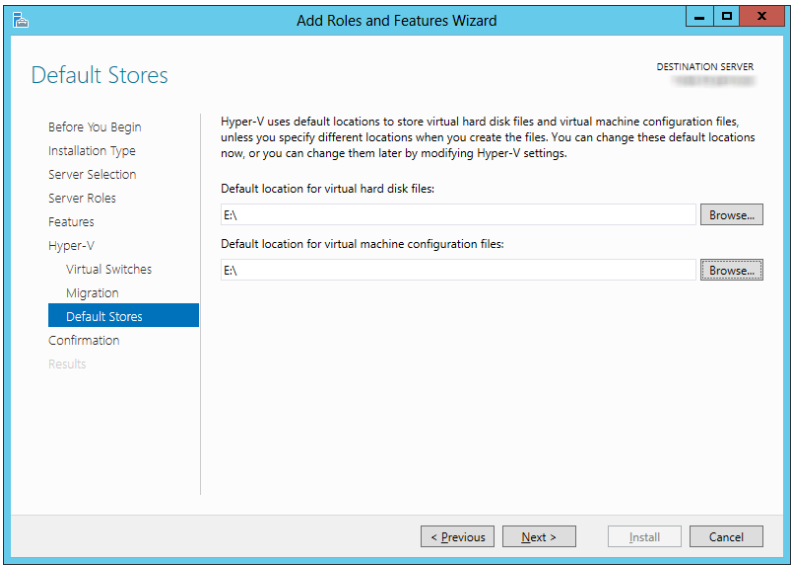


6. At the **Virtual Machine Migration** screen, leave the values at their defaults, and click **Next**.

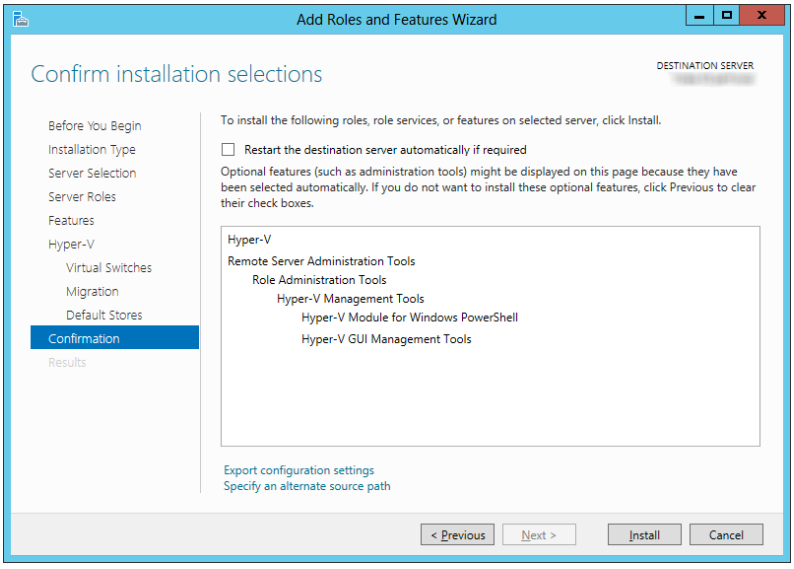


7. For **Default Stores**, specify the hard drive and file location on the **Host** where the virtual hard disk and configuration files will be kept.

   Click **Next**.

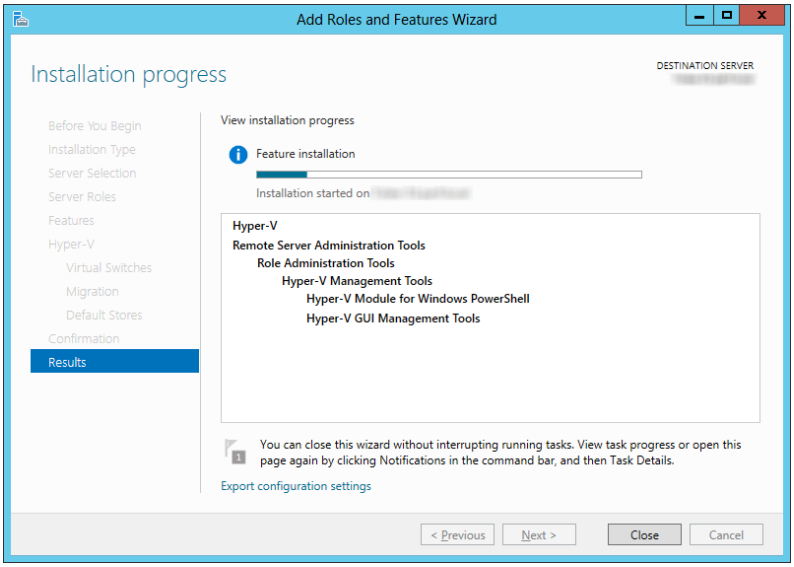


8. The **Host** has all of the information it needs. Click **Install** to add the Hyper-V role to the server.

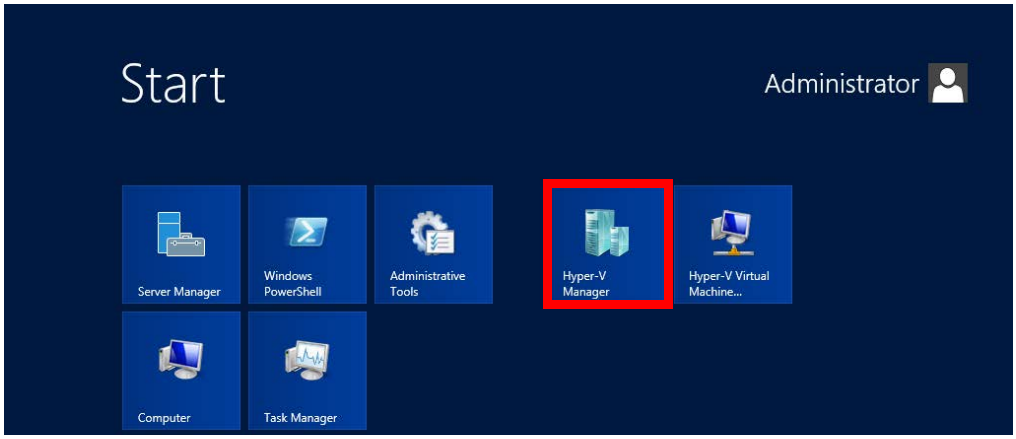


9. Support for Hyper-V virtual environments will be installed on the computer.

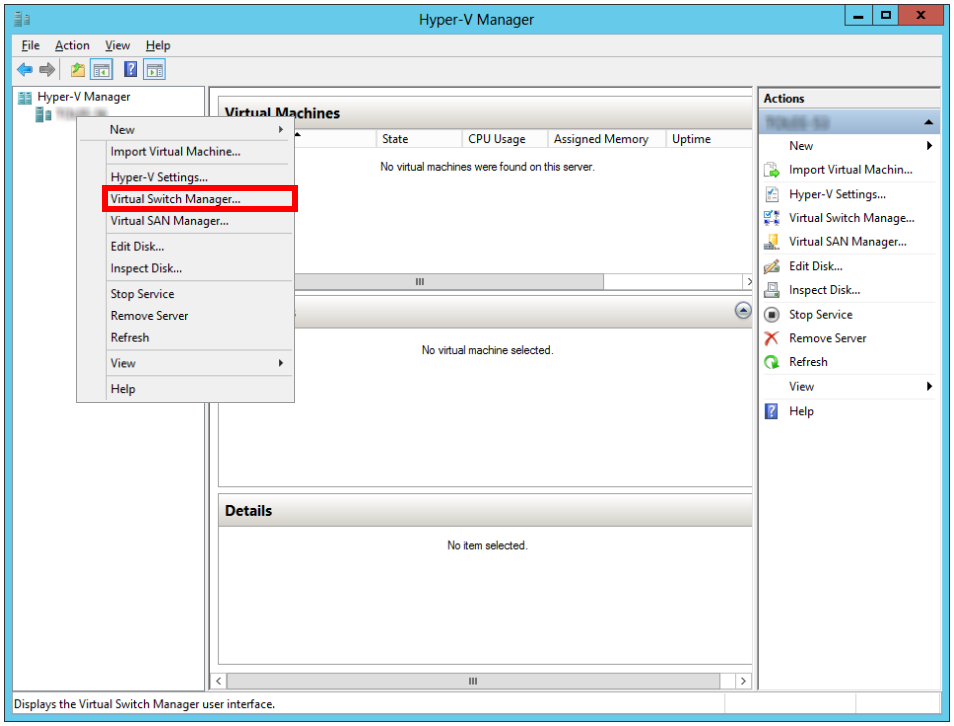
   When finished, click **Close**, then **restart the server**.



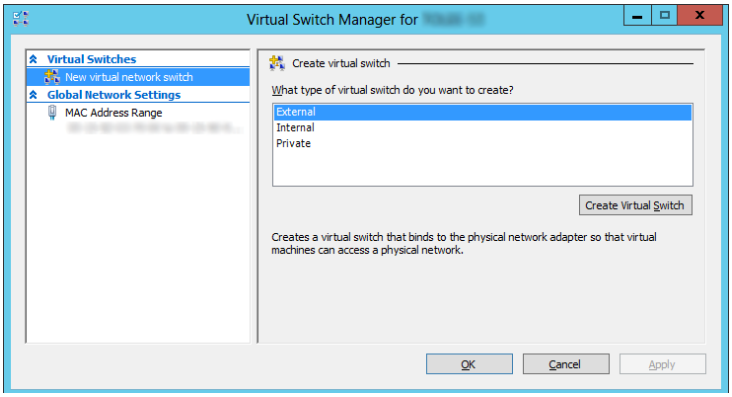
10. After the restart, open the **Start** window and select **Hyper-V Manager**.



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**.

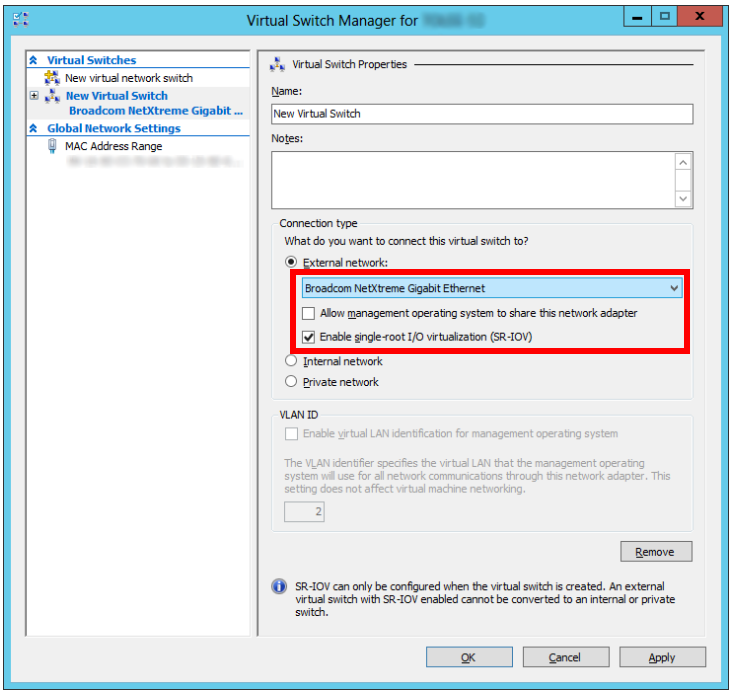


13. Enter a name for the switch.

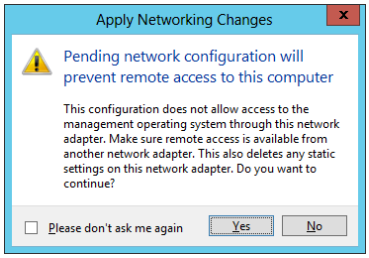
    Select a virtual switch from the list of those available on the dropdown menu. One switch is typically used exclusively for managing the virtual environment. Choose any **other** switch than the one used for management functions.

    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.

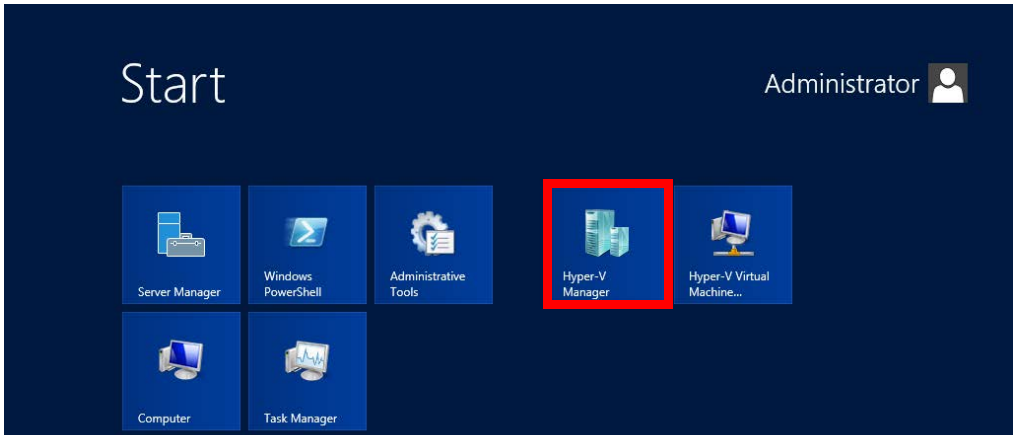


The **Host** has been configured and is ready to create new virtual environments.

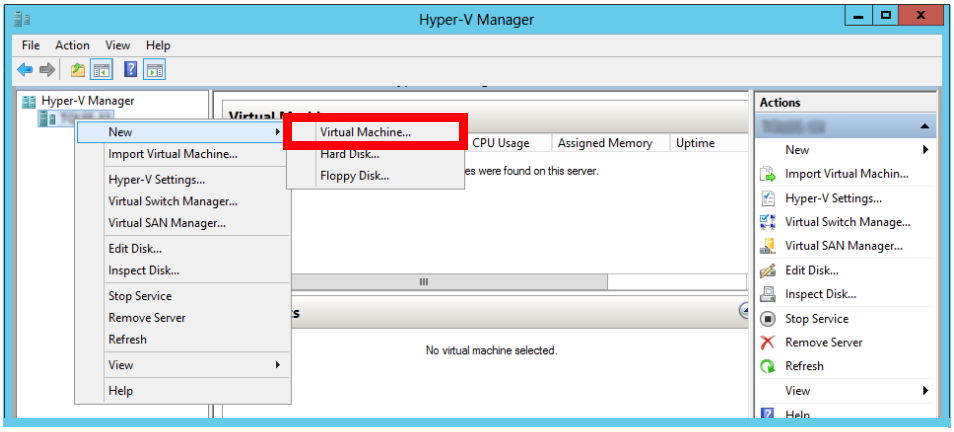
Creating the Guest Environment on the Host

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**.

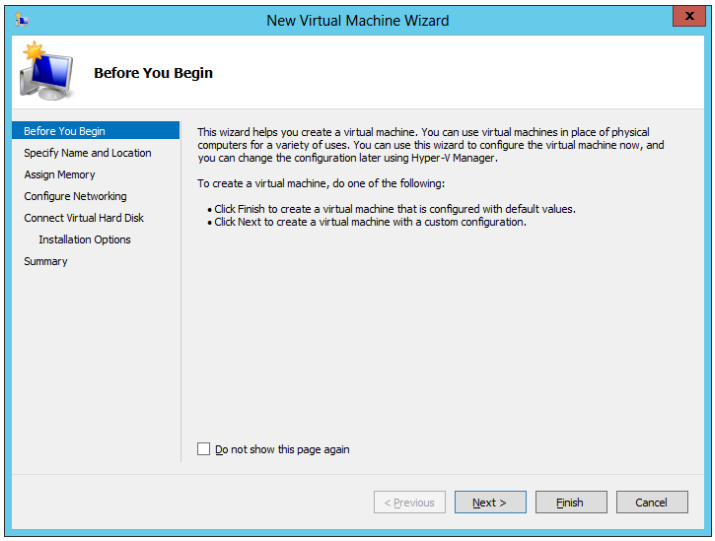


2. On the **Manager** screen, right-click the **Host** computer and select **New > Virtual Machine...**.

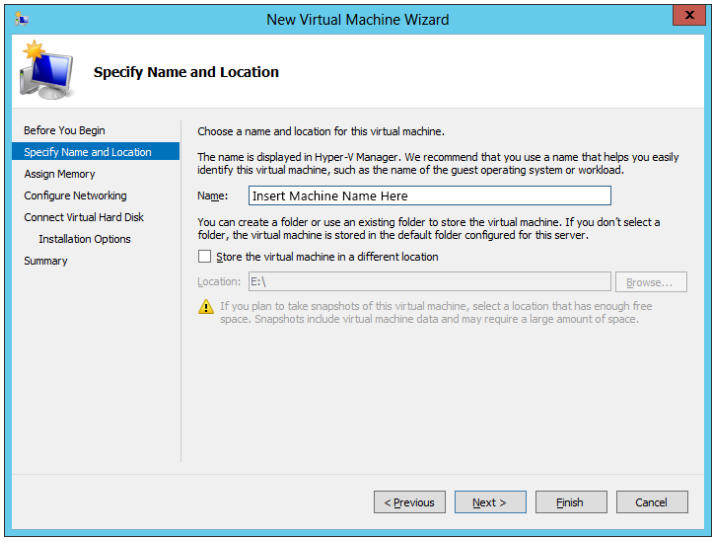


3. The **New Virtual Machine Wizard** will guide you through the process to create a new virtual environment on the selected server.

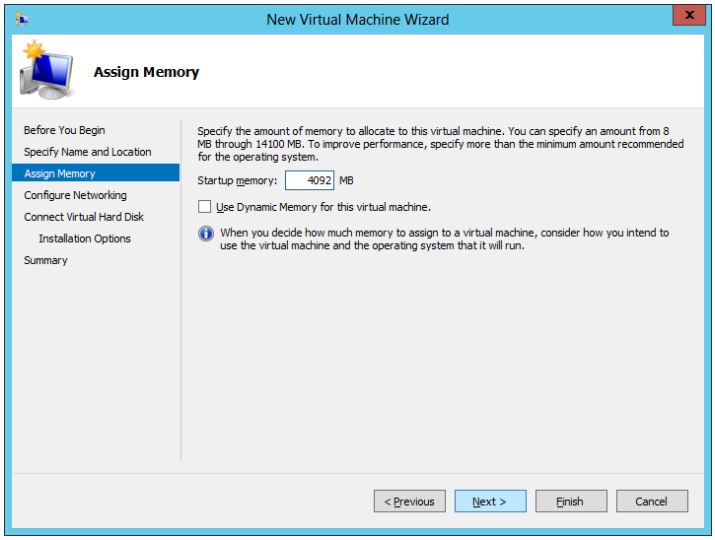
   Click **Next** to continue.



4. Give the **Guest** a name. You can also choose to store the data for the environment in a different location.

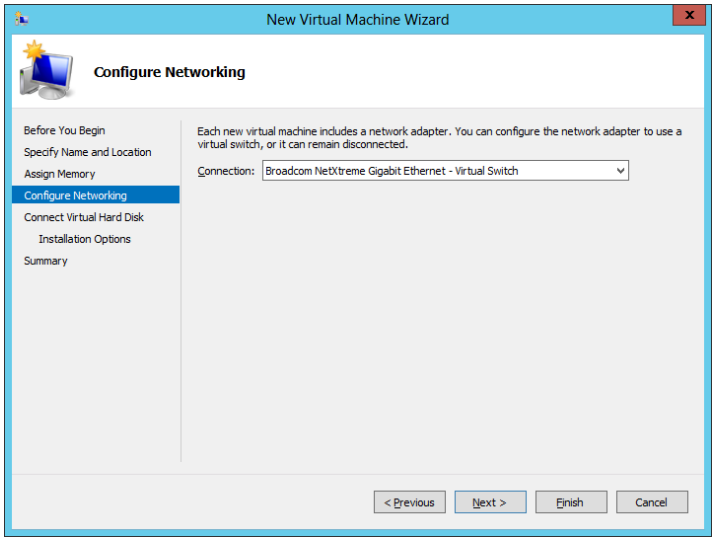


5. Specify the amount of memory the **Guest** will have. This must be at least as much as required by the version of Messaging to be installed. It is recommended that a minimum of 4GB be configured.

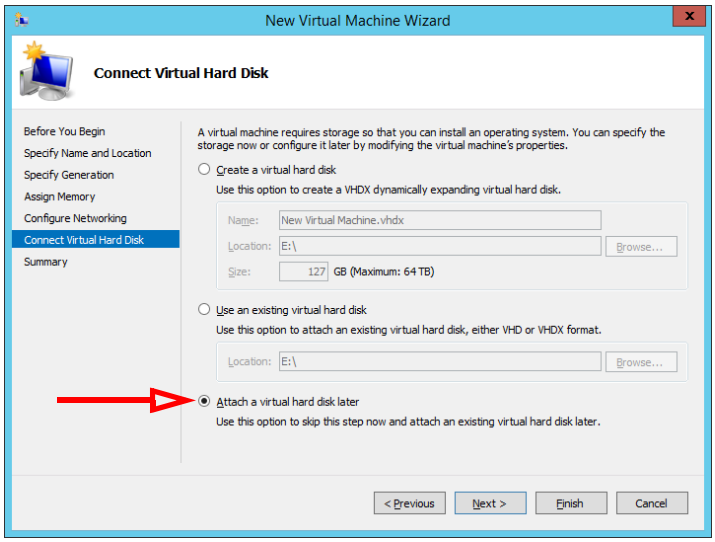


Note: The **Host** must have sufficient RAM installed to dedicate the desired amount of memory to the **Guest** environment, and still have enough remaining for its own needs.

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. Messaging requires this connection to provide access to the network and to the Internet.

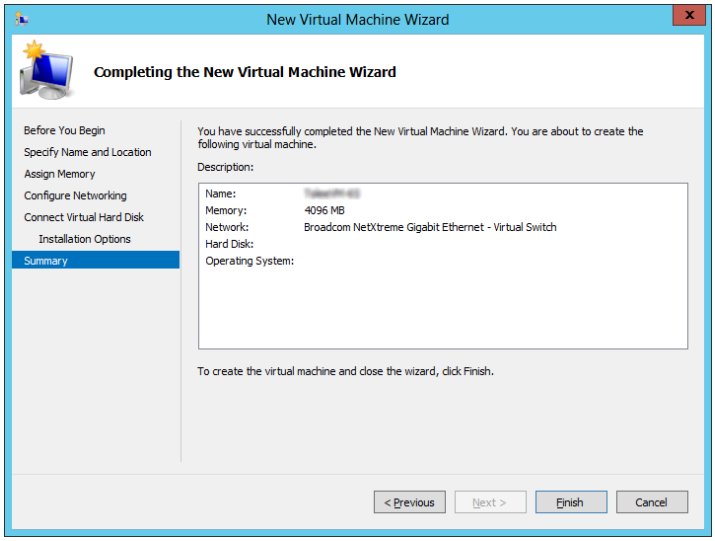


7. Select **Attach a virtual hard disk later**. Click **Next**.

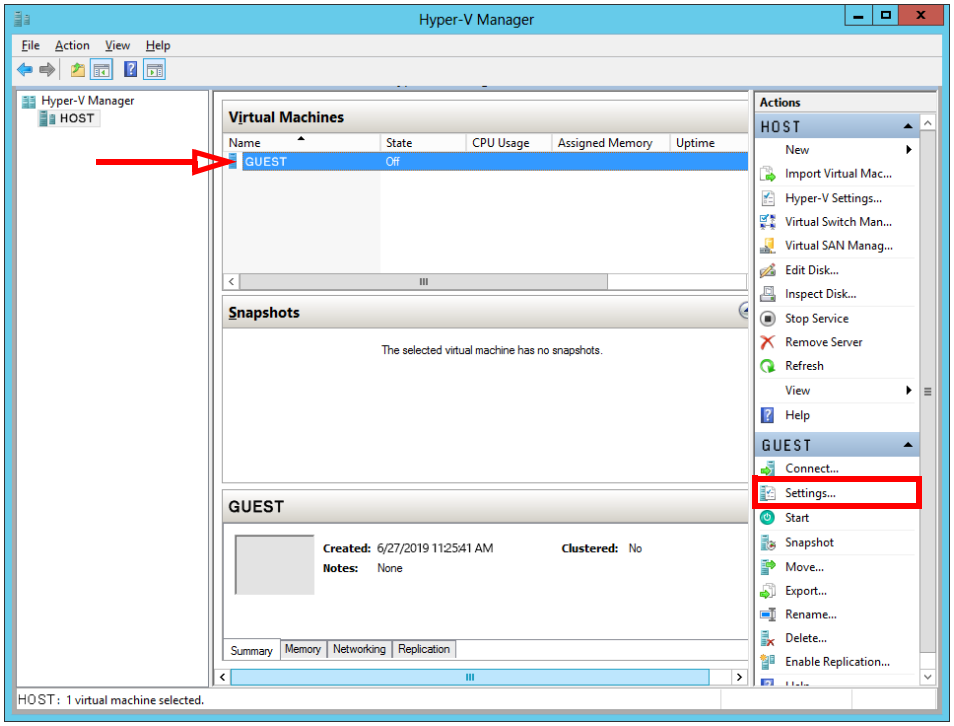


8. The **Host** has all of the necessary information to build the virtual machine.

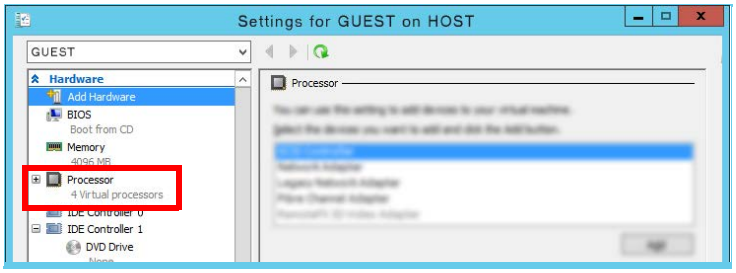
   Review the settings and click **Finish** to create the new **Guest** environment.



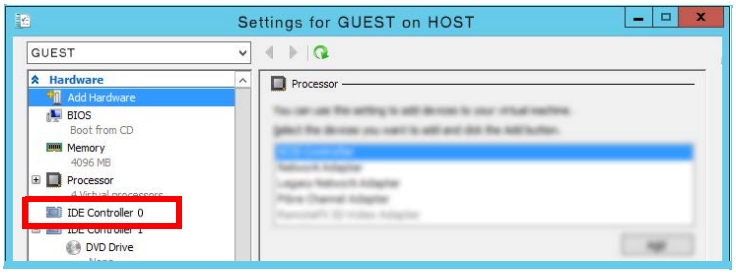
9. When the virtual machine has been created, you are returned to the Hyper-V Manager screen. The new **Guest** environment is displayed.



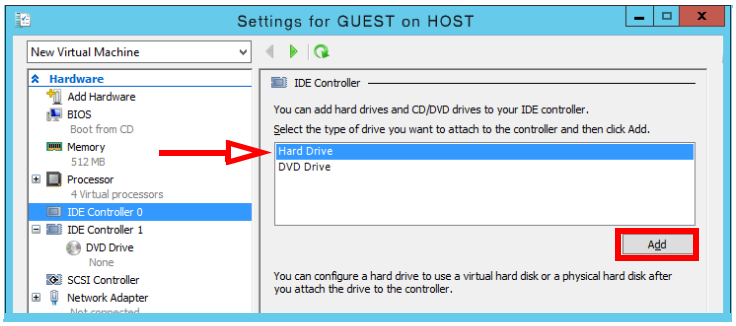
10. Open **Settings** for the **Guest** machine, and verify or set the number of processors needed to properly support Messaging.



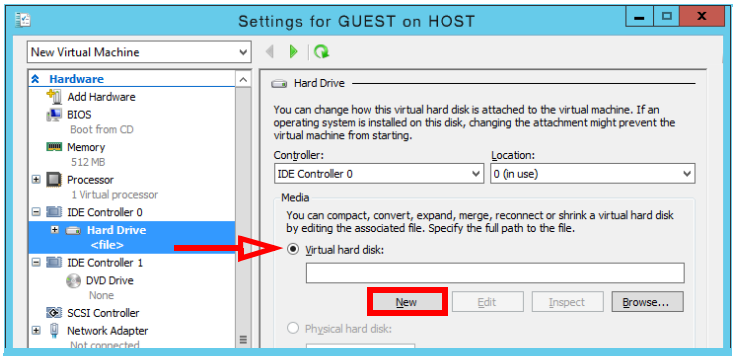
11. Open the settings for **IDE Controller 0**.



12. Select **Hard Drive**, then click **Add**.

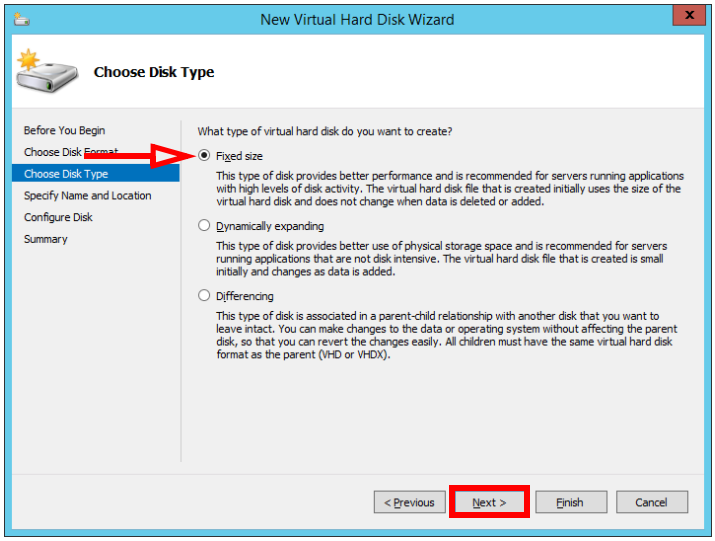


13. Enable **Virtual hard disk**. Click **New**.

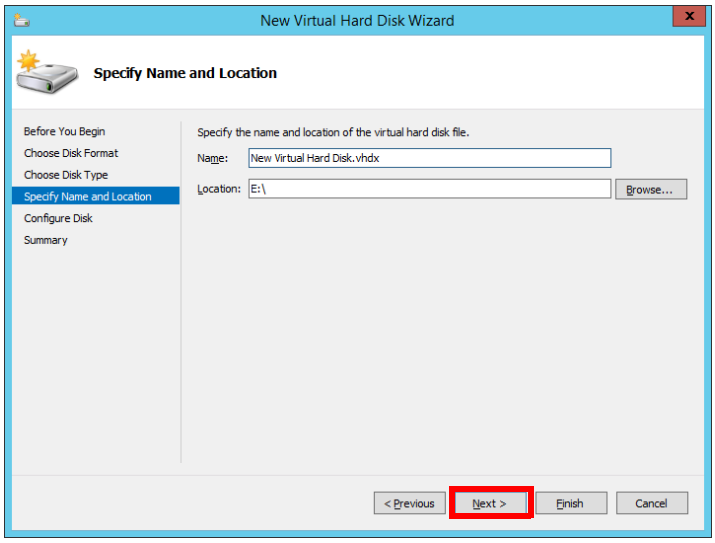


14. In the **New Virtual Hard Disk Wizard**, click **Next** until you reach **Choose Disk Type**.

    Enable **Fixed size**, and click **Next**.

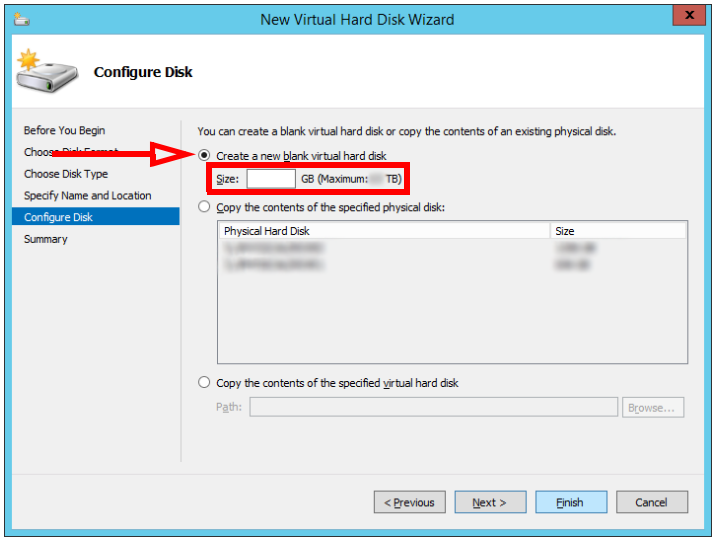


15. Specify the name for the drive, and a path to its location on the disk. Click **Next**.



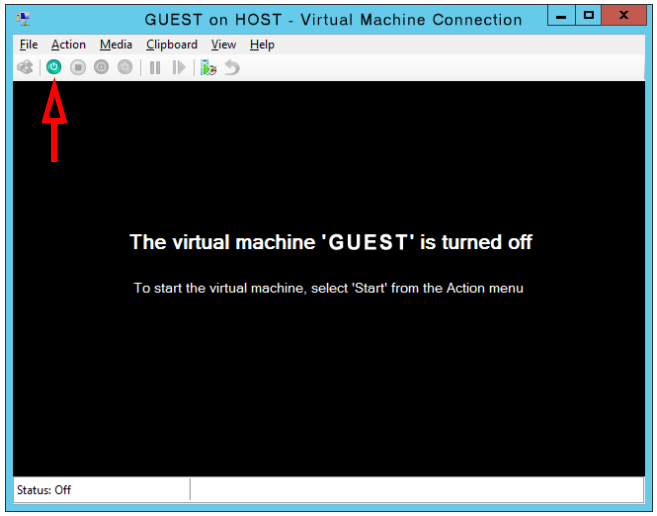
16. Enable **Create a new blank virtual hard disk**.

    Enter the size for the drive in the space provided.



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 IX Messaging software.



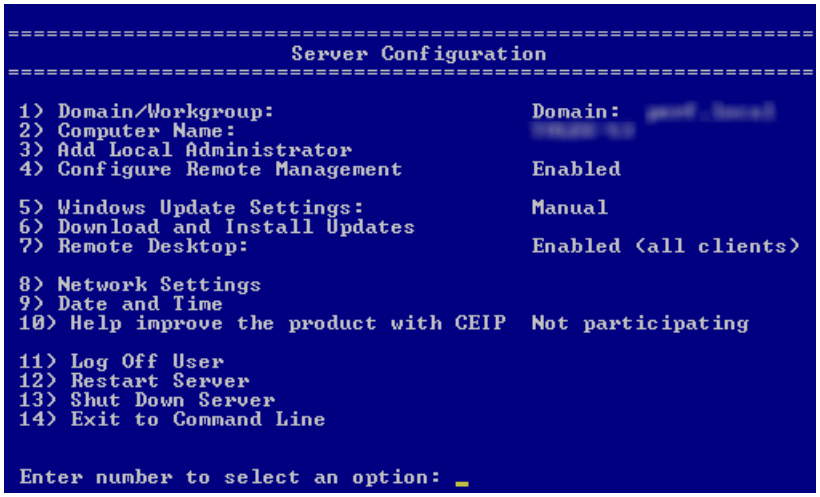
Note: The virtual machine has no operating system and no applications installed. Once the machine is on, it must be treated as a new computer. Install and configure an appropriate version of Windows and Avaya IX Messaging.

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.

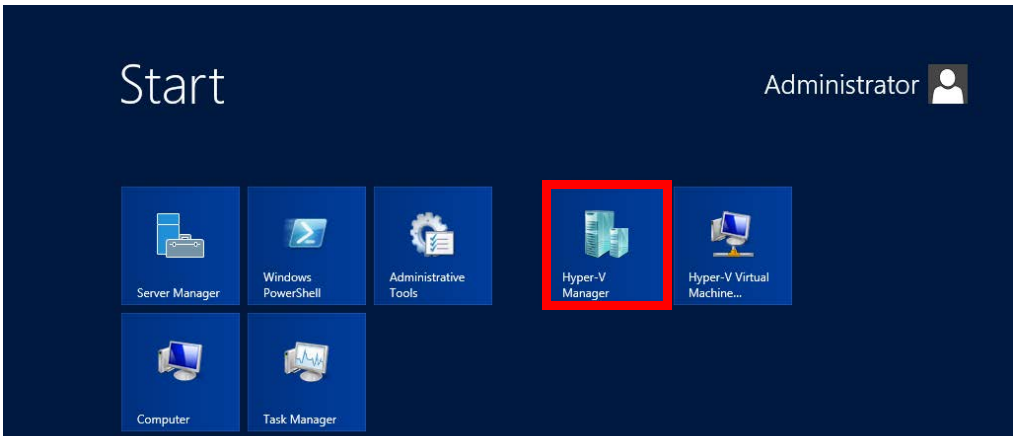


Define the following items according to your site's networking requirements:

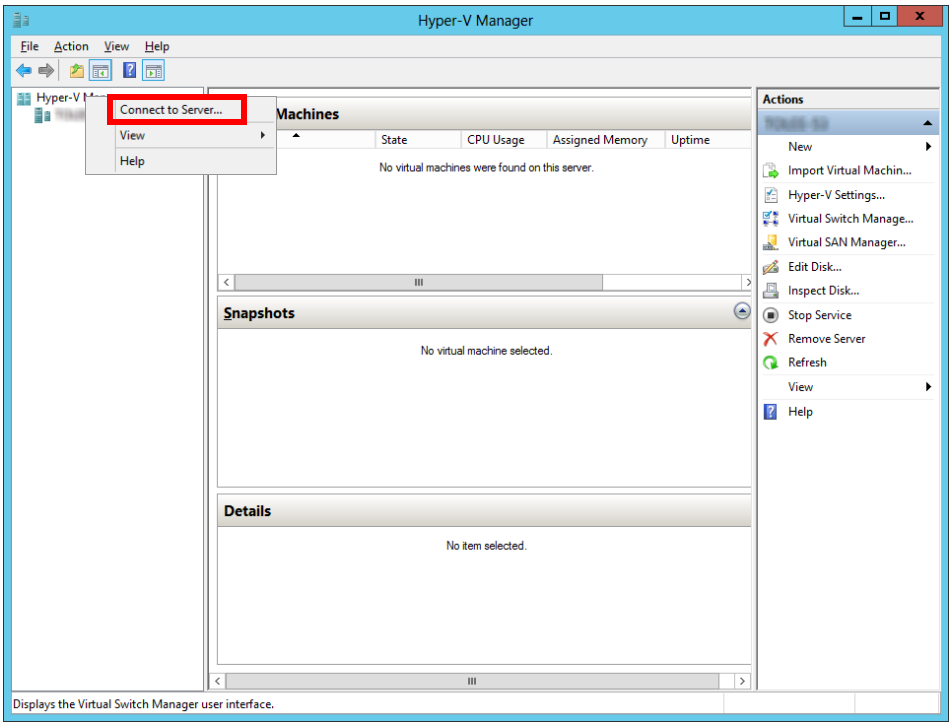
- Domain/Workgroup
- Computer Name
- Windows Update Settings
- Download and Install Updates
- Network Settings
- Date and Time

All of the other items are optional.

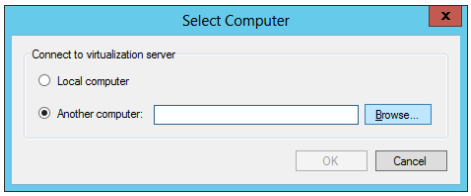
5. From a computer that has Windows Server 2012 with the Hyper-V Role installed, open **Hyper-V Manager**.



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 632.

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.

24 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 IX Messaging 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 Messaging.

For Single Server installations: Minimum Client Hardware Specifications on page 46 in the Technical Operating Guide.

For HA installations: System Requirements and Capacity on page 21 in this document.

During testing, the following AWS server configurations were validated.

MODEL	INSTANCE TYPE	vCPU (#)	MEMORY (GiB)	STORAGE (GiB)	BANDWIDTH (Mbps)
m4.xlarge	General Purpose	4	16	EBS only	750
m5.xlarge	General Purpose	4	16	EBS only	Up to 2120
c5.xlarge	Compute Optimized	4	8	EBS only	Up to 2250

Important Note

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 Primary server (HA) **DO** require an Internet connection to validate the license.

Installation

Avaya IX Messaging can be installed in a Single Server (SS) or High Availability (HA) configuration.

Follow the standard installation procedures for Messaging 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 IX Messaging 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.**

25 SINGLE SIGN-ON (SSO)

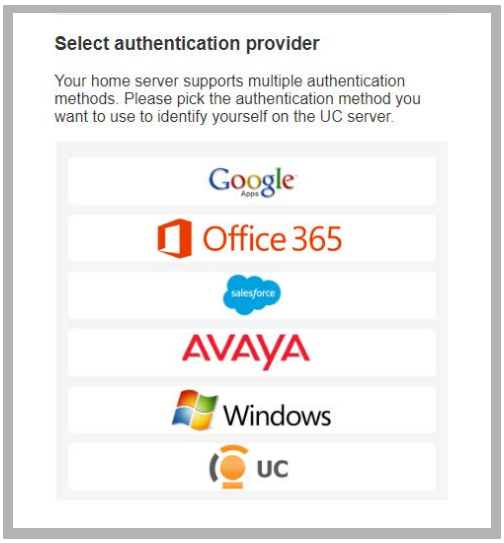
In This Chapter:

Introduction

Legacy SSO

Logging in to Avaya IX Messaging applications (**Web Admin**, **Web Access**, **Web Reports** and **Messaging Admin**) is handled using a 3rd party authentication provider, such as Salesforce, Google, Office 365 or Windows. This Single Sign-On process let's clients use their credentials from the other applications to access Messaging. This is known as **Legacy SSO**.

Clients open an application, are passed through Messaging and then onto the provider. The client's credentials are authenticated by the provider and access is granted.



Hybrid SSO

The preferred method for authentication is **Hybrid SSO** as it offers a higher level of security for your connections by adding a certificate validation layer. The Voice Server, or the Consolidated Server in a High Availability environment, is authenticated on the Avaya licensing server through a certificate enabled handshake. The client then uses whichever login credentials they have available to complete the connection from their current location.

Clients open an application and are passed through to Messaging. If the connection to the accounts.zang.io server has been validated by the certificate, the login request is sent to the provider for authentication. If either the connection is not valid, or if the client's credentials are incorrect, then access is denied.

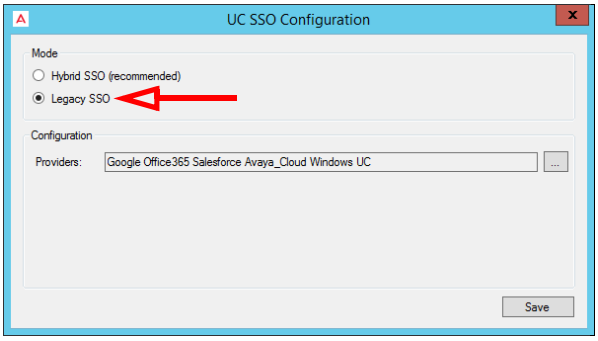
Important: The **Hybrid SSO** login procedure requires an active Internet connection. Only **Legacy SSO** can be used if Internet access is disabled / locked-down (i.e. at high security, isolated sites).

A the end of the installation routine, you are asked to select the SSO method to employ.

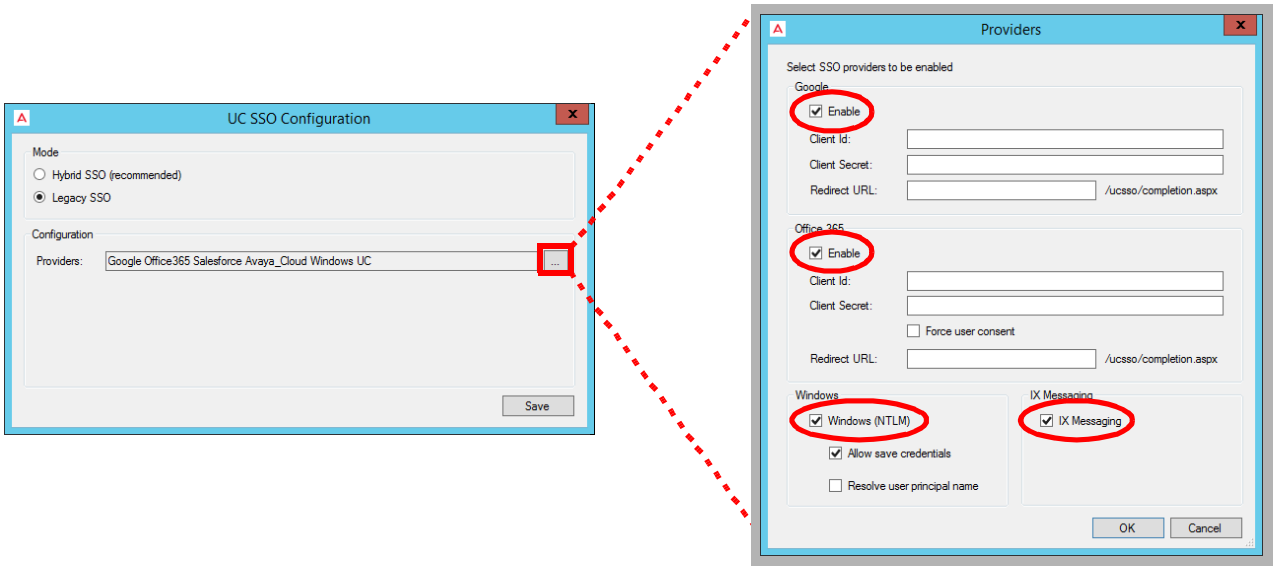
Legacy SSO

To use the **Legacy SSO** login method:

- On the SSO Configuration screen, enable **Legacy SSO**.



- From the Providers dropdown menu, enable the authentication providers that you want your clients to use to access **Web Admin**, **Web Access**, **Web Reports** and **Messaging Admin**. Items that are disabled will not appear during login.



Filling out these fields is optional and only required if you make use of OAuth2 when connecting to these providers.

- **Client Id**: Enter the OAuth2 client ID for the provider you have chosen.
- **Client Secret**: Enter the OAuth2 client secret value for the provider you have chosen.
- **Redirect URL**: Enter the URL for your company given by the provider you have chosen.

Resolve user principal name: When logging in to Windows, you must provide both the domain or computer name and a username (e.g. salesdomain\brian or mycomputer\bob). When **Resolve user principal name** is enabled, enter these details in the form userName@domain (e.g. fred@fredsplace.main). This format must be used throughout the program wherever SSO login details are required to access other applications.

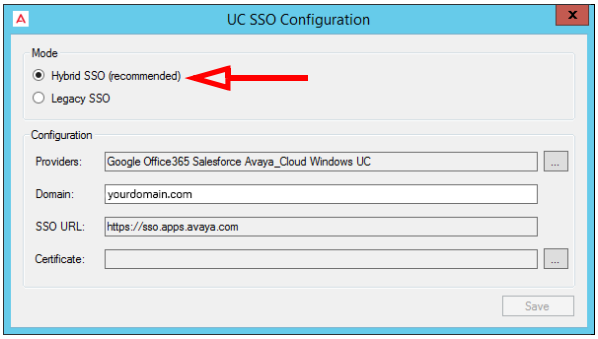
- Enable all that apply, then click **OK**.
- Click **Save** when finished.

Hybrid SSO

Important: The **Hybrid SSO** login procedure requires an active Internet connection. Only **Legacy SSO** can be used if Internet access is disabled / locked-down (i.e. at high security, isolated sites).

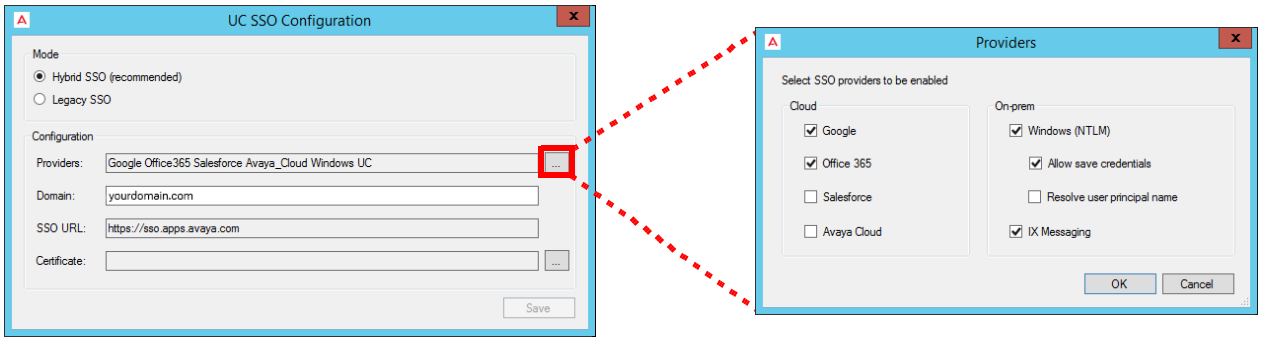
To use the **Hybrid SSO** authentication method:

- On the SSO Configuration screen, enable **Hybrid SSO**.



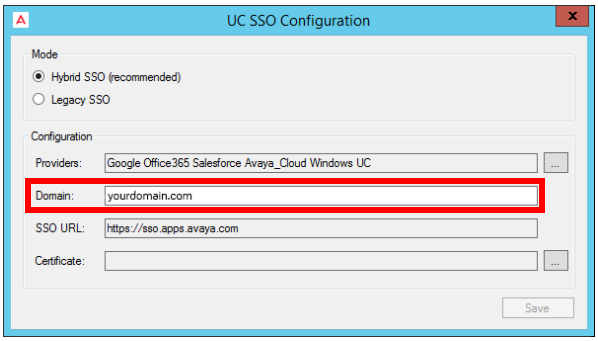
- From the Providers dropdown menu, enable the authentication credentials that you want your clients to use to access **Web Admin**, **Web Access**, **Web Reports** and **Messaging Admin**. Items that are disabled will not appear during login.

  Enable all that apply, then click **OK**.



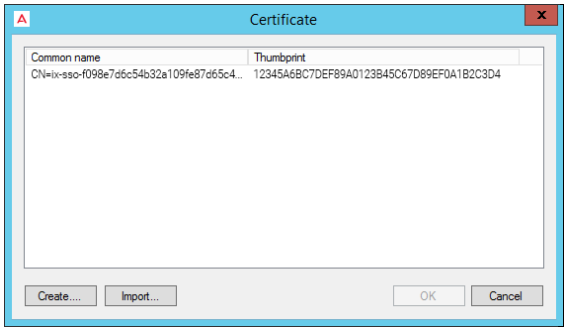
Resolve user principal name: When logging in to Windows, you must provide both the domain or computer name and a username (e.g. salesdomain\jcarter or posSystem\rosier). When **Resolve user principal name** is enabled, enter these details in the form userName@domain (e.g. fred@fredsplace.main). This format must be used throughout the program wherever login details are required to access other applications.

- Enter the domain name where your Voice / Consolidated server is located in the space provided.

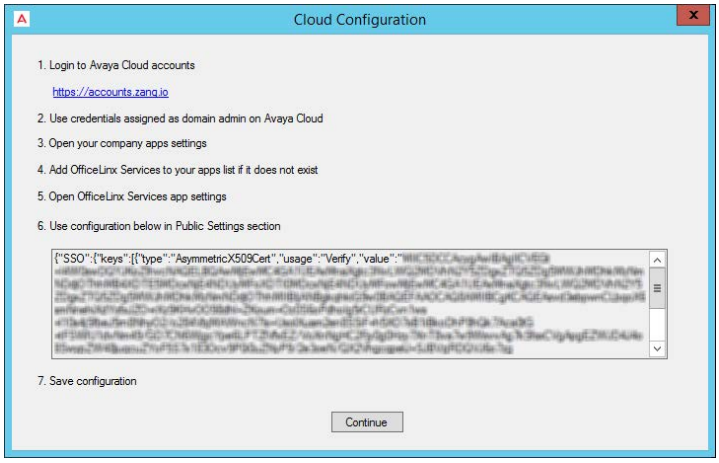


- A certificate is required when using Hybrid SSO. Click the button to the right side of the Certificate field. Choose **Create** to have Messaging build a certificate for you. Or if you have a certificate in **PFX** format that you would rather use, click **Import** and select that file instead.

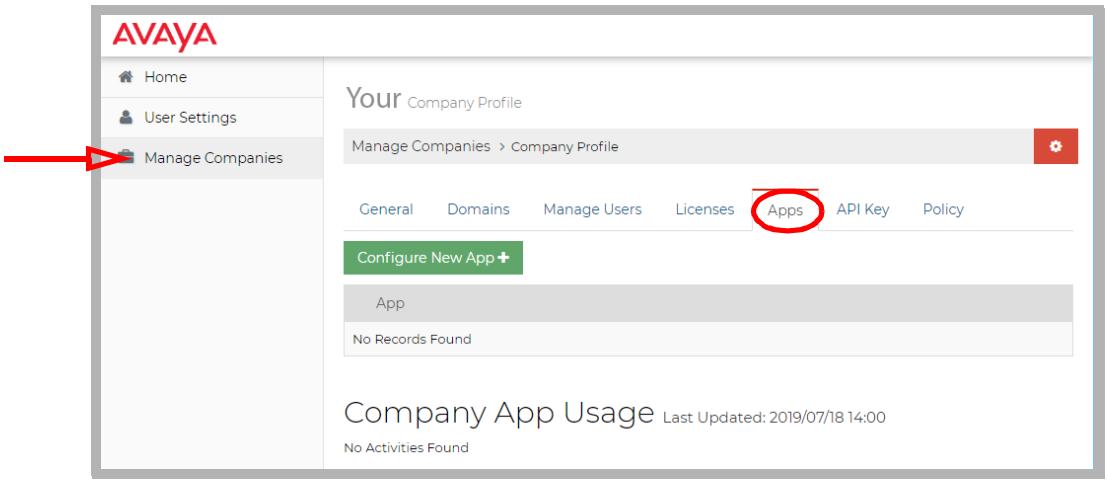
  Select the certificate to use, then click **OK**.



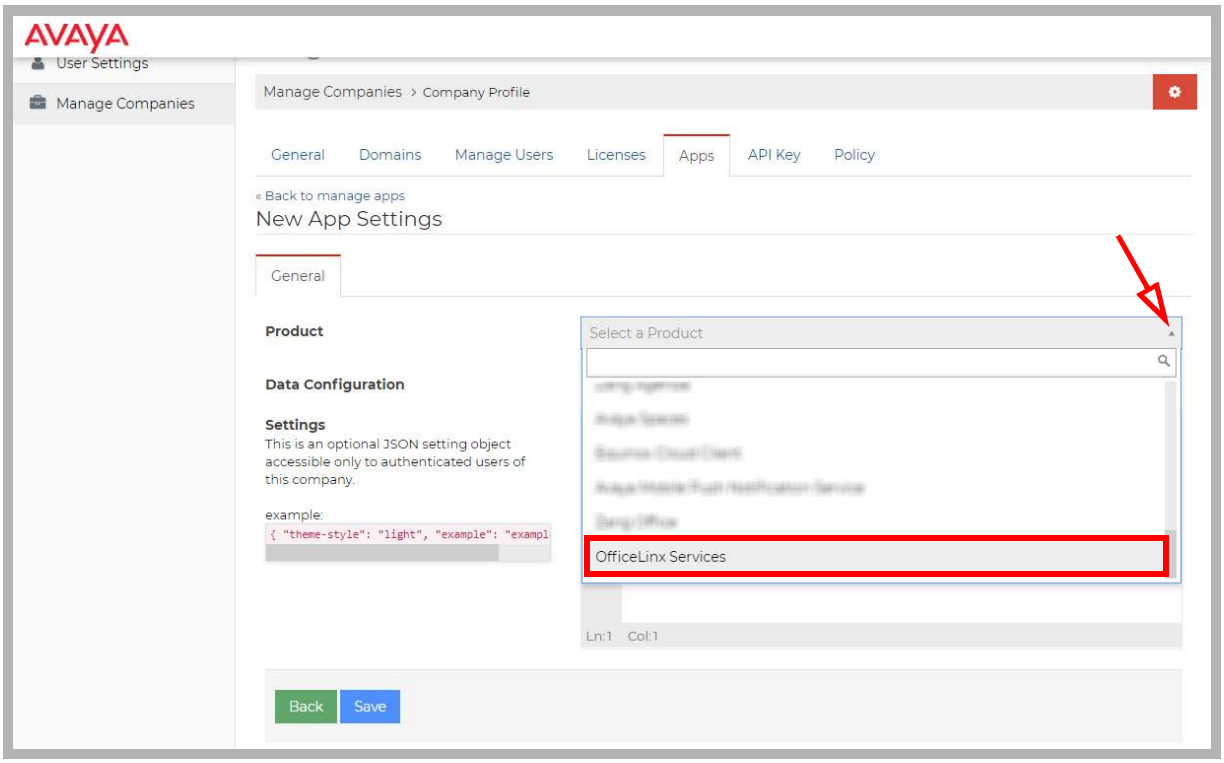
- Once back at the SSO Providers screen, click **Save**.
- Follow the instructions on this window to complete the installation.



1. Click the link, or enter the URL into the address bar of a web browser to open the Avaya Cloud Accounts site.
2. Login using credentials for an account with administrator rights to the domain.
3. Go to **Manage Companies**, select a company (if more than one), and open the **Apps** tab.

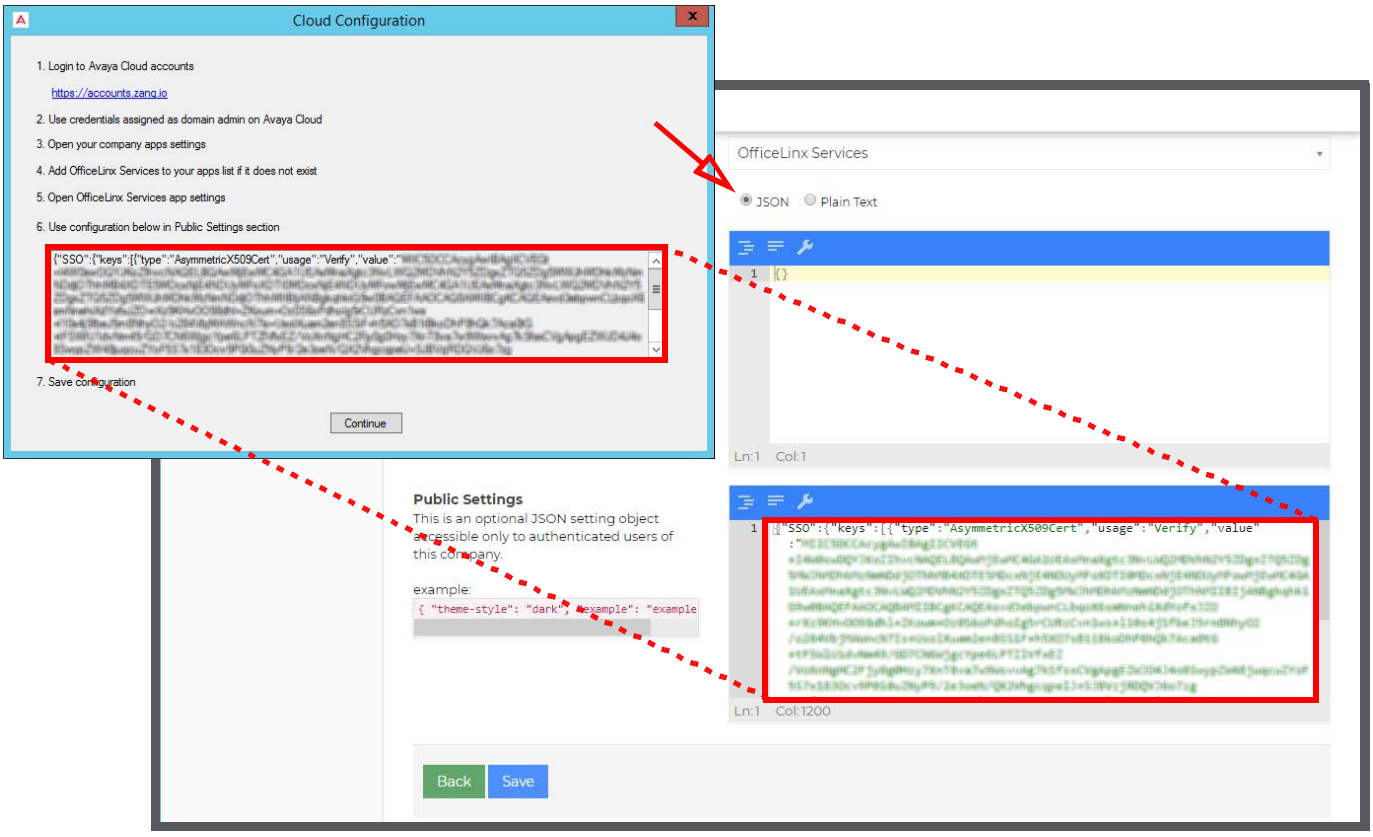


4. Click **Configure New App+**. On the **Product** dropdown menu, select **IX Messaging Services**.



5. You should land on the IX Messaging Services Application Settings page.

6. Ensure that the option for **JSON** is enabled then scroll down to **Public Settings**. Copy the string from the Cloud Configuration panel and paste it into the space provided.



Caution: Be careful to copy the **entire** string from the Cloud Configuration panel. It may extend below the bottom of the pane.

7. Click **Save** when ready. Returning to the Cloud Configuration panel, click **Continue** to complete the Hybrid SSO configuration.

As long as the strings on both the Voice / Consolidated server and the Avaya Cloud server match, users will be able to access the applications using their available credentials.

If these strings are not the same, then users will not be able to login using any credentials.

26 UPGRADING AN ASP130 SERVER

Introduction

This chapter covers the steps necessary to upgrade an existing Avaya Solutions Platform 130 from Release 4.0 (ESXi 6.5, Update 3) to Release 5.0 (ESXi 7.0, Update 2).

Procedure

1. Take the backup of Avaya IX Messaging and keep on remote servers.
   See the UC Folder And File Structure chapter of the Avaya IX Messaging Server Configuration Guide for details on Backing Up System Files.
2. To do the graceful shutdown of the application, log in to the Avaya IX Messaging application through vSphere Web Client, and do the following:
   - Select the application, right-click, and then click **Guest OS > Shut down**.
     The system displays the following message:
     Are you sure you want to shut down <virtual_machine_name>.
   - To proceed, click **Yes**.

Note: If you have a virtual machine on the host, perform a graceful shutdown of the virtual machine.

Important: Ensure that there are no calls running on the system.

3. Upgrade Avaya Solutions Platform 130 from Release 4.0 to 5.0.
   For information about upgrading Avaya Solutions Platform 130 from Release 4.0 to 5.0, see “Avaya Solutions Platform 130 Series: Upgrading to ESXi 7.0 Update 2 from ESXi 6.5.x” available from support.avaya.com.
4. If the Avaya Solutions Platform 130 upgrade is successful, power on Avaya IX Messaging and ensure that it is up and running.
   If Avaya IX Messaging is not up and running, go to step 5.
   If the Avaya Solutions Platform 130 upgrade fails:
   - Do the fresh deployment of Avaya Solutions Platform 130 Release 5.0.
     For information about installing Avaya Solutions Platform 130, see “Installing the Avaya Solutions Platform 130 Series” available from support.avaya.com.
   - Deploy Avaya IX Messaging at the same version it was before the Avaya Solutions Platform upgrade.
   - Restore the backup that is taken at step 1 and ensure everything is working fine.
     See the UC Folder And File Structure chapter of the Avaya IX Messaging Server Configuration Guide for details on Restoring Files.
5. **(Optional)**
   If Avaya IX Messaging is not up and running:
   - Do the fresh deployment of Avaya IX Messaging at the same version that it was before the Avaya Solutions Platform 130 upgrade.
   - Restore the backup that is taken at step 1 and ensure everything is working fine.
     See the UC Folder And File Structure chapter of the Avaya IX Messaging Server Configuration Guide for details on Restoring Files.

Note: If multiple applications are on the same server, follow the upgrade order for restoring the backup.

APPENDIX A: REVISION HISTORY

DATE	ISSUE	CHANGE SUMMARY
30 September, 2019	10.8 (1)	Initial Document Release
1 October, 2019	10.8 (2)	Added warning not to take snapshots / checkpoints on virtual machines while the servers are operating.
4 October, 2019	10.8 (3)	Reinstated and updated chapter on upgrading from Officelinx 9.x+ to IXM 10.8.
16 October, 2019	10.8 (4)	Added the SSO configuration step to the upgrade section.
17 October, 2019	10.8 (5)	Carbonite Availability v 8.3 has not been validated, so we only officially support version 8.2 for now. Strengthened warning against Carbonite in High Security sites.
7 November, 2019	10.8 (6)	Modified Maximum System Capacity requirements.
15 November, 2019	10.8 (7)	Creating self-signed certificates may not be allowed at JITC sites. Added a procedure to create public and private certificates for HA environments.
2 December, 2019	10.8 (8)	Added Role setup to HA installation for Windows 2016 machines. 2012 and 2016 have different requirements.
23 January, 2020	10.8 (9)	Moved the HA upgrade section into its own chapter. Revised Carbonite chapter to reflect that it can only be used on the Consolidated server, not on the Primary or Secondary servers.
4 February, 2020	10.8 (10)	Removed server specs from WebLM. Directed users to Avaya docs. Added new option to SSO configuration: Resolve user principal name. New note for upgrades requiring the use of the correct user account when logging in.
10 February, 2020	10.8 (11)	There is a new path and procedure for upgrades. Download the files in a zip file, unpack and launch the installer. Changed the VM Support chapter to include HA support for the Primary server.
25 February, 2020	10.8 (12)	Added note to TLS section to make explicit support for UC management programs like Avaya Aura. New paragraph on license expiration milestones for HA Primary server not functioning. Included System Requirements chapter from TOG for sizing referencing.
3 March, 2020	10.8 (13)	Added chapter supporting Windows Server 2019.
25 March, 2020	10.8 (14)	New chapter on how to backup Remote CSE servers in an HA system.
16 May, 2020	10.8 (15)	Cleaned up leftover references to TSE.
28 May, 2020	10.8 (16)	New chapter on stopping services before updating Windows.
24 June, 2020	10.8 (17)	Added Geo Redundancy requirements to the HA chapter.

DATE	ISSUE	CHANGE SUMMARY
7 July, 2020	10.8 (18)	Added the SRM to the list of services that must be stopped before updating the Windows O/S.
29 July, 2020	10.8 (19)	Adjusted the minimum requirements for installation.
31 August, 2020	10.8 (20)	Updated system and O/S requirements.
9 October, 2020	10.8 (21)	Corrected an omission in the Windows 2012 installation procedure.
27 October, 2020	10.8 (22a)	Included a note that each Remote CSE Server can only support a single email type.
4 January, 2021	10.8 (23)	Updated installation to say that Microsoft .NET Framework 4.7.2 is required.
12 April, 2021	10.8 (24)	Added requirements for VMWare client provisioning. Corrected several steps in the DB Migration process.
21 April, 2021	10.8 (25)	Fixed some configuration issues and changes to Carbonite setup. Included Windows 2019 support to HA environments.
6 July, 2021	10.8 (26a)	Updated installation specifications to require RAID 10 hard drive array.
28 July, 2021	10.8 (27)	Updated the TCP/IP Ports table. Removed support for vMotion.
10 August, 2021	10.8 (28)	Added requirement to select port 5061 for MWI TCP and TCP setup.
16 September, 2021	10.8 (29)	New chapter for updating an ASP130 from version 4.0 to 5.0. Included procedure for adding additional Secondary voice Servers to an HA environment.
30 September, 2021	10.8 (30)	Clarified the upgrade steps when moving from and older version of Officelinx (<10.x) to a later version requires moving to 10.1 first.
5 October, 2021	10.8 (31)	Revised the procedure for removing unwanted language packs. Added new provision for passwords (only one per user at a time).
28 October, 2021	10.8 (32)	Removed references to POP3 and IMAP4 as they are not supported.
26 November, 2021	10.8 (33)	Time zones for each server in an HA environment must be configured identically. Added support for Edge Chromium.
1 December, 2021	10.8 (34)	Note: Using an administrator account to perform routine functions leaves the servers open to malicious software attacks. Therefore, it is strongly recommended that each user with administrative privileges is also assigned a standard user account. To maintain security integrity, the administrator account should only be used when necessary, and should be immediately logged out afterwards.
14 December, 2021	10.8 (35)	Adjusted the order of operations when updating an HA installation. Removed references to DVDs.
16 December, 2021	10.8 (36)	Added some clarification on the EFS certificates for JITC installations and how they are used.