IP Office™ Platform 10.0

Installing Avaya one-X® Portal for IP Office™ Platform

15-601140 Issue 11g - (21 September 2017)

© 2017 AVAYA All Rights Reserved.

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

Documentation disclaimer
"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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 a 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 IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING 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. 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 Designated Processor that hosts 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 type(s)
Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. 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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software
"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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 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 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
Customer acknowledges and agrees that it is responsible 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.

Contents

1. one-X Portal for IP Office

1.1 Providers 10
1.2 one-X Portal for IP Office Settings..... 11
1.3 Small Community Network Support..... 13
1.4 Terminal services support..... 13

2. Installation (Windows)

2.1 Installation Requirements..... 17
2.1.1 Exchange Server Requirements..... 20
2.2 Check the IP Office Security Settings..... 21
2.3 Add one-X Portal for IP Office Licenses..... 22
2.4 Configure Users for one-X Portal for IP Office..... 23
2.5 Checking Available Server Ports..... 24
2.6 Install the one-X Portal for IP Office Software..... 26
2.6.1 one-X Portal for IP Office software upgrade..... 27
2.7 Initial Server Configuration..... 28
2.8 Test User Connnection..... 31
2.9 Adding Certificates..... 32
2.10 Configuration for 300+ IP Office Users..... 33

3. Configuring Microsoft Exchange Server Integration

3.1 Install and Enable Digest Authentication..... 37
3.2 Create the AvayaAdmin User Account..... 38
3.3 Configure the AvayaAdmin User Account..... 38
3.4 Set Impersonations Rights for AvayaAdmin..... 38

4. Desktop Client Group Policy Installation

4.1 Creating a Distribution Point..... 41
4.2 Creating a Group Policy Object..... 42
4.3 Assigning an MSI Package..... 43
4.4 Publishing an MSI Package..... 44
4.5 Redeploying an MSI Package..... 45
4.6 Removing an MSI Package..... 46
4.7 Silent Installation Commands..... 46

5. Document History

Index 49

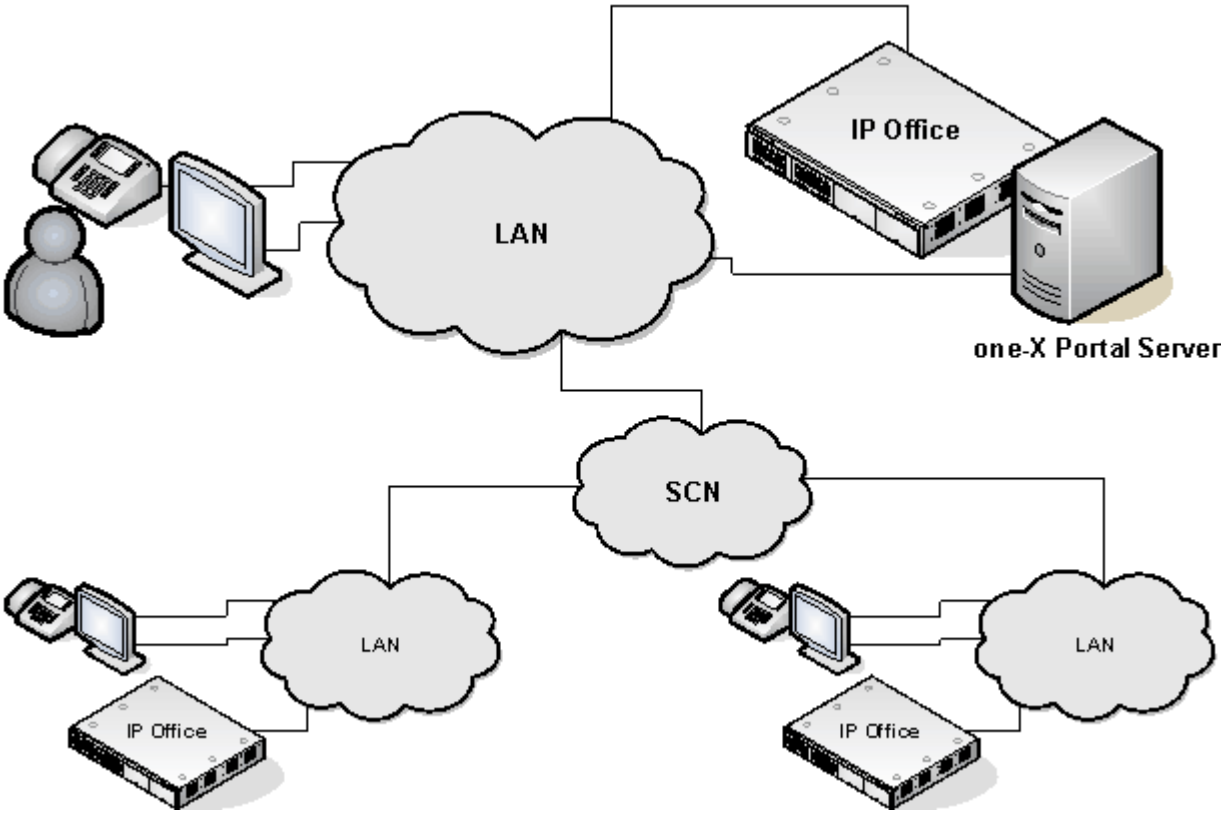
Chapter 1.
one-X Portal for IP Office

1. one-X Portal for IP Office

This documentation covers the installation of one-X Portal for IP Office supported by IP Office Release 10.0. It details the Windows installation, which is supported with the IP500 V2 only.

It does not cover Linux installation (IP Office Server Edition, IP Office Application Server and Unified Communications Module), however other sections are still applicable to configuring Linux based servers and understanding their operation.

one-X Portal for IP Office is a server application that allows IP Office users to control their phone and various telephony settings through a web browser. A single one-X Portal for IP Office server can support multiple IP Offices when they are connected in a single IP Office Small Community Network 13 (SCN).



one-X Portal for IP Office supports up to 750 simultaneous sessions in a network even if more IP Office users are configured for portal usage. This applies whether using a Windows or Linux based one-X Portal for IP Office server.

one-X Portal for IP Office installs as a service with an integral web server. Both user and administrator access to one-X Portal for IP Office is via web browser to the server. The one-X Portal for IP Office service communicates with the IP Office system using the IP Office's TSPI (Telephony Service Provider Interface) service. This service is configured through the security settings of the IP Office control units.

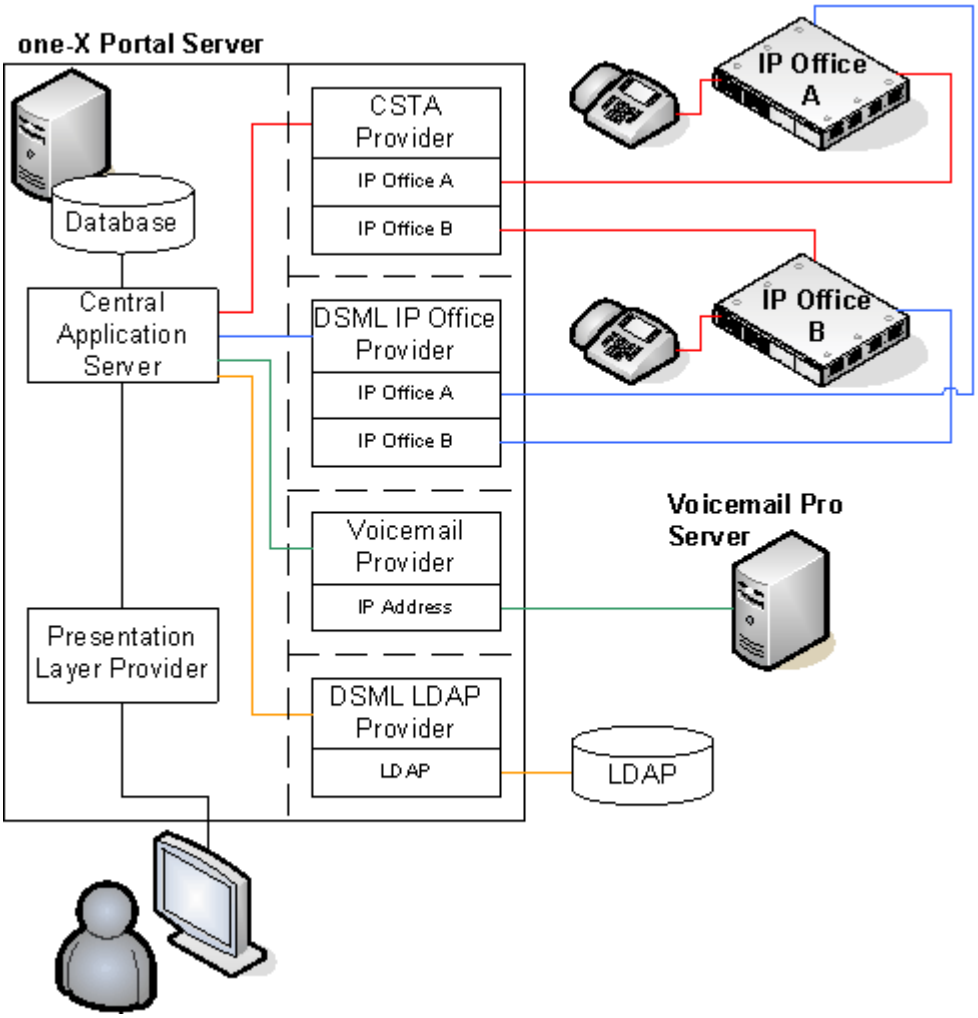
In addition to using one-X Portal for IP Office directly for telephony functions, the portal server and its link to the IP Office telephone system is used to support and enable a range of other applications:

- **Desktop Clients**
  The one-X Portal for IP Office supports a number of desktop client through which the user access one-X Portal for IP Office functions without having to use the full one-X Portal for IP Office browser interface.
  - **one-X Portal Call Assistant**
    This Windows user application adds an icon to the system tray that then shows popup call and message notifications. The user can also make and control their calls using the application.
  - **Avaya IP Office Plug-in**
    This desktop client integrates with the user's Microsoft Outlook and allows them to make and control calls from within their Outlook.
- **one-X Mobile Preferred for IP Office**
  The one-X Mobile application can be installed on Android and iOS mobile phones.
- **Microsoft Lync**
  User's can use the Microsoft Lync client to make and receive calls.
- **Web Conferencing**
  Selected users can host web conferences for visual presentations and document sharing in parallel with audio conferences.

1.1 Providers

A key idea to understand for one-X Portal for IP Office is providers. Providers are components of one-X Portal for IP Office, each of which performs a specific role. The different types of provider are:

- **Presentation Level Provider**
  This type of provider handles the browser connections between users and the one-X Portal for IP Office server.
- **Telephony CSTA Provider**
  This type of provider handles telephony communications to and from the IP Office systems assigned to it.
- **Directory DSML IP Office Provider**
  This type of provider handles obtaining directory information from the IP Office phone systems assigned to it.
- **Directory DSML LDAP Provider**
  Handles obtaining LDAP directory information from an LDAP source. LDAP sources are assigned to the provider during installation.
- **VoiceMail Provider**
  Handles direct interaction with the voicemail server for features such as message playback via the browser.



During installation:

- One provider of each type is created.
- The IP Offices indicated during installation are assigned to the Telephony CSTA and Directory DSML providers. Following installation, additional IP Offices can be assigned as they are added to the Small Community Network.
- A Directory DSML LDAP provider is created even if no LDAP source is assigned. The actual LDAP sources can be assigned after installation.
- A Voicemail provider is created even if no Voicemail servers are configured.

1.2 one-X Portal for IP Office Settings

The sections below detail which user and directory data is stored by the one-X Portal for IP Office server and which is stored by the IP Office systems.

Directories

The various directories available to a one-X Portal for IP Office user are taken from a number of sources:

- **Personal Directory**
  As personal directory records are added, they are stored by both the one-X Portal for IP Office application and by the telephone system and kept in synch. The telephone system can only store up to <%PERSONAL_DIR_CAPCITY %> personal directory entries per user (subject to its own system limits).
  - Personal directory records stored by one-X Portal for IP Office can contain several numbers, with one selected as the Primary phone number. The matching records stored in the IP Office configuration contains just one number, that being the one selected as the Primary phone number. Changing the Primary phone number selection in one-X Portal for IP Office will update the number stored in the IP Office configuration to match.
  - Any contacts uploaded from the IP Office Plug-in for Microsoft Office are listed in the Outlook group under the Personal tab. They are stored in the one-X Portal for IP Office only, and are in addition to the maximum <%PERSONAL_DIR_CAPCITY%> Personal Directory contacts.
  - The system limit for total personal directory records depends on the IP Office control unit being used. When this limit is reached, additional personal directory records are stored by one-X Portal for IP Office only.
    - **IP500/IP500v2:** 10800 total personal directory records.
  - For users with a 1608, 1616, 9500 or 9600 phones, they can edit or delete contacts through the phone's menus (primary phone number only).
- **System Directory**
  The system directory contains records for all the users and groups on the IP Office systems assigned to one-X Portal for IP Office plus the system directory entries stored in the configuration of those systems. It does not include directory records those systems obtain by LDAP and or HTTP import.
  - In an IP Office Small Community Network, the system directory entries configured on one IP Office system can be dynamically shared by other IP Offices in the network. This is a Centralized System Directory. The IP Office used to store the system directory used by the other systems should be one of those also assigned to one-X Portal for IP Office.
  - If multiple IP Office systems are configured to operate with one-X Portal for IP Office, the system directories of each are combined by one-X Portal for IP Office into a single system directory for use by one-X Portal for IP Office users. If the same name exists in more than one IP Office system directory, that name will exist as multiple records in the one-X Portal for IP Office system directory. If this is undesirable, the centralized system directory feature supported by IP Office 5.0 and higher systems should be used to have the system directory record configured on just one IP Office but shared by HTTP import on the other IP Offices.
  - Since the system directories are available to all one-X Portal for IP Office users, the number must be dialable by all one-X Portal for IP Office users. Alternatively, short codes should be used to ensure that numbers selected from the one-X Portal for IP Office system directory are interpreted correctly by the user's own IP Office.
  - The one-X Portal for IP Office administrator can add System Directory contacts that are stored as part of the one-X Portal for IP Office configuration rather than IP Office configuration. These contacts can have multiple phone numbers and email addresses in the same way as user's Personal Directory contacts, but are available to all one-X Portal for IP Office users.
- **External Directory**
  The external directory is not stored by one-X Portal for IP Office. Instead one-X Portal for IP Office performs a live search of the external directory source configured for one-X Portal for IP Office usage.

User Settings

User settings for telephony operation are mainly stored by the IP Office system on which that user is configured. Only a small number of settings are stored by the one-X Portal for IP Office server.

Setting	one-X Portal for IP Office	IP Office	Source/Storage
Personal Directory	✓	✓	A user's personal directory is stored in the configuration of both one-X Portal for IP Office and their IP Office. Changes in either are synchronized where possible.
Call Log	–	✓	A user's call log is stored in the configuration of their IP Office.
Voicemail Messages	–	✓	Details of the user's voicemail messages are taken from the voicemail server via the IP Office.
Profiles	✓	–	A user's profiles are stored by the one-X Portal for IP Office server. When a profile is made active, it alters various user settings on the IP Office. If the IP Office configuration settings are altered by another method, the user's profile is changed to 'Detected'.
DND Exceptions	–	✓	A user's Do Not Disturb exception numbers are stored in the configuration of their IP Office.
Keyboard Shortcuts	✓	–	A user's keyboard shortcuts are stored by one-X Portal for IP Office.
Sound Configuration	✓	–	A user's one-X Portal for IP Office sound preference is stored by one-X Portal for IP Office.
Park Slots	✓	–	The park slot numbers used for a user's one-X Portal for IP Office park buttons are stored by one-X Portal for IP Office.

Note that those settings stored by one-X Portal for IP Office are lost if one-X Portal for IP Office is reinstalled rather than upgraded.

1.3 Small Community Network Support

one-X Portal for IP Office is supported within an IP Office Small Community Network (SCN).

- Each IP Office on which one-X Portal for IP Office users are located must meet the requirements for one-X Portal for IP Office. That includes systems to which one-X Portal for IP Office users temporarily hot desk. This means that all systems in the SCN must be the same IP Office software release.
- one-X Portal for IP Office does not provide additional SCN features. It only supports SCN features that are supported by the IP Office systems. For example, the park buttons provided by one-X Portal for IP Office are not supported between different systems in an SCN. This means that one-X Portal for IP Office users can only park and unpark calls on the IP Office on which they are registered.
- one-X Portal for IP Office supports up to 750 simultaneous sessions in a network even if more IP Office users are configured for portal usage. This applies whether using a Windows or Linux based one-X Portal for IP Office server. However, in a IP Office Server Edition Select network up to 3000 simultaneous users are support if using a standalone Linux based one-X Portal for IP Office server on a suitable server.
- Linux based one-X Portal for IP Office servers support the auto-discovery of the IP Office systems in the network from the first system to which they connect. This option is not supported for Windows based one-X Portal for IP Office servers.

1.4 Terminal services support

one-X Portal for IP Office supports terminal services using Citrix and Microsoft Terminal Services clients.

Chapter 2.
Installation (Windows)

2. Installation (Windows)

This section covers the installation of a one-X Portal for IP Office server using default settings. Installers with advanced one-X Portal for IP Office experience can use the custom option.

- **Important**
  Installation of one-X Portal for IP Office is greatly simplified if each IP Office contains at least one user already licensed and configured for one-X Portal for IP Office operation. It is also vital to check the security settings of each IP Office.

Installation Process

The basic installation process consists of the following stages:

1. Check the installation requirements 17
2. Check IP Office Security Settings 21
3. Add one-X Portal for IP Office Licenses 22
4. Configure IP Office Users for one-X Portal for IP Office 23
5. Checking Available Ports 24
6. Install the one-X Portal for IP Office Software 26
7. Initial Server Configuration 28
8. Test User Connection 31

2.1 Installation Requirements

Ensure that the following requirements are met before beginning installation of the one-X Portal for IP Office software on the server PC. Failure to do so will cause the one-X Portal for IP Office server to operate incorrectly.

IP Office Software

- **IP Office Applications DVD**
  The IP Office Applications DVD for IP Office Release 10.0 includes the software for installation of one-X Portal for IP Office. It also includes software for installation of IP Office Manager and the IP Office System Status Application which are required during one-X Portal for IP Office installation.

IP Office System Requirements

- **IP Office System**
  If the system is running pre-IP Office Release 10.0 software, it must be upgraded. For more information on the upgrade process, see one-X Portal for IP Office software upgrade 27.

- **IP Office Small Community Network Support**
  Operation with multiple IP Office's is only supported within a single IP Office Small Community Network (SCN).

- **IP Office Licensing**
  Users licensed and configured with the ***Office User***, ***Teleworker User*** or ***Power User*** profiles can be configured for as one-X Portal for IP Office users. Those licensed and configured for with ***Teleworker User*** or ***Power User*** profiles can also be enabled for one-X Portal for IP Office telecommuter mode.

Server PC Requirements

one-X Portal for IP Office is currently supported with all components installed on a single server. During installation you have to be logged in using an account with full administrator rights.

The following are the server requirements for one-X Portal for IP Office deployments with up to 300 IP Office users. For one-X Portal for IP Office deployments with more than 300 IP Office users, see Configuring one-X Portal for IP Office Server for 300+ IP Office Users 33.

	Up to 300 User	300+ Users
Operating System	• Windows Server 2008 R2 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit)	• Windows Server 2008 R2 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit)
Processor	• Intel Pentium D945 core or AMD Athlon 64 4000+.	• Intel Core 2 Duo CPU E8400 @ 3.00 GHz.
RAM Memory	• 4GB	• 8GB
Hard Disk Space	• 20GB	• 20GB

- **Supported Microsoft Exchange Servers**
  Connection to the following Microsoft Exchange servers is supported for presence integration:
  - Exchange 2007
  - Exchange 2010
  - Exchange 2013

- **TCP/IP Port:**
  The default ports are 8080 and 8666. These can be changed if required during installation of the server software. See Checking Available Ports 24.

- **Firewall Exceptions**
  Exceptions should be added to the server firewall for incoming access on the TCP ports above. If the firewall is also used to control outgoing access, an exception for access to TCP port 50814 on the IP Office IP address should also be added.

Voicemail Server Requirements

The playback of a user's messages through their phone is supported using embedded voicemail or Voicemail Pro.

Voicemail playback through the one-X Portal for IP Office user's browser and personalized greeting recording and control requires a Voicemail Pro voicemail server installed as follows:

- Microsoft IIS should be installed and running before installation of the Voicemail Pro voicemail server software. Set the following IIS options:
  - **Enable Direct Metabase Edit**.
  - **IIS Configuration Compatibility**.
  - SSL should be disabled for the default website.
- The Voicemail Pro voicemail server installation should include the **Web Voicemail Pro (UMS)** component.
- The voicemail server must be in the same subnet as the one-X Portal for IP Office server.
- Check that the IIS on the voicemail server can be browsed by server name from the one-X Portal for IP Office server PC. Enter ***http://<voicemail_server_name>/localstart.asp*** into a browse. If the IIS server does not respond, resolve the DNS routing between the servers before proceeding with the one-X Portal for IP Office installation.

After the Voicemail Pro is installed, you will see Voicemail Pro related virtual directories under **IIS > sites**.

The following 3 directories should be available:

- **NamesGreetings**
- **PersonalGreetings**
- **VoicemailAccounts**

To manually create the aforementioned virtual directories and specify the path:

- **NamesGreetings:** VMPro Installation Dir/VM/Names.
- **PersonalGreetings:** VMPro Installation Dir/VM/Greetings.
- **VoicemailAccounts:** VMPro Installation Dir/VM/Accounts.

If there is an error during the installation of Voicemail Pro, then the three directories will not be available.

1. Ensure that the Voicemail Server is in the same subnet where the Tomcat server is installed.
2. Include the computer name of the system where the Voicemail pro server is installed at the No Proxy Settings/Exception list of the browser in order to listen to the Voicemail or Greeting on the browser.

Information Required

For the server PC:

- **IP Address**.
- **User Account:** A user account with full administrator rights. This account should be used for the software installation.
- **Computer Name:** This name will become part of the URL users use to access one-X Portal for IP Office.

For each IP Office system:

- IP Address.
- Name and password for security settings access.
- Name and password for configuration settings access.
- one-X Portal for IP Office Licenses.
- Users who will be using one-X Portal for IP Office including IP Office user name and password.
- The IP address of the Voicemail Pro voicemail server being used by the IP Office.

LDAP Information

To enabled the External tab in the one-X Portal for IP Office Directory gadget, details of the customer's LDAP server and an search configuration details are required.

- LDAP Server URL.
- User name and password.
- Base DN/Search Base.
- Field names.

one-X Portal for IP Office User Requirements

- **Browser**
  Web browser with LAN access to the one-X Portal for IP Office server. one-X Portal for IP Office is tested using the following web browsers:
    - **Internet Explorer 8.0, 10.0 and 11.0.**
    - **Firefox**
    - **Google Chrome**
    - **Safari 7**
- The browser should be Javascript enabled.
- The **Remember me on this computer** option requires the browser to allow cookies.
- For sounds to be used, for example ringing for a call waiting, or voicemail playback through the computer, a media player such as **Windows Media Player** or **Quick Time** must be installed. When using a browser other than Internet Explorer, Windows Media Player can be supported by the addition of the Firefox Windows Media Play plugin. This plugin is available from http://port25.technet.com/pages/windows-media-player-firefox-plugin-download.aspx. Currently, this plugin is useable with Google Chrome, Mozilla Firefox and Windows Safari.
- The playback of voicemail messages on the user computer requires the user browser to have the IP address of the voicemail server added to the proxy server exceptions.
- **Language**
  one-X Portal for IP Office currently supports:

• **Brazilian**	• **English (US)**	• **Italian**	• **Russian**
• **Chinese**	• **English (UK)**	• **Japanese**	• **Spanish (Latin)**
• **Czech**	• **French**	• **Korean**	• **Swedish**
• **Dutch**	• **German**	• **Polish**	• **Turkish**

- **Phone**
  one-X Portal for IP Office can be used with most phones supported by the telephone system.
    - For analog phone users, the user's **Call Waiting On** and **Off Hook Station** settings should be selected in the user's IP Office configuration.

2.1.1 Exchange Server Requirements

one-X Portal for IP Office supports Exchange server calendar mining feature. one-X Portal for IP Office mines the calendar details of users configured on Microsoft Exchange server and updates the presence status of the users on one-X Portal for IP Office.

- **Supported Microsoft Exchange Servers**
  Connection to the following Microsoft Exchange servers is supported for presence integration:
  - Exchange 2007
  - Exchange 2010
  - Exchange 2013
- **IP Address** of the Microsoft Exchange server.
- **User Account:**
  A user account (*AvayaAdmin*) is created and given rights to mine the details of the users configured on the Exchange server.
- **TCP/IP Port:**
  The default port is 6669. For more details see Checking Available Ports 24.
- **Firewall Exceptions**
  If the Exchange server is hosted by a service provider and it outside the internal network, then port 6669 has to be opened on the router or firewall to allow inbound traffic from the Exchange server to the one-X Portal for IP Office server.

2.2 Check the IP Office Security Settings

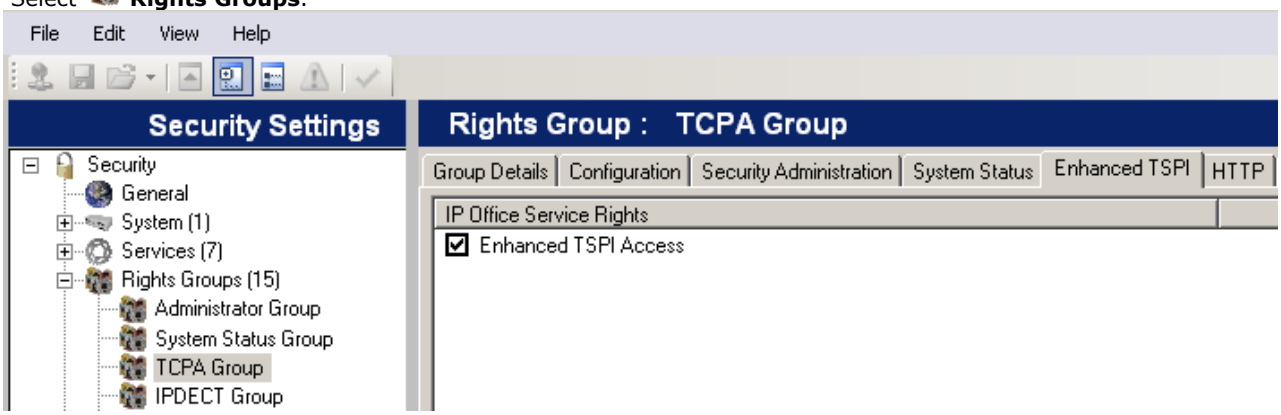
Before attempting to connect an IP Office to a one-X Portal for IP Office server you must check the IP Office security settings. one-X Portal for IP Office uses a specific service and security service user account for the connection. This service is not necessarily present by default.

- **Important: Perform this Process from the one-X Portal for IP Office Server PC**
  The IP Office security settings and other IP Office configuration actions are to be performed using IP Office Manager installed on the server PC. Doing this is also a basic test of the network routing between the server PC and the IP Office system. These can be installed from the IP Office Applications DVD.
- **Important: Security Name and Password**
  This process uses the default security name and password assumed by one-X Portal for IP Office installation for TCPA/TSPI access to an IP Office system. If using the **Advanced** option during one-X Portal for IP Office installation, alternate names and passwords can be used. Only installers with experience of previous one-X Portal for IP Office installations should use the Advanced option.

To check the IP Office Service User Account for one-X Portal for IP Office:

1. Start IP Office Manager and select **File | Advanced | Security Settings**.
2. Select the IP Office system and click **OK**. Enter the user name and password for access to the IP Office's security settings.
3. Select **Services**. The list of services will include an entry for an ***Enhanced TSPI*** service. This is the service used by the one-X Portal for IP Office service to access the IP Office. You need to ensure that the IP Office security configuration includes a **Service User** and **Rights Group** configured to use this service.

4. Select **Rights Groups**.



5. The list of **Rights Groups** should contain a group called ***TCPA Group***. Select this group and then the **Enhanced TSPI** tab. The option for **Enhanced TSPI Access** should be selected as shown above. If this is not the case correct the security settings, creating a new group if necessary.
6. Select **Service Users**. The list of **Service Users** should include a user called ***EnhTcpaService***. In the service user details, this user should be set as a member of the **TCPA Group**. If this is not the case correct the security settings, creating a new user.
   - The user's default password is ***EnhTcpaPwd1***. The password can be changed. However, if changed, the **Advanced** options must be used during the initial server configuration 28 to set the matching password for the CSTA provider connection to the IP Office system.
7. If you have had to make changes to the security settings, click on the icon to save the new security settings.

2.3 Add one-X Portal for IP Office Licenses

Each user for one-X Portal for IP Office must be configured for an ***Office User***, ***Teleworker User*** or ***Power User*** user profile. Each of those user profiles requires appropriate licenses added to the IP Office system configuration. The licenses should be added to the IP Office configuration and validated before the one-X Portal for IP Office is installed.

- **IP Office Licensing**
  Users licensed and configured with the ***Office User***, ***Teleworker User*** or ***Power User*** profiles can be configured for as one-X Portal for IP Office users. Those licensed and configured for with ***Teleworker User*** or ***Power User*** profiles can also be enabled for one-X Portal for IP Office telecommuter mode.

- **Users Exiting Without Logging Out**
  If a user closes their browser rather than logging out, the license they were using remains consumed for up to 6 hours. A user can refresh their browser without being logged out. All data is retrieved from the server again as if they had just logged in again. The user can also navigate to another website and back to one-X Portal for IP Office and remain logged in. If the user presses the **Esc** button, they are prompted whether they wish to log out, if they do not, the browser is refreshed. With some browsers, for example Firefox, a user can close their browser without logging out and when they reopen the browser they are logged straight back in.

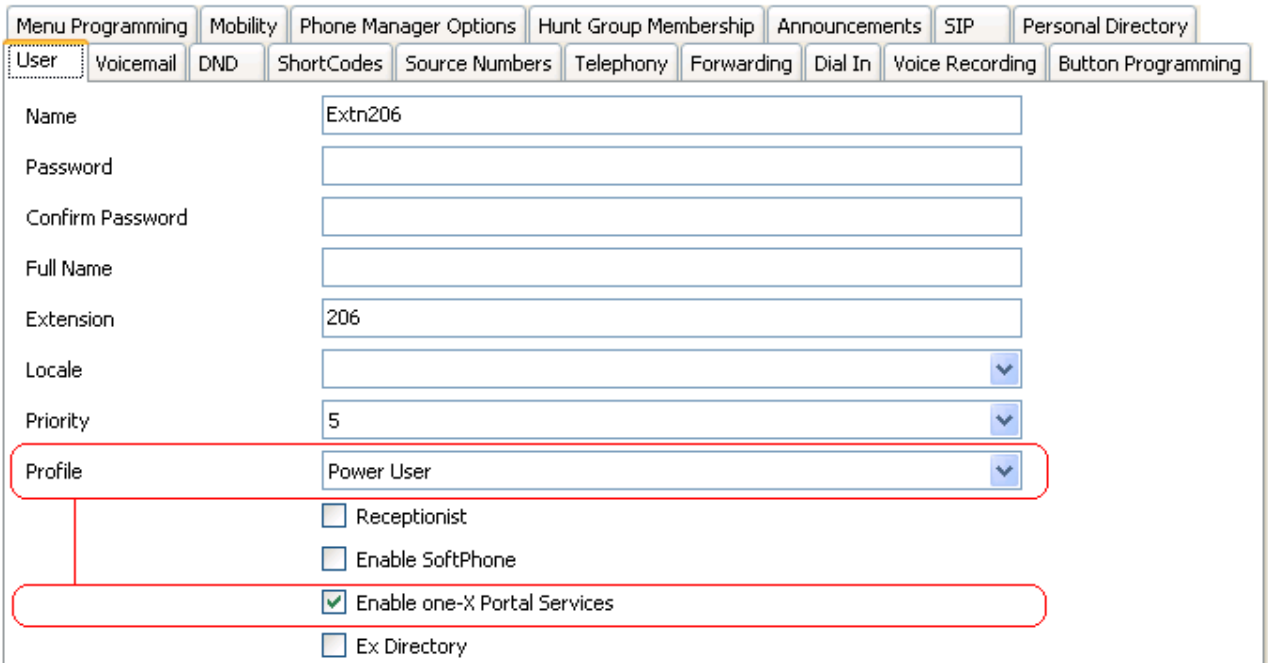
2.4 Configure Users for one-X Portal for IP Office

At least one user on each IP Office system to be supported should be configured as a one-X Portal for IP Office user before the one-X Portal for IP Office server is installed.

- **IP Office Licensing**
  Users licensed and configured with the ***Office User***, ***Teleworker User*** or ***Power User*** profiles can be configured for as one-X Portal for IP Office users. Those licensed and configured for with ***Teleworker User*** or ***Power User*** profiles can also be enabled for one-X Portal for IP Office telecommuter mode.

To configure a user for one-X Portal for IP Office:

1. Start IP Office Manager and click on the icon.
2. Select the IP Office and click **OK**.
3. Enter the user name and password for access to the IP Office's configuration settings.
4. Click on **User**.
5. Select the user who you want to enable for one-X Portal for IP Office operation.
6. Select the **User** tab.



7. Select the **Profile** which you want the user to use and for which the IP Office system has licenses. For one-X Portal for IP Office the supported profiles are ***Office User***, ***Teleworker User*** or ***Power User***. The later two are also able to support the one-X Portal for IP Office Telecommuter features. If you want to grant access to the one-X Portal for IP Office user page, then select the **Enable one-X Portal Services** check box.
8. Note the user **Name** and **Password**. These are used by the user to login to one-X Portal for IP Office.
   - For analog phone users, the user's **Call Waiting On** and **Off Hook Station** settings should be selected in the user's IP Office configuration.
9. Repeat the process for any other users who will be using one-X Portal for IP Office services.
10. Click on to save the updated configuration back to the IP Office system.

2.5 Checking Available Server Ports

The one-X Portal for IP Office application installs as a service (*Avaya one-X Portal*) listening on a port. By default it uses port 8080. The backup and restore service also use port 8666 by default.

It is important to check that these ports are not already in use by other applications. If they are, a different unused port number should be specified during the one-X Portal for IP Office software installation. The only way to change the ports following installation is to remove and then reinstall the software.

Whichever ports are selected, ensure that incoming TCP access to those ports is allowed in the server's firewall exceptions.

The default port configuration on Windows is 8443 and Linux is 9443. Both these ports should be unoccupied.

Ports used by the one-X Portal for IP Office

In addition to the ports used to access the one-X Portal for IP Office server from a browser client, various components of the one-X Portal for IP Office also use ports to communicate. The full set of ports used by one-X Portal for IP Office are listed below:

- **4560** - This port is used by log4j socket appender.
- **5222** - This port is used for XMPP client/server communication.
- **5269** - This port is used for XMPP server to server federation. This port federates with the external XMPP enabled servers. If the customer is not intending to federate with external XMPP servers then this port does not need to be opened on the firewall.
- **6669** - Inbound traffic from the Microsoft Exchange server to the portal for calendar notifications.
- **8005** - This port is used by the Tomcat shutdown listener.
- **8443** - This port is used for HTTPS access on Windows installation of one-X Portal for IP Office. Note: This port is used by Avaya Communicator and one-X Mobile.
- **8444** - This port is used for initial communication between the mobility client (Android/iPhone) and the one-X Portal for IP Office. If customer is **NOT** using the mobility client or is only using it on the internal WiFi network, then this port does not need to be opened on the firewall.
- **8063** - This port is used for web socket based delivery. Open this port on the machine that runs **one-X Portal for IP Office**. This port is also used by Avaya Communicator, Microsoft Outlook plugin and Call assistant plug-in for HTTPS access to the **one-X Portal for IP Office** server.
- **8666** - This port is used by the JVMX component of the one-X Portal for IP Office. This port number can be changed during installation.
- **8069** - This port is used for web socket based delivery. Open this port on the machine that runs **one-X Portal for IP Office**. This port is used by Avaya Communicator for Windows, Microsoft Outlook plugin and Call assistant plug-in for HTTP access to the **one-X Portal for IP Office** server.
- **8080** - Default HTTP browser access port. This port number can be changed during installation.
- **8082** - The database component of the one-X Portal for IP Office uses this port.
- **8086** - This port is used for HTTPS access to mybuddy.
- **9092** - This port is used by the Database client listener.
- **9094** - This port is used for OpenFire XML RPC (Remote Procedure Call) and administration console.
- **9095** – This port is used by the OpenFire admin console (https).
- **9443** - This port is used for HTTPS access on Linux installation of one-X Portal for IP Office. Note: This port is used by Avaya Communicator and one-X Mobile.

Note:

- Ports **5222**, **5269** and **8444** need to be opened on the customer's firewall or router, if the mobility client is to be used on a cellular network or if external XMPP access is required.
- Ports **8086**, **9094** and **9095** need not be opened on the customer's firewall or router.

Listing Ports Already in Use

To check which ports are already in use on the server, the command **netstat -an > ports.txt** can be used. This will create a text file ***ports.txt*** listing all the ports on which the server is currently listening. Check that none of the ports required by one-X Portal for IP Office are already in use. If they are, there will be a conflict between the application already using the port and one-X Portal for IP Office when one-X Portal for IP Office is installed.

Reserved Ports

There are a number of ports used by other Avaya IP Office applications. If any of these are specified during installation, the installer will ignore the selection and default to installing on port 8080. Examples of reserved ports are:

- **8888** - Default port used by ContactStore for IP Office.
- **8089** - Default port used by IP Office Conferencing Center application.

Other Commonly Used Ports

Ports in the 8000 range are also frequently used by other applications.

- **8081** - Default port used by IIS for SharePoint Administration access.

2.6 Install the one-X Portal for IP Office Software

Prerequisite:

- Do not start software installation until the previous installation steps (IP Office security settings 21, one-X Portal for IP Office licenses 22, user configuration 23) have been completed.
- Ensure that you have logged in to the server using an account with full administrator rights. Alternatively right click the one-x install package and select *Run as administrator* option.
- To install on a Windows server, ensure that you disable the User Account Control (UAC) in the User Accounts section of the Windows Control Panel before beginning the installation, then restart the server. If you login as an user with administrator rights and do not disable the UAC you cannot complete the installation successfully.
- During installation if the system displays the following error :*Error 1330 - Invalid Digital Signature,* install Microsoft updates on Windows 2008/2012 server.

To install the server software:

1. In the IP Office Application DVD, right-click **setup.exe** and select *Run as Administrator* to start the server software installation process. The system displays **Avaya IP office one-X Portal InstallShield Wizard**.
   - If you have a previous version of the one-X Portal for IP Office installed, you need to upgrade it to the new version. For more information on the upgrade process, see one-X Portal for IP Office software upgrade 27.
2. Choose the language that you want to use during the installation.
3. Click **OK**. The system displays **Preparing to Install** screen. If you do not want the system to proceed with the installation process, click **Cancel**. The system displays **Welcome to the InstallShield Wizard for Avaya one-X Portal for IP Office**.
4. Click **Next**. The system displays **License Agreement**.
5. Select **I accept the license terms in the agreement**, you agree with the terms. To print the license terms in the agreement, click **Print**.
6. Click **Next**. If the system has more than 8 GB of RAM, you are prompted to select one of the following:
   - **Configure for up to 750 IP Office users (uses 7 GB of system RAM)**
     This option requires additional server configuration. See Configuring one-X Portal for IP Office Server for 300+ IP Office Users 33 .
   - **Configure for up to 300 IP Office users (uses 4 GB of system RAM)**
8. Click **Install**.
9. Do one of the following:
   - To review or change the installation settings, click **Back**.
   - To exist the installation wizard, click **Cancel**.
   - To proceed with the installation, click **Install**.
   - The system displays **Application Information** window, that contains the default HTTP Port, JMX Port, and the backup location on the server. You can set the HTTP Port, JMX Port and the Backup location on the server. For information about the ports, see Checking Available Ports 24. After one-X Portal for IP Office is installed, you can change the port number only by removing and then reinstalling the one-X Portal for IP Office software.
10. Click **Next**. The system displays **InstallShield Wizard Completed**.
11. Select one of the following options:
    - Start Avaya one-X Portal for IP Office service. If you do not select this option, you need to start theone-X Portal for IP Office service manually before it can be configured.
    - Show the readme file
    - Show the Windows Installer log
12. Click **Finish**. Proceed to Initial Server Configuration 28.

2.6.1 one-X Portal for IP Office software upgrade

You can upgrade a previous version of **one-X Portal for IP Office** to a new version.

- You will have to add the **XMPP domain name** and restart the services while upgrading from **one-X Portal for IP Office** 5.0 and 6.0 to 10.0**.**
- Ensure that you have logged in to the server using an account with full administrator rights. Alternatively, right click the one-x install package and select *Run as administrator* option.
- To install on a Windows 2008/2012 server, ensure that you disable the User Account Control (UAC) in the User Accounts section of the Windows Control Panel before beginning the installation, then restart the server. If you login as an user with administrator rights and do not disable the UAC you cannot complete the installation successfully.

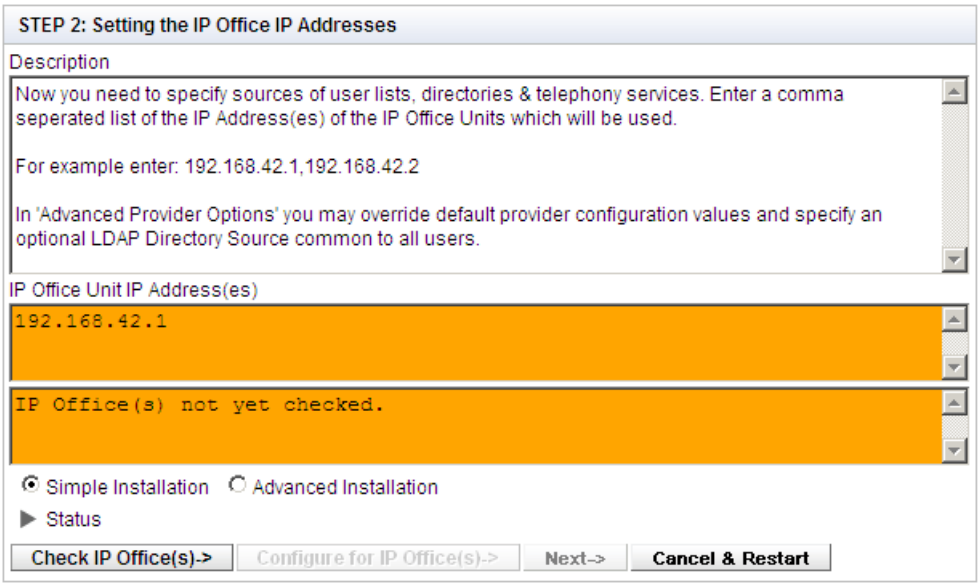
To upgrade:

1. In the IP Office Application DVD, right-click **setup.exe** and select *Run as Administrator* to start the server software installation process. The system displays **Avaya IP office one-X Portal InstallShield Wizard**.
2. Choose the language that you want to use during the installation.
3. Click **OK**.
4. The system displays **Preparing to Install** screen. If you do not want the system to proceed with the installation process, click **Cancel**.
5. The system displays **Welcome to the InstallShield Wizard for Avaya one-X Portal for IP Office**.The system also displays the current version of **one-X Portal for IP Office** that is installed on the system and prompts you to proceed with the upgrade.
6. Click **Next**. The system displays **License Agreement**.
7. Select **I accept the license terms in the agreement**, you agree with the terms. To print the license terms in the agreement, click **Print**.
8. Click **Next**. If the system has more than 8 GB of RAM, you are prompted to select one of the following:
   - **Configure for up to 750 IP Office users (uses 7 GB of system RAM)**
     This option requires additional server configuration. See Configuring one-X Portal for IP Office Server for 300+ IP Office Users 33.
   - **Configure for up to 300 IP Office users (uses 4 GB of system RAM)**
9. Click **Install**. Do one of the following:
   - To review or change the installation settings, click **Back**.
   - To exist the installation wizard, click **Cancel**.
   - To proceed with the installation, click **Install**.
10. The system displays **Application Information** window, that contains the default HTTP Port, JMX Port, and the backup location on the server. You can set the HTTP Port, JMX Port and the Backup location on the server. For information about the ports, see Checking Available Ports 24. After one-X Portal for IP Office is installed, you can change the port number can only after removing and then reinstalling the one-X Portal for IP Office software.
11. Click **Next**. The system displays **InstallShield Wizard Completed**. Select one of the following options.
    - Start Avaya one-X Portal for IP Office service. If you do not select this option, you need to start theone-X Portal for IP Office service manually before it can be configured.
    - Show the readme file
    - Show the Windows Installer log
12. Click **Finish**.

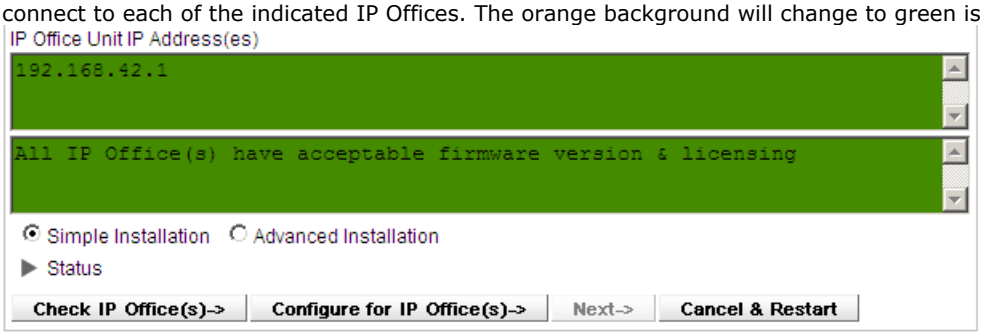
2.7 Initial Server Configuration

At this stage, the one-X Portal for IP Office server software has been installed 26 and the service started. However the one-X Portal for IP Office server still requires initial configuration. During this configuration it will connect to the IP Office systems.

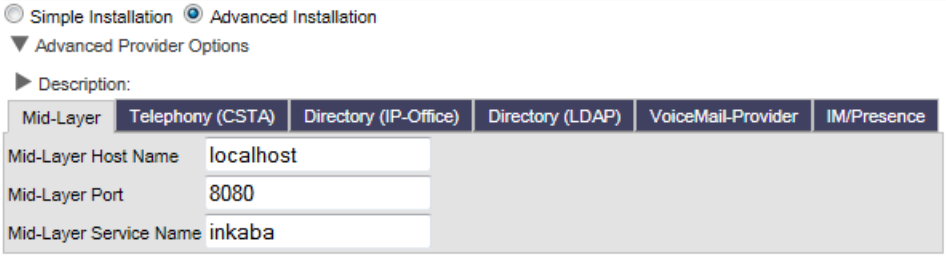
1. If you did not select **Start the Avaya one-X Portal Service** during the software installation, start the service manually.
2. On the one-X Portal for IP Office server, open a web browser and enter ***http://127.0.0.1:8443/onexportal-admin.html***.
   - If the service has only just been started, you have to wait a while whilst the services are started. This can take up to 15 minutes before one-X Portal for IP Office responds. One way to monitor progress is to use Windows Task Manager. Typically as one-X Portal for IP Office is starting, the **PF Usage** will gradually increase. Once is reaches approximately 2.3GB, one-X Portal for IP Office has started.
   - The message ***System is currently unavailable - please wait*** is displayed while the one-X Portal for IP Office application is still starting. When the message disappears approximately 15 minutes after the one-X Portal for IP Office service was started.
3. When the login menu is displayed, check that the version reported matches the version expected.
4. Enter the default administrator name (***Administrator***) and password (***Administrator***) and click **Login**.
5. The **License Agreement** page is displayed. When you have read the license, select **Have Read & Agree** and then click on **Next**.
6. The menu now allows entry of the IP addresses of the IP Office systems to which you want the one-X Portal for IP Office server to connect.



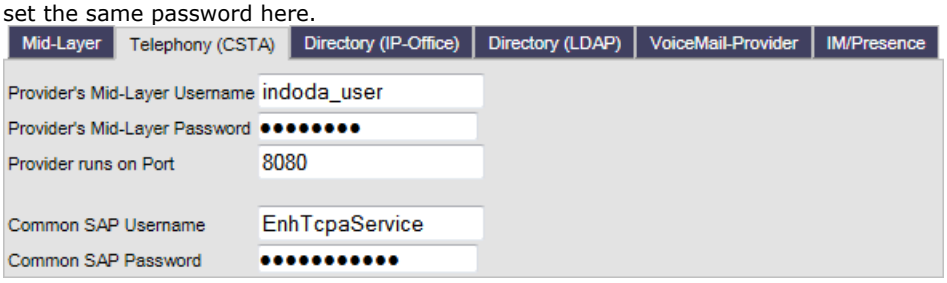
   - In the following menus, the ▶ **Status** icon can be used to show/hide status messages about the actions being performed by the installation process.
   - You can enter the addresses of multiple IP Office systems in your Small Community Network. For IP Office Release 9.1, you can enter just one address. The one-X Portal for IP Office is informed by the first system about the others in your network. This however takes a while to occur after initial installation and assumes that the security settings of all the systems are the same.
7. Enter the addresses in the form and select **Check IP Office(s)**. The one-X Portal for IP Office server will attempt to connect to each of the indicated IP Offices. The orange background will change to green is this is successful.



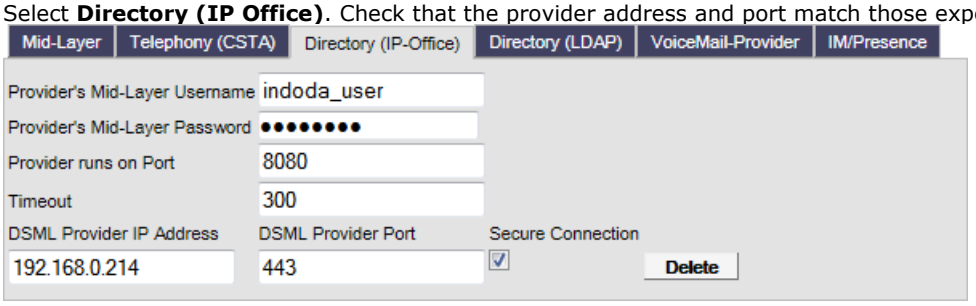
8. Click on **Advanced Installation**. and expand the **Advanced Provider Options** section.



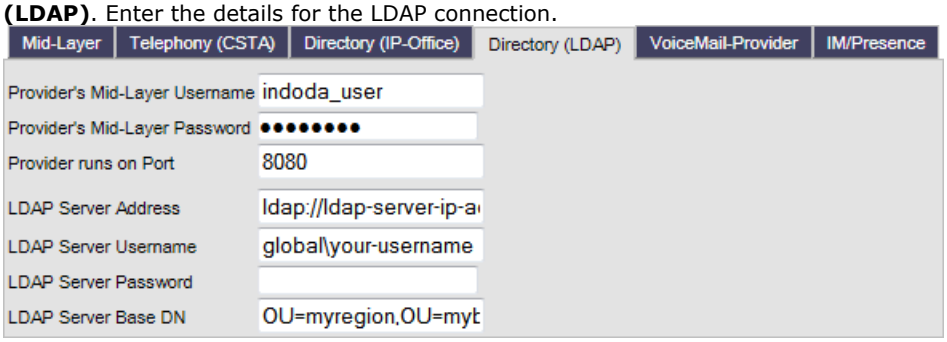
a. Select **Telephony (CSTA)**. If you changed the password used for the IP Office system's ***EnhTcpaService*** user, set the same password here.



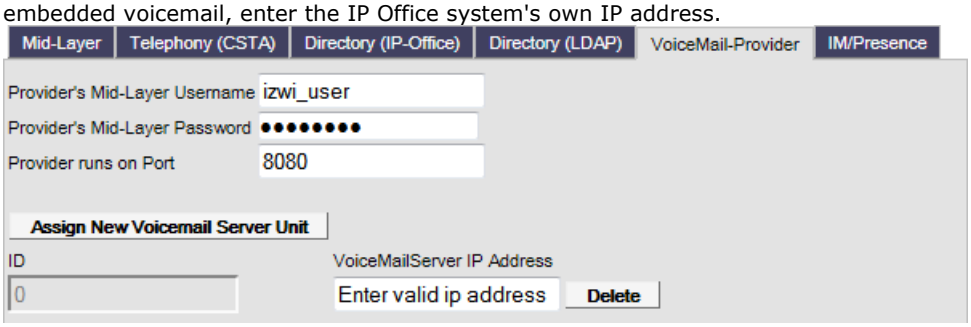
b. Select **Directory (IP Office)**. Check that the provider address and port match those expected.



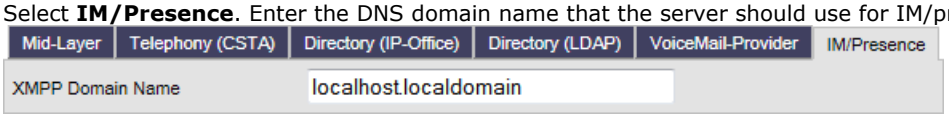
c. If the customer has an LDAP directory source that they want used for the external directory, select **Directory (LDAP)**. Enter the details for the LDAP connection.



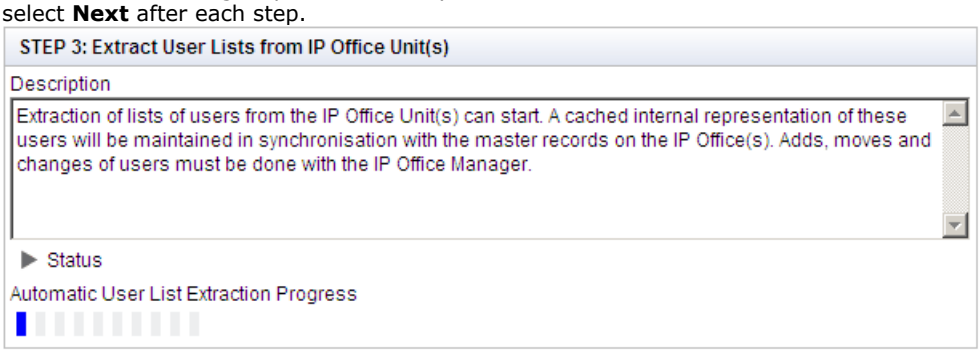
d. Select **VoiceMail-Provider**. Enter the IP address of the voicemail server. For a Small Community Network, enter the address of the centralized voicemail server (not that of the backup or any distributed voicemail servers). For embedded voicemail, enter the IP Office system's own IP address.



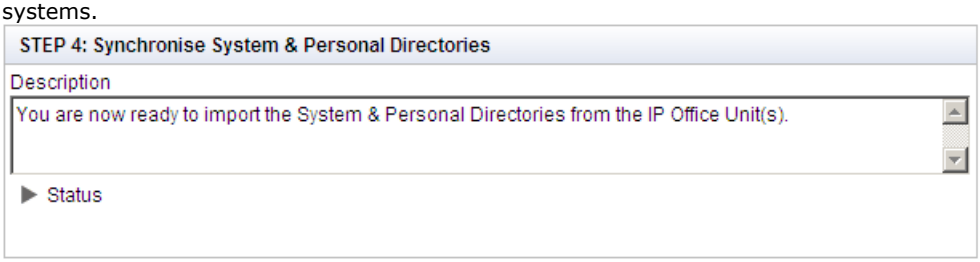
e. Select **IM/Presence**. Enter the DNS domain name that the server should use for IM/presence service.



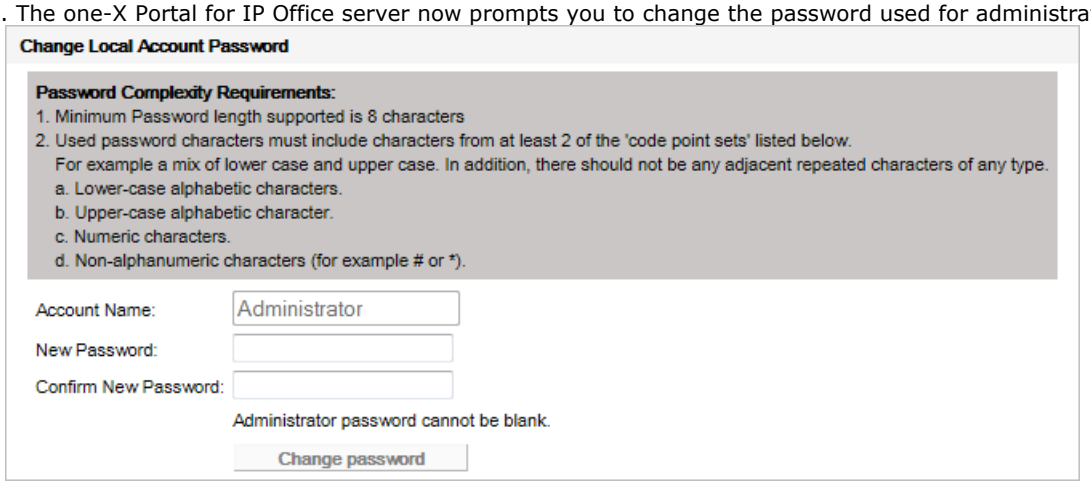
9. Click on **Configure for IP Office(s)**. The one-X Portal for IP Office server will connect with each IP Office and automatically extract details of the IP Office users. If **Simple Installation** was selected, the installer will go through this and the following steps automatically. If **Advanced Installation** was selected, the installer will require you to select **Next** after each step.



10. Having extracted user details, the one-X Portal for IP Office server extracts directory details from the IP Office systems.



11. The one-X Portal for IP Office server now prompts you to change the password used for administrator access.



12. Enter a new password and click **Change Password**. The initial configuration is complete. Note that it will still be at least another 5 minutes before the one-X Portal for IP Office is usable by end users.

2.8 Test User Connnection

From a user PC rather than the server PC, check that a user can login to one-X Portal for IP Office and use it to make and answer calls.

To login as a user:

1. From a user PC, use a web browser to browse to the one-X Portal for IP Office server. Type ***https://<server_address>:8443/onexportal.html***.
2. Enter the user's name and password.
3. Click **Login**.
4. Check that the user can see the system directories and, if configured, search the external directory.
5. Check that the user can see and edit their personal directory.
6. Make a call to the user's extension. The call should be shown within the **Calls** gadget. Answer the call using the **Calls** gadget.
7. Check that the answered call appears in the **Call Log** gadget.
8. Make a call using the **Calls Gadget**.
9. If the system includes a voicemail server, check that the **Messages** gadget shows messages in the user's mailbox.
10. Select **Logout**.

2.9 Adding Certificates

Secure connection to the server for instant messaging and presence may require the server to include certificate. For example this is a requirement for one-X Communicator to use TLS.

For Linux based one-X Portal for IP Office, the portal shares the certificates added to the server's web management menus. However, for Windows based portal servers, the certificate needs to be added through the one-X Portal for IP Office administrator menus.

To add a certificate:

1. Login to the one-X Portal for IP Office administrator menus.
2. Click **Configuration** and select **Certificate**.
3. Click **Import** and select the certificate to upload to the server.

2.10 Configuration for 300+ IP Office Users

If you deploy one-X Portal for IP Office for more than 300 simultaneous active users, you not only need additional resources for the server computer but also need to modify some configuration settings on the server computer. Before you begin the installation review Installation Requirements 17.

- **Note:** After each time you upgrade one-X Portal for IP Office to a newer version, you must follow step 3 33 above to configure the server computer.

System Requirements

The following are the Windows server requirements for the deployment of one-X Portal for IP Office with more than 300 IP Office users:

	Up to 300 User	300+ Users
Operating System	• Windows Server 2008 R2 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit)	• Windows Server 2008 R2 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit)
Processor	• Intel Pentium D945 core or AMD Athlon 64 4000+.	• Intel Core 2 Duo CPU E8400 @ 3.00 GHz.
RAM Memory	• 4GB	• 8GB
Hard Disk Space	• 20GB	• 20GB

To configure a Windows server to support 300+ users

1. Do the following:

   - If your system is not running one-X Portal for IP Office 10.0 already, install 26 or upgrade 27 to one-X Portal for IP Office 10.0.
   - If your system is already running one-X Portal for IP Office 10.0, stop the one-X Portal service:

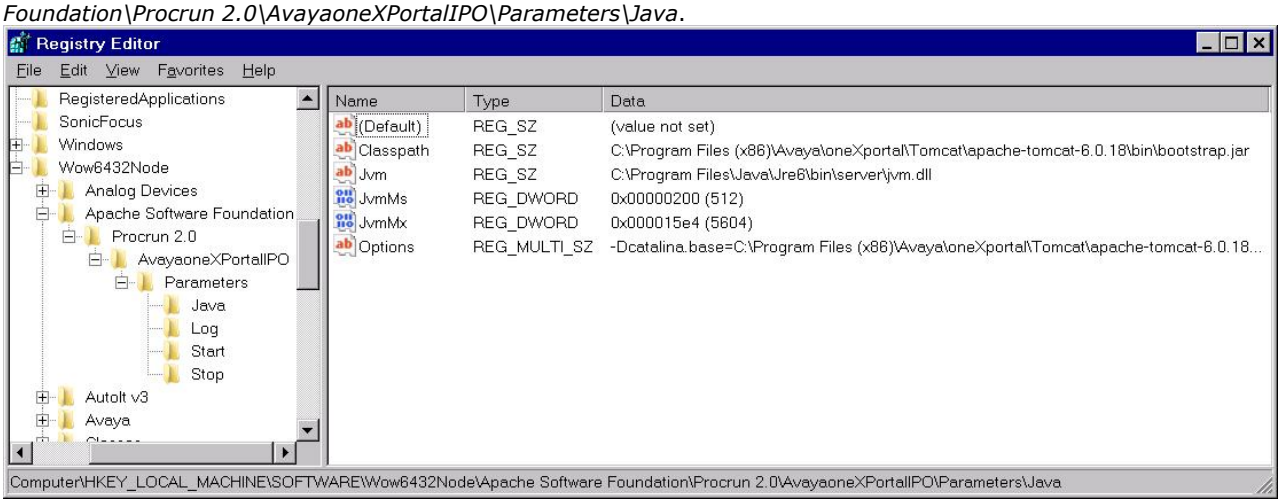
     a. Click **Start > Run**, type *services.msc* in the **Open** field, and click **OK**.

     b. In the **Services** window, right-click one-X Portal for IP Office in the list of services, and click **Stop** on the pop-up menu

2. Proceed as follows to modify the Windows registry:

   a. Click **Start > Run**, type *regedit* in the **Open** box, and click **OK**.

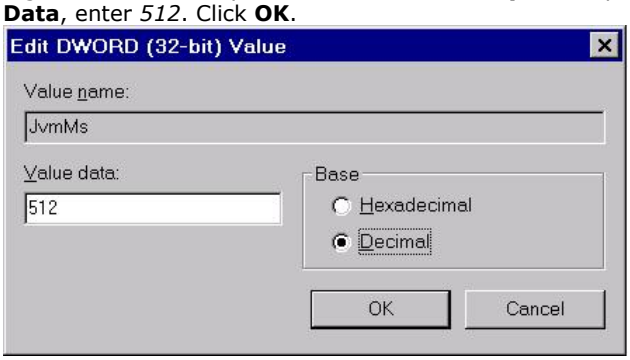
   b. Locate and select the registry key *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\AvayaoneXPortalIPO\Parameters\Java*.



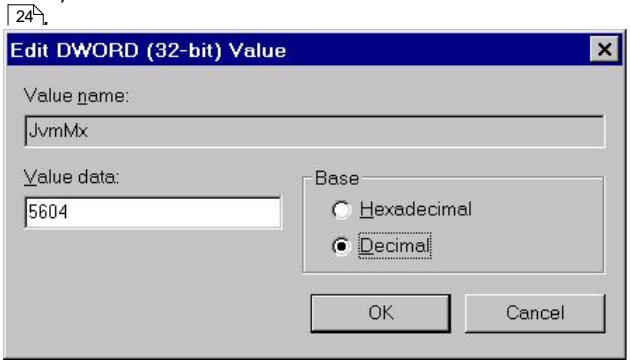
   c. Click **File**, and then click **Export**.
   This step backs up the key before you make any changes. You can import this file back into the registry later if your changes cause a problem.

   d. Right-click the subkey ***Jvm*** and click **Modify** on the pop-up menu. In the **Value Data** field enter ***<JRE Installation Path>\bin\server\jvm.dll***. where *<JRE Installation Path>* is the JRE installation path. Ensure that you specify the JRE installation path where the x64 bit java was installed; the default path is *C:\Program Files\Java* , not *C:\Program Files (x86)\Java*. If you do not specify the correct path the system will not be able to start the service.

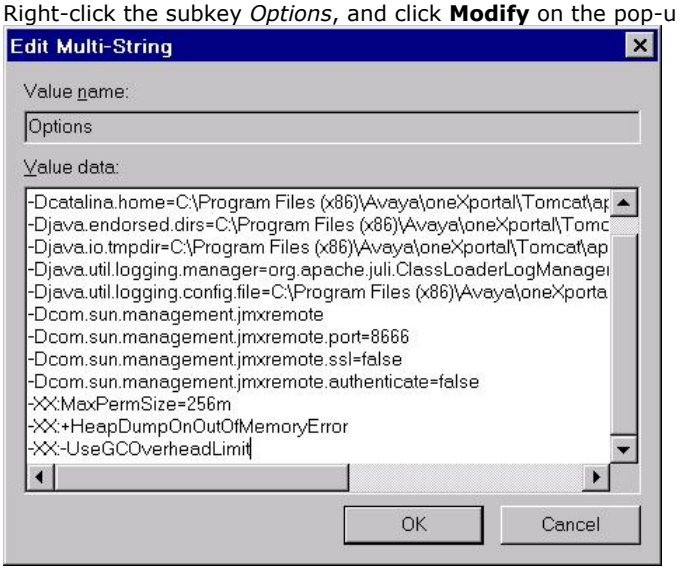
e. Right-click the subkey ***JvmMs*** and click **Modify** on the pop-up menu. Under **Base**, select **Decimal**. In **Value Data**, enter *512*. Click **OK**.



f. Right-click the subkey ***JvmMx*** and click **Modify** on the pop-up menu. Under **Base**, select **Decimal**. In **Value Data**, enter *5604*. Click **OK**. For more information about the available ports see, *Checking Available Server Ports* 24



g. Right-click the subkey *Options*, and click **Modify** on the pop-up menu. Add the following parameters:



- *-XX:MaxPermSize=256m*
- *-XX:+HeapDumpOnOutOfMemoryError*
- *-XX:-UseGCOverheadLimit*

h. Click **OK.**

i. Press **F5,** and close the **Registry Editor** window.

3. Proceed as follows to start the one-X Portal service:

a. Click **Start > Run**, type *services.msc* in the **Open** field, and click **OK**.

b. In the **Services** window, right-click one-X Portal for IP Office in the list of services, and click **Start** on the pop-up menu.

Chapter 3.

Configuring Microsoft Exchange Server Integration

3. Configuring Microsoft Exchange Server Integration

The one-X Portal for IP Office can connect to an Exchange server to provide presence integration based on a user's calendar meetings and appointments.

Exchange Server Requirements

one-X Portal for IP Office supports Exchange server calendar mining feature. one-X Portal for IP Office mines the calendar details of users configured on Microsoft Exchange server and updates the presence status of the users on one-X Portal for IP Office.

- **Supported Microsoft Exchange Servers**
  Connection to the following Microsoft Exchange servers is supported for presence integration:
  - Exchange 2007
  - Exchange 2010
  - Exchange 2013
- **IP Address** of the Microsoft Exchange server.
- **User Account:**
  A user account (*AvayaAdmin*) is created and given rights to mine the details of the users configured on the Exchange server.
- **TCP/IP Port:**
  The default port is 6669. For more details see Checking Available Ports 24 .
- **Firewall Exceptions**
  If the Exchange server is hosted by a service provider and it outside the internal network, then port 6669 has to be opened on the router or firewall to allow inbound traffic from the Exchange server to the one-X Portal for IP Office server.

Process Summary

You must perform the following steps to enable the one-X Portal for IP Office to update the users' presence based on Microsoft Exchange Server 2007 or 2010 calendar meetings or appointments.

1. Install and enable Digest Authentication 37
2. Create an AvayaAdmin user account 38
3. Configure the AvayaAdmin user account 38
4. Set impersonation rights for AvayaAdmin 38

3.1 Install and Enable Digest Authentication

IIS Digest authentication needs to be installed and enabled on the server running Microsoft Exchange. To use Digest authentication on IIS 7 and later, you must install the service role and then for the EWS web site disable Anonymous authentication and enable Digest authentication. For full details of the installation process refer to http://www.iis.net/configreference/system.webserver/security/authentication/digestauthentication.

- **Warning: Interaction with OCS**
  IP Office integration with Microsoft Exchange for Calendar mining cannot be configured and used if Microsoft Office Communication Server (OCS) and Office Communicator are already deployed. If this is the case, enabling digest authentication can stop the Microsoft OCS from working. There is a continual prompting for authentication in the Office Communicator and an error message is generated.

To install the Digest authentication role service:

a. Windows Server 2008 or Windows Server 2008 R2

1. Click **Start** and select **Administrative Tools** and then **Server Manager**.
2. In the **Server Manager** hierarchy pane, expand **Roles** and click **Web Server (IIS)**.
3. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then click **Add Role Services**.
4. On the **Select Role Services** page, select **Digest Authentication** and then click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Results** page, click **Close**.
7. You can now enable digest authentication, see below.

b. Windows Server 2012 or Windows Server 2012 R2

1. On the taskbar, click **Server Manager**.
2. In **Server Manager**, click the **Manage** menu, and then click **Add Roles and Features**.
3. In the **Add Roles and Features** wizard, click **Next**. Select the installation type and click **Next**. Select the destination server and click **Next**.
4. On the **Server Roles** page, expand **Web Server (IIS) | Web Server | Security** and select **Digest Authentication**. Click **Next**.
5. On the **Select features** page, click **Next**.
6. On the **Confirm installation selections** page, click **Install**.
7. On the **Results** page, click **Close**.
8. You can now enable digest authentication, see below.

To enable Digest authentication:

1. Open **Internet Information Services (IIS) Manager**:
   - **Windows Server 2012 or Windows Server 2012 R2:**
     On the taskbar, click **Server Manager**. Click **Tools** and then click **Internet Information Services (IIS) Manager**.
   - **Windows Server 2008 or Windows Server 2008 R2:**
     On the taskbar, click **Start**. Select **Administrative Tools** and then click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name, expand **Sites**.
3. Click **EWS**.
4. Scroll to the **Security** section in the **Home** pane, and then double-click **Authentication**.
5. In the **Authentication** pane, select **Anonymous Authentication** and click **Disable**.
6. In the **Authentication** pane, select **Digest Authentication**, and click **Enable**.
7. Now proceed to creating the AvayaAdmin user account 38.

3.2 Create the AvayaAdmin User Account

Ensure that the user name of the new account that you create is **AvayaAdmin**. The batch file that automatically sets the rights to mine to the calendar details of the users configured on the Microsoft Exchange server only works for that user name.

To create AvayaAdmin user account on the Exchange server:

1. In the Microsoft Exchange server window, right click **Mailbox**.
2. Select **New Mailbox**.
3. Choose **User Mailbox** as the mailbox type. Click **Next**.
4. Select **New User** as the **User Type**.
5. Type the User Information such as **First name**, **Lastname**, **User Log on name (User Principal Name)**, and **Password**. Click **Next**.
6. Set the **Mailbox Settings** and type the alias details for the mailbox user. Click **Next**.
7. Click **New**, the system displays the configuration summary of the mailbox. Click **Next**.
8. Click **Finish**, the system creates the **AvayaAdmin** user account.

3.3 Configure the AvayaAdmin User Account

You must configure the **AvayaAdmin** user account such that its password never expires and a password change is not required upon next login.

To configure the AvayaAdmin user account:

1. After creating the **AvayaAdmin Mailbox**, launch the **Active Directory Users and Computers** application.
2. Click **Users**.
3. Double-click on the ***AvayaAdmin*** user.
4. Select the **Account** tab.
5. Check the **Password never expires** checkbox.
6. Uncheck the **User must change password at next login** checkbox.
7. Click **OK**.

3.4 Set Impersonations Rights for AvayaAdmin

A powershell script is used to configure the necessary impersonation rights for the **AvayaAdmin** user to mine the calendar details of the other users configured on the Microsoft Exchange Server. This script is provided with the one-X Portal for IP Office.

To download the powershell script:

1. Log in to the one-X Portal for IP Office administrator menus.
2. Click **Configuration** and select **Exchange Service**.
3. Right-click the **Download Powershell script** link.
4. Select **Save link as** and save the script file to a location under the primary drive *C:* . The script cannot be run from other locations such as the desktop.

To set the impersonations rights for AvayaAdmin:

1. In the Exchange Server, go to **Start > Run**.
2. Type ***powershell -noexit <drive>\avaya.ps1***, where *<drive>* is the main drive where you saved the *AvayaAdmin.ps1* batch file.
   - After the batch file is executed successfully the system displays: *Permissions for mailbox AvayaAdmin updated successfully.*
   - If you have not created the AvayaAdmin user account 38 on the Microsoft Exchanger Server, the system displays: *Create mailbox AvayaAdmin and run this script again*.

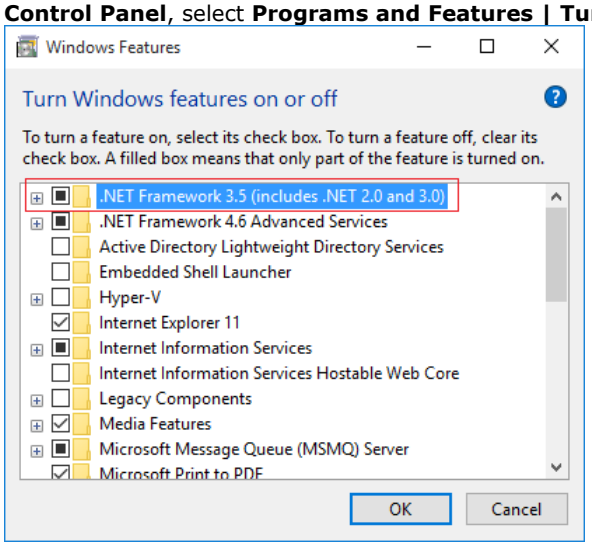
Chapter 4.

Desktop Client Group Policy Installation

4. Desktop Client Group Policy Installation

You can install Avaya IP Office Desktop Clients through group policy. This tutorial describes how to deploy a MSI on multiple machines using a group policy.

- **Prerequisite:**
  Ensure that the following are present on all the remote PCs:
  - **.NET Framework 4.5.2**
    The install package for this can be downloaded from the **Configure | Desktop Integration** page within one-X Portal for IP Office.
  - **.NET Framework 3.5**
    Support for .NET Framework 3.5 must also be enabled within the Windows Features on the user PC (from the **Control Panel**, select **Programs and Features | Turn Windows features on or off**).



  - **Microsoft Office 2007 PIA**
  - **Microsoft VSTO 2010 Runtime v4.0 (10.0.40303 or later)**
- **Note:**
  GPO installation of the Avaya IP Office Outlook Plug-in is not supported for Outlook 2007.

Deployment Methods

Group policy supports two methods of deploying an MSI package:

- **Assign software**
  A program can be assigned per-user or per-machine. If it is assigned per-user, the program is installed when the user logs on. If it is assigned per-machine, the program is installed for all users when that machine starts.
- **Publish software**
  A published program is added to the **Add or Remove Programs** list and the user is able to install it from there.

Deployment Summary

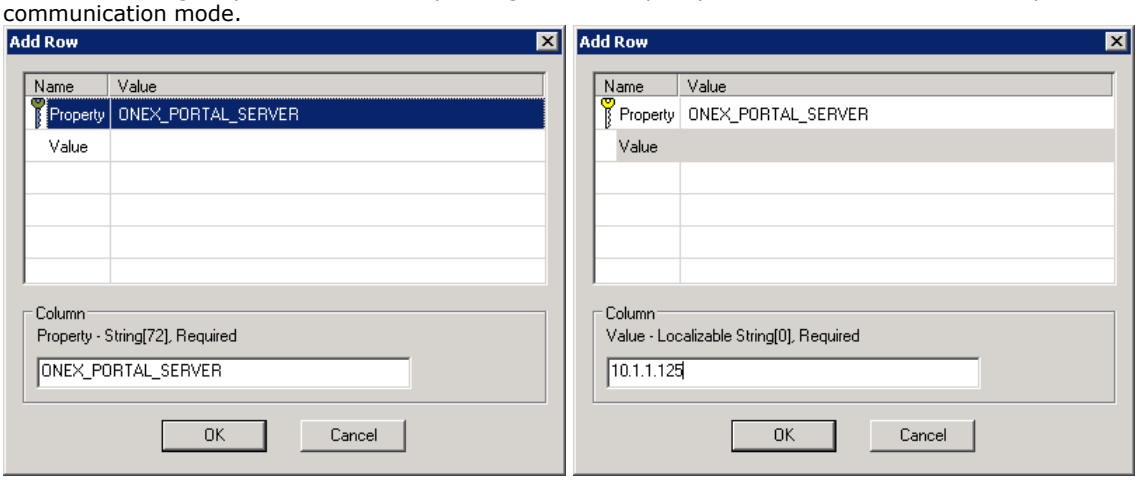
1. Create a Distribution Point 41
2. Create a Group Policy Object 42
3. Assign an MSI Package 43
4. Publish an MSI Package 44
5. Redeploy an MSI Package 45
6. Remove an MSI Package 46
7. Silent Installation 46

4.1 Creating a Distribution Point

The first step in deploying an MSI is to create a distribution point on the publishing server.

To create a distribution point:

1. Log on to the server as an Administrator.
2. Create a shared network folder to contain the MSI package.
3. Set the permissions on this folder allow remote access to the distribution package
4. In the shared folder, perform an administrative install of the desktop client executable. The command line for an administrative installation is ***AvayaOneXDesktopClients.exe /a***
5. Download the open source ORCA tool from: http://www.softpedia.com/progDownload/Orca-Download-79861.html. This creates an MSI package.
6. After downloading and installing ORCA, right-click on the MSI file and select **Edit with Orca**.
7. From the left-hand **Table** item select **Property Table**.
8. From the list of tables select **Property**. Scroll to the bottom of the table, right-click and select **Add Row**.
9. Add the following Properties with corresponding values to specify one-X Portal server address, port and secure communication mode.



- ONEX_PORTAL_SERVER = <Server IP address or fully qualified domain name>
- PORT_NUMBER = <Server port number>
- SECUREMODE = <1 for enabled or 0 for disabled>

10. After adding all the properties, save the MSI file and close the ORCA tool.

4.2 Creating a Group Policy Object

An MSI package is deployed (distributed) using a Group Policy Object.

To create a Group Policy Object (Windows Server 2003):

1. Click on the **Start** button.
2. Go to **Programs**.
3. Select **Administrative Tools** and then select **Active Directory Users and Computers**.
4. Right-click your domain name in the console tree and select the **Properties**.
5. Select the **Group Policy** tab.
6. Click **New**.
7. Set the name of the policy (for example ***MyApplication***).
8. Click **Properties** and select the **Security** tab.
9. Check the **Apply Group Policy** checkbox only for the groups to which the policy should be applied.
10. Click on the **OK** button.

To create a Group Policy Object (Windows Server 2008 or later):

1. Create a **Container** or **Organizational Unit**.
2. Open the **Active Directory Users and Computers** window.
3. In the console tree, right-click your domain, and then select **New**.
4. Select **Organizational Unit**.
5. Provide a name for the container and uncheck the checkbox **Protect container from accidental deletion** so as to be able to delete this container later. If checkbox is marked, it is not possible to delete this container.
6. In the same **Active Directory Users and Computers** window, add to the Container the users and machines for which the policy needs to be applied. New domain users and computers can be created in this container.
   - Alternatively you can move the users from the **USERS** account to the container and machine accounts from **COMPUTERS** account to the container. Moving the users or machines prompts a warning.
7. Click on the **Start** button.
8. Go to **Programs**.
9. Select **Administrative Tools** and then select **Group Policy Management**.
10. Expand the tree for your domain and select the newly created container or organizational unit.
11. Right-click and select **Create a GPO in this domain, and Link it here...**.
12. Provide a name for the GPO and click the **OK** button to close the window. The GPO is added to the container and also to the Group Policy Objects list.
13. Right-click the GPO in the container and select **Edit** to open the **Group Policy Management Editor**. Select how you want the policy installed. If you assign the application to a user, it is installed when the user logs on to the computer. If you assign the application to a computer, it is installed when the computer starts.

4.3 Assigning an MSI Package

A package can be assigned per-user or per-machine. Assigned packages are automatically silently installed.

To assign a package (Windows Server 2003):

1. Click on the **Start** button.
2. Go to **Programs**.
3. Select **Administrative Tools** and then select **Active Directory Users and Computers**.
4. Right-click your domain name in the console tree and select the **Properties**.
5. Select the **Group Policy** tab.
6. Select the object you want and click **Edit**.
7. Expand **Software Settings** under **Computer Configuration**.
8. Right-click **Software Installation**, select **New** and then click **Package**.
9. In the **Open** dialog, type the full UNC path of the shared package you want to assign. Do not use the **Browse** button. Make sure that you use the UNC path to the shared package.
10. Click on the **Open** button.
11. Click on **Assigned** and then click **OK**. The package is added to the right pane of the **Group Policy** window.
12. Close the **Group Policy** snap-in. Click **OK** and exit the **Active Directory Users and Computers** snap-in.
13. When the client computers start, the assigned package will be installed automatically.

To assign a package (Windows Server 2008 or later):

1. In the **Group Policy Management Editor**, go to **Computer Configuration** and select **Policies and Software Settings**.
2. Select **Software Installation**.
3. Right-click and select **New** and then select **Package**.
4. In the open dialog box, make sure to type the full UNC path of the shared installer package. For example: *\\<machine_name>\MyGPO\DesktopClients.msi*
5. Click **Open** and **Select the Deployment Method** as Assign and click **OK**.
6. From the command-line window, run the command to force update of group policy. *gpupdate/Force*

4.4 Publishing an MSI Package

You can publish a package in order to allow the target user to install it by using Add or Remove programs.

To publish a package on (Windows Server 2003):

1. Click on the **Start** button.
2. Go to **Programs**.
3. Select **Administrative Tools** and then select **Active Directory Users and Computers**.
4. Right-click your domain name in the console tree and select the **Properties**.
5. Select the **Group Policy** tab.
6. Select the object you want and click **Edit**.
7. Expand **Software Settings** under **User Configuration**.
8. Right-click **Software Installation**, select **New** and then click **Package**.
9. In the **Open** dialog, type the full UNC path of the shared package you want to publish. Do not use the **Browse** button. Make sure that you use the UNC path to the shared package.
10. Click on the **Open** button.
11. Click on **Publish** and then click **OK**. The package is added to the right pane of the **Group Policy** window.
12. Close the **Group Policy** snap-in. Click **OK** and exit the **Active Directory Users and Computers** snap-in.
13. Test the package:
    a. Log on to the target computer.
    b. Click on the **Start** button and go to **Control Panel**.
    c. Double-click **Add or Remove programs** and select **Add New Programs**.
    d. In the **Add programs from your network** list select the program you published.
    e. Use the **Add** button to install the package.
    f. Click **OK** and then **Close**.

To publish a package (Windows Server 2008 or later:

1. In the **Group Policy Management Editor**, go to **Computer Configuration**.
2. Select **Policies and Software Settings**.
3. Select **Software Installation**.
4. Right-click and select **New** then select **Package**.
5. In the open dialog box, make sure to type the full UNC path of the shared installer package. For example: *\\<machine_name>\MyGPO\DesktopClients.msi*
6. Click **Open**.
7. Select the **Deployment Method** as **Publish** and click **OK**.
8. From the command-line window, run the command to force update of group policy. *gpupdate/Force*

4.5 Redeploying an MSI Package

Sometimes you may need to redeploy a package, for example when doing an upgrade.

To redeploy a package (Windows Server 2003):

1. Click on the **Start** button.
2. Go to **Programs**.
3. Select **Administrative Tools** and then select **Active Directory Users and Computers**.
4. Right-click your domain name in the console tree and select the **Properties**.
5. Select the **Group Policy** tab.
6. Select the object you used to deploy the package and click **Edit**.
7. Expand the **Software Settings** element (per-user or per-machine) which contains the deployed package.
8. Expand the **Software Installation** element which contains the deployed package.
9. Right-click the package in the right pane of the **Group Policy** window.
10. Select the **All Tasks** menu and click **Redeploy application**.
11. Click **Yes** for reinstalling the application wherever it is installed.
12. Close the **Group Policy** snap-in.
13. Click **OK** and exit the **Active Directory Users and Computers** snap-in.

To redeploy a package (Windows Server 2008 or later):

1. In the **Group Policy Management Editor**, go to **Computer Configuration** and select **Policies and Software Settings**.
2. Select **Software Installation**.
3. Right-click and select **Existing GPO**.
4. Right click and click **Redeploy application**.
5. Click the **Yes** button for reinstalling the application wherever it is installed.
6. Close the **Group Policy** snap-in.
7. Click **OK** and exit the **Group Policy Management** snap-in.
8. From the command-line window, run the command to force update of group policy.
   gpupdate/Force

4.6 Removing an MSI Package

Group Policy allows you to remove packages which have been deployed in the past. For more details read http://support.microsoft.com/kb/816102.

To remove a package:

1. Click on the **Start** button.
2. Go to **Programs**.
3. Select **Administrative Tools** and then select **Active Directory Users and Computers**.
4. Right-click your domain name in the console tree and select the **Properties**.
5. Select the **Group Policy** tab.
6. Select the object you used to deploy the package and click **Edit**.
7. Expand the **Software Settings** element (per-user or per-machine) which contains the deployed package
8. Expand the **Software Installation** element which contains the deployed package
9. Right-click the package in the right pane of the **Group Policy** window
10. Select the **All Tasks** menu and click **Remove**
11. Select from the following options:
    - **Immediately uninstall the software from users and computers**
    - **Allow users to continue to use the software but prevent new installations**
12. Click the **OK** button to continue .
13. Close the **Group Policy** snap-in.
14. Click **OK** and exit the **Active Directory Users and Computers** snap-in.

4.7 Silent Installation Commands

You can install the Avaya IP Office Plug-in silently on a PC using the following command line options:

- **Install only Call Assistant:**
  AvayaOneXDesktopClients.exe /s /v"/qn SECUREMODE=<1 or 0> PORT_NUMBER=<PORTNUMBER> ONEX_PORTAL_SERVER=<one-X Portal Server IP or FQDN> ADDLOCAL=callAssistant,ChangeARP"
- **Install only Outlook plug-in:**
  AvayaOneXDesktopClients.exe /s /v"/qn SECUREMODE=<1 or 0> PORT_NUMBER=<PORTNUMBER> ONEX_PORTAL_SERVER=<one-X Portal Server IP or FQDN> ADDLOCAL=OutlookPlugin,ChangeARP"
- **Install Both:**
  AvayaOneXDesktopClients.exe /s /v"/qn SECUREMODE=<1 or 0> PORT_NUMBER=<PORTNUMBER> ONEX_PORTAL_SERVER=<one-X Portal Server IP or FQDN>"

Note: If the user does not want to provide value of one-X Portal server or port number then do not include those properties. Do not add a space before or after the "=" in property values. A SECUREMODE value other than 0 or 1 defaults to 0.

Chapter 5.
Document History

5. Document History

Date	Issue	Change Summary
3rd March 2016	**11a**	• Updated for IP Office Release 10.0.
9th June 2016	**11b**	• First release.
1st September 2016	**11c**	• Correct some errant mentions of Flare.
1st November 2016	**11d**	• Updated .NET requirements 40 for desktop client support to .NET 4.5.2. • Remove mentions of Google Talk.
23rd November 2016	**11e**	• Update personal contacts capacity to 250.
1st September 2017	**11f**	• Minor grammar corrections.
21st September 2017	**11g**	• Correction to user test page 31, can't use local host IP address.

Index

8

8080 24

A

Add
- Licenses 22

Administrator
- Login 28

Applications DVD 17

B

browser 17

C

Configuration
- During installation 28
- User 23

Cookies 17

D

Directories 11
Directory DSML IP Office Provider 10
Directory DSML LDAP Provider 10
DVD 17

E

Edit
- IP Office Security Settings 21

Enable one-X Portal Services 23
Enhanced TSPI 21
Enhanced TSPI Access 21
Enhanced TSPI service 21
EnhTcpaService 21
Explorer 17
External Directory 11

F

Firefox 17
Firewall 17, 24

H

Hard Disk 17

I

Initial configuration 28
Install
- Software 26

Internet Explorer 17
IP Office
- Applications DVD 17
- Check 28
- License 22
- Security Settings 21
- Select 28
- System Requirements 17
- User configuration 23

J

JavaScript 17

L

License
- Add 22

Listing Ports 24
Login 31
- Administrator 28

M

Mozilla Firefox 17

N

Name 23

O

Operating System 17

P

Password 23
- Change 28

Personal Directory 11
Port 17
- 8080 26
- Set 26

Ports 24
Presentation Level Provider 10
Provider 10

Q

Quick Time 17

R

RAM Memory 17
Remember me on this computer 17
Reserved Ports 24
Rights Group 21

S

Safari 17
Security Settings 21
Server
- PC Requirements 17

Service User 21
Services 21
Settings
- User 23

Software
- Install 26

System Directory 11

T

TCPA Group 21
Telephony CSTA Provider 10
Test
- User Login 31

U

User
- Configuration 23
- Login 31
- Name 23
- Password 23
- User name 23

W

Windows Media Player 17

© 2017 Avaya Inc. All rights reserved.