IP Office 9.0

Implementing one-X Portal for IP Office

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 its hardware and Software ("Product(s)"). 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: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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.
"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.

License types

Designated System(s) License (DS). End User may install and use each copy 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, 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.

Database License (DL). End User may install and use each copy 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 a single instance of the same database.

CPU License (CP). End User may install and use each copy 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 pecified 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 the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/licenseinfo under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). 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 Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.
For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

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 9.0. 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 11 (SCN). one-X Portal for IP Office supports up to 750 simultaneous sessions.
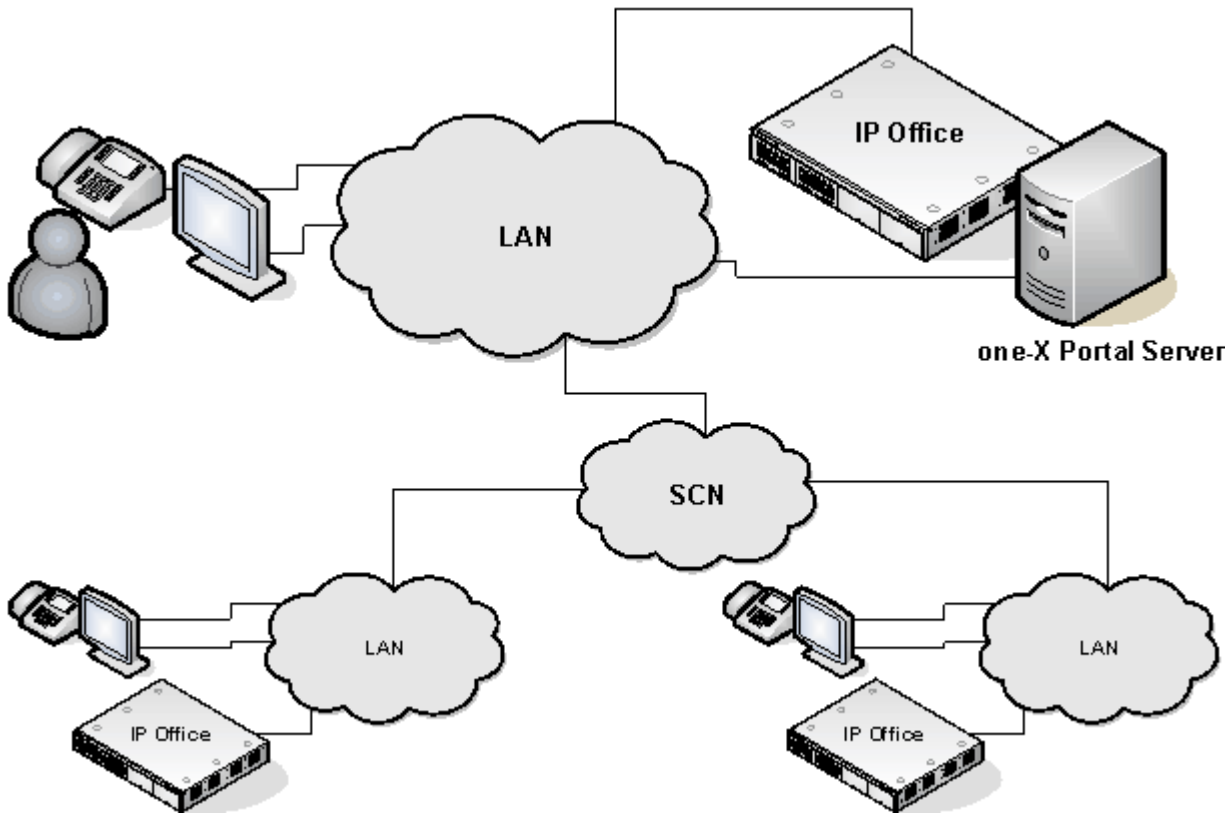
one-X Portal for IP Office installs as a service with an integral web server. Both user and administrator access to one-X Portal for IP Office is via web browser to the one-X Portal for IP Office server.

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.

one-X Portal for IP Office is a licensed application, with each IP Office requiring a one-X Portal for IP Office license for those users configured to use 21 one-X Portal for IP Office.

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.
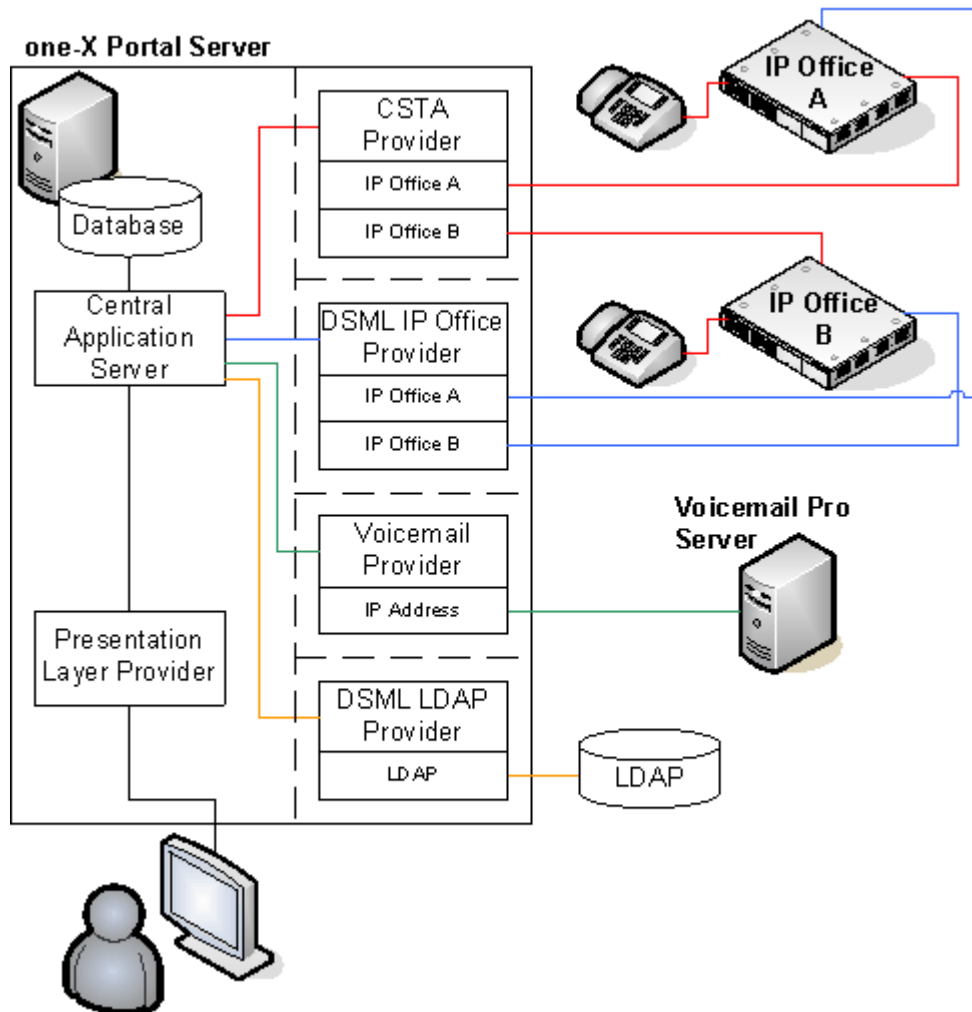
During installation:

- 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. The Voicemail provider is to be manually configured to the IP address of the Voicemail server. Restart the one-X Portal for IP Office after configuring the Voicemail provider.

Note: Automatic configuration of the Voicemail provider is not supported during the installation of the one-X Portal for IP Office version 9.0.

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 100 personal directory entries per user (subject to its own system limits), any additional entries beyond that are stored by one-X Portal for IP Office only.

- 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.

- 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. • 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. • 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).
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 Telephony Notes

Incoming Calls

The calls that reach the one-X Portal for IP Office user still fully controlled by the IP Office system settings. For example the user's call waiting settings, number of appearance buttons, etc. This applies to both user calls and calls to hunt groups of which the user is a member. Issues with incoming calls not alerting the one-X Portal for IP Office user will be down to IP Office system configuration settings.

Outgoing Calls

The outgoing calls that the one-X Portal for IP Office user can make will be subject to the user's IP Office configuration settings. The one difference is that the user can use one-X Portal for IP Office to make additional calls. For example, when all the appearance buttons on a user's phone are in use, they can still use one-X Portal for IP Office to make additional calls.

On some phones, the call log shown by the phone and the redial function use information stored by the phone. Typically this will not include calls made using one-X Portal for IP Office.

Call Gadget Buttons

Within the sub-tab shown for each call being handled by the one-X Portal for IP Office users, a number of buttons are included. The buttons indicate actions that the user can perform or initiate and vary according to factors such as the type of phone, the current state of the call, whether the user already has other calls connected or held, etc.

It is important to understand that it is not the one-X Portal for IP Office application that controls which buttons are displayed. The actions currently performable on each call are indicated to one-X Portal for IP Office as part of the information from the IP Office system.

When the user is using a phone that the IP Office system cannot force off-hook, the following differences are applicable.

- When an incoming calls is presented while the phone is on-hook, one-X Portal for IP Office will not enable the **Answer** button. The user needs to manually take the phone off hook to answer the call using the phone's own controls.

- When making a call from one-X Portal for IP Office with the phone is on-hook (for example after entering a number and clicking on **Call** or having selected to play a voicemail message), the IP Office will call the user's phone and will only make the outgoing call when answered.

Some phones allow actions such as entering the number to call without going off-hook. This is called en-bloc dialing. The IP Office system, and therefore the one-X Portal for IP Office, is unaware of such activity until the prepared digits are sent from the phone.

- This typically applies to phones on DECT system and to SIP extensions.

- Avaya 1400, 1600, 9500 and 9600 Series phones can be optionally set to use en-bloc dialing.

1.4 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 6.0 and higher supports up to 750 simultaneous sessions.

1.5 Terminal services support

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

Chapter 2.
Installation

2. Installation

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 <u>at least one user</u> already licensed and configured for one-X Portal for IP Office operation. It is <u>also vital</u> to check the security settings of each IP Office.

Installation Process

The basic installation process consists of the following stages:

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 9.0 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 9.0 software, it must be upgraded. For more information on the upgrade process, see one-X Portal for IP Office software upgrade 25.

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

  - Each IP Office must be running IP Office Release 9.0 or higher software.

  - Each user and group name must be unique.

  - Each user and group extension number must be unique. The IP Office System Status Application (SSA) should be used to check for name and extension conflicts before installation of one-X Portal for IP Office.

- **IP Office Release 6+ Licensing**
  This release of IP Office uses user profiles licenses. 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.

  - For systems being upgraded from IP Office Release 5, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for IP Office for users set to the **Basic User** profile.

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:

- **Operating System:** Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), and Windows Server 2012 (64-bit). Note that user capacity is restricted to 300 on servers running a 32-bit operating system. For 64-bit Windows servers, additional configuration steps are required to exceed 300 users. See Configuring one-X Portal for IP Office Server for 300+ IP Office Users 44.

- **Processor:** Intel Pentium D945 core or AMD Athlon 64 4000+.

- **RAM Memory:** 4 GB

- **Available Hard Disk Space:** 20 GB.

- **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 22.

- **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**.

- **IIS6 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:

  - **Google Chrome 8 onwards**

  - **Internet Explorer 7.0/8.0/9.0**

  - **Mozilla Firefox 3.5 onwards**

  - **Safari 5.0**

- 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 *English*, *French*, *German*, *Italian*, *Dutch*, *Brazilian Portuguese*, *Latin Spanish*, *Russian* and *Simplified Chinese*. The language it uses will be the best match to the browser language preferences.

- **Phone**
  one-X Portal for IP Office can be used with most phones supported by the telephone system. The operation of analog and SIP phones does affect the method of operation of the one-X Portal for IP Office application, see Telephony Notes 10 .

- 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.

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.

Information Required

- Microsoft Exchange server 2007 or Microsoft Exchange server 2010.

- **IP Address** of the Microsoft Exchange server.

- **User Account:** *AvayaAdmin* user account with rights to mine the details of the users configured on the Exchange server. For more details see Creating AvayaAdmin user account 39 .

- A batch file that automatically sets the impersonation rights for the *AvayaAdmin.* For more details see setting impersonation rights.

- **TCP/IP Port:**
  The default port is 5269. For more details see Checking Available Ports 22 .

- **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. The IP Office Manager also tests 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.

1. If not already done, install IP Office Manager from the IP Office Applications DVD.

2. Start IP Office Manager and select **File | Advanced | Security Settings**.

3. Select the IP Office system and click **OK**.

4. Enter the user name and password for access to the IP Office's security settings.

5. 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 Right Group configured to use this service.
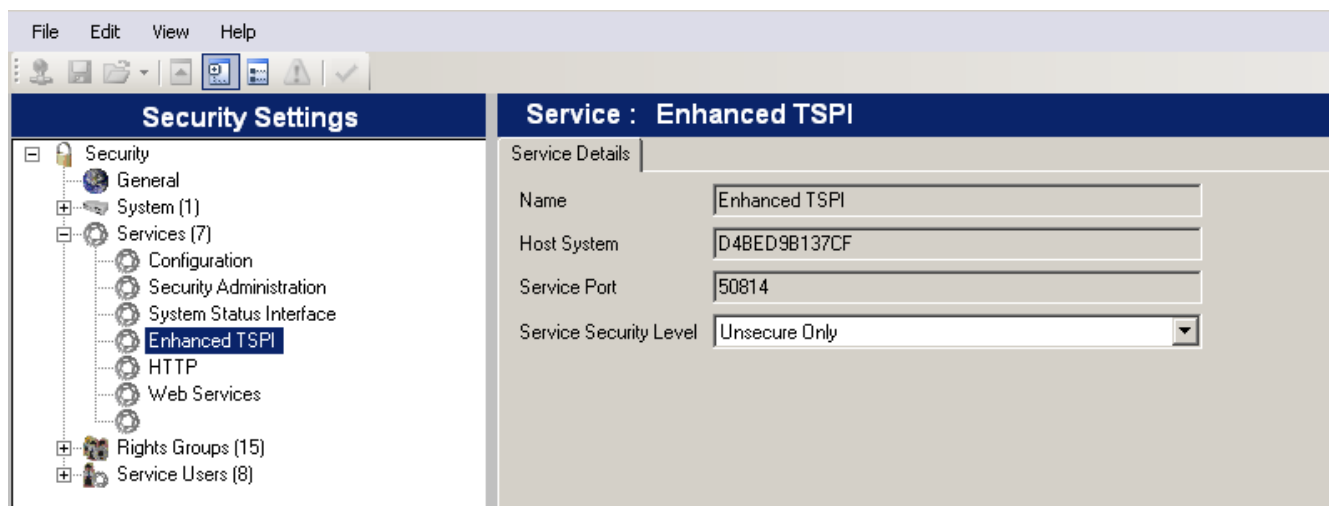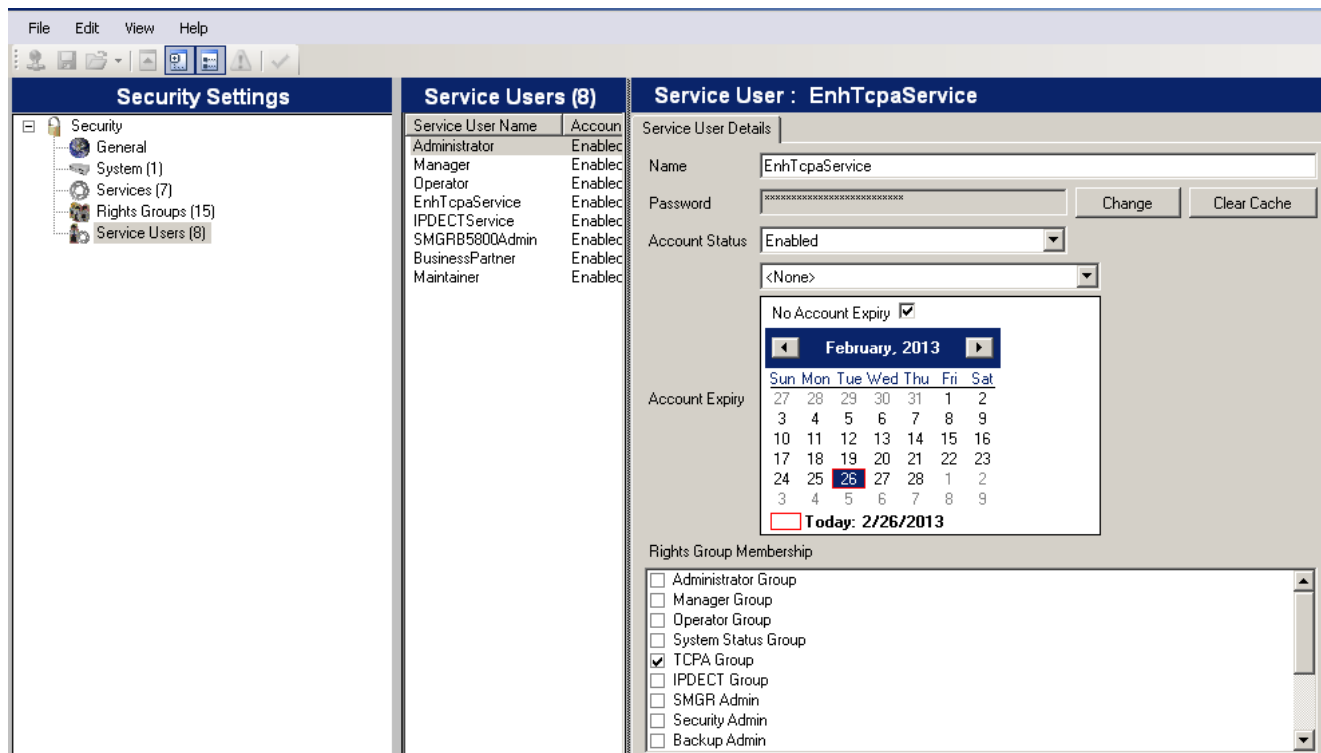

6. Select 👥 **Rights Groups**.
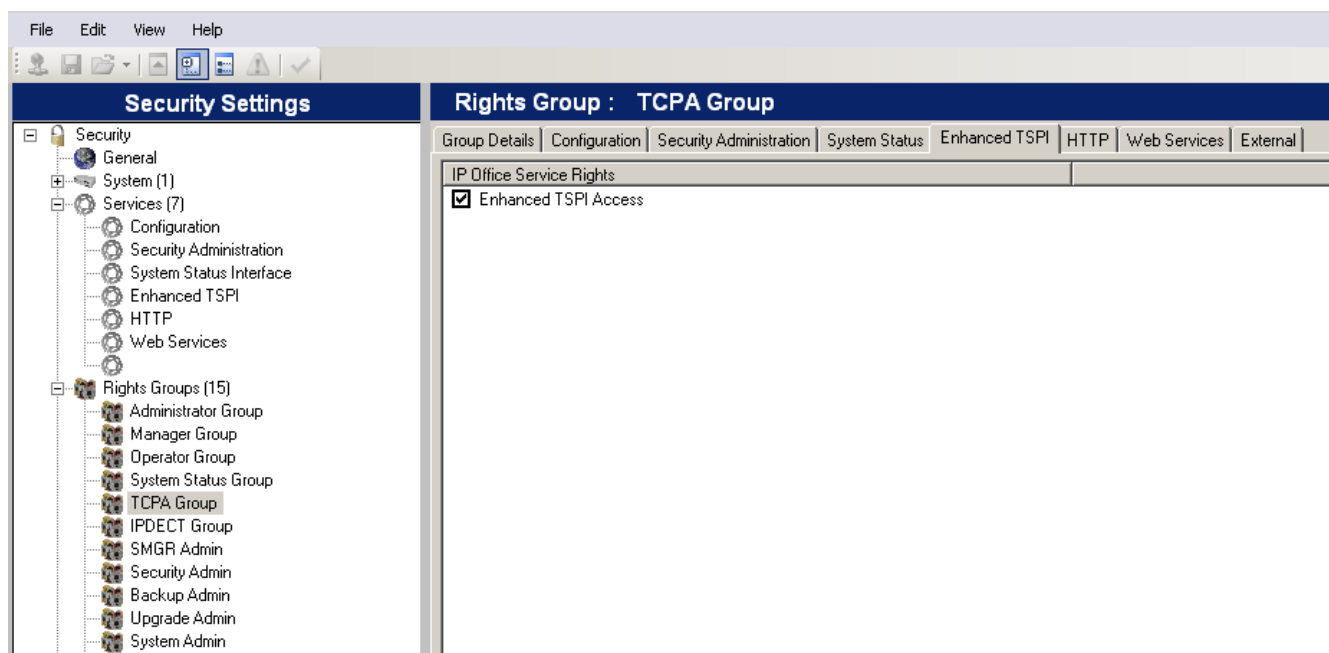
7. The list of **Rights Groups** should contain a group called *TCPA Group*. Select this group and then the **Enhanced TSPI** tab. The option for **Enhanced TSPI Access** should be selected as shown above. If this is not the case correct the security settings, creating a new group.

8. Select 🔧 **Service Users**.

9. 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 password should be *EnhTcpaPwd1*.

10. 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 requires a one-X Portal for IP Office license. The licenses should be added to the IP Office configuration and validated before the one-X Portal for IP Office is installed.

Each one-X Portal for IP Office license is specific to the serial number of the IP Office system's Feature Key serial number and licenses a specific number of users. Multiple licenses can be added for a larger total number of users.

- **IP Office Release 6+ Licensing**
  This release of IP Office uses user profiles licenses. 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.

  - For systems being upgraded from IP Office Release 5, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for IP Office for users set to the *Basic User* profile.

  - For one-X Portal for IP Office 6.0 and higher, a user can refresh their browser without being logged out. All data will be 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 still be logged in. If the user presses the **Esc** button they will be prompted to ask whether they wish to log out, if they do not, the browser will be refreshed. With some browsers, for example Firefox, a user can close their browser without logging out and when they reopen the browser they will be logged straight back in. If a user closes their browser rather than logging out, the license they were using will remain consumed for up to 6 hours.

Note: IP Office users are required to have *Power User* license to use Mobility Client. The profile of the user should be set to *Power User*.

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 🗝 **License**.

5. Click on 🗔 to enter a new license.

6. Enter the license or licenses provided for one-X Portal for IP Office operation on that system.

7. If the license has been entered correctly, the **License Type** will show *one-X Portal for IP Office*. The **License Status** will be *Unknown*. The **Instances** will show the number of users who can now be configured for one-X Portal for IP Office operation using that license.

8. Click on 🖫 to save the updated configuration back to the IP Office system.

9. Reload the IP Office configuration and select 🗝 **License** again.

10. Check that the **License Status** is now *Valid*.

11. Repeat this process for any other IP Office's that will be supported by the one-X Portal for IP Office server.

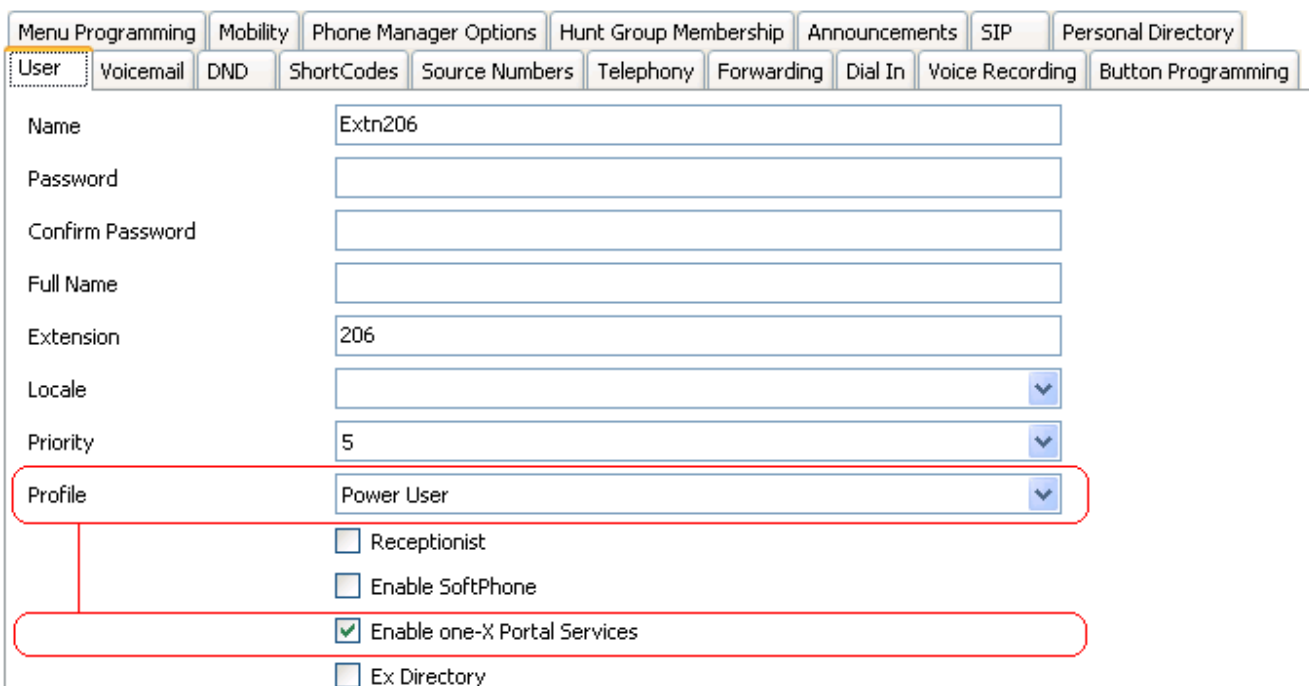# 2.4 Configure Users for one-X Portal for IP Office

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

- **IP Office Release 6+ Licensing**
  This release of IP Office uses user profiles licenses. 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.

  - For systems being upgraded from IP Office Release 5, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for IP Office for users set to the **Basic User** profile.

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.

Menu Programming	Mobility	Phone Manager Options	Hunt Group Membership	Announcements	SIP	Personal Directory

User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming

Name	Extn206
Password	
Confirm Password	
Full Name	
Extension	206
Locale	
Priority	5
Profile	Power User

- ☐ Receptionist
- ☐ Enable SoftPhone
- ☑ Enable one-X Portal Services
- ☐ Ex Directory

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.

10. Repeat the process for any other users who will be using one-X Portal for IP Office services.

11. 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.

A. 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 servers or XMPP enabled servers such as Google Talk. If the customer is not intending to federate with external XMPP servers then this port does not need to be opened on the firewall.

- **8005** - This port is used by the Tomcat shutdown listener.

- **8069** - This port is used for web socket based delivery. Open this port on the machine that runs the **one-X Portal for IP Office**.

- **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.

- **8443** - This port is used for HTTPS access to one-X Portal for IP Office (Only for Windows installation of the one-X Portal for IP Office).

- **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.

- **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.

- **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 to one-X Portal for IP Office (Only for Linux installation of the one-X Portal for IP Office).

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.

B. 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.

C. 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.

D. 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

- **Important**
  Do not start software installation until the previous installation steps (IP Office security settings 18, one-X Portal for IP Office licenses 20, user configuration 21) have been completed.

Prerequisite:

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.

! **WARNING: Windows 2008/2012 Server Installation**
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.

Note: During installation if the system displays the following error :*Error 1330 - Invalid Digital Signature,* install Microsoft updates on Windows 2008/2012 server.

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**.

Note: 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 25.

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**.

   The system displays **Ready to Install the Program** window.

   If the configuration of the system on which you are installing one-X Portal for IP Office has more than 8 GB of RAM, the system prompts you to configure up to 750 IP Office users.

7. Select one of the following:

   - Configure for up to 750 IP Office users (uses 7 GB of system RAM).

     You can also manually configure more than 300 IP Office users. For more information see, Configuring one-X Portal for IP Office Server for 300+ IP Office Users 44 .

   - Configure for up to 300 IP Office users (users 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 22. 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.

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**.

13. Proceed to <u>Initial Server Configuration</u> 27 .

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. Upgrade from **one-X Portal for IP Office** 5.0, 6.0, 6.1, 7.0, 8.0 and 8.1 to 9.0 is supported.

Note: 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 9.0**.**

- 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.

- **!** **WARNING: Windows 2008/2012 Server Installation**
  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.

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**.

    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**.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.

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**.

    The system displays **Ready to Install the Program** window.

    If the configuration of the system on which you are installing one-X Portal for IP Office has more than 8 GB of RAM, the system prompts you to configure up to 750 IP Office users.

7. Select one of the following:

    - Configure for up to 750 IP Office users (uses 7 GB of system RAM)

      You can also manually configure more than 300 IP Office users. For more information see, Configuring one-X Portal for IP Office Server for 300+ IP Office Users 44 .

    - Configure for up to 300 IP Office users (users 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 22 . 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.

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**.

2.7 Initial Server Configuration

At this stage, the one-X Portal for IP Office server software has been installed 23 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://127.0.0.1:8080**. If the software was installed using a different port number, replace the 8080 with that port number.

3. If the service has only just been started, you will 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.

4. The web server installed by the one-X Portal for IP Office installer should respond with its default web page.
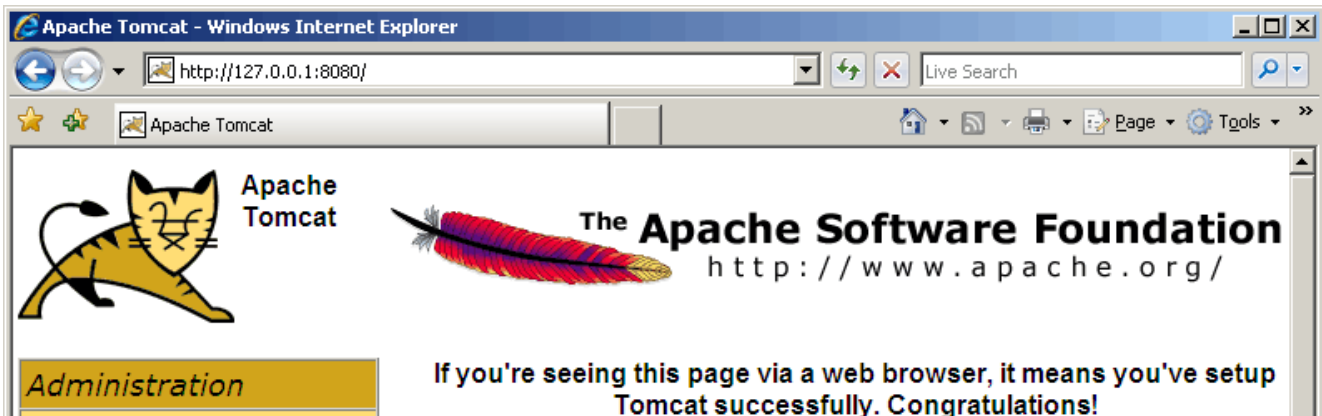
5. Add **/onexportal-admin.html** to the browser address. This is the login path for the administrator access to the one-X Portal for IP Office application.

6. The message **System is currently unavailable - please wait** is displayed with the one-X Portal for IP Office application starts. When the message disappears approximately 15 minutes after the one-X Portal for IP Office service was started, you can login.

7. Check that the version reported matches the version expected. If not refer to the Troubleshooting section.

8. Enter the default administrator name (*Administrator*) and password (*Administrator*) and click **Login**.

9. The **License Agreement** page is displayed.

STEP 1: License Agreement

You must read and accept this agreement.

AVAYA END USER LICENSE AND WARRANTY

For Customer Purchases from a Reseller

THIS END USER LICENSE AND WARRANTY AGREEMENT ("AGREEMENT") GOVERNS THE WARRANTY OF AVAYA'S PRODUCTS AND THE USE OF AVAYA'S PROPRIETARY SOFTWARE. READ THIS AGREEMENT CAREFULLY, IN ITS ENTIRETY, BEFORE INSTALLING OR USING THE AVAYA PRODUCT (S) (AS DEFINED BELOW). BY INSTALLING OR USING THE AVAYA PRODUCT(S), OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING OR USING THE PRODUCT(S) (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. ("AVAYA"). ANY USE OF THE PRODUCT(S) WILL CONSTITUTE YOUR ASSENT TO THE TERMS OF THIS AGREEMENT (OR RATIFICATION OF ANY PREVIOUS CONSENT).

Have Read & Agree
☐

Next-> | Cancel

10. When you have read the license, select **Have Read & Agree** and then click on **Next**.

11. 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.

STEP 2: Setting the IP Office IP Addresses

Description

Now you need to specify sources of user lists, directories & telephony services. Enter a comma seperated list of the IP Address(es) of the IP Office Units which will be used.

For example enter: 192.168.42.1,192.168.42.2

In 'Advanced Provider Options' you may override default provider configuration values and specify an optional LDAP Directory Source common to all users.

IP Office Unit IP Address(es)

192.168.42.1

IP Office(s) not yet checked.

⦿ Simple Installation ○ Advanced Installation
▶ Status

Check IP Office(s)-> | Configure for IP Office(s)-> | Next-> | Cancel & Restart

- In the following menus, the ▶ **Status** icon can be used to show/hide status messages about the actions being performed by the installation process.

12. 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.

13. If the customer has a Voicemail Pro voicemail server, click on **Advanced Installation**.

- Click on the **Voicemail Provider** tab and enter the IP address of the Voicemail Pro voicemail server. For IP Offices in a Small Community this should be 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.

14. If the customer has provided details of an LDAP directory source, click on **Advanced Installation** if not already selected.

- Click on the **Directory (LDAP)** tab. Enter the LDAP server information into the fields labeled LDAP.

Provider Editor

ID	3
Name	Default-DSML-LDAP-Provi
URL	http://localhost:8080/ldapdir
Provider Type Selector	Directory Source (DSML LDAP)

LDAP Server(s) Assigned

DSML LDAP Config Editor

Mid-Layer URL
http://localhost:8080/inkaba

Mid-Layer Username
indoda_user

Mid-Layer Password
••••••••••••••••••••

Mid-Layer Password Hash
7BDDEE71046BA3FA2763

Run On Port
8080

Created	2010-06-24 17:06:59.3170(

Close

LDAP Server(s) assigned to Provider

This control enables you to add & delete the LDAP Server(s) mapped to a provider.
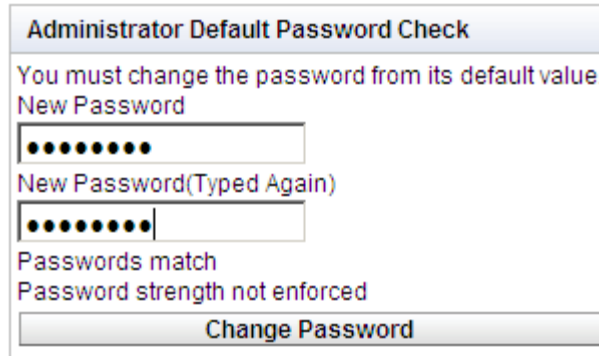Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 1 LDAP Server(s) may be assigned to a provider.
Distribution of providers over several servers may be needed for effective performance.
The factors are: server performance, IP Office utilisation & network latency.

ID	LDAP Server URL	User	Password	Base DN		
0	ldap://135.xx.xxx.xxx:xxx	global\john	••••••••	OU=emea,OU=Global Use	Edit Field Mapping	Delete

Close

15. 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.

STEP 3: Extract User Lists from IP Office Unit(s)

Description

Extraction of lists of users from the IP Office Unit(s) can start. A cached internal representation of these users will be maintained in synchronisation with the master records on the IP Office(s). Adds, moves and changes of users must be done with the IP Office Manager.

▶ Status

Automatic User List Extraction Progress

16. Having extracted user details, the one-X Portal for IP Office server will extract directory details from the IP Office systems.

STEP 4: Synchronise System & Personal Directories

Description

You are now ready to import the System & Personal Directories from the IP Office Unit(s).

▶ Status

17. The one-X Portal for IP Office server will now prompt you to change the password used for administrator access.

Administrator Default Password Check

You must change the password from its default value.
New Password

●●●●●●●●

New Password(Typed Again)

●●●●●●●●

Passwords match
Password strength not enforced

Change Password

18. Enter a new password and click **Change Password**.

19. 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.

1. From a user PC, uses a web browser to browse to the one-X Portal for IP Office server. Type
   http://127.0.0.1:8080/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 IP Office system includes a voicemail server, check that the **Messages** gadget shows messages in the user's mailbox.

10. Select **Logout**.

2.9 Advanced Provider Configuration Options

You can configure the providers The options available through Advanced Installation should not currently be adjusted except for the settings on the Directory (LDAP) tab. That tab can be used to enter the details of the LDAP source to be used.

1. Select **Configuration > Providers**.

2. Click **Get All**.

3. Select a provider.

4. Click **Edit**.

The following providers are listed:

- **Telephony (CSTA)**

- **Directory (IP-Office)**

Provider Editor

ID	2
Name	Default-DSML-IPO-Provide
URL	http://localhost:8080/ipoffice
Provider Type Selector	Directory Source (DSML IP-Office) ▾

IP Office(s) Assigned

DSML IPO Config Editor

Mid-Layer URL
http://localhost:8080/inkaba

Mid-Layer Username
indoda_user

Mid-Layer Password
••••••••••••••••••

Mid-Layer Password Hash
7BDDEE71046BA3FA2763

Run On Port
8080

Created	2010-06-24 17:06:59.25600

Close

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
Distribution of providers over several servers may be needed for effective performance.
The factors are: server performance, IP Office utilisation & network latency.
Timeout value should be numeric and must be between 30 to 600

ID	IP Address	User	Password	Timeout	
0	148.xxx.xxx.xxx			300	Delete

Close   Assign New IP Office Unit

- **Directory (LDAP)**

Provider Editor

ID	3
Name	Default-DSML-LDAP-Provi
URL	http://localhost:8080/Idapdii
Provider Type Selector	Directory Source (DSML LDAP)

LDAP Server(s) Assigned

DSML LDAP Config Editor

Mid-Layer URL
http://localhost:8080/inkaba

Mid-Layer Username
indoda_user

Mid-Layer Password
••••••••••••••••••

Mid-Layer Password Hash
7BDDEE71046BA3FA2763

Run On Port
8080

Created	2010-06-24 17:06:59.31700

Close

LDAP Server(s) assigned to Provider

This control enables you to add & delete the LDAP Server(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 1 LDAP Server(s) may be assigned to a provider.
Distribution of providers over several servers may be needed for effective performance.
The factors are: server performance, IP Office utilisation & network latency.

ID	LDAP Server URL	User	Password	Base DN		
0	ldap://135.xx.xxx.xxx:xxx	global\john	••••••••	OU=emea,OU=Global Use	Edit Field Mapping	Delete

Close

LDAP Field Mappings

Name	givenName
Last name	sn
Work phone	telephoneNumber
Home phone	homePhone
Other phone	cel
Work email	mail
Personal email	personalMail
Other email	otherMail

Close **Defaults**

- **Presentation Layer**

Provider Editor

ID	1
Name	Default-Presentation_Layer
URL	http://localhost:8080/inyam
Provider Type Selector	Application Presentation Layer

Client/Svr. Config Editor

Mid-Layer URL

http://localhost:8080/inkaba

Mid-Layer Username

inyama_user

Mid-Layer Password

••••••••••••••••••

Mid-Layer Password Hash

7BDDEE71046BA3FA2763

Created	2010-06-24 17:01:42.14000

[Close]

- **Voicemail Provider**

Provider Editor

ID	5
Name	Default-VMPro-Provider
URL	http://localhost:8080/izwi
Provider Type Selector	VoiceMailServer (VMPro) ⌄

VoiceMail Server Assigned

VoiceMail Config Editor

Mid-Layer URL
http://localhost:8080/inkaba

Mid-Layer Username
izwi_user

Mid-Layer Password
••••••••••••••••••

Mid-Layer Password Hash
7BDDEE71046BA3FA2763

Run On Port
8080

Created	2010-06-24 17:06:59.39300(

Close

Voicemail Server Assigned to Provider

This control enables you to add & delete the Voicemail server Unit(s).
Changes apply to the local copy of the VMPRO provider record & must be committed to take affect.

ID	VoiceMailServer IP Address	
0	135.xx.xxx.xx	Delete

Close   **Assign New Voicemail Server Unit**

5. Complete the details as required. Then continue as per normal .

2.10 Configuring Microsoft Exchange server for IM/Presence

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.

- Installing Digest Authentication 38
- Enabling Digest Authentication 38
- Creating AvayaAdmin user account 39
- Configuring AvayaAdmin user account 39
- Setting impersonation rights for AvayaAdmin user account 39

2.10.1 Installing Digest Authentication

Before you begin

- Ensure the **Digest Authentication** role is installed.

Note: Installing digest authentication is only applicable to IIS 7.x. By default, digest authentication is available on IIS 6.0.

To install Digest Authentication:

1. On the **Exchange Server** taskbar, click **Start > Administrative Tools > Server Manager**.

2. In the **Server Manager** pane, expand Roles and click **Web Server**.

3. In the **Web Server** (**IIS**) pane, scroll to **Role Services** and click **Add Role Services**.

The system displays the **Add Role Services** wizard.

4. In the **Select Role Services** dialog, select **Digest Authentication**.

5. Click **Next**.

6. In the **Confirm Installation Selections** dialog, click **Install**.

7. On the **Results** dialog, click **Close**.

2.10.1.1 Enabling Digest Authentication

After installing Digest Authentication 38, you have to enable the Digest Authentication on IIS 7.x and IIS 6.0.

To enable the IIS 7.x Digest Authentication (Windows Server 2008 or Windows Server 2008 R2):

1. On the **Exchange Server** taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

2. Expand **Server Name**.

3. Expand **Sites**.

4. Click **EWS**.

5. Under the **IIS Section**, double-click **Authentication**.

6. In the **Authentication** pane, select **Digest Authentication**.

7. In the **Actions** pane, click **Enable**.

To enable the IIS 6.0 Digest Authentication:

1. On the **Exchange Server** taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

2. Expand **Server Name**.

3. Expand **Sites**.

4. Right-click **EWS** and select **Properties**.

5. Select **Directory Security** tab.

6. In the **Anonymous access and authentication control** section, click **Edit**.

7. In the **Authenticated access** section, select **Digest authentication for Windows domain servers**.

8. Click OK twice.

Restart the IIS for the changes to take effect.

Note: IP Office integration with Microsoft Exchange for the purposes of Calendar mining cannot be configured and used, if Microsoft Office Communication Server (OCS) and Office Communicator is already deployed. Hence, 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.

2.10.2 Creating AvayaAdmin user account

To create **AvayaAdmin** user account on the Microsoft Exchange server.

Note: 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 for **AvayaAdmin**. It does not set the rights to mine the calendar details of the users configured on the Microsoft Exchange server for other usernames.

1. In the Microsoft Exchange server window, right click **Mailbox**.

2. Select **New Mailbox**.

3. Choose **User Mailbox** as the mailbox type.

4. Click **Next**.

5. Select **New User** as the **User Type**.

6. Type the User Information such as **First name**, **Lastname**, **User Log on name (User Principal Name)**, and **Password**.

7. Click **Next**.

8. Set the **Mailbox Settings** and type the alias details for the mailbox user.

9. Click **Next**.

10. Click **New**, the system displays the configuration summary of the mailbox.

11. Click **Next**.

12. Click **Finish**, the system creates the **AvayaAdmin** user account.

2.10.2.1 Configuring 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.

Perform the following steps 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**.

2.10.2.2 Setting impersonations rights for AvayaAdmin user account

Before you begin

1. *AvayaAdmin* user account should be configured on the Microsoft Exchange Server.

2. *avaya.ps1* **batch file:** Download the batch file that automatically sets the impersonations rights to mine the details of the users configured on the Microsoft Exchange Server.

   a. Log in as **Administrator** on one-X Portal for IP Office.

   b. Click **Configuration**> **Exchange Service**.

   c. Right-click the **Download Powershell script** link.

   d. Select **Save link as...**

Save the batch file on the main drive. For example, **C** drive.

Note: You will not be able to execute the batch file or set the impersonations rights to the AvayaAdmin user if you save the batch file on 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 display a message that reads: *Permissions for mailbox AvayaAdmin updated successfully*.

If you have created the Avaya Admin user account on the Microsoft Exchanger Server, the system displays a message that reads: *Create mailbox AvayaAdmin and run this script again*.

2.11 Installing Avaya IP Office Plug-in using group policy

You can install Avaya IP Office Plug-in through group policy.

Prerequisite:

Ensure that the .Net Framework 4.0, Microsoft Office 2007 PIA and Microsoft VSTO 2010 Runtime version 4.0 (10.0.40303 or later) are present on all remote machine.

Deploying a Microsoft Installer (MSI) on multiple machines by using group policy.

1. Methods of deployment 40
2. Creating a distribution point 40
3. Creating a Group Policy Object 40
4. Assigning an MSI package 41
5. Publishing an MSI package 41
6. Redeploying an MSI package 42
7. Removing an MSI package 42
8. Command to install Avaya IP Office Plug-in silently 42

2.11.1 Methods of deployment

Group policy supports two methods of deploying a MSI package:

• **Assign software** - A program can be assigned for each user or for each machine. If the program is assigned for each user, the system installs the program when the user logs on. However, if the program is assigned for each machine then system installs the program for all users when the machine starts.

• **Publish software** - A program can be published for one or more users. The system adds this program to the *Add or Remove Programs* list and you can install the program from *Add or Remove Programs* list.

2.11.2 Creating a distribution point

The first step in deploying a MSI using a Group Policy Object (GPO) is to create a distribution point on the publishing server.

To create a distribution point on the publishing server:

1. Log into the server as an Administrator.

2. Create a shared network folder.

3. Set permissions on this folder to allow access to the distribution package.

4. In the shared folder, perform an administrative install for a MSI package contained in an **.EXE** file

Command line for administrative installation: *AvayaOneXDesktopClients.exe /a*

2.11.3 Creating a Group Policy Object

A MSI package is distributed using a GPO.

To create an object for your package:

1. Click **Start**.

2. Select **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

3. Right-click the domain name in the console tree and select **Properties context**.

4. Select **Group Policy** tab and click **New**.

5. Type the name of the policy.

   For example, MyApplication

6. Click **Properties** and select **Security** tab.

7. Enable **Apply Group Policy** checkbox only for those groups to which you want to apply the policy.

8. Click **OK**.

2.11.4 Assigning an MSI package

You can assign a MSI package for each user or for each machine. Also, when you assign the package the system automatically installs the package.

To assign a package:

1. Click **Start**.

2. Select **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

3. Right-click the domain name in the console tree and select **Properties context**.

4. Select **Group Policy** tab

5. Select the object you want to edit and click **Edit**.

6. In **Computer Configuration**, go to **Software Settings**

7. Right-click **Software Installation** and select **New**

8. Click **Package**

9. Click **Open**

10. In the **Open** dialog type the full UNC path of the shared package you want to assign

   Note: Do not browse to the UNC location in the **Open** dialog. Make sure that you type the UNC path to the shared package.

11. Click **Assigned** a then click **OK**

   The system lists the package in the right pane of the **Group Policy** window.

12. Close the **Group Policy** window, and click **OK**

13. Close **Active Directory Users and Computers** window

When you start the client computer, the system automatically assigns the package.

2.11.5 Publishing an MSI package

Using Group Policy, you can publish a package so that the user can install the package from *Add or Remove programs* list
.

To publish a package:

1. Click **Start**.

2. Select **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

3. Right-click the domain name in the console tree and select **Properties context**.

4. Select **Group Policy** tab

5. Select the object you want to edit and click **Edit**

6. In **Computer Configuration**, go to **Software Settings**

7.Right-click **Software Installation** and select **New**

8. Click **Package**

9. Click **Open**

10. In **Open** dialog type the full UNC path of the shared package you want to publish

   Note: Do not browse to the UNC location in the **Open** dialog. Make sure that you type the UNC path to the shared package.

11. Click **Publish** and then **click OK**

   The system lists the package in the right pane of the **Group Policy** window

12. Close the **Group Policy** window, and click **OK**

13. Close **Active Directory Users and Computers** window

To check if the package is published:

1. Log into a client computer

2. Click **Start** and go to **Control Panel**

3. Double-click **Add or Remove Programs** and select **Add New Programs**

   The system lists the package in the **Add or Remove Programs** list

4. Click **Add** to install the package

5. Click **OK** and then click **Close**

2.11.6 Redeploying an MSI package
Sometimes you may need to redeploy a package. For example, when you upgrade the system.

To redeploy an MSI package:

1. Click **Start**.

2. Select **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

3. Right-click the domain name in the console tree and select **Properties context**.

4. Select **Group Policy** tab

5. Select the object you want to edit and click **Edit**

6. In **Computer Configuration**, go to **Software Settings**

7.Right-click **Software Installation**

8. In the right pane of **Group Policy** window, right-click the package you want to redeploy

9. Select **All Tasks** menu and click **Redeploy application**

10. Click **Yes** to reinstall the application

12. Close the **Group Policy** window, and click **OK**

13. Close **Active Directory Users and Computers** window

2.11.7 Removing an MSI package
To redeploy an MSI package:

1. Click **Start**.

2. Select **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

3. Right-click the domain name in the console tree and select **Properties context**.

4. Select **Group Policy** tab

5. Select the object you want to edit and click **Edit**

6. In **Computer Configuration**, go to **Software Settings**

7.Right-click **Software Installation**

8. In the right pane of **Group Policy** window, right-click the package you want to redeploy

9. Select **All Tasks** menu and click **Remove**

10. Select one of the following options:

- Immediately uninstall the software from users and computers

- Allow users to continue to use the software but prevent new installations

11. Click **OK**

12. Close the **Group Policy** window, and click **OK**

13. Close **Active Directory Users and Computers** window

2.11.8 Command to install Avaya IP Office Plug-in silently
The command to install Desktop Clients silently:

Type : *AvayaOneXDesktopClients.exe /s /v"/qn"* in the command line

Chapter 3.

Configuring one-X Portal for IP Office Server for 300+ IP Office Users

3. Configuring one-X Portal for IP Office Server for 300+ IP Office Users

one-X Portal for IP Office supports more than 300 users by default on IP Office Release 9.0 Server Edition and IP Office Release 9.0 Application Server platforms. However, if deploying one-X Portal for IP Office on a Windows server for more than 300 IP Office users, you not only need additional resources for the server computer but also need to modify some configuration settings on the server computer. Note that for one-X Portal for IP Office deployments with more than 300 IP Office users, the maximum limit is 750 users.

Before you begin the installation review <u>Installation Requirements</u> 15.

On Windows operating system

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

- **Operating System:** Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit) or Windows Server 2012 (64-bit).

- **Processor:** Intel® Core™ 2 Duo CPU E8400 @ 3.00 GHz.

- **System RAM:** 8 GB.

- **Available Hard Disk Space:** 20 GB.

Configuring Windows server to support 300+ IP Office users

1. Do the following:

    - If your system is not running one-X Portal for IP Office 9.0 already, <u>install</u> 23 or <u>upgrade</u> 25 to one-X Portal for IP Office 9.0.

        Note: *Do not select* the **Start the Avaya one-X Portal for IP Office Service** check box.

    - If your system is already running one-X Portal for IP Office 9.0, 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*.
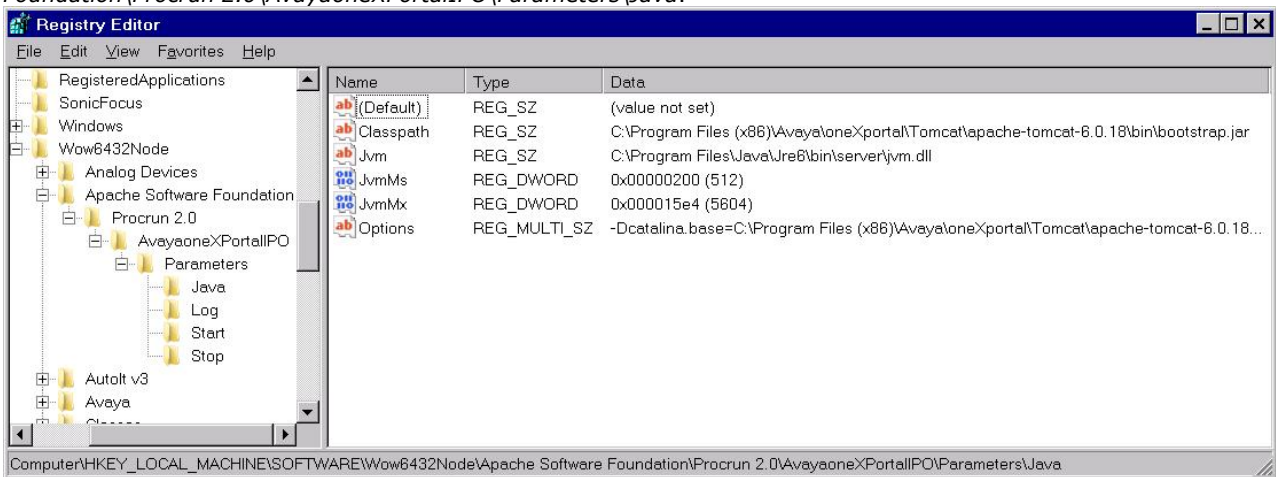
c. Click **File**, and then click **Export**.
This step backs up the key before you make any changes. You can import this file back into the registry later if your changes cause a problem.

d. Right-click the subkey *Jvm*, and click **Modify** on the pop-up menu.

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**.

Edit DWORD (32-bit) Value

Value name:

JvmMs

Value data:

512

Base
- ○ Hexadecimal
- ● Decimal

OK   Cancel
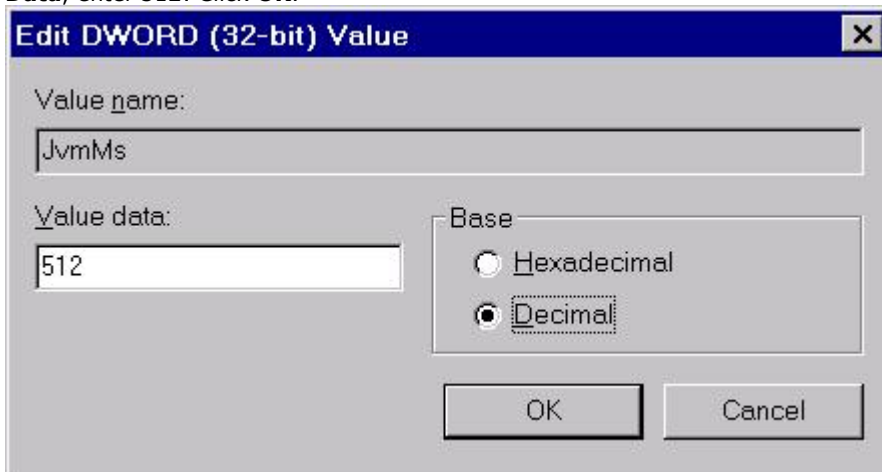
f. Right-click the subkey *JvmMx*, and click **Modify** on the pop-up menu. Under **Base**, select **Decimal**. In **Value Data** , enter *5604*. Click **OK**.

For more information about the available ports see, *Checking Available Server Ports* 22 .

Edit DWORD (32-bit) Value

Value name:

JvmMx

Value data:

5604

Base
- ○ Hexadecimal
- ● Decimal

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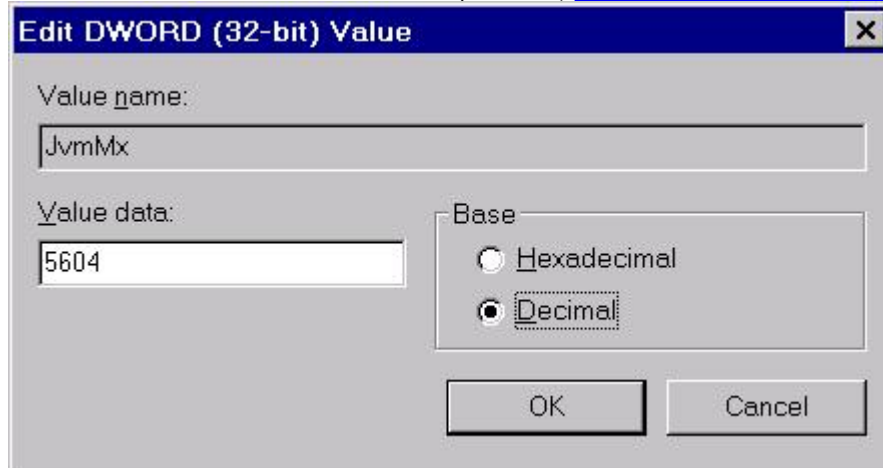
g. Right-click the subkey *Options*, and click **Modify** on the pop-up menu. Add the following parameters:

- *-XX:MaxPermSize=256m*

- *-XX:+HeapDumpOnOutOfMemoryError*

- *-XX:-UseGCOverheadLimit*
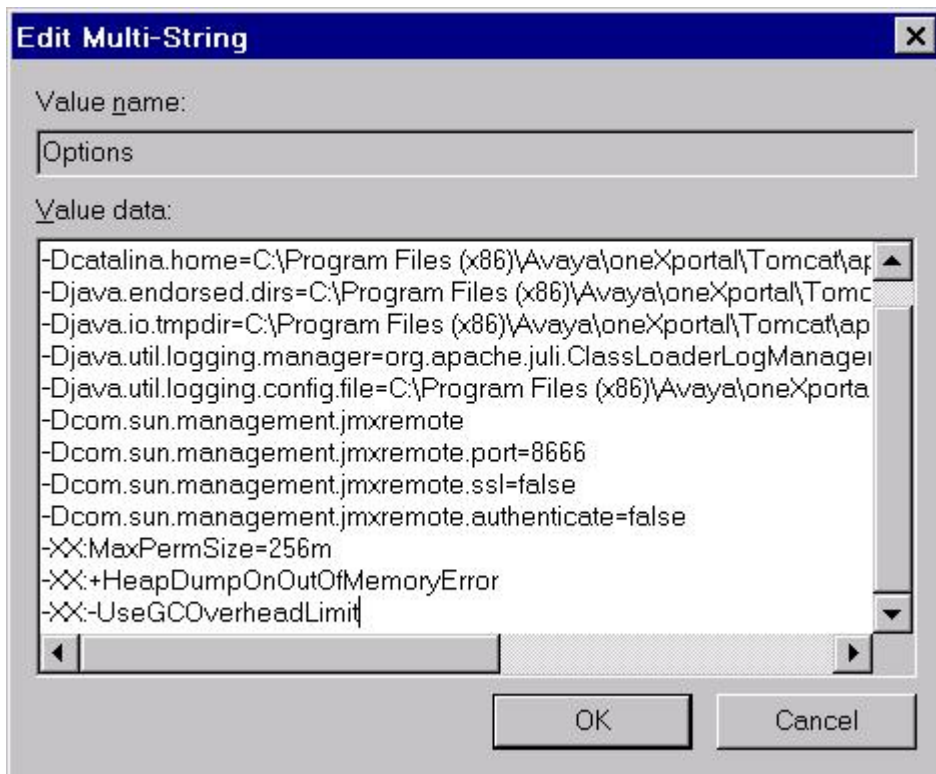
- Click **OK.**

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

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

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

- 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.

Note: After each time you upgrade one-X Portal for IP Office to a newer version, you must follow step 3 ⁴⁴ above to configure the server computer.

Chapter 4.
Glossary

4. Glossary

CSTA - Computer Supported Telecommunications Application.

Indoda - The Zulu word for 'man'.

Induna - The Zulu word for 'advisor', 'great leader' or 'ambassador'.

Inyama - The Zulu word for 'meat' or, when applied to people, 'flesh'. For example 'inyama nenyama' is 'face to face' or 'in the flesh'.

Inkaba - The Zulu word for 'navel' or 'centre'. For example 'inkaba yedolobha' is 'town centre'.

Izwi - The Zulu word for 'voice'.

TCPA - Thin Client Productivity Application.

TSPI - Telephony Service Provider Interface.

XMPP - Extensible Messaging and Presence Protocol

XML RPC - XML Remote Procedure Call

Chapter 5.
Document History

5. Document History

Date	Issue	Change Summary
6th November 2013	**9b**	• Updated supported user figures to 300 for 32-bit OS and 750 for 64-bit OS.
19th November 2013	**9c**	• Clarified support more than 300 user. Use of third-party Linux is not a supported option.

Index