Administering Avaya one-X® Mobile for IP Office

Release 9.1
December 2014

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.

For full support, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759.

For full support, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03–600758.

To locate this document on our website, simply go to http://www.avaya.com/support and search for the document number in the search box.

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: http://support.avaya.com 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, HTTP://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, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 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" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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 or such successor site as designated by Avaya. 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, Hosted Service(s), 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, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Getting started

Overview

Avaya one-X® Mobile for IP Office is an application that works with the IP Office suite to provide enterprise communications on mobile phones. The two versions of the client are: Preferred and Essential. The installation and configuration for each version is different. IP Office Releases 8.0 and later support the Avaya one-X Mobile Preferred version.

The one-X Mobile Essential and one-X Mobile Preferred clients provide enterprise dialing, transferring, and conferencing capabilities, which the corporate communication network uses to seamlessly extend services to the mobile phones of employees. The one-X Mobile Preferred client provides a number of additional features that include:

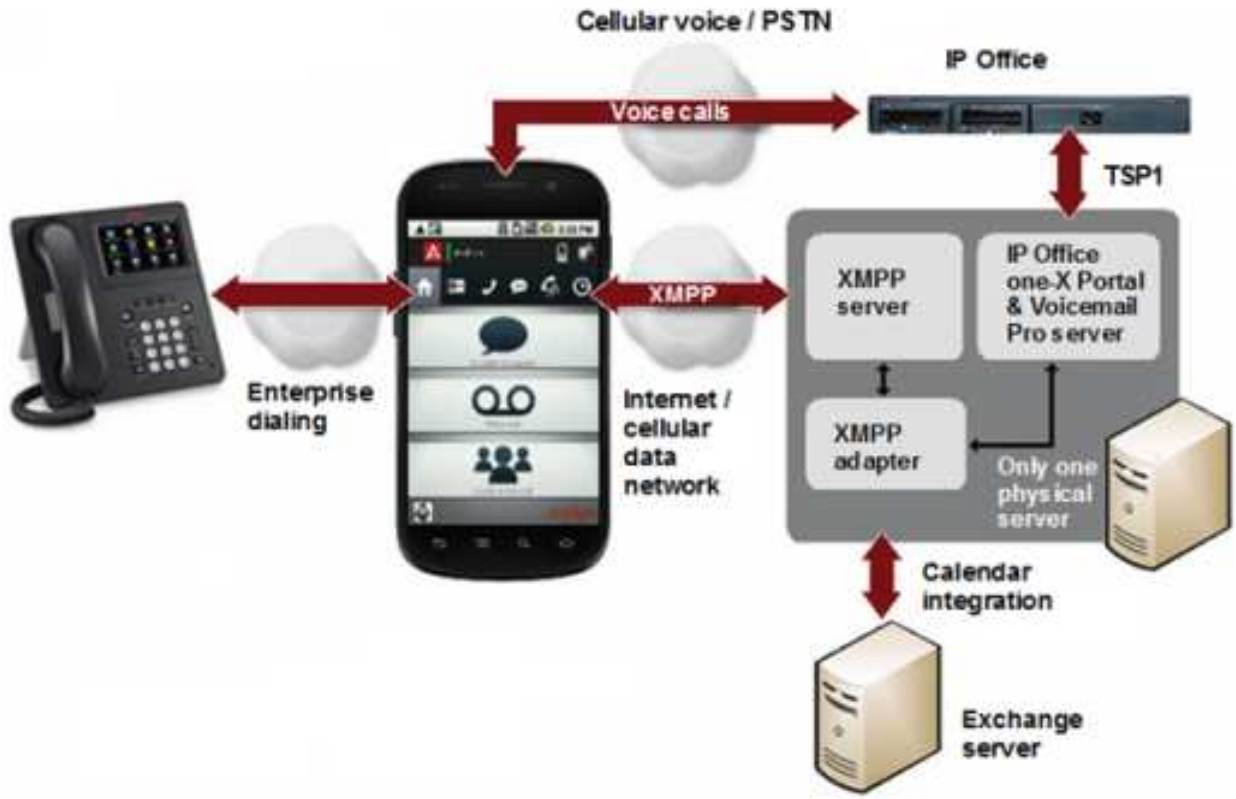
- Presence information for users and for the contacts of the users.
- Geo-location presence and tracking using the on-board GPS of the mobile phone.
- Instant messaging with contacts and user groups defined on the IP Office server and also with external contacts.
- The capability to play voice mail messages, pick-up incoming voice mail messages, view current presence of the voice mail caller, and return calls.
- Rich conference controls with click-to-conference for users and groups, entry and exit notifications, and the capability to view and manage conference participants.
- Integration with Microsoft Exchange Server to provide information about the availability of users.
- Real-time notifications of communications arriving on the server, such as new voice mail or instant messages, changes in the availability of contacts, and conference participants dialing into a conference bridge.

To configure your mobile phone for Avaya one-X® Mobile, follow the appropriate link:

- Preferred client configuration overview on page 16
- Essential client configuration overview on page 22

System architecture

In the following diagram, the Avaya one-X Mobile Preferred client leverages corporate infrastructure with IP Office and IP Office applications to deliver enterprise communications to mobile phones.



The IP Office server pushes the Contacts list to the mobile phone. Users need not configure the Contacts list.

The one-X Mobile Preferred client architecture uses the XMPP server that integrates with Avaya one-X® Portal and Microsoft Exchange Server and offers the following advantages to the mobile user:

- Corporate instant messaging and presence information through integration with the XMPP server.
- View calendar information of contacts and share calendar information with other contacts by integrating with Microsoft Exchange Server.

Related documentation

Because Avaya one-X® Mobile integrates with IP Office and IP Office applications, you must gain access to the IP Office documentation suite to administer this application. The following related documents are available on the Avaya Support website at support.avaya.com:

- *IP Office Manager*
- *Administering Avaya one-X® Portal for IP Office*
- *Implementing Avaya one-X® Portal for IP Office*
- *Implementing Voicemail Pro*
- *IP Office Application Server Installation and Maintenance* for Linux deployments

System requirements

Avaya one-X® Mobile integrates with IP Office and IP Office applications. When you deploy one-X Mobile Preferred as part of an IP Office solution, the system requirements depend on the server where the IP Office applications, such as Avaya one-X® Portal and Voicemail Pro, are installed. With the appropriate licensing, you can deploy IP Office applications on Windows Servers 200x and also Linux servers.

The following sections outline the licensing and application requirements for each client and also the supported operating systems and network requirements for the one-X Mobile Preferred client.

Licensing

The Avaya one-X Mobile Essential client for IP Office requires an Essential Edition system license.

The Avaya one-X Mobile Preferred client for IP Office has the following licensing requirements:

- Preferred Edition system license
- One Mobile Worker or Power User license per client

Note:

On a Mid-Market setup, the mobility client supports only the Power User license. The Mobile User license is unavailable.

Application requirements

IP500s on Releases 4.2 and later, support the Avaya one-X Mobile Essential client. IP Office Releases 8.0 and later, support the Avaya one-X Mobile Preferred client. The system requires trunks that support clearing supervision, which include the following:

- IP500 Universal PRI not on T1 robbed-bit or E1R2 channels set to Loop Start emulation
- IP500 BRI
- SIP RFC2833

For one-X Mobile Essential, ensure that the available DID/DDI numbers are equal to the number of features that you want to implement.

Preferred client supported operating systems

Windows:

Windows Server 2003, Windows Server 2008, and Windows Server 2012 support IP Office applications. If you are using one-X Mobile Preferred on a Windows server, you must install the following applications before performing the administration:

- Avaya one-X® Portal
- Voicemail Pro with the Web Voicemail component installed

  For information on installing the Web Voicemail component, see *Implementing Voicemail Pro*.

Linux:

If you are using one-X Mobile Preferred on a Linux server, you must install the following applications before performing the administration:

- IP Office Application Server

  IP Office Application Server is a single installer for Linux and selected IP Office applications. The IP Office Application Server installation installs the base operating system, the IP Office server applications, and Web pages for managing the server. The base operating system is CentOS 5 or CentOS 6, a Linux operating system. IP Office Application Server is configured and managed remotely using a Web browser.

  For information about installing the IP Office Application Server, see *IP Office Application Server Installation and Maintenance*.

- Avaya one-X® Portal

  The Avaya one-X® Portal for IP Office application is configured and managed remotely using a Web browser.

- Voicemail Pro

  The Voicemail Pro application is configured and managed remotely using the Windows Voicemail Pro client. You can download and install a copy of the Voicemail Pro client from IP Office Application Server.

  Note:

  The Avaya one-X® Mobile application requires the Voicemail Pro application.

Preferred client network requirements

The Avaya one-X Mobile Preferred application must be able to connect through the Internet to Avaya one-X® Portal and to the IP Office system, using either a 3G network or an external Wi-Fi service. Your network setup must support this capability and cellular voice connectivity.

If you deploy Avaya one-X® Portal and IP Office behind a router or firewall, ensure that the following TCP ports can gain access through the firewall:

- Ports 5222 and 8444 must be open for Avaya one-X® Mobile to communicate with the Avaya one-X® Portal server. Port 5222 is for XMPP traffic and Port 8444 is for bootstrap REST API call traffic.
- Port 5269 must be open for the Avaya one-X® Portal server to be able to link with another XMPP server outside the company firewall.
- Ports 5060 and 5061 for VoIP and the RTP ports.

In addition, you must assign an FQDN to the public IP address of the router fronting Avaya one-X® Portal that is resolvable over the Internet. You must configure the router to forward packets destined to ports 5222, 5269, and 8444 to Avaya one-X® Portal. Perform this by creating port forwarding rules on the router.

To determine the host name information, see the following:

- Linux Server Edition — Application Server Installation
- *IP Office Application Server Installation and Maintenance*

Supported platforms

The one-X Mobile Preferred client is available for most Apple and Android mobile phones, while the one-X Mobile Essential client is available for Windows Mobile, Symbian, Android, and BlackBerry mobile phones.

Before you begin the installation, ensure that the application supports your mobile phone by using the following reference table. After you confirm support for your mobile phone, use the table to identify the download location of the Avaya one-X® Mobile client.

one-X Mobile Preferred			
Operating System	**Operating System version support**	**Mobile phone model tested**	**Download location**
iPhone (iOS)	7.x or 8.x	iPod Touch or 4S or 5 or 5C or 5S or 6 or 6+	Apple App Store
Android	2.1 or later	Works on smartphones with the listed OS version	Google Play Store
	4.0 or later	For VoIP, supported mobile phones are Samsung Galaxy S3, Samsung Galaxy S4, Samsung Note 2, LG Optimus E975, and HTC One-S	

one-X Mobile Essential			
Operating System	**Operating System version support**	**Mobile phone model tested**	**Download location**
iPhone (iOS)	5.0	iPhone 3G or 3GS iPhone 4 or 4S	Apple App Store (one-X Mobile *Lite*)
Android	2.2 2.3.3	Works on smartphones with the listed OS version	Google Play Store
Blackberry	5.0 or later	5.0 (9700 nontouch screen) 6.0 (9800 touch screen)	Blackberry App World
Symbian	4.6.6 4.7.5	Nokia 6121 Nokia 6220 Nokia E51 Nokia E52 Nokia E55 Nokia E63 Nokia E66 Nokia E71 Nokia E72	support.avaya.com

one-X Mobile Essential			
Operating System	**Operating System version support**	**Mobile phone model tested**	**Download location**
		Nokia E75	
Windows Mobile	6 6.1	HTC Touch Pro HTC Touch Pro 2 HTC Touch Diamond HTC Touch Diamond2	support.avaya.com

Chapter 2: Installing Avaya one-X® Mobile

Installation methods

The installation methods vary depending on the mobile phone and the chosen client. A provisioned installation is possible only if IP Office Manager is configured correctly. For more information, see the following sections.

Installing one-X Mobile Essential

You can install one-X Mobile Essential using the application store. Use the reference table under Supported platforms on page 11 to determine the download location for a mobile phone. You must then configure the application appropriately.

Installing one-X Mobile Preferred

You can choose to install one-X Mobile Preferred either as a provisioned installation or a basic installation. The benefit of a provisioned installation is the auto-configuration of various parameters within the application, such as the server name, port, username, and password.

- **Basic installation:**

  The traditional method of installation is to download the application from the application store and install the application.

  The caveat to the basic installation is that you need to manually configure the application.

- **Provisioned installation:**

  When an installer or administrator adds a new user using IP Office Manager or Web Manager and assigns that user an appropriate *Power User* or *Mobile Worker* license, you can configure that user to automatically receive a welcome email by enabling the **Send Mobility Email** check box. When IP Office updates, the user receives an email that contains the following information:

  - A brief introduction of one-X Mobile Preferred for IP Office
  - Instructions and links to install and configure the client on the mobile phone

  Note:

  Activate the email links from the mobile phone and not from a PC. On an Android mobile phone, the email includes a single link to install and configure the application. On an Apple mobile phone, the email includes separate links to install and configure the application.

  The host name defined in the email must match that of the Windows server on which Avaya one-X® Portal is installed.

Note:

On Linux Server Edition systems, an administrator must use the Web Control Web interface to configure the network settings so that the auto-configuration email link uses the FQDN instead of the IP address of the server. In Web Control, navigate to **Settings > System > Host Name** to change the network settings. If you change the domain name using any other method, the email links might not work correctly.

The Avaya one-X® Portal server communicates the UCM host FQDN to the IP Office control unit, which relays the information to Avaya one-X® Mobile using the Mobility Email. Avaya one-X® Mobile uses this host FQDN to communicate with the Avaya one-X® Portal server and fetch the XMPP domain name as configured during the Avaya one-X® Portal server administration.

Configuring call facility using Avaya one-X® Mobile

The first time you use the application, either the installer or the user must configure the *call facility* on the Home screen.

When using Avaya one-X® Mobile, the server uses third-party call control to first call the Avaya one-X® Mobile user and when the user answers, connect the user to the destination. In essence, when using third-party call control, the server attempts to find the user and makes a call to that user first. In the request, the client indicates to the server where to find the user. The complete process is known as *call facility* and you must configure the settings when you make the first call.

In every call-oriented request, the client provides the call facility configuration, which the server uses to find the user. Before the first call, and at any point when a call facility is undetermined, the system displays a pop-up to alert the user and to request the configuration of the call facility.

The supported call facility options are **Mobile phone**, **Home phone**, **Work phone**, **Custom phone number**, and **VoIP**. The default call facility option is *Work phone*. Use the application interface to change the preferred call facility:

- IP Office stores the phone numbers for **Mobile phone** and **Home phone**. You can configure the numbers using Avaya one-X® Portal or through the mobile application.
- The phone number for **Work phone** is the extension that IP Office assigns to the user. You cannot configure this number using Avaya one-X® Portal or through the mobile application.
- The phone number for **Custom phone number** is stored only on the mobile application. Avaya one-X® Portal does not store custom phone numbers.
- In the **VoIP** mode, the mobility client has an extension and performs all call control functions including mid-call features.

To manually set and clear the call facility, and if necessary, add a prefix dial number, use the following procedure.

Note:

The user must configure the call facility only on one mobile phone, whether or not the user logs into multiple mobile phones. The popup does not appear on any additional mobile phone.

Procedure

1. On the Home screen, tap **Call Facility**.

   The system displays the menu with options to set or clear the phone number.

2. If you select **Set phone number**, enter the number in the text field, and press **OK**.

   When you start entering the number, Avaya one-X® Mobile filters and lists any of the matching numbers already entered for the corresponding call facility.

   If the call facility requires a prefix number, for example, the user has to press 9 to dial an external number, select the **Phone system requires a prefix** check box, and enter the prefix number in the **Prefix** field.

3. If you select **Clear phone number**, the system clears the call facility number.

   The application provides a confirmation message and returns to the Home screen.

Chapter 3: Configuring Avaya one-X® Mobile Preferred for IP Office

Preferred client configuration overview

The Avaya one-X Mobile Preferred client communicates with Avaya one-X® Portal to determine the feature and extension configurations. Use the following procedures to configure the XMPP domain, the Avaya one-X® Mobile users, the XMPP groups, the connection to Microsoft Exchange Server, calendar access, and the mobile twinning feature.

Configuring the XMPP domain

Use the following procedure to configure or change the XMPP domain of Avaya one-X® Portal.

Before you begin

Open the Administrator interface in Avaya one-X® Portal.

Procedure

1. Choose one of the following options:
   - If you are using Avaya one-X® Portal for the first time, the system displays a wizard. In the wizard, select **Advance > IM /Presence Server**.
   - If you are not using the wizard, select **Configuration > IM/Presence**.
2. In the **XMPP Domain Name** field, enter the FQDN that the Avaya one-X Mobile Preferred client uses to register with the server.

   Note:

   Do not leave the value in the field to the default, 127.0.0.1. Enter a correct XMPP domain name so that the iPhone client can connect to the server.

   The FQDN must be accessible from the Internet if you want to use Avaya one-X® Mobile outside your WLAN. Avaya recommends that you use a split DNS so that the server name outside your WLAN resolves into the public IP address of the NAT or firewall. Also, the server name inside your network resolves into the private IP address on the LAN.
3. Click **Save**.

The system displays a dialog box to confirm the change before restarting the server. The dialog box also displays a message stating that `IM/Presence functionality will cease working until the server is restarted.`

4. If you choose to continue, the system displays a progress bar to indicate that the XMPP domain name changes are being saved.

   After a successful save, the system displays another dialog box to restart Avaya one-X® Portal.

5. Restart Avaya one-X® Portal.

Configuring users

Use the following procedure to configure the IP Office users who can use the one-X Mobile Preferred client.

Note:

If you are using a *Basic User* profile, you cannot register the one-X Mobile Preferred client.

Before you begin

Open the Avaya IP Office Manager interface.

Procedure

1. In IP Office Manager, select **User** in the navigation list.
2. Right-click **User** and select **New**.
3. In the **User** tab area, in the **Name** field, enter a name or extension number.

   The name is the name that the user enters in the **Username** field of the one-X Mobile Preferred client. The name can be up to 15 characters long.

   The application uses the name that you enter in this field for caller display and voice mail.

4. In the **Password** and **Confirm Password** fields, enter a password.

   Note:

   A mobility client that does not have a password configured cannot connect to the mobility server. If you configure the IP Office user without a password, that user must enter the extension number in the **Password** field of the mobility client.

5. In the **Full Name** field, enter the first and last name of the user.

   Avaya one-X® Mobile displays this name in the Contacts list.

6. In the **Profile** field, choose one of the following profiles with the associated license:
   - **Power User**
   - **Mobile User**

     On a Mid-Market setup, the *Mobile User* profile is unavailable.

7. Select the **Enable one-X Portal Services** check box *only* if you want to grant access to the Avaya one-X® Portal user page.

   For the *Mobile User* profile, this requires an extra license.

8. (Optional) To enable VoIP for a user, select the **Enable Mobile VoIP Client** check box.
9. (Optional) For enterprise dialing purposes, click the **Telephony** tab, and in the **Call Settings** area, configure the value in the **No Answer Time (secs)** field between 20 and 25 seconds.

   Note:

   Calls made using enterprise dialing have to account for network delays. As such, a user with **No Answer Time (secs)** set to 15 seconds or less might experience dropped calls where the service provider has configured a shorter or equivalent no-answer time. In this case, due to a delay in the network, the service provider call-answer settings take effect prior to the IP Office **No Answer Time (secs)** setting.

   Similarly, if **No Answer Time (secs)** is set for too long, for example, 50 seconds, this might give the service provider voice mail the time to activate prior to IP Office voice mail. Hence, a call made using enterprise dialing goes to the voice mail of the service provider instead of IP Office voice mail. Service providers vary based on location and network delay times vary between service providers, so you must ensure that you set an appropriate delay.

10. (Optional) To enable the user to view multiple incoming calls, select the **Call Waiting On** check box, .
11. To save the changes, click **OK**.

Configuring the XMPP group

IP Office supports user groups for the following advantages:

- Distribution of voice messages to a group
- Ease of navigation in folder names
- Invite a group to a conference
- Invite a group to a group chat
- Control the size of the roster for optimizing real-estate and bandwidth for mobile phones

The mobility clients display updates on user presence only for users that are in the same group. For example, if *A* and *B* are in the same XMPP group, *A* and *B* can view the presence updates of each other. If *A* and *B* are not in any administrator defined XMPP group, by default *A* and *B* are in the *System* group. Hence, *A* and *B* can view the presence updates of each other.

If *A* and *B* are in different groups, that is, *A* is in G1 and *B* is in G2, *A* and *B* cannot view the presence updates of each other.

If you add *A* to an administrator defined XMPP group, *A* is automatically removed from the *System* group.

Procedure

1. In IP Office Manager, select **Group** in the navigation list.
2. Right-click **Group** and select **New**.
3. In the **Group** tab, in the **Name** field, type a name for the XMPP group.
4. In the **Profile** field, select **XMPP Group**.
5. To add a few users to the group, click **Edit**.
6. In the **Available Users** list, select the users and click **Append**.
7. Click **OK**.
8. To save the changes, click **OK**.

Configuring the connection to Microsoft Exchange Server

To provide calendar information to the one-X Mobile Preferred client users, you must first configure the connection between Avaya one-X® Portal and Microsoft Exchange Server.

Avaya one-X® Portal connects to Microsoft Exchange Server using Exchange Web Services, logging in to Exchange using a service account that has the required permissions to query user calendar information. The name of the service account is *AvayaAdmin* and the account must have impersonation rights.

Impersonation rights are the permissions provided to the *AvayaAdmin* account to gain access to the database of Microsoft Exchange Server for information about users. The *AvayaAdmin* account then passes the user information to Avaya one-X® Portal when Avaya one-X® Portal requests such information.

Before you begin

If Avaya one-X® Portal and Microsoft Exchange Server are in the same Windows domain, you must enable digest authentication on Microsoft Exchange Server. For information on how to enable digest authentication, see the procedures in *Implementing Avaya one-X® Portal for IP Office*.

About this task

Use the following procedure to configure the *AvayaAdmin* account on the Exchange server and configure impersonation rights to the *AvayaAdmin* account. You must gain access to both Microsoft Exchange Server and Avaya one-X® Portal to complete this procedure.

Procedure

1. On the Exchange server, create a new mailbox called **AvayaAdmin**.
2. Log in to Avaya one-X® Portal as an administrator, and click **Configuration** in the left navigation pane.
3. Click **Exchange service** .

4. At the bottom of the Avaya one-X® Portal Exchange service Web page, right-click the **Download Powershell script** link and save the script as `c:\avaya.ps1` on the Exchange server.
5. On the Exchange server, click **Start > Run**, type `powershell c:\avaya.ps1` and press **OK**.

   This step runs the `avaya.ps1 powershell` script, which adds the required Exchange permissions to the *AvayaAdmin* service account.
6. On the Avaya one-X® Portal Exchange service Web page, enter the following information:
   - Enter the service account name as **AvayaAdmin**.
   - Enter the password that you defined when the *AvayaAdmin* account was created on the Exchange server.
   - Enter the IP address or domain name of the Exchange server.
   - Enter the port number as **6669**.
   - If your company uses an HTTP proxy and the Exchange server is located outside your company, enter the IP address of the HTTP proxy server or the domain name and proxy port number.
7. Click **Save**.
8. To test the configuration, click **Validate Exchange Service Configuration**.

   The box above the **Validate Exchange Service Configuration** button displays the test results. If the configuration is successful, the test results display: `The Exchange Service Configuration is valid. The Exchange Server is reachable. The Service account has impersonation rights.`

Next steps

After you configure the integration between Microsoft Exchange Server and Avaya one-X® Portal, you must configure calendar access for each user. For more information, see Configuring calendar access on page 20.

Configuring calendar access

You can configure Avaya one-X® Portal to update user presence with calendar meeting and appointment information based on information from Microsoft Exchange Server. The information is made available to the one-X Mobile Preferred client.

Before you begin

You must configure Microsoft Exchange Server. For more information, see Configuring the connection to Microsoft Exchange Server on page 19.

About this task

To configure calendar access for each user, perform the following procedure on the IP Office Manager interface.

Procedure

1. Log in to IP Office Manager as an administrator.
2. In the left navigation pane, select the *User* that you want to configure.
3. In the **User** tab area, in the **Email Address** field, enter the Exchange email address for that user.
4. Click **OK**.

Enabling the mobile twinning feature

Use the mobile twinning feature to twin an external mobile phone with an internal extension. When you receive a call on your extension, the number that is twinned also rings. Use the mobile twinning feature on the client application to control how you receive incoming calls.

By default, IP Office Manager disables the mobile twinning controls for all users. To ensure that the mobile twinning controls are visible in the client application, you must select the **Mobility Features** check box.

Procedure

1. In IP Office Manager, in the left navigation pane, select a *User*.

   Ensure that the license for the user is *Power User*.
2. In the **Mobility** tab, select the **Mobility Features** check box.
3. To save the changes, click **OK**.

Chapter 4: Configuring Avaya one-X® Mobile Essential for IP Office

Essential client configuration overview

Users of one-X Mobile Essential have the following options:

- Manually configure the mobile phone.
- Import a configuration file that includes the required IP Office system information, which determines the features available to the mobile user.

The import option is available during the installation of the client on Android, Blackberry, Symbian, and Windows mobile phones. To customize the system information and specify the features available to the mobile user, you must create a configuration file for deployment, instead of updating the users to manually configure the settings. The user can then import the configuration file.

However, on Apple mobile phones, you can only configure the client by using the **Settings** menu in Avaya one-X® Mobile.

The following sections include the required information about prefixes and codes, feature name extensions, and enterprise settings that you require to configure one-X Mobile Essential on all supported mobile phones.

Configuring the client

Use the following information to configure the one-X Mobile Essential client.

A configuration file consists of the following types of tags:

1. **Prefixes and codes:** These tags are mandatory or optional that specify system information.
2. **FNE tags:** Feature name extension tags. For more information, see the Feature Name Extensions (FNEs) on page 28.
3. **Enterprise Settings:** Additional settings to provide sub-menus to the client application. For Android and Blackberry, use standard 2-level XML format.

The package that you download from the Avaya support website includes a sample configuration file. The package contains all tags that the administrator must configure.

Note:

Do not use the **+** character in front of the prefixes. The example file usually includes the **+** character in front of the prefixes. Some mobile phones do not recognize the **+** character and cannot complete the call.

For a Windows Mobile device, the configuration file must have the file name extension of **.ini**, whereas Symbian devices must have a file name extension of **.1xme**, and Android and Blackberry devices require a file name extension of **.onexcs1k**.

The following list suggests guidelines for modifying the configuration file:

- Fill in the values for the tags that you want to use.
- Do not change the tag name or equal sign (=) for a tag.
- Do not remove any tag rows. If tag values are unavailable or not provided, leave the value position blank.
- Do not remove the terminating semi-colon (;) for a tag. The client application ignores any characters after the semi-colon so that the user can add description text.
- The following tags are mandatory, although not necessarily the values shown in the following example:

```
DDI_PREFIX = +1555776
INTERNATIONAL_DIRECT_DIAL_PREFIX = 011;
NATIONAL_DIRECT_DIAL_PREFIX = 1;
HOME_COUNTRY_DIAL_CODE = 1;
ARS_CODE = ;
EXTENSION_LENGTH = 3;
NATIONAL_NUMBER_LENGTH = 10;
USERS_EMERGENCY_NUMBERS = 112,999,911;
```

For Android and Blackberry mobile phones

Use the following table to determine the settings supported and required for Android and Blackberry mobile phones:

Telephony Setting	XML Key	Required	Android	Blackberry
Service Number	serviceNumber	Yes	Yes	Yes
Emergency Number. Valid values: 911, 112, 999, 08	emergencyNumber	No	Yes	Yes
Custom Emergency Number	customEmergencyNumber	No	Yes	Yes
Number of Digits for Local Number. Valid values: 5, 6, 7, 8, 9, 10	localNumber	No	Yes	Yes
Outside Line Code	outsideLineCode	No	Yes	Yes
Long Distance Code	longDistanceCode	Yes	Yes	Yes
International Code	internationalCode	Yes	Yes	Yes

Telephony Setting	XML Key	Required	Android	Blackberry
Home Country Code	localCountryCode	Yes	Yes	Yes
Sim Ring Enable Code (PCAA)	pcaFfcEnableCode	Yes	Yes	Yes
Sim Ring Disable Code	pcaFfcDisableCode	Yes	Yes	Yes
Call Forwarding Enable Code	callForwardingEnableCode	No	Yes	Yes
Call Forwarding Disable Code	callForwardingDisableCode	No	Yes	Yes
Voicemail	voicemail	No	Yes	Yes
Extension Number of Digits. Valid values: 3, 4, 5, 6	extensionDigits	No	Yes	Yes
MFAC	MFAC	Yes	Yes	Yes
End of Sequence	EOS	Yes	Yes	Yes
Conference Digit	conferenceDigit	Yes	No	Yes
Toggle Digit	toggleDigit	Yes	No	Yes
Disconnect Digit	disconnectDigit	Yes	No	Yes

The following is an example of a configuration file for Android and Blackberry mobile phones:

```
<?xml version="1.0" encoding="UTF-8"?>  <mobileXSettings>
    <emergencyNumber>911</emergencyNumber>
    <customEmergencyNumber></customEmergencyNumber>
    <outisdeLineCode>9</outsideLineCode>
    <extensionDigits>4</extensionDigits>
    <MFAC>#</MFAC>
    <EOS>295</EOS>
    <localCountryCode>1</localCountryCode>
    <longDistanceCode>1</longDistanceCode>
    <internationalCode>011</internationalCode>
    <serviceNumber>16137717514</serviceNumber>
    <pcaFfcEnableCode>281</pcaFfcEnableCode>
    <pcaFfcDisableCode>280</pcaFfcDisableCode>
    <callForwardingEnableCode>283</callForwardingEnableCode>
    <callForwardingDisableCode>282</callForwardingDisableCode>
    <voicemail>1234</voicemail>
    <conferenceDigit>1</conferenceDigit>
    <toggleDigit>2</toggleDigit>
    <disconnectDigit>3</disconnectDigit>  </mobileXSettings>
```

For Windows Mobile and Symbian mobile phones

For Windows Mobile, the configuration file is *settings.ini* . For Symbian single-mode phones, the configuration file is *setting.1xme* . For some phones, after you install the software, you can change the settings file values using the phone interface.

The following is a brief description of the tags for prefixes and codes for use in either configuration file. The values that you enter for these tags depend on your country and the settings of your IP Office system. Examples of values for the United States are provided in the following tags:

LOCATION_NAME = ;

This is a required tag for Windows Mobile .ini settings file only. The tag is not present and is not required for a Symbian configuration file. The string defines the location name of the Avaya one-X® Mobile server and the mobile phone displays the name in the Avaya one-X® Mobile menu. If you have multiple locations, each location must have a unique LOCATION_NAME value.

Example: `LOCATION_NAME = Boston;`

PRE_IMS = ;

This tag is not used by IP Office.

DID_PREFIX = ;

This required tag defines the DID/DDI prefix that is used to specify the FNE features in IP Office. For example, if you are using 73255512XX as DID/DDI numbers to activate your FNEs, the DID_PREFIX as shown would be set intentionally short 2 digits because the FNE tag is populated with the last 2 digits (e.g. IDLE_APPEARANCE_SELECT = 85;). The DID_PREFIX and the FNE digits when put together must equal the full DID/DDI number.

Example: `DID_PREFIX = 173255512`

INTERNATIONAL_DIRECT_DIAL_PREFIX = ;

This required tag specifies the international call prefix for your country.

Example: `INTERNATIONAL_DIRECT_DIAL_PREFIX = 011`

NATIONAL_DIRECT_DIAL_PREFIX = ;

This optional tag specifies the prefix for dialing national numbers.

Example: `NATIONAL_DIRECT_DIAL_PREFIX = 1`

HOME_COUNTRY_DIAL_CODE = ;

This required tag is the home country code.

Example: `HOME_COUNTRY_DIAL_CODE = 1`

ARS_CODE = ;

This optional tag sets the ARS access code.

Example: `ARS_CODE = 9`

EXTENSION_LENGTH = ;

This required tag sets the dial plan length of IP Office.

Example: `EXTENSION_LENGTH = 5`

NATIONAL_NUMBER_LENGTH = ;

This required tag specifies the number of digits for a national number. This field accepts multiple numbers separated by commas for countries that have different number lengths.

Example: NATIONAL_NUMBER_LENGTH = 9, 10

USERS_EMERGENCY_NUMBERS = ;

This is a required tag that specifies the numbers dialed for emergency.

Example: USERS_EMERGENCY_NUMBERS = 911

SETTINGS_PIN = ;

This is an optional tag. When set, the client prompts the user to input this PIN when installing or modifying the configuration.

Example: SETTINGS_PIN = 1234

The following table includes the sample configuration files for Windows Mobile and Symbian mobile phones:

Windows Mobile 'settings.ini'	Symbian 'settings.1xme'
Dialing Prefixes and Codes	*Dialing Prefixes and Codes*
PRE_IMS=Dial; DID_PREFIX = 1555776; INTERNATIONAL_DIRECT_DIAL_PREFIX = 011; NATIONAL_DIRECT_DIAL_PREFIX = 1; HOME_COUNTRY_DIAL_CODE = +1; ARS_CODE = ; EXTENSION_LENGTH = 3; NATIONAL_NUMBER_LENGTH = 10; USERS_EMERGENCY_NUMBERS = 112,999,911; SETTINGS_PIN = 1234;	DID_PREFIX = 1555776; INTERNATIONAL_DIRECT_DIAL_PREFIX = 011; NATIONAL_DIRECT_DIAL_PREFIX = 1; HOME_COUNTRY_DIAL_CODE = +1; ARS_CODE = ; EXTENSION_LENGTH = 3; NATIONAL_NUMBER_LENGTH = 10; USERS_EMERGENCY_NUMBERS = 112,999,911; SETTINGS_PIN = 1234;
DDI Suffixes for Features: These are used with the DDI_Prefix above to complete the DDI number for a particular FNE feature	*DDI Suffixes for Features: These are used with the DDI_Prefix above to complete the DDI number for a particular FNE feature*
IDLE_APPEARANCE_SELECT = 9900; ACTIVE_APPEARANCE_SELECT = 9901; AUTO_CALL_BACK_TOGGLE = 9902; DISABLE_AUTO_CALL_BACK_TOGGLE = 9903; CALL_FORWARDING_ALL_ACTIVATION = 9904; CALL_FORWARDING_BUSY_NO_ANSWER_ACTIVATION = 9905; CALL_FORWARDING_DISABLE = 9906; CALL_PARK = 9907; CALL_UNPARK = 9908; CALL_PICKUP_GROUP = 9909; CALL_PICKUP_DIRECTED = 9910; CALL_PICKUP_GROUP_EXTENDED = ; CALLING_PARTY_NUMBER_BLOCK = 9912; CALLING_PARTY_NUMBER_UNBLOCK = 9913; CONFERENCE_ON_ANSWER = 9914; DROP_LAST_ADDED_PARTY = 9915; EXCLUSION = 9916; HELD_APPEARANCE_SELECT = 9917; OFF_PBX_ENABLE = 9919; OFF_PBX_DISABLE = 9920; SEND_ALL_CALLS_ENABLE = 9924; SEND_ALL_CALLS_DISABLE = 9925; TRANSFER_ON_HANGUP = 9926; TRANSFER_TO_COVERAGE = 9927;	IDLE_APPEARANCE_SELECT = 9900; ACTIVE_APPEARANCE_SELECT = 9901; AUTO_CALL_BACK_TOGGLE = 9902; DISABLE_AUTO_CALL_BACK_TOGGLE = 9903; CALL_FORWARDING_ALL_ACTIVATION = 9904; CALL_FORWARDING_BUSY_NO_ANSWER_ACTIVATION = 9905; CALL_FORWARDING_DISABLE = 9906; CALL_PARK = 9907; CALL_UNPARK = 9908; CALL_PICKUP_GROUP = 9909; CALL_PICKUP_DIRECTED = 9910; CALL_PICKUP_GROUP_EXTENDED = ; CALLING_PARTY_NUMBER_BLOCK = 9912; CALLING_PARTY_NUMBER_UNBLOCK = 9913; CONFERENCE_ON_ANSWER = 9914; DROP_LAST_ADDED_PARTY = 9915; EXCLUSION = 9916; HELD_APPEARANCE_SELECT = 9917; OFF_PBX_ENABLE = 9919; OFF_PBX_DISABLE = 9920; SEND_ALL_CALLS_ENABLE = 9924; SEND_ALL_CALLS_DISABLE = 9925; TRANSFER_ON_HANGUP = 9926; TRANSFER_TO_COVERAGE = 9927;
Enterprise Settings	*Enterprise Settings*

Windows Mobile 'settings.ini'	Symbian 'settings.1xme'
`SUB_MENU_NAME = My Company;` `<Voicemail> = *17;`	`SUB_MENU_NAME = My Company;` `<Voice Mail> = *17;`

For Apple mobile phones

The client configuration for one-X Mobile Essential on Apple mobile phones must occur during the initial startup. When you install and open the application for the first time, a welcome message indicates that you must configure the client. If you do not configure the client, the application does not work. The configuration occurs in the **Settings** menu of iPhone as opposed to a configuration file.

You can access the **Settings** menu of iPhone and configure the client using the information in the following table:

Configurable parameter	Description
System type	EC500
Dialing parameters	• **Emergency Number:** The public safety emergency number. For example, 911. • **Outside Line (ARS Code):** The code to use to gain access to an outside line. • **Local Numbers - # of digits:** The number of digits to dial for a local number. • **Local Country Code:** The local country code. • **Long Distance Code:** The code to dial for long distance calls. • **International Code:** The code to dial for international calls.
CS1000-specific settings	*DO NOT ALTER THIS SETTING*
EC500-specific settings	Set the following FNE parameters to the appropriate DDI number for each feature in IP Office: • **Off–PBX Call FNE (Simultaneous Ring) Enable** FNE19: “Enable Twinning” in IP Office • **Off–PBX Call FNE (Simultaneous Ring) Disable** FNE20: “Disable Twinning” in IP Office • **Call Appearance FNE Active** FNE01: “Steal Call” in IP Office • **Call Appearance FNE Idle** FNE00: “System Dial Tone” in IP Office • **Send AIL Calls FNE Enable** FNE24: “DND On” in IP Office • **Send AIL Calls FNE Disable** FNE25: “DND Off” in IP Office

Feature Name Extensions

A Feature Name Extension (FNE) is a number that you dial from your mobile phone to use an Avaya IP Office feature.

All FNEs that the administrator activates must associate to a Direct Inward Dialing/Direct Dial-In (DID/DDI) number that comes in over a supported trunk type. The administrator configures this in IP Office. Also, you must configure the DID/DDI number in the configuration file for the Avaya one-X® Mobile client.

The following table lists the supported IP Office FNEs, the corresponding FNE number, and the tag name. The table also lists support for the Android and Blackberry mobile phones.

When you create an FNE service short code in the IP Office configuration, enter the FNE number in the telephone number field. Use the tag names listed in the table to activate or deactivate a specific feature in the client configuration files for Symbian and Windows Mobile devices. Activate a feature by populating a valid DID/DDI number in the associated tag. An empty tag does not activate the feature.

FNE Number	Feature	Tag Name	Android and Blackberry
00	System Dial Tone	`IDLE APPEARANCE SELECT = ;`	Yes
01	Steal Call	`ACTIVE_APPEARANCE_SELECT = ;`	Yes
02	Auto Call Back	`AUTO_CALL_BACK_TOGGLE = ;`	No
04	Forward All Calls	`CALL_FORWARDING_ALL_ACTIVATION = ;`	Yes
05	Forward Busy and No Answer Calls	`CALL_FORWARDING_BUSY_NO_ANSWER_ ACTIVATION = ;`	Yes
06	Call Forward Disable	`CALL_FORWARDING_DISABLE = ;`	Yes
07	Park Call	`CALL_PARK = ;`	No
08	Call UnPark	`CALL_UNPARK = ;`	No
09	Pick Up Group	`CALL_PICKUP_GROUP_EXTENDED = ;`	No
10	Directed Call Pick Up	`CALL_PICKUP_DIRECTED = ;`	No
12	Withheld CLI (To External Calls off IPO)	`CALLING_PARTY_NUMBER_BLOCK = ;`	No
13	Enable CLI (To External Calls off IPO)	`CALLING_PARTY_NUMBER_UNBLOCK = ;`	No
14	Conference Add	`CONFERENCE_ON_ANSWER = ;`	Yes
15	Drop Call	`DROP_LAST_ADDED_PARTY = ;`	Yes
16	Private Call (cannot be intruded or recorded)	`EXCLUSION = ;`	Yes
17	Held Appearance Select	`HELD_APPEARANCE_SELECT = ;`	Yes

FNE Number	Feature	Tag Name	Android and Blackberry
18	Same as FNE 00 - Dial Tone Appearance (a=)	`IDLE_APPEARANCE_SELECT = ;`	Yes
19	Enable Twinning	`OFF_PBX_ENABLE = ;`	Yes
20	Disable Twinning	`OFF_PBX_DISABLE = ;`	Yes
24	DND On	`SEND_ALL_CALLS_ENABLE = ;`	Yes
25	DND Off	`SEND_ALL_CALLS_DISABLE = ;`	Yes
26	Blind Transfer	`TRANSFER_ON_HANGUP = ;`	Yes
27	Transfer to Voicemail	`TRANSFER_TO_COVERAGE = ;`	No
31	Used for Mobile Call Control		Yes
32	Used for Mobile Direct Access		Yes
33	Used for Mobility Callback with system mobile call control		Yes

Chapter 5: The VoIP client

Avaya one-X Mobile Preferred for IP Office supports Voice over Internet Protocol (VoIP) calls. VoIP is a set of technologies and transmission techniques that delivers voice over IP networks, such as the Internet.

You can make and receive VoIP calls using Avaya one-X® Mobile. Configure the Avaya one-X® Mobile client to work in the VoIP mode to make calls over Wi-Fi or 3G or 4G data networks, thus eliminating cellular voice charges. Change to the VoIP mode to reduce costs, especially on international calls.

VoIP supports G.711a/mu, G.722, and G.729A with or without silence suppression. The codec list and order is only configurable on the Android mobility clients based on the data connection type, Wi-Fi versus cell data network.

Note:

Avaya one-X® Mobile for IP Office on Apple mobile phones does not support G.723 codecs.

VoIP prerequisites

The prerequisites for VoIP are as follows:

- User license is *Power User*.
- The mobile application connects to IP Office 9.0 or later.
- Mobile phone is running on Android 4.0 or later, or iOS 5.0 or later.
- Supported mobile phones are Samsung Galaxy S3, Samsung Galaxy S4, Samsung Note 2, LG Optimus E975, and HTC One-S.
- In IP Office Manager, in the **User** tab, select the **Enable Mobile VoIP Client** check box.

Networking information

By default, the VoIP client uses TLS. If the administrator disables TLS on IP Office, the mobile phone automatically uses TCP. However, Avaya recommends TLS for Android phones, as TCP causes connection issues on some Android mobile phones.

If you are connecting to IP Office using a VoIP client from a remote network, that is, a home network or a public hotspot, use the following configuration:

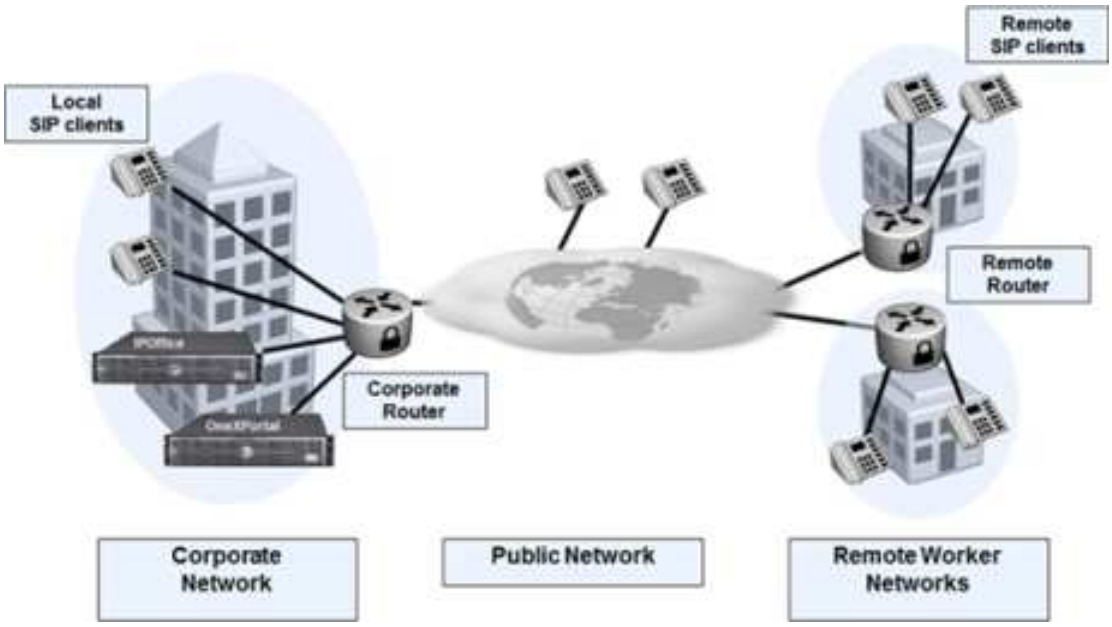
- By default, the firewall fronting IP Office opens TCP ports 5060 and 5061. For security reasons, Avaya recommends you to change these ports and forward to IP Office.
- Some router configurations might require forwarding of the ports that are in use by RTP. The default port range for RTP in IP Office Manager is 49152 to 53246. For security reasons, Avaya recommends you to change these ports by selecting a port that does not conflict with any other active RTP port.
- Enable and configure the *Remote Worker* feature on IP Office.
- Disable SIP ALG on remote network firewall.

Note:

In IP Office, you can change the TCP 5060 port and TLS 5061 port to any other port that is inactive. The port you change, must not conflict with any other active port. The changed port automatically gets configured to the one-X preferred mobility clients.

SIP remote worker overview

In the deployment diagram, IP Office is installed inside an enterprise network and provides SIP-based telephony services to users that are connected directly on that enterprise network as well as to users that are connecting remotely from their branch offices, homes, and other locations.



At any of these sites, there might be a non-SIP-aware NAT or firewall that prevents proper communication. The intent of the *Remote Worker* feature is to enable unobstructed communication between IP Office and remote users without requiring the help of a SIP-aware NAT or firewall or any external SBCs.

In the deployment diagram, the SIP clients can be categorized as follows:

- For SIP clients that are on the corporate network, that is, local workers, NAT traversal is not required.
- For SIP clients that are directly on the public Internet, that is, remote workers, the SIP clients must traverse the corporate router, local NAT, to work with IP Office.
- For SIP clients that are behind home or private routers, that is, remote workers, the SIP clients must traverse the home router, remote NAT, the corporate router, and local NAT to work with IP Office.
- If IP Office is located on the public Internet, local NAT traversal is not required for the SIP clients that are located in the public network or the remote network.

For local NAT traversal, IP Office must:

- Discover the public IP address of LANx.
- Identify clients from the public Internet.
- Use the private address of LANx during SIP transactions with clients from the corporate network.
- Use the public address of LANx during SIP transactions with clients from the public Internet.

In the deployment diagram, the LANx of IP Office has the *Remote Worker* feature turned on and the LANx is behind the corporate NAT. In this case, the SIP clients that are located on the public network or on the remote network are remote clients. These SIP clients require the remote worker license to register with IP Office.

If the LANx of IP Office has the *Remote Worker* feature turned on and the LANx is on the public Internet, only the SIP clients that are behind home or private routers require the remote worker license. In this case, the SIP clients that are directly on the public Internet do not require the remote worker license.

Note:

If the remote client is behind its own NAT, but has SIP-ALG turned on or supports full STUN capability, in this case, the remote client appears as a SIP client located on the public Internet to IP Office and does not require the remote worker license.

The *SIP Remote Worker* feature complements the remote worker feature for H.323 clients. Hence, you must perform configuration settings for SIP as you did for H.323 to include support for the *Remote Worker* feature, the extension level remote worker capability, and the user level remote worker licensing,

Supported SIP remote clients include Flare for iPad, Flare for Windows, one-X Mobile Preferred for iPhone, and one-X Mobile Preferred for Android. The *SIP Remote Worker* feature supports all transport protocols for signaling including UDP, TCP, and TLS.

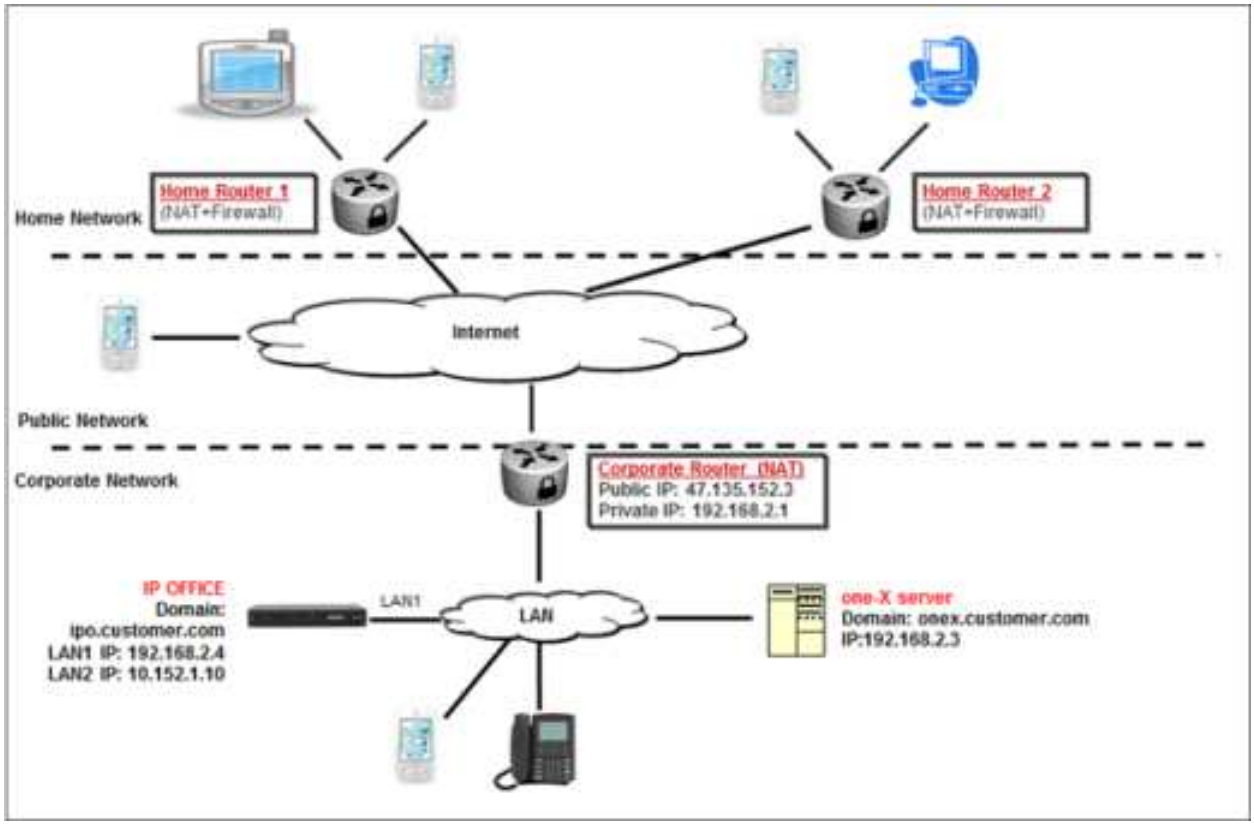
Note:

All media involving remote SIP clients is relayed on IP Office. Hence, this needs more bandwidth in IP Office.

SIP remote worker supports the following deployments:

- Native IP Office SIP remote worker
- SIP remote worker using Avaya SBCE

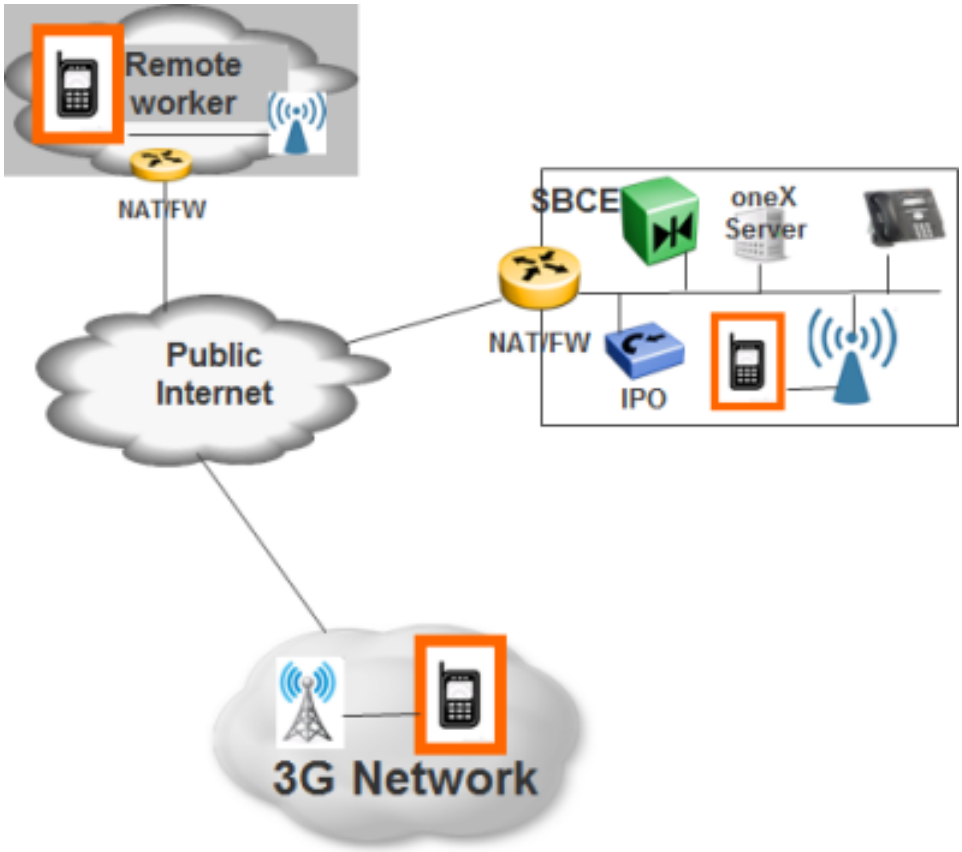
Native IP Office SIP remote worker



With native IP Office SIP remote worker, IP Office and the SIP remote clients exchange the SIP signaling and the media packets. These media packets seamlessly traverse through the remote NAT on remote router, across the public Internet, reach the corporate router, traverse through the corporate NAT on corporate router, and reach IP Office.

You do not need any special configuration on the remote NAT. Functionally, the remote SIP client works exactly as a local SIP client. All telephony features that are supported for the local SIP clients are available for the remote SIP clients.

SIP remote worker with Avaya SBCE



You can deploy the SIP remote worker with Avaya SBCE using the following options:

- Two-wire: 2 SBCE interfaces in DMZ and private network
- Single-wire: SBCE located on the LAN

You must direct port forwarding for SIP signaling ports and media ports to the SBC to allow SIP traffic and media through the SBC. You must configure the rest of the port forwarding rules as in the native SIP remote worker case. IP Office views SBCE remote workers as local users. Hence, you do not require the IP Office SIP remote worker licenses for any remote workers.

You must ensure that the Flare remote workers located behind the SBCE use the alphanumeric SIP domain names instead of IP address when the remote workers are registering with IP Office. You can achieve this by using the appropriate SBCE configuration.

SIP remote worker requirements

The SIP remote worker requirements are as follows:

- Use non-standard SIP listening ports to avoid interference with SIP ALGs.
- Ensure that the administrator configures the port forwarding rules in the NAT or firewall so that remote workers can connect to IP Office or one-X.
- Use the correct forward destination for each port.
- Disable the firewall on the ports that you use.
- To troubleshoot the remote worker connection issues, use the firewall logs of the router.

Seamless roaming

Seamless roaming is an important feature of the *Mobility* and *Flare* clients. Technologies used to support seamless roaming include the DNS and the SIP remote worker.

Advantages include:

- One-time provisioning.
- *Always on* and ever-present supporting mobile workforce.
- Seamless roaming from inside or outside the corporate network without changing the configuration of the mobile phones.

Note:

You cannot have seamless call handoff on roaming.

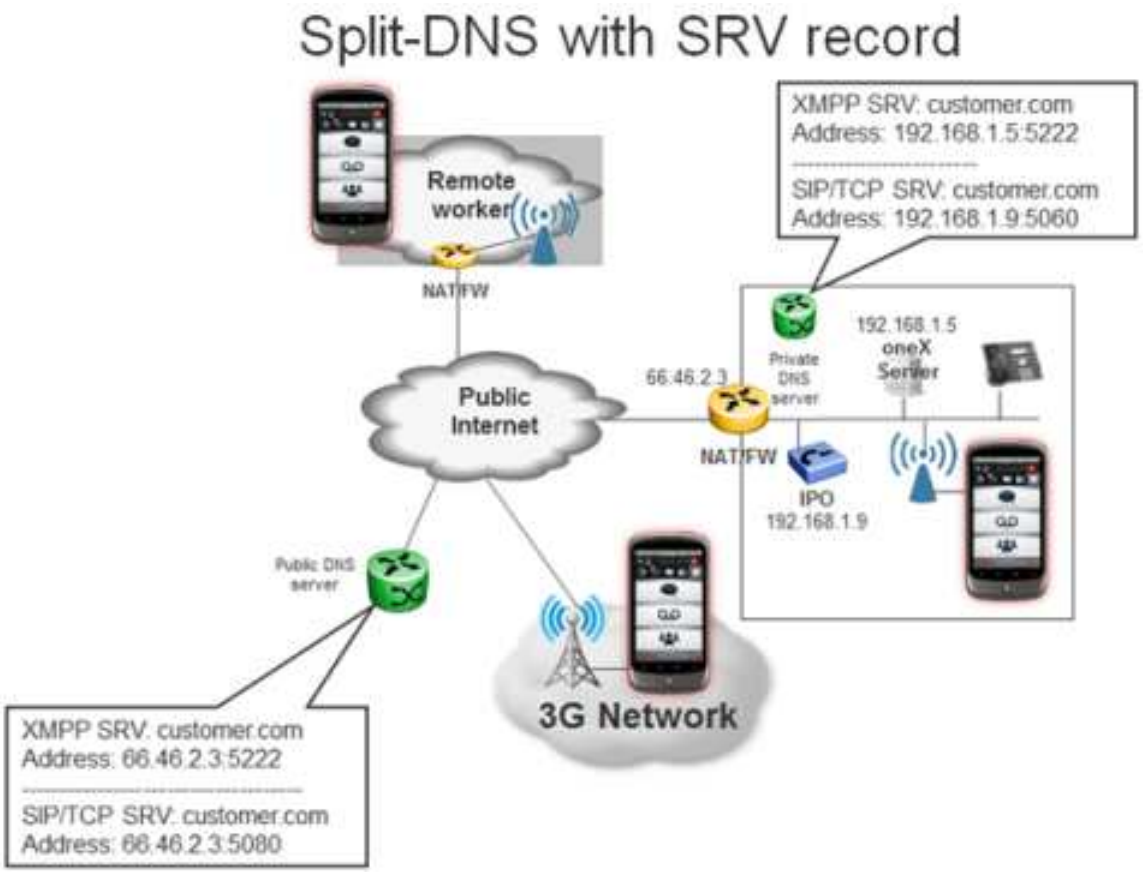
DNS is the vehicle for the seamless roaming of the mobility solution. You can provision clients using the DNS resolvable names. For example, to use the SIP domain in IP Office and the XMPP domain in Avaya one-X® Portal. The clients resolve the DNS names while roaming between networks. These DNS names are registered with the public DNS using DNS *A* or SRV records.

DNS A records:

DNS *A* records are the most basic DNS records and resolve the DNS name to a single IP address. Services such as XMPP and SIP run on standard ports. Separate XMPP and SIP domains are required for IP Office 500v2 with separate one-X, as IP Office and one-X have different IP addresses.

SRV records:

SRV records allow customers to have differentiated resolution of same DNS for services such as SIP, XMPP, and SMTP. Hence, you can use the same DNS name for SIP and XMPP. You can use non-standard ports for SIP and XMPP. You can resolve different services into different IP addresses, such as, one-X versus IP Office.

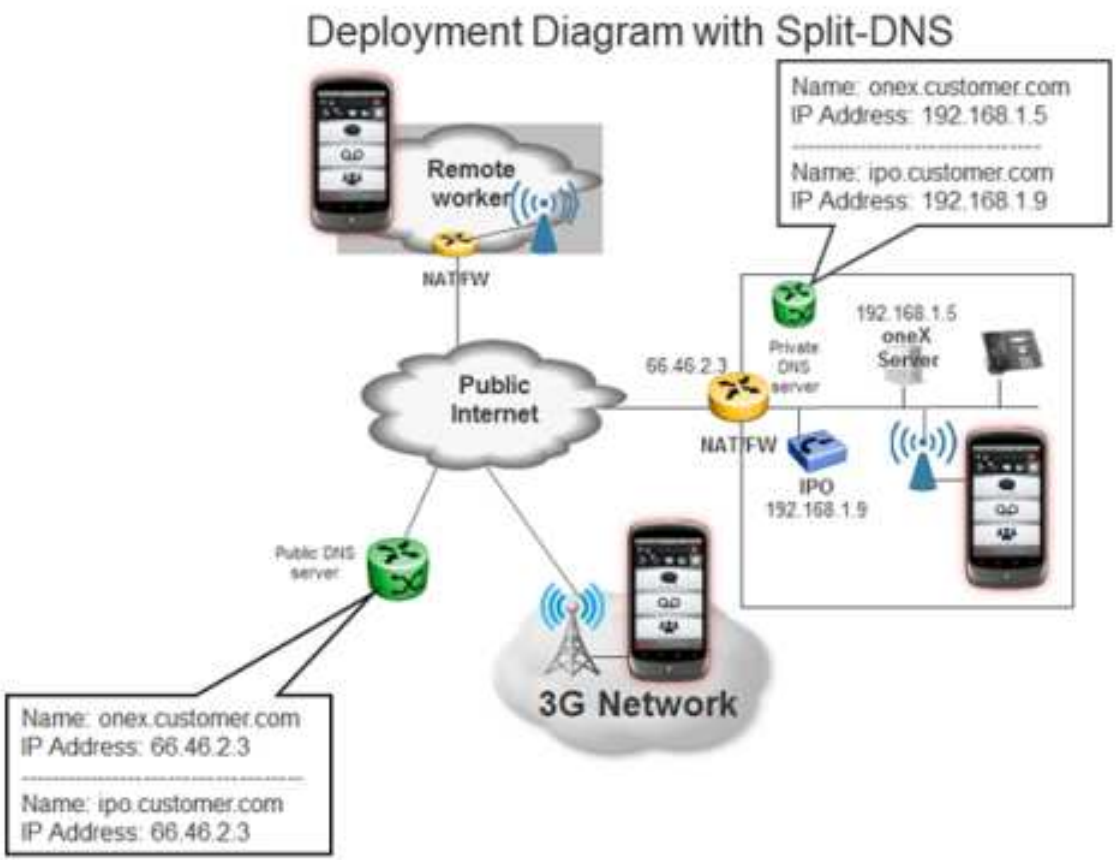


Use Split-DNS for proper operation of clients inside the corporate network:

- Prevent local SIP users from being seen as remote.
- Avoid router hairpinning if supported by router.

  Hairpinning:

  The concept of hairpinning is explained as follows. Configure a phone inside the network with the DNS resolvable name, for example, for IP Office. This name must be resolvable through the public DNS and must point to the public IP address of the router. If inside the network you use the DNS name, the phone attempts to reach IP Office by using the public IP address of the router. The router then realizes that the request is made from inside the network to its own public address on the particular port. The router understands that there is a port forwarding rule and that it has to allow the packet to reach IP Office. This complete process is known as hairpinning.



Split-DNS provides an alternative DNS resolution for public DNS names on a local network. Split-DNS is needed if roaming is used. If roaming is not used, use the local IP address for local non-roaming clients and use the public DNS or public IP address for public-side-only clients.

Use Split-DNS so that local clients can contact IP Office or Avaya one-X® Portal directly and avoid hairpinning. Hairpinning is an issue with the VoIP clients.

Split-DNS requires an *always-on* local DNS server.

Relation between the SIP remote worker and mobility features

Avaya mobility clients such as Flare and one-X mobile can operate as remote workers with the help of the *SIP Remote Worker* feature. Mobility clients can now seamlessly roam between the inside and outside the corporate network.

In the VoIP mode, the mobility client gets an extension and performs all call control features including midcall features. You can choose the call-back mode when Wi-Fi connectivity is unavailable or when the data connection does not provide adequate voice quality.

SIP remote worker license

IP Office controls the SIP remote worker license at a user level. The SIP remote worker license is enabled for users with the appropriate user package, that is, *Teleworker User* and *Power User*.

one-X Mobile Essential edition	one-X Mobile Preferred edition
You can give the non-floating remote worker license to up to four users.	You can give the remote worker license to all *Teleworker Users* and *Power Users*.
You do not have the option to buy an extra license.	For users that are not *Teleworker Users* and *Power Users*, you can give the remote worker license to up to four of these users.

LAN configuration

Configuring LAN settings for remote worker support

Before you begin

- Ensure that LAN1 is on a private network and is behind the corporate router, that is, NAT and firewall.
- Open the Avaya IP Office Manager interface.

Procedure

1. In IP Office Manager, in the left pane, in the navigation list, select **System**.
2. In the right pane, click the **LAN1** tab.
3. Click the **LAN Settings** tab.
4. In the **IP Address** field, type the primary IP address of LAN1.
5. Click the **VoIP** tab.
6. To enable the SIP registration, select the **SIP Registrar Enable** check box.
7. To enable the SIP remote worker on this interface, select the **SIP Remote Extn Enable** check box.

   Note:

   You can select the **SIP Remote Extn Enable** check box on either LAN1 or LAN2, but not both.

8. To provision the SIP domain name, in the **Domain Name** field, type the SIP domain name. For example, *ipo.customer.com*.

   The fully qualified domain name must be resolvable from both the public Internet and the corporate network.

9. In the **Layer 4 Protocol** area, configure the following ports:
   - Select the **UDP** check box, and in the **Remote UDP Port** field, select a free port.

     Note:

     By default, IPO selects port 5060. For security reasons, Avaya recommends you to change the port by selecting a port that does not conflict with any other active port.
   - Select the **TCP** check box, and in the **Remote TCP Port** field, select a free port.

     Note:

     By default, IPO selects port 5060. For security reasons, Avaya recommends you to change the port by selecting a port that does not conflict with any other active port.
   - Select the **TLS** check box, and in the **Remote TLS Port** field, select a free port.

     Note:

     By default, IPO selects port 5061. For security reasons, Avaya recommends you to change the port by selecting a port that does not conflict with any other active port.

   You must add the selected ports to the port forwarding table at corporate router.
10. In the **Port Number Range (NAT)** area, configure the RTP ports for the remote client.
    - In the **Minimum** field, select a port that does not conflict with any other active RTP port.

      Note:

      By default, IPO selects 49152 as the RTP port. For security reasons, Avaya recommends you to change the port by selecting a port that does not conflict with any other active RTP port.
    - In the **Maximum** field, select a port that do not conflict with any other active RTP port.

      Note:

      By default, IPO selects 53246 as the RTP port. For security reasons, Avaya recommends you to change the port by selecting a port that does not conflict with any other active RTP port.

    The H.323 remote worker, the SIP remote worker, and the public SIP trunks share the selected ports. You must add these ports to the port forwarding table at corporate router.
11. Click the **Network Topology** tab.
12. In the **Public IP Address** field, type the public IP address of the corporate router.

    You can identify this address using a public STUN server, or you must manually provision the address.
    - If the public IP address of the corporate router is static, type the IP address manually.
    - If the public IP address of the corporate router is dynamic, complete the details in the **STUN Server Address**, **STUN Port**, **Firewall/NAT Type**, and **Run STUN on startup** fields.

Note:

If you select **H323 Remote Extn Enable** or **SIP Remote Extn Enable**, you cannot enter the IP address as 0.0.0.0. Also, if you save the value in the **Public IP Address** field as 0.0.0.0, then local NAT traversal is not supported.

13. Click the **DNS** tab.
14. To provision the corporate DNS server, in the **DNS Server IP Address** field, type the corporate DNS server IP address.
15. Click **OK**.

Corporate router configuration

Service	Port number	Transport protocol	Forward to	Comments
SIP	5060 5061	TCP or UDP TLS	IP Office	Port number depends on **IP Office Manager** > **LANx** > **VoIP** > **SIP Registrar Enable** > **Remote UDP/TCP/TLS Port**.
RTP	54000-54500	UDP	IP Office	Port number depends on **IP Office Manager** > **LANx** > **VoIP** > **Port Number Range (NAT)**.
H.323	1719-1720	TCP	IP Office	Port number depends on **IP Office Manager** > **LANx** > **VoIP** > **H.323 Gatekeeper Enable** > **H.323 Remote Extn Enable**.
HTTP	80	TCP	IP Office	
Avaya one-X® Portal or XMPP	5222, 8080, 8063, 8443, and 9443	TCP	The Avaya one-X® Portal server	

Home router configuration

Ensure that you turn on *NO SIP-ALG*.

Avaya one-X® Portal server configuration

In the Administrator interface of Avaya one-X® Portal, configure the XMPP domain. For more information, see Configuring the XMPP domain on page 16.

The fully qualified domain name must be resolvable using the local DNS or the public service.

DNS server resolution

Public DNS Service must provide resolution for:

- Public IP address of the WAN interface of IP Office
- Public IP address of the corporate router
- SIP registration TCP port for remote SIP extension
- SIP registration UDP port for remote SIP extension
- SIP registration TLS port for remote SIP extension

Private DNS service must provide resolution for:

- Primary IP address of the LAN interface of IP Office
- Local IP address of the corporate router
- SIP registration TCP port for local SIP extension
- SIP registration UDP port for local SIP extension
- SIP registration TLS port for local SIP extension

WAN configuration

Configuring WAN settings for remote worker support

Before you begin

- Ensure that LAN1 is on a private network and is behind the corporate router, that is, NAT and firewall.
- On LAN1, clear the **SIP Remote Extn Enable** check box.
- On LAN1, disable the remote UDP, TCP, and TLS ports.
- Configure the SIP domain name for LAN1. For example, *ipo.customer.com*.
- Open the Avaya IP Office Manager interface.

Procedure

1. In IP Office Manager, in the left pane, in the navigation list, select **System**.
2. In the right pane, click the **LAN2** tab.
3. Click the **LAN Settings** tab.
4. In the **IP Address** field, type the primary IP address of LAN2.

   LAN2 is directly on DMZ and has a public IP address that you can reach from the Internet.
5. Click the **VoIP** tab.

6. To enable the SIP registration, select the **SIP Registrar Enable** check box.
7. To enable the SIP remote worker on this interface, select the **SIP Remote Extn Enable** check box.

   Note:

   You can select the **SIP Remote Extn Enable** check box on LAN1 or LAN2, but not both.
8. In the **Domain Name** field, configure the SIP domain name. For example, *ipo1.customer.com*.

   If you select the **SIP Registrar Enable** check box for both LAN1 and LAN2, the SIP domain names must be identical.
9. In the **Layer 4 Protocol** area, configure the following ports:
   - Select the **UDP** check box, and in the **Remote UDP Port** field, select **5060**.
   - Select the **TCP** check box, and in the **Remote TCP Port** field, select **5060**.
   - Select the **TLS** check box, and in the **Remote TLS Port** field, select **5061**.

   Note:

   You must add these ports to the port forwarding table at corporate router.
10. In the **Port Number Range (NAT)** area, because you do not require local NAT traversal in this setup, the original RTP port number range is used for all media on this interface, that is, **Minimum** is *49152* and **Maximum** is *53246*.
11. Click the **Network Topology** tab.
12. In the **Public IP Address** field, type the address as 0.0.0.0.

    Configure the *Public IP Address* of LAN2 as the primary IP address. In this setup, the SIP clients on public Internet, for example on DMZ, are not considered remote and do not require the remote worker license. Only those clients behind their own home router are considered remote clients and subject to the remote worker license. Because local NAT traversal is not required in this setup, you can set the value in the **Public IP Address** field as 0.0.0.0.
13. Click **OK**.

Corporate router configuration

Service	Port number	Transport protocol	Forward to
Avaya one-X® Portal	8080	TCP	Avaya one-X® Portal server
Avaya one-X® Portal	8063	TCP	Avaya one-X® Portal server
XMPP	5222	TCP	Avaya one-X® Portal server

Home router configuration

Ensure that you turn on *NO SIP-ALG*.

Avaya one-X® Portal server configuration

In the Administrator interface of Avaya one-X® Portal, configure the XMPP domain. For more information, see Configuring the XMPP domain on page 16.

The fully qualified domain name must be resolvable using the local DNS or the public service.

DNS server resolution

Public DNS Service must provide resolution for:

- Public IP address of the WAN interface of IP Office
- Public IP address of the corporate router
- SIP registration TCP port for remote SIP extension
- SIP registration UDP port for remote SIP extension
- SIP registration TLS port for remote SIP extension

Private DNS service must provide resolution for:

- Primary IP address of the LAN interface of IP Office
- Local IP address of the corporate router
- SIP registration TCP port for local SIP extension
- SIP registration UDP port for local SIP extension
- SIP registration TLS port for local SIP extension

Certificates

Generating a certificate

Procedure

1. To generate a certificate for IP Office, in the Application Server Web Control, navigate to **Settings** > **General** > **Certificates**.

2. To generate a certificate, in the Certificate Settings area, perform one of the following:
   - For IPO 500 V2 server machines, select the **Create certificate for a different machine** check box.
   - For IPO Server Edition machines, clear the **Create certificate for a different machine** check box.
3. In the **Machine IP** field, type the IP address.
4. In the **Password** and **Confirm Password** fields, type the password.
5. In the **Subject Name** field, type the host name.

   Note:

   The host name should match the XMPP domain name configured in Avaya one-X® Portal.
6. **(Optional)** In the **Subject Alternative Name(s)** field, you can change the Subject Name and Machine IP details.

   Note:

   By default, the application populates the Subject Name and Machine IP in the **Subject Alternative Name(s)** field.

   Important:
   - If the XMPP domain is configured with proper DNS domain name, then the XMPP domain name must match Subject name or DNS field in the alternative subject names.
   - If the XMPP domain is configured with IP address, then the XMPP domain name must match the Subject name or IP field of the Subject alternative names
7. Click **Generate**.

   The system displays a Warning dialog box.
8. In the Warning dialog box, click the link and save the certificate.

Importing certificate

About this task

Use this task to import a certificate in IP Office Manager.

Procedure

1. To import the certificate in IP Office Manager, navigate to **Advanced** > **Security Settings** > **System** > **Certificates**.
2. Click **Set**.

   The system displays a Certificate Source dialog box.

3. In the Certificate Source dialog box, select **Import certificate from file**.
4. Browse and select the certificate.
5. Click **Open**.

   The system displays a Password dialog box.
6. In the **Enter your password** field, type the password you created in the Application Server Web Control.
7. Click **OK** twice.
8. Click the save icon .

Configuring remote SIP clients

Procedure

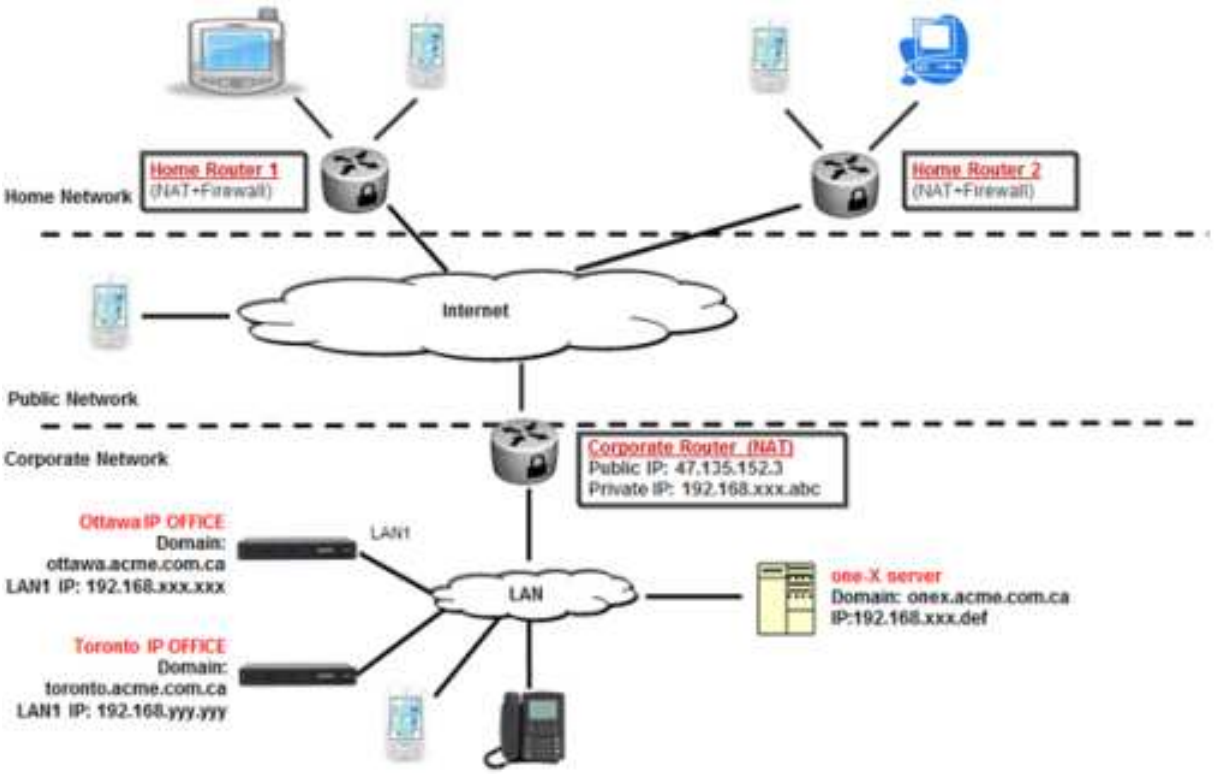
For the iOS or Android clients, in the Settings screen, in the **Server ID** field, type the domain name of the Avaya one-X® Portal server.

Configuring mobility VoIP and XMPP ports for multiple IP Office servers

About this task

You might have a configuration wherein there are multiple IP Office servers in the same private network with mobility users on both IP Office servers.

In the following example, there are two IP Office servers in the same private network with a single one-X server all behind a single router.



The sample configuration is as follows:

Procedure

1. For each IP Office server, in IP Office Manager, in **System** > **LAN1** > **VoIP** configure the following:
   - Configure the Ottawa office with the **Remote UDP Port** as 5070 and **Port Number Range (NAT)** range as 54100 to 54199.
   - Configure the Toronto office with the **Remote UDP Port** as 5072 and **Port Number Range (NAT)** range as 54200 to 54299.
2. In the **Domain Name** field, configure a unique SIP domain name for each IP Office.
   - For Ottawa office, ottawa.acme.com.ca.
   - For Toronto office, toronto.acme.com.ca.

   If you want mobility users to roam, that is, Wi-Fi to 3G or 4G and vice-versa, with mobile phones, the IP Office domain names must be resolvable from the public Internet. If needed, use Split-DNS to resolve the domain names when using local Wi-Fi.
3. Configure the router with the port forwarding rules:
   - VoIP SIP Registration:
     - Port 5070 forward to 192.168.xxx.xxx, Ottawa IP Office
     - Port 5072 forward to 192.168.yyy.yyy, Toronto IP Office

- For VoIP SIP RTP speech:
  - Ports 54100 to 54199 forward to 192.168.xxx.xxx, Ottawa IP Office
  - Ports 54200 to 54299 forward to 192.168.yyy.yyy, Toronto IP Office

4. Open XMPP ports 5222 and 8443 and forward to the one-X server IP address.

Chapter 6: Troubleshooting

Troubleshooting the Avaya one-X® Mobile Preferred client

Connectivity

Error messages

An icon in the Status bar of the one-X Mobile Preferred application displays the status of the connection to IP Office. When the application disconnects from the Avaya one-X® Portal server, the icon turns red. A red or yellow icon indicates a connection issue. Users can press the *Trouble* icon to view a popup that displays more information on the problem.

If you cannot register the one-X Mobile Preferred application using VoIP, the phone icon turns gray.

The following table lists the error messages and the possible causes of the error.

Problem	Reason
Unknown server	The configured server cannot be resolved through DNS.
Server unreachable	Avaya one-X® Mobile cannot contact the server using the configured server name and port.
Server request timeout	The connection to the configured server on a specified port timed out.

Problem	Reason
Invalid user credentials	The configured user name or password is incorrect.
User has no XMPP account	The one-X Mobile Preferred client contacted the server to retrieve the XMPP account information and found that the user has no active XMPP account.
Failed to retrieve XMPP account information	The one-X Mobile Preferred client contacted the server to retrieve the XMPP account information and was unable to complete the operation.
Network is unavailable	The connection to the server failed because the network is unavailable on the mobile phone.
XMPP connection is unavailable	The client was unable to establish or maintain an XMPP connection to the server.
You don't have a conference configured on the server	The user attempting to initiate the conference does not have a valid conference bridge number. You must configure the bridge number in the Avaya one-X® Portal Web page in **Configure > Telephony > Conference Bridge Number**.
A call made via enterprise dialing is dropped	Because of a delay in the network, the service provider call-answer settings took effect prior to the IP Office **No Answer Time (secs)** setting.
A call made via enterprise dialing goes to the service provider's voice mail instead of IP Office voice mail	The **No Answer Time (secs)** setting in IP Office is set too high, such that the service provider voice mail settings took effect first.
Invalid Server Certificate	Failed server certificate validation attempt results in this error message.
iPhone one-X Mobile Preferred client fails to connect despite providing the correct credentials and the server domain is reachable	Ensure that the XMPP domain is not 127.0.0.1 and you configure the correct domain. For more information, see Configuring the XMPP domain on page 16.

Troubleshooting connection issues

When the one-X Mobile Preferred client is disconnected from IP Office, the one-X Mobile Preferred client attempts to establish a connection in the background. Use the following list to troubleshoot connection problems if the application cannot connect to IP Office.

- Ensure that the user has an appropriate license.
- Verify that the following TCP ports are open: port 5222 and port 8444. Port 5222 is for XMPP traffic and port 8444 is for bootstrap REST API call traffic.
- Verify that the FQDN resolves to the correct IP address.
- If Avaya one-X® Mobile can connect when the user is on a cellular network, but cannot connect on an internal Wi-Fi network, verify that your router supports packet hair-pinning. If the router does not support packet hair-pinning, deploy a split DNS solution to resolve the problem.
- Ensure that the **Server certificates** check box is not selected in the client settings.

Making calls

Calls to or from external locations

When a user initiates a call through the one-X Mobile Preferred client, the application signals IP Office to call the user at the location set in Avaya one-X® Mobile. After the user picks up the telephone at that location, IP Office dials the number that the user wants to reach. This approach means that calls route through the enterprise PBX. External telephone numbers must therefore meet any enterprise dialing requirements. For example, some external calls require the user to dial **9** before the number.

If the user location is set to an external phone number or if the user is trying to reach an external number and cannot make a call, verify the following:

- Check whether the number has the correct dialing prefix.
- Check whether the dial plan configuration in IP Office is correct.
- Check whether a dial plan rule is configured in Avaya one-X® Mobile. If not, determine whether you must configure a dial plan rule in the application.
- Check whether the user has the necessary permissions to call that number.

Call status

In one-X Mobile Preferred, the user can view whether the contacts are on the deskphone. However, the status might appear incorrect if a contact is on a call using a home or a mobile phone. Contacts using a home or a mobile phone might not appear as on the deskphone.

Enterprise dialing

You might have issues with dropped calls or calls forwarding to an undesired voice mail if you use enterprise dialing. The reason is that twinned calls have to account for network delays.

A user with **No Answer Time (secs)** set to 15 seconds or less might experience dropped calls where the service provider has configured a shorter or equivalent no-answer time. In this case, because of a delay in the network, the service provider call-answer settings take effect prior to the IP Office **No Answer Time (secs)** setting.

Similarly, if **No Answer Time (secs)** is set for too long, for example, 50 seconds, this might give the service provider voice mail the time to activate prior to IP Office voice mail. Hence, a call made using enterprise dialing goes to the voice mail of the service provider instead of IP Office voice mail.

Service providers vary based on location, and network delay times vary between providers, so you must ensure that you set an appropriate delay.

Voice mail

If a user cannot play voice mail messages on Avaya one-X® Mobile, use the following list to troubleshoot the cause of the problem.

- Verify that Avaya one-X® Portal includes the IP address of the Voicemail Pro server. To view the list of providers, from the Administrator interface, select **Configuration** > **Providers** and click **Get All**.

- If Avaya one-X® Portal and Voicemail Pro are installed on separate servers, verify that Avaya one-X® Portal can resolve the domain name or the computer name of the Voicemail Pro server.

Instant messaging

Presence

If the presence of a user displays incorrect information, verify whether the user has logged in to multiple XMPP clients simultaneously. For example, user logs in to Avaya one-X® Mobile and Avaya one-X® Portal simultaneously.

If a user logs in to multiple XMPP clients, the application displays the presence information for that user on the last logged in client to other users. For example, if a user logs in to Avaya one-X® Mobile and has a presence of **Away**, and then also logs in to Avaya one-X® Portal with a presence of **Available** then the user status reads **Available**, being the most recent.

Receiving instant messages

Avaya one-X® Mobile incorporates the *Shared presence* feature of IP Office that synchronizes all Avaya XMPP clients with respect to user presence. As a result, when a user sends an instant message, the recipient receives the message at all Avaya IM clients, regardless of presence.

For example, if a user logs in to Avaya one-X® Mobile and has a presence of **Away**, and also logs in to Avaya one-X® Portal with a presence of **Available**, that user receives instant messages at both locations.

After receiving an instant message, the application sends the reply to the location of the originating message, regardless of presence. However, if the client for the originating message is offline, then the application sends the reply to all online clients in use by the originator. If all clients are offline, the originator receives the message when the originator comes online on a client.

If the originating message comes from a third-party XMPP client, such as Softphone, the presence of the originator might be independent of other clients and not shared. In this scenario, the application sends the reply to the client where the presence indicates the best availability.

Ensure that users manage presence information correctly and ensure that users log out of applications that are not in use. The presence setting on any XMPP client must be an accurate reflection of the user presence at that client.

Geo-presence

When you enable geo-presence in Avaya one-X® Mobile, the mobile phone provides the location information using GPS signals. If the location information is incorrect, verify the following:

- Check if the user is within the GPS signal range.

  Move within range of the GPS signals, such as near a window or outside a building, to update the geo-presence information.

- Check the level of detail that the user is publishing.

When the user sets **Location Precision** to **City**, **Neighborhood,** or **Street**, the application uses cloud-based services to obscure the location information and display only the precision level that you want. Depending on the network or service conditions, the cloud-based service might not respond and geo-presence information might not update as a result. These conditions are rare and usually temporary. If the condition continues, to avoid the use of cloud-based services, set **Location Precision** to **Maximum**.

Note:

The battery consumption on mobile phones increases if you use geo-presence.

Logs

The Avaya one-X Mobile Preferred client collects and submits logs to the Avaya one-X® Portal server when a Wi-Fi or 3G data connection is available.

Note:

By default, the application disables logging. If you enable logging, the battery consumption on mobile phones increases. Enable logging only if instructed by support personnel.

If a user submits logging information, the location of the log depends on the operating system in use by the mobile phone.

Every time the application shuts down abnormally, the application sends logs and backtraces to Avaya without requiring any user action. The application uploads the information over Wi-Fi if the user configures the Wi-Fi settings on the application. Avaya receives notifications of new reports hourly through email.

The application transfers all logs over an encrypted channel and strips the password information. The End User License Agreement (EULA) of the application includes information on log transfers to Avaya.

Application logs include a lot of information. You can isolate the error log entries by running the **`grep 'E/ScsCommander' <name of log file>`** command.

Submitting logs on Android mobile phones

Log settings are available on the Android mobile phones in the **Menu** > **Settings** > **Advanced** menu. You can direct users to provide the following information:

Menu items	Description
Submit Problem Report	The option to submit the problem report about the application to technical support.
Logging Settings	The options to set logging information that technical support personnel can use. The options are: • **Logging Level:** The option to select the level of logging.

Menu items	Description
	• **Log limit (MB):** The option to specify the size limit for the logs. The default is *16* MB. • **XMPP Debugging:** The check box to enable or disable additional XMPP debugging.
File Transfer Options	The following file transfer options are available when you submit information to technical support: • **Wi-Fi Only:** The check box to enable or disable Wi-Fi use for transfer of all files. • **Pending file transfers:** The option to view the number of pending file transfers and delete the transfers that are pending.

Procedure

On the mobile phone, select **Menu** > **About** > **Log Upload**. The one-X Mobile Preferred client submits the log to the following locations:

- If you are running Avaya one-X® Portal on a Linux server, the path is: `/opt/Avaya/oneXportal/x.x.x_xxx/apache-tomcat/logs/smack-file-transfer`, where x.x.x_xxx is the version of Avaya one-X® Portal server.

  The log name is in the format `logs_217_11_08_17_15_47_55.zip`, where **217** is the user, then the date, and time when you took the logs.

- If you are running Avaya one-X® Portal on a Windows server, the path is: `\Program Files (x86)\Avaya\oneXportal\Tomcat\Server\logs\smack-file-transfer`

  Note:

  To troubleshoot connectivity issues, you can install a file manager application, such as OI File Manager. Use the file manager application to send the logs directly from the mobile phone using email to the Avaya server in the cloud. Avaya receives notifications of new reports hourly through email.

- If Wi-Fi or 3G connection is unavailable, the Android mobile phone stores the logs locally in the `Android/data/com.avaya.ScsCommander/files/staging` path.

Submitting logs on Apple mobile phones

Log settings are available on the iPhone mobile phones in the **Menu** > **Settings** > **Mobile** > **Logging** menu. You can direct users to provide the following information:

Menu items	Description
Verbose Logging	Turn **ON** to troubleshoot any issue.
Support Email	The support email address where you can send the logs.
Version	The version of the application.

Procedure

1. On the mobile phone, select **System Messages > Report Problem**.

   The **System Messages** icon resembles a bell in the status bar.

   The one-X Mobile Preferred client consolidates the logs and submits the logs by email.
2. Enter a valid email address with a descriptive subject, and tap **Send**.

   Note:

   If the client shuts down abnormally, the **System Messages** menu includes a notification for you to send an event log.

Using openfire Web console

Use the openfire Web console solution to check XMPP accounts, rosters, server properties, current XMPP sessions, and more.

By default, the openfire Web console is disabled.

1. In the Avaya one-X® Portal installation folder, open the **openfire** > **bin** folder.
2. Configure the following:
   - To enable on Windows: `AdminConsoleManager.bat enable`
   - To disable on Windows: `AdminConsoleManager.bat disable`
   - To enable on Linux: `./AdminConsoleManager.sh enable`
   - To disable on Linux: `./AdminConsoleManager.sh disable`
3. Restart the Avaya one-X® Portal server.
4. Gain access to the openfire Web console by entering `http://<host>:9094` in a Web browser.
5. Use the following credentials to log in:
   - **Username:** admin
   - **Password:** admin

   Note:

   Do not add a port forwarding rule for 9094.

Troubleshooting the Avaya one-X® Mobile Essential client

The one-X Mobile Essential client relies on DTMF to issue commands to IP Office, so the troubleshooting options are few. If a feature name extension is not working as intended, use the following procedure.

If the following procedure does not resolve the issue, you might need to reinstall the application and try again. Also, verify that the hardware components are functional.

Procedure

1. Dial the DDI Line for the corresponding feature.
2. Perform the DTMF commands as needed.
   - If successful, double-check your configuration parameters.
   - If unsuccessful, double-check the Mobile Call Control settings in IP Office.
   - If all else fails, uninstall and then reinstall the application.

Troubleshooting VoIP issues

Procedure

Perform the following checks to troubleshoot VoIP issues:

- Use SysMonitor (Avaya IP Office SysMonitor) SIP Phone Status to check the SIP registrations.

- Use the Android and iPhone client to check the registration error messages.
- Use the Android client details dialog box:
  - Check if the RX/TX counters are running.

- If the Android client is local, the local IP address of IP Office must be *Remote*.
- If the Android client is remote, the public IP address of IP Office of the corporate router must be *Remote.* Also, the remote ports must be from the RTP port range.

Index

R

S

T

U

V

W

X