



Avaya one-X Mobile Preferred for IP Office Administration Guide

01.02
March 2012

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

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

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya 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). End User 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). Customer 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"). (see "Third-party Components" for more information).

Copyright

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

the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

Contents

Chapter 1: Getting Started.....	7
Overview.....	7
System requirements.....	9
Chapter 2: Configuration.....	11
Configuring the XMPP domain.....	11
Configuring users.....	11
Configuring the connection to the Microsoft Exchange server.....	13
Configuring calendar access.....	14
Chapter 3: Troubleshooting.....	17
Connectivity.....	17
Making calls.....	18
Voicemail.....	19
Instant messaging.....	19
Geo-presence.....	20
Viewing logs.....	20
Index.....	23

Chapter 1: Getting Started

Overview

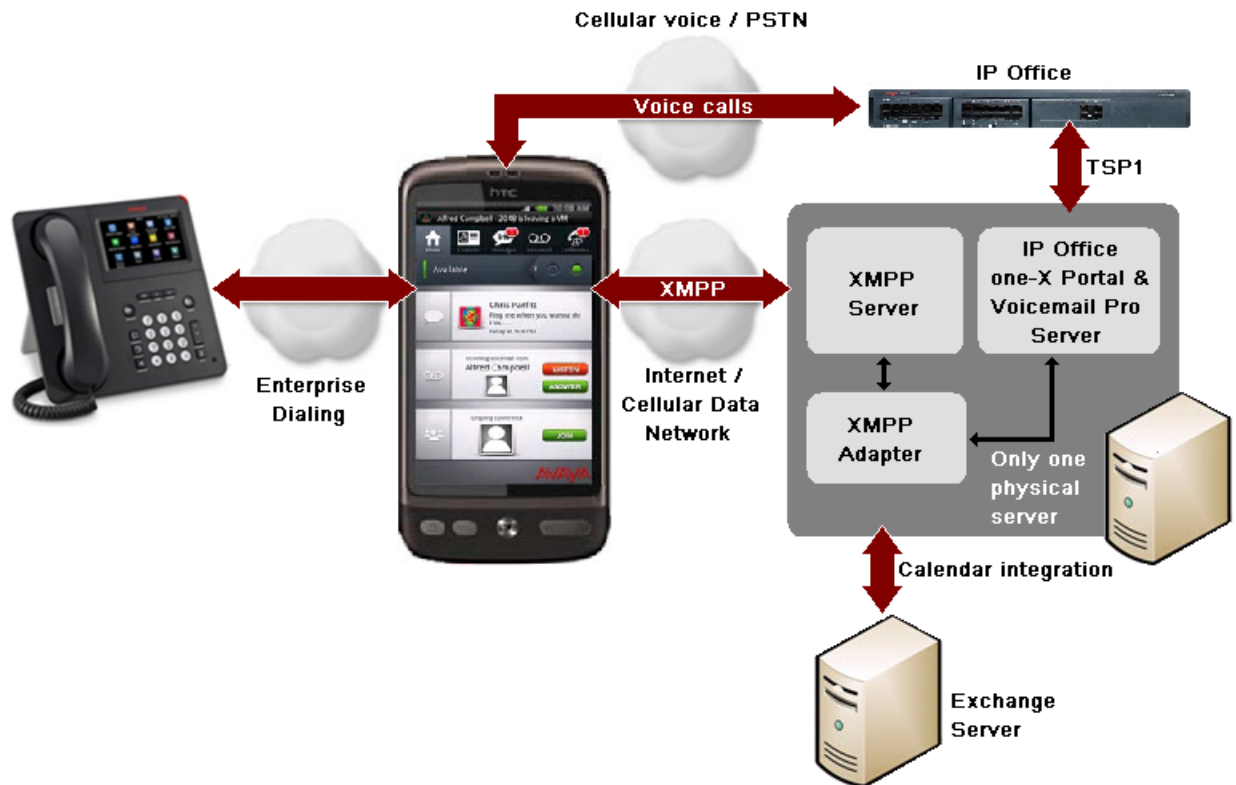
The Avaya one-X Mobile Preferred for IP Office is an application that works with the IP Office suite to provide enterprise communications on mobile devices. It is only supported on IP Office release 8.0 and is not supported by earlier releases. The application provides enterprise calling, messaging, voicemail, and conferencing. These capabilities allow the corporate communication network to be seamlessly extended to the mobile phones of employees. The one-X Mobile features include:

- enterprise dialing and dial plans
- presence information for the user and for the user's contacts
- geo-location presence and tracking using the on-board GPS of the mobile device
- instant messaging with contacts and user groups defined on the IP Office server, as well as with external contacts
- visual voicemail with the ability to play voicemail messages, pick-up incoming voicemail messages, view the current presence of the voicemail caller, and return calls
- rich conference controls with click-to-conference for users and groups, entry and exit notifications, and the ability to view and manage conference participants
- integration with the Microsoft Exchange Server to provide information about the availability of users
- real-time notifications of communications arriving on the server, such as new voicemail or instant messages, changes in the availability of contacts, and conference participants dialing into user's conference bridge

System architecture

The system architecture integrates the Avaya one-X Mobile with IP Office and its applications and to deliver enterprise communications to mobile devices.

The diagram below demonstrates how the Avaya one-X Mobile allows users to leverage your existing corporate infrastructure from a mobile device.



For example, the diagram shows how users can make enterprise calls from their mobile devices. Long-distance or international numbers can be dialed on the mobile device, and routed through the Avaya PBX.

In addition, users only need to use the Contacts list to remain connected. The Contacts list is pushed to the mobile device from the IP Office server; there is no need for users to configure their Contacts list, and when employees are out of the office, everyone can remain connected and reachable. Corporate voicemail is also integrated on the one-X Mobile application.

The architecture uses the XMPP server that is integrated with the one-X Portal and the Microsoft Exchange Server to extend several capabilities to the mobile worker:

- the integration with the XMPP server allows corporate instant messaging and presence information to be available to mobile users
- the integration with the Microsoft Exchange Server allows users to view calendar information about their Contacts, and provide their own Calendar information to other users

Supported platforms

The one-X Mobile is available for Apple and Android mobile devices. It is supported on the following devices:

- devices with Android operating system 2.1 and above
- iPhones with iOS4 and iOS5 operating systems

Related documentation

Because the Avaya one-X Mobile is integrated with IP Office and its applications, you will need access to the IP Office documentation suite to administer this application. The following related documents are available on the Avaya Support website, at www.avaya.com/support:

- *IP Office Application Server Installation and Maintenance* (for Linux deployments only)
- *IP Office Manager*
- *Administering the one-X Portal for IP Office*
- *Installing one-X Portal for IP Office*
- *Implementing Voicemail Pro*

System requirements

The one-X Mobile Preferred for IP Office is a mobile application that is fully integrated with IP Office and its applications. This integration allows remote users to keep in touch with enterprise voicemail, instant messaging, and conferencing. When you deploy one-X Mobile Preferred as part of an IP Office solution, the system requirements depend on the type of server where the IP Office applications, such as the one-X Portal and Voicemail Pro, are installed. You can deploy IP Office applications on Windows Servers 200x, or Linux servers. The sections below outline the requirements for each operating system, as well as the overall network requirements.

Windows operating systems

IP Office applications are supported on Windows Server 2003 or Windows Server 2008.

If you are using a Windows server, you must install the following applications:

- one-X Portal
- Voicemail Pro with the Web Voicemail component installed. For information about how to install the Web Voicemail component, see “UMS Web Services” in the manual *Implementing Voicemail Pro*.

Linux operating systems

If you are using a Linux server, you must install the following applications:

- IP Office Application Server
- one-X Portal
- Voicemail Pro

The 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 installed is CentOS 5, a Linux operating system.
- The IP Office Application Server is configured and managed remotely using web browser access.
- The one-X Portal for IP Office application is configured and managed remotely using web browser access.
- 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 the IP Office Application Server. Voicemail Pro is required by the one-X Mobile application.

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

Licensing

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

- Preferred Edition with Mobile Worker or Power User license for each client

Network requirements

The Avaya one-x Mobile application must be able to connect from the Internet to the one-X Portal and to the IP Office system, using either using a 3G network or an external WiFi service. Your network setup must support this capability.

If the one-X Portal and IP Office will be deployed behind a router or firewall, the following TCP ports need to be allowed access through the firewall:

- ports 5222 and 8444 must be open in order for the one-X Mobile application to communicate with the one-X Portal server; port 5222 is for XMPP traffic and port 8444 is for bootstrap REST API call traffic
- port 5269 needs to be open for the one-X Portal server to be able to federate with another XMPP server outside the company firewall

In addition, an FQDN that is resolvable over the Internet must be assigned to the public IP address of the router that is fronting the one-X Portal. That router must be configured to forward packets destined to ports 5222, 5269 and 8444 to the one-X Portal; you can achieve this by creating port forwarding rules on the router.

You must ensure that your network meets these requirements before you deploy the one-X Mobile application.

Chapter 2: Configuration

Configuring the XMPP domain

Use the following procedure to configure the XMPP domain that will be used by Avaya one-X Mobile application.

Before you begin

Perform this procedure from the Administrator interface of the one-X Portal.

Procedure

1. Choose one of the following options:
 - If you are launching the one-X Portal for the first time, a wizard displays. In the wizard, choose **Advance > IM /Presence Server**.
 - If you are not using the wizard, select the **Configuration > IM/Presence**.
 2. In the **XMPP Domain Name** field, enter the FQDN that the Avaya one-X Mobile application will use to register to server.
 -  **Note:**
The FQDN must be reachable from the internet if you wish to use the one-X Mobile application outside of your WLAN. Avaya recommends that you use a split DNS so that the server name outside of your WLAN is resolved into the public IP address of the NAT or firewall. The server name inside your network is resolved into the private IP address on the LAN.
 3. Click **Save**.
 4. Restart the one-X Portal server.
-

Configuring users

Use the following procedure to configure the IP Office users who will use the Avaya one-X Mobile application.

Before you begin

Perform this procedure on the Avaya IP Office Manager interface.

Procedure

1. In Manager, select **User** in the navigation list and click the **User** tab.
2. In the **Name** field, enter a name or extension number; this is the name that users will enter in the Username field of the one-X Mobile application. The name can be up to 15 characters in length.
The name that you enter in this field is also used for caller display and voicemail.
3. In the **Password** field, enter a password and re-enter it in the **Confirm Password** field.

 Note:

The Mobility Server will not allow connections from a Mobility Client that does not have a password configured. If the IP Office user has been setup without a password then that person's extension number must be entered in the Mobility Client in the **Password** field.

4. Enter the first and last name of the user in the **Full Name** field.
The name that you enter in this field is displayed in the Contacts list in the one-X Mobile application.
5. Select the option to **Enable one-X Portal Services**.
6. **Optional:** For enterprise dialing purposes, access Call Settings and re-configure a **No Answer Time** (we recommend between 20 and 25 seconds; see Note below).

 Note:

Calls made via enterprise dialing have to account for network delays. As such, a user with a **No Answer Time** set to 15 seconds or less might experience dropped calls since the user's server provider might have a shorter (or equivalent) no-answer time and network delays have caused the user's default **No Answer Time** to be delayed. Similarly, a **No Answer Time** that is set for too long (for example, 50 seconds) could allow time for the server provider's voicemail to activate instead of IP Office's voicemail. Since server providers vary based on location, and network delay times vary between providers, ensure that you have an appropriate delay.

7. Click **OK** to save the changes.
To allow a user to connect to the Preferred Mobility Client, choose one of the following profiles (with the associated licenses applied):
 - Mobile user
 - Power user

*** Note:**

The 'Basic user' profile will not allow the Preferred Mobility Client to register.

Configuring the connection to the Microsoft Exchange server

To provide calendar information to one-X Mobile users, you must first configure the connection between the one-X Portal and the Microsoft Exchange server.

Before you begin

If the one-X Portal and the Microsoft Exchange Server are in the same Windows domain, you must enable digest authentication on the Microsoft Exchange Server before you begin this procedure. For information about how to enable digest authentication, see the procedures in the *Installing one-X Portal for IP Office* manual.

About this task

The one-X Portal connects to Microsoft Exchange using Exchange Web Services, logging into Exchange using a service account that has the required permissions to query users' calendar information. The name of the service account is AvayaAdmin, and the account must have impersonation rights.

Impersonation rights are the permissions given to the AvayaAdmin account to access into the database of Exchange server for information about users; it then passes such information to one-X Portal when the one-X Portal requests it.

In the following procedure, you will configure the AvayaAdmin account on the exchange server, and configure impersonation rights to the AvayaAdmin account. You will need access to both the Exchange Server and the one-X Portal to complete this procedure.

Procedure

1. On the Exchange server, create a new mailbox called **AvayaAdmin**.
2. Login to the one-X Portal as the administrator, and click **Configuration** in the left navigation pane.
3. Click **Exchange Service**.
4. Click on **Download Powershell script** at the bottom of the one-X portal Exchange Service page 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 executes the `avaya.ps1` powershell script, which adds the required Exchange permissions to the AvayaAdmin service account.

6. On the one-X portal **Exchange Service** page, enter the following information:
 - Enter **AvayaAdmin** for the service account.
 - 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 a port number of **6669**.
 - If your company uses an HTTP proxy and the Exchange server is located outside of your company, enter the IP address of the HTTP proxy servers or the domain name and proxy port number.
7. Click **Save**.
8. Click **Validate Exchange Service Configuration** to test the configuration.

The test results display in the box above the button. If the configuration is successful, the following results display: "The Exchange Service Configuration is valid. The Exchange server is reachable. The Service account has impersonation rights."

Next steps

After you have configured the integration between the Exchange Server and the one-X portal, you must configure calendar access for each user. See [Configuring calendar access](#) on page 14 for more information.

Configuring calendar access

You can configure the one-X Portal to update users' presence with calendar meeting and appointment information based on information from the Microsoft Exchange Server; the information is then made available to the one-X Mobile application.

Before you begin

Before you can configure this feature, you must configure the Microsoft Exchange Server. See [Configuring the connection to the Microsoft Exchange server](#) on page 13 for more information.

About this task

Use the following procedure to configure calendar access for each user. Perform this procedure on the IP Office Manager interface.

Procedure

1. Log into Manager as an administrator.
2. In the left navigation pane, select the **User** that you wish to configure.

3. Select the **Voicemail** tab and in the **Voicemail Email** field, enter the Exchange email address for that user.
 4. Click **OK**.
-

Chapter 3: Troubleshooting

Connectivity

Error messages

An icon in the Status bar of the one-X Mobile application shows the status of the connection to IP Office. When the application is disconnected from the one-X Portal server, the icon turns red. Users can press the icon to view an error message. The following table lists error messages and their possible causes.

Problem	Resolution
Unknown server	The configured server cannot be resolved through DNS.
Server unreachable	The one-X Mobile application is unable to contact the server using the configured server name and port.
Server request timeout	Connection to configured server on a specified port timed out.
Invalid user credentials	The configured user name or password is incorrect.
User has no XMPP account	The one-X Mobile application contacted the server to retrieve XMPP account information and found that the user has no active XMPP account .
Failed to retrieve XMPP account information	The one-X Mobile application contacted the server to retrieve XMPP account information and was unable to complete the operation.
Network is unavailable	The connection to the server failed due to network not being available on the device.
XMPP connection is unavailable	The client was unable to establish or maintain an XMPP connection to the server.
A call made via enterprise dialing is dropped	The delay in the network allowed the server provider's call-answer settings to take effect prior to the IP Office No Answer Time setting.
A call made via enterprise dialing goes to the server provider's voicemail instead of IP Office's voicemail	The No Answer Time setting in IP Office is set too high, such that the server provider's voicemail settings took effect first.

Troubleshooting connection issues

When the one-X Mobile application is disconnected from IP Office, it continues to attempt to establish a connection in the background. Use the following list to troubleshoot connection problems if the application remains unable to connect to IP Office.

- Ensure that there is a license for the user.
- 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 is resolving to the correct IP address.
- If the one-X Mobile application can connect when the user is on a cellular network, but is unable to connect on an internal WiFi network, verify that your router supports packet hair-pinning. If your router does not support packet hair-pinning, deploy a split DNS solution to resolve the problem.

Making calls

Calls to or from external locations

When a user initiates a call through the one-X Mobile, the application signals IP Office to call the user at the location currently set in one-X Mobile. After the user picks up the phone at that location, the one-X Mobile then dials the number that the user wishes to reach. This approach means that calls are routed through the enterprise PBX. External phone 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's location is set to an external phone number, or if the user is trying to reach an external number, and is unable to place a call, verify the following:

- Does the number have the correct dialing prefix?
- Is the dial plan correctly configured in IP Office?
- Is a dial plan rule configured in the one-X Mobile application? If not, determine whether you need to configure a dial plan rule in the application.
- Does user have the necessary permissions to call that number?

Call status

The one-X Mobile allows users to view whether their contacts are currently on the phone; however, this status can appear incorrectly if a contact is on a call using a home or cell phone. Contacts who are on a call using a home or cell phone can appear as if they are not on the phone.

Enterprise dialing

You may experience issues with dropped calls or calls forwarding to an undesired voicemail if you use enterprise dialing. The reason is that twinned calls have to account for network delays. A user with a **No Answer Time** set to 15 seconds or less (in IP Office Manager) might experience dropped calls since the user's server provider might have a shorter (or equivalent) no-answer time and network delays have caused the user's default **No Answer Time** to be delayed. Similarly, a **No Answer Time** that is set for too long (for example, 50 seconds) could

allow time for the server provider's voicemail to activate instead of IP Office's voicemail. Since server providers vary based on location, and network delay times vary between providers, ensure that you have an appropriate delay.

Voicemail

If the user is unable to play voicemail messages on the one-X Mobile application, use the following list to troubleshoot the cause of the problem.

- Verify that the IP address of the Voicemail Pro provider is defined in one-X Portal. From the Administrator interface, select **Configuration > Providers > VmPro Provider**.
- If one-X Portal and Voicemail Pro are installed on separate servers, verify that the one-X Portal can resolve the domain name or computer name of Voicemail Pro server.

Instant messaging

Presence

If the presence of the user appears to be incorrect, verify whether the user is logged in to multiple XMPP clients at the same time. For example, is the user logged in to the one-X Mobile application, as well as the one-X Portal?

When a user is logged in to multiple XMPP clients, the presence that others will see for that user is the one that indicates the best availability. For example, if a user is logged in to the one-X Mobile application and has a presence of "Away," and is also logged in to the one-X portal with a presence of "Available," then "Available" is shown as the user's status.

Receiving instant messages

If a user is not receiving instant messages in the one-X Mobile application, verify whether the user is logged in to multiple XMPP clients at the same time. When a user is logged in to multiple XMPP clients, instant messages are sent only to clients where the presence indicates the best availability. For example, if a user is logged in to the one-X Mobile application and has a presence of "Away," and is also logged in to the one-X portal with a presence of "Available," the instant message is sent to the one-X Portal.

Ensure that users properly manage their presence information. The presence setting on any XMPP client must be an accurate reflection of the user's actual presence at that client. Ensure that users log out of clients that they are not using.

Geo-presence

When geo-presence is enabled in the one-X Mobile application, the mobile device provides location information using GPS signals. If the location information is not updating correctly, verify the following:

- Is the user in a location where the mobile device cannot receive GPS signals, such as inside a building?

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

- What level of detail is the user publishing?

When the user sets the Location Precision to **City**, **Neighborhood**, or **Street**, the application uses cloud-based services to obscure the location information and show only the desired level of precision. Depending on network or service conditions, this cloud-based service may not respond and geo-presence information is not updated as a result. These conditions are rare and usually temporary; if the condition continues, set the Location Precision to **Maximum** to avoid the use of cloud-based services.

Viewing logs

The one-X Mobile application can collect logs and submit them to the one-X Portal server when there is a WiFi or 3G data connection available. Log settings are available on the one-X Mobile application under the **Settings > Advanced** menu. You can direct users to provide the following information:

Menu items	Description
Logging Settings	This menu provides access to logging information that you can provide if you need technical support. The options available are: • Logging level: the level of logging information captured. • Log limit: the file size limit for logs collected. The default is 16 MB. • XMPP debugging: enable or disable additional XMPP debugging. • Submit problem report: collect troubleshooting data about the application and submit it to technical support.

File Transfer Options	The following file transfer options are available when you submit information to technical support: • WiFi only: use WiFi for all file transfers. • Pending file transfers: view the number of pending file transfers and purge transfers that are pending.
-----------------------	---

About this task

When a user submits logging information, the location of the logs depends on the operating system that you are using.

Procedure

Choose one of the following options:

- If you are running the 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 one-X Server. The log name is in the format `logs_217_11_08_17_15_47_55.zip`, where “217” is the User followed by date and time the logs were taken.
- If you are running the one-X Portal on a Windows server, the path is: `C:\Program Files (x86)\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\logs\smack-file-transfer Linux - /opt/Avaya/oneXportal/8.0.x_xxx/apache-tomcat/logs/smack-file-transfer`

* Note:

If you are using logs to troubleshoot connectivity issues, you can install a file manager application such as OI File Manager so that logs can be emailed directly from the device.

- If there is no WiFi or 3G connection available, the logs are stored locally on the device. For Android devices, the location is `Android/data/com.avaya.ScsCommander/files/staging`. For iPhones, you can access device logs using a tool called “iPhone Configuration Utility”. You can download the tool from the Internet:
 - iPhone Configuration Utility 3.3 for Window
 - iPhone Configuration Utility 3.3 for Mac OS X

Index

C		configuring 13
calendar access 14	S	system 7
configuring 14	architecture 7	overview 7
calls 18	system architecture 7	system requirements 9
troubleshooting 18	T	
configuring 11–13	troubleshooting 17–21	
Microsoft Exchange Server 13	calls 18	
users 12	connection issues 17	
XMPP domain 11	geo-presence 20	
G	instant messaging 19	
geo-presence 20	logs 21	
troubleshooting 20	voicemail issues 19	
I	U	
instant messaging 19	users 12	
troubleshooting 19	configuring 12	
L	V	
logs 21	voicemail 19	
viewing 21	troubleshooting 19	
M	X	
Microsoft Exchange Server 13	XMPP domain 11	
	configuring 11	

