Open Mobile for Android

iPass Open Mobile™ makes secure, simple and effective network access a reality. No matter where work takes you, iPass Open Mobile provides on-demand global connectivity to the corporate network through a worldwide network of Wi-Fi providers. iPass Open Mobile ensures a secure and controlled session to address the critical requirements of today’s IT departments.

As an administrator, you will use the Open Mobile Portal to configure your Open Mobile profiles, test, and then deploy clients to your user base. You can also use the Open Mobile Portal to run reports on your user base, usage patterns, and client deployment.

Open Mobile (2.7.0 and later) for Android uses a DNSJava Library.

Topics

Latest Release Documents

- Open Mobile 2.9.x for Android Quick Start Guide
- Open Mobile 2.9.0 for Android Release Notes

Previous Release Documents

Open Mobile for Android Printable Administrator's Guide

The Open Mobile for Android Printable Administrator's Guide is not an interactive PDF. Its function is strictly for printing.

- Open Mobile for Android Administrator's Guide

android

Installation

Installation of the Android client can be accomplished by either an activation email or by download from the Android Market.

This page includes details on the following:

System Requirements

The latest version of Android requires:

- A Wi-Fi capable phone running Android OS 2.2 and later.
- A screen with HVGA or higher resolution.
- The app can be distributed through the Android Market, private market, Web sites, or email.
- Users need an iPass account in order for the service to function. In addition, the user must be connected to the Internet (by Wi-Fi or 3G network) to activate Open Mobile.
- **Supported Languages:** English, Simplified Chinese, Traditional Chinese, Dutch, French, German, Italian, Japanese, Korean, Russian, Spanish, and Thai.

Required Network Configurations

Click here for a complete list of required network configurations for Open Mobile access.

Installation and Activation

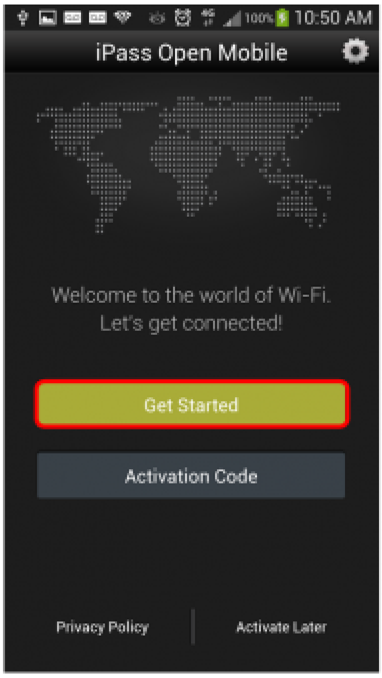
Downloading from the Google Play Store

The app can be downloaded from the Google Play Store and activated from the Welcome Screen.

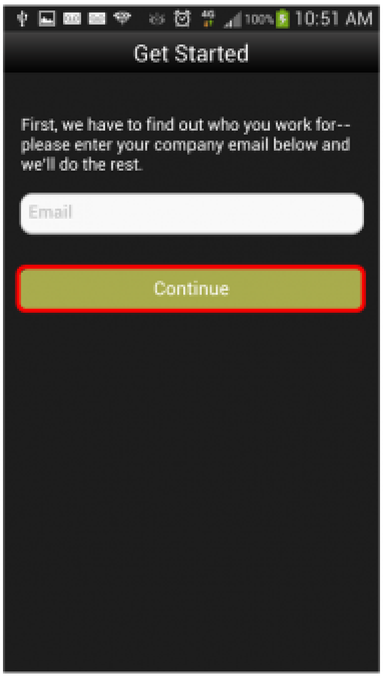
Get Started Wizard

Follow the instructions below to activate Open Mobile using the Get Started Wizard:

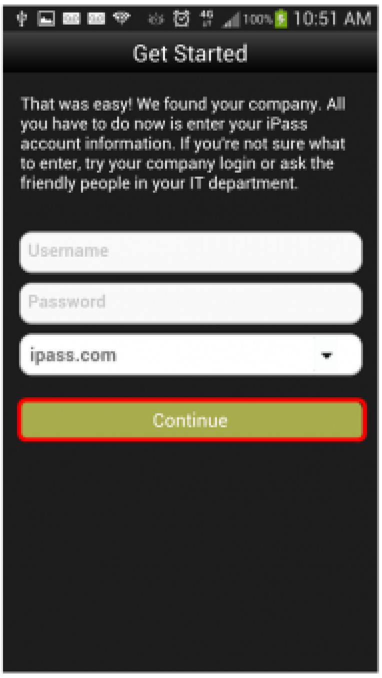
1. Download the app.
2. On the **Welcome** screen, tap **Get Started**. You will need to be connected to the Internet to activate the app.
3. Enter your corporate email address and tap **Continue**.
4. Enter your Username, Password, and Domain and tap **Continue**.
5. Tap **Finish Activation**.



Welcome to the world of Wi-Fi. Let's get connected!



First, we have to find out who you work for--please enter your company email below and we'll do the rest.



That was easy! We found your company. All you have to do now is enter your iPass account information. If you're not sure what to enter, try your company login or ask the friendly people in your IT department.

Activation Code

You can have your users activate with a specific profile by sending them the Profile ID and the optional PIN. Follow the instructions below to activate with an Activation Code:

1. Download the app.
2. On the **Welcome Screen**, tap the **Activation Code** button. You need to be connected to the Internet.
3. Enter **Profile ID**, **Email**, and optional **PIN** (if you do not have a PIN, leave the PIN field blank).
4. Tap **Activate**.

Test Profile Mode

If you are testing the app, tap the bottom left corner of the screen three times to enter Test Profile Mode before entering the Profile ID and PIN.

Activation Email

A pre-written email with download and activation instructions is available in the Open Mobile Portal (see Market Distribution). The instructions include an Activation URL that a user who has downloaded the application can tap to perform an automatic activation.

You can review and make any necessary changes to the email before sending it out.

Private Installer

Follow the instructions below to install from a private installer:

1. On the Home screen, tap **Menu | Settings | Applications**, and check **Unknown Sources**.
2. Download the app from an email attachment, download link, or Private Market.
3. In some cases when downloading using a link or email attachment, the user will have to navigate to the Download folder using a suitable file manager app, such as Files, My Files, or Astro. From there, the user taps the installer to launch it and taps **Install** to install.
4. When the installer is complete, tap **Open** to launch the app.

Unactivated Clients

A user without the correct Profile ID and PIN can tap **Activate Later** on the Welcome screen. Without activation, the user has access to the Usage Meter and Hotspot Finder, but cannot use the app to connect to iPass networks. The app can be activated at any time by tapping **Menu | Activate**.

Activation Failure Logs

If the profile activation fails, the app will collect this information in a troubleshooting log, which can then be sent for diagnosis to the appropriate party, such as your technical support team.

If activation fails, the user can take the following steps:

1. Tap **Options**.
2. Tap **Send Logs**.
3. In the dialog, select a transmission method for the log, such as email, Gmail, or transfer to a Box.net folder.

Your technical support representatives can then retrieve and view the file for more information.

Uninstallation

To uninstall the app, the user can browse to **Settings | Applications | Manage Applications**, select the app from the list, and then tap the **Uninstall** button.

Go to: Open Mobile for Android Help

installation, activation, requirements

DNSJava License Information

Go to: Open Mobile for Android Help

dnsjava, license

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Required Network Configurations for Open Mobile Access

For maximum connectivity, customer firewalls, proxies and other network systems must allow access from the various services that comprise the iPass Open Mobile Service. We have two options for our customers to follow, based on the stringency of their security policies. The *Simple* option keeps the number of rules to a minimum by opening up only the required ports, but allows all hosts from the iPass production networks. The *Advanced* option utilizes the same ports, but allows the customer to lock down the firewall to just the hosts that are currently in service. While this works just as well, it requires more rules in your firewalls, and if iPass adds services in the future, you may need to revisit these rules and open more hosts to our service.

Simple Option

This option opens up only the necessary TCP ports to two /20 blocks of IP space that are owned and maintained by iPass. TCP ports 80, 443 and 577 must be opened from the following IP blocks in order for the iPass Open Mobile service to function. If you are configuring a device that uses a white-listing format (such as an Access Gateway), you should allow the domains of `ipass.com` as well as `i-pass.com`.

IP Addresses	Location
216.239.96.0/20 (216.239.96.0 - 216.239.111.255)	All iPass Data Centers
216.231.192.0/20 (216.231.192.0 – 216.231.207.255)	All iPass Data Centers

Advanced Option

The following advanced configuration allows the customer to allow only the specific hosts that are currently in use.

If you use the *Advanced Option*, you will need to return to this page occasionally to make sure that your configuration is up-to-date.

RoamServer

The iPass RoamServer links the customer network to the iPass Network. It serves as a secure relay between the enterprise authentication database and the iPass Transaction centers. It is installed on the customer network, or can be hosted by iPass or an iPass partner.

The following IP addresses must be able to communicate with the iPass RoamServer through TCP on port 577:

- 216.239.98.125
- 216.239.99.125
- 216.239.100.125
- 216.239.101.125
- 216.239.104.125
- 216.239.105.125
- 216.239.108.125
- 216.239.109.125
- 216.239.110.125
- 216.239.111.125

These IP addresses are strictly for configuration of firewalls and similar devices, and should not be used for other purposes. In general, these IP addresses cannot be directly contacted, such as through a PING utility.

Open Mobile Administration

Open Mobile Portal

The Open Mobile Portal URL is https://openmobile.ipass.com, and the ports required to reach the management system are TCP ports 80 and 443. The IP addresses for the Portal include:

- 216.239.98.122
- 216.239.99.122
- 216.239.99.250
- 216.239.100.122
- 216.239.101.122
- 216.239.104.122
- 216.239.105.122
- 216.239.108.122
- 216.239.109.122
- 216.239.110.122
- 216.239.111.122

Open Mobile Client Installer Server

The client installer server provides client installer software once a profile is published to Test or Production status on the Open Mobile Portal.

The server requires TCP port 80, and the URL is http://om-clientinstaller.ipass.com. The following IP addresses must be accessible:

- 216.239.98.98
- 216.239.99.98
- 216.239.99.244
- 216.239.100.98
- 216.239.101.98
- 216.239.104.98
- 216.239.105.98
- 216.239.108.98
- 216.239.109.98
- 216.239.110.98
- 216.239.111.98

Open Mobile Client

The Open Mobile client must have access to the servers, URLs, and processes listed here.

Open Mobile Data Collector

The Open Mobile Data Collector receives connection and system information reported by the client and ties it to the reports available in Open Mobile Insight.

The Data Collector requires TCP ports 80 and 443, and the URL is om-datacollector.ipass.com. The following IP addresses must be accessible:

- 216.231.200.230
- 216.239.98.102
- 216.239.99.102
- 216.239.100.102
- 216.239.101.102
- 216.239.104.102
- 216.239.105.102
- 216.239.108.102
- 216.239.109.102
- 216.239.110.102
- 216.239.111.102

Open Mobile Update Server

The Open Mobile Update Server informs clients if updates are available for Open Mobile software, configurations or directories.

The Update Server requires TCP port 80, and the URL is http://om-updater.ipass.com. The following IP addresses must be accessible:

- 216.231.200.231

- 216.239.98.124
- 216.239.99.124
- 216.239.100.124
- 216.239.101.124
- 216.239.104.124
- 216.239.105.124
- 216.239.108.124
- 216.239.109.124
- 216.239.110.124
- 216.239.111.124

Open Mobile Download Server

The Open Mobile Download Server retrieves update files for Open Mobile software, configurations, and directories.

The Download Server requires TCP port 443, and the URL is https://om-download.ipass.com. The following IP addresses must be accessible:

- 216.231.200.232
- 216.239.98.123
- 216.239.99.123
- 216.239.100.123
- 216.239.101.123
- 216.239.104.123
- 216.239.105.123
- 216.239.108.123
- 216.239.109.123
- 216.239.110.123
- 216.239.111.123

iPass Client ID Servers

iPass Client ID servers are contacted the first time an iPass client makes a network connection, to obtain a unique client identifier. The identifier is used in all transactions to ensure security of client connections. ClientID servers communicate through TCP port 80, and the URL is http://did01.ipass.com. Access is required to the following IP addresses in order to obtain the ID:

- 216.239.98.97
- 216.239.99.97
- 216.239.99.205
- 216.239.100.97
- 216.239.101.97
- 216.239.104.97
- 216.239.105.97
- 216.239.108.97
- 216.239.109.97

- 216.239.110.97
- 216.239.111.97

OpenAccess

OpenAccess service needs to register with the server through ports 80 and 443 at the following URL:

- https://dapi.devicescape.net/register

The following URLs should also be available for OpenAccess:

- http://alive.devicescape.net:80
- http://dapi.devicescape.net:80
- https://dapi.devicescape.net:443
- https://api.devicescape.com:443

Sniff Servers

The iPass Sniff Servers are used by Open Mobile to determine if an Internet connection can be made, or if further action (such as accepting local terms and conditions) is required. The sniff servers communicate through TCP port 80, and the URLs are http://sniff.gslb.i-pass.com and http://sniff.i-pass.com. The following IP addresses must be accessible:

- 216.231.200.235
- 216.239.98.121
- 216.239.99.121
- 216.239.100.121
- 216.239.101.121
- 216.239.104.121
- 216.239.105.121
- 216.239.105.143
- 216.239.108.121
- 216.239.109.121
- 216.239.110.121
- 216.239.111.121

Connection Quality Test Servers

These servers are only required for the **Connection Quality Indicator** and **Speed Test** features on Open Mobile for Windows 2.2.0 and later clients. The Connection Quality Test servers communicate through TCP port 80 over HTTP, and the URLs are:

- http://qos-naw.ipass.com
- http://qos-nae.ipass.com
- http://qos-apac.ipass.com

- http://qos-emea.ipass.com.

The following IP addresses must be accessible:

- 216.239.98.99
- 216.239.99.99
- 216.239.100.99
- 216.239.101.99
- 216.239.104.99
- 216.239.105.99
- 216.239.105.143
- 216.239.108.99
- 216.239.109.99
- 216.239.110.99
- 216.239.111.99

Local Windows Client Processes

On Windows platforms, these Open Mobile processes must be running in order for the Open Mobile client to have full functionality. Each must be allowed explicit access through the user's personal firewall.

Process	Description
iMobility.exe	Main executable for the Open Mobile client.
iMobilityService.exe	Controls the user interface and intermediates between iMobility.exe and the Open Mobile platform.
iPlatformService.exe	Main service that controls policy enforcement.
iPlatformHost.exe (2 instances)	Enables the client to impersonate the user or system account. Two instances must be running: one each in the system and user contexts.
iPassLogonPolicy.exe	Enables Windows Logon Processing.

Go to: Other Product Documents > Tech Notes

requirements, firewall, roamserver, tech notes

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Profiles

A client *profile* is a set of customization options that determine the features, policy settings, and behavior of the Open Mobile client. Profiles are created in the Open Mobile Portal.

The Open Mobile Portal

The Open Mobile Portal is a powerful Web-based tool that enables you to manage all of your clients, issues, and accounts in one place. To launch the Open Mobile Portal, browse to https://openmobile.ipass.com.

The Open Mobile Portal includes the following capabilities:

- Centrally manage your Open Mobile client profiles, including configuration, deployment, and testing.
- View your open iPass Technical Support tickets.
- Download important documentation.
- Review your iPass accounts, including invoices and outstanding balances
- Run reports on your user data.

Creating a Profile

To create a profile:

1. Select the Configuration tab and then select **Manage Profiles.**
2. Click the **Create New Profile** button on the top-right corner of the screen and then continue past the instruction page.
3. Enter the following:
   - **Profile Name**: Enter a name for the new profile.
   - **Platform:** Select *Android*.
   - **Software Version**: Select *Open Mobile Android.*
4. Click **Save & Continue.**

You can now edit the profile to enable your desired features. These features will include at least one account definition and your network policy settings. You may also wish to create and apply a brand to your profile.

Profile ID

Users who download the app from the Android Market without an activation link will need the Profile ID to activate. The Profile ID is automatically generated by the Open Mobile Portal.

PIN

A PIN (Personal ID Number) provides an extra level of security for users activating the client. Adding a PIN is optional and should only be applied to a profile if your users are downloading the app from the Android Market. A PIN is usually an alphanumeric string a few characters in length.

A PIN may not contain any of these special characters: space( ), dollar sign ($), ampersand (&), plus (+), percent sign (%), at sign (@), apostrophe(‘), comma (,), forward slash (/), colon(:), semicolon (;), equals (=) , question mark (?), quotation mark (”), greater than (>), less than (<), pound sign (#).

To create an optional PIN for this profile:

1. On the **Configure a profile** page, click **Edit.** The **Edit Profile Details** dialog box is displayed.
2. Enter a PIN and click **Save**.

Once you have published to Test, you may no longer change the profile's PIN.

Profile Finder

Available in: Android 2.4 and later

The Profile Finder feature enables easier activation of Open Mobile for users who already have a profile ID for another platform. For example, a user may have Open Mobile installed on a Windows laptop. The Windows installation includes a profile ID (viewable on the **About** dialog). The user can use this Windows Profile ID to activate a new Open Mobile Android profile.

To enable the Profile Finder for your Open Mobile users, on the Open Mobile Portal, designate a profile as a Favorite for the Android platform. This will be the default profile received by your Android users. (Favorite profiles may not include a PIN.)

Subsequent to this, a user can download and install Open Mobile for Android from the Android Market. When choosing to activate Open Mobile on an Android device, the user can enter any valid profile ID (such as one from the Windows installation of Open Mobile). Open Mobile will connect to the Internet, use the supplied Profile ID to locate the Favorite profile for iOS, download it, and install it on the Android device.

More Information

For more information on creating and using profiles, see Manage Profiles.

Go to: Open Mobile for Android Help

android, profile, manage profiles, profile finder, pin, profile id

Distributing the Client

Customers have access to two methods of distributing Android clients.

- **Android Market:** Users download the app from the Android Market (where it is already available), and the app is customized with a user's profile when activated. iPass will automatically upgrade the software every time a new version releases.
- **Private Distribution:** For more control over distribution and branding, direct distribution involves downloading an installer (.apk file) from the Open Mobile Portal and distributing it through email, download link, private market, push software, or other means.

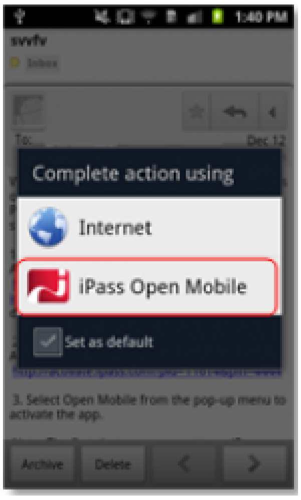
Market Distribution

The Open Mobile Portal includes user instructions for downloading and activating the client.

- Click the **Create Email** button, to automatically create an email with default instructions included in the body.
- Click **Copy to Clipboard** to copy the instructions to your clipboard. You can then paste the default instructions wherever they are needed (such as a website, document, or text editor).

Activation by URL

The activation and download instructions include an activation link. After the user downloads the app, the app can be activated by tapping on the activation link and tapping on **iPass Open Mobile** from the popup menu.



3. Select Open Mobile from the pop-up menu to activate the app.

Private Distribution

To download an installer (.apk) file, click **Download Software and Profile Installer.** Direct distribution options can include:

- Posting a download link on a Web site, then providing the link to the end users by email.
- Emailing the private installer as an attachment. (Note that some email clients may not properly handle the .apk file attachments.)
- Uploading the private installer to your private version of the Android Market. (Private installers downloaded from the Open Mobile Portal cannot currently be uploaded to the public Android Market).

Automatic Upgrades

Currently, all software upgrades are managed through the Android Market unless the profile has been assigned a custom package name (the custom package name feature is optional and may not be available to your account). Users will be notified when a new version is available, and they will be able to download the latest version of the app.

To ensure your users receive all important upgrades, we recommend you have them visit the **My Apps** section of the Android Market and select **Allow automatic updating** next to the app entry.

Go to: Open Mobile for Android Help

android, distribution, android market, upgrades, activation

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

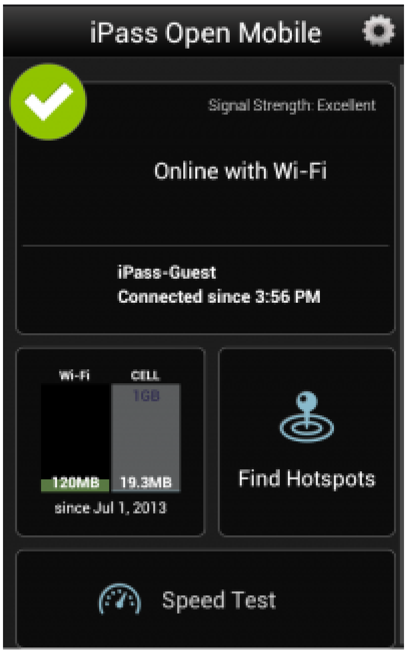
User Interface

The Open Mobile interface is simple and easy to use. This page includes the following items:

- Dashboard
- Connection Manager
- Usage Meter
- Hotspot Finder
- Speed Test
- Settings
- Notification Options

Dashboard

The **Dashboard** section includes four main sections, along with a **Settings** button in the top right corner. The four main sections represent your current connection (the **Connection Manager**), your past connections (the **Usage Meter**), your future connections (the **Hotspot Finder**), and your ability to test your connection (**the Speed Test**).

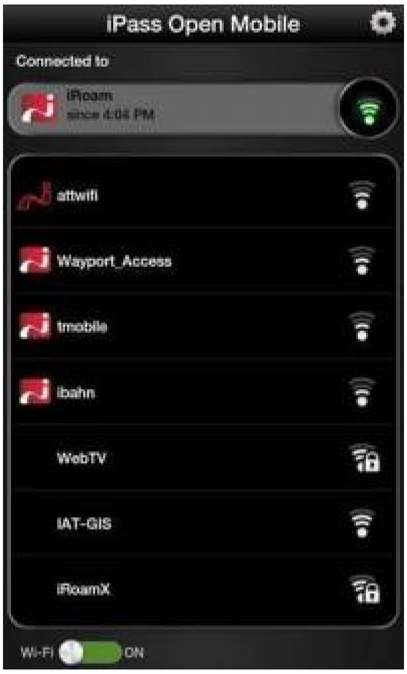


Connection Status Indicator

A green circle with a white check mark will appear when a user is connected to a network.

Connection Manager

The app displays Available Networks and their signal strength. The list is refreshed every 15 seconds. To connect or disconnect from a network, tap the network name.



Connected to
iRoam
since 4:04 PM

Wi-Fi ON

Usage Meter

There are three dialogs in the Usage Meter section. To move between them swipe your finger from left to right (or right to left).

For more details, please see the Android Usage Meter help page.

Hotspot Finder

Open Mobile includes a Hotspot Finder that enables users to locate iPass Wi-Fi hotspots anywhere in the world. Users can enter a location (address, city, zip code, or airport code) in the search box or use the list of nearby hotspots. By tapping on a hotspot location on the list, users can reach a picture of the hotspot location along with the option to call the location or receive GPS directions.

For more details, please see our Hotspot Finder help page.

Speed Test

The Speed Test measures the latency, download speed, and upload speed of a hotspot connection. When a Speed Test is initiated, Open Mobile will ping test servers and choose the one with the fastest response. Open Mobile will then download a test file from that server and upload a test file to that server. After the test is complete, Open Mobile will display the results and indicate the connection quality.

For more details on the Speed Test, please visit the Android Speed Test help page.

Settings

Tapping the **Settings** button will open a window with six options:

- **Account Settings**
- **Usage Settings**
- **Manual Login Settings**
- **About**
- **Take A Tour**
- **Help**
- **Offline Hotspot Finder**

For details on the settings options listed above, please visit our Android Settings help page.

Notification Options

Users can manage how often they receive notifications informing them that an iPass network is available.

For more details on notifications, please visit out Android Notification Options help page.

Go to: Open Mobile for Android Help

auto-connect, hotspot finder, usage limits, android

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

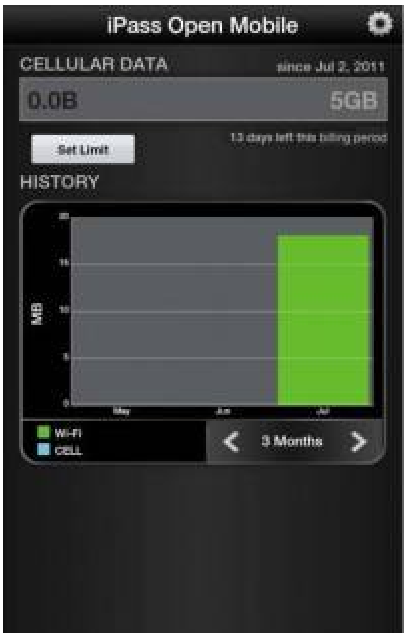
Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Usage Meter

There are three dialogs in the Usage Meter section. To move between them swipe your finger from left to right (or right to left).

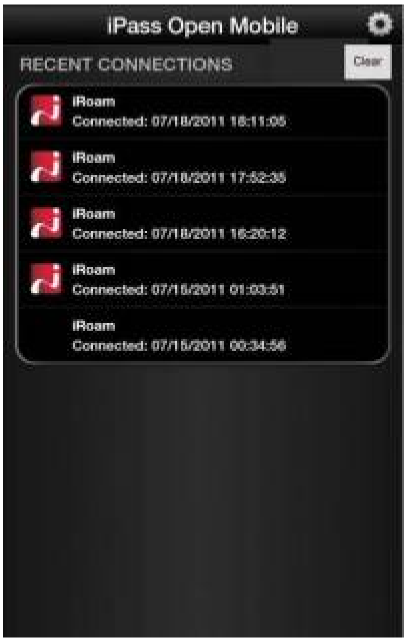
Cellular Data Usage



To set the cellular data limit:

1. Tap the **Set Limit** button to open the **Cellular Data Usage Alerts** dialog.
2. Tap the box under **My billing begins on** to set the calendar day when your monthly billing cycle begins.
3. To set your monthly limit (in gigabytes or megabytes), first tap the box next to **Alert me when I am near my monthly limit** (to add a check mark), and then tap the box under **My monthly limit is** to enter your monthly limit.
4. Tap **Save**.

Recent Connections



iPass Open Mobile

RECENT CONNECTIONS

Clear

iRoam
Connected: 07/18/2011 18:11:05

iRoam
Connected: 07/18/2011 17:52:35

iRoam
Connected: 07/18/2011 16:20:12

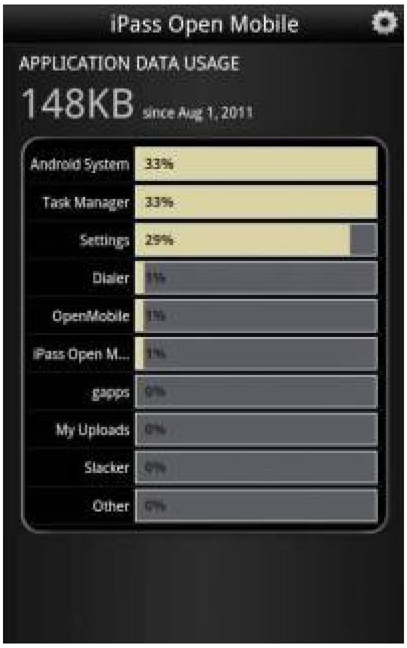
iRoam
Connected: 07/15/2011 01:03:51

iRoam
Connected: 07/15/2011 00:34:56

This dialog will display your twenty most recent network connections. Tap **Clear**, if shown, to clear the connection history.

If the device is running Android OS 2.1 or earlier, this will be the only dialog seen in the Usage Meter.

Application Data Usage



iPass Open Mobile

APPLICATION DATA USAGE

148KB since Aug 1, 2011

Android System	33%
Task Manager	33%
Settings	29%
Dialer	1%
OpenMobile	1%
iPass Open M...	1%
gapps	0%
My Uploads	0%
Slacker	0%
Other	0%

This dialog will display a list of the user’s top ten applications in order of their data usage (showing the total usage and each applications percentage of the total).

Open Mobile for Android Help > User Interface

Hotspot Finder

Filtering: Tapping on the filtering icon (☰) will allow users to filter their hotspot search by type, like hotels, restaurants, and airports.

Hotspot Finder: The Hotspot Finder is available by tapping **Find Hotspots** on the dashboard. A list of nearby hotspots will automatically appear on the Hotspot Finder screen; however, users can search for hotspots by address, city, zip code, or airport code.

Detailed View: By tapping on a specific hotspot location, the user can pull up detailed information about that location, like: name of the establishment, address, GPS directions (to the location), phone number, hours, and even a company website.

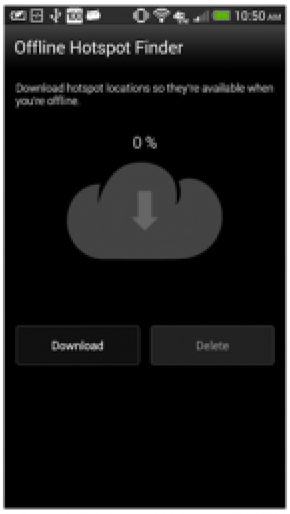
Map View: Pressing the map icon (🗺) will pull up a map of nearby hotspots.

Location icon: Pressing the location icon (⌖) will refresh the search for nearby hotspots.

A custom Hotspot Finder can be configured for profiles in the Open Mobile Portal.

Offline Hotspot Finder

The Hotspot Finder also features an offline mode that allows users to download a list of iPass hotspots that they can later access without an Internet connection. Before the Offline Hotspot Finder can be utilized, users must download a list of hotspots that correspond to the location where they will be without a connection.



10:50 AM

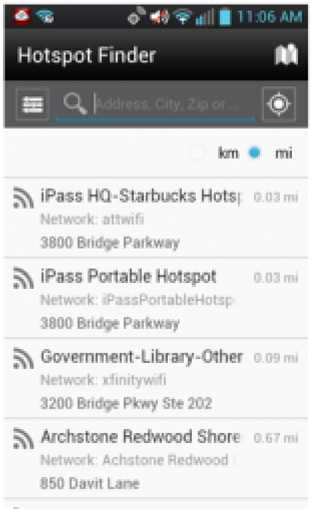
Offline Hotspot Finder

Download hotspot locations so they're available when you're offline.

0 %

Download | Delete

Offline Hotspot Finder



11:06 AM

Hotspot Finder

Address, City, Zip or ...

○ km ● mi

iPass HQ-Starbucks Hotsp 0.03 mi
Network: attwifi
3800 Bridge Parkway

iPass Portable Hotspot 0.03 mi
Network: iPassPortableHotsp
3800 Bridge Parkway

Government-Library-Other 0.09 mi
Network: xfinitywifi
3200 Bridge Pkwy Ste 202

Archstone Redwood Shore 0.67 mi
Network: Achstone Redwood
850 Davit Lane

Hotspot Finder

To download a list of hotspots for later use:

1. Tap the **Settings** icon on the top-right side of the screen.
2. Tap the **Offline Hotspot Finder** option.
3. Tap the **Download** option.

To use the Offline Hotspot Finder:

1. Before using the Offline Hotspot Finder, the user must download a hotspot list as shown above.
2. Tap on the **Find Hotspots** option on the dashboard.
3. The hotspot finder will try to pinpoint the user's location based on their most recent location information. Tapping the location icon will refresh a search.

Go to: Open Mobile for Android Help > User Interface

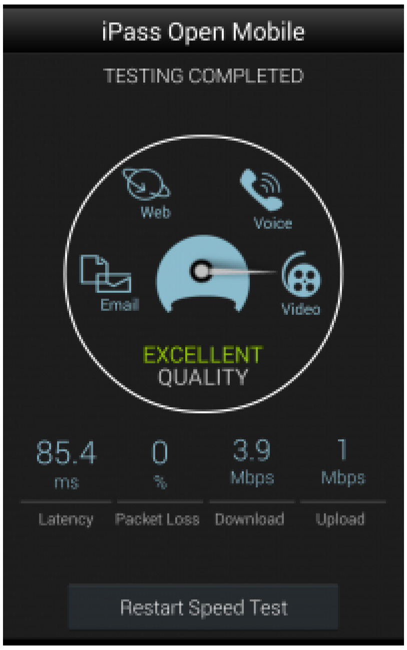
From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Speed Test

The Speed Test measures the latency, packet loss, download speed, and upload speed of a hotspot connection. When a Speed Test is initiated, Open Mobile will ping test servers and choose the one with the fastest response. Open Mobile will then download a test file from that server and upload a test file to that server. After the test is complete, Open Mobile will display the results and indicate the connection quality.


iPass Open Mobile

TESTING COMPLETED

85.4 ms	0 %	3.9 Mbps	1 Mbps
Latency	Packet Loss	Download	Upload

To test the speed of a connection:

1. Navigate to the Speed Test screen by tapping the **Speed Test** button on the welcome screen.
2. Tap **Start** when prompted. You can tap **Cancel** to stop the test.
3. When the test is finished, your hotspot’s latency will be displayed in milliseconds and its download and upload speed will be displayed in megabits or kilobits per second, while a percentage will show how many packets of data were lost. A speedometer will indicate whether your connection is suitable for (from slowest to fastest): Email, Web, Voice, or Video.

Connection quality will vary based on a number of factors (such as the number of users at a location, the signal strength, or provider network congestion). iPass cannot always guarantee the speed of available networks.

Open Mobile for Android Help > User Interface

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

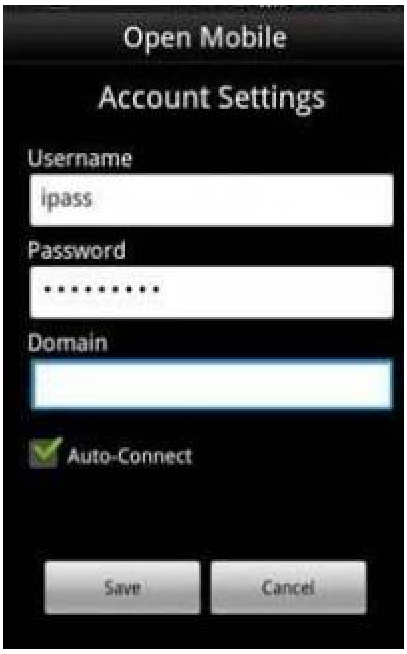
Settings

Tapping the **Settings** button will open a window with seven options:

- Account Settings
- Usage Settings
- Manual Login Settings
- About
- Take A Tour
- Help
- Offline Hotspot Finder

Account Settings

The user enters or changes iPass account credentials here, including Username, Password, Domain, and possibly Prefix (not shown above).



Username
ipass

Password
••••••••••

Domain

☑ Auto-Connect

Auto-Connect

If the **Allow user to save password setting** is enabled for the profile , Auto-Connect can be enabled by checking the box next to it.

The app will automatically re-connect to a network when the user is unintentionally disconnected (after signal loss, for example).

When multiple networks are available in the same location, the client uses a sophisticated algorithm to determine which network to Auto-Connect.

If the user chooses to disconnect from an Auto-Connect network, Auto-Connect will be disabled until the user explicitly attempts to connect again.

If the user disables Save Password while Auto-Connect is enabled, then Auto-Connect will automatically be disabled.

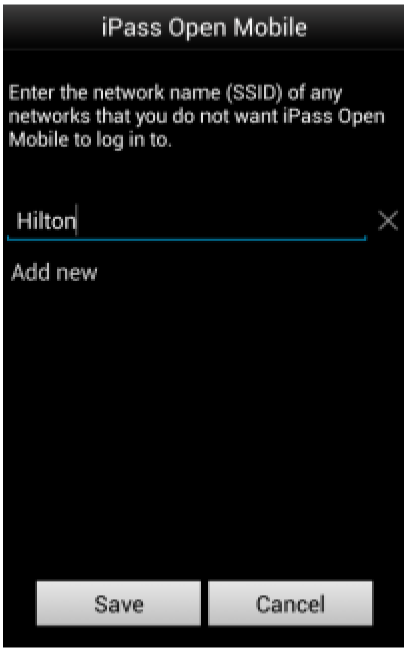
In Open Mobile 2.6.0 for Android and later, you can choose whether to make the Auto-Connect box visible to the user, as well as the default value for the Auto-Connect setting. For more information, see here.

Usage Settings

The user can set cellular data usage limits and their monthly billing cycle for the usage meter under **Usage Settings** above.

Manual Login Settings

Requires: Open Mobile 2.7.0 for Android or later. You can create a list of networks (by SSID) that you do not want Open Mobile to log in to.



iPass Open Mobile

Enter the network name (SSID) of any networks that you do not want iPass Open Mobile to log in to.

Hilton

To add a network to the Manual Login list:

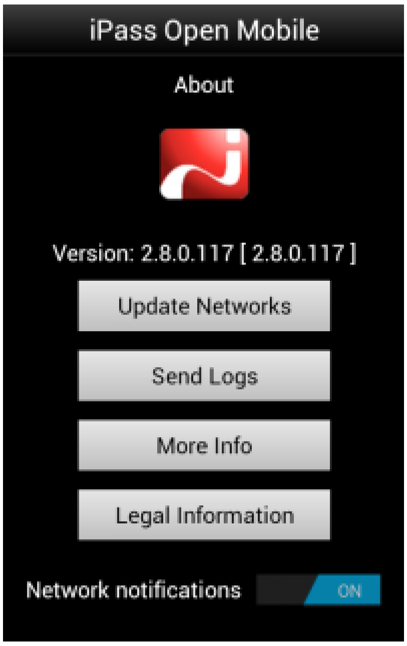
1. Tap the **Settings** button
2. Tap **Manual Login Settings**.
3. Tap the field and use the keyboard to enter the SSID of the network you would like to manually log

in to.

4. To add another network, tap **Add New**.
5. When you are done, tap **Save**.

About

There are four buttons on the **About** dialog: **Update Networks**, **Send Logs**, **More Info**, and **Legal Information**.

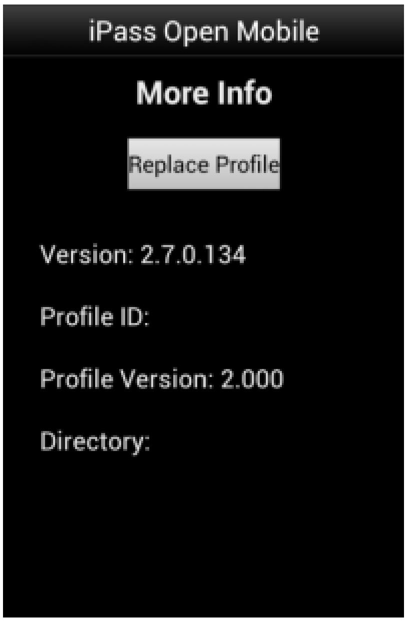


Version: 2.8.0.117 [2.8.0.117]

- Tap **Update Networks** to check for any available Profile and Directory update (not software update). These updates happen automatically every 24 hours.
- Tap **Send Logs** to select a method to send your current logs to your IT Help Desk.
- Tap **More Info** for more information on your version of Open Mobile. The user can also replace their profile here.
- Tap **Legal Information** to access legal details.

Replace Profile

On the **More Info** screen, the user can replace their profile by tapping the **Replace Profile** button. Once they have continued passed the warning message, they will be returned to the **Activation** screen where they can enter the new Profile ID and (if necessary) PIN.



iPass Open Mobile

More Info

Version: 2.7.0.134

Profile ID:

Profile Version: 2.000

Directory:

Take A Tour

By tapping **Take A Tour**, you can access a series of informative panels.

Help

By tapping the **Help** option, the user has access to an informative set of Frequently Asked Questions (FAQs) to help them if they are having trouble connecting to an iPass network.

Offline Hotspot Finder

The Offline Hotspot Finder allows users to download a list of iPass hotspots that they can later access without an Internet connection. For more details on using this feature, please see the Offline Hotspot Finder section.

Open Mobile for Android Help > User Interface

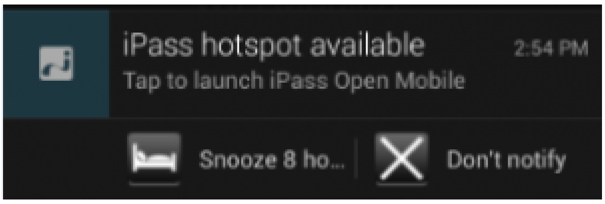
From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Notification Options

Users can manage how often they receive notifications informing them that an iPass network is available.



iPass hotspot available

Tap to launch iPass Open Mobile

2:54 PM

To manage notifications:

1. Drag down the notification bar when the **iPass hotspot available** message appears.
2. Open the iPass notification by dragging it down with two fingers (this takes place in the notification drawer).
3. Notification options:
   - Tap on **Snooze 8 hours** to turn off notifications for an eight hour period.
   - Tap on **Don't notify** to stop notifications.

To restore notifications at any time:

1. In the iPass welcome screen, tap on the options icon on the top right side of the screen.
2. Tap on the **About** option.
3. Find the **Network notifications** toggle option and tap on **ON**.

Open Mobile for Android Help > User Interface

Account Definitions

An *account definition* is comprised of the specific credential types required for a successful login. When logging in to Open Mobile, users are prompted for the required credentials for the account definition, based on the settings you configure.

For example, one account definition may require username and password, while another may require a password and domain name but no username. Account definitions are created in the Open Mobile Portal.

You can create multiple account definitions as needed, but you must create at least one for use on the iPass network that includes username, password, and domain.

An account definition represents the attributes used to create an account. It does not represent a particular user's login credentials.

Credential Types

Credential types are highly configurable to accommodate a variety of login and authentication schemes. This allows you take granular control over the user's login experience. For example, you can control whether or not the user is prompted for a domain prefix when logging in, or whether the prefix is pre-supplied.

- The field labels for accounts in Open Mobile can be changed and customized. For example, you can change the label Username to another value, such as Login Name.
- The values of several attributes may be pre-populated.
- Field Labels even can be hidden so that the information never needs to be entered by the end user.

Account credentials can be configured as follows:

- **Username:** username can be re-labeled.
- **Password:** password can be re-labeled.
- **Domain:** domain can be re-labeled. You can also choose to allow the user to enter the domain, select it from a drop-down list of previously entered domains, or to use a specific domain.
- **Prefix:** prefix can be re-labeled, pre-populated, and hidden from the end user.
- **Authentication Format:** In some cases, an authentication format that differs from the standard iPass authentication may be desired. You can use any of the following tokens to assign a format to the authentication string for the profile: %a for prefix, %u for username, and %d for domain. Your iPass technical contact will be able to advise you on how to define an alternate authentication format for your Open Mobile profile.

Account Settings

Username

A username is required for authentication on the iPass network. In addition to authentication, this username will be used in reporting statistics. You can configure username as follows:

Option	Description
Field Label	The label for the Username field can be changed. For example, if your organization uses employee IDs for user accounts, the label for the username field can be changed to read Employee ID, which would help instruct the user as to what value to use for this account.

Password

A password is required for authentication on the iPass network. Although an Open Mobile password can be any number of characters in length, some iPass providers support only a RADIUS limit of 15 characters for password size. As a result, Open Mobile users with passwords longer than 15 characters may encounter issues at some network locations.

Password Encryption

An Open Mobile is encrypted in three ways when it is stored locally: first, by characteristics derived from the user; second, by machine characteristics; and third, using an AES 256 key.

Option	Description
Field Label	The label for the Password field can be changed. For example, if you configured the label for username to be *Email Username*, you could also configure the label for the password to be *Email Password*.

Valid Password Values

An Open Mobile password (for client connections or Portal logins) may include any of these characters:

- Alphanumeric: A-Z, a-z, 0-9.
- Special: accent mark (`), approximation mark (~), exclamation point (!), at-sign (@), pound sign (#), dollar sign ($), percentage (%), carat (^), ampersand (&), asterisk (*), left or right parenthesis, dash (-), underscore (_), equals sign(=), plus sign (+), left or right bracket ({, }), left or right square bracket ([,]), slash (/), backslash (\), pipe (|), colon(:), semicolon(;), question mark (?), period (.), apostrophe (‘), comma (,), quotation mark (”), greater than sign(>), less than sign (<), space ( ).

Unicode characters are not supported for Open Mobile passwords.

Domain

A routing domain is required for iPass authentication. The routing domain is used to differentiate one customer’s users from another and is established during the initial setup of service with iPass.

The routing domain does not have to be a registered Internet domain or even in the format of an Internet domain. However, It must be unique across the iPass customer base.

If the routing domain field is not used for iPass authentication routing, it can be used for authentication routing on the customer network. For instance, in a multiple domain Active Directory model, a domain name may be necessary to differentiate usernames that might exist in more than one domain (for example, jdoe@europe.acme.com instead of jdoe@asia.acme.com).

Fully Qualified Domains: A pre-filled domain may be fully qualified. However, you can you can only configure domains with a root suffix that matches a domain which is already registered to you. For example, if you were configuring a domain for example1.com, then sales.example1.com would be an acceptable fully qualified domain, but sales.example2.com would not be.

Options	Description
Display Name	The label for the Domain field can be changed.
Pre-Filled Domain	You can choose to pre-fill the domain field with a fixed value. If the domain field is used for iPass authentication and only one domain is to be used, then pre-filling the domain field (and making it non-editable) will ensure that the user utilizes the correct domain name.
Drop-Down List	You can choose to pre-configure a list of domains from which the user can choose.
User Text Entry	Allows users to type in their own domain name. (If the user could be part of a large list of domains, or the profile in use is shared among multiple customers, then this is the most desirable option.)
Allow Edit	If enabled, the user can edit the pre-populated domain.
Hide Field	You can choose to hide a pre-filled domain field from users completely.

Prefix

If the routing domain field is needed for customer authentication routing, then a routing prefix field can be enabled. If chosen, this value must be unique across the iPass customer base. A routing prefix can be used to differentiate one customer’s users from another. This prefix is typically established during the initial establishment of service with iPass.

Options	Description
Field Label	The label for the Prefix field can be changed.
User Text Entry	Allows users to type in the prefix name. **Note:** *If the prefix is not recognized by iPass, the connection will not succeed. As a result, it is recommended that you disable this option.*
Pre-Filled Prefix	Administrators can choose to pre-fill the prefix field with a fixed value. This is the most commonly used option.
Allow Edit	If enabled, the user can edit the pre-populated prefix. **Note:** *If the prefix is not recognized by iPass, the connection will not succeed. As a result, it is recommended that you disable this option.*

Hide Field	You can choose to hide a pre-filled prefix field from users completely. This is the most commonly used option.

Authentication Format

In some cases, an authentication format that differs from the standard iPass authentication may be desired. You can use any of the following tokens to assign a format to the authentication string for the profile: %a for prefix, %u for username, and %d for domain.

Your iPass technical contact can advise you on how to define an alternate authentication format for an Open Mobile profile.

Go to: Open Mobile for Android Help

authentication format, password, username, accounts, credentials, domain prefix, android

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Networks and Policies

Open Mobile serves as a Wi-Fi connection manager that can be used to connect to various types of Wi-Fi networks.

Network Types

Use the client to connect to home and other personal Wi-Fi networks.

Private and public Wi-Fi: if the proper credentials are used, the client can be used to connect to Wi-Fi hotspots in hotels, cafes and other venues.

Home/ personal Wi-Fi: home or personal Wi-Fi networks can be added to the user's network directory in the Open Mobile Portal, enabling quick and easy connections at home.

Security

The following security types are supported:

- Open (None)
- WEP-Open (key index 1-4)
- WEP-Shared (key index 1-4)
- WPA-PSK/TKIP
- WPA-PSK/AES
- WPA2-PSK/TKIP
- WPA2-PSK/AES

Network keys can be entered and edited by the user. To edit a network key, hold down a finger on a network name, then enter and save the key in the **Edit Network** dialog.

Time-Based Session Limits

To help control connection costs, you can set limits for the duration of Wi-Fi and Dial connection sessions. Currently, Time-Based Session limits may only be imposed on GIS access points. Please see our Configure Time-Based Session Limits page for help.

Manual Login

Add networks by SSID and Mac Address that the user will have to log into manually. This will prevent iPass from automatically logging into these networks with the user's iPass credentials. Please see our Configure Manual Login page for additional help.

Hotspot Finder

The Hotspot Finder feature allows you to configure the app searches for hotspots.

On Open Mobile for Android versions 2.8.0 and later, there are two options:

- **In-App Hotspot Finder**: The In-App Hotspot Finder provides the user with detailed venue information, a map, directions to hotspot locations, and other features described in detail here. This option also gives your users access to the Offline Hotspot Finder.
- **Web Based Hotspot Finder**: Choose this option to direct your users to a website with a Hotspot Finder. You can leave the default address in the **Hotspot Finder URL** field or enter a custom URL to direct users to your own Hotspot Finder website. If you choose this option your users will not have access to the Offline Hotspot Finder.

On Open Mobile for Android versions 2.7.x and earlier, you can choose the default or a custom Web Based Hotspot Finder.

iPass Hotspot Connectivity

The app can be used to connect to Wi-Fi hotspots that are part of the iPass network. Connecting at these locations with an accompanying iPass account enables the user to bypass the normal login and billing associated with that location.

Non-iPass Hotspot Connectivity

The app can also be used to assist with login at hotspots that are not part of the iPass network service.

If a hotspot login procedure is needed, a small browser window is launched that enables the user to complete the log in to that hotspot. If a login attempt to an iPass Hotspot fails, the user is given the option either to retry logging in, or to log in to the hotspot through the non-iPass Hotspot browser login window.

Inherited Connections

Open Mobile will detect Wi-Fi connections made with other connection managers and can inherit such connections, becoming the connection manager of choice.

Non-broadcast Wi-Fi networks (which do not broadcast their SSIDs) can be inherited from the Android native Wi-Fi client. However, once inherited, the client will be able to detect and connect to the network.

802.1X connections are currently not enabled. However, if an 802.1x connection is made using the Android native Wi-Fi client, Open Mobile can inherit this connection, and if the 802.1x network is added as a personal network using the Android native Wi-Fi client, Open Mobile can connect to it.

An inherited connection will be charged like any connection initiated by the app.

Connection data is collected from inherited connections and will be used and displayed in Open Mobile Insight reports.

User Authorization

The Subscription Management feature allows you to restrict a profile to a group or groups of users (set up in your LDAP server). Please see our Subscription Management page for help.

OpenAccess

You can make the free OpenAccess Wi-Fi access points available to your users in the iPass Portal. Use of an OpenAccess hotspot will not incur the user any cost to connect and are marked with this icon:

For some free networks, Open Mobile may display both the free, OpenAccess version and the iPass (pay) version of the network.

If a user attempts to connect to a free OpenAccess network and the connection fails, then if there is an alternate iPass network available, the user will be connected to the iPass network instead. However, depending on your access plan, there may be an additional charge incurred for connection to the iPass access point. This capability is currently not configurable.

Enabling Wi-Fi

To enable Wi-Fi, check the **Enable Wi-Fi** box.

To assign directories to this profile, select each one from the Available Lists (on the left), and click the right arrow (**>**) button to add them to the Assigned Lists (on the right). You can add iPass and custom directories. When you are finished, click **Save**.

If the network to which a user is connected (such as a local walled garden) is not able to access the iPass sniff servers used for Internet detection, the user will be warned that Open Mobile is not online, but will remain connected to the network.

Authentication Format Overrides

After network lists have been assigned, Authentication Format overrides can be applied by clicking **Set Authentication Format** above the Assigned Lists. Accounts are generally assigned to an entire profile, and connections made using the account will use the authorization format defined for the account. However, accounts can be assigned for directories. Any authorization formats assigned to such accounts will override the more general one.

Preferred and Prohibited Networks

Special rules for network display can be set for individual networks in your Wi-Fi directories, controlling how these networks will be displayed to users. These rules supersede any Network Ranking settings. To prefer and prohibit networks, select Configure next to Preferred and Prohibited Networks.

Preferred networks: A network defined as preferred will always be used for connections (if possible), and shown at the top of the Available Networks list.

Prohibited networks: A network defined as prohibited will never be used for connections. A prohibited network can be shown as disabled or even hidden entirely from the user.

Speed Test

Test the speed and quality of your connection with the Connection Profiler feature.

Go to: Open Mobile for Android Help

android, network policies, authentication format overrides, openaccess, security

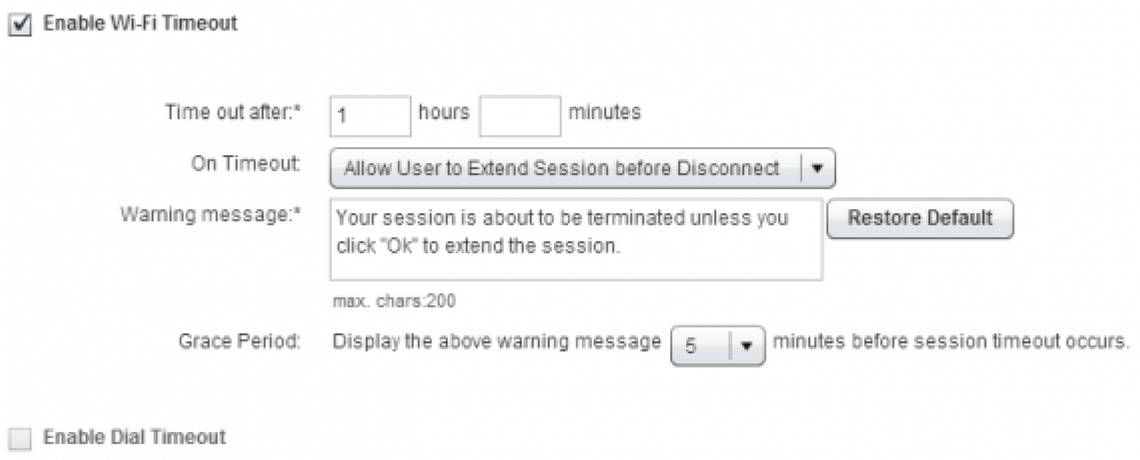
From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Configure Time-Based Session Limits

To help control connection costs, you can set limits for the duration of Wi-Fi and Dial connection sessions. Currently, Time-Based Session limits may only be imposed on GIS access points.



☑ Enable Wi-Fi Timeout

Time out after:* 1 hours minutes

On Timeout: Allow User to Extend Session before Disconnect ▾

Warning message:* Your session is about to be terminated unless you click "Ok" to extend the session.

max. chars:200

Grace Period: Display the above warning message 5 ▾ minutes before session timeout occurs.

□ Enable Dial Timeout

To enable limits on the duration of Wi-Fi or dial sessions:

1. Under **Time-Based Session Limits**, click **Configure**.
2. Select **Enable Wi-Fi Timeout**, or select **Enable Dial Timeout**.
3. In **Time out after**, enter the duration limit in hours and minutes.
4. In **On Timeout,** select the action to be taken when the timeout arrives.
5. In **Warning Message**, enter the message to be displayed to the user, or use the default.
6. In **Grace Period**, select an interval before the timeout when the message will be displayed to the user.
7. Click **Save**.

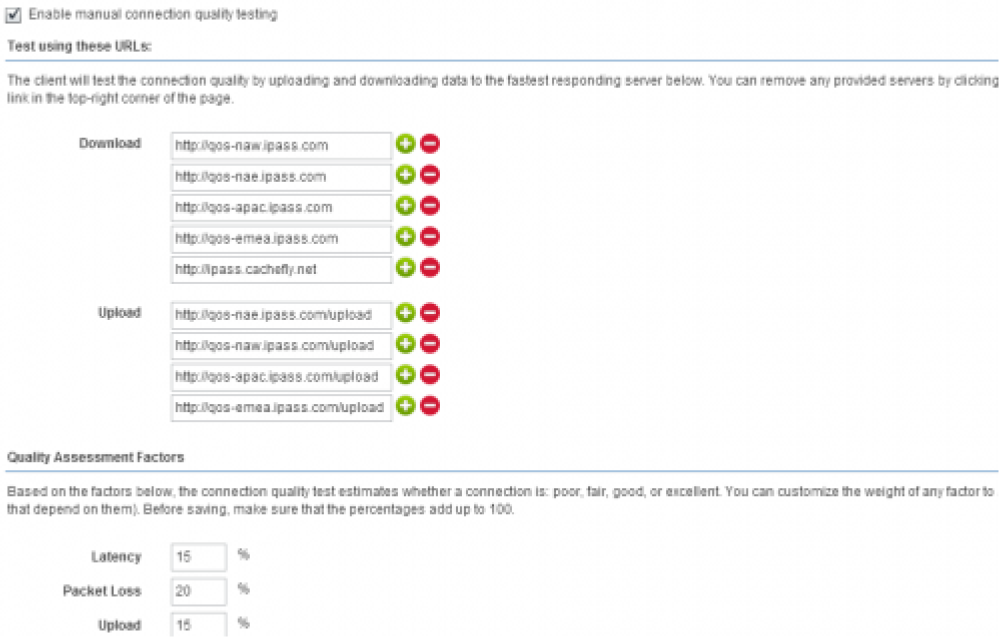
Configuration Settings > Connectivity > Configure Networks and Policies

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Connection Profiler



☑ Enable manual connection quality testing

Test using these URLs:

The client will test the connection quality by uploading and downloading data to the fastest responding server below. You can remove any provided servers by clicking link in the top-right corner of the page.

Download
http://qos-naw.ipass.com
http://qos-nae.ipass.com
http://qos-apac.ipass.com
http://qos-emea.ipass.com
http://ipass.cachefly.net

Upload
http://qos-nae.ipass.com/upload
http://qos-naw.ipass.com/upload
http://qos-apac.ipass.com/upload
http://qos-emea.ipass.com/upload

Quality Assessment Factors

Based on the factors below, the connection quality test estimates whether a connection is: poor, fair, good, or excellent. You can customize the weight of any factor to that depend on them). Before saving, make sure that the percentages add up to 100.

Latency 15 %
Packet Loss 20 %
Upload 15 %

Check the box next to **Enable connection quality testing** to test a network's connection.

Testing using these URLs

The following Connection Quality Test Servers are included by default (depending on your version of the client all of these servers may not be available):

Server Location	IP Address	URL
Download		
Santa Clara	216.239.99.99	http://qos-naw.ipass.com/
Atlanta	216.239.111.99	http://qos-nae.ipass.com/
Hong Kong	216.231.203.233	http://qos-apac.ipass.com/
London	216.239.105.143	http://qos-emea.ipass.com/
N/A [1)]	205.234.175.175	http://ipass.cachefly.net
Upload		
Atlanta	216.239.111.99	http://qos-nae.ipass.com/upload
Santa Clara	216.239.99.99	http://qos-naw.ipass.com/upload
Hong Kong	216.231.203.233	http://qos-apac.ipass.com/upload
London	216.239.105.143	http://qos-emea.ipass.com/upload

You can add or remove test servers:

- You can remove a test server by clicking the red minus button (⊖)
- You can add a test server by clicking the green plus button (⊕)

Utilize whichever servers make the most sense for your users. For example, if your main presence is in London and you want the connection test to always test the user's connection to the main location, you should only include the London server (and remove the others). Otherwise, you may want to include all of the iPass default locations so that the test is more indicative of the local connection your users are on.

If you want to include your own test server, it needs the ability to answer http download requests. The filenames the connection test uses are: `1mb.test` and `5mb.test`. These files need to be uncompressed 1 MB and 5 MB files. For an example, you can download the test files from any of the test servers above (for example http://qos-naw.ipass.com/1mb.test or http://qos-naw.ipass.com/5mb.test). The server needs to be able to service the full URL (with the test files), for example:

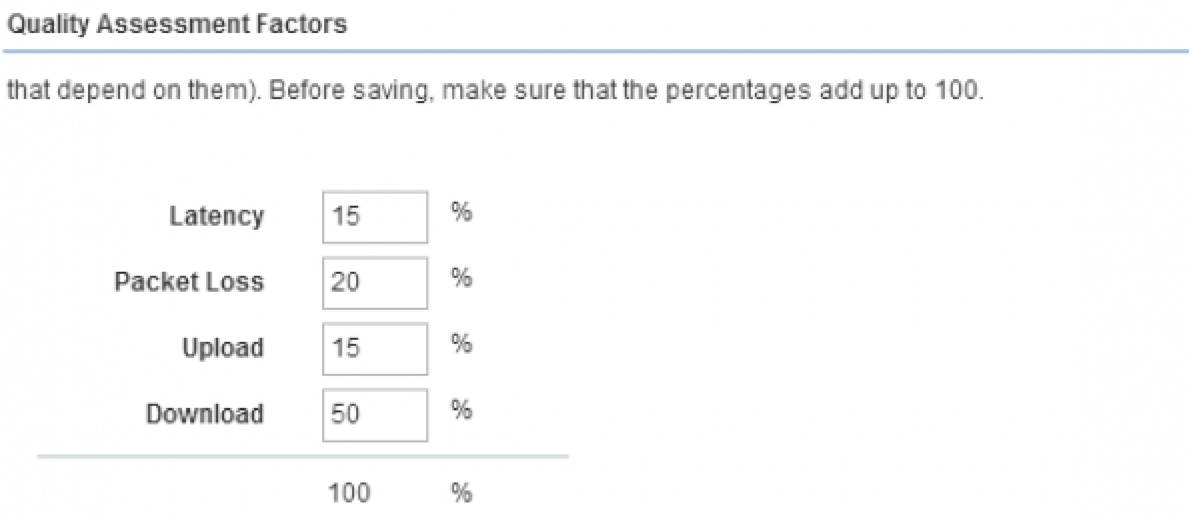
- http://myserver.mycompany.com/1mb.test
- http://myserver.mycompany.com/5mb.test.

Note: When adding a URL to the Connection Profiler, do not include the filename, for example:

- http://myserver.mycompany.com

Adding your test server to the default iPass test servers can be helpful in situations where a user is located in a geographic region where iPass does not have a test server. You can also choose to have all connection tests go to your test server by removing the iPass default test servers (after adding your test server).

Quality Assessment Factors



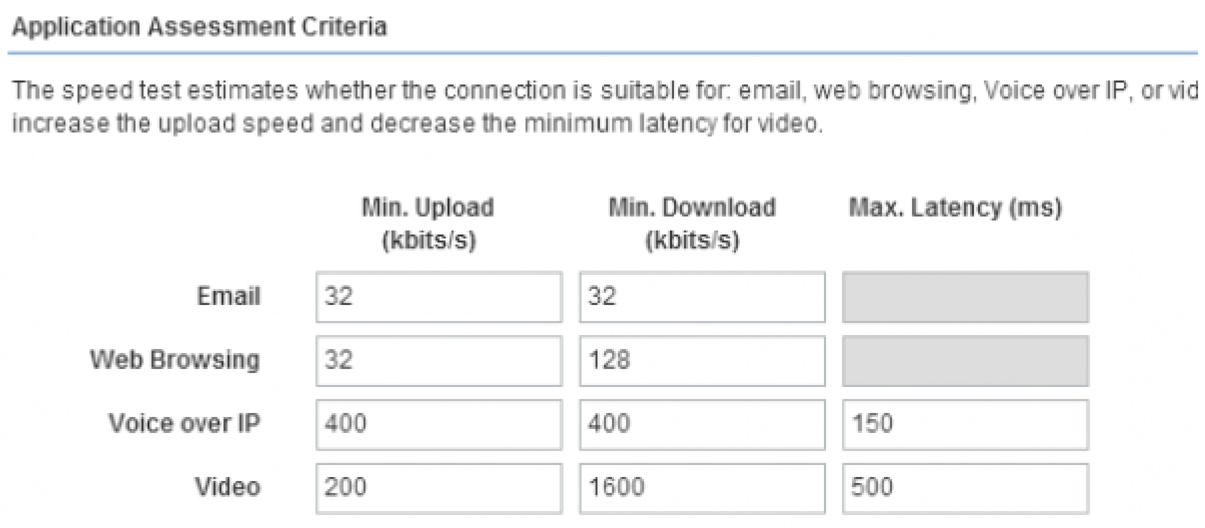
Quality Assessment Factors

that depend on them). Before saving, make sure that the percentages add up to 100.

Latency	15	%
Packet Loss	20	%
Upload	15	%
Download	50	%
	100	%

You can increase or decrease the weight (as a percentage) of each factor. The sum of all percentages must add up to 100 (the 100 underneath the last box does not change dynamically). You can restore the default values by clicking **Restore Defaults**.

Application Assessment Criteria



Application Assessment Criteria

The speed test estimates whether the connection is suitable for: email, web browsing, Voice over IP, or vid increase the upload speed and decrease the minimum latency for video.

	Min. Upload (kbits/s)	Min. Download (kbits/s)	Max. Latency (ms)
Email	32	32	
Web Browsing	32	128	
Voice over IP	400	400	150
Video	200	1600	500

You can adjust minimum upload speed (in kilobits per second), minimum download speed (in kilobits per second), and the maximum latency (in milliseconds) for the application assessment icons that appear at the bottom of the **Speed Test** window. You can restore the default values by clicking **Restore Defaults**.

When you are finished configuring the Connection Profile click **Save**.

Go to: Open Mobile for Android Help > Networks and Policies

android, connection profiler, speed test

[1] This server is cached at the ISP and is most likely located somewhere in North America

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Client Look and Feel

If you have branding capabilities enabled, you may apply an existing brand to your Android profile.

To apply an existing brand to your profile:

1. Click **Select a brand**.
2. From the dropdown list, choose the brand to apply.
3. Click **Save.**

See Branding for more information on creating a brand for your Android profile.

Go to: Open Mobile for Android Help

look and feel, branding, android

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

3G Offloading

Available for: *Android 2.2 and later clients*

In general, a 3G data connection can be much more costly than a local Wi-Fi connection. To help control high connectivity costs, you can configure the client to force existing 3G connections to auto-connect to a set of specified Wi-Fi networks, if Wi-Fi is in range and available.

In order to enable forced auto-connect to less expensive Wi-Fi networks, the following conditions must be met:

- Forced Auto-connect must be enabled for a custom directory in the user's client profile, and the SSID must be in the custom directory.
- Open Mobile must be activated and the enabled Android 2.2.0.103 profile loaded on the user's device.
- The user's credentials have been entered and saved in the app.
- The Android device must be 3G-enabled and have 3G signal of at least -72 dbM.
- The offload SSID must be detectable for 15 seconds (when the device is in screen off/dark mode).

Enabling Forced Auto-Connect for a Profile

Before users can use 3G offloading, you must enable this capability in their client profiles on the Open Mobile Portal.

To enable one or more Wi-Fi directories for Forced Auto-Connect:

1. Select (or create) an Android profile for which you wish to enable Forced Auto-Connect. (Complete instructions for profile creation are found in the Open Mobile Portal Administrator's Guide, available from the Open Mobile Portal.)
2. Under **Networks and Policies**, click **Configure**.
3. Under **Actions**, click **Configure**.
4. Under **Assign or Remove Wi-Fi Hotspot Lists**, using the arrow keys, assign one or more custom directories to the profile.
5. In the **Assigned Lists** column, click **Set Authentication Format**.
6. Select a custom directory for which you wish to enable Forced Auto-Connect.
7. Under **Forced Auto-Connect**, from the drop-down list, select *Yes*.
8. Repeat Steps 6-7 for each additional custom directory.
9. When complete, click **Save**.
10. Continue to edit the profile as needed, then save it and publish to your users.

The User Experience

The experience for a user with a 3G offload enabled depends on whether the Android device has its screen turned on, or is dark (but is still powered on).

In order to enable Auto-Connect, the user must enter and save valid login credentials in the app.

Screen On

With the screen on, and the device connected to a 3G network, a user may travel into range of a valid offload SSID. As soon as the network detected, and the network signal strength is within specifications, the user’s 3G connection will be ended, and replaced with a Wi-Fi connection.

Offload SSIDs will also be used for regular Auto-Connect connections, if the screen is on and the user is not already connected to a 3G network.

Screen Off

With the screen off (dark), and the device connected to a 3G network, a user may travel into range of a valid offload SSID. If the network is detected for at least 15 seconds, and the network signal strength is within specifications, the user’s 3G connection will be ended, and replaced with a Wi-Fi connection.

Go to: Open Mobile for Android Help

3g offloading, android

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

On-Campus Roaming

Available for: *Android 2.6.0 and later clients*

If On-Campus Roaming (OCR) is enabled, users can log in to a corporate network with an 802.1x connection. Although Wi-Fi is ubiquitous, security and authentication standards may widely vary from location to location. OCR enables users to be more productive on a far-flung corporate campus, and allows easy access for guests and contractors, without needing to use multiple connection managers.

Campus hotspots are automatically detected and presented as Wi-Fi networks. Users can log in using their regular Open Mobile credentials. Open Mobile sets the proper SSID and security method.

In order for a user to connect to an 802.1x network, the network must be included in a custom directory, and the directory included in an Open Mobile profile installed on the user's device.

Open Mobile for Android supports the PEAP-MSCHAPV2 and TTLS-MSCHAPV2 authentication types (both with and without certificate authentication) for use with OCR.

OCR networks will be displayed in Open Mobile with the custom networks icon:

Forced Auto-Connect: If the Forced Auto-Connect option is enabled for the directory, users will automatically be connected to the 802.1x network if it is within range (and their credentials have been saved).

Ordinarily, Open Mobile will only display, and permit connections to, local 802.1x networks that are specified in a custom network directory. However, if a user connects to one of these networks using the native Android connection setting, Open Mobile will display the connected network in the list of Available Network. However, it will not facilitate disconnection and will serve as a display-only observer for the network.

Configuring OCR for an Android Profile

The process of configuring OCR for an Open Mobile for Android profile is as follows:

1. Create (or choose) a profile for which to enable OCR.
2. Download the sample directory file, and customize the sample directory to specify the settings for a single 802.1x network.
3. Upload the custom directory to the Open Mobile Portal.
4. If connectivity will include certificate validation, upload the certificate as a profile attachment.
5. Publish the profile to test, and then distribute the test profile to your test users.
6. After testing is complete, publish the profile to production and distribute it to your user base.

Creating an OCR 802.1x Directory

An OCR 802.1x directory must be a validly formatted XML file that describes a single 802.1x network. You will need to determine values for the network parameters in the file, and then specify them in the XML file settings. To specify more than one 802.1x network, use a separate directory file for each one.

An annotated sample OCR directory can be downloaded here. Edit and save it to create your own 802.1x directory. The sample directory includes instructions for customizing the file with your own network information.

You should use an XML editor to edit the file.

To create an OCR 802.1x directory for a single 802.1x network,

1. Download the sample file.
2. Open the file in an XML editor of your choice.
3. Following the annotations in the file, edit the file as needed for a single network.
4. To enable certificate authentication, in the XML file, ensure that the *ValidateCertificate* flag is set to true, and replace the value *myrootCAcert.cer* with the name of your actual certificate file.
5. Save the file with the desired filename.

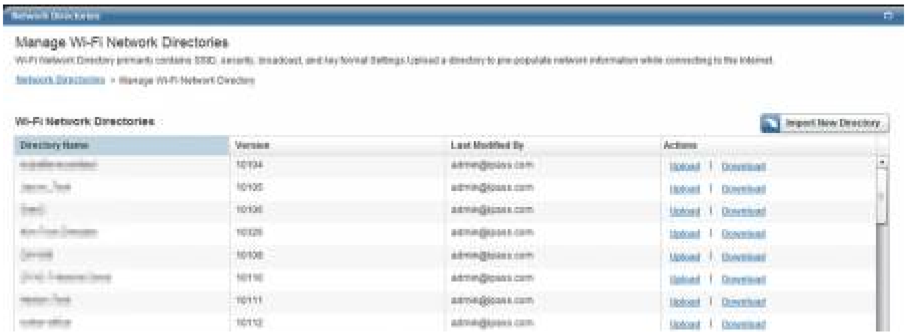
Enabling OCR for a Profile

Enabling OCR for an Android 2.6.0 or later profile involves uploading the directory file to the Open Mobile Portal to make it available for assignment, and then actually assigning it to a profile. In addition, to enable certificate authentication, the certificate file must be attached to the selected profile.

Uploading the Directory File

To upload an OCR directory file to the Open Mobile Portal,

1. Log into the Open Mobile Portal.
2. Under **Client Configuration**, pick **Upload Networks.**
3. Under **Wi-Fi Networks Directories**, click **Manage**.
4. On the **Wi-Fi Directories** page, click **Import Directory**.
5. On the **Import Wi-Fi Directory** page, in **Display Name**, enter the name of the directory as it will be displayed in the Portal (for example, *Corporate HQ Directory*).
6. Click **Browse**. Select the directory XML file you have previously created. The directory will now be available to add to profiles.



Network Directories

Manage Wi-Fi Network Directories

Wi-Fi Network Directory primarily contains SSID, security, broadcast, and key format Settings. Upload a directory to pre-populate network information while connecting to the Internet.

Network Directories > Manage Wi-Fi Network Directory

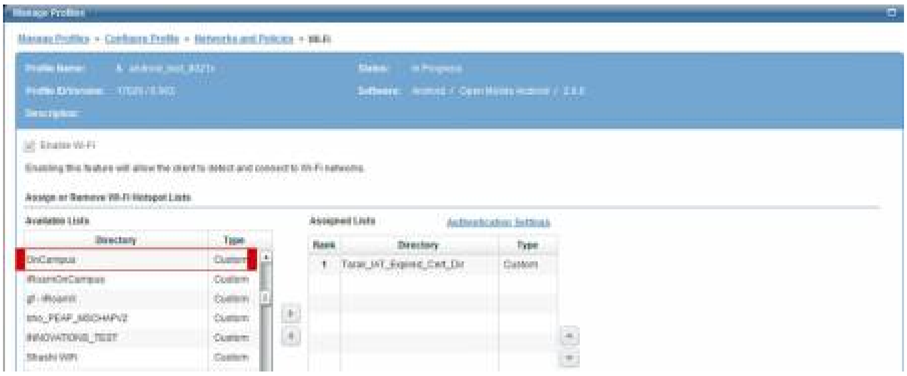
Wi-Fi Network Directories

Directory Name	Version	Last Modified By	Actions
[illegible]	10104	admin@ipass.com	Upload | Download
[illegible]	10105	admin@ipass.com	Upload | Download
[illegible]	10106	admin@ipass.com	Upload | Download
[illegible]	10129	admin@ipass.com	Upload | Download
[illegible]	10108	admin@ipass.com	Upload | Download
[illegible]	10110	admin@ipass.com	Upload | Download
[illegible]	10111	admin@ipass.com	Upload | Download
[illegible]	10112	admin@ipass.com	Upload | Download

Assigning the Directory to a Profile

To add an uploaded OCR directory file to a profile,

1. Under **Client Configuration**, pick **Manage Profiles.**
2. Select (or create) an Android 2.6.0 or later profile to which you will add the customer directory.
3. Under **Actions**, pick *Manage*.
4. Under **Networks and Policies**, click **Configure**.
5. For **Wi-Fi**, under **Actions**, click **Configure**.
6. Under **Available Lists**, the OCR directory you have previously uploaded will be displayed. Select it, and then click the right arrow to assign it to the profile.
7. To enable Forced Auto-Connect for the directory, click **Authentication Settings.** Select the directory in the list of assigned directories. Under **Forced Auto-Connect**, select *Yes*. Then, click **Back**.
8. Continue assigning other directories if needed, repeating Steps 6-7.
9. Click **Save** to save your directory assignments.



Manage Profiles

Manage Profiles > Configure Profile > Networks and Policies > Wi-Fi

Profile Name: [illegible]

Status: In Progress

Profile ID/Version: [illegible]

Software: Android / Open Mobile Android / 2.6.0

Description:

☑ Enable Wi-Fi

Enabling this feature will allow the client to detect and connect to Wi-Fi networks.

Assign or Remove Wi-Fi Hotspot Lists

Available Lists

Directory	Type
OnCampus	Custom
iRoamOnCampus	Custom
gll - iRoam	Custom
bho_PEAP_MSCHAPV2	Custom
INNOVATIONS_TEST	Custom
Shashi WiFi	Custom

Assigned Lists

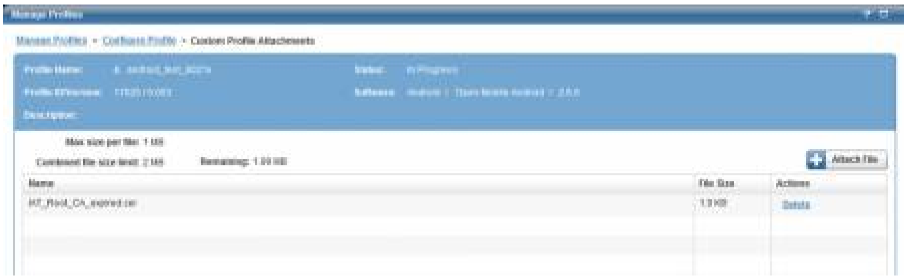
Rank	Directory	Type
1	Taran_IAT_Expired_Cert_Dir	Custom

Attaching the Certificate

If you choose to enable certificate authentication for your selected OCR authentication type, the certificate must be included in the OCR-enabled profile as a profile attachment. (You may attach multiple certificates to a profile if necessary.)

1. Under **Client Configuration**, pick **Manage Profiles.**
2. Select the Android 2.6.0 or later profile to which you have previously assigned the OCR directory.
3. Under **Actions**, pick *Manage*.
4. Under **Custom Profile Attachments**, click **Configure**.
5. On the **Custom Profile Attachments** page, click **Attach File**.

6. Locate the certificate file you wish to upload, and pick **Open**. The file is now attached to the profile. (Note that the name of the selected certificate file must match the name of the certificate you specified in the custom directory XML file.)
7. Continue to upload other certificates as needed.



Manage Profiles

Manage Profiles > Configure Profile > Custom Profile Attachments

Profile Name: [illegible] Status: In Progress

Profile ID/Version: [illegible] Software: [illegible]

Description:

Max size per file: 1 MB

Combined file size limit: 2 MB Remaining: 1.99 MB

Name	File Size	Actions
HT_Root_CA_expired.cer	1.3 KB	Delete

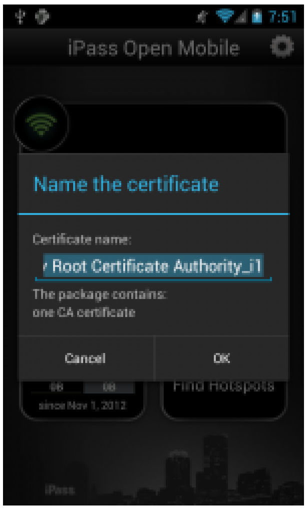
Next Steps

You can now continue to edit the selected profile as needed with any other desired settings. When complete, publish the profile to Test and distribute it to your test users. Perform thorough testing on your OCR-enabled profile. After testing, the profile may be published to production and distributed to your user base.

Enabling the Security Certificate on an Android Device

If On-Campus Roaming has been enabled for a device, and you have chosen to attach a security certificate to the profile, then when first launching Open Mobile, the user will be required to install the certificate. The user will also be prompted to set a lock screen PIN or password for the device, if one has not been previously set.

- On Android OS 2.2 or 2.3, the user should follow the prompts to enable the lock screen PIN or password for the device. Do not rename any certificate filename; use the default name. The certificate filename is presented, but the user should use the default name and not rename the file.
- On Android 4.0 and later versions, this procedure is called Enabling Credential Storage. The user can follow the prompts to enable credential storage on the device, as well as to set the lock screen PIN or password. The certificate filename is presented, but the user should use the default name and not rename the file.



Name the certificate

Certificate name:

Root Certificate Authority_i1

The package contains:
one CA certificate

Go to: Open Mobile for Android Help

ocr, 802.1x

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Branding

Branding capabilities are optional and may not be available for your enterprise. If available, you can brand the client on the **Account** tab in the Open Mobile Portal.

Before Creating a Brand

Branding requires that you make design decisions, create product and component names, and upload image files for client components. You should assemble the required files and text labels before beginning the process of creating a brand.

After Creating a Brand

Once you have created one or more client or portal brands, you can publish them to production. Only one brand may be active at a time, and it cannot be deleted. (Deleting a brand could cause conflicts with deployed profiles that use an existing brand.)

Branding Your Client

A client brand comprises the set of icons, images, text strings, additional help content, and colors you choose to include in the client's look and feel. The complete list of client branding options includes these selections. If no element is selected, the default is used.

Please click this link for a complete list of branding options.

Creating a Custom Package Name (Optional)

Creating a custom package name is optional. If this capability is enabled for your enterprise, attaching a custom package name to a client will prevent that client from automatically upgrading with each iPass release in the Android Market. In turn, this will prevent certain branded elements from reverting to their defaults with each upgrade.

To create a custom package name:

1. On the **Configuration** tab, select **Register Packages**.
2. In the **Package Name** field, enter the custom package name.

3. Click the **+** button.
4. Click the **Save** button.

Creating a Brand

To create a new client brand for a supported platform:

1. Log in to the Open Mobile Portal, and select the **Configuration** tab.
2. Click **Manage Brands**, and then click **Create Brand.**
3. On the **Create a Brand** tab, enter values for the following:
   - In **Brand Name**, enter a new brand name.
   - For **Platform**, select *Android*.
   - If **Class** is shown, select a class from the dropdown.
   - After **Software Version**, select the software version from the dropdown.
   - If **Package Name** is shown, select a package name from the dropdown.
4. Select the branding tabs as needed to enter your desired branding elements. The Image Map interactively displays the components of the user interface, as you change them, so you can preview your brand before you save it.
5. When the brand is complete, click **Save**.

Once created, you can publish the brand so that you can include it in your client profiles.

Editing a Brand

To edit an existing client brand:

1. Under **List of Brands**, select the brand you wish to edit.
2. In the **Actions** column, click **Manage**.
3. Enter the requested text strings, or upload the requested files.
4. When complete, click **Save**.

A published brand may not be edited.

Publishing a Brand

A published brand can be included in profiles, and can be shared with your child accounts. A published brand may not be edited.

To publish a brand:

1. Create a brand (see above).
2. From the **List of Brands**, select the brand you wish to publish. Then, in the **Actions** column, click

Publish.

3. On the **Publish Client Brand** page, click **Publish**, and then click *Yes* to confirm publication.

Sharing a Client Brand

Once a brand is published, it can be shared with your child accounts. These accounts will be able to include the brand in their own client profiles. (You can only share a brand one level down—that is, with your immediate child accounts.)

To make a brand shareable:

1. On the List of Brands, select the published brand you wish to share. Then, in the **Actions** column, click **Share**.
2. On the **Share Client Brand** dialog, select the direct child accounts with which you wish to share the brand.
3. Click **Share**, and then click *Yes* to confirm sharing.

Applying the Brand to a Profile

Once you have created and published a brand, you can apply it to a profile.

To apply a brand and styling to a supported client:

1. On the **Configure a Profile** page, under **Brands and Features**, click **Configure**.
2. Click **Select a Brand**.
3. Under **Client Branding**, select a brand from the drop-down list of previously created brands. Only a single brand may be assigned to a profile at one time.
4. Click **Save**.

Distribution

Branded clients have to be distributed using a private installer created in the Open Mobile Portal, and if the branding has changed, the private installer has to be redistributed (a profile update and migration will not generate the branding changes).

Upgrading from a Previous Version

There are two upgrade scenarios:

- If the default package name is used, software upgrades are managed through the Android Market and users will be notified when a new software version is available.

- If a custom package name is used, software upgrades are controlled by the Administrator, who will have to redistribute the software (the private installer available on the Open Mobile Portal) with each upgrade.

Go to: Open Mobile for Android Help

branding, android

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Android Branding Elements

The complete list of client branding options includes the items shown in the table. If no element is selected, the default is used. Default images are illustrated in the Portal.

Each column in the following tables indicates the file type or requirement. If the requirement is an image file, the file dimension is given in pixels. When creating a brand, only the Brand Name and Software Version is required. All other elements are optional.

An interactive Image Map labels each of these elements, showing a live preview of your brand as you create it.

Android

Client Elements	**Version 2.0**	**Version 2.1.x**	**Version 2.2.0 and later**
Brand Name			
Brand Name	Alphanumeric string, max 35 characters. Required.	Alphanumeric string, max 35 characters. Required.	Alphanumeric string, max 35 characters. Required.
Class	Select from dropdown	Select from dropdown	Select from dropdown
Software Version	2.0	2.1.x	2.2.0
Package Name	N/A	N/A	Select from dropdown
Image/Icon			
Logo	N/A	N/A	Custom Package Name, 75px (w) x 75px (h), PNG format , max file size 11 KB
Splashscreen	N/A	N/A	Custom Package Name, 480px(w) x 800px, PNG format, max file size 100 KB
Background	N/A	N/A	Custom Package Name, 720px(w) x 1280px, PNG format, max file size 1 MB
OpenAccess Icon	72px (w) x 72px (h) , PNG format, file size max 150 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB
iPass Icon	72px (w) x 72px (h) , PNG format, file size max 150 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB
Custom Wi-Fi	72px (w) x 72px (h) , PNG format, file size max 150 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB
Text			

Application Name	N/A	N/A	Custom Package Name, Alphanumeric string, max 20-25[1] characters
Network Alert Message	N/A	N/A	Custom Package Name, Alphanumeric string, max 80 characters
Installer			
Launcher Icon	N/A	N/A	Custom Package Name, 72px (w) x 72px (h) in PNG format, max file size11 KB
Notification Icon	N/A	N/A	Custom Package Name, 24px (w) x 24px (h) in PNG format, max file size11 KB

Image File Types: Open Mobile requires two image file types in branding: .PNG (Portable Network Graphics format) and .ICO (Icon format) files. PNG files are used for many branding elements because, unlike other image formats, they are highly scalable, universal across platforms, and low-loss. ICO files are required by Windows for correct display on the Windows taskbar. Note that ICO files, in particular compressed ICO files, may not display consistently on all Windows platforms. Both of PNG and ICO file types are easily created in many image editor applications.

The Configuration Tab > Manage Brands > Create a Client Brand

android branding

[1] Because there is limited space for the Application Name in the client's User Interface, there is a limit of 20-25 characters depending on the language and the characters used (this limit is not imposed by the Open Mobile Portal). You should use the interactive Image Map to ensure that your Application Name fits.

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Support

Troubleshooting Logs

Open Mobile logs connection data, which can be useful in troubleshooting connectivity or application issues.

To send logs:

1. Tap the **Settings** button and then tap **About**.
2. Tap **Send Logs.**
3. Select a method for sending the logs (the choice varies by device depending on what you have installed). The easiest method is probably email.
   - If you select email, a message should open with the logs attached. Enter the support email address (in the To: field), any message you would like to include, and send the email.

Troubleshooting Tips

Wi-Fi users can occasionally run into difficulties in connection, such as those listed here.

Duplicate SSID

The client identifies iPass Wi-Fi networks by their network name (SSID). A network name that duplicates a network name in the iPass Network directory will display the iPass logo, normally indicating that it is an iPass network. However, there are some circumstances where the indicated network is not actually an iPass location, such as the following:

- The local provider is using a name that is also used by one of the iPass network providers.
- The local provider has other locations that are part of the iPass service, but has excluded this particular location.

For more information, please see Incorrect Identification of Non-iPass Hotspots.

Failed Venue Login

On occasion, an association to a Wi-Fi access point is successful, but the log in to the venue fails because of a timeout, authentication failure, or some other error.

Connecting to an iPass network requires a successful association, but in addition, Open Mobile must also receive an IP address from the venue and it must be able to pass HTTPS communication to the access gateway. A weak signal can cause a failure in the IP address assignment or HTTPS communication. Moving closer to the access point, or moving to a location with a stronger signal, may resolve this situation.

Back-End Infrastructure Issues

Authentication errors can occur if the back-end authentication infrastructure is not available. This could be an outage at the provider, or with your RoamServer or AAA system.

Personal Wi-Fi

Some common issues that can occur for personal Wi-Fi access points include:

- The home access point has MAC address filtering, which prohibits the user from communicating over it even if a successful association is made.
- A weak signal prevents association.
- The location is 802.1x-enabled. 802.1x connections are not currently supported.

Go to: Open Mobile for Android Help

support, troubleshooting, android

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**

Incorrect Identification of Non-iPass Hotspots

An SSID displayed with an iPass logo normally indicates that the hotspot is part of the iPass network. However, this is not always true. In some cases, the iPass logo is displayed because the hotspot been falsely identified as part of the iPass network. In such cases, a connection attempt will fail.

Wi-Fi Network Identifiers

Because of the limitations of Wi-Fi technology, only a few network identifiers are broadcast locally for iPassConnect and Open Mobile to read: security type, MAC address, and network name (SSID):

- For nearly all public hotspots, the security type is Open, so security type is not helpful in determining a hotspot is part of the iPass network.
- Hotspot MAC address information is not provided to iPass, and further, is subject to change at any time (as equipment is replaced or re-provisioned). Even if accurate information on hotspot MAC addresses were provided to iPass, with over half a million Wi-Fi hotspots supported (and many hotspots possessing dozens of distinct MAC addresses), it would be nearly impossible for iPass to keep such information current in each individual client.
- This leaves the network name (SSID) as the only useful identifier to determine whether the hotspot is provided by an iPass network provider. In the huge majority of cases, SSID is indeed enough to provide accurate identification, and users can trust that the location is indeed part of the iPass service.

False Identification Scenarios

However, there are a few situations where hotspots may be falsely identified as iPass hotspots.

Partial Network Footprint

In some cases, a provider will only provide a portion, but not all, of their network footprint to iPass, while using the same SSID for all of their locations. As a result, locations that are not provided to iPass would be falsely identified as iPass hotspots.

iPass makes every attempt to include a provider’s entire footprint in its network to prevent such false identifications, but sometimes 100% coverage is not possible. In some cases, iPass has even chosen not to add the provider to its network to avoid false identifications. Only when a provider has critical high-volume locations that iPass customers have deemed as very important to them has such a partial footprint been added.

Temporary Access Change

Sometimes a venue that includes regular iPass hotspots will temporarily change its Wi-Fi access for a specific event, which can cause confusion with new, temporary access changes. For example, a hotel hosting an event may ask all participants to use a special password for wireless access during the duration of the event. During that time, the iPass hotspot may not be available by normal authentication, which will make it unavailable to iPass users. This is usually a venue-specific (and temporary) behavior that iPass cannot influence.

Coincidence

A user may come across a network that just happens to have the same SSID as one of those in the iPass directory. This is rare, but can happen.

Prevention

The following provisions will be helpful to prevent connection failures to Wi-Fi hotspots.

User Education

User education is key. When orienting new users on the iPass service, it is important to mention the potential situation, and instruct them that they may have to choose an alternate hotspot or even connection type (such as Mobile Broadband) to complete their connection.

Open Mobile Alternate Connection

If Open Mobile for Windows fails to authenticate to an iPass hotspot, it will attempt to connect the user as a non-iPass one. As a result, the user will still have a chance to connect to a local network, even if this is not an iPass network.

Open Mobile PPR Feature

For Open Mobile for Windows 1.4.1 clients and later, the Prohibit, Prefer, or Rename (PPR) feature provides granular management for problematic networks. Specific networks can be annotated so that users can see additional information about them, or can even be prevented from displaying altogether. PPR works at the profile level, so all users with a given Open Mobile profile will be affected by the PPR settings.

Open Mobile 1.4.1 for Windows customers who encounter a network name that produces a false identification as an iPass network can use the PPR fixture to assist users who are attempting to connect to the network.

For example, an annotation could be created to clarify an SSID to users, such as: “Not all locations with this name are iPass hotspot locations.”

Alternatively, in the case where the access for a network has been temporarily changed, such as at a hotel venue, the network could be temporarily excluded (prohibited) from the Available Networks list for all users of the Open Mobile profile.

Go to: Other Product Documents > Tech Notes

hotspots, wi-fi, tech notes

From:
http://help-dev.ipass.com/ - **Open Mobile Help**

Permanent link:
http://help-dev.ipass.com/doku.php?id=wiki:ebook

Last update: **2013/02/05 22:21**