



Open Mobile 2.4 for Android Administrator Guide

VERSION 1.01, JULY 2012

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065 USA

www.ipass.com
+1 650-232-4100
+1 650-232-0227 fx

TABLE OF CONTENTS

Welcome to Open Mobile	5
Documentation.....	5
Features and Benefits	5
Key Features	5
Key Benefits.....	6
Creating a Profile	8
The Open Mobile Portal.....	8
Creating a Profile	8
Profile ID and PIN	9
Profile ID	9
PIN.....	9
Profile Finder	10
Accounts	10
Username	10
Password	10
Domain	10
Prefix.....	11
Authentication Formats.....	11
Networks and Policies	12
Wi-Fi Networks	12
Preferred and Prohibited Networks	12
Hotspot Finder	12
Client Look and Feel	12
Publish the Profile	13
Distributing and Installing	14
Technical Requirements	14
Supported Languages	14
Distribution Methods	14
Open Mobile Portal	14
Market Distribution.....	15
Installation	16

TABLE OF CONTENTS

Activation Email	16
Downloading from the Android Market	16
Private Installer	16
Unactivated Clients	17
Activation Failure Logs	17
Upgrades	17
Important Note on Upgrades	17
Uninstallation	17
 The Open Mobile Interface	 18
Dashboard	18
Connection Manager	19
Usage Meter	19
Usage Meter	19
Application Data Usage	20
Recent Connections	20
Hotspot Finder	21
Options	22
About	22
Account Settings	23
Usage Settings	23
 Wi-Fi Connectivity	 25
Network Types	25
Security	25
iPass Hotspot Connectivity	25
Non-iPass Hotspot Connectivity	25
Inherited Connections	25
 Forced Wi-Fi Auto-Connect (3G Offloading)	 27
The User Experience	28
 Brands	 29
Before Creating a Brand	29
After Creating a Brand	29

TABLE OF CONTENTS

Branding Your Client	29
Creating a Custom Package Name (Optional)	30
Creating and Editing a Client Brand	30
Publishing a Brand	31
Applying the Brand to a Profile	32
Distribution.....	32
Upgrading from a Previous Version	32
Support for Open Mobile	33
Troubleshooting Logs.....	33
Troubleshooting Tips	33

Welcome to Open Mobile

iPass Open Mobile™ makes secure, simple, and effective network access a reality. No matter where you are, your client provides on-demand global connectivity around the world. As an administrator, you will use the Open Mobile Portal to configure your client profiles, test, and then deploy clients to your user base. You can also use Open Mobile Insight to run reports on your user base, usage patterns, and client deployment.

Documentation

The following additional documentation is available on the Open Mobile Portal:

- *iPass Open Mobile Quick Start Guide*: gives users a quick summary of how to install and connect with your client app.
- *iPass Open Mobile Release Notes*: includes news and information about the latest release of Open Mobile.
- *iPass Open Mobile Portal Guide*: explains use of the Open Mobile Portal, the browser-based configuration platform for managing Open Mobile.
- *iPass Open Mobile Portal Release Notes*: includes news and information about the latest release of the Open Mobile Portal.

Features and Benefits

This chapter summarizes the key features and benefits of Open Mobile.

Key Features

Network Support

Open Mobile includes support for public, private, corporate campus, home and personal Wi-Fi.

Intuitive User Experience

The client provides a simple, intuitive user experience.

- Lightweight, always-on connectivity management agent across home, at-work and mobile access methods.
- Automatic network detection.
- User profiles enable configuration and customization of the client's capabilities.

Smart Network Selection

Smart Network Selection assists the user in connecting.

- Automatically detects Wi-Fi connections.
- Notifies user of available access, sorted by a customer-defined mix of cost, performance, and security considerations.
- Auto-connects to preferred networks, based on IT policy, to create automatic connectivity.

Authentication

Easily authenticate users across the worldwide iPass Network.

- Use existing enterprise user credentials to connect to the iPass Mobile Network.
- iPass can even host an LDAP server and authenticate for you.

Web-based Management Portal

The Web-based Open Mobile Portal provides these capabilities:

- Client configuration and testing.
- Client deployment and installer packaging.
- Basic reporting on usage.
- Access to iPass Ticketing.
- iPass billing and account information.

Profile Configuration and Testing

Open Mobile profiles enable you to customize the user experience based on the mobility needs of your enterprise.

- Web-based configuration, validation, testing and provisioning greatly simplifies service creation.
- Design your own mobility footprint including iPass, corporate, personal, and third-party public networks.
- Profiles can be customized for business organizations, departments, or user roles.

Support

- Extensive logging capabilities and capability to enable users to e-mail logs to their customer support staff (using Gmail).

Languages

- Open Mobile is available in English, Simplified Chinese, Traditional Chinese, Dutch, French, German, Italian, Japanese, Korean, Spanish, and (for Android OS 2.2 and later) Thai.

Key Benefits

Open Mobile provides a simple, consistent interface for all connectivity options, on and off the iPass network.

Simple Mobility Experience

- The app enables mobile professionals to connect to the Internet using Wi-Fi networks around the world.
- It provides a lightweight, always-on connectivity management agent across home, at-work, and mobile access.
- Connecting to disparate networks is managed for the user automatically. Users need not engage in the often-challenging process of entering SSIDs, or figuring out which network or connection manager to use.
- Log in to third-party networks is simplified. Users are assisted to access non-iPass Wi-Fi locations by automatically presenting the venue's logon window and procedures.
- OpenAccess networks, in the iPass network footprint, provide free Wi-Fi connectivity.

Smart Management Control

- Web-based Portal enables IT to provision, deploy, and manage enterprise mobility, including the ability to

manage the end user experience when connecting to any type of network.

- Configuration flexibility and automation.
- Mix and match networks into your own custom footprint.
- Give different user segments different connectivity options and rules based on need and cost envelope.
- Test and deploy software easily and automatically.

Security Solutions Integration

- Universal Internet AAA: You can implement a universal authentication and authorization process across all Internet connections, regardless of provider, leveraging your existing user directory.

Creating a Profile

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 Customer Care tickets.
- Download important documentation.
- Review your iPass accounts, including invoices and outstanding balances
- Run reports on your user data.

Complete instructions for using the Open Mobile Portal are contained in the *iPass Open Mobile Portal Guide*.

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 2.4*.
4. Click **Save & Continue**.

You can now edit the profile to enable your desired features. Complete instructions for creating and editing client profiles are contained in the *iPass Open Mobile Portal Guide*.

Profile ID and PIN

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, select **Edit** (circled in red in the screenshot above). The **Edit Profile Details** dialog box is displayed.
2. Enter a PIN and select **Save**.

Once you have published to Test, you can no longer change the PIN.

Profile Finder

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.

Accounts

By configuring Accounts, you can select and customize the Account Credential fields of your end users.

Username

Username is required for iPass authentication. You can change how this field is labeled in the client (or select the default Username label).

Password

A password is required for iPass authentication. You can change how this field is labeled in the client (or select the default Password label).

Domain

A routing domain is required for iPass authentication. The routing domain differentiates 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, but 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). Domain can be configured as follows:

Option	Description
Pre-Filled Domain	You can choose to pre-fill the domain field with a fixed value. If only one domain is 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	Allows users to type in their own domain name. (If the user is part of a large list of domains, or the

Option	Description
Entry	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.

Option	Description
Pre-Filled Prefix	You can choose to pre-fill the prefix field with a fixed value. If only one prefix is used, then pre-filling the prefix field (and making it non-editable) will ensure that the user utilizes the correct prefix.
Drop-Down List	You can choose to pre-configure a list of prefixes from which the user can select.
User Text Entry	Enables users to type in their own prefixes.
Allow Edit	If enabled, the user can edit the pre-populated prefix.
Hide Field	You can choose to hide a pre-filled prefix field from users completely.

Authentication Formats

You can define your own format for authentication strings to be used with all connections made with a given account definition. Authentication string formats are constructed from tokens, each representing a portion of the authentication requirements. You can use any of the following tokens to assign a format to the authentication string for the profile.

Attribute	Token	Description
Network Prefix	%p	Prefix used when authenticating to the network.
Network Suffix	%s	Suffix used when authenticating to the network.
Customer Prefix	%a	Prefix associated with the account defined for use when authenticating to the network.
Username	%u	Username used when authenticating to the network.
Customer Domain	%d	Suffix associated with the account defined for use when authenticating to the network.

An example of a valid authentication format would be %p%u%d. Assume these values for the tokens:

- %p (network prefix) = EXAMPLECO/
- %u (username) = testuser
- %d (customer suffix) = testdomain.com

The resulting authentication string passed would be:

EXAMPLECO/testusertestdomain.com.

If no forward slash were part of the network prefix, the string would be EXAMPLECOtestusertestdomain.com.

Networks and Policies

Configuring the Networks and Policies will enable you to add Wi-Fi directories to the profile, enable Auto-Login, and redirect the Hotspot Finder to another site. You have to configure Wi-Fi networks to enable Wi-Fi and assign directories.

Wi-Fi Networks

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 > button to add them to the **Assigned Lists** (on the right). You can add iPass and custom directories. When you are finished, click **Save**.

Do not add custom directories that include networks with walled garden or proxy access to the Internet. These networks may not be able to access the iPass sniff servers used for Internet detection, and as a result, the user will be disconnected.

Authentication Format Overrides

After network lists have been assigned, Authentication Format overrides can be applied by selecting the **Set Authentication Format** link 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.

Hotspot Finder

iPass provides a Wi-Fi hotspot finder at <http://mobile-hotspot-finder.ipass.com/smartphone>. However, you can customize this URL if you would prefer to use a different hotspot finder, by setting a custom URL in the profile. In the Open Mobile Portal, to set a custom hotspot finder, select **Configure** next to **Hotspot Finder**, and then select **Custom** to enter the URL.

Client Look and Feel

If you have branding capabilities enabled, and would like to apply a brand to this profile, click on the **Select a brand** button, choose the brand from the dropdown list, and then select **Save**. Please see *Brands* on page 29 for more information.

Publish the Profile

When you are ready to test the profile, select the **Publish to Test** button in the bottom-right corner (you will have to push it again after reading instructions). After you have finished testing the profile, select the **Publish to Production** button in the bottom-right corner of the Download Installers page.

Distributing and Installing

Technical Requirements

Using Open Mobile requires the following:

- A Wi-Fi capable device running Android OS 2.2 or later, including Android OS 4.0.
- 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

iPass Open Mobile 2.4 is available in English, Simplified Chinese, Traditional Chinese, Dutch, French, German, Italian, Japanese, Korean, Spanish, and Thai.

Distribution Methods

There are two basic methods of distributing Open Mobile, and customers have access to both.

- **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.** 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.

Open Mobile Portal

After creating a profile, select **Download** next to the profile on the **Manage Profiles** page.

The screenshot shows the 'Download Installers' page in the iPass Open Mobile Portal. The page includes a sidebar with navigation options like 'Open Mobile Client', 'Manage Profiles', 'Manage Templates', 'Download Software', 'Device Support', 'Upload Networks', 'Request Domains', 'Register Packages', and 'Mobile Number Mgmt'. The main content area displays profile details (Profile Name, Status, Profile ID/Version, Software, Description, PIN) and a 'Download' section. This section contains instructions for downloading the app from the Android Market and activating it. Two red arrows highlight key features: one points to the 'Create Email' and 'Copy to Clipboard' buttons, labeled 'Android Market Download Instructions', and the other points to the 'Download Software and Profile Installer' link, labeled 'Private Installer (.apk) File'.

Market Distribution

The Open Mobile Portal includes user instructions for downloading and activating the client. By selecting the **Create Email** button, an email will open with the default instructions included in the body. By selecting the **Copy to Clipboard** button, you can paste the default instructions wherever they are needed (website, document, or text editor, for example).

Activation by URL

The activation and download instructions include an activation link (in the second step). After the user downloads the app, it can be activated by tapping on the activation link and selecting the activation link from the popup menu.

Private Distribution

To download an installer (.apk) file, select **Download Software and Profile Installer**.

Here are a few direct distribution options:

- Post a download link on a Web site, then providing the link to the end users by email.
- Email the private installer as an attachment. (Note that some email clients may not properly handle the .apk file attachments.)
- Upload the private installer to your private version of the Android Market.

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.

Installation

Activation Email

A pre-written email with download and activation instructions is available in the Open Mobile Portal (see **Market Distribution** above). 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.

Downloading from the Android Market

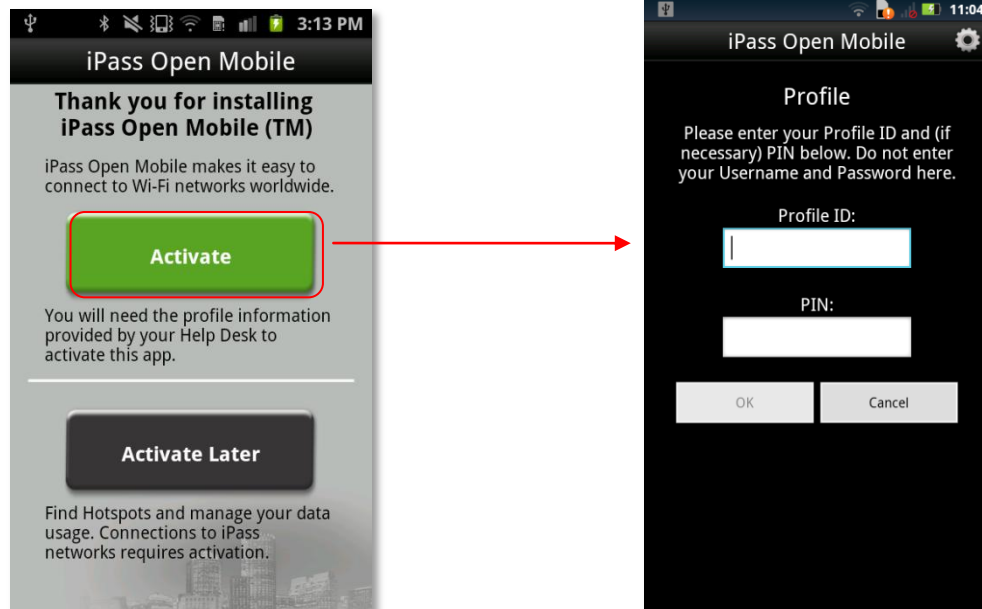
Alternatively, if the user knows the Profile ID and PIN, the app can be downloaded from the Android Market and activated from the Welcome Screen.

To install the app from the Android Market:

1. Download the app from the Android Market.
2. On the Welcome Screen, tap the **Activate My Account** button.
3. Enter your Profile ID and (if necessary) PIN.

*If you are using a Test profile, tap three times on the bottom of the screen (under the **OK** button) to enter Test Profile Mode before entering your Profile ID and PIN.*

4. Tap **OK**.



Private Installer

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, link to download, 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 Now**.

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.

Upgrades

All users will receive software upgrades from the Android Market (regardless of how the app was distributed).

Important Note on Upgrades

To ensure that your users receive important upgrades, we recommend that you have them go to their **My Apps** section in the Android Market and check **Allow automatic updating** next to the app entry.

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.

The Open Mobile Interface

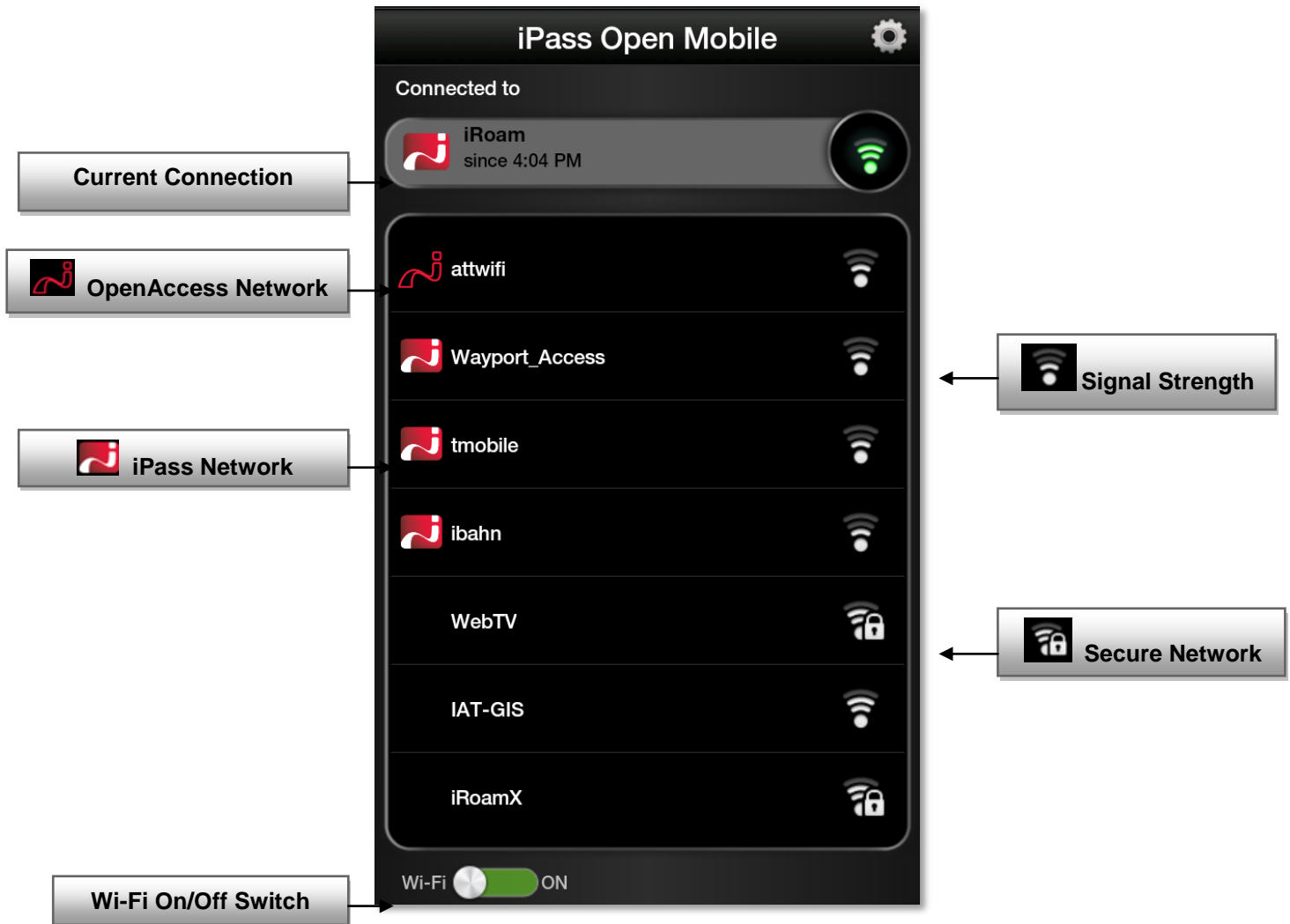
The Open Mobile interface is illustrated here.

Dashboard

There are three main buttons on the dashboard with an options button in the top right corner. The three main buttons represent your current connection (the Connection Manager), your past connections (the Usage Meter), and your future connections (the Hotspot Finder).



Connection Manager



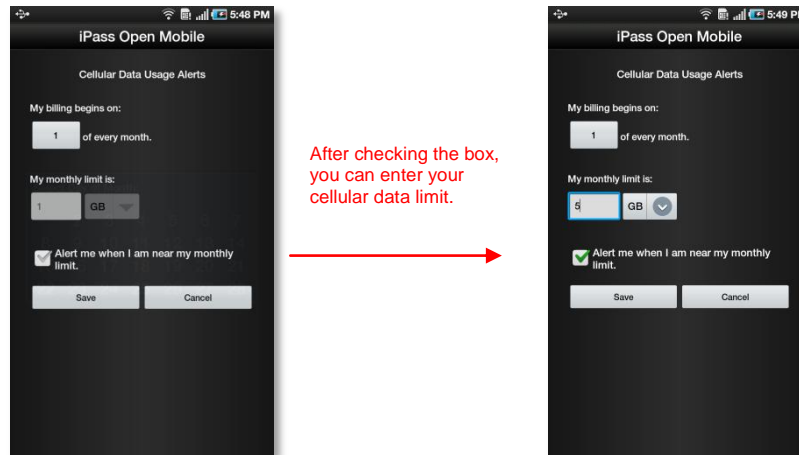
Each app displays Available Networks and their signal strength. The list is refreshed every 15 seconds. To connect or disconnect from a network, simply tap on it.

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.

Usage Meter

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** then tap the box under **My monthly limit is**.



Application Data Usage

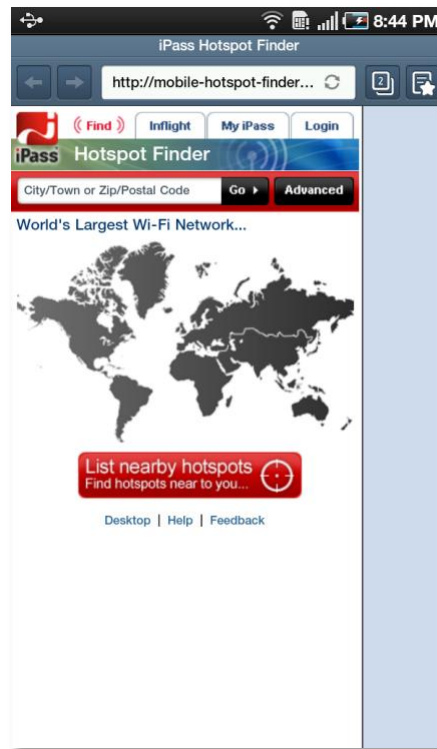
This dialog will display a list of the user's top ten applications in order of their data usage (showing the total usage and each applications percentage of the total).

Recent Connections

This dialog will display your twenty most recent network connections with a timestamp of when the connection happened.

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

Hotspot Finder

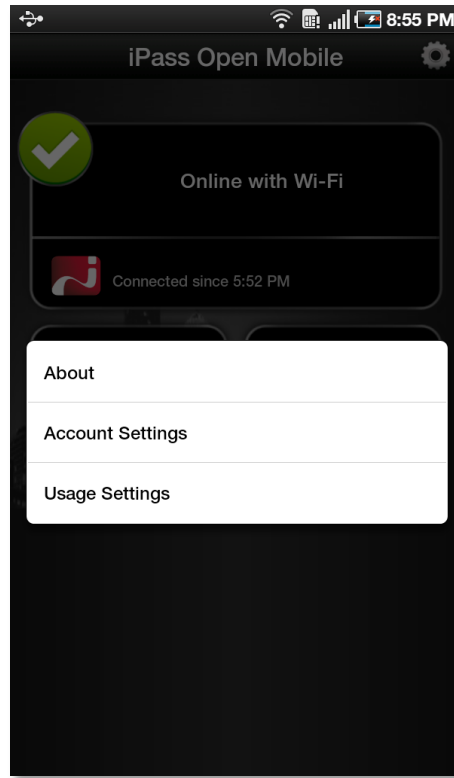


Open Mobile includes a Hotspot Finder that enables users to locate iPass Wi-Fi hotspots anywhere in the world. Users can enter a location in the search box or tap the **List nearby hotspots** button for a list of hotspots and their locations. The Hotspot Finder requires an Internet connection to function.

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

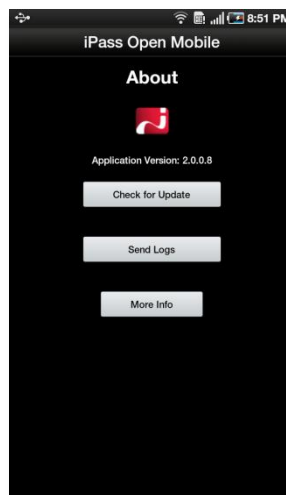
Options

Tapping the **Options** button will open a window with three options: **About**, **Account Settings**, and **Usage Settings**.



About

There are three buttons on the **About** dialog: **Check for Update**, **Send Logs**, and **More Info**. **Check for Update** will check for any available Profile and Directory update (not software update)—these updates happen automatically every 24 hours. **Send Logs** will open an email with an attachment of your current logs to your IT Help Desk (see page 33 below for more information on this feature). **More Info** will display more information on your version of Open Mobile.



Account Settings



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

Auto-Connect

The Auto-Connect feature lets users automatically connect to OpenAccess and iPass-authenticated networks (a zero-click experience). If enabled, Auto-Connect can make connecting to the Internet a 'zero-click' experience.

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.

Auto-Connect will be disabled if "Allow User to Save Password" is disabled in the user's Open Mobile profile.

Usage Settings

The user can set cellular data usage limits and their monthly billing cycle for the usage meter under Usage Settings. For more details, see the Usage Meter section on page 19.

The screenshot shows the 'iPass Open Mobile' app interface on an Android device. The status bar at the top displays the time as 5:48 PM and various system icons. The app title 'iPass Open Mobile' is at the top of the screen. Below it, the section 'Cellular Data Usage Alerts' is visible. The first setting is 'My billing begins on:', with a numeric input field containing '1' and the text 'of every month.' The second setting is 'My monthly limit is:', with a numeric input field containing '1', a unit dropdown menu showing 'GB', and a small downward arrow icon. Below these settings is a checkbox labeled 'Alert me when I am near my monthly limit.', which is currently checked. At the bottom of the screen are two buttons: 'Save' and 'Cancel'.

Wi-Fi Connectivity

Open Mobile serves as a Wi-Fi connection manager that can be used to connect to various types of Wi-Fi networks. The iPass website includes a Hotspot finder that can be used to locate iPass Network access points, located at <http://mobile-hotspot-finder.ipass.com/smartphone>. However, the app can also be used to connect to non-iPass network access points, making it truly a universal Wi-Fi connection manager.

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.

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.

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.

Forced Wi-Fi Auto-Connect (3G Offloading)

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.
- The Wi-Fi hotspot SSID must be in the custom directory.
- The user's credentials have been entered and saved in the app.
- The Android device must be 3G-enabled.
- 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.

Directory	Auth Format Override	Enable USID	Forced Auto-Connect
DTAG T-Mobile Direct	Default	No	Yes
OpenAccess	Default	Yes	No
North America	Default	Yes	No

Buttons: Cancel, Save, Reset

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 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, any 3G connection will be ended (if there is one), and a Wi-Fi connection will be made.

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), 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, any 3G connection will be ended (if there is one), and a Wi-Fi connection will be made.

Brands

Branding capabilities are optional and may not be available on your account. You can brand the client under 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. Default images are illustrated in the Open Mobile Portal.

The set of elements you can brand depend on whether you have the default package name or a custom package name (these additional elements depend on a custom package name to work properly). The ability to create a custom package name is optional and may not be available to your account at this time.

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

If the requirement is an image file, the file dimension is given in pixels.

Default Package Name

Branding Element	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	2.0 and later
Image or Icon	
Logo	75px (w) x 75px (h), PNG format, file size max 11 KB
OpenAccess	20px (w) x 20px (h), PNG format, file size max 11 KB
iPass Network	20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Network	20px (w) x 20px (h), PNG format, file size max 11 KB

Custom Package Name

Branding Element	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	2.0 and later
Image or Icon	
Logo	75px (w) x 75px (h), PNG format, file size max 11 KB
Splash Screen	480px(w) x 800px (h), PNG format, file size max 100 KB
Background	720px (w) x 1280px (h), PNG format, file size max 1 MB
OpenAccess	20px (w) x 20px (h), PNG format, file size max 11 KB
iPass Network	20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Network	20px (w) x 20px (h), PNG format, file size max 11 KB
Text	
Application Name	Alphanumeric string, max 20-25* characters
Network Alert Message	Alphanumeric string, max 80 characters
Installer	
Launcher Icon	72px (w) x 72px (h), PNG format, file size max 11 KB
Notification Icon	24px (w) x 24px (h), PNG format, file size max 11 KB

**Keep the application name as short as possible. A long application name may not display correctly on some device screens. You can use the interactive Image Map to ensure that your Application Name fits.*

Creating a Custom Package Name (Optional)

Creating a custom package name is optional and may not be available to your account at this time. 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 the default with each upgrade, and therefore, they are only available when a custom package name has been applied.

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 and Editing a Client Brand

To create a new client brand for a supported platform:

1. Log in to the Open Mobile Portal, and select the **Account** tab.
2. Under **Branding**, click **Client Options**.
3. Click the **Create a Brand** button.

4. Enter the fields on the **Create a Brand** tab:

- In **Brand Name**, enter a new brand name.
- After **Platform**, select **Android**.
- If you see a **Class** field (optional), select a class from the dropdown.
- After **Software Version**, select the software version from the dropdown.
- If you see a **Package Name** field (optional), select a package name from the dropdown.

5. 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.

6. When the brand is complete, click **Save**.

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

Visual Style Guidelines

When creating a new look for your client application, some guidelines can be helpful to improve the appearance of your new user interface.

Keep your choice of colors within a monochromatic family of hues (such as blue, aqua, or green) to promote color harmonies.

Use a maximum of three separate shades to simplify the client's appearance.

Choose colors with a low saturation to avoid dazzling the viewer.

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

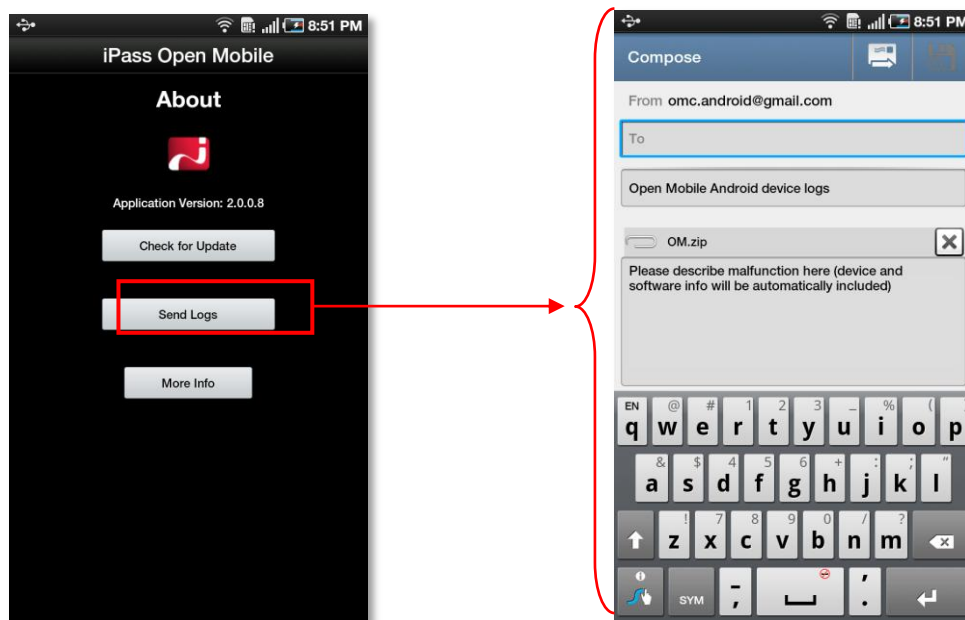
There are two upgrade scenarios:

- 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.

Support for Open Mobile

Troubleshooting Logs

Open Mobile enables users to send troubleshooting logs for support using the **Send Logs** button. These logs are located in the directory /sdcard/iPass/OM/Log. Logs can be sent by corporate email, standard email, or by SMS message.



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.

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 not just a successful association. The client 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.

Copyright ©2012, iPass Inc. All rights reserved.

Trademarks

iPass, iPassConnect, ExpressConnect, iPassNet, RoamServer, NetServer, iPass Mobile Office, DeviceID, EPM, iSEEL, iPass Alliance, Open Mobile, WiFi Mobilize, and the iPass logo are trademarks of iPass Inc.

All other brand or product names are trademarks or registered trademarks of their respective companies.

Warranty

No part of this document may be reproduced, disclosed, electronically distributed, or used without the prior consent of the copyright holder. Use of the software and documentation is governed by the terms and conditions of the iPass Corporate Remote Access Agreement, or Channel Partner Reseller Agreement.

Information in this document is subject to change without notice.

Every effort has been made to use fictional companies and locations in this document. Any actual company names or locations are strictly coincidental and do not constitute endorsement.