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.

Topics

Latest Release Documents

- Open Mobile 2.6.0 for Android Quick Start Guide
- Open Mobile 2.6.0 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

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

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

Last update: **2012/08/07 19:27**

Installation

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

System Requirements

Open Mobile 2.6.0 for Android has the following system requirements:

- A Wi-Fi capable device running Android OS 2.2 or later, including Android OS 4.0 or 4.1.
- 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 is available in English, Simplified Chinese, Traditional Chinese, Dutch, French, German, Italian, Japanese, Korean, Spanish, and Thai.

Required Network Configurations

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

Installation and Activation

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.

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 **Activate**.

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, 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.

installation, activation, requirements

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

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

Last update: **2012/08/07 19:27**

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.

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

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

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

Last update: **2012/08/07 19:27**

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 selecting the activation link from the popup menu.

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.
android, distribution, android market, upgrades, activation

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

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

Last update: **2012/08/07 19:27**

User Interface

The Open Mobile interface is simple and easy to use.

Dashboard

The **Dashboard** section includes three main buttons, with the **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

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.

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

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

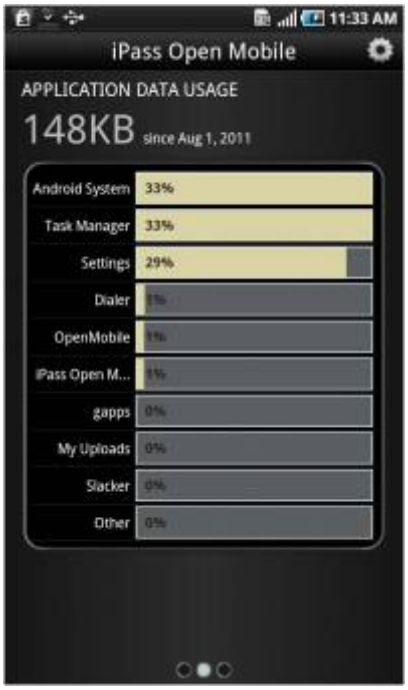
After checking the box, you can enter your cellular data limit.

Recent Connections

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



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).

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**.

- Tap Check for Updateto check for any available Profile and Directory update (not software update)—these updates happen automatically every 24 hours.
- Tap Send Logsto select a method to send your current logs to your IT Help Desk.
- Tap More Infofor 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

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.**

auto-connect, hotspot finder, usage limits, android

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

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

Last update: **2012/08/07 19:27**

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.

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

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

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

Last update: **2012/08/07 19:27**

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. 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.

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.

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

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

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

Last update: **2012/08/07 19:27**

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.

look and feel, branding, android

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

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

Last update: **2012/08/07 19:27**

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.

3g offloading, android

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

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

Last update: **2012/08/07 19:27**

On-Campus Roaming

Available for: Android 2.6.0 and later clients only

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.

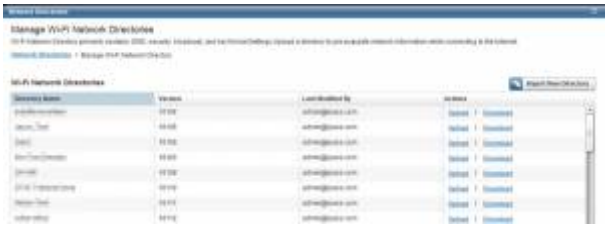
Enabling OCR for a Profile

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.



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.

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.

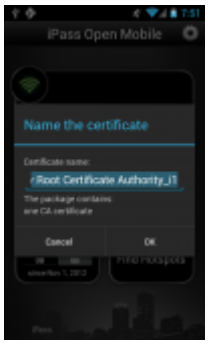
Next Steps

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.



ocr, 802.1x

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

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

Last update: **2012/08/07 19:27**

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.

A complete list of branding elements is shown here.

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.

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.

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.

branding, android

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

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

Last update: **2012/08/07 19:27**

Support

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 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.

support, troubleshooting, android

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

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

Last update: **2012/08/07 19:27**