iPass Open Mobile Portal 2.7
Administrator Guide

VERSION 1.0, JUNE 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

The Open Mobile Portal

The Open Mobile™ Portal is a powerful, Web-based tool that enables you to manage all of your Open Mobile account information in one place, including configuration and deployment of your Open Mobile clients.

Portal Requirements

Using the iPass Open Mobile Portal requires the following:

- An Internet connection.
- One of the following browsers, with both JavaScript and Adobe Flash Player 10 enabled:
  - Internet Explorer 8 or later.
  - Mozilla Firefox 3.5 or later.

> *To check your version of Adobe Flash Player, browse to http://www.adobe.com/software/flash/about.*
>
> *To install the latest version, browse to http://get.adobe.com/flashplayer.*

Logging In

Portal users can log in using either Open Mobile username, or email address. Email address can be a convenient way of logging in if the username has complex prefixes or domains.

To log in to the Open Mobile Portal,

1. Browse to https://openmobile.ipass.com.
2. In **Login**, enter either your email address or your Open Mobile user name. (Login is not case-sensitive.)
3. In **Password**, enter your Open Mobile password.

Login Identity

In order for Portal administrators to log in to the Portal, you must add them as Portal users under **Account | Administrator Provisioning.** They can then use either their email address or their Open Mobile network access credentials to log in.

Once logged in to the Portal, your login identity is shown in the navigation bar at the top of the page.

Idle Timeout: For security purposes, you will be logged out of the Portal automatically after 30 minutes of inactivity.

Navigation

The Portal is divided into a set of tabs, each giving access to a distinct set of Portal functions and tools.

- **Dashboard:** Displays commonly used Open Mobile news and information.
- **Configuration:** Enables configuration of Open Mobile profiles.
- **Reports:** Run reports on your enterprise's Open Mobile usage.
- **Account:** Set or edit your account details.

Other tabs may be shown, depending on the iPass products and services your enterprise has chosen.

Each tab may include a set of windows with distinct information. For example, the Dashboard includes separate windows for general information, tickets, and service alerts. You can enlarge these windows to display across the entire page by using the **Resize** button in the upper-right corner of the window. To shrink the window to its original size, click **Resize** again.

> *User access to Portal functionality is governed by the role assigned to the user and by the features that are available to the enterprise. As a result, some user accounts may not have access to all of the functionality described here. See Roles on page 86 for more information on role-based access.*

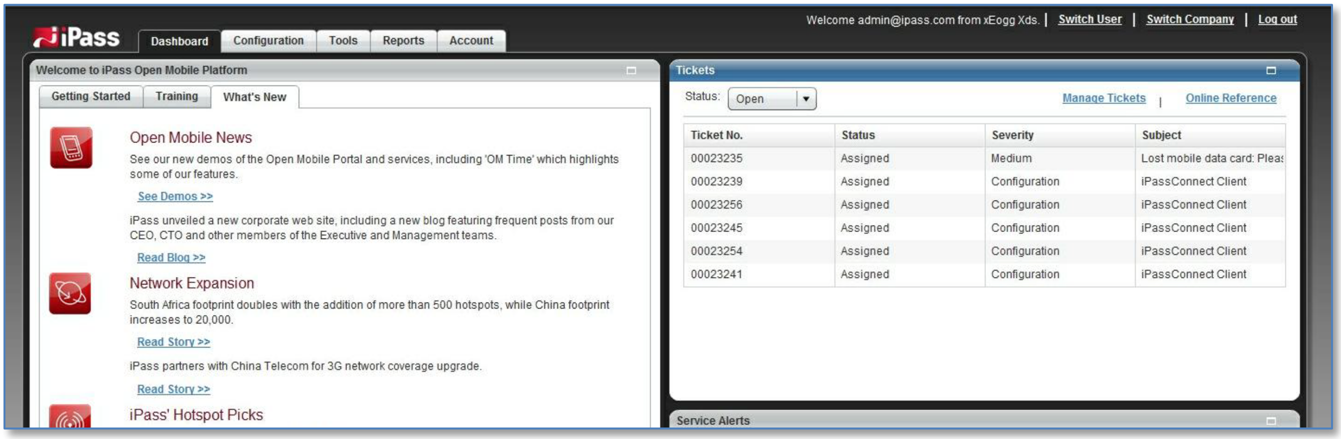
Online Help

There is a help icon (?) in the top-right corner of most pages in the Open Mobile Portal. Clicking on the icon will open a window with helpful information on that particular page.

> *Some Administrators have the ability to remove these links in the Account tab, see page 92 for more information.*

The Dashboard Tab

The **Dashboard** is your central location for managing your Open Mobile clients.



Welcome admin@ipass.com from xEogg Xds.

Welcome to iPass Open Mobile Platform

Open Mobile News

See our new demos of the Open Mobile Portal and services, including 'OM Time' which highlights some of our features.

See Demos >>

iPass unveiled a new corporate web site, including a new blog featuring frequent posts from our CEO, CTO and other members of the Executive and Management teams.

Read Blog >>

Network Expansion

South Africa footprint doubles with the addition of more than 500 hotspots, while China footprint increases to 20,000.

Read Story >>

iPass partners with China Telecom for 3G network coverage upgrade.

Read Story >>

iPass' Hotspot Picks

Tickets

Status: Open

Ticket No.	Status	Severity	Subject
00023235	Assigned	Medium	Lost mobile data card: Pleas
00023239	Assigned	Configuration	iPassConnect Client
00023256	Assigned	Configuration	iPassConnect Client
00023245	Assigned	Configuration	iPassConnect Client
00023254	Assigned	Configuration	iPassConnect Client
00023241	Assigned	Configuration	iPassConnect Client

Service Alerts

Welcome

Getting Started

For new users of the Portal, the **Getting Started** tab includes links to important Open Mobile documentation. Documentation includes the Open Mobile User Guides, Open Mobile Administrator Guides, and supporting technical documents.

Training

The **Training** tab includes links to iPass Training programs for both administrators and end users.

What's New

The **What's New** tab includes the latest news and information from the world of Open Mobile.

Online Reference

Click **Online Reference** to launch a searchable repository of iPass documentation.

> *Carrier customers can replace the three Dashboard tabs with a single tab that includes customized content. For more information, see page 89.*

Tickets

The **Tickets** window lists all of your iPass tickets presently on file in your account at Salesforce.com. You can filter the tickets list by Status: Open or Resolved.

To view or edit a ticket, click **Manage Tickets**. The Salesforce.com ticket tracker will open in your Web browser.

Service Alerts

The **Service Alerts** window displays current iPass service and network alert information.

The Configuration Tab

The **Configuration** tab enables you to configure and deploy Open Mobile clients to your end users.

About Profiles

An Open Mobile profile is a set of customization options that determine the features, policy settings, and behavior of the Open Mobile client. Your enterprise can maintain any number of profiles, each addressing the needs of some portion of your user base. For example, one profile could be maintained for your sales department, and another profile could be maintained for your telecommuting workforce.

Each profile is assigned a profile ID, a version number, and a status.

A profile *template* is a collection of pre-configured settings that can be used as the basis for new profile. Using profile templates to create new profiles can speed profile creation and standardize the user experience.

For more information on creating and using profile templates, see page 48.

The Profile Lifecycle

The profile management lifecycle includes the following phases:

- **Configuration:** During the Configuration phase, you configure a profile using the Configuration tools in the Open Mobile Portal. You choose the settings for connectivity, policy, and security for your users. When a profile is being configured, it is considered a draft and has the status of *In Progress.* You may only have one profile at a time with a status of In Progress.
- **Testing:** During the Testing phase, a profile is tested with a limited set of users to make sure it fully addresses the requirements of the set of Open Mobile users for which it is intended. Modifications made to a profile during testing will create a new version of the profile. Profiles being tested have a status of *Test*. You may have any number of Test profiles.
- **Production:** Profiles in Production may be deployed to your Open Mobile user base and have the status of *Production*. You may have any number of Production profiles.

Before Beginning

Before starting your profile configuration, you should have an understanding of the mobility needs of your end users, to determine whether you want company-wide or separate department-level profiles. Other information you should be prepared with includes:

- The operating system platform (Windows, Mac OS X, Android, or iOS).
- Any routing prefixes or domains your company uses.
- Security considerations, such as whether you will integrate a VPN with Open Mobile.
- Policy enforcement considerations, such as whether you will integrate an anti-virus or personal firewall solution.
- If the profile will be based on a template, the name of the template used.

Managing Profiles

You can create a new profile in one of three ways: brand new, from a profile template, or copied from an existing profile.

Creating a New Profile

To create a new profile,

1. Click **Configuration** | **Manage Profiles**, and then click **Create**.
    - **Optional:** if this is your first iOS or Android profile and you would like it to be your favorite profile, click the **Android** or **iOS** button (with the red star) next to the **Create** button. If you already have an Android or iOS profile, these buttons will not appear.
2. On the **Creating a Profile** page, review the information presented, and then click **Continue**.
3. Under **Profile Name**, type the name of the profile. A profile name must be an alphanumeric string, 100 or less characters in length, and can only include the following special characters: ampersand (&), period (.), space ( ), hyphen (-), and underscore (_).
4. Under Description, type a short description of the profile.
5. Under Platform, pick an operating system platform from the drop-down list.
6. Under Software Version, pick a version for the client software from the drop-down list. Version selection will determine the feature base available to you for configuration.
7. Under How would you like to create a profile?, select one of the following:
    - **Create brand new profile:** Create a new profile with empty configuration settings.
    - **Create profile from template:** Use the pre-configured settings from the selected template. If chosen, select the profile template you wish to use from the drop-down list of your published templates. (The name of the selected template is displayed next to the drop-down.)
    - **Create from an existing profile:** Create a copy of an existing profile, which you will then be able to modify. If chosen, select the existing profile from the list that you will copy.
8. Click **Save & Continue.** A newly created profile is automatically assigned a new Profile ID, given a version number of .001, and a status of *In Progress.*
9. To configure the newly created profile, on the **Configure Profile** page, select a configuration setting, and then click **Configure**. (A profile created from a template or from an existing profile will have many or all configuration settings already configured.)
10. Choose the values for the setting as needed, then click **Save.**
11. Continue editing additional configuration settings as desired.
12. When complete, click **Save** to save the profile. (You can also save the profile and go back to edit it in the future.)

Configuration settings are explained in detail beginning on page 16.

Managing Profiles

You can view, edit, and delete profiles on the **Configuration | Manage Profiles** page.

> ***Service Packages:*** *The types of profiles to which your company has access may be restricted by the service package you are assigned. For more information, consult with your Open Mobile service provider.*

Favorite Profile

The favorite profile is the profile you plan to distribute to most of your users. You can favorite, or unfavorite a profile for each platform and class by clicking on the star that appears next to it on the **Manage Profiles** page. When the Profile Finder is implemented in future releases of the clients, it will automatically download the favorite profile.

> *Profiles with a PIN cannot be favorite profiles (otherwise the Profile Finder would not work).*

There are four types of stars:

- **Red Star:** marks a favorite profile (in production)
- **Gray Star:** marks a favorite profile (not published to production yet)
- **Empty Star:** marks all other profiles (not the favorite profile)
- **No Star:** marks profiles with a PIN (that cannot be a favorite profile)

Viewing a Profile

To view the settings for a profile,

1. Click **Configuration | Manage Profiles**.
2. Find the profile you wish to view, and in the **Select an action** dropdown menu next to that profile, select **Manage**.
3. On the **Configure Profile** page, select a configuration setting to edit, and then click **View.**
4. View the settings as needed.
5. When complete, click **Back.**

Editing a Profile

You can edit In Progress and Test profiles. Production profiles may not be edited.

To edit a profile,

1. Click **Configuration | Manage Profiles**.
2. Find the profile you wish to edit, and in the **Select an action** dropdown menu next to that profile, select **Manage**.
3. On the **Configure Profile** page, select a configuration setting to edit, and then click **Configure**.
4. Edit the configuration settings as needed, then click **Save**.
5. Continue setting configuration settings as desired.
6. To edit the profile description, at the top of the **Configure Profile** page, in the blue bar, click **Edit**. In the **Edit Profile Details** dialog, in **Description**, edit the description as needed.
7. (Android profiles only) Optionally, if you wish to set or edit an activation PIN on an Android profile, click **Edit**. In the **Edit Profile Details** dialog, select **PIN**. Then, enter the actual PIN (up to 50 alphanumeric characters in length).
8. If you wish to move this profile to testing, click **Publish to Test**. Otherwise, to save the changes to your profile without changing its status, click **Return to Profile Management**.

Deleting a Profile

You can choose to delete all versions of a profile, or just the latest version. Deleting the latest version of a profile will cause the previous version to become the latest version. (If there is no other version of this profile, the entire profile will be deleted.)

You can delete a profile regardless of its status. Deleting a profile cannot be undone.

To delete a profile,

1. Click **Configuration | Manage Profiles**.
2. Find the profile you wish to delete, and in the **Select an action** dropdown menu next to that profile, select **Manage**.
3. Under **Actions**, select **Delete Profile** from the drop-down list.
4. Select one of the following delete options:
    - **Delete version <N>,** where N is the latest version of this profile. Deleting this version will make the previous version of the profile into the current version. If this is the only version of the profile, it will be completely deleted.
    - **Delete all the profile versions:** This will delete all versions of this profile. This action cannot be undone.
5. Click **Yes, I want to delete it**.
6. Click **Yes** to confirm deletion.

Searching for Profiles

You can search your profiles by Profile Name to locate a particular profile. The search is case-insensitive, and will return all profiles the names of which begin with the text you enter.

To search by profile name,

1. In the **Search Profiles** box, enter the name (or partial name) for which you wish to search.
2. Click **Search**. All profiles matching your search are presented.

Profile Templates

You can speed the process of creating a profile by using a profile *template*, which contains pre-configured settings. Using profile templates to create profiles can provide a consistent connection experience across a company's user base and across those of your child companies. Templates can be created for profiles on any platform.

Profile Template Status

Like profiles, profile templates have a status to reflect their position in the publication process.

- A *draft* template is still in progress, and can be edited as required until it is ready. A draft profile cannot be used to create profiles.
- A *published* template has been finalized and is ready to be used to create profiles. A published template can be shared with a company's child companies. However, a published template may not be edited or deleted.
- Because a published template may be shared with your child companies, it will not include your company-

specific settings like domains, prefixes, and custom network directories. Those settings will need to be re-configured in any profiles created from your published template.

Creating a New Profile Template

You can create a new profile template in one of two ways:

- You can create a profile and then save it as a template, enabling you to re-use the profile's settings or edit them as needed. Best practice is always to create templates this way. Using a published profile as a template will ensure that the profile's settings have already been tested. These tested settings will then be inherited by any profiles based on this template.
- You can save an existing template, modify its settings, and then save it as a new template.

Creating a Template from a Profile

You can create a template from an already existing profile, and then either use it as created, or modify and then save its settings.

To create a new profile template from a profile,

1. Click **Manage Profiles**.
2. From the list of profiles, select the profile you wish to save as a template. Then, under **Actions**, click **Manage**.
3. On the **Configure Profile** page, in the **Action** drop-down, select **Save as Template.**
4. Review the information on the **Getting Started** page, and then click **Continue**.
5. On the **Create a Template** page, enter values for the following:
    - **Template Name:** The profile template name.
    - **Template Description:** An optional short description of the template.
6. Click **Save and Continue**. The template is now saved in the Draft state.
7. On the **Manage Template** page, you can now review any of the template settings by selecting a settings category and clicking **View**. Optionally, click **Configure** to set any values for the template that will be different from the profile it is based on. For example, to adjust the Quick Launch applications configured with the profile template, next to **Quick Launch**, click **Configure**, then edit the Quick Launch settings for the template.

A draft template will remain in Draft status until you publish it.

Creating a New Template from an Existing Template

You can create a template from an already existing template, and then either use it as created, or modify and then save its settings.

To create a template from an existing template,

1. Select **Manage Templates**.
2. On the list of profile templates, select the template you want to create a new template from, and then, under **Actions**, click **Manage**.
3. On the **Manage Template** page, in the **Action** drop-down, select **Save as New Template**.
4. On the **Create a Template** page, enter values for the following:

- **Template Name:** The profile template name.
- **Template Description:** An optional short description of the template.

5. Click **Save and Continue**. The new template is now saved in the Draft state.
6. On the **Manage Template** page, you can now review any of the template settings by selecting a settings category and clicking **View**. Optionally, click **Configure** to set any values for the new template that will be different from the template it is based on. For example, to adjust the Quick Launch applications configured with the profile template, next to **Quick Launch**, click **Configure**, then edit the Quick Launch settings for the template.

A draft template will remain in Draft status until you publish it.

Publishing a Draft Profile Template

A published template can be used to create new profiles and can be shared with your child accounts. A published template may not be edited or deleted. In addition, a published template will not include any company-specific settings like domains, prefixes, custom network directories, and ODF integrations. All of these settings will be removed from a draft template when it is published.

To publish a draft template,

1. Select **Manage Templates**.
2. On the list of profile templates, select the template you want to publish, and then, under **Actions**, click **Manage**.
3. On the **Manage Template** page, click **Publish**.
4. On the **Publish Template** page, select **Yes, I am ready to publish this template**.
5. Click **Publish**. The template is now published.

Sharing a Published Profile Template

You can share a published template with any of your child accounts that match the following criteria:

- The template's platform must be available to the child account (for example, if the template is made for the Mac OS X platform, the account must be able to create Mac OS X profiles).
- The child account must share the same brand as any included in the template.

A shared template may not be unshared.

To share a published template,

1. Select **Manage Templates**.
2. On the list of profile templates, select the template you want to share, and then, under **Actions**, click **Share**.
3. On the **Share Template** page, the child accounts that are eligible for template sharing are listed.
4. Under **Child Accounts**, select the checkbox next to each child account with which you wish to share the template. (To filter out a selection of child accounts, in **Search by Company ID**, enter the name of the child account you wish to search on. Only the accounts matching your search criterion will be shown in the list.)
5. Click **Share**. Your template is now available for use by your child accounts.

Deleting a Draft Profile Template

You may delete templates with a status of Draft.

To delete a draft template,

1. Select **Manage Templates**.
2. On the list of profile templates, select the template you want to delete, and then, under **Actions**, click **Manage**.
3. On the **Manage Template** page, in the **Action** drop-down, select **Delete Template.**
4. Click **Yes, I want to delete it** to confirm deletion.

Profile History

A profile's history includes all of its previous versions. These are recorded on the Open Mobile Portal and can be managed as required. (Profile history does not include profile versions you have deleted.)

To view the history of a profile,

1. Click **Configuration** | **Manage Profiles**.
2. On the list of existing profiles, select the profile you wish to view.
3. Click **+.** The list expands to show all previous versions of the profile.

About Profile Version Numbers

A profile's version number will indicate the profile's status in its lifecycle—whether it is draft, test, or production. Profile version numbers take the form <production version>.<test version>, where <production version> is an integer, and <test version> is a three-digit number.

- Production profile numbers end in .000.
- If the version number ends in a number other than .000, the profile is a draft or test profile.

For example, a profile with version number 3.000 is a production profile, and profile with version number 3.004 is a test profile (in fact, the fourth version of that particular test profile).

As a profile proceeds through its lifecycle (from draft, to test, to production), it is automatically assigned a version number.

- Editing and saving a test profile will create a new test version, and will automatically increment the test version number by .001.
- Publishing a test profile to production will increment the <production version> number by 1.000 and reset the <test version> number to .000.

Profile version numbering is automatic as you move it through its lifecycle. A version number cannot be manually assigned to a profile.

For example, a newly created profile is automatically assigned a status of Test and a version number of 0.001. As the profile is tested and edited, and successive versions are created, the version number is automatically incremented by .001 to 0.002, 0.003, and so on. Finally, when the test profile is published to production, the profile version is automatically changed to 1.000. Later successive edits of this production profile (for testing) would then increment that number to 1.001, 1.002, 1.003, and so on.

Upgrading Profile Versions

Production profiles will not be upgraded to a new profile version unless a new production version is available (that is, a new profile ending in .000).

For example, a user has profile version 2.000 (a production profile). The Open Mobile administrator is testing new versions of this profile and generates test versions 2.001 and 2.002. A user attempting to upgrade the 2.000 profile would be informed that no profile upgrade was available (because the only profile versions available are test profiles). To enable a profile upgrade of a production profile, one of these test versions could be pushed to production as version 3.000. The creation of a production version would allow users with 2.000 to upgrade to 3.000.

Migrating a Profile to a New Software Version

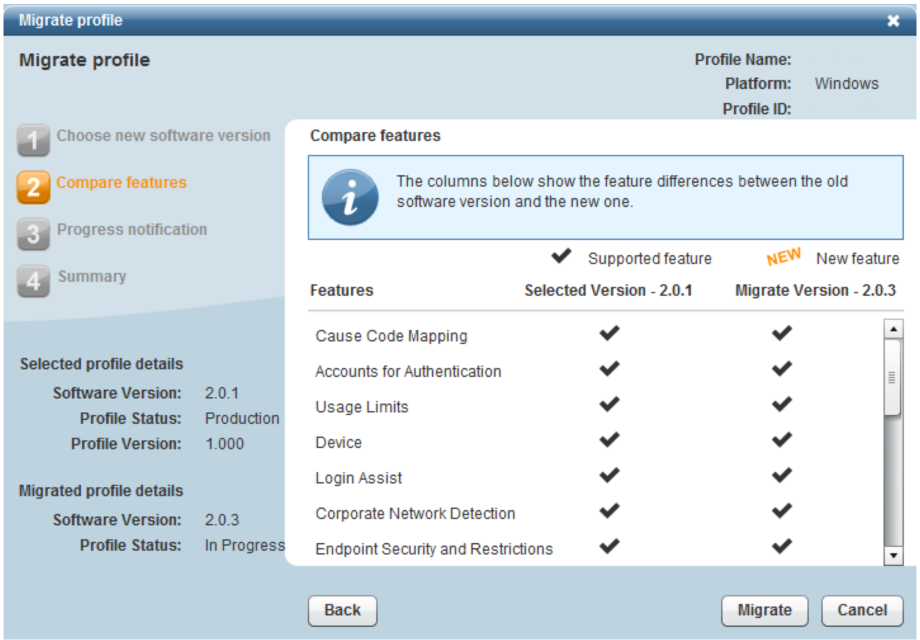
Production profiles created for some versions of Open Mobile for Windows can be migrated to new versions of the Open Mobile software. You can migrate Open Mobile 1.4.1 profiles to Open Mobile 1.4.3, and Open Mobile 1.4.x profiles to Open Mobile 2.0.1.

However, a new version of Open Mobile may include different settings than those used by an earlier version, or even include entirely new features. The Profile Migration tool enables you to compare these different or new settings between the two software versions and then decide whether to perform the migration.

Updating the Profile

The migration process creates a new version of the profile, with a status of In Progress, which you can configure, deploy to test, and eventually publish.

For example, production profile P1 has a profile version number of 2.000, and was created for the 1.4.1 version of Open Mobile for Windows. You wish to migrate P1 to use with Windows version 1.4.3. After migration, you would have a new version of P1, named P2, with a version number of 2.001 and a status of In Progress. P2 would be treated like any other In Progress profile, and could be configured, deployed to test users, and eventually pushed to production.



Migrate profile

Profile Name:
Platform: Windows
Profile ID:

Compare features

The columns below show the feature differences between the old software version and the new one.

✓ Supported feature NEW New feature

Features	Selected Version - 2.0.1	Migrate Version - 2.0.3
Cause Code Mapping	✓	✓
Accounts for Authentication	✓	✓
Usage Limits	✓	✓
Device	✓	✓
Login Assist	✓	✓
Corporate Network Detection	✓	✓
Endpoint Security and Restrictions	✓	✓

Selected profile details

Software Version: 2.0.1
Profile Status: Production
Profile Version: 1.000

Migrated profile details

Software Version: 2.0.3
Profile Status: In Progress

To migrate a production profile to a new software version,

1. From the list of profiles, select the production profile you wish to migrate to a new software version, and click **Manage**.
2. On the **Configure Profile** page, in **Action**, select **Migrate** from the drop-down list. The Migration wizard will launch.
3. Review the profile parameters and click **Start**.
4. In **Migrate software version to**, select a new software version from the drop-down list, and then click **Next**.
5. On the **Compare Features** dialog, review the feature comparison between the two versions. A checkmark indicates a feature that is supported in the specified software version, while **New** indicates a feature that is new in the more recent software version. You may need to select values for these new features.
6. After reviewing the differences, click **Migrate**. The migration is performed.
7. Click **Next** to review your results.
8. Click **Close**.

Next Steps

The migrated profile (which will now have a status of In Progress) can now be sent through the normal profile lifecycle: from In Progress, to Test, and then to Production. Users with the migrated profile will automatically be prompted to update their profiles to receive the new version, and to download the new Open Mobile software to accompany it, using the regular update process. For more information on the update process in the Open Mobile client, see the *Open Mobile 2.0.1 Administrator's Guide*, available from the iPass Online Reference as article #3209.

> *When migrating a Windows 1.4.x client to Windows 2.x, the migrated client will receive the newer Windows 2.x skin. To emulate the older UI, you can create a brand with the same look and feel as the older client and include it in the profile.*

Rolling Back a Production Profile

Rolling back a production profile will move all users on the profile to a previous version of the profile. You can only roll back the latest version of a production profile to a previous production version. For example, if a profile had production versions 1.000 and 2.000, version 2.000 could be rolled back, but not version 1.000.

The rollback process creates a new version of the selected profile, with all the settings of the profile to which you have chosen to roll back. The new version will be given a version number of <original number>.001 (for example, 2.001), and a status of *In Progress.* Since you can only have one profile with a status of *In Progress*, the rolled back profile will replace any profile you currently have in progress.

After rollback, you can manage the profile like any other profile, including editing settings and publishing it to Test.

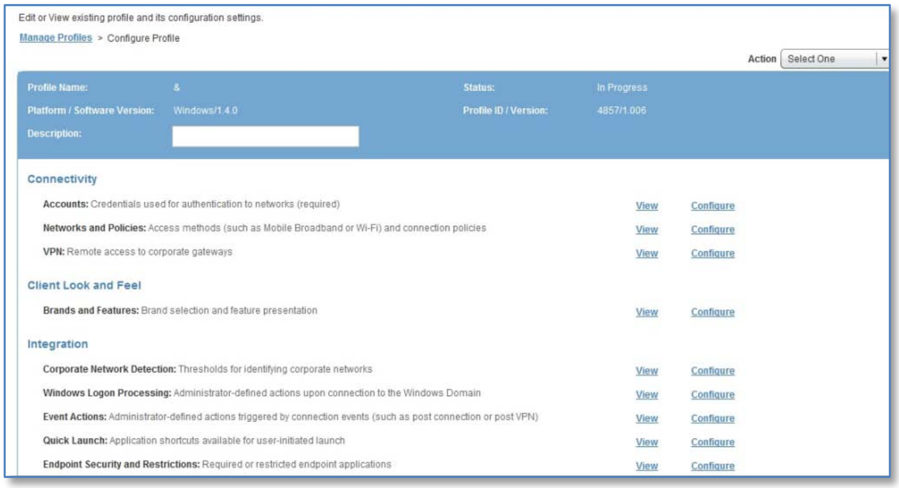
To roll back a production profile,

1. Click **Configuration | Manage Profiles**.
2. On the list of existing profiles, select the profile you wish to roll back, and then click **Manage.**
3. In the **Action** drop-down, select **Roll back to a Previous Production Profile**.

4. An explanatory message is displayed. Under **Select Profile Version,** select the version of the profile to which you wish to roll back.
5. Click **Continue**. The new profile is created.

Configuration Settings

Configuration settings are chosen on the **Configure Profile** page. The page enables you to configure the profile's setting categories.



Edit or View existing profile and its configuration settings.

Manage Profiles > Configure Profile

Action: Select One

Profile Name: &
Status: In Progress
Platform / Software Version: Windows/1.4.0
Profile ID / Version: 4857/1.006
Description:

Connectivity

Accounts: Credentials used for authentication to networks (required)

Networks and Policies: Access methods (such as Mobile Broadband or Wi-Fi) and connection policies

VPN: Remote access to corporate gateways

Client Look and Feel

Brands and Features: Brand selection and feature presentation

Integration

Corporate Network Detection: Thresholds for identifying corporate networks

Windows Logon Processing: Administrator-defined actions upon connection to the Windows Domain

Event Actions: Administrator-defined actions triggered by connection events (such as post connection or post VPN)

Quick Launch: Application shortcuts available for user-initiated launch

Endpoint Security and Restrictions: Required or restricted endpoint applications

Categories displayed on the Configuration page will dynamically change, depending on your choice of operating system and client version. If a category is not shown, it is not available for configuration in the profile. For example, Android 1.1 clients do not support Quick Launch, and would not be shown when configuring an Android 1.1 profile.

Applying Configuration Settings: Profile settings cannot be applied on a partial basis. When a profile is applied to a user's Open Mobile client, the user receives all of the settings associated with that profile: for example, all VPN settings, account definitions, and branding options.

Category	Settings	Available For
Connectivity	*Accounts:* Configure a profile's account definitions and authentication (required). *Networks and Policies:* Configure a profile's connection settings and the network types that your users will connect to (such as Mobile Broadband, Wi-Fi, Ethernet, dial, and DSL). *VPN:* Integrate a third party Virtual Private Network to ensure a secure connection to corporate resources.	Windows, Express (Wi-Fi only), Mac OS X (Wi-Fi, Mobile Broadband), Android (Wi-Fi only), iOS (Wi-Fi only)
Client Look and Feel	*Brands and Features:* Change the appearance of the Open Mobile client and Portal.	Windows, Express, Mac, Android (2.x), iOS (2.1.0)
Integration	*Corporate Network Detection*: Set tests for corporate network connections. *Windows Logon Processing*: Configure optional Windows logon processing. *Event Actions*: Configure actions triggered by connection events. *Quick Launch:* Set applications or URLs for user-initiated launch. *Login Assist:* Facilitate logins to frequently used Web sites. *Endpoint Security and Restrictions:* Set policies to be enforced when connected or disconnected from the Internet. *Run Once Packaging:* Deliver third-party software components. *Proxy Settings:* Enable proxy login. *Conflict Detection:* Configure settings to interoperate with third party connection clients. Custom Profile Attachments: Attach scripts and executables.	Windows, Mac OS X (Event Actions only)
Localization	Localize Message: Localize custom messages	Windows 2.1 and later

Connectivity

Connectivity settings deal with making and managing network connections to a variety of network types.

Manage Accounts

Accounts are used to authenticate users on the iPass network, a VPN, or other network. The definition of an account determines the attributes required for a successful login and authentication. Different account definitions may have different attributes: one account definition might use username and password; a second might use password, prefix, and domain. An account definition represents the attributes required for users to create an account; it does not represent a particular user's login credentials.

> *At least one account is required for your Open Mobile users to authenticate, so creating an account should be the first task you perform when creating a profile.*

For Windows profiles, 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.

Account Attributes

Account attributes are highly configurable to accommodate a variety of login and authentication schemes. This enables you to take granular control over the user's login experience. You can customize account attributes in a variety of ways.

- **Re-labeling:** The field labels for accounts can be changed and customized. For example, you can change the label *Username* to another value, such as *Login Name.*
- **Pre-population:** Many attribute values can be pre-populated with a value of your own choosing.
- **Drop-down list:** For some attributes, users can be prompted with a drop-down list with multiple selections.
- **Hidden:** Some fields can be hidden entirely from the end user.

Attribute Options

Account attributes can be configured as follows:

- **Username:** Username can be re-labeled, pre-populated, and hidden from the end user*.*
- **Password:** Password can be re-labeled, pre-populated, and hidden from the end user. In addition, you can control how Open Mobile caches the password and set the duration of the cache: forever, until Open Mobile is restarted, until sleep or hibernation, a specific interval, or never.
- **Domain:** Domain can be re-labeled. You can also choose to allow the user to enter the domain, to select it from a drop-down list of previously entered domains, or to use a specific domain.
- **PIN:** (Windows 1.4.1 and later clients) Some accounts, such as those used for VPNs, require a Personal Identification Number for authentication. (For example, NCP VPN requires such a PIN.) You can choose to allow the user to enter the PIN or to pre-fill it with a PIN.
- **Token:** (Windows 2.x clients) Authentication token can be re-labeled, pre-populated, and hidden from the end user. You can also specify how long Open Mobile will save the token.
- **Prefix:** Prefix can be re-labeled, pre-populated, and hidden from the end user.
- **Authentication Format:** In some cases, an authentication string that differs from the standard iPass authentication string may be desired.

About 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. Only include tokens for authentication attributes that are or will be enabled for the account.

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. *In Windows clients before 1.4.1, Open Mobile automatically appends a forward slash character (/) to the end of the %a token.* *However, for Windows 1.4.1 and later clients, you must add in the slash character manually after the customer prefix.*
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.
Literal String	N/A	Literal string. For example, if the domain value is always example.com, then example.com could be used as part of the authentication format in place of %d.

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 to Open Mobile would be:

EXAMPLECO/testuser@testdomain.com.

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

Authentication Format Overrides

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 connections of a specific type (such as Mobile Broadband), as well as for directories. Any authorization formats assigned to such accounts will override the more general one.

The hierarchy of accounts works as follows:

- A default (master) account is defined for each entire profile. If no account is assigned at a more specific level, this account and its associated authentication format is used for connections.
- An account can be assigned for a specific connection type (for example, Wi-Fi). You can also define an authorization format to be used with the account, which will override the format defined for the default account.
- An account can be assigned for connections made to specific network directory. Again, you can also define an authorization format to be used with the account, which will override the format defined for the default account.

In addition, you can choose whether to enable USID (Unique Session Identifier) for connections made to networks in the directory.

USID

Each Open Mobile session (and connection attempt) is assigned a Unique Session Identifier (USID) for tracking purposes. By default, USID is prepended to the authentication format before the username (for example, <network prefix>/<USID>/<username>@<domain>.

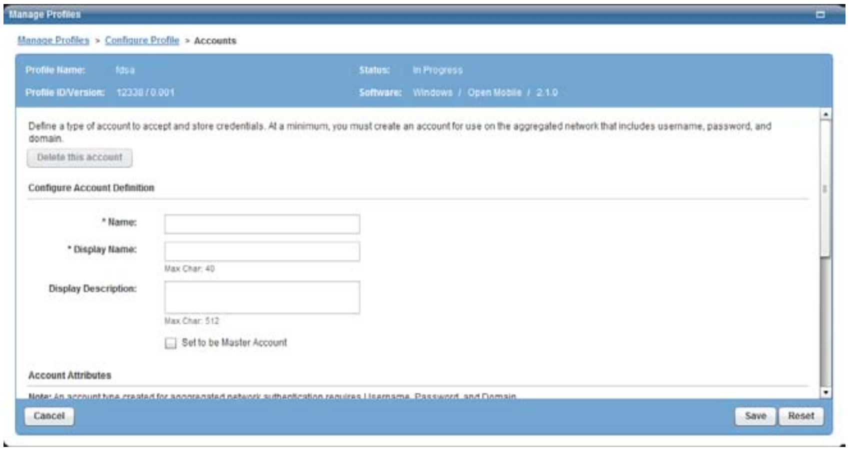
USID is enabled by default for connections made to access points in the iPass network directory. However, because the authentication format with USID may exceed 20 characters in length, which is longer than many networks will support, you can choose whether to include USID in directory-level authentication format overrides, to keep the authentication format under the character limit for custom directories.

See the *Networks and Policies* section on page 20 for more information on defining authentication format overrides for connection types or directories.

Creating an Account Definition

You must define an iPass account before defining other accounts.

For the iPass account, use the account name *iPass*, and select username, password, and domain for attributes.


Manage Profiles
Manage Profiles > Configure Profile > Accounts

Profile Name: fdsa

Status: In Progress

Profile ID/Version: 12338 / 0.001

Software: Windows / Open Mobile / 2.1.0

Define a type of account to accept and store credentials. At a minimum, you must create an account for use on the aggregated network that includes username, password, and domain.

Delete this account
Configure Account Definition

* Name:

* Display Name:

Max Char: 40

Display Description:

Max Char: 512

□ Set to be Master Account

Note: An account type created for aggregated network authentication requires Username, Password, and Domain.

To define an account,

1. Under **Accounts**, click **Define New Account**.
2. Under **Configure Account Definition**, in **Name**, enter the name of the account.
3. In **Display Name**, enter the account name, as you would like it to appear in Open Mobile.
4. In **Display Description**, enter a brief description of the account. This will be displayed to the user when logging in and used as a reminder to the user of login information.
5. If this will be the default account type, select **Set to be Master Account.**
6. Under **Account Attributes**, select the attributes that are required for this account. (Username, password, and domain are required for any account used on the iPass network.) Then, select the configuration settings for each attribute as required.
   i. Username
   ii. Password. (For the Android client, select whether the password can be saved by the user.)
   iii. Domain
   iv. PIN (Windows 1.4.1 or later clients only)

v. Token (Windows 2.x clients only)

vi. Prefix

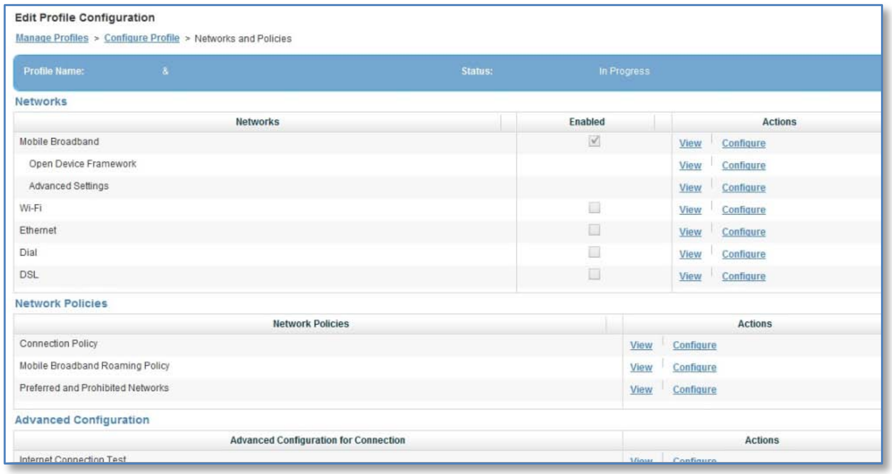
vii. Authentication Format

7. Click **Save**.

> ***iPass End-to-End Encrypted Login (iSEEL):*** *iSEEL uses 131-bit ECC (Elliptic Curve Cryptography) in conjunction with 128-bit Public Key Unidirectional SSL tunnels to protect Internet passwords over the iPass network. Passwords are encrypted before they are ever transmitted over a connection, and they are not decrypted until reaching the iPass POD Transaction Center.*

Networks and Policies

Network and policy settings control the networks to which your users can connect, and the behavior of Open Mobile concerning these networks.



Edit Profile Configuration

Manage Profiles > Configure Profile > Networks and Policies

Profile Name: & Status: In Progress

Networks

Networks	Enabled	Actions
Mobile Broadband	☑	View | Configure
Open Device Framework		View | Configure
Advanced Settings		View | Configure
Wi-Fi	□	View | Configure
Ethernet	□	View | Configure
Dial	□	View | Configure
DSL	□	View | Configure

Network Policies

Network Policies	Actions
Connection Policy	View | Configure
Mobile Broadband Roaming Policy	View | Configure
Preferred and Prohibited Networks	View | Configure

Advanced Configuration

Advanced Configuration for Connection	Actions
Internet Connection Test	View | Configure

Networks

Choose the network types for which to enable connectivity in your Open Mobile client: Mobile Broadband, Wi-Fi, Ethernet, Dial, and DSL. You must enable at least one network type or your users will not be able to connect.

Networks are collected in network *directories*. A network directory is a list of networks for a particular network type, such as Mobile Broadband, Wi-Fi, or Dial. Each network entry in the directory includes all of the necessary attributes to make a connection of that type. Many default iPass network directories are available for inclusion in profiles. In addition, customers can create their own custom network directories and include those in profiles. At this time, custom network directory types include Wi-Fi and Mobile Broadband.

> *Before choosing networks, make sure you have configured at least one account definition.*

To enable and configure a network type,

1. Click **Configure**.

2. Under **Networks**, choose one or more network types to enable.

3. Select an enabled network type, and then click **Configure**.
4. If required, choose an authentication format override for the connection type or directories.
5. Assign any network directories for the connection type to the profile.
6. Save your settings.

Mobile Broadband

Available for: All Windows and Mac 1.2 or later clients

Open Mobile can detect and connect to Mobile Broadband networks.

You must enable Mobile Broadband in order to be able to configure any additional Mobile Broadband settings. These include settings for Open Device Framework, Advanced Mobile Broadband, and Mobile Broadband Roaming Policy.

> *In Windows 1.4.1 clients and later, BlackBerry devices are treated in all respects like Mobile Broadband networks (such as network ranking).*

Authentication Format Override

Available for: Windows 1.4.1 and later clients.

You can specify the authentication format used by an account, with a format used just for Mobile Broadband connections. You can also specify the authentication format for connections made using specific Mobile Broadband directories. These authentication formats will override the account's default authentication format. Authentication tokens used in overrides must already be defined in the account.

> *This is an advanced feature and will not be required for most Open Mobile profiles. For more information on authentication format, see page 17.*

To specify an authentication format override for Mobile Broadband connections,

1. In **Account**, select the account used for Mobile Broadband connections.
2. In **Authentication Format Override**, specify the new format.

To specify an authentication format override for one or more Mobile Broadband directories,

1. Under **Assign or Remove Mobile Broadband Directories**, using the arrow keys, assign one or more directories to the profile.
2. In the **Assigned Directories** column, click **Set Authentication Format**.
3. For each directory in the list for which you wish to use a new authentication format:
   - Under **Account**, select the account used.
   - Under **Auth Format Override**, enter the new authentication format used.
   - Under **Enable USID**, select whether to use Unique Session ID for connections.
4. Click **Save**.

Mobile Broadband Network Directories

By default, your users will be able to connect to iPass Mobile Broadband networks. In addition, you can choose to enable one or more previously uploaded Mobile Broadband networks to which your users can connect.

To add one or more Mobile Broadband networks to Open Mobile, using the arrow controls, move the directories from the **Available Directories** column to the **Assigned Directories** column**.** Use the up and down arrows to change the sort order of the assigned directories.

Open Device Framework Settings

Available for: Windows 1.3 or later clients with Mobile Broadband enabled.

Open Device Framework settings enable you to include support in a profile for Mobile Broadband devices that have been integrated with Open Mobile using ODF. This support can be added to the profile for three different Windows platforms: Windows XP, Windows 7, and Windows Vista. (You must have previously added support for these devices on the **Device Support** page; see page 56 for more information.) For more information on ODF integration, consult the *ODF Training Workbook*, available from the iPass Online Reference as article #3151.

The **List of Supported Devices** shows all devices currently supported by ODF.

To add ODF support for devices to the profile,

1. From the list of supported devices, select the devices for which you wish to add support.
2. For each selected device, select the Windows platforms for which the device will be supported.
3. Click **Save**.

> *It is strongly recommended that any new devices for which you have added support be included in a test profile first before deployment. Because of the nature of ODF integration, effective device support will likely require deploying a test profile, testing, correcting, and then re-uploading the corrected ODF files until successful.*

Advanced Mobile Broadband Options

Available for: Windows clients with Mobile Broadband enabled.

These advanced Mobile Broadband options provide additional controls for Mobile Broadband users. When your advanced mobile broadband options are selected, click **Save**.

Network Selection: select a network selection type from the drop-down list.

- *Automatic*: the Mobile Broadband device will choose a network.
- *Manual*: the user is prompted to choose a network.

Allow the user to disable the use of the client for managing Mobile Broadband connections: if selected, the user can disable Open Mobile for managing Mobile Broadband connections.

Enable SMS: Select **Enable SMS** to enable receipt (and for Windows 1.4.1 and later clients, sending as well) of SMS messages in the Open Mobile client over Mobile Broadband connections. The user must have an SMS-capable Mobile Broadband device to receive or send SMS messages.

Allow user to modify Mobile Broadband connection profile settings…: If selected, the user will be able to modify Mobile Broadband connection settings, including access point name, network name, dial string, DNS address, username, and password.

Allow Mobile Broadband to connect simultaneously with Wi-Fi or Ethernet: *(Windows 2.1.0 and later)* if selected, the user will be able to connect to multiple networks at a time or MNAAT (for example, users will not be disconnected from a

Mobile Broadband network when they dock their laptop and connect by Ethernet). If not selected, the user will only be able to connect to one network at a time (ONAAT).

Allow the user to select frequency bands: If enabled, the user will be able to select Mobile Broadband frequency bands used by Mobile Broadband devices. Only the bands supported by the device will be shown by Open Mobile.

Allow the user to select radio access technologies: If enabled, the user will be able to select the radio access technology from a range of choices (2G, 3G, and 4G). If disabled, then Open Mobile will select the network bearer.

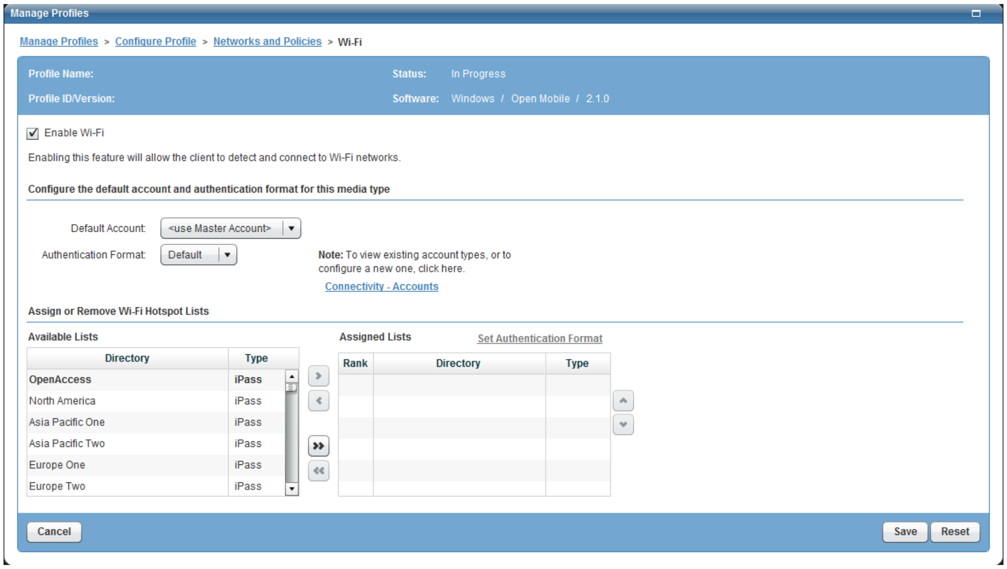
Technical error code messaging for connection failures: If enabled, upon failure of a Mobile Broadband connection, any error messages displayed to the user will include technical error codes. These error codes are not user-friendly, and it is recommended that you disable this feature for any profiles published to production.

- These messages are customizable. Custom messages must be contained in an appropriately formatted XML file.
- You can download and review a sample technical error code message file by clicking **Sample Error Code File.**
- To upload your own error code file, click **Browse**, select your custom error code file, and then click **Upload**.

Wi-Fi

Available for all clients.

Open Mobile can detect and connect to Wi-Fi networks.



Manage Profiles

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

Profile Name:

Profile ID/Version:

Status: In Progress

Software: Windows / Open Mobile / 2.1.0

☑ Enable Wi-Fi

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

Configure the default account and authentication format for this media type

Default Account: <use Master Account>

Authentication Format: Default

Note: To view existing account types, or to configure a new one, click here.

Connectivity - Accounts

Assign or Remove Wi-Fi Hotspot Lists

Available Lists

Directory	Type
OpenAccess	iPass
North America	iPass
Asia Pacific One	iPass
Asia Pacific Two	iPass
Europe One	iPass
Europe Two	iPass

Assigned Lists

Set Authentication Format

Rank	Directory	Type

Authentication Format Override

You can specify the authentication format used by an account, with a format used just for Wi-Fi connections. You can also specify the authentication format for connections made using specific Wi-Fi directories. These authentication formats will override the account's default authentication format. Authentication tokens used in overrides must already be defined in the account.

> *This is an advanced feature and will not be required for most Open Mobile profiles. For more information on authentication format, see page 17.*

To specify an authentication format override for Wi-Fi connections,

1. In **Default Account**, select the account used for Wi-Fi connections.
2. In **Authentication Format Override**, specify the new format.

To specify an authentication format override for one or more Wi-Fi directories,

1. Under **Assign or Remove Wi-Fi Hotspot Lists**, using the arrow keys, assign one or more directories to the profile.
2. In the **Assigned Lists** column, click **Set Authentication Format**.
3. For each directory in the list for which you wish to use a new authentication format:
   - Under **Account**, select the account used.
   - Under **Auth Format Override**, enter the new authentication format used.
   - Under **Enable USID**, select whether to use Unique Session ID for connections.
   - (For Android 2.2 and later clients) Under **Forced Auto-Connect**, select whether to force users to automatically connect to access points in the directory when within range.
4. Click **Save**.

Forced Auto-Connect

Available for: Android 2.2 and later clients.

If enabled for a directory that is included in an Android 2.2 client, users will be forced to connect automatically to Wi-Fi hotspots in the directory when within range. This can be an effective way to enforce user connections to Wi-Fi, rather than the more costly Mobile Broadband connections.

Wi-Fi Network Directories

By default, your users will be able to connect to iPass Wi-Fi networks. In addition, you can choose to enable one or more previously uploaded Wi-Fi networks to which your users can connect.

To add one or more Wi-Fi networks to Open Mobile, using the arrow controls, move the directories from the **Available Directories** column to the **Assigned Directories** column**.** Use the up and down arrows to change the sort order of the assigned directories.

OpenAccess: OpenAccess Wi-Fi access points are free connections included in the iPass network. If enabled, users can connect to OpenAccess networks at no additional charge. To enable OpenAccess in Open Mobile, add the OpenAccess directory to the profile.

> ***Opt-In Services:*** *Additional directories, such as Swisscom, are available as opt-in services. If a user attempts to connect to a service to which your enterprise has not opted in, the authentication will fail.*

Advanced Wi-Fi Options

Enable Wi-Fi in order to be able to configure advanced Wi-Fi settings, which provide additional connectivity options.

Allow the user to disable the use of the client for managing Wi-Fi connections: if selected, the user will can disable Open Mobile for managing Wi-Fi connections.

Allow Wi-Fi to connect simultaneously with Mobile Broadband or Ethernet: *(Windows 2.1.0 and later)* if selected, the user will be able to connect to multiple networks at a time or MNAAT (for example, a user will not be disconnected from a Wi-Fi network when they dock their laptop and connect by Ethernet). If not selected, the user will only be able to connect to one network at a time (ONAAT).

Personal Networks: *(Windows, Mac OS X only)* If enabled, end users will be able to configure and save personal network settings in Open Mobile for use on their machine.

Enable 802.1x Network Configuration: *(Windows only)* If enabled, Open Mobile will be able to scan for, define, and test 802.1x networks (such as EAP-TLS). Select one of the following options:

- *View and edit network configurations:* Users will be able to view and change 802.1x settings.
- *View, edit, and export network configurations:* Users will be able to view and change 802.1x settings. In addition, users will be able to export their network settings to a file, which you can include in profiles for use by other users.

Enable Ethernet

Available for: Windows clients.

Select **Enable Ethernet** to enable Open Mobile to connect to Ethernet access points.

Authentication Format Override

Available for: Windows 1.4.1 and later clients.

You can specify the authentication format used by an account, with a format used just for Ethernet connections. These authentication formats will override the account's default authentication format. Authentication tokens used in overrides must already be defined in the account.

> *For more information on authentication format, see page 17.*

To specify an authentication format override for Ethernet connections,

1. In **Default Account** drop-down list, select the account used for Ethernet connections.
2. In the **Authentication Format** drop-down list, select whether to use the standard authentication format (default), or to override it with a new one. If override is selected, enter the new format.

Enable Dial

Available for: Windows clients.

Select **Enable Dial** to allow Open Mobile to connect to dial-up access points.

> *The iPass network of dialup access points also includes ISDN networks. Proper hardware for connection to ISDN networks is required.*

Authentication Format Override

Available for: Windows 1.4.1 and later clients.

You can specify the authentication format used by an account, with a format used just for Dial connections. These authentication formats will override the account's default authentication format. Authentication tokens used in overrides must already be defined in the account.

> *For more information on authentication format, see page 17.*

To specify an authentication format override for Dial connections,

1. In **Default Account** drop-down list, select the account used for Dial connections.
2. In the **Authentication Format** drop-down list, select whether to use the standard authentication format (default), or to override it with a new one. If override is selected, enter the new format.
3. Under **Include Unique Session ID**, select whether to use Unique Session ID for connections.

Enable DSL

Available for: Windows 1.4.1 and later clients.

Select **Enable DSL** to enable Open Mobile to connect to DSL access points.

Authentication Format Override

Available for: Windows 1.4.1 and later clients.

You can specify the authentication format used by an account, with a format used just for DSL connections. These authentication formats will override the account's default authentication format. Authentication tokens used in overrides must already be defined in the account.

> *This is an advanced feature and will not be required for most Open Mobile profiles. For more information on authentication format, see page 17.*

To specify an authentication format override for DSL connections,

1. In **Default Account** drop-down list, select the account used for DSL connections.
2. In the **Authentication Format** drop-down list, select whether to use the standard authentication format (default), or to override it with a new one. If override is selected, enter the new format.

Network Policies

Network policies enable you to exercise control over user connectivity.

Connection Policy

Available for: Windows clients, Express clients.

Network Policy

Network Ranking settings control the order in which networks are ranked and displayed in the Open Mobile Available Networks list, with highest-ranked networks shown at the top of the list.

Ranking is determined by a complex algorithm that factors network type, connection history, signal strength, and provisioner type to determine the display order. The most influential factors in your particular network ranking depend on the ranking option you select from the following:

- **Favor previously connected networks (for consistency):** Ranks any networks to which the user has previously connected.
- **Favor known networks (for security):** Ranks networks about which Open Mobile has information. In order of priority, these are personal networks, networks that are listed in a directory, and any networks to which the user has previously connected.

- **Favor Wi-Fi (to reduce costs):** Ranks Wi-Fi networks above others, but connection history, directory, and signal strength are also considered, and due to these factors, Wi-Fi may still not be the top network.
- **Favor signal strength (for best performance):** Ranks the wireless networks (that is, Wi-Fi or Mobile Broadband) with the strongest current signals.
- **Favor Mobile Broadband:** Ranks Mobile Broadband networks above others, but connection history, directory, and signal strength are also considered, and due to these factors, Mobile Broadband may still not be the top network.
- **Always show Mobile Broadband at the top of Available Networks list:** Mobile Broadband networks will always be shown at the top of the list, independent of any other considerations.
- **Disable peer-to-peer connections:** If selected, peer-to-peer connections will be disabled when connected by Open Mobile.

> *If enabled, then Prefer and Prohibit rules will supersede Network Policy settings. See page 29 for more information.*

Auto-Connect

Select any network types you wish to enable for Auto-Connect (corporate and Wi-Fi networks, personal Wi-Fi, and Mobile Broadband home and roaming networks). Users will be automatically connected to these networks, when possible. (Credentials must be saved locally by users in order for them to Auto-Connect.)

Auto-Login

Available for: iOS clients.

Select **Enable Auto-Login for corporate and Wi-Fi networks** to enable automatic login to hotspots already known to iOS. (The hotspot must have been previously logged into by the user in order for iOS to recognize it.)

Mobile Broadband Policy

Available for: Windows 1.4.1 and later clients.

Mobile Broadband policy settings enable you to set usage thresholds for warning messages to be displayed to Mobile Broadband users, as well as usage limits on a monthly basis. You can set separate policies for roaming usage, non-roaming usage, and personal hotspot usage, as well as customize messages displayed to users when thresholds are exceeded.

> *Mobile Broadband settings are not applicable to connections that were initially established using a third-party connection manager.*

In the setting descriptions below:

- N represents an entry box where an amount can be specified.
- Where shown*, total megabytes* represents the total of incoming and outgoing traffic.
- A default message is provided for all warnings and alerts; click **Customize Message** to enter your own message instead. (This message will be displayed exactly as entered and will not be localized).

Roaming Usage Tab

Roaming usage policy settings control the behavior of Open Mobile when a Mobile Broadband user is roaming outside a regular service area.

Mobile Broadband Roaming Policy

- **Enable Roaming:** if enabled, the user will be alerted whenever roaming.
- **Display Roaming Alert When User Attempts to Connect Outside Their Home Network:** If enabled, a roaming message will be displayed to roaming users.
- **Limit Roaming Usage per Month to N Megabytes Transferred:** if enabled, users will be limited to this number of megabytes transferred in a monthly period.
- **High-bandwidth Warning:** Select to enable, and then define the number of megabytes transferred in a period of minutes that will trigger the high-bandwidth warning.

Additional Roaming Warning Messages

- **Initial Warning After N Megabytes Transferred:** enter the number of megabytes of roaming usage that will trigger the first user warning.
- **Incremental Warning After Each N Megabytes Transferred:** the user will be warned again each time the number of megabytes specified here are used.
- **Show a warning message when trying to connect after the monthly roaming limit has been reached:** if enabled, the user will be warned when trying to connect if the usage threshold has been exceeded for the month.

Billing Period

- **Begin Roaming Period:** select a day of the month from which roaming usage will be counted.

Usage Policy Tab

Usage policy settings control the behavior of Open Mobile when a Mobile Broadband user is in the regular service area for the Mobile Broadband provider.

Mobile Broadband Usage Policy

- **Limit usage per month to N megabytes transferred:** if enabled, users will be limited to the specified number of megabytes transferred in a monthly period.
- **High-bandwidth Warning:** Select to enable, and then define the number of megabytes transferred in a period of minutes that will trigger the high-bandwidth warning.

Additional Warning Messages

- **Initial warning after N megabytes transferred:** enter the number of megabytes of roaming usage that will trigger the first user warning.
- **Incremental warning after each N megabytes transferred:** the user will be warned again each time the number of megabytes specified here is used.
- **Show a warning message when trying to connect after the monthly data limit has been reached:** if enabled, the user will be warned when trying to connect if the usage threshold has been exceeded for the month.

Billing Period

- **Begin Roaming Period:** select a day of the month from which roaming usage will be counted.

Personal Hotspot Policy

Personal hotspot policy settings control the behavior of Open Mobile when it cannot be determined whether the user is in the provider's service area.

> *Ensure that any SSIDs entered for your personal hotspot policy are unique. Open Mobile will impose the policy on any other networks with the same SSID.*
>
> *For example, a personal hotspot has an SSID of 'LocalNetwork' and an Open Mobile policy is set up on that basis. Later, an Open Mobile user visits a café that provides Wi-Fi and also has an SSID of 'LocalNetwork'. Open Mobile would impose the personal hotspot policy on usage from the café.*

Personal Hotspot Policy

- **SSIDs of MiFi Devices:** If profile users utilize of any MiFi devices (mobile Wi-Fi hotspots), enter the SSIDs of these devices here, one per line.
- **Limit Roaming Usage per Month to N Megabytes Transferred:** if enabled, users will be limited to this number of megabytes transferred in a monthly period.
- **High-bandwidth Warning:** Select to enable, and then define the number of megabytes transferred in a period of minutes that will trigger the high-bandwidth warning.

Additional Warning Messages

- **Initial Warning After N Megabytes Transferred:** enter the number of megabytes of roaming usage that will trigger the first user warning.
- **Incremental Warning After Each N Megabytes Transferred:** the user will be warned again each time the number of megabytes specified here are used.
- **When Trying to Connect:** if enabled, the user will be warned when trying to connect if the usage threshold has been exceeded for the month.

Billing Period

- **Begin Roaming Period:** select a day of the month from which roaming usage will be counted.

Preferred and Prohibited Networks

Available for: Windows clients (1.4.1 and later) and Android clients (2.0.0 and later).

Special rules to prefer or prohibit networks can be set for individual networks in your Wi-Fi and Mobile Broadband directories, as well as for different security types, controlling how Open Mobile will display these networks to users. Prefer/prohibit rules supersede any Network Policy settings.

- **Preferred Networks:** A network (name or MAC address) defined as preferred will always be used for connections (if possible), and shown at the top of the Available Networks list. (Step 4 in the following process)
- **Prohibited Networks:** A network (name or MAC address) defined as prohibited will never be used for connections. A prohibited network can be shown as disabled or even hidden entirely from the user. (Step 4 in the following process)
- **Rename:** A rule can also be used to rename a network in the list of Available Networks, choosing a display name that is clearer and more convenient for your users. For example, if your corporate network has a non-descript SSID (for example, corp-hq-east), Open Mobile could display the SSID as something friendlier like *My Corporate Network*. (Step 5 in the following process)
    - **Annotation:** In addition to display name, an *annotation* can be used to explain details about the network, which would be displayed to users in Open Mobile when the network is detected. (Step 5 in the following process)
- **Disabled Security Types:** You can set a policy to disable a single security type, such as WPA-PSK-AES, from

use in Open Mobile. (Step 3 in the following process)

Using this page, you can set a policy type, a policy rule, and a display name or annotation.

To set a special network rule, or to set a display name or annotation,

1. Click **Configure**.
2. Click **Define New Policy**.
3. **Under Policy Type,** do one of the following:
    - Select **Network Name**, and enter the name of the network for which you will define a policy. (For purposes of a Prefer/Prohibit rule, SSIDs are case-insensitive). Proceed to Step 4.
    - Select **Network MAC Address**, and enter the network MAC address for which you will define a policy. Proceed to Step 4.
    - Select **Security**, and then select a type of wireless network to disable in Open Mobile, based on security type, from the drop-down list. Then, click **Save** to save your policy.

      > *If **Unsecured networks** is selected, many iPass Wi-Fi networks (that use credential authentication but do not have WEP or WPA security) will no longer be accessible. This policy is only recommended for users that connect exclusively with Mobile Broadband outside of the corporate network.*
4. Under **Policy Rule**, pick one of the following one of the following:
    - *Prefer Network:* Select this to prefer connections to this network (name or MAC address) and show it at the top of the Available Networks list.
        - To make the preferred network exclusive, select Disable connections to all other networks when this network is available.
    - *Prohibit Connections:* Select this to prevent access to this network (name or MAC address), select **Prohibit connections to this network.** Then select one of the following:
        - **Gray out network in Available Networks list**: the network will be shown in Open Mobile, but disabled.
        - **Do not display this network:** hides the network from Open Mobile users.
    - *Other:* Choose **Other** to disable Auto-Connect for a particular network (name or MAC address). (This setting has no effect on preferred or prohibited networks.)
        - To force users to connect manually to the network, select **Disable Auto-Connect to this network.**
5. Under Display Name and Annotation:
    - In **Display Name**, enter the name you would like displayed for this network in the Available Networks list.
    - In **Annotation**, enter the text of the network annotation.
6. Click **Save**.

Time-Based Session Limits

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

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

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

Advanced Configuration

Internet Connection Test

Available for: Windows clients, Express clients.

Open Mobile performs a network test to determine whether the user has an Internet connection. An HTTP request is sent to iPass test server URLs. However, if restrictions on your corporate network architecture prevent reaching the default URLs, you can substitute your own URL instead. To set a custom URL, select **Custom**, then specify the URL and the response substring (which is displayed in the URL).

Hotspot Finder

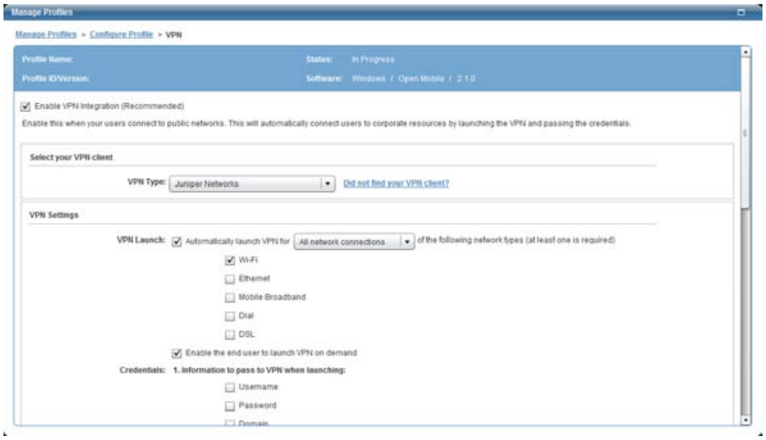
Available for: Android clients, iOS clients.

iPass provides a Wi-Fi hotspot finder at http://www.ipass.com/mobilehotspot. However, you can customize this URL if you would prefer to use a different hotspot finder. To set a custom hotspot finder URL, select **Custom**, then specify the URL.

VPN Integration

Available for: Windows clients, Express clients, Mac OS X clients.

An integrated VPN is automatically launched with Open Mobile, which can pass the VPN login credentials and ensure a secure connection to corporate resources. Enabling VPN integration is recommended for all Open Mobile for Windows clients.



Manage Profiles

Manage Profiles » Configure Profile » VPN

Profile Name: Status: In Progress

Profile ID/Version: Software: Windows / Open Mobile / 2.1.0

☑ Enable VPN Integration (Recommended)

Enable this when your users connect to public networks. This will automatically connect users to corporate resources by launching the VPN and passing the credentials.

Select your VPN client

VPN Type: Juniper Networks ▾ Did not find your VPN client?

VPN Settings

VPN Launch: ☑ Automatically launch VPN for All network connections ▾ of the following network types (at least one is required)

☑ Wi-Fi
☐ Ethernet
☐ Mobile Broadband
☐ Dial
☐ DSL

☑ Enable the end user to launch VPN on demand

Credentials: 1. Information to pass to VPN when launching:

☐ Username
☐ Password
☐ Domain

> *You must define at least one account for authentication before configuring VPN integration.*

Because a VPN is not required when on a corporate network, you have the option of enabling or disabling the VPN control switch in the Open Mobile UI. You can choose to enable the control with or without user confirmation, or to disable the control completely.

Supported VPN Products (Windows and Mac OS X only)

Open Mobile supports the following VPN products:

Windows Clients

- Check Point
- Cisco AnyConnect SSL
- Cisco IPSec
- Juniper Networks
- NCP
- Nortel

In addition, using Custom VPN Integration, you can integrate a wide variety of VPN solutions into Open Mobile. Custom VPN integration is described on page 35.

Mac Clients

- Cisco AnyConnect
- Juniper SSL

> *Custom VPN integration is not available for Mac OS X clients.*

VPN Configuration Settings

The VPN configuration settings are shown here. Depending on your VPN solution, some of these settings may be disabled.

Option	Description
Select your VPN client	Select your VPN from the drop-down list. (Your selection of VPN may restrict some of the configuration settings that follow.) *If you select **Check Point**, you must define at least one method of Corporate Network Detection (CND), and at least one of your CND rules should be configured to detect the network that is available through your VPN tunnel. (For more information on Corporate Network Detection, see page 38.)*
VPN Launch for [Network Connection Types] of the following network types	Select a network connection type that will trigger VPN launch, as well as which network types for which the VPN will be automatically launched. Network connection types include: ■ *All network connections*: The VPN will be launched for all Open Mobile connections (those initiated in Open Mobile, as well as those inherited from other connection managers). ■ *Initiated connections*: The VPN will only be launched on connections initiated in Open Mobile. (That is, connections inherited from another connection manager will not trigger a VPN launch.) *Network Types* include Wi-Fi, Ethernet, Mobile Broadband, Dial, and DSL. The VPN will automatically be launched for the selected types. Any number of these may be selected, but at

	least one type is required.
Enable the end user to launch the VPN on demand	*(VPN On-Demand)* If selected, the user will be able to launch the VPN using the **VPN** button in the Open Mobile client UI. If not selected, the VPN is launched automatically on the specified connection types.
VPN Account and Authentication	VPN authentication can be performed either by certificate or account credentials. - **Authenticate using certificate (Cisco AnyConnect and Nortel only):** If selected, VPN authentication will be performed by certificate. - Enter a default profile name, or leave blank for the VPN client to auto-select a profile. - Select **Enable Gateway/Profile** selection to enable the user to select a gateway from the profiles defined in the VPN client. - **Authenticate using account:** If selected, VPN authentication will be performed by account credentials passed from the Open Mobile account you define. Then, select or enter the following: - **Information to pass to VPN when launching:** Select one or more credential types (username, password, domain, and token) to pass to the VPN. - **Select account…:** Select the account from which the credentials are to be drawn. - A green check mark indicates that the credential type has been configured for that account. - A red X indicates that the credential type has not been configured for that account definition. You will not be able to save the integration if a red X is present. Select (or configure) another account to use.
Default Gateway/Profile	Optionally, enter the name of the default VPN gateway or profile, and whether gateway/profile selection is enabled for the user. - If gateway/profile selection is not enabled, you will need to specify the name of the default profile. - If no default is specified, or the default does not match any existing entries in the VPN client, Open Mobile will select the first profile available in the VPN client. (Note that the user can override the default in Open Mobile under **Options | VPN**.) Alternately, to specify the VPN gateway or profile for an SSL VPN such as Juniper, you can upload a file that includes VPN gateway information. A VPN gateway file is *required* if you use credential values other than username and password, such as Username/PIN+Token Code. An example of a VPN gateway file is available for download on the **VPN Integration** page. If you create your own file, save the file as an .ini file before uploading it. For more information, you consult the tech note *Open Mobile VPN Integration Gateway File.*

VPN GUI Visibility	**Hide VPN GUI When Launching:** If selected, the VPN interface will be hidden from the end user. (In order for this feature to function, you must configure VPN Auto-Connect.) VPN GUI visibility does not affect the VPN system tray icon, just the visibility of the main VPN UI.
VPN Connectivity	- **(VPN Timeout)** Choose the number of seconds before a VPN connection is timed out (before the attempt is considered failed and automatically canceled). - **(Auto-Disconnect)** Whether the VPN will be disconnected if the user switches networks. - **(Auto-Teardown)** If selected, Open Mobile will teardown the Internet connection when the VPN is disconnected for any reason. - If Auto-Teardown is enabled, choose a value for the number of times Open Mobile should attempt to reconnect once disconnected. If zero, no reconnection attempt will be made.

To enable VPN integration,

1. Select **Enable VPN Integration** (Recommended).
2. Under **VPN Type**, select your VPN client from the drop-down list.
3. Under **VPN Settings**, select the behavior of your VPN client, based on the offered prompts. Depending on the VPN type, you may be prompted to enter specific connection or network types for which to automatically launch the VPN, account and authentication information, and the settings for the VPN gateways.
4. Under **VPN Connectivity**:
   - Indicate the number of seconds allowed for a VPN connection.
   - Indicate the number of reconnection attempts the VPN will take when accidentally disconnected.
   - Indicate whether Open Mobile should disconnect from the Internet if the VPN is disconnected, and if yes, enter the number of times that Open Mobile should attempt to automatically reconnect the VPN before disconnecting from the Internet.
5. For Windows 2.x clients, under **When on Corporate Network**, choose whether to enable the **VPN** control in the Open Mobile interface.
   - **Enable VPN Control but require no user confirmation upon VPN connection attempt:** If connected to a corporate network, the user can launch the VPN with no confirmation required.
   - **Enable VPN Control but require user confirmation upon VPN connection attempt:** If connected to a corporate network and the VPN is launched, the user will be prompted to confirm the VPN connection attempt.
   - **Disable VPN Control:** (not recommended) Disables the VPN Control completely. Users will not be able to launch the VPN if a corporate network is detected. (Note that a false-positive CND test will deny the user VPN access, so make sure that your CND test criteria will have no chance to return any erroneous or spurious results.)
6. Click **Save.**

Custom VPN Integration

Open Mobile supports the integration of many industry-standard VPN solutions. However, it is possible to integrate Open Mobile with a much wider variety of VPNs, using the Custom VPN Integration feature.

Requirements: Configuring custom VPN integration requires the following:

- You must define at least one method of Corporate Network Detection (CND), as well as enabling VPN polling, so Open Mobile can provide proper monitoring, status messages, auto-teardown, and other related features.
- In addition, at least one of your CND rules should be configured to detect the network that is available through your VPN tunnel. (For more information on Corporate Network Detection, see page 38.)
- When configuring the VPN integration, you will need to enter a connect command line, which can use either the literal path or %PROGRAMFILES% variable. Examples of a proper command line include:
  - For 32-bit path: C:\Program Files\YourVPN\example.exe -profile USCorpGWA -user <UserName> -password <UserPassword> -domain <UserDomain>
  - For 32-bit path and x86 path for 64-bit: %PROGRAMFILES%\YourVPN\example.exe -profile USCorpGWA -user <UserName> -password <UserPassword> -domain <UserDomain>

To integrate a custom VPN,

1. Select **Enable VPN Integration (Recommended)**.
2. Under **Select your VPN client**, select *Custom VPN*.
3. In Custom **VPN Name**, enter the name of your custom VPN client.
4. In **Connect Command**, enter the VPN command-line parameters needed to connect with the VPN client.

   > *You have to include <UserName>, <UserPassword>, or <UserDomain> in the command line in order to select an account definition under **VPN Settings**.*

5. In **Disconnect Command**, enter any command-line parameters needed to disconnect the VPN client.
6. Under **VPN Launch,** pick one or more network types for which to automatically launch the VPN, and whether the user will be able to launch the VPN on demand.
7. Specify any additional settings as prompted.
8. Click **Save**.

   > *If a custom VPN is configured to pass username and password, the password will be shown in clear text in the Task Manager.*

Custom VPN integration is not supported by iPass. Customers are responsible for all testing of custom VPN integration.

Client Look and Feel

Client Look and Feel settings include applying your own brand to the Open Mobile client, as well as determining the visual display settings for features such as the Quick Launch toolbar, SMS, and RSS displays.

Branding

You can style your version of the Open Mobile client by applying brands you have already created. You should already have created one or more brands before applying them to a client profile. See page 62 for more information.

Only a single brand may be assigned to a profile at one time.

> *Brands are supported by clients built for all versions of Open Mobile for Windows, for versions 1.2 and later of Open Mobile for Mac OS X, for versions 1.3 and later of Open Mobile for Android, and for versions 2.1.0 and later of Open Mobile for iOS.*

Windows 1.x Clients

To apply a brand and styling to a Windows 1.x client,

1. On the **Configure Profile** page, under **Brands and Features**, click **Configure**.
2. Click **Select a Brand.** Then, under **Client Branding,** select a brand from the drop-down list of previously created brands.
3. Click Customize **Visual Style.** Then, select the visual style for the client Quick Launch, RSS, Search, and SMS settings.
4. Click **Save**.

Windows 2.x or Express Clients

For Windows 2.x (or Express) clients, you can apply an existing brand, or apply a brand based on the settings in an existing Windows 1.x profile.

To apply a brand to a Windows 2.x or Express client,

1. On the **Configure Profile** page, under **Brands and Features**, click **Configure**.
2. Under **Assign a brand to this profile**, select one of the following:
   - **Choose a published brand for <platform>:** Select to apply a brand you have already created.
   - **Choose a brand based on an existing profile:** Select to apply an existing brand, based on the settings in an existing Windows 1.x profile.
3. Select the brand or profile from the drop-down list.
4. Click **Save**.

Mac Clients

To apply a brand and styling to a Mac client,

1. On the **Configure Profile** page, under **Brands and Features**, click **Configure**.
2. Click **Select a Brand.** Then, under **Client Branding,** select a brand from the drop-down list of previously created brands.
3. Click **Customize Visual Style.** Then, select the visual style for the client Quick Launch, RSS, Search, and SMS settings.
4. Click **Save**.

Android 2.x Clients

To apply a brand and styling to an Android 2.x client,

1. On the **Configure Profile** page, under **Brands and Features**, click **Configure**.

2. Click **Select a Brand**. Then, under **Client Branding**, select a brand from the drop-down list of previously created brands.
3. Click **Save**.

iOS Clients 2.1.0 and later

To apply a brand and styling to an iOS client,

1. On the **Configure Profile** page, under **Brands and Features**, click **Configure**.
2. Click **Select a Brand**. Then, under **Client Branding**, select a brand from the drop-down list of previously created brands.
3. Click **Save**.

Customize Visual Style (Mac)

Visual style settings for Mac include informational features such as RSS and Search.

RSS Settings

You can enable an RSS feed in Open Mobile, specifying a single URL for news and headlines to be streamed to users.

Search

You can define an Internet search engine for use with Open Mobile. If enabled, users will be able to perform Internet searches directly in Open Mobile. To enable search, select it in the Open Mobile Portal. Then, upload a search file, which is an HTML file formatted as follows:

- The file must be self-contained, requiring no additional resources uploaded, but may reference external or internet resources. It should not refer to itself, as the upload process may change the filename.
- Maximum size of the search window in Open Mobile is 319 pixels wide by 125 pixels high.
- Specify html { overflow: auto } in the CSS line to prevent the vertical scrollbar from showing.
- Avoid the use of any scripts, if possible.

An example search file is shown here, enabling search on a popular search engine.

```
   <?xml version="1.0" encoding="UTF-8"?>

   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

   <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

   <head>

     <title>MySearchPage</title>

       <meta name="created" content="Wed, 28 Apr 2010 22:28:23 GMT" />

     <meta name="description" content="" />

     <meta name="keywords" content="" />

     <style type="text/css">

     html {

           overflow: auto;

     }

     <!--

   .body {
    height: 125px;
    width: 319px;
    background-color: #EFEFEF;
    color: #000000;
    max-width: 319px;
    max-height: 125px;
   }
   -->
   </style>
   </head>
   <body bgcolor="#FFFFFF" text="#000000" link="#0000FF" vlink="#800080" alink="#FF0000" leftmargin="0px" topmargin="0px">
   <div class="body">
   <form action="http://www.google.com/cse" id="cse-search-box" target="_blank">
     <div>
       <input type="hidden" name="cx" value="013516449520835724295:3fa3ka1eqy4" />
       <input type="hidden" name="ie" value="UTF-8" />
       <input type="text" name="q" size="31" />
       <input type="submit" name="sa" value="Search" />
     </div>
   </form>
   <script type="text/javascript" src="http://www.google.com/cse/brand?form=cse-search-box&amp;lang=en"></script>
   </div>
   </body>
   </html>
```

Integration

Integration settings control the integration of Open Mobile with a variety of tools and applications.

Corporate Network Detection (CND)

Available for: Windows clients.

Open Mobile can be configured to detect when a user is connected to a corporate or campus network at a given venue. Corporate network detection (CND) is important if you want Open Mobile to apply security or other corporate policies. For example, there might be different policies applied when a user is connected to the corporate network instead of just being connected to the Internet.

You can enable any number of different test methods for corporate networks. Multiple tests can improve the chances of making a successful detection of the corporate network. The complexity and number of tests used will depend upon the size and uniqueness of the corporate network being detected.

In some cases, a combination of tests is required to accurately determine whether Open Mobile detects a corporate network. For example, in the course of connecting, a user could receive a DHCP IP address within your normal DHCP IP range. However, because public addressing is used, the same user could receive the same DHCP IP address on a different network. By adding a second corporate network detection method, such as by DNS Server address, you can ensure that corporate networks are more accurately detected.

CND tests come in two types, local and remote.

- *Local:* In a local test, some attribute of the local machine is used as a test criterion, such as the presence of a particular Registry entry.
- *Remote*: For a remote test, Open Mobile must check a remote attribute through the network, such as whether a URL is currently reachable.

Test Scores

Each test is assigned a score from 1 to 100, which represents the weight given to the test to determine corporate network connectivity. A positive result for the test means the score for that method will be included in the determination. (There are no partial scores.) For example, if the Assigned IP Address method is used with a score of 50, and the user matches the specified IP address, then the score of the Assigned IP Address will be 50.

In order for a location or venue to be identified as a corporate network, the scores of all tests with positive results must be greater than the Minimum Qualifying Score for the location venue. For example, if a venue has a Minimum Qualifying score of 80, then the Assigned IP Address method in the example above (with a score of 50) would not qualify even if it were a positive result, and would not be used to determine whether the venue was part of a corporate network.

CND and Performance Impact

Because of processing time, network traffic and other factors, CND tests can affect on the performance of the Open Mobile client. Configure as few methods as possible to get optimal results. When possible, use local CND tests, as opposed to remote tests. Local tests will not affect network traffic.

Note that configuring too many corporate network detection methods can significantly affect the performance of the Open Mobile client. You should use as few methods as possible to get the optimal performance results for your users.

Corporate Network Detection Methods

The following CND tests are available to configure:

Test	Type	Test is Positive If…	Notes
Domain	Local	Machine belongs to the specified domain.	The machine is checked to see if it is attached to the domain and connected to the domain network. For example, If the machine is in the corp.example.com domain, and if the machine is connected to the corporate network then CND will detect the corporate network. *Note: Windows does not always return the correct value for the connected domain. It is recommended that you use another CND test in conjunction with this one.*
Assigned IP Address	Local	Result matches a single IP address	Use of IP addresses can be effective if registered IP addresses are in use, and might be the only detection method needed. If public addressing is used, then this detection method may still be helpful to use along with some other methods, but it will likely not be usable on its own.
Registry Entry	Local	Registry entry found	(Windows machines only.) Some VPN products change a Windows registry value when the VPN tunnel is established. Some firewall products have a location detection capability that may also set a registry value. In these instances, checking

Test	Type	Test is Positive If…	Notes
			a specific registry value can be a valuable method in network detection.
Service Set Identifier (SSID)	Local	Specified SSID is detected	A wireless network station name (SSID) can be configured as a detection method. This method is optimal for determining if a user is connected by Wi-Fi to the corporate network, and can be conclusive for Wi-Fi if the SSID in use is a unique name.
Virtual Adapter	Local	Specified virtual adapter is enabled	Some VPN products utilize a virtual adapter for VPN connectivity. When the VPN has established a connection, the virtual adapter is enabled. When the VPN connection is not established, the virtual adapter becomes disabled. To determine the virtual adapter name and URI, when the VPN is connected, at the command line, run ipconfig/all and check for the VPN client adapter description.
DHCP Server Address	Remote	Result matches a DHCP server IP address	A DHCP server address can be configured as a factor in network detection, especially in circumstances where the DHCP server addresses are not part of a commonly used public addressing (10.1.1.1, 192.168.1.1, etc.). In large networks where there are dozens (or hundreds) of DCHP servers, this method may require a significant configuration effort.
DNS Server Address	Remote	Result matches DNS server IP address	A DNS server address can be configured as a factor in network detection, especially in circumstances where the DNS server addresses are not part of a commonly used public addressing (10.1.1.1, 192.168.1.1, etc.). This can be a very effective method when a company has a master set of DNS servers with unique IP addresses.
Gateway Address	Remote	Result matches gateway address	Best used in very flat network architectures where there are few default gateway addresses.
Network Device Reachable	Remote	Specified network device is reachable by PING	In environments where no other tests can be used and where SNMP traffic is not filtered, this can be an effective method in determining corporate network detection. If using this method, it is advisable to configure more than one IP address or device, to handle cases where the primary device checked is not available. Because this method generates network traffic and will require a few seconds to make a determination, avoid using this method unless no other methods will work for that network.
Network Printer Reachable	Remote	Specified network printer is reachable by PING	Because this method generates network traffic and will require a few seconds to make a determination, avoid using this method unless no other methods will work for that network.
Network Share Reachable	Remote	Specified network share is reachable by PING	Because this method generates network traffic and will require a few seconds to make a determination, avoid using this method unless no other methods will work for that network.
URL Reachable	Remote	Specified URL is reachable by PING	Because this method generates network traffic and will require a few seconds to make a determination, avoid using this method unless no other methods will work for that network.

To add a new corporate network for detection,

1. Click **Define New Networks**.
2. In **Corporate Network Name**, enter the name of the corporate network. (This will be displayed in the client, and may not be changed once the rule is saved.)
3. In **Network Adapter Name**, select a name for the network adapter used to connect to the corporate network from the drop-down list. (If *Any* is chosen, the user will be able to connect to the network using any connectivity type.)
4. In **Minimum Qualifying Score**, set a minimum qualifying score for the test used to determine whether this network is a corporate network.
5. Under **Select Network Resources**, select a network resource from the drop-down list that will be used as a method of network detection. Then, enter the requested network attributes, as needed.

6. In **Score**, using the slider, assign a score to the network resource from 0 to 100.
7. If you wish to add more network resources, click **+**, then repeat steps 5-6.
8. Click **Save**.

Connect Before Logon

Available for: Windows 2.1 and later clients.

If Connect Before Logon is enabled, users will be able to establish a network connection (and subsequent VPN connection) before logging on to Windows. Connect Before Logon lets you control the use of login scripts, password caching, mapping network drives to local drives, and other operations that require a network connection.

To enable Connect Before Logon,

1. Select **Enable Connect Before Logon using the integrate Microsoft Pre-Logon Access Provider (PLAP)**.
2. In **Allow the client to wait this many seconds before connection**, enter the number of seconds the client should wait before establishing a network connection.
3. If you are creating a profile for Windows 2.2 or later clients, you can specify an account to use for connecting to the Internet (and possibly logging on to Windows or a VPN) by checking the box and selecting the account from the dropdown menu.
4. Click **Save**.

> *If Connect Before Logon (CBL) has been added to their profile after migrating the profile from an earlier version of Open Mobile, users will have to reinstall the new version of Open Mobile. Connect Before Logon will not work if the user only performs a software update.*

Windows Logon Processing

Available for: Windows clients.

Windows logon processing can display messages regarding password expiration, run logon scripts, or perform Active Directory group policy updates. These actions are executed after a successful corporate network detection test.

- **Password expiration notice:** if an enterprise uses expiring passwords, users will typically be reminded about password expiration dates when they log in to the corporate LAN. However, users who only use Open Mobile to connect to corporate resources will not receive such reminders. As a result, their passwords may expire, which will prevent them from signing in. Logon processing enables the IT administrator to send a reminder message to Open Mobile users as well, to prevent password expiration.
- **Login scripts**: You can configure a script to run at logon, and specify the connection types that it will run on.
- **AD group policy updates:** If selected, the user’s system will run gpupdate.exe and update the user’s local active directory policies.

To specify advanced features,

1. **Password expiration notice:** Select **Password expiration notice** to send password expiration messages to all users. Then, specify a title for the warning message window, the text of the warning message, and the number of days before expiration that the message will be displayed.

> *In the text of the expiration warning message, you can use "{0}" as a variable to indicate the number of days until expiration. For example, if you set number of days until expiration as 4, then you could set the message to be "Your password expires in {0} days." This would be displayed as "Your password expires in 4 days."*

2. **Login scripts:** Select **Login scripts** to run a logon script when the user logs in to Windows. Then select the script to run, either the default logon script or a custom logon script already included on the user's system. Finally, select the connection types you wish the script to run on.
3. **AD group policy updates:** To run gpupdate.exe upon connection, select **AD group policy updates** to enable Active Directory group policy updates, and then select the connection types you wish the updates to run on.
4. Under **Settings for the above selected actions**, select the run context for all of the advanced features. Each of the advanced features will run at the same specified settings.

Event Actions

Available for: Windows clients, Mac OS X clients.

Event Actions enable you to configure automatic launching actions that will be executed when a connection event occurs. For example, you can set an event action to launch a mail application that is triggered by a change in network status, like the establishment of an Internet connection.

Event actions may come in these types (depending on your client version):

Type	Action Will Run…
On Startup of User Interface	When the client's graphic user interface is opened.
Before Establishing an Internet Connection	Before Open Mobile establishes a connection to the Internet.
Before Detecting the Internet on a New Connection	After the Internet connection has been initiated but before the Internet connection is complete
After Establishing an Internet Connection	After Open Mobile establishes a connection to the Internet. (Note: Mac OS X clients support only this action type.)
Before Establishing a VPN Connection	After the VPN connection has been initiated but before the VPN connection is complete.
After Establishing a VPN Connection	After the VPN is connected.
After Establishing a Corporate Network Connection	After connecting to a Corporate Network.
Before Disconnecting a VPN Connection	After the VPN has been disconnected but before the VPN disconnection is complete.
After Disconnecting a VPN Connection	After the VPN has been disconnected.
Before Disconnecting an Internet Connection	After an Internet connection has been disconnected but before the Internet disconnection is complete.
After Disconnecting an Internet Connection	After Open Mobile disconnects from the Internet. (Note: Only supported by Windows 1.4.1 and later clients for non-DSL connections.)
When User Launches Application	When Open Mobile starts up.
When User Exits Application	After Open Mobile is exited.

To add a new event action,

1. Click **Add New Event Action**.

2. In **Action Name**, enter the name of the action.
3. In **Description**, type a short description of the application.
4. In **Application Path**, enter either a local application path, or a complete URL (which will open in the end user's default browser).

   > ***Environmental Variables:*** *For Windows clients,* ***Application Path*** *supports Windows environmental variables, but these must be specified in the format $$ENV:<VARIABLE NAME>$$, where <VARIABLE NAME> is the name of the environmental variable. Examples, $$ENV:systemroot$$\system32, $$ENV:USERPROFILE$$, $$ENV:PROGRAMDATA$$ (on Windows Vista or Windows 7).*

5. In **Executable File Name**, enter the executable file name.
6. In **Arguments,** enter any arguments the application needs to run. If there is more than one argument, separate them by space characters.
7. In **Event Type**, select an event type.
8. In **At frequency of**, select how often the event will be triggered.
9. In **Run Context,** select a run context for the application (user or system context) from the drop-down list.
10. In **Run Mode,** pick a run mode from the drop-down list.
11. If available, select one or more connection types that the action will apply to, by selecting the corresponding checkbox for each. If you select Wi-Fi, you can also select particular Wi-Fi connection types.
12. If you would like the Event Action to launch in a hidden window, select the checkbox next to **Run Hidden**.
13. Click **Save**.

Event Sequence

The sequence in which actions of the same type will run is initially determined by the order that they were added to the profile. However, if you have more than one action of the same type, you can re-define the sequence in which the actions are run. For example, if you define a set of three Post-Connect actions, you can choose which Post-Connect action to run first, which to run second, and which to run third.

To set the sequence of an event action,

1. In the list of event actions, click **Change Sequence.**
2. Actions are shown by type, in sequence from top to bottom. Select an action for which you wish to change the sequence. Using the arrow keys, move the action up or down in the sequence of actions for that type.
3. Click **Save**.

For example, if you wished to change an action from second to first, select the action numbered 2 and drag it to the row of the action numbered 1.

Quick Launch

Available for: Windows clients.

Quick Launch provides users with an easy way to access commonly used programs and websites. Quick Launch items can be launched from the Open Mobile right-click menu, or from the toolbar in the Open Mobile interface.

To add a Quick Launch item,

1. Click **Add Application/URL**.
2. In **Name**, enter the name of the application as it will appear in Quick Launch menu.
3. In **Description**, type a short description of the application.
4. In **Type**, select whether the item is an application or URL.
5. In **URL/Application Path**, enter either a complete URL (which will open in the user's default browser) or a local application path. By default, if no path is specified, Open Mobile searches for Quick Launch applications in the default Windows directory (C:\Windows).
6. In **Arguments,** enter any arguments the application needs to run. If there is more than one argument, separate them by space characters.

   > *Windows Environmental variables are not supported in the Quick Launch application path. However, they are supported in the **Arguments** field.*

7. In **Start application/program in**, enter the directory in which the application will start.
8. In **Icon**, click **Browse**, and then browse to the application's icon file. The icon will be displayed in the Open Mobile Quick Launch toolbar.

   > *If no icon is selected, the Quick Launch item will not be displayed in the Quick Launch Toolbar. However, it will still be displayed (by name) in the Open Mobile system tray right-click menu.*

9. **Always Visible in Application Bar:** If checked, the application icon will not scroll in the toolbar.
10. If Open Mobile should automatically connect to the Internet when this application is Quick Launched from the system tray, select the corresponding checkbox.
11. If Open Mobile should automatically connect to corporate resources by VPN when this application is Quick Launched, select the corresponding checkbox.
12. Click **Save**.

About Quick Launch Toolbar Icons

When uploading toolbar icons, the icon file should follow these standards:

- PNG file, 24px (w) X 24px (h) size, with a maximum file size of 11KB.
- The graphic should touch all edges of the image (no transparent borders).
- Icons are best created in Adobe Illustrator or similar application.

Login Assist

Available for: Windows 2.x clients.

Login Assist enables you to expedite user logins to specified websites by automatically passing credentials to the site's login page. The user is prompted to enter credentials upon first connecting to the page. Open Mobile then uses these credentials for subsequent logins.

In order to use Login Assist with a website, the following is required:

- Users must use Microsoft Internet Explorer to browse to the site.
- Windows User Account Control (UAC) must be disabled.
- The site must have an HTML-based login page. (Flash logins are not supported.)

The Open Mobile Portal comes with a set of pre-loaded Login Assist entries, but you can add your own, as needed.

Auto-Submit: If enabled, Auto-Submit will automate the login process by automatically clicking the **OK** or **Login** button on the site after credentials are submitted. (The user will not need to interact with the login process at all.)

Login Assist Logo: if enabled, the Login Assist logo is displayed next to the login dialog on the actual web site.

> *Login Assist can be used in conjunction with Quick Launch. The user would select Quick Launch load the URL in a browser, and Login Assist would automatically pass the site credentials. With Auto-Submit enabled, this would make logging into the site a one-click experience.*

Adding an Existing Login Assist Entry to a Profile

You should make sure an Open Mobile account has been defined for the profile before configuring Login Assist. The account should contain the required login credentials (typically username and password) for the site.

To add an existing Login Assist entry to a profile,

1. From the rotating list of Login Assist web sites, select the site you would like to add. (Use the arrow buttons to scroll the list left or right to select the entry.)
2. Under the rotating list, select **Enable <Site>**, where <Site> is your selected site.
3. In the **Assign Account** drop down, select an account. The credentials from this account will be passed to the browser when logging in to the site.
4. To enable Open Mobile to automatically submit the account credentials, select **Auto-Submit Login.**
5. To display the Login Assist logo on the login page, select **Show Login Assist logo by input fields.**
6. Click **Save**.

Creating a New Login Assist Entry

You can create your own Login Assist entries for websites of your choice. This involves creating an XML file that specifies login credentials. A sample file is available for download from the Login Assist page.

For more information on creating your own Login Assist entries, see the tech note *Open Mobile Login Assist*, available from the iPass Online Reference (article #3402).

Endpoint Security and Restrictions

Available for: Windows clients.

Endpoint security and restrictions enables you to set policies for applications to run when connected by Open Mobile. These policies can either require an application to run, or prohibit one from running, when Open Mobile connects to the Internet. For example, you could set a requirement for users to be protected by a selected anti-virus application when connected. Another policy could prevent users from using a specific file sharing application when Open Mobile is connected.

There are two important features of endpoint security:

- **Pre-Connect:** If the designated application is not running when the user attempts to connect to the Internet, Open Mobile will attempt to launch it, and will not connect to the Internet without the application running.

- **Automatic Teardown:** An Internet connection may only be maintained if the designated application is running. If the application is stopped for any reason while the user is connected to the Internet, the Internet connection is automatically torn down.

You can configure enforcement through a command-line executable if the designated applications are in violation of policy.

In addition, you can configure the user notifications that will be displayed if the designated applications are in violation.

Endpoint Security Checks for Windows 1.x Clients

When setting up endpoint security for a profile, you can enforce the use of a qualified anti-virus, firewall, or other application when the user is connected to the Internet. A *qualified* application is one that is listed in the user's local Windows Security Center (in Windows 7, the Action Center) for anti-virus or firewall protection.

Enforcement Policies for Windows 1.x Clients

An enforcement policy ensures that a qualified application is running before network connections are permitted.

To enable an enforcement policy for Windows 1.x clients,

1. Select **Enable Endpoint Security Checks**.
2. To enforce an anti-virus solution, select **Enforce the use of qualified anti-virus software as determined by Windows Security Center**.
3. Under **Require that this application runs**, indicate the following:
    - Whether Pre-Connect will be required.
    - Whether Auto-Teardown will be enabled.
4. Repeat Steps 1 through 3 for a firewall application, if desired.
5. Additional applications can be included in an enforcement policy, if desired. To include a new application, click **Add New Application.** Then, under **Required Application:**
6. Enter the application name.
7. In **Executable File Name**, click **Browse**, and then browse to the executable file name.
8. Under **This application is required to run**, indicate the following:
    - Before connecting to the Internet
    - Continuously after a connection is established to the Internet
9. Click **Save**.
10. Add additional applications by repeating steps i-iv.
11. If you want a custom executable to enforce the policy in your environment, select **Try to enforce this policy through a custom executable** (such as a .bat file). Then, in **Command**, enter the syntax of the custom executable.
12. Configure the method by which Open Mobile will interact with the user if in violation of the Pre-Connect or Auto-Teardown policies. You can choose one of the following options for each:
    - *Show the end user a message in a pop-up dialog box.* If selected, enter your message in the

Message box.

- *Show the end user a message in a tooltip.* If selected, enter your message in the **Message** box.
- *Prompt the end user for confirmation to continue.* If selected, the user is prompted to acknowledge the enforcement of the policy.

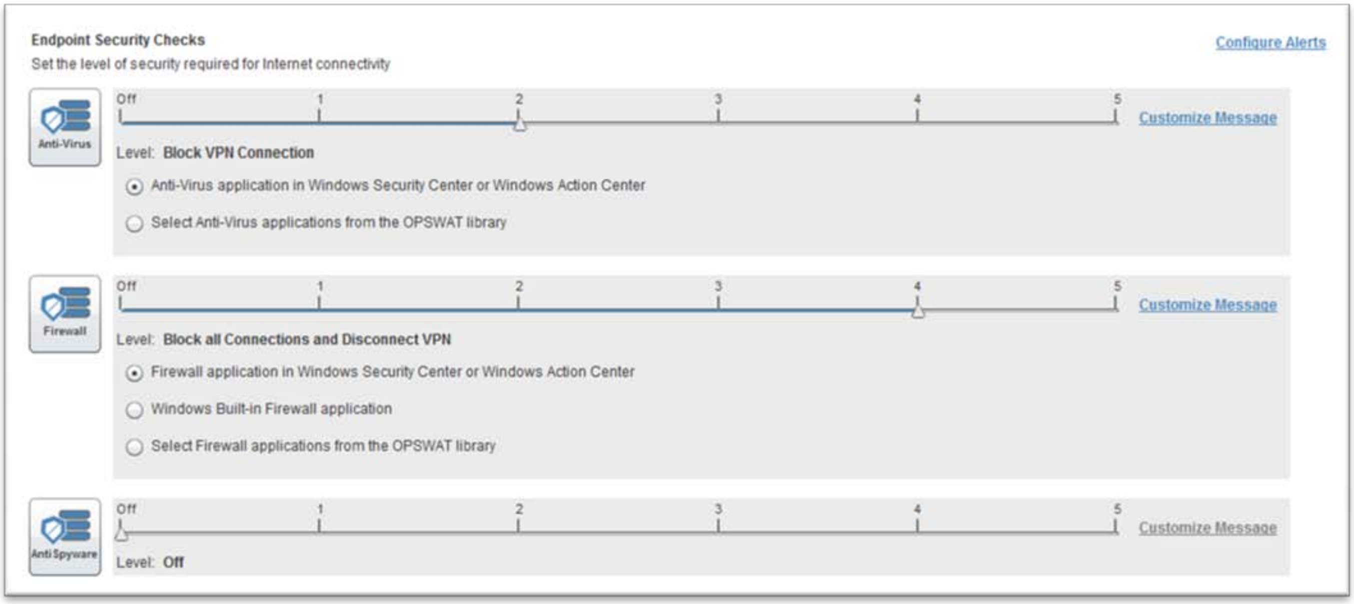
13. Click **Save**.

Restriction Policies for Windows 1.x Clients

You can restrict the usage of designated applications when connected to the Internet. Open Mobile will automatically shut down the restricted application process when detected.

To enable a restriction policy for Windows 1.x clients,

1. Select **Enable Endpoint Application Restrictions**.
2. Click **Add New Application**. Then, under Restricted Application:
   - Enter the application name.
   - In **Executable File Name**, click **Browse**, and then browse to the executable file name.
3. Click **Save**.
4. Select the method by which Open Mobile will interact with the user if in violation of the restriction policy. You can choose one of the following options for each:
   - *Show the end user a message in a pop-up dialog box.* If selected, enter your message in the **Message** box.
   - *Show the end user the following message in a tooltip.* If selected, enter your message in the **Message** box.
   - *Prompt the end user for confirmation to continue.* If selected, your users will be prompted to acknowledge the enforcement of the policy.
5. Click **Save**.



Endpoint Security Checks

Set the level of security required for Internet connectivity

Configure Alerts

Anti-Virus

Level: Block VPN Connection

● Anti-Virus application in Windows Security Center or Windows Action Center

○ Select Anti-Virus applications from the OPSWAT library

Firewall

Level: Block all Connections and Disconnect VPN

● Firewall application in Windows Security Center or Windows Action Center

○ Windows Built-in Firewall application

○ Select Firewall applications from the OPSWAT library

Anti Spyware

Level: Off

Endpoint Security for Windows 2.x Clients

For Windows 2.x clients, you can configure two types of application policy:

- *Required* applications must be running when the user attempts to connect.
- *Restricted* applications may not be running when the user attempts to connect.

You can set the actions taken by Open Mobile when either one of these policies is violated.

Required Applications

For Required applications, you can configure:

- A qualified anti-virus, firewall, or other application. A *qualified* application is one that is listed in the user's local Windows Security Center (in Windows 7, the Action Center) for anti-virus, firewall, or anti-spyware protection.
- A specific antivirus, firewall, or anti-spyware application certified from the OPSWAT library. (OPSWAT certification is a security software interoperability certification program for a variety of application types.)
- For firewalls, the Windows built-in Firewall.
- A custom security application that you can specify. You can also specify a remediation action for the application to repair the executable if it stops running. The remediation action can be a command or batch file.
- In addition, you can set a security level for each security category to control Open Mobile behavior and connection experience.

You can select a security level for anti-virus, firewall, spyware, and other security applications. The table below shows the behavior for each security level if the designated application is not running at the time of the user connection.

Security Level	If the application is not running at connection time…
Off	Open Mobile will take no action.
1: Prompt to Continue	The user will be prompted to continue making a connection.

2: Block VPN Connection	The VPN connection will be blocked.
3: Block Internet and VPN Connections	Internet and VPN connections are blocked.
4: Block All Connections and Disconnect VPN	All connections are blocked. If the application stops running during the connection, any connected VPN is disconnected.
5: Block and Disconnect all Connections	All connections are blocked. If the application stops running during the connection, the connection is terminated completely.

For example, a policy sets a Security Level 1 for the Windows Firewall. If the user attempts to connect when Windows Firewall is disabled, Open Mobile will prompt the user before attempting to connect.

Another policy sets a Security Level 4 for an anti-virus application listed in the user's Windows Security Center. If the anti-virus is not running at connection time, the connection is blocked. In addition, if the user later disables the anti-virus application during the connection, Open Mobile will immediately disconnect any VPN connection. Further, it will block the reconnection until the anti-virus application is re-started.

To designate a Required application,

1. Next to **Endpoint Security and Restrictions**, click **Configure**.
2. Click the **Required Applications** tab.
3. Optionally, click **Configure Alerts** to customize the alerts shown to users. Then, set messages for:
    - **Prompt to continue message:** shown to users when Security Level 1 is set.
    - **Block connection message:** shown to users when a connection is blocked.
    - **Disconnect message**: shown to users when being disconnected.
4. Select one or more application types for security. (None of these types are required. Only choose the types you need for your policy.)
    - **Anti-Virus:** Using the slider, select a security level for anti-virus applications. Then, select the type of application:
        - **Anti-virus application in Windows Security Center or Windows Action Center**: If chosen, any qualified anti-virus application will be used to validate the security level.
        - **Select Anti-Virus applications from the OPSWAT Library:** If chosen, using the arrow controls, move 1 or more of the listed applications from the **Available Applications** to the **Selected Applications** column.
        - Optionally, click **Customize Message** to create the custom message shown to users when the application is not running.
    - **Firewall:** Using the slider, select a security level for firewall applications. Then, select the type of application:
        - **Firewall application in Windows Security Center or Windows Action Center**: If chosen, any qualified firewall application will be used to validate the security level.
        - **Windows Built-in Firewall Application:** If chosen, the Windows Firewall will used to validate the security level.

  - **Select Firewall applications from the OPSWAT Library:** If chosen, using the arrow controls, move 1 or more of the listed applications from the **Available Applications** to the **Selected Applications** column.
  - Optionally, click **Customize Message** to create the custom message shown to users when the application is not running.
- **Anti-Spyware:** Using the slider, select a security level for anti-spyware applications. Then, select the type of application:
  - **Select Anti-Spyware applications from the OPSWAT Library:** If chosen, using the arrow controls, move 1 or more of the listed applications from the **Available Applications** to the **Selected Applications** column.
  - Optionally, click **Customize Message** to create the custom message shown to users when the application is not running.
- **Add New Application:** Click **Add New Application** to add any additional security application. Then, under Add Application, enter the following:
  - **Application Name:** Name of the selected application (up to 25 characters in length).
  - **Executable File Name**: enter or browse to the location of the executable on the user's machine.
  - **Remediation Action:** the path name, plus any parameters needed, of the command or batch file to be executed if the executable stops running.
  - **Enforcement Level:** use the slider to select a security level for this application
  - **Customize Message:** create a custom message to show users when the application is not running.

5. Click **Save**.

> *In Windows 1.4.x clients, a single message is configured for all required endpoint applications. However, Windows 2.x clients enable individual control over such messages. If a Windows 1.4.x client is migrated to Windows 2.x, the single message will be used as the default for all required applications. This can result in a confusing user experience as the same message is displayed multiple times. As a result, when migrating from 1.4.x clients, make sure to configure different messages for each required application.*

Restricted Applications

You can designate any application as *Restricted*. Restricted applications may not be running when the user attempts to connect, or Open Mobile will take the action you specify depending on the restriction level.

Restriction Level	If the application is running at connection time…
Prompt to Continue	Open Mobile will prompt the user with the specified message.
Terminate Application	The application process will be ended.

To designate a restricted application,

1. Next to **Endpoint Security and Restrictions**, click **Configure**.
2. Click the **Restricted Applications** tab.
3. Click **Add New Restriction**.
4. On the **Add Restriction** dialog, in **Application Name**, enter the name of the restricted application.
5. In **Executable File Name**, click **Browse**, and then select the application path.
6. In **Restriction Level**, use the slider to select the restriction level for the application.
7. In **Customize Message**, enter the message shown to users, or use the default.
8. Click **Submit**.

Run Once Packaging

Available for: Windows 2.0 and later clients.

If available, Run Once Packaging enables Open Mobile administrators to create a downloadable package for end users that can deliver third-party software components, or upgrades to device drivers and firmware. Subsequent processing or of the delivered files can be performed by means of an included script or executable that customers create.

About Run Once Packaging

Run Once Packaging is intended for dynamic delivery of device drivers or firmware updates. However, a properly constructed Run Once package could be used to deliver nearly any software component to users.

A Run Once package is created as part of an Open Mobile profile. When the Open Mobile client receives a test or published profile that specifies an unexecuted Run Once package, the client downloads the package, and then runs the associated script or executable. By default, a package runs in the user context, but can be set to run in the administrator context. A profile may include any number of packages, and each package can be up to 16 MB in size.

Package files themselves are not included in an Open Mobile profile. A profile merely includes the package definition file, ropimage.xml, which includes the specifications and download URLs for the actual package files.

- A Run Once package does not ‘install’ or ’uninstall’ in the Windows context. The package is merely a vehicle for the one-time delivery of a payload of files, controlled by a script written by an Open Mobile administrator. (Note, however, that depending on the individual files included in a package, these may be subsequently installed or uninstalled in the Windows context. For example, upon being executed, an MSI file would be installed in the Windows context, but this is the expected functionality for MSI files and not part of the ROP feature.)
- A Run Once package delivers no other files than the ones specified in the package, nor does a package itself alter any Windows registry entries. (As above, an individual file in a package may alter registry entries as part

of its normal functionality, but this is not part of the ROP feature.)

Because of the power and flexibility of Run Once Packaging, an Open Mobile administrator should plan, design, and collect the included files for a Run Once package before assembling the package on the Open Mobile Portal. Any included scripts and the overall package functionality should be tested thoroughly before deploying to users.

About the ROP Script or Launch Action

Execution of the files in the Run Once package is accomplished by one of two means:

- A script or executable can be included in the package that will install the component files to the user's system. An ROP script can be any valid script that runs on Windows, such as a VBScript or JavaScript file, batch file, or compiled executable. There is no required syntax for such scripts or executables, and they may be up to 16 megabytes in size (that is, up to the 16 MB package size limit). The designer of the package is responsible for creating (and testing) the ROP script or executable.
- Alternatively, a package can be launched by operating system commands. A package need not include a script or executable of any kind, and could be executed entirely through OS commands. For example, if a package comprised an MSI file, the package could be launched by having the user invoke the local msiexec.exe executable.

About Included Files

The files to be included in a package (such as device driver files) should be collected before creating the package on the Open Mobile Portal. An included file may be any valid Windows file. Each file can be up to 16 MB in size.

Creating a Run Once Package

To create a Run Once package,

1. On the **Configure Profile** page, next to **Run Once Packaging**, click **Configure**.
2. In **Package Name,** enter the name of the package (under 200 characters).
3. In **Startup Command**, enter the syntax for your ROP script or executable to run, including all arguments. Startup Command may be up to 2000 characters in length.
   - For a batch file, begin the startup command with cmd.exe /c, followed by the name of the script (for example, cmd.exe /c mybatch.bat).
   - For a VBScript or JavaScript, use wscript.exe <script name>.
   - For an HTA script, use mshta.exe <script name>.
   - For a Power Shell script, use ps.exe <script name>.
   - For Windows 1.4.1 clients (only), the startup command must include %ROPTEMP%, which is the path of the temporary folder to which the package is downloaded (for example, cmd.exe /c %ROPTEMP%\test.bat %ROPTEMP). This is not necessary for Windows 1.4.2 and later clients, as the script's working folder is set to the folder where it resides.
   - Always use the full path for the script name if its location is not in the Windows path.
4. To run the startup command from the System account with the administrator privilege, select **Run startup command as System User.**
5. Click **Add New File,** and then browse to the location of a component file.

6. Repeat Step 5 for each subsequent included file.

7. Click **Save.**

For more information about Run Once Packaging, consult the *Open Mobile for Windows Administrator's Guide.*

Proxy Support

Available for: Windows 2.x clients.

You can set proxy server authentication settings for all users of a given profile. The authentication settings passed to a proxy server can be taken from local Windows domain credentials, or from the credentials of an Open Mobile account. (This account can be one for general use, or can be created specifically for proxy authentication.)

If using account credentials (as opposed to local Windows credentials) make sure one or more accounts have been defined in the profile before choosing proxy server settings.

To specify proxy server settings for the profile,

1. On the **Configure Profiles** page, next to **Proxy Support**, click **Configure**.

2. Under **Authenticate to the proxy using**, select one of the following:

   - **Local Windows domain credentials:** to pass local Windows login credentials to the proxy server.
   - **Account credentials:** to pass credentials from a general or dedicated Open Mobile account. Then, select the account used.

3. Under **Maximum number of authentications per day**, select the number of authentication attempts to the proxy server to be performed in a 24-hour period. (This period is measured from the time of the first authentication attempt.)

4. Click **Save**.

> *In Windows 1.4.x and earlier clients, Open Mobile includes a (non-configurable) ability to authenticate to proxy servers using Windows domain credentials. However, in Windows 2.x clients, in order to authenticate to proxy servers, you must affirm whether to use Windows domain credentials or whether to use separate account credentials. This applies both to new Windows 2.x profiles and to profiles upgraded to Windows 2.x from earlier versions.*

Conflict Detection

Available for: Windows 2.x clients.

The Conflict Detection tool, available for Windows 2.0 and later clients, enables you to configure settings to enable Open Mobile to interoperate with other connection manager applications.

Connection management applications use various system resources, such as network adapters. Some connections managers require an exclusive use of some of these resources. This may interfere with Open Mobile operations, resulting in various conflicts. In order for Open Mobile to function with such connections managers, it needs to determine conflicts and resolve them.

To enable Conflict Detector for a profile, you will need to configure an XML file with your Conflict Detector settings, and then upload it to a profile. For information on Conflict Detector and how to configure a conflict detector XML file, see the document *Conflict Detector User Guide*, available from the iPass Online Reference as article #3509.

To add Conflict Detector to a profile,

1. On the **Configure Profiles** page, next to **Conflict Detection**, click **Configure**.
2. On the **Conflict Detection** page, select **Enable Conflict Detection**.
3. Under **Upload File**, click **Browse**, and browse to your conflict detection file.
4. Click **Save**. The file is added to the Open Mobile Profile.

Custom Profile Attachments

Available for: Windows 2.2 clients and later.

The Custom Profile Attachments feature allows you to attach scripts and executables used for Custom VPN launches or special connect actions (such as an Event Action, Quick Launch, or Conflict Detector) so that they are part of a profile and don't have to be manually packaged. You can upload a new file or update an existing file.

To attach a file:

1. Click the **Attach File** button.
2. Browse to the file you would like to attach, select it and click **Open**.
3. Your file will show up in the list.

To delete a file, click the **Delete** link and click **Yes** to confirm.

> *Individual files have a size limit of 1 MB and the total size of all uploaded files is limited to 2 MB.*

Localization

For Windows client 2.1.0 and later, an XML file with all the strings that can be customized in the Open Mobile Portal can be downloaded for localization in French, German, or Japanese.

To localize customized messages,

1. Click **Download English translation template** to download an XML file with all possible customized strings (including messages that have not been customized or enabled).
2. Have the strings translated. You should make sure that the translator preserves the XML format and all of the tags.
3. After you receive the translations, return to the **Localize Messages** page.
4. Next to the appropriate language, click **Browse**. Navigate to the translated XML file and click **Open**. The name of the translated file will appear in the box. Repeat this process for each translated language.
5. When all of your translated files have been uploaded, click **Save**.

Testing a Profile

You should test a profile before deploying it to your end users, to make sure it fully addresses both your users' needs and the needs of your business or department. Typically, profile testing is done with a small group of selected users.

While testing, only your test users should receive any changes to the profile. Once you are satisfied with your testing, you can deploy the profile to production, and it can be distributed to your user population at large.

To publish a profile to testing,

1. On the **Configure Profile** page, click **Publish to Test**.
2. On the **Publish to Test** page, click **Publish to Test**.
3. Optionally, in **Notes**, enter any notes you wish to make about the test profile.
4. Click **Publish as Test Profile.** The profile status is changed to Test and the profile minor version number is automatically incremented**.**
5. You can now download an installer file that will install Open Mobile and your profile.
   - For Windows 1.4.1 and later clients, you can download a ZIP archive that contains only the profile settings, which can be imported into an existing Open Mobile installation. See the *Open Mobile Administrator's Guide,* available from the iPass Online Reference as article #3209, for instructions on how to import a profile into Open Mobile.
   - Separately, if dial connections are enabled, you can also download the dialer plug-in installer.

These installers can be distributed to your test users through your preferred software distribution method.

> *The build process for installers can take some time. Give the process a few moments to complete.*

Profile Deployment

After testing the profile with selected end users, you can now publish it to production and deploy it.

To publish a profile to production,

1. On the **Configure Profile** page, click **Publish to Production**.
2. On the **Publish to Production** page, select **Publish to Production**.
3. Optionally, in **Notes**, enter any notes you wish to make about the test profile.
4. Click **Publish to Production.** The profile status is changed to *Production* and the profile major version number is automatically incremented**.**
5. You can now download an installer file that will install Open Mobile and your profile. Separately, if dial connections are enabled, you can also download the dialer plug-in installer. These installers can be distributed to your users through your preferred software distribution method.

> *If you are making changes to an existing test profile, once changed to Production status, it will be automatically deployed to the users who have the test profile. Test users need take no action to receive it.*
>
> *The build process for installers can take some time. Give the process a few moments to complete before attempting to download a newly created installer.*

Download Profile

Windows

Software and Profile Installer: Click **Download Software and Profile Installer** to download an MSI file to your local machine. This file can then be distributed to your end users.

Profile Archive: In addition, for Windows 1.4.1 and later clients, you can download a ZIP archive that contains only the settings corresponding to a profile, which can be imported into Open Mobile. An imported profile will overwrite a user's existing profile settings. For information on importing a profile, consult the *Open Mobile Administrator's Guide.*

> *Open Mobile MSI installers are digitally signed in order to enforce group security policy. Each MSI file's digital signature includes the filename. As a result, you should always save any downloaded installers with the default file name as supplied by the Open Mobile Portal. Do not rename an installer file, as this can cause installation issues.*

If dial connectivity is enabled the Dialer Plug-in installer will also be listed here.

Mac

Software and Profile Installer: Click **Download Software and Profile Installer** to download a DMG file to your local machine. This file can then be distributed to your end users.

Android

Android Market: Instructions are included on this page for users to download and install the app from the Android Market.

Software and Profile Installer: Click **Download Software and Profile Installer** to download a ZIP file to your local machine. The zip file contains two APK files:

- The base APK file is named com.iPass.OpenMobile_base.apk (or com. <Package Name>_base.apk). It works like the Android Market version and requires activation (the user will have to enter a Profile ID and PIN).
- The profile bundle .apk file is named com.iPass.OpenMobile_profile_bundle.apk (or com. <Package Name>_profile_bundle.apk). It does not require activation, and the user just needs to enter their account credentials to start using it.

For more information on downloading the Open Mobile for Android installer, consult the *Open Mobile for Android Quick Start Guide*

iOS

iTunes Store: Instructions are included on this page for users to download and install the app from the iTunes Store.

Download Software

The **Download Software** page lists the currently available production Open Mobile for Windows dialer plug-in installers. Each installer is packaged as an MSI file. Click a link to download the corresponding software package to your local system.

Device Support

The Device Support page enables you to manage your Mobile Broadband devices. These Mobile Broadband devices may be integrated with Open Mobile in one of the following ways:

- **Full Integration:** devices that are fully integrated have support included in Open Mobile and tested by iPass. Open Mobile integrates over one hundred Mobile Broadband device models from major manufacturers. These fully integrated devices work smoothly with Open Mobile right out of the box. You need take no further actions to use them for Open Mobile connections.
- **ODF Integration:** Open Device Framework (ODF) is a toolkit for extending support to devices that are not officially integrated in Open Mobile, enabling you to use such devices for Open Mobile connections. ODF integration involves creating and testing an XML integration file for each device model, verifying its functionality, and then including the integration file in an Open Mobile profile. iPass maintains a library of sample ODF support files that customers can use in their own integrations. In addition, customers are able to create their own integration files for devices that iPass has not yet covered.

Use the **Device Support** page to add your own integration files to Open Mobile. These files can then be used as part of your Open Mobile profiles. See page 22 for more information.

You can search the device library to check if the device is supported by Open Mobile.

To verify support of a device in Open Mobile,

1. Under **Search for Device Support,** select your search criteria using the drop-down lists.
2. Click **Search.** Any devices matching your search criteria are shown on one of three tabs:
   - **Integrated Support**: The **Integrated Support** tab lists devices that are already fully integrated with Open Mobile.
   - **ODF Samples:** iPass has created sample ODF integration files for devices shown on the **ODF Samples** tab. You can download and use any of these files as a basis for creating your own device integrations. These files will require adjustments, testing, and verification before you deploy them in profiles, to ensure that they will work correctly with your particular device. Because of the similarity of many devices, especially those from the same manufacturers, it may be possible to adapt a sample ODF file for a device that is similar to yours for your own requirements.
   - **My Device Support:** Devices shown on the **My Device Support** tab have been integrated by your enterprise, using the ODF integration instructions given by iPass.

My Devices Support

You can integrate a wide variety of devices using the ODF toolkit. A complete discussion of the ODF integration process is beyond the scope of this guide. For more information, consult the *iPass ODF Training Workbook.*

The **My Device Support** tab includes sample device ODF integration files that you can use as a starting point for the creation of your own integration files. In addition, you can create files from scratch for your own devices.

Once the proper XML files have been created, they can be uploaded to the Open Mobile Portal for use in your Open Mobile client profiles.

To add device support to your device library,

1. Create (or edit an existing) XML file as outlined in the ODF documentation.
2. On the **My Device Support** tab, click **Create Device Support**.
3. Under **Device XML File**, click **Browse** and select your ODF file. Then, click **Upload.**

4. The file is read and the manufacturer, family, and model are displayed. If you would like to change the display of any of these values, in **Manufacturer**, **Family** and **Model**, enter the desired new values.
5. In **Device Support Name,** enter the name you will assign to this device support.
6. In **Description**, enter a description of the support.
7. In **Minimum Software Version Supported**, from the drop-down list, select a minimum version of the Open Mobile client that will include this device.
8. Enter values for the following device attributes:
   - **Device Type:** select a device type (CDMA or GSM).
   - **Form Factor:** select a device form factor from the drop-down list.
   - **Device Driver:** enter the filename of the device driver.
   - **NDIS 6.2 Compliant Driver:** indicate whether the device driver is NDIS 6.2 compliant.
   - **Device firmware:** enter the filename of the device firmware.
   - **Comments to Customer:** enter any comments on the device support that you wish to share with customers.
9. Click **Save**.

Upload Networks

You can upload your own network listings to your Open Mobile directory. Network listings can include Mobile Broadband networks and Wi-Fi networks. Once uploaded, your users will be able to view and connect to these networks using Open Mobile, and the network connection settings will be pre-populated with the information you include in the directory.

Managing Your Mobile Broadband Directories

The **Mobile Broadband Network Directories** list shows all of your current Mobile Broadband directories. You can sort this list by name, version number, or the account that last modified the directory.

- Click **Download** to download a directory to your local system.
- Click **Upload** to upload a new version of an existing directory.

Uploading a Mobile Broadband Network Directory

You upload your network listings as an XML file. For more information, consult *Creating a Mobile Broadband Directory for Open Mobile*, available from the Open Mobile Portal.

A sample directory file is available for download.

To upload a new Mobile Broadband network directory,

1. Create your network directory XML file.
2. Click **Import New Directory**.
3. In **Display Name**, enter the name of the directory as you would like it to be displayed in the list.
4. In **Directory File**, click **Browse**, and then select the XML directory file.
5. Click **Upload File.** The directory is automatically assigned a version number.

Managing Your Wi-Fi Directories

The **Wi-Fi Network Directories** list shows all of your current Mobile Broadband directories. You can sort this list by name, version number, or the account that last modified the directory.

- Click **Download** to download a directory to your local system.
- Click **Upload** to upload a new version of an existing directory.

Uploading a Wi-Fi Networks Directory

You upload your network listings as an XML file. . For more information, consult *Creating a Wi-Fi Directory for Open Mobile*, available from the Open Mobile Portal.

A sample directory file is available for download.

To upload a new Wi-Fi network directory,

1. Create your network directory XML file.
2. Click **Import New Directory**.
3. In **Display Name**, enter the name of the directory as you would like it to be displayed in the list.
4. In **Directory File**, click **Browse**, and then select the XML directory file.
5. Click **Upload File.** The directory is automatically assigned a version number.

Request Domains

On the **Request Domains** page, you can submit a request for one or more authentication domains. (Domains are also known as *realms*.) Typically, different groups within your business organization use different authentication domains. You can choose to have multiple domains to segment user communities, or to display extra information in your iPass Call Detail Records (CDRs).

A domain does not need to be a registered ICANN Internet domain, but it must be unique across all iPass customers. (iPass will verify this after it receives your domain request.)

Once domains are approved by iPass, the domains can be pre-populated in Open Mobile and included in the authentication string that Open Mobile uses to authenticate the user.

An example of an authentication string with a domain would be user@example.com.

Prefixes

Domains can be included in the authentication string as a realm prefix, in which case they are appended to the front of the user name. Although case-insensitive, prefixes are upper case by convention. A prefix must be 3-5 alphabetical characters and followed by a forward slash (for example, ZZZ/). Spaces and @ are not allowed. If a realm prefix is specified here, it will be applied, but it will not be displayed in the client.

Domain Requests

- The **Active Domains** list shows the list of your currently active domains.
- The **Domain Requests** list shows Pending Requests, Rejected Requests, and Approved Requests.

To request an additional domain,

1. Click **Request Additional Domains**.
2. In **Domain Name**, enter the name of the domain.
3. If you wish to include the domain name as a prefix, under **Treat as a Prefix?,** click **Yes**.
4. If you wish to request more than one domain, click **Add**, and then repeat steps 1 through 3 for each additional domain.
5. Click **Submit**. Your domain request is submitted to iPass. Requests for new domains typically receive a response in 1-2 business days.

> *You may only have one pending request at a time, but you may include any number of domains in that single request. Before making another request, please wait for the first request to be processed.*

Register Packages

Available for: Android 2.x clients.

Android clients, which are distributed through the Android Market, need to be registered with a valid, unique package name. A valid package name must be in the format: <three-letter top-level domain>.<organization's domain>.<one of the organization's sub-domains>. The name must be an alphanumeric string (A-Z, a-z, 0-9) and may not contain special characters. An example would be `com.iPass.OpenMobile`.

To register a package name,

1. In **Package Name**, enter a valid package name.
2. Click **+**. The new package name is added to the list of existing packages.
3. Click **Save**.

To delete a package name,

1. From the list of packages, select the name to be deleted.
2. Click **-.** The package name is deleted from the list.
3. Click **Save**.

Once you have registered the package name, you can assign it to a particular Android client brand.

Mobile Number Management

Open Mobile uses IMSI to identify each Mobile Broadband device, not its phone number. In order for the device to show in some Open Mobile reports, each IMSI must be mapped to its corresponding phone number in the Open Mobile Portal.

To do this, you must upload a properly formatted XML file containing the mappings. An example file is shown here.

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileMappings>
 <MobileMapping>
```

```
        <phone>15551111111</phone>
        <imsi>111111111111111</imsi>
 </MobileMapping>
 <MobileMapping>
        <phone>15552222222</phone>
        <imsi>222222222222222</imsi>
 </MobileMapping>
</MobileMappings>
```

The XML file may contain up to 500 phone numbers. If you need to import more data, please break it up into multiple files, each containing a maximum of 500 phone numbers.

To view mapped phone numbers,

1. Click **Mobile Number Management**.
2. Under **Mobile Number Management**, click **Manage**. The existing devices are displayed.

To import new device mappings,

1. On the **Manage Mobile Numbers** page, click **Import Mobile Nos**.
2. On the **Import Mobile Nos.** page, in **Mobile Nos. File**, click **Browse**, and then select your XML mapping file.
3. Click **Upload File.** The device mappings are imported and displayed in the Open Mobile Portal.

If you need to edit existing device mappings, then prepare an XML file with your edited mapping data. Upload the file as if you were importing a new set of device mappings. The edited data will overwrite any existing phone numbers and IMSI data.

Client Preferences

For Windows clients 2.1.0 and later, you can configure how the client identifies users who have not entered their account credentials (such as Username) when it sends SQM records. If the box is checked, the client will include the Windows' User Name or the Device Name to identify the user in the SQM record, and if the box is not checked, the client will use a randomly generated Dialer ID to identify the user in the SQM record.

Manage Brands

If enabled for your company, you can create a customized look and feel for some clients.

Brand options are supported by clients built for these versions of Open Mobile:

- All Windows clients
- Mac OS X clients version 1.2 and later
- Android clients version 2.x and later
- iOS clients version 2.1 and later (logo on the About screen)

Once created, you assign the brands you create to an actual client on the **Configuration** tab**.**

The **Brands** list shows the list of your current brands. You can sort on brand status and the date of last update.

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.

Once created, a brand cannot be deleted. (Deleting a brand could cause conflicts with deployed profiles that use an existing 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.

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 the items shown in the table. If no element is selected, the default is used. Default images are illustrated in the Portal.

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

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

Windows version 1.x

Client Elements	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	1.x
Image/Icon	
Logo	312px (w) x 25px (h), PNG format , file size max 11 KB
System Tray Image	16px (w) x 16px (h), PNG format, file size max 11 KB
Taskbar Icon	32px (w) x 32px (h), ICO format, file size max 500 KB
Expand Arrow	20px (w) x 20px (h), PNG format, file size max 11 KB
Collapsed Arrow	22px (w) x 22px (h), PNG format , file size max 11 KB
OpenAccess Icon	Version 1.3 and later, 20px (w) x 20px (h), PNG format, file size max 11 KB

Client Elements	Requirement
iPass Icon	Version 1.3 and later, 20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Mobile Broadband	Version 1.3 and later, 20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Wi-Fi	Version1.3 and later, 20px (w) x 20px (h), PNG format, file size max 11 KB
Text	
Application Title	Alphanumeric string, max 35 characters
Additional Help Title	Version 1.3 and later, Alphanumeric string, max 35 characters
Additional Help Content	Version 1.3 and later, Maximum file size 800 KB
Alternate Help Title	Version 1.3 and later, Alphanumeric string, max 35 characters
Alternate Help Content	Version 1.3 and later, Maximum file size 800 KB
Color	
Application Name	Hexadecimal color value
Application Bar	Version 1.3 and later, Hexadecimal color value
Header Bar	Hexadecimal color value
Footer Bar	Hexadecimal color value
Network Highlight	Hexadecimal color value
Connect Button	Version 1.3 and later, Hexadecimal color value
Disconnect Button	Version 1.3 and later, Hexadecimal color value
Other Buttons	Version 1.3 and later, Hexadecimal color value
Installer	
Company Name	Alphanumeric string, max 35 characters.
Relative Install Path	Relative path may not include characters such as /:*?"<>| Environmental variables may be included.
Logo Icon	16px (w) x 16px (h) , ICO format, file size max 500 KB

Windows version 2.x

Client Elements	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	2.x
Core Branding	
Logo	300px (w) x 35px (h), PNG format , file size max 11 KB
Application Title	Alphanumeric string, max 35 characters
System Tray Image	16px (w) x 16px (h), PNG format, file size max 11 KB
Taskbar Icon	32px (w) x 32px (h) , ICO format, file size max 500 KB
Additional Branding	
OpenAccess Icon	20px (w) x 20px (h) , PNG format, file size max 11 KB
iPass Icon	20px (w) x 20px (h) , PNG format, file size max 11 KB
Custom Mobile Broadband	20px (w) x 20px (h) , PNG format, file size max 11 KB
Custom Wi-Fi	20px (w) x 20px (h) , PNG format, file size max 11 KB
Title Text Color	Hexadecimal color value
Titlebar Color	Hexadecimal color value
Additional Help Title	Alphanumeric string, max 35 characters
Additional Help Content	Maximum file size 800 KB
Alternate Help Title	Alphanumeric string, max 35 characters
Alternate Help Content	Maximum file size 800 KB
RSS Feed URL	Valid URL (see page 66)
First Launch Tutorial	None (see page 66)
Device Notification	None (see page 68)
Device Notification (U.S. English)	Version 2.1.0 or later, valid XML (see page 68)

Device Notification (French)	Version 2.1.0 or later, valid XML (see page 68)
Device Notification (German)	Version 2.1.0 or later, valid XML (see page 68)
Device Notification (Japanese)	Version 2.1.0 or later, valid XML (see page 68)
Choose a search provider	Valid XML (see page 67)
Internet Links	
Custom Hotspot Finder Name	Alphanumeric string
Custom Hotspot Finder URL	Valid URL
Installer	
Company Name	Alphanumeric string, max 35 characters.
Relative Install Path	Relative path may not include characters such as /:*?”<>| Environmental variables may be included.
Desktop Icon	16px (w) x 16px (h) , ICO format, file size max 500 KB

Mac version 1.x

Client Elements	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	1.x
Image/Icon	
Online Menubar Image	16px (w) x 16px (h), PNG format, file size max 16 KB
Offline Menubar Image	16px (w) x 16px (h), PNG format, file size max 16 KB
OpenAccess Icon	20px (w) x 20px (h), PNG format, file size max 11 KB
iPass Icon	20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Mobile Broadband	20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Wi-Fi	20px (w) x 20px (h), PNG format, file size max 11 KB
Text	
Application Title	Alphanumeric string, max 35 characters
Alternate Help Title	Alphanumeric string, max 30 characters
Alternate Help Content	Mac OSX supported help file, Maximum file size 800 KB
Color	
Status Color	Hexadecimal color value
Background Color	Hexadecimal color value
Installer	
Installer Title	Alphanumeric string, max 35 characters
Application Icon	ICNS file, must be 16x16, 32x32, 48x48, 128x128, 256x256, 512x512 pixel size, max 512 KB file size
Installer Logo	620px (w) x 420px (h), PNG format, max 64 KB file size

Mac version 2.x

Client Elements	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	2.x
Image/Icon	
Logo	24px (w) x 24px (h), PNG format, file size max 16 KB
Menubar Image	16px (w) x 16px (h), PNG format, file size max 16 KB
OpenAccess Icon	20px (w) x 20px (h), PNG format, file size max 11 KB
iPass Icon	20px (w) x 20px (h), PNG format, file size max 11 KB

Client Elements	Requirement
Custom Mobile Broadband	20px (w) x 20px (h), PNG format, file size max 11 KB
Custom Wi-Fi	20px (w) x 20px (h), PNG format, file size max 11 KB
Text	
Application Title	Alphanumeric string, max 35 characters
Alternate Help Title	Alphanumeric string, max 30 characters
Alternate Help Content	Mac OSX supported help file, Maximum file size 800 KB
Color	
Status Color	Hexadecimal color value
Background Color	Hexadecimal color value
Internet Links	
Custom Hotspot Finder Name	Alphanumeric string
Custom Hotspot Finder URL	Valid URL
Installer	
Installer Title	Alphanumeric string, max 35 characters
Application Icon	ICNS file, must be 16x16, 32x32, 48x48, 128x128, 256x256, 512x512 pixel size, max 512 KB file size
Installer Logo	620px (w) x 420px (h), PNG format, max 64 KB file size

Android

Client Elements	Version 2.0	Version 2.1.x	Version 2.2.0
Brand Name			
Brand Name	Alphanumeric string, max 35 characters. Required.	Alphanumeric string, max 35 characters. Required.	Alphanumeric string, max 35 characters. Required.
Class	Select from dropdown	Select from dropdown	Select from dropdown
Software Version	2.0	2.1.x	2.2.0
Package Name	N/A	N/A	Select from dropdown
Image/Icon			
Logo	N/A	N/A	Custom Package Name, 75px (w) x 75px (h), PNG format , max file size 11 KB
Splashscreen	N/A	N/A	Custom Package Name, 480px(w) x 800px, PNG format, max file size 100 KB
Background	N/A	N/A	Custom Package Name, 720px(w) x 1280px, PNG format, max file size 1 MB
OpenAccess Icon	72px (w) x 72px (h) , PNG format, file size max 150 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB
iPass Icon	72px (w) x 72px (h) , PNG format, file size max 150 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB
Custom Wi-Fi	72px (w) x 72px (h) , PNG format, file size max 150 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB	20px (w) x 20px (h) , PNG format, file size max 11 KB
Text			
Application Name	N/A	N/A	Custom Package Name, Alphanumeric string, max 20-25* characters
Network Alert Message	N/A	N/A	Custom Package Name, Alphanumeric string, max 80 characters
Installer			
Launcher Icon	N/A	N/A	Custom Package Name, 72px (w) x 72px (h) in PNG format, max file size11 KB
Notification Icon	N/A	N/A	Custom Package Name, 24px (w) x 24px (h) in PNG format, max file size11 KB

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

iOS version 2.1.0

Client Elements	Requirement
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Software Version	2.1.0
Image/Icon	
Logo	250px (w) x 250px (h), PNG format , file size max 150 KB

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

Additional Help File

As part of branding Windows and Mac OS X clients, you can include your own additional help file, which can supplement, or replace completely, the existing Open Mobile Help file. You can use additional help to detail company contact information, company-specific procedures or documentation, or other information you wish to display to users.

If you choose to use Additional Help as part of client branding, you must specify a title for the help as well as create the actual content for the help.

Additional Help Title: The additional help title will appear as an item on the Open Mobile Help menu.

Additional Help File: The additional help file content must be a single file of any type, up to 800 KB in size, with these restrictions:

- A default reader or viewer for the file must be installed on the client computer and associated with the file type. For example, if you chose to provide Additional Help in PDF format, you must ensure that an appropriate PDF reader is installed on the client computer and that the reader will be invoked if the file is opened.
- The filename extension must be registered (associated) with the viewer on the client computer.

> *If HTML is chosen for the Additional Help file, it must be a single, local HTML file, but this HTML file can link to online content.*

RSS Settings

You can enable an RSS feed in Open Mobile, specifying a single URL for news and headlines to be streamed to users.

First Launch Tutorial

Windows clients 2.0 and later include an Open Mobile Tutorial, which is launched when the user first runs Open Mobile. This Tutorial is enabled by default, but can be disabled for branded clients.

Internet Links

Windows and Mac clients include a set of Internet links by default. These include

- **iPass Hotspot Finder:** enables users to locate Wi-Fi hotspots worldwide.
- **Smart Phone Information URL:** gives information about the Smartphone versions of Open Mobile.

In addition, you can include a custom Hotspot Finder. Select the **Show Custom Hotspot Finder** checkbox, and enter the name and URL of the Hotspot Finder.

Search

For Windows and Mac clients, you can define an Internet search engine for use with Open Mobile. If enabled, users will be able to perform Internet searches directly in Open Mobile. To enable search, select it in the Open Mobile Portal. Then, upload a search file, which is an HTML file formatted as follows:

- The file must be self-contained, requiring no additional resources uploaded, but may reference external or internet resources. It should not refer to itself, as the upload process may change the filename.
- Maximum size of the search window in Open Mobile is 319 pixels wide by 125 pixels high.
- Specify html { overflow: auto } in the CSS line to prevent the vertical scrollbar from showing.
- Avoid the use of any scripts, if possible.

An example search file is shown here, enabling search on a popular search engine.

```
   <?xml version="1.0" encoding="UTF-8"?>

   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

   <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

   <head>

     <title>MySearchPage</title>

       <meta name="created" content="Wed, 28 Apr 2010 22:28:23 GMT" />

     <meta name="description" content="" />

     <meta name="keywords" content="" />

     <style type="text/css">

     html {

           overflow: auto;

     }

     <!--

   .body {

    height: 125px;

    width: 319px;

    background-color: #EFEFEF;

    color: #000000;

    max-width: 319px;

    max-height: 125px;

   }

   -->

   </style>
   </head>
   <body bgcolor="#FFFFFF" text="#000000" link="#0000FF" vlink="#800080" alink="#FF0000"
leftmargin="0px" topmargin="0px">
   <div class="body">
   <form action="http://www.google.com/cse" id="cse-search-box" target="_blank">
     <div>
       <input type="hidden" name="cx" value="013516449520835724295:3fa3ka1eqy4" />
       <input type="hidden" name="ie" value="UTF-8" />
       <input type="text" name="q" size="31" />
       <input type="submit" name="sa" value="Search" />
     </div>
   </form>
   <script type="text/javascript" src="http://www.google.com/cse/brand?form=cse-search-
box&amp;lang=en"></script>
   </div>
   </body>
   </html>
```

Device Notifications

For Windows clients 2.0 and later, Device Notification will send a message to users running Open Mobile who attach a smartphone or tablet by USB cable if enabled. The message will contain information about the Open Mobile smartphone clients for iOS and Android.

In Windows clients 2.1.0 and later, the Device Notification can be customized and localized.

To customize Device Notification,

1. Click **Download English translation template**
2. Edit the strings in the XML file (preserving the tags) and then save the file.
3. Return to the **Create Client Brand** page and click **Browse** next to U.S. English.
4. Navigate to the XML file that you saved and click **Open**. The file name will appear in the box.

To localize Device Notification,

1. Click **Download English translation template**. If you would like to customize the strings, follow the steps above first.
2. Have the strings translated. You should make sure that the translator preserves the XML format and all of the tags.
3. After you receive the translations, return to the **Create Client Brand** page.
4. Next to the appropriate language, click **Browse**. Navigate to the translated XML file and click **Open**. The name of the translated file will appear in the box. Repeat this process for each translated language.

Creating and Editing a Client Brand

To create a new client brand for a supported platform,

1. Under **Branding**, click **Client Options**.
2. Click **Create a Brand**.
3. On the **Create a Brand** tab, in **Brand Name**, enter a new brand name.
4. Under **Platform**, select a platform for the brand from the drop-down list.
5. (For Android clients) Under **Class**, select a class of brand from the drop-down list.
6. Under **Software Version**, select the version number of Open Mobile for which the brand is intended.
7. (For Android clients) In **Package**, select a previously registered package name to associate with the brand.
8. Select the branding tabs as needed to enter your desired branding elements.

   > *The Image Map interactively displays the components of the Open Mobile user interface, as you change them, so you can preview your brand before you save it.*

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

Once created, you can publish the brand so that you can include it in your Open Mobile 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 your Open Mobile profiles, and can be shared with your child accounts. A published brand may not be edited.

To publish a brand,

1. Create a brand.
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** page, select the direct child accounts with which you wish to share the brand.
3. Click **Share**, and then click **Yes** to confirm sharing.

Searching for Brands

You can search your brands by Brand Name to locate a particular brand. The search is case-insensitive, and will return all brands whose names begin with the text you enter.

To search by brand name,

1. In the **Search** box, enter the name (or partial name) for which you wish to search.
2. Click **Search**. All brands matching your search are presented.

The Reports Tab

A variety of reports are available to assist in understanding, analyzing, and managing your Open Mobile user base.

iPass Data Collector

The iPass Data Collector system is a set of tools designed to monitor user connection experience, as well as model and measure the quality of critical nodes throughout the iPass global virtual network.

The Data Collector captures detailed status and usage information from every connection attempt (both successful and unsuccessful), and uploads this information to a central iPass database at regular intervals. It records and reports data about access points used, client configuration, error codes, connection speeds, time to authenticate, and other information critical to diagnosing network health and users' connection experience.

Real-time access to connection data enables iPass to:

- Gather detailed information about each user login experience.
- Measure and monitor the quality of hundreds of network providers to evaluate adherence to stringent service level goals.
- Measure actual service quality levels (not just averages) experienced by each customer during each network session.
- Locate and resolve access point problems before users experience failed connections
- Identify user training or help system improvements that will reduce user errors in the future.

Client ID

Client ID is a unique identifier that is issued to every instance of Open Mobile when it is installed. If Open Mobile were uninstalled and then re-installed, the new instance would receive a new client ID.

Reports List

There are nine reports available in three categories: User Connection Reports, End User Support Reports, and Mobile Broadband Management Reports.

User Connections Reports:

- **Connection Summary** displays successful and failed connections by connection type for a specific date range. See page 72.
- **Usage Summary** displays a summary of that data usage (in MB) of your users and your top ten users. See page 73.
- **Connection Data** enables you to export all connection data for a given date range. See page 75.

End User Support Reports:

- **User Activity** summarizes data useful for troubleshooting user connections. See page 78.
- **Exceptions** (report) displays users that are having the least success with the service for a specific date range. See page 79.
- **Devices & Platforms** displays current users, their operating systems, and client versions. See page 80.

Mobile Broadband Management Reports:

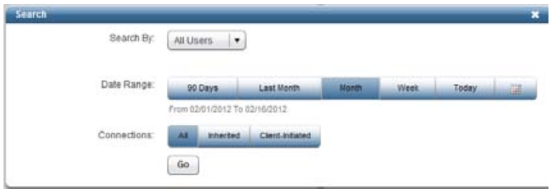
- **MBB Usage Rate** displays individual usage for three brackets: light, moderate, and heavy. See page 81.
- **Roaming by Country** displays any Mobile Broadband roaming usage by country. See page 83.

Connection Summary

The Connection Summary displays the connections by network type and the success rate by each network type.

Search

When you first arrive on the Connection Summary page, you will see a Search dialog box.



Search By: All Users

Date Range: Month

From 02/01/2012 To 02/16/2012

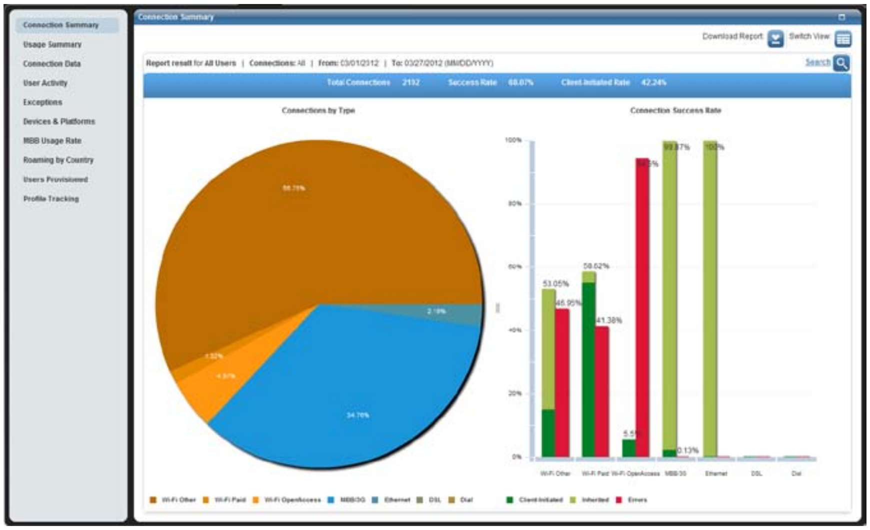
Connections: All

To initiate a Connection Summary report,

1. In the **Search By** dropdown menu, select one of the following:
   - **All Users** for a summary of all of your users
   - **User ID** for a summary of a specific user
   - **Profile ID** for a summary of users on a single profile
   - **Mobile No.** for a summary of a single mobile number
   - **Domain** for a summary of users on a specific domain
2. After **Date Range**, click one of the date ranges shown or click the calendar icon to enter a custom date range.
3. After **Connections**, click **All** (for all connections), **Inherited** (for a summary of only connections that Open Mobile inherited from the native connection client), or **Client-Initiated** (for a summary of only connection that Open Mobile initiated).
4. When you are finished, click **Go**. You can return to the Search dialog box by clicking on the **Search** icon in the top-right corner of the Connection Summary page.

Connection Summary Report

Connections by Type are displayed in a pie chart and the success rate by each network type is displayed in a bar graph. You can also view a table of the connections by network type and their rate of success by clicking the **Switch View** icon in the top-right corner.



Connection Summary

- Connection Summary
- Usage Summary
- Connection Data
- User Activity
- Exceptions
- Devices & Platforms
- MBB Usage Rate
- Roaming by Country
- Users Provisioned
- Profile Tracking

Download Report · Switch View

Report result for **All Users** | **Connections:** All | **From:** 03/01/2012 | **To:** 03/27/2012 (MM/DD/YYYY)

Search

Total Connections 2132 **Success Rate** 68.07% **Client-Initiated Rate** 42.24%

Connections by Type

Each network type is color coded and they include: MBB/3G (Mobile Broadband connections), Ethernet, DSL, Dial, and Wi-Fi (which is split into three types: Wi-Fi Paid for all paid iPass networks, Wi-Fi OpenAccess for all OpenAccess connections, and Wi-Fi Other for all other Wi-Fi connections).

Connection Success Rate

Each network type has two bars, green for success rate and red for the error rate. If All connections is selected in the search, the green (success) bar is split into two types of connections: dark green for client-initiated (connections initiated by the Open Mobile client) and light green for Inherited (connections inherited by Open Mobile from the native connection client).

Switch View

To drill down to the numbers, click the **Switch View** icon to see the Connections by Type table.

Connections by Type

The Connections by Type table has the following columns:

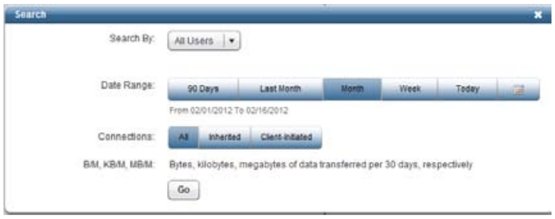
- **Connection Type** shows the network type (Wi-Fi Paid, Wi-Fi OpenAccess, Wi-Fi Other, MBB/3G or Mobile Broadband, Ethernet, DSL, and Dial)
- **Attempts** shows the total numbers of connection attempts
- **Client-Initiated** shows the total number of attempts made by Open Mobile (and not inherited from the native connection client)
- **Successes** shows the total number of successful connections
- **Errors** shows the total number of connections that failed due to an error
- **Success Rate** shows the percent of total attempts that were successfully connected

Usage Summary

The Usage Summary Report displays the total usage in megabytes per thirty days for your Open Mobile users. Data can be filtered by User ID or domain.

Search

When you first arrive on the Usage Summary page, you will see a Search dialog box.



Search ✕

Search By: All Users ▾

Date Range: 90 Days | Last Month | Month | Week | Today

From 02/01/2012 To 02/16/2012

Connections: All | Inherited | Client-Initiated

B/M, KB/M, MB/M: Bytes, kilobytes, megabytes of data transferred per 30 days, respectively

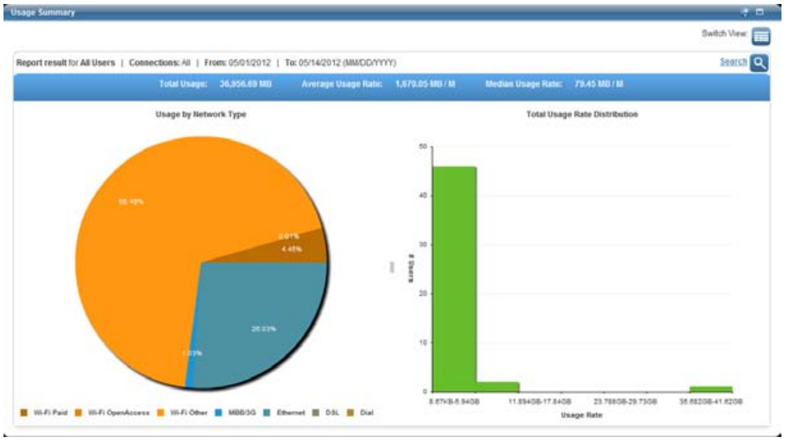
Go

To initiate a Usage Summary report,

1. In the Search **By** dropdown menu, select one of the following:
   - **All Users** for a summary of all of your users
   - **User ID** for a summary of a specific user
   - **Profile ID** for a summary of users on a single profile
   - **Domain** for a summary of users on a specific domain
2. After **Date Range**, click one of the date ranges shown or click the calendar icon to enter a custom date range.
3. After **Connections**, click **All** (for all connections), **Inherited** (for a summary of only connections that Open Mobile inherited from the native connection client), or **Client-Initiated** (for a summary of only connection that Open Mobile initiated).
4. When you are finished, click **Go**. You can return to the Search dialog box by clicking on the **Search** icon in the top-right corner of the Usage Summary page.

Usage Summary Report

Usage by network type is displayed in a pie chart and the total usage rate distribution is displayed in a bar graph. You can also view tables of the usage rate by network type and top ten users by clicking the **Switch View** icon in the top right corner



Usage Summary

Switch View:

Report result for **All Users** | **Connections:** All | **From:** 05/01/2012 | **To:** 05/14/2012 (MM/DD/YYYY)

Search

Total Usage: 36,956.69 MB **Average Usage Rate:** 1,670.05 MB / M **Median Usage Rate:** 79.45 MB / M

Usage by Network Type

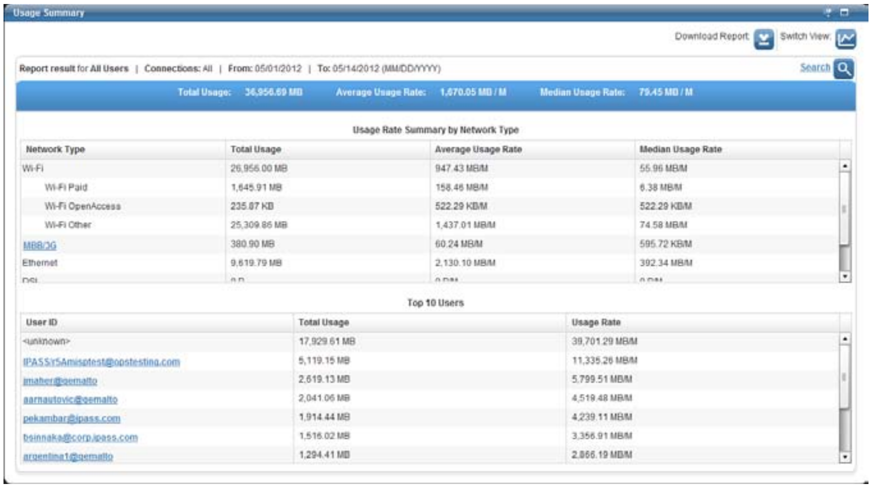
This pie chart shows the share of the total data usage by network type for the selected date range. The network types are Wi-Fi Paid (for all paid iPass network connections), Wi-Fi OpenAccess (for all OpenAccess or DeviceScape connections), Mobile Broadband (listed as MBB/3G), Ethernet, DSL, and Dial.

Total Usage Rate Distribution

This bar graph shows the distribution of users by their data usage during the selected date range.

Switch View

To view tables of the usage rate by network type and top ten users, click the **Switch View** icon.



Report result for All Users | Connections: All | From: 05/01/2012 | To: 05/14/2012 (MM/DD/YYYY)

Total Usage: 36,956.69 MB   Average Usage Rate: 1,670.05 MB / M   Median Usage Rate: 79.45 MB / M

Usage Rate Summary by Network Type

Network Type	Total Usage	Average Usage Rate	Median Usage Rate
Wi-Fi	26,956.00 MB	947.43 MB/M	55.96 MB/M
Wi-Fi Paid	1,645.91 MB	158.46 MB/M	6.38 MB/M
Wi-Fi OpenAccess	235.87 KB	522.29 KB/M	522.29 KB/M
Wi-Fi Other	25,309.86 MB	1,437.01 MB/M	74.58 MB/M
MBB/3G	380.90 MB	60.24 MB/M	595.72 KB/M
Ethernet	9,619.79 MB	2,130.10 MB/M	392.34 MB/M
DSL	0 B	0 B/M	0 B/M

Top 10 Users

User ID	Total Usage	Usage Rate
<unknown>	17,929.61 MB	39,701.29 MB/M
IPASS/r5Amisptest@opstesting.com	5,119.15 MB	11,335.26 MB/M
imaher@gemalto	2,619.13 MB	5,799.51 MB/M
aarnautovic@gemalto	2,041.06 MB	4,519.48 MB/M
pekambar@ipass.com	1,914.44 MB	4,239.11 MB/M
bsinnaka@corp.ipass.com	1,516.02 MB	3,356.91 MB/M
argentina1@gemalto	1,294.41 MB	2,866.19 MB/M

Usage Rate Summary by Network Type

This table shows the distribution of data usage over network types. Along with total usage, the table shows average and median data usage per thirty days. The network types are Wi-Fi Paid (for all paid iPass network connections), Wi-Fi OpenAccess (for all OpenAccess or DeviceScape connections), Mobile Broadband (listed as MBB/3G), Ethernet, DSL, and Dial. Clicking on MBB/3G will send you to the Mobile Broadband Usage Rate report.

Top 10 Users

This table lists the top ten users by total data usage in the date range selected. It also shows each user's average usage rate per thirty days (MB/M). You can open the User Activity report by clicking on a User ID.

Connection Data

Not a report per se, the Connection Data function enables you to export all connection data for a given date range. Using the calendar control, choose a period of 1-31 days, and then click **Download**. The data will be downloaded as a CSV file, which can then be viewed in any spreadsheet application.

The file contains the following columns:

- **Company:** Company ID number (assigned by iPass) that identifies each account
- **User ID:** Username identifying the user
- **Login String:** Full login string including prefix (where available)
- **Profile ID:** Profile ID number (assigned by the Open Mobile Portal) identifying the user's profile
- **Session ID:** Unique identifier for each connection
- **Start Time:** Timestamp of when the connection was initiated
- **Session Length:** Length of time in seconds for this connection (where available)
- **Authentication Time:** Length of time in seconds that it took to authenticate the user
- **Connection Type:** Type of media used for the connection. Possible results include*:

  - **Wi-Fi**
  - **Ethernet**
  - **MBB/3G** (Mobile Broadband)
  - **Dial**
- **Connection Status:** Whether the connection was successful (SUCCESS) or failed (FAIL).
- **Paid Network:** Whether the connection was over a paid network (Yes) or not (No).
- **Connection Status Code:** Numeric code that describes the connection. Possible results include*:
  - **0** for successful connection
  - **1** for failed connection
  - **-2** for lost connection to a GIS (iPass) network on an Android device
  - **50** for a successful connection on an Android device
  - **52** for a failure to log in to a DeviceScape network
  - **100** for a login failure (usually due to incorrect credentials)
  - **-103** for a connection cancelled by the user
  - **-105** for a failure to authenticate
  - **255** for a network failure
  - **717** for a network failure (no IP addresses available in the static IP address pool)
  - **14402** for an unexpected network failure
  - **14403** for an authentication failure or timeout
  - **14407** for a connection inherited from another client

    > *For a full list of possible Connection Status Codes, please see Online Reference article number 3468.*

- **Disconnect Code:** Numeric code that describes the reason for disconnection (where available). Possible results include*:
  - **0** for unknown reason
  - **1** for a user initiated disconnection
  - **2** for the firewall going down
  - **3** for the VPN not running
  - **4** for an idle timeout
  - **5** for a connection reaching the usage limit
  - **6** for a Windows logoff
  - **9** for the anti-virus application not running
  - **10** for a third-party application failure
  - **14** for disconnection on suspend
  - **15** for a disconnection on resume
  - **17** for a disconnection on Ethernet enforcement
  - **100** for a default disconnection reason
- **Client IP Address:** IP Address of the computer or device that made the connection (where available)

- **Downloaded Bytes:** Amount of data downloaded during this connection
- **Uploaded Bytes:** Amount of data uploaded during this connection
- **Cell ID:** Cell number of the Mobile Broadband device that made the connection (where available)
- **Roaming Status:** Whether or not the Mobile Broadband connection was on a roaming network (TRUE or FALSE)
- **Signal Strength:** Signal strength of the radio (as a percentage out of 100)
- **APN:** Access Point Name for Mobile Broadband connections (where available)
- **Country:** Country where the connection was made (where available)
- **IMEI:** International Mobile Equipment Identity for Mobile Broadband connections (where available)
- **IMSI:** International Mobile Subscriber Identity for Mobile Broadband connections (where available)
- **Network Name:** Name of the Mobile Broadband service provider
- **Network Type:** Communication network protocol for Mobile Broadband connections. Possible results include*:
  - **EVO**
  - **CDMA**
  - **EDGE**
  - **HSDPA**
  - **UMTS**
- **Client MAC Address:** MAC address of the device or computer making the connection
- **Access Point MAC Address:** MAC address of the network (where available)
- **SSID:** Service Set Identification or the name of the Wi-Fi network for this connection (where available)
- **Auth Method:** Wi-Fi method used to authenticate (where available). Possible results include*:
  - **GI** for GIS (iPass) Network
  - **DS** for DeviceScape Network
  - **OCR** for On Campus Roaming Network (802.1x)
- **Security Mode:** Numerical code identifying the security method for the Wi-Fi network (where available). Possible results include*:
  - **0** for None
  - **1** for WEP Open
  - **2** for WEP shared
  - **3** for WPA PSK TKIP
  - **4** for WPA PSK AES
  - **5** for WPA PSK TKIP 11i
  - **6** for WPA PSK AES 11i
  - **7** for WPA2
- **Access Procedure:** Procedure used to authenticate the user to this Wi-Fi network (where available).Possible results include*:
  - **GI** for a GIS (iPass) Network
  - **GC.1** for a GIS Captcha Network
  - **DS.1** for a DeviceScape Network

  - **TTLS-PAP**
  - **TTLS-MSCHAPV2**
  - **PEAP-GTC**
  - **PEAP-MSCHAPV2**
  - **FAST-GTC**
- **Network ID:** Number identifying a network configured in a directory (where available)
- **Service Name:** Name of the Service Provider for DSL connections (where available)

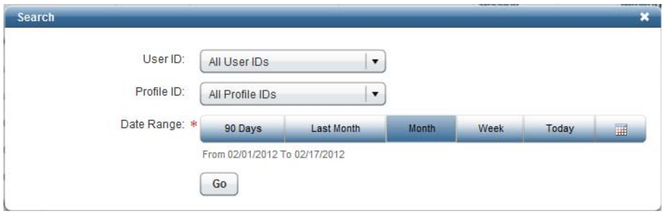
*Lists of codes and results may not include all possible values.

User Activity

The User Activity report shows data on user activity within the specified date range. This information can be useful when attempting to troubleshoot a user's connectivity issues.

Search

When you first arrive on the User Activity page, you will see a Search dialog box.



User ID: All User IDs

Profile ID: All Profile IDs

Date Range: * Month

From 02/01/2012 To 02/17/2012

To initiate a User Activity report,

1. In the User ID dropdown menu, select one of the following:
   - **All User IDs** for all of your users.
   - **Specify User ID** for a specific user.
2. In the Profile ID dropdown menu, select one of the following:
   - **All Profile IDs** for all of your profiles.
   - **Specify Profile ID** for a specific profile.
3. After **Date Range**, click one of the date ranges shown or click the calendar icon to enter a custom date range.
4. When you are finished, click **Go**. You can return to the Search dialog box by clicking on the **Search** icon in the top-right corner of the User Activity page.

User Activity

This table will show all user activity over the date range that you chose and it contains the following columns:

- **User ID** identifies each user.
- **OS** is the Operating System on which the client is installed.
- **Platform** is the version of the client.
- **Start Time** is this session's start time.
- **Session Length** is the length of this session.
- **Status** lists if the connection was a success or error.

- **Paid Network** is whether the connection was over a paid network (Yes) or not (No).
- **Network Type** is the type of network for this connection (Wi-Fi, Mobile Broadband, Ethernet, etc).
- **Network** is the network that provided the connection (if applicable).
- **Region** is the region of the network directory (if applicable).

> *The region will not necessarily show the location of the connection, especially if the user connects to a network with an SSID that is in multiple directories.*

- **Profile** is the Profile ID and Profile Name.
- **Uploaded KB** is the amount of data in kilobytes that were uploaded in this session.
- **Downloaded KB** is the amount of data in kilobytes that were downloaded in this session.
- **Status Code** is the status code reported by the client.
- **Message** is the message for the status code reported by the client.
- **Inherited/Initiated** shows if the connection was initiated by the Open Mobile client or inherited from another connection client.
- **Access Procedure** shows the security type for the network (if applicable).
- **VPN Drilldown** will show a **VPN Info** link with information on the VPN connection (if applicable).

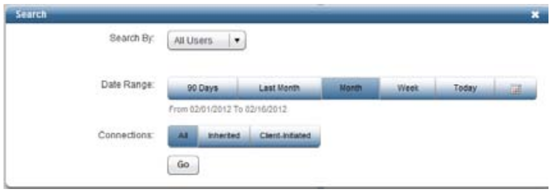
You can click the **Download Report** icon in the top-right corner to download an Excel spreadsheet of this table.

Exceptions

This report displays users that are having the least success with the service for a specific date range.

Search

When you first arrive on the Exception page, you will see a Search dialog box.



Search By: All Users

Date Range: Month

From 02/01/2012 To 02/16/2012

Connections: All

To initiate an Exceptions report,

1. In the **Search By** dropdown menu, select one of the following:
   - **All Users** for all of your users
   - **User ID** for a specific user
   - **Domain** for a specific domain
2. After **Date Range**, click one of the date ranges shown or click the calendar icon to enter a custom date range.
3. After **Connections**, click **All** (for all connections), **Inherited** (for a summary of only connections that Open Mobile inherited from the native connection client), or **Client-Initiated** (for a summary of only connection that Open Mobile initiated).
4. When you are finished, click **Go**. You can return to the Search dialog box by clicking on the **Search** icon in the top-right corner of the Exceptions page.

Exceptions

This table will show the users with the least success over the date range that you chose and it contains the following columns:

- **User ID** identifies each user, click on the link to see this user's recent activity. You can open the User Activity report by clicking on a User ID.
- **Error Rate** is the percent of connections in the selected date range that resulted in error for this user during the selected date range.
- **Connection Attempts** is the total number of connection attempts by this user in the selected date range.
- **Errors** is the total number of connections that resulted in error for this user during the selected date range.
- **Successes** is the total number of successful connections for this user during the selected date range.

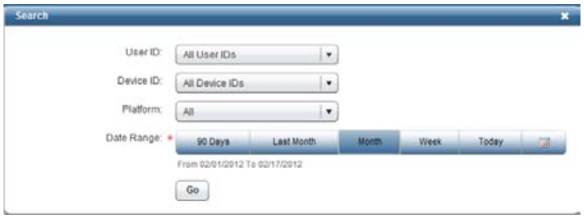
You can click the **Download Report** icon in the top-right corner to download a CSV file of this table.

Devices and Platforms

This report displays two pie charts showing the distribution of your client by Operating Systems and client versions, and if you click Switch View you can see a table showing more details of your user's devices.

Search

When you first arrive on the Devices and Platforms page, you will see a Search dialog box.



Search

User ID: All User IDs

Device ID: All Device IDs

Platform: All

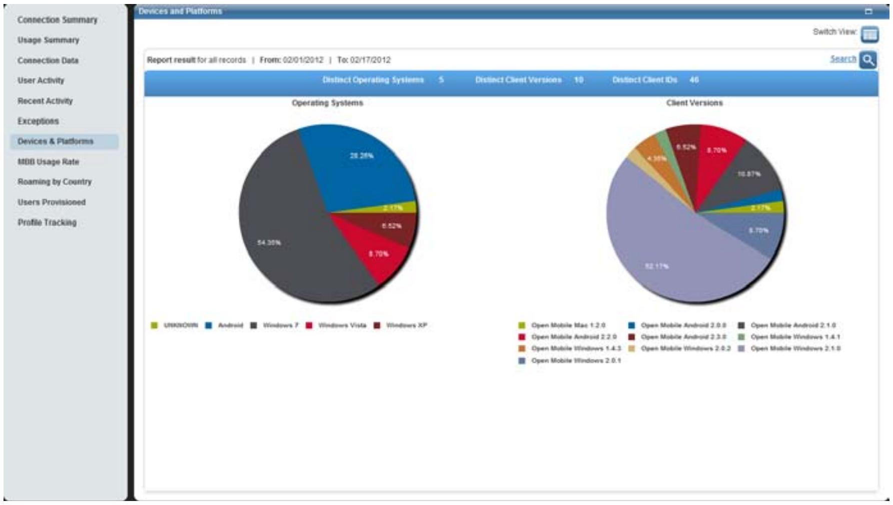
Date Range: * Month

From 02/01/2012 To 02/17/2012

To initiate a Devices and Platforms report,

1. In the **User ID** dropdown menu, select one of the following:
   - **All User IDs** for all of your users.
   - **Specify User ID** for a specific user.
2. In the **Device ID** dropdown menu, select one of the following:
   - **All Device IDs** for all devices.
   - **Specify Device ID** for a specific device ID.
3. In the Platform dropdown menu, select **All** or a specific Operating System.
4. After **Date Range**, click one of the date ranges shown or click the calendar icon to enter a custom date range.
5. When you are finished, click **Go**. You can return to the Search dialog box by clicking on the **Search** icon in the top-right corner of the Device and Platforms page.

Operating System and Client Version



Report result for all records | **From:** 02/01/2012 | **To:** 02/17/2012

Distinct Operating Systems 5 Distinct Client Versions 10 Distinct Client IDs 46

These pie charts show what percent of your users are on each applicable Operating System and Client Version respectively.

Switch View

By clicking the **Switch View** icon you can see these details in a table.

Device User Summary

This table will show of your user's devices over the date range that you chose and it contains the following columns:

- **User ID** identifies each user. You can open the User Activity report by clicking on a User ID.
- **Client Version** is the version of the client installed.
- **OS** is the Operating System on which the client is installed.
- **Client ID** identifies each installed client.
- **MBB Device Model** is the Mobile Broadband device model (if applicable).
- **MBB Device ID** is the Mobile Broadband device ID (if applicable).
- **MBB Manufacturer** is the Mobile Broadband device manufacturer (if applicable).
- **MBB Driver Version** is the Mobile Broadband device driver (if applicable).
- **MBB Firmware Version** is the Mobile Broadband firmware (if applicable).

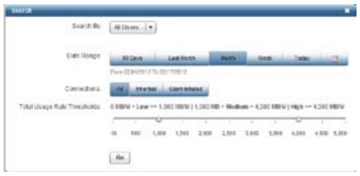
You can click the **Download Report** icon in the top-right corner to download a CSV file of this table.

Mobile Broadband Usage Rate

The Mobile Broadband Usage Rate shows Mobile Broadband data usage.

Search

When you first arrive on the Mobile Broadband Usage page, you will see a Search dialog box.



Search By: All Users

Date Range: Month

From 02/01/2012 To 02/17/2012

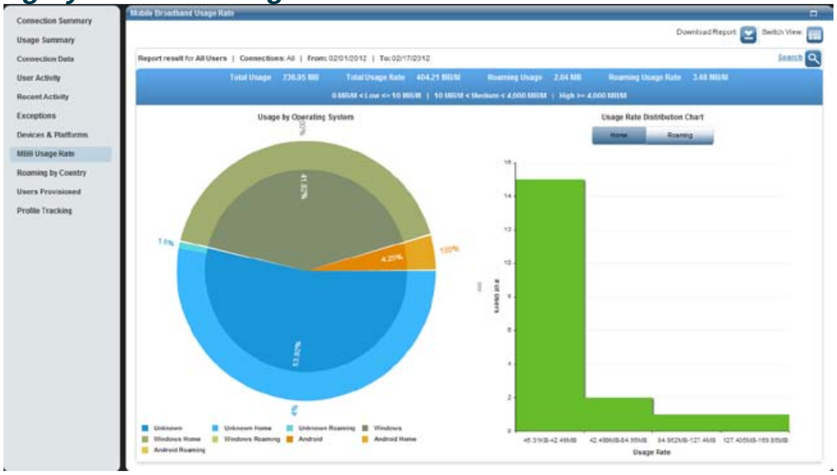
Connections: All

Total Usage Rate Thresholds: 0 MB/M < Low <= 1,000 MB/M | 1,000 MB < Medium < 4,000 MB/M | High >= 4,000 MB/M

To initiate a Mobile Broadband Usage Rate report,

1. In the **Search By** dropdown menu, select one of the following:
   - **All Users** for all of your users
   - **User ID** for a specific user
   - **Profile ID** for a specific profile.
   - **Domain** for a specific domain.
2. After **Date Range**, click one of the date ranges shown or click the calendar icon to enter a custom date range.
3. After **Connections**, click **All** (for all connections), **Inherited** (for a summary of only connections that Open Mobile inherited from the native connection client), or **Client-Initiated** (for a summary of only connection that Open Mobile initiated).
4. Under **Total Usage Rate Thresholds**, select the range of data usage in megabytes that you would like to view. Changing the range will automatically adjust the definition of low, medium, and high usage.
5. When you are finished, click **Go**. You can return to the Search dialog box by clicking on the **Search** icon in the top-right corner of the Exceptions page.

Usage by Operating System and Usage Rate Distribution Chart



Report result for All Users | Connections: All | From: 02/01/2012 | To: 02/17/2012

Total Usage 236.95 MB Total Usage Rate 404.21 MB/M Roaming Usage 2.04 MB Roaming Usage Rate 3.48 MB/M

0 MB/M < Low <= 10 MB/M | 10 MB/M < Medium < 4,000 MB/M | High >= 4,000 MB/M

The Operating System pie chart shows what percent of your users are on Windows, Android, or Mac. Within each operating system, you can view what percentage of your users were Roaming.

The Usage Rate Distribution pie chart shows the distribution of users for the date range and usage range you selected. By clicking the **Home** or **Roaming** button you can see this data usage on home networks or roaming networks respectively.

Switch View

By clicking the **Switch View** icon you can see these details in a table.

Mobile Broadband Usage Table

This table will show of your user's devices over the date range that you chose and it contains the following columns:

- **User ID** identifies each user, click the link to see this user's recent activity.
- **Home Usage** is the total data used in the home network for the selected date range.

- **Home Usage Rate** is the rate of data usage in the home network per thirty days.
- **Roaming Usage** is the total data used in roaming networks for the selected date range.
- **Roaming Usage Rate** is the rate of data usage in roaming networks per thirty days.
- **Total Usage** is the total Mobile Broadband data used for the selected date range.
- **Total Usage Threshold** defines the usage as low, medium, or high depending on the total usage rate threshold you selected.

You can click the **Download Report** icon in the top-right corner to download a CSV file of this table.

Roaming by Country

The Mobile Broadband Roaming by Country report summarizes data usage by country. A summary at the top of the table shows the total data usage (in megabytes) , total roaming users, total roaming usage (in megabytes), and the percent of roaming usage for the selected time range. A table displays each country, the number of users in that country, and the data usage in that country (in megabytes) for the selected date range. Click the **Customize Report** button at the top of the screen to change the date range (once the date range has been selected click **Go**).

The Account Tab

Use this tab to manage the details of your iPass Open Mobile account.

Company Address

You can view and edit your company's corporate and billing addresses on file with iPass.

To edit a corporate or billing address,

1. Under the corresponding address, click **Edit**.
2. Enter the information in the requested fields.
3. Click **Save**.

Company Contacts

You can view and edit your company contacts on file with iPass. Contacts are classified by type, which includes Business, Technical, Corporate, or Other.

The **Contacts** list displays all company contacts. Click **Expand All** to show the list in more detail.

To add a new contact,

1. Click Add New Contact.
2. Enter the requested personal information for the contact.
3. Select one or more **Type** for the contact.
4. Indicate which e-mail notifications the contact will receive: Hourly Abuse Report and Daily URA Alerts Report.

To edit or delete an existing contact,

1. In the **Contacts** list, click **Expand All**, and then select the contact you wish to edit.
2. Click **Manage**.
3. Do one of the following:
   - Edit the details of the contact as needed, and then click **Save**.
   - To delete the contact, click **Delete this Contact**.

Manage Administrators

On the **Manage Administrators** page, you manage all of your Open Mobile Portal administrator accounts. You can add new administrator accounts individually, or import a list of administrators from a properly formatted XML file. After you have added an Administrator, in the action column next to their name:

- Click **View** to see (but not edit) the Administrator's information.
- Click **Edit** to change the Administrator's information.
- Click **Delete** to delete the Administrator (if available).

- Click **Manage Assigned Roles** to change the Administrator's assigned roles.

To add a new Admin:

1. Click **Add**.

> *If you switched to a Child Company with Hosted Authentication allowed (see page 92), the first entry you will see is **Admin Type**. Select **Admin** (for Administrators with credentials hosted on their own servers) or **Hosted Admin** (for Administrators with credentials hosted by iPass).*

2. Optionally, in **Company ID**, enter the company ID of the user's company.
3. Enter the **Username**, which must be the roaming username (the username used to log in to Open Mobile with the domain included). If this is a Hosted Admin, the domain is already included in the field (and should not be added).
4. Enter the user name's first name, last name and email address.
5. Optionally, enter the Contracts Employee ID (the employee ID of the Account Manager specified in the Contract Database).
6. Under **Roles**, using the arrow keys, assign roles to the user by moving one or more roles from the **Unassigned Roles** to the **Assigned Roles** column.
7. Click **Save**.

Adding Multiple Users

Multiple user accounts can be imported from an XML file. A user file must include each user's first name, last name, user name, and email address. An example is shown here, containing two new users: Jane Smith and Jessica Wood:

```
<users>
 <user>
       <fname>Jane</fname>
       <lname>Smith</lname>
       <username>jsmith123@example.com</username>
       <email>jsmith@example.com</email>
 </user>
 <user>
       <fname>Jessica</fname>
       <lname>Wood</lname>
       <username>jwood123@example.com</username>
       <email>jwood@example.com</email>
 </user>
</users>
```

To import multiple users,

1. Create and save your user import XML file.

2. Click Import Users.
3. In **User File**, click **Browse**, and select the XML file containing the user accounts.
4. Click Upload File.

Manage Roles

You manage access to the Open Mobile Portal by assigning *roles* to your users. A role is comprised of privileges enabling the performance of tasks or granting access to information. For example, a role called *Service Rep* could include privileges to grant access to sections of the Open Mobile Portal that includes Customer Care-related information. Any users with that role would have all the privileges included in the role.

The Open Mobile Portal includes several pre-defined roles, and, in addition, you can create your own.

Administering Roles

When iPass provisions Portal accounts, the User Admin role enables you to assign roles to other users. You should use the User Admin role to create other roles for your organization as needed, and then assign users to the new roles. You can use the roles included in the User Admin role, or create other roles to fit your needs.

Parent-Child Roles

Roles can be defined as children of other roles. A role that is a child of another role will inherit all the privileges of its parent role, as well as including additional privileges unique to that role. A user assigned to the child role will have all of the privileges of the child role, as well as all the privileges of any roles that are its parents.

To define a role as the parent of another role, assign the role just as you would assign privileges to the role.

> *For example, Role A includes two child roles: Role B and Role C. Any users assigned to Role B will have all the privileges of Roles A and B, but not of Role C.*

A role can have any number of parents and any number of children. However, a role that is the parent of another role may not also be defined as the child of the same role.

Privileges

Roles are comprised of privileges, which enable access to specific tasks or views in the Open Mobile Portal. Privileges always enable, and never disable, access. For example, users in a role with Privileges A and B can perform tasks A and B. A privilege will never prevent a user from performing a task, or cancel other privileges.

Privileges cannot be assigned directly to users. Instead, privileges are included in roles, which are then assigned to users.

The scope of a privilege defines its domain of influence over users in parent and child companies. A privilege prefixed by a caret (^) can affect other users in the same company or any of your child companies.

Managing Roles

To create a new role,

1. Click **Create New Role**.
2. In **Role Name**, enter the name of the role.

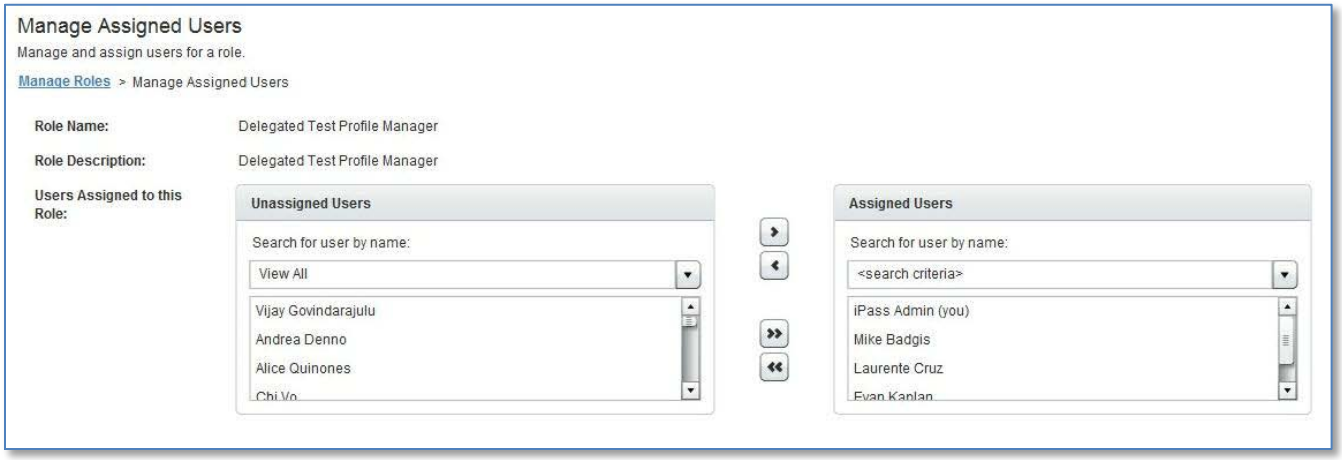
3. In **Role Description,** enter the description of the role.
4. Under **Assigned Roles and Privileges**, click **Expand All** to view all roles and the privileges currently assigned to each role.
5. Select one or more roles and privileges from the list, and then click the right arrow to move your selections to the **Selected Roles** list. (You can click **View Assigned Privileges** to view a summary of the current privileges assigned to the role.)

   > *Assigning a role to another role will include all the assigned role's privileges in the second role, and will make the new role into a child of the assigned role. For example, if Role A were assigned to Role B, then Role B would include all the privileges of Role A, and Role B would be a child of Role A. In addition, you could add additional privileges to Role B beside the ones included in Role A, or even add other roles.*

6. Using the arrow controls, continue selecting roles and privileges until the new role is complete.
7. Click **Save**.

To manage the users assigned to a role,

1. On the **Mange Roles** list, select the role you want to assign users to, and then select **Manage Assigned Users** from the dropdown menu**.**
2. Under **Unassigned Users**, select a user to assign to the role. (Under **Search for user by name**, you can view all users or enter a search criterion to filter the entire list of users. For example, you could search for all users named James.)
3. Using the right arrow, move your selected users from the **Unassigned Users** column to the **Assigned Users** column.
4. Using the arrow controls, repeat steps 2 and 3 until you have you have assigned (or unassigned) all desired users to the role.
5. Click **Save.**



Manage Assigned Users

Manage and assign users for a role.

Manage Roles > Manage Assigned Users

Role Name: Delegated Test Profile Manager

Role Description: Delegated Test Profile Manager

Users Assigned to this Role:

Unassigned Users

Search for user by name: View All

Vijay Govindarajulu
Andrea Denno
Alice Quinones
Chi Vo

Assigned Users

Search for user by name: <search criteria>

iPass Admin (you)
Mike Badgis
Laurente Cruz
Evan Kaplan

To edit an existing role,

1. On the **Roles** list, select the role you want to edit, and then click **Edit**.

2. Edit the role as needed.
3. Click **Save**.

To delete a role,

1. On the **Roles** list, select the role you want to delete, and then click **View**.

   > *Always exercise caution when deleting roles. Make sure that when you delete a role that its privileges are not unique to the role, or deleting it may make some privileges unavailable to anyone else.*

2. Click **Delete This Role**.
3. Click **OK** to confirm deletion.

Managing Customer Roles

In addition to assigning customers to roles, roles can be assigned to customers.

To manage a customer's roles,

1. Click **Manage Customer Roles**.
2. From the list of customers, select the customer for which you wish to manage roles. (You can search for customer by Customer ID by entering the customer's ID in the search box and clicking **Search**.)
3. Under **Actions**, click **Manage**. The Assigned Roles list shows all roles currently assigned to the selected customer.
4. Click **Manage Assigned Roles**.
5. Under **Available Roles**, select a role to assign to the customer.
6. Using the right arrow, move your selected role from the **Available Roles** column to the **Assigned Roles** column.
7. Using the arrow controls, repeat steps 2 and 3 until you have you have assigned all desired roles to the customer.
8. Click **Save**.

Invoices and Payments

The **Invoices and Payments** section enables you to view the financial details of your iPass account.

Invoice History

The **Invoice History** page displays all invoices or vouchers with iPass. By default, the page displays invoices and vouchers for the current month, but you can use the calendar control to specify a date range.

Invoices and vouchers can be sorted by date, number, due date, and amount.

To view the details of an individual invoice or voucher, under **Actions**, click **View Details.**

Aging Balance

The **Aging Balance** page displays any unpaid balance with iPass. The current balance is shown, as well as for the last 30, 60, 90, and 120 days.

Aging balance can be sorted by invoice date, invoice number, unpaid balance, and debit.

To view the details of a particular balance item, under **Actions**, click **View Details.**

Payment History

The **Payment History** page displays your payment history with iPass. By default, the page displays the payment history for the current month, but you can use the calendar control to specify a date range.

Payment history can be sorted by check date, check number, type, status, and amount.

To view the details of an individual check, under **Actions**, click **View Details.**

Payment Methods

The **Payment Methods** page displays the methods that you can use to make a payment to iPass: credit card, check, or wire transfer.

Manage Portal Brands

If enabled for your company, you can create a customized look and feel for the Portal.

Branding the Portal

You can create and then publish a brand for your Open Mobile Portal users. A Portal brand consists of these elements:

- The brand name.
- Your corporate logo.
- (Carrier customers only) Optional Custom Dashboard content. Carrier customers can replace the Portal Dashboard with their own content, if desired.

Portal Brand Elements	Specification
Brand Name	
Brand Name	Alphanumeric string, max 35 characters. Required.
Settings	
Corporate Logo	115px (w) x 25px (h), PNG format, and 5 KB file size. Required.
Dashboard Title	Alphanumeric String
Dashboard Content	Valid XML file (see page 90)

An interactive Image Map shows a live preview of your brand as you create it.

Customizing the Portal Dashboard

As part of Portal branding, carrier customers can customize the appearance of the Portal Dashboard with their own title and content. Typically, a custom Dashboard consists of news, company information, and useful links to external sites.

By default, the Dashboard consists of three tabs: **Getting Started, Training,** and **What's New.** If you choose to replace the Dashboard with your own content, these three tabs will be replaced with a *single* tab displaying your content.

Your content must be uploaded in a properly constructed XML file. You can download a sample XML file from the Portal branding page that illustrates the correct XML format.

Custom Dashboard XML

All content in the <MainPanel> node must be tagged with one or more of the following tags:

Tag	Description	Attributes
<Text>	Standard text. Width fixed at 100%.	■ **wordwrap**: (required) 'true' or 'false' (required) default = true ■ **style**: (optional) 'normal or 'heading' (default = normal)
<Break>	Line break. Can specify exact height spacing in pixels	■ **height :** (optional) vertical spacing in pixels (default = 10px)
<Hyperlink>	Standard anchor tag for links (will always launch link in external window).	■ **href:** (required) URL such as 'http://www.ipass.com'
<Section>	A container to group components with custom alignment and formatting.	■ **align:** (required) 'horizontal' or 'vertical' (default = vertical) ■ **paddingLeft:** (optional) left margin for section, in pixels (default = 0px) ■ **paddingRight :** (optional) right margin for section, in pixels (default = 0px)

Any of these tags can be used multiple times, to create as many of the appropriate elements as needed.

Use the **Preview** buttons to display a preview your custom content. This enables you to view the results of your XML and then revise as needed.

Creating and Editing a Portal Brand

To create a new Portal brand,

1. Click **Manage Portal Brands**.
2. Click **Create a Brand**.
3. On the **Brand Name** tab, enter a new brand name.
4. Click the **Settings** tab.
5. Under Logo, click **Browse** to your corporate logo image and select it. (In the interactive Image Map, above the tabs, each element is labeled. You can see the effect your branding will have on the appearance of the Portal.)
6. If desired, in **Dashboard Title,** enter the name of your custom Dashboard. In Dashboard Content, click **Browse** to browse to your Dashboard content file.

> *Click **Preview** to preview how the Dashboard content will be displayed. If you need to make changes, edit the content, upload it again, and preview the new content as needed.*

7. Select **Show Tickets Panel** to display the **Tickets** panel.
8. Select **Show Service Alerts** to display the **Service Alerts** panel.
9. Click **Save**.

Once created, you must activate the brand to make it visible to your Portal users.

To edit an existing Portal brand,

1. From the **List of Brands**, select the brand you wish to edit.
2. In the **Actions** column, click **Edit**.
3. Edit the brand as desired.
4. When complete, click **Save**.

Activating a Portal Brand

An activated brand will be visible to your Portal users. You can only have one brand active at a time.

To activate a Portal brand,

1. From the **List of Brands**, select the brand you wish to activate.
2. In the **Actions** column, click **Set as My Active**.
3. On the **Activate Portal Brand** page, click **Set as Active**.
4. Click **Yes** to confirm activation.

> *An active brand can be deactivated by selecting another brand to be your active one.*

Setting the Default Brand for Child Companies

You can set a published Portal brand as the default your child companies. When users from the child companies log into the Portal, the brand will be displayed.

To set a Portal brand as the default for your child companies,

1. From the **List of Brands**, select the brand you wish to activate.
2. In the **Actions** column, click **Set as Child Default**.
3. On the **Set as Child Default Brand** page, click **Set Child Default**.
4. Click **Yes** to confirm.

Portal Preferences

Localization

You can change the language displayed in the Reports tab by selecting English or French in the dropdown menu and then clicking **Save**. You have to log out and log in to see the changes.

Online Help

Check the box to show page-level help icons. Portal users can click on these icons to open a help window, with content from this guide, in their browser. Uncheck the box to prevent the icons from appearing—you may want to suppress the help icons if you need a branded, white-labeled, or customized version of the help.

Account Settings

Hosted Authentication

If hosted authentication is available to your account and you switched to a Child Company, you can allow Hosted Authentication by checking the box next to **Allow Hosted Authentication**.