

HP Anywhere

For the Windows® operating system

Software Version: 9.1

Administrator Guide

Document Release Date: August 2012

Software Release Date: August 2012



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

<http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Administrator Guide	1
Contents	5
Welcome to This Guide	7
Overview	8
HP Anywhere Architecture	9
Mini Apps	9
Implementation Workflow	10
Mobile Client	11
Home	12
Front Page	12
Settings	13
Catalog	14
Authorization Roles	15
Assign HP Anywhere Roles to LDAP Users	15
Administrator Console	17
Log into the Administrator Console	17
Administrator Console Tabs	18
Mini Apps	18
View Installed Mini Apps	18
View Mini App Details	19
Install a Mini App	21
Catalog	21
Data Source	21
Personas	22
Settings	22
Alerts and Push Notifications	24
Configure Push Notifications for iOS Devices (Apple)	24
Configure Push Notifications for Android Devices (Google)	26
Troubleshooting Push Notifications	27

Apple	27
Android	27
Changing Default Ports in HP Anywhere	28
Additional Port Configuration Changes	30
Opening Ports in a Firewall	30
Mobile Client Configuration	32
HP Anywhere Server URL	32
iOS Developer Certificate	32
Android Keystore	33
Artifacts to Send to the HP Anywhere Support Team	33
Deploy the WAR File and Publish the Client URL	34
End User Alerts	35
Alert Rules	35
Follow Items	36

Welcome to This Guide

This guide explains how to set up the HP Anywhere server, enabling the administrator to download mini apps to the end user's mobile devices.

It also provides a detailed explanation of the HP Anywhere Administrator Console.

Chapter 1

Overview

HP Anywhere is a multi-platform application for distributing and consuming IT Management information and operations on mobile devices (smartphones and tablets) on different platforms, such as iOS and Android. HP Anywhere allows you to mobilize HP Software products that you are familiar with, in new ways.

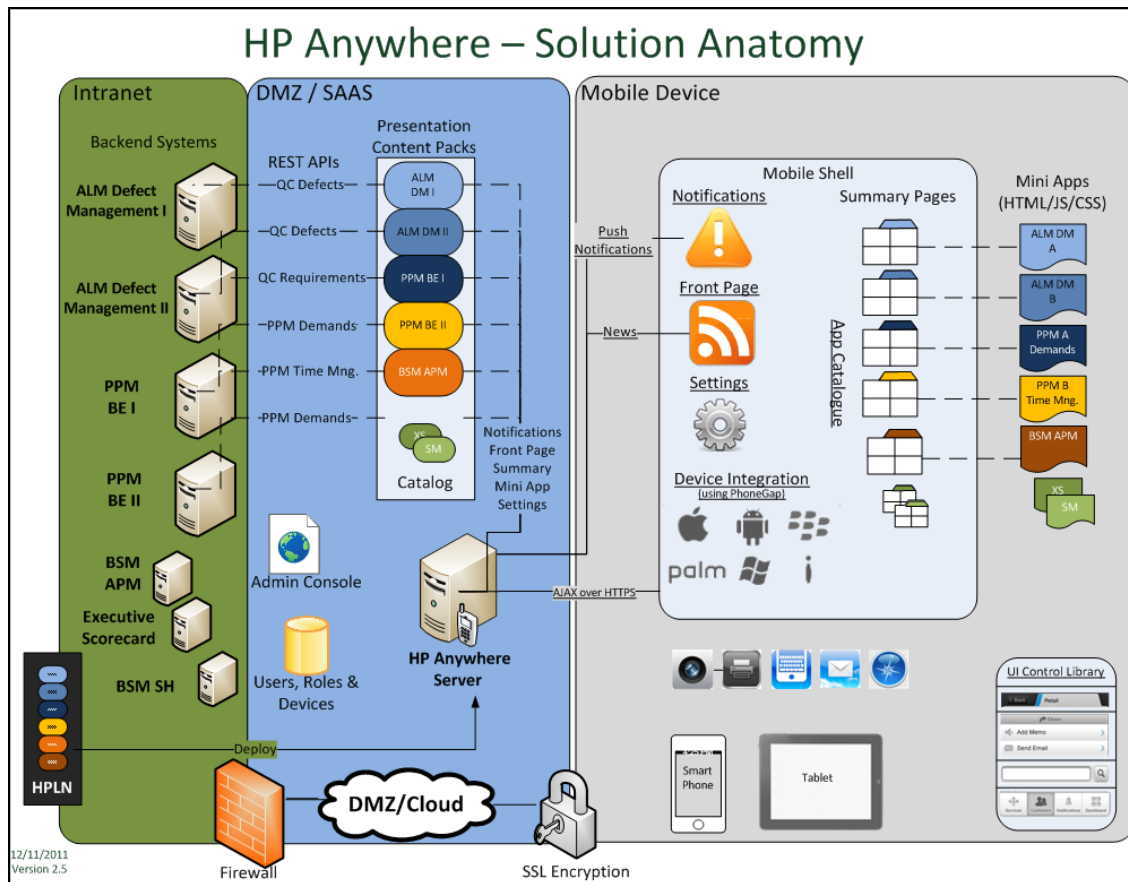
HP Anywhere is comprised of three components:

- **HP Anywhere Server:** Provides the platform for connecting to the mini app versions of your IT Management Systems
- **HP Anywhere Client:** The mobile application that is distributed and installed on the end user devices. Via the client, the end user connects to the HP Anywhere server and retrieves data of the relevant mini apps.
- **Mini Apps:** Applications that are downloaded to the end user devices at runtime via the mobile client application. These applications provide interface to specific IT Management tasks or modules.

HP Anywhere provides a hybrid solution - mini apps are built once and can be run on multiple platforms with all the advantages of the native application.

HP Anywhere Architecture

The following diagram provides an overview of the HP Anywhere architecture.



The HP Anywhere Architecture is comprised of three areas:

- **Backend Servers** - Provides the data of each mini app.
- **HP Anywhere Server** - Provides the platform for connecting to the mini apps.
- **Mini Apps** - Divided into two areas:
 - Client side - The interface that the end user sees on their mobile device
 - Server side - The interface that act as a proxy between the mobile device and backend:

Mini Apps

The administrator is responsible for downloading the mini apps from HPLN and making them available to the end user. The end user can then install the mini app onto their HP Anywhere mobile client .

Examples of currently available mini apps are:

- HP ALM Defect Management for Smartphone
- HP Executive Scorecard for Smartphone
- HP Executive Scorecard for Tablet
- HP ITFM Finance Management
- HP PPM Demand Management for Smartphone
- HP BSM Service Health for Smartphone
- HP BSM Application Performance Management for Smartphone

See the Support Matrix at <http://support.openview.hp.com/selfsolve/manuals> for the latest supported versions of each mini app and its corresponding backend application.

Implementation Workflow

This section presents the steps to be performed in order to implement HP Anywhere. The scenario includes three roles: Mini App Developer, Administrator, and End User.

1. **Mini App Developer:** Develop the mini app and upload it to a cloud service named HP Live Network (HPLN).
2. **Administrator:** Install the mini apps from HPLN and enable them from the Administrator Console. After the mini apps are installed and enabled, the end user can see them on the mobile device. The administrator chooses the mini apps according to the end user's role. The mini apps are presented on the end user mobile device based on the persona selected by the end user during registration to the HP Anywhere application.
3. **End User:** Download the HP Anywhere client from the provided link and log into HP Anywhere on the mobile device. The end user can select additional mini apps from the catalog.

The following diagram shows the interface between the HP Anywhere Client, Server and the mini apps:



HP Anywhere supports a single sign-on mechanism, authenticating the user once only, and then ensuring that authorization definitions are carried over to all the mobile access use cases.

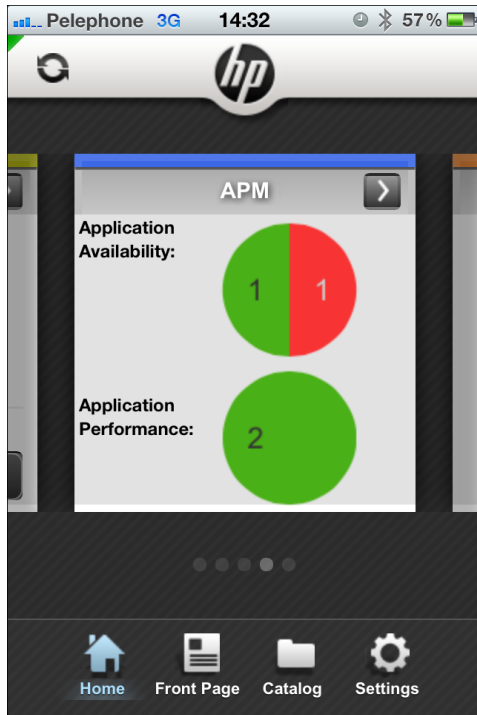
Mobile Client

The mobile client consists of the following sections:

- "Home" on next page
- "Front Page " on next page
- "Settings" on page 13
- "Catalog" on page 14

Home

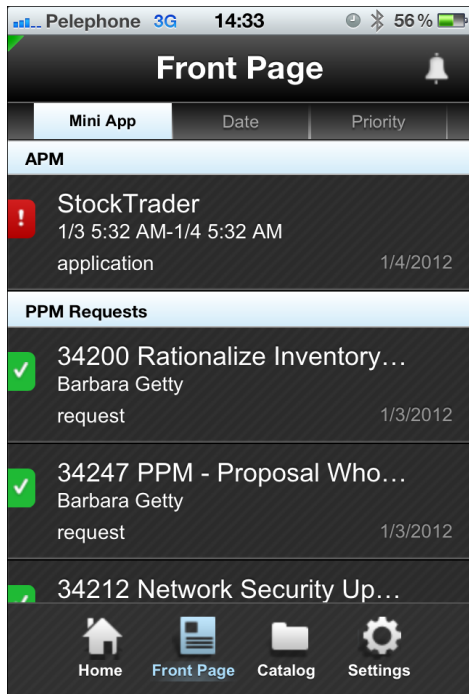
The Home Page presents an aggregated view of activity for each mini app. This view provides enough information at a glance to make quick decisions and decide whether or not to drill down further.



Front Page

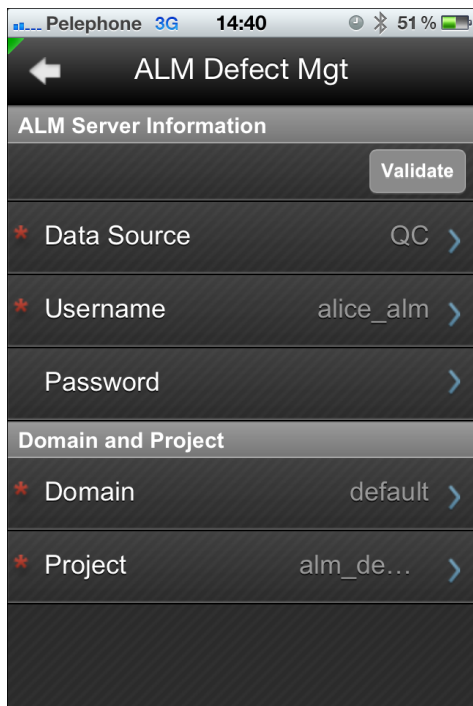
The Front Page shows important items from the different mini apps installed on the mobile device. These items can be sorted according to mini app, date and priority.

Any alerts that have occurred are shown on the Front Page. From the Front Page view, the end user can drill down directly to the point in a mini app where an action can take place.



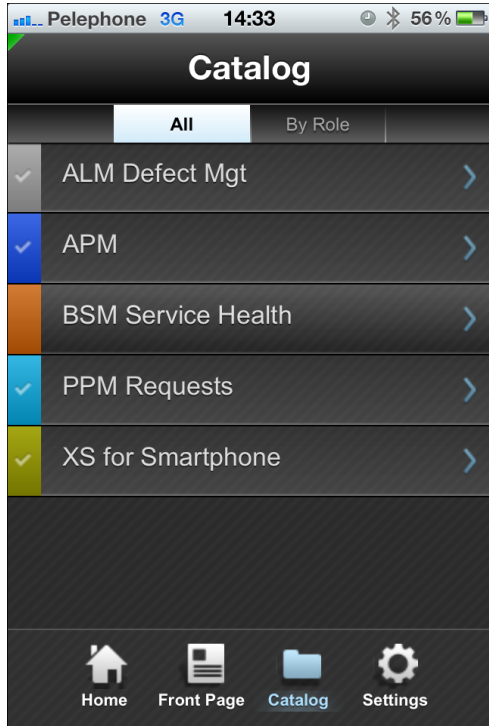
Settings

In the Settings Page, the end user can change the specific settings of each mini app.



Catalog

In the Catalog Page, the end user can select the mini apps to install/uninstall on the mobile device in addition to the default mini apps provided according to his/her role.



Chapter 2

Authorization Roles

HP Anywhere implements three types of user roles:

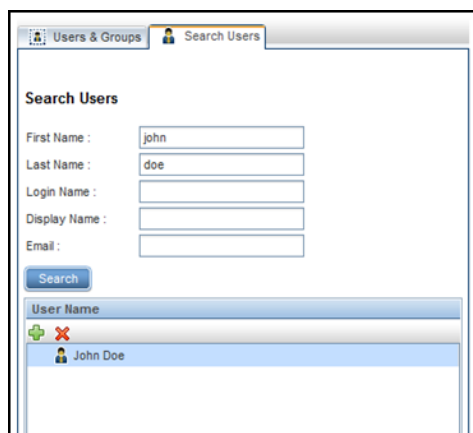
- **Admin:** For logging in to the "Administrator Console" on page 17.
- **BSF_Admin_Role:** Users with the role BSF_Admin_Role are permitted to login to the User Management UI to manage users and assign roles to them.
- **Tester:** Users with the role Tester can test new mini apps. When a new mini app is installed, all the services it contains are disabled by default. A user with tester role can test these new services before the Admin user enables them.

Assign HP Anywhere Roles to LDAP Users

After HP Anywhere has been installed, only a single user exists with the name 'admin' and role 'Admin'.

After configuring the LDAP staging environment, you need to map real LDAP users to HP Anywhere authorization roles as follows:

1. Open the User Management UI: **http://<url>:<port>/bsf**.
2. Log into AUM (BSF) using your temporary admin user (name: **admin**) with the password that the administrator configured during the post-installation.
3. Select the **User Management** tab.
4. Then, select the **Search Users** tab.



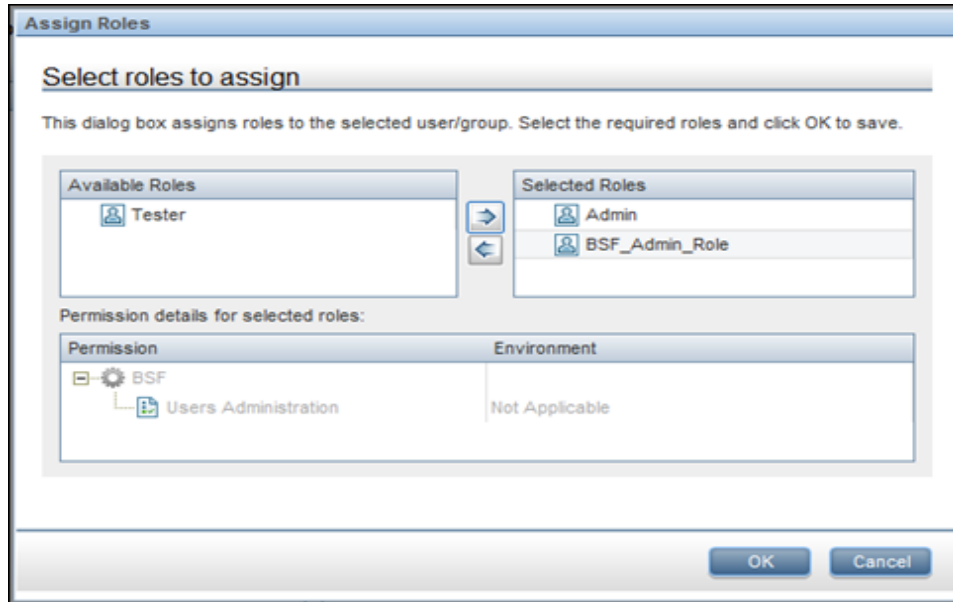
The screenshot shows the 'Search Users' interface in the HP Anywhere User Management UI. It features a search form with the following fields: 'First Name' (containing 'john'), 'Last Name' (containing 'doe'), 'Login Name', 'Display Name', and 'Email'. A 'Search' button is located below the form. Below the search results, there is a table with a header 'User Name' and one entry: 'John Doe'.

Note: The search operation is not case sensitive. You can use an asterisk (*) character in the search to search for any character(s).

5. Type the name of the (LDAP) user to search for.

Note: You can map roles to a group of users and not only single users.

6. From the right pane, under **Roles and Permissions**, select **Assign Role**. The Assign Roles window opens:



7. Add one or more roles (**Admin**, **BSF_Admin_Role** and **Tester**) to the selected user.

Note: You must assign the **Admin** and **BSF_Admin_Role** roles to at least one of the users. In this way, the user(s) can login to the "Administrator Console" on page 17 and User Management UI.

Chapter 3

Administrator Console

The Administrator Console is the central location from which you, the HP Anywhere administrator, manage and configure your mini apps.

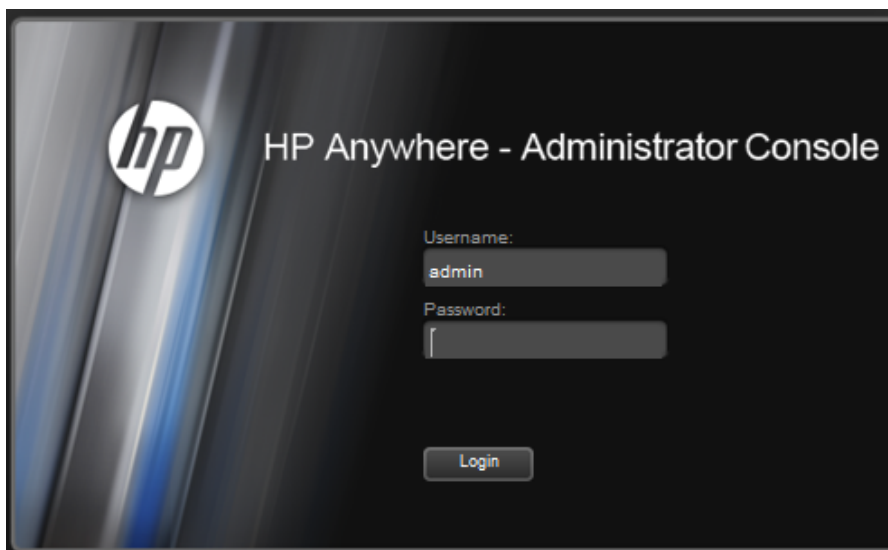
From the Administrator Console, you can:

- View and enable available mini apps
- Install a new mini app on the server
- Configure personas and associate them with mini apps
- Configure the backend data source instances
- Configure system settings

Log into the Administrator Console

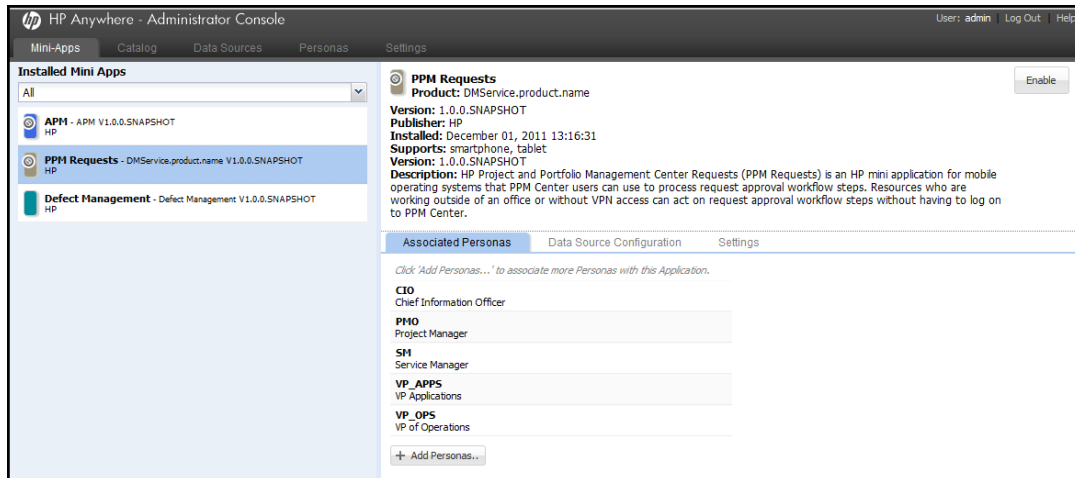
To log into the Administrator Console:

1. Go to the URL **http://<hostname>:20002/btoa/admin/**. The login page opens:



2. Enter your user name and password.

After your login is authenticated, the Administrator Console main screen opens:



Administrator Console Tabs

The Administrator Console tabs, located at the top Administrator Console page, contain options for managing the different HP Anywhere components. Click on a link for more information on each option.

- **Catalog:** Presents the list of available mini apps that have been uploaded to HP Live Network (HPLN). For details, see "[Catalog](#)" on page 21
- **Mini Apps:** Presents the list of mini apps and their details. For details, see "[Mini Apps](#)" below
- **Data Sources:** Presents the list of data sources along with their instances. For details, see "[Data Source](#)" on page 21
- **Personas:** Opens a list of personas defined in the system. For details, see "[Personas](#)" on page 22
- **Settings:** Presents various system parameters, including Google and Apple Push Notification parameters, and parameters related to each mini app. For details, see "[Settings](#)" on page 22

Mini Apps

The Mini Apps tab presents the list of the mini apps that the administrator has installed from the Catalog. From the mini app list, the admin user can enable or disable a mini app. Upon installation, all mini apps are disabled by default.

When the admin user enables a mini app, it becomes available to the end user on their mobile device.

Before enabling a mini apps, you must ensure that the relevant configuration has been set. For example, configuring the data source, and the relevant settings where appropriate.

View Installed Mini Apps

The left area of the Admin Console window shows a list of all the mini apps that the administrator has installed from the HP Catalog.

Each mini app is listed along with its version number, publisher name, and product name.

Each product may have a number of different mini apps, each with its own unique identifier - publisher name, product name, and version.


A mini apps can be in enabled/disabled state. If the mini app is disabled, the end user will not see it on their device.

To disable a mini app, click the Disable button in the top right corner of the window.

To enable a disabled mini app, click the Enable button in the top right corner of the window.

Note: HP Anywhere never uninstalls a mini app, only upgrades/updates it. However, you can change the configuration of a mini app, or disable it as required.

HP Anywhere assigns a specific color to each mini app, both in the Admin Console and on the mobile device, making it easy to recognize.

Note: If no data source is defined for the mini app, a  sign appears next to the mini app name.

View Mini App Details

The mini app details area is located on the right side of the Admin Console window.

At the top of the area, a detailed description of the mini app is shown along with the date of installation on the Anywhere server site.

Under the description, there are three tabs:

- "Associated personas " below
- "Data source configuration" below
- "Settings " on next page

Associated personas

The list shown in this tab contains built-in personas (roles). You can associate additional personas with the mini app using the **Add personas** button. You can select more than one persona using the **Ctrl** button. End users will select their roles from this list on their mobile device

Personas shown in gray are built-in to the system can cannot be updated or removed.

To remove the association of a persona from the mini app, click **X** next to the persona name.

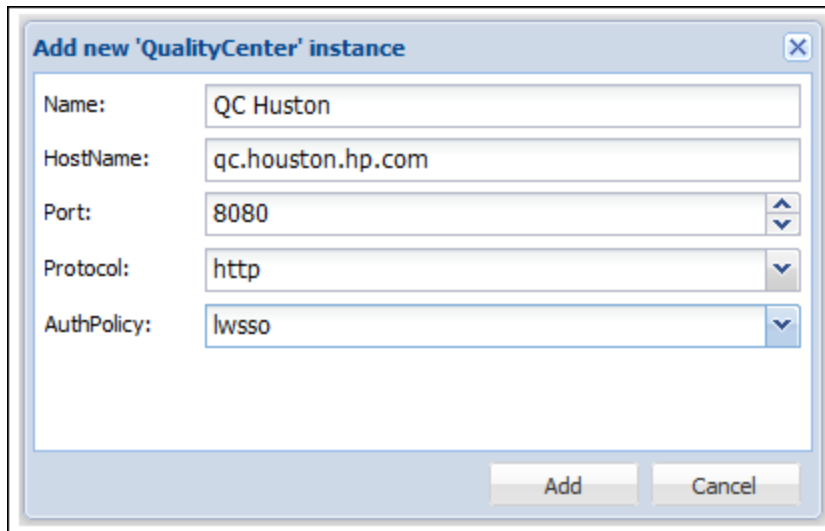
You can manage the list of persona from the Admin Console menu. For details, see "[Persona Management](#)" (on page 1).

Data source configuration

Each mini app (or group of mini apps) is connected to the HP Anywhere backend. The mini app is a proxy to a product. In the Data source configuration tab, you configure this connection. Each data source can be used by more than one mini app.

You can add a new data source using the **Add Instance** button.

1. Fill in parameters of the new instance (data source provider).



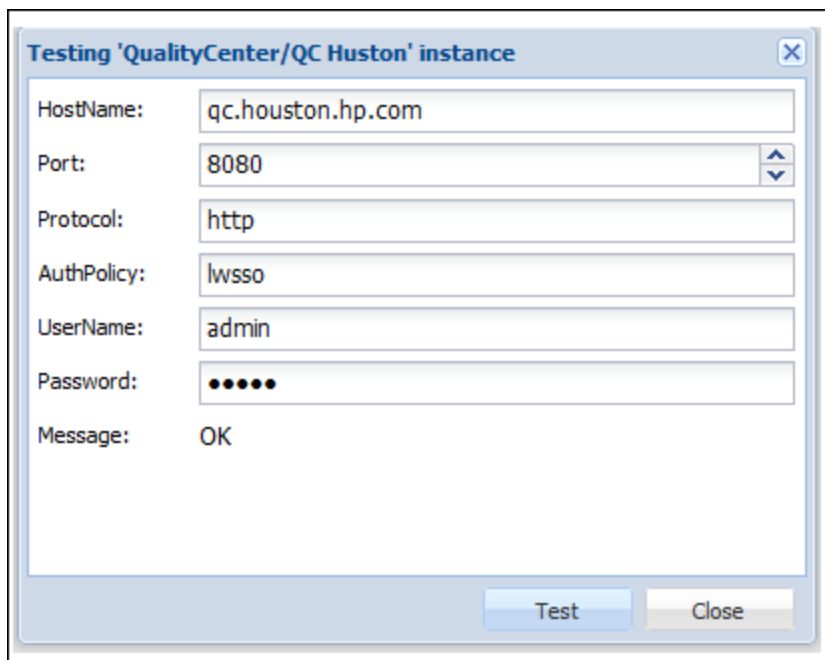
The screenshot shows a dialog box titled "Add new 'QualityCenter' instance". It contains the following fields:

- Name: QC Huston
- HostName: qc.houston.hp.com
- Port: 8080
- Protocol: http
- AuthPolicy: lwsso

At the bottom right, there are two buttons: "Add" and "Cancel".

2. After adding the new instance, click **Test** to test that the connection with the backend is valid.

In the Test dialog box, two new fields are shown, for use in identification in the backend: User Name and Password.



The screenshot shows a dialog box titled "Testing 'QualityCenter/QC Huston' instance". It contains the following fields:

- HostName: qc.houston.hp.com
- Port: 8080
- Protocol: http
- AuthPolicy: lwsso
- UserName: admin
- Password: •••••
- Message: OK

At the bottom right, there are two buttons: "Test" and "Close".

3. Type in the User Name and Password and click **Test**.


Settings

From this tab, you can configure the global settings of the mini app. This tab may be empty. For details on Push notification configuration for each mini app, see the relevant Getting Started Guide for your mini app.

Install a Mini App

After a mini app has been enabled, you can install it onto the HP Anywhere server:

1. Select the mini app and click the Install button in the corner of the Details area. A confirmation message opens.
2. Click **Yes** to approve the installation.

After installing a mini app, it is marked with the  icon.


Catalog

Presents the list of available mini apps that have been uploaded to HP Live Network (HPLN).

The administrator can download and install these mini apps onto the HP Anywhere server from the Catalog.

You can filter the catalog list by selecting one of the options from the Filter by drop down list:

- **All:** Shows all the mini apps (installed and not yet installed).
- **New:** Shows the new mini apps available that have not yet been installed on the HP Anywhere server.
- **Updates Available:** Shows the installed mini apps for which an updated version is available.

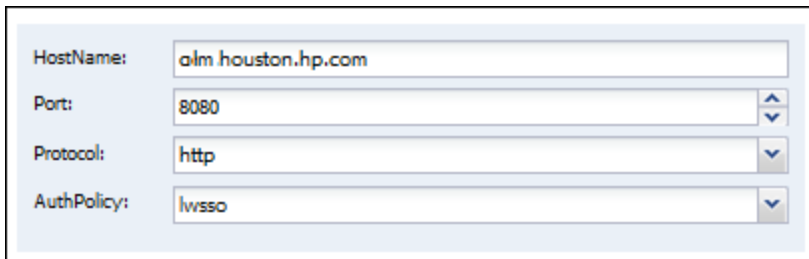
These mini apps are marked in the list with the Update icon .

- **Up to Date:** Shows the mini apps that are installed and are in the latest version.

Data Source

Presents the list of data sources along with their instances. This area contains the same information as in the Data Source tab of the Mini App Management area. See "[Mini Apps](#)" on page 18.

A data source defines the structure of the data, i.e., the type of information it contains. For example, the ALM Defects data source is made up of four types of information: Host Name, Port, Protocol and Authentication Policy. A data instance defines a single occurrence of the information content. For example:



HostName:	<input type="text" value="olm houston.hp.com"/>
Port:	<input type="text" value="8080"/>
Protocol:	<input type="text" value="http"/>
AuthPolicy:	<input type="text" value="lvss0"/>

On the mobile device, the end user selects the relevant data source instance from which the mini app will retrieve its data.

Each mini app defines its own data source information. The relevant data source is added as part of the mini app installation.

You can add, delete, or edit data source instances. If you make changes to a data source instance, all the mini apps that use this data source instance are automatically updated with the new information.

To add a new data source instance, click **Add Instance...**

For details on adding a new data instance, see **Data source configuration:** in "Mini Apps " on page 18.

Personas

Opens a list of personas defined in the system. There are two types of persona in the system:

- **Built-in (shown in gray):** Supplied with the system. You cannot delete them or change their details.
- **Custom (shown in black):** Customized persona added by the administrator.

To add a new persona:

1. Click **Add Persona** and in the Name field, type in a persona name. The Name field (Key) is automatically in upper case and must not contain spaces.
2. In the **Description** field, type in a description for this persona. This description is mandatory as this is the text that will appear as a role name on the end user's mobile device.

Note: The end user does not see the persona name on their device, they only see the **Description** text.

To delete customized persona:

1. Click **X** next to the persona name.
2. When the message opens, click **Yes** to confirm the deletion.

Settings

In the Settings area you define generic settings that affect the entire system.

The **General** category is for HP Anywhere settings parameters and contains settings related to the Push Notification.

Each mini app can have its own system settings. These are shown in the Admin Console Settings area.

For example, **settings.xs.content_name** is the name of the category that contains the parameters related to the XS mini app.

Some categories are divided into different sections, containing parameters related to the same subject.

The following screen shows an example of the parameters for the HP Anywhere General category:

General
Edit Category's settings:

Timer Frequency

Alerts frequency for Front Page data

Storage Frequency of HPLN Manager Meta...

Google Push Notifications (C2DM)

HTTP Proxy URL

HTTP Proxy port

C2DM Authentication Code

C2DM Thread Pool Size

Apple Push Notifications (APNS)

Enable Feedback Service Timer

Feedback Service timer schedule expression

APNS Certification File Path

APNS Certificate Password

SOCKS Proxy URL

SOCKS Proxy port

APNS Thread Pool Size

For each parameter, a tooltip shows the parameter description and an indication of when changes to this parameter take affect.

To update the value of a parameter:

1. Select the related category.
2. In the parameter field, type or select a new value from the drop down menu.
3. Click **Save**.

Note: Mandatory parameters are shown in red. For example:

HTTP Proxy url	<input type="text"/>
HTTP Proxy port	<input type="text"/>
settings.c2dm.auth.token.name	<input type="text"/>

Chapter 4

Alerts and Push Notifications

HP Anywhere is supplied with an Alerts and Push Notifications engine. This feature enables end users to receive push notifications on their mobile device about information to which they are subscribed.

HP Anywhere supports Push Notifications for the following device types:

- iOS devices (iPhone, iPad). See ["Configure Push Notifications for iOS Devices \(Apple\)"](#) below.
- Android devices. ["Configure Push Notifications for Android Devices \(Google\)"](#) on page 26

In order to use Push notifications, configure each device type as described in the relevant sections.

Note: Push notifications from the HP Anywhere server require an internet connection for accessing Google and Apple services.

Configure Push Notifications for iOS Devices (Apple)

Before configuring Push notifications for iOS devices, you must have an Apple Push Notifications Service (APNS) certificate. For details on how to obtain the APNS certificate file and password, see ["Mobile Client Configuration"](#) on page 32.

To configure push notifications:

1. In the Administrator Console, select the **Settings** tab.

General
Edit Category's settings:

Timer Frequency

Alerts frequency for Front Page data	30
Storage Frequency of HPLN Manager Meta...	24

Google Push Notifications (C2DM)

HTTP Proxy URL	
HTTP Proxy port	
C2DM Authentication Code	
C2DM Thread Pool Size	20

Apple Push Notifications (APNS)

Enable Feedback Service Timer	True
Feedback Service timer schedule expression	0 0 0 * * *
APNS Certification File Path	
APNS Certificate Password	
SOCKS Proxy URL	
SOCKS Proxy port	
APNS Thread Pool Size	20

2. Set the value of the following fields:
 - a. APNS Certification File Path – This is the full path to the file, for example “C:\myCert.cer”.
 - b. APNS Certificate Password
 - c. SOCKS Proxy URL (Optional)
 - d. SOCKS Proxy port (Optional)

Note: Use SOCKS protocol with ports 2195 and 2196 for Push notifications.

3. Use JMX to test the connection as follows:
 - a. Go to: <http://<host>:<port>/ViewObjectRes//Server%3Atype%3DPushNotifications>.
 - b. Click **testAPNSConnection**.
 - c. Verify that the following message is shown with the value `true`:

The operation returned with the value:
true

If the connection test fails, try the troubleshooting tips in "Alerts and Push Notifications" on page 24.

Configure Push Notifications for Android Devices (Google)

Before configuring Push notifications for Android devices, you must have a Cloud To Device Messaging Framework (Google C2DM) authentication code. For details on how to obtain a C2DM authentication code, see "Mobile Client Configuration" on page 32.

To configure push notifications:

1. In the Administrator Console, select the **Settings** tab.

General
Edit Category's settings:

Timer Frequency

Alerts frequency for Front Page data	30
Storage Frequency of HPLN Manager Meta...	24

Google Push Notifications (C2DM)

HTTP Proxy URL	
HTTP Proxy port	
C2DM Authentication Code	
C2DM Thread Pool Size	20

Apple Push Notifications (APNS)

Enable Feedback Service Timer	True
Feedback Service timer schedule expression	0 0 0 * * *
APNS Certification File Path	
APNS Certificate Password	
SOCKS Proxy URL	
SOCKS Proxy port	
APNS Thread Pool Size	20

2. Set the value of the following fields:

- a. C2DM Authentication Code
- b. HTTP Proxy URL (Optional)
- c. HTTP Proxy port (Optional)

Note: Use HTTPS protocol with port 443 for Push notifications.

3. Use JMX to test the connection as follows:

- a. Go to: **http://<host>:<jmx-port>/ViewObjectRes//Server%3Atype%3DPushNotifications.**

Note: The initial jmx port is 21942.

- b. Click **testC2DMConnection**.
- c. Verify that the following message is shown with the value `true`:

```
The operation returned with the value:  
true
```

If the connection test fails, try the troubleshooting tips in "Troubleshooting Push Notifications" below.

Troubleshooting Push Notifications

Apple

Problem: APNS test connection fails

Solution 1: You may need to define a SOCKS proxy in order to get a internet connection. Set the SOCKS proxy URL and port and try again.

Solution 2: Replace the Apple certificate file with a new one. If the connection still fails, you need to update the admin setting in order to reload the certificate (HP Anywhere reads the certificate upon startup or when settings are updated).

Android

Problem: C2DM test connection fails

Solution: You may need to define an HTTP proxy in order to get a internet connection. Set the HTTP proxy URL and port and try again.

Problem: Users on Android devices do not receive Push notifications

Solution: Make sure that a Google account exists on the mobile device. You can only receive push notifications from apps on an Android device after a Google account is set.

Chapter 5

Changing Default Ports in HP Anywhere

HP Anywhere is supplied with definitions for the following default ports:

- 20001 - Glassfish admin
- 20002 - HTTP port
- 20003 - HTTPS port
- 20007 - JMS port
- 20010 - Apache connector port

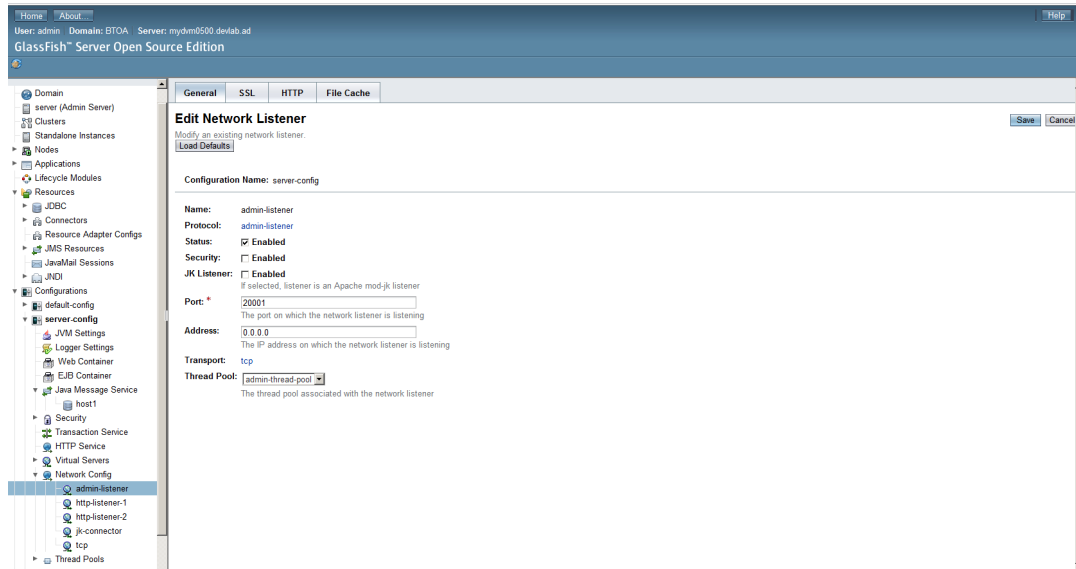
You can change these ports as required as follows:

1. Open the Glassfish Admin Console from the following link:
2. `http://<HOST>:20001`
3. From the left menu, select **Configurations > Server Config > Network Config > Network Listeners**.

Name	Port #	Protocol	Thread Pool	Enabled
<input type="checkbox"/> admin-listener	20001	admin-listener	admin-thread-pool	true
<input type="checkbox"/> http-listener-1	20002	http-listener-1	http-thread-pool	true
<input type="checkbox"/> http-listener-2	20003	http-listener-2	http-thread-pool	true
<input type="checkbox"/> jk-connector	20010	jk-connector-protocol	http-thread-pool	true

The following ports are shown:

- **admin-listener** - 20001 (Glassfish admin)
 - **http-listener-1** - 20002
 - **http-listener-2** - 20003
 - **jk-connector** - connector to Apache Web Server - 20010
4. Select each port name to see the current port number and change it. For example for the GlassFish admin listener port, select **admin-listener** and change the port number in the Port Number field.



For the jms port configuration - port 20007, select **Configurations > Server Config > Java Message Service > Hosts1** and change the port number in the Port Number field.



Additional Port Configuration Changes

After you have made these changes in the GlassFish Admin Console, you must make additional configuration changes in the relevant xml, batch and properties files.

1. Port 20001

File Name	Change
<HPA_HOME>/bin/ setDomainProperties.bat	Replace 20001 with the new glassfish admin port.
<HPA_HOME>/confwizard/conf/configwizard/fm/configwizard/Main/ configwizard.flow.xml	Replace 20001 with the new glassfish admin port.

2. Port 20002

File Name	Change
<HPA_HOME>/glassfish/glassfish/BTOA/config/conf/ resources.properties	Replace 20002 with the new http port.

3. Port 20003

File Name	Change
<HPA_HOME>/glassfish/glassfish/BTOA/config/conf/ lwssofmconf.xml	Replace 20003 with the new http port.
<HPA_HOME>/glassfish/glassfish/BTOA/config/conf/ client-config.properties	Replace 20003 with the new http port.

4. Port 20007

File Name	Change
<HPA_HOME>/bin/cluster.properties	Replace 20007 with the new jms port.
<HPA_HOME>/bin/setDomainProperties.bat	Replace 20007 with the new jms port.

Delete the folder **domains/domain1/imq/instances/imqbroker_host1/fs370**.

Opening Ports in a Firewall

To allow HP Anywhere to transfer data/communicate through a firewall:

- For an internal firewall (for connections from web server to Glassfish), open the HTTP port for incoming connections (port 20010 if you did not change it).
- For an external firewall (for connections from clients to web server in DMZ), open port 80 for incoming connections.

For Push notifications open the following ports:

- For Google's C2DM notifications, open port 443 (HTTPS protocol) for outgoing connections.
- For Apple's APNS notifications, open ports 2195 and 2196 (SOCKS protocol) for outgoing connections.

For details on Alerts and Push notifications for iOS and Android devices, see "[Alerts and Push Notifications](#)" on page 24.

Chapter 6

Mobile Client Configuration

In order to implement HP Anywhere on its end users mobile devices, each customer must have its own mobile client configuration.

This configuration is comprised of customizing the server address and enabling push notification.

In order to run the configuration you must obtain the following information:

- "HP Anywhere Server URL" below
- "iOS Developer Certificate" below
- "Android Keystore" on next page

HP Anywhere Server URL

The HP Anywhere server URL must include the port number and must be in the following format:

```
http://<web_address>:<port>
```

For example:

```
http://www.your-server-address.com:80
```

When running the mobile client for the first time, it will use this address as the default address. The end user can change the address on the mobile device at a later stage.

iOS Developer Certificate

In order to generate the iOS Developer Certificate with Push Notification enabled, you must follow the steps below:

1. Sign up to iOS Developer Enterprise Program at <http://developer.apple.com/programs/ios/enterprise/> .
2. Follow the instructions at <http://developer.apple.com/ios/my/certificates/howto.action> to generate a certificate.
3. Follow the instructions at <http://developer.apple.com/ios/manage/bundles/howto.action> to generate an app id for Apple push notification with the bundle identifier of `com.hp.btoa.your-company-name`.
4. Run your Mac OS keychain (password management system) application.
5. Select the login keychain.
6. Select the Certificates category.
7. Choose your certificate and export it using the **File > Export Items** option. A P12 Public Key

Cryptography Standards file is produced.

8. Send the P12 file to the HP Anywhere support team leader.

Android Keystore

Generating an Android keystore is a straightforward process. There is no need to contact Google during this process.

Note: In order to use push notification, you must have a valid Google email account (your-app-name@gmail.com). Send your email address and password to the HP Anywhere support team, and you will receive the AuthToken to be used in the HP Anywhere configuration.

In order to generate an Android keystore using Eclipse, follow the steps below:

1. Read <http://developer.android.com/sdk/installing.html>.
2. Install Android Development Tools (ADT) from <http://developer.android.com/guide/developing/tools/index.html>.
3. Install Eclipse (Software Development Environment) from <http://www.eclipse.org/downloads/>. (Select one of the download options, for example, Eclipse IDE for Java Developers.)
4. Start **Eclipse**.
5. Create a new temporary Android project.
6. Right click on the project name and select **Android Tools > Export Signed Application Package**.
7. In the new screen, click **Next** and select **Create New Keystore**.
8. Choose a location and password and click **Next**.
9. In the next screen, fill the required fields and click **Next**.
10. Click **Finish**.
11. Send the new keystore to the HP Anywhere support team leader with your server URL and the two passwords you used during the keystore creation.

Note: For detailed information, see <http://developer.android.com/guide/publishing/app-signing.html>.

Artifacts to Send to the HP Anywhere Support Team

After performing the above steps, you need to send certain files and information to the HP Anywhere support team in order to generate a WAR file containing iOS and Android shells.

For iOS, send the following information:

- P12 certificate (File with private/public key certificates).
- Developer name (e.g., “iPhone Distribution: your-company-name”).
- Provisioning profile (File with .mobileprovision extension).

For Android, send the following information:

- Keystore with two passwords.
- Keystore alias.
- Gmail address with password.

Additionally, you need to send your server address so that it can be used as the default server in the mobile client.

After sending all the above artifacts, the HP Anywhere support team sends you a WAR file.

Deploy the WAR File and Publish the Client URL

To deploy the WAR file received from the support team, perform the following steps:

1. Login to the Glassfish Administration Console (By default, your server address with port 20001).
2. From the sidebar options, select **Applications**.
3. Go to the “btoa-client” line and select **Deploy**.
4. Select the new WAR file and confirm the operation.
The URL is now available.
5. Publish the URL **http://www.your-server-address.com:80/btoa/client** to the end users by SMS, email, QR (Quick Response) code or any other distribution method.
6. Your end users can now connect to **http://www.your-server-address.com:80/btoa/client**, perform authentication and install HP Anywhere onto their iPhone/iPad/Android device.

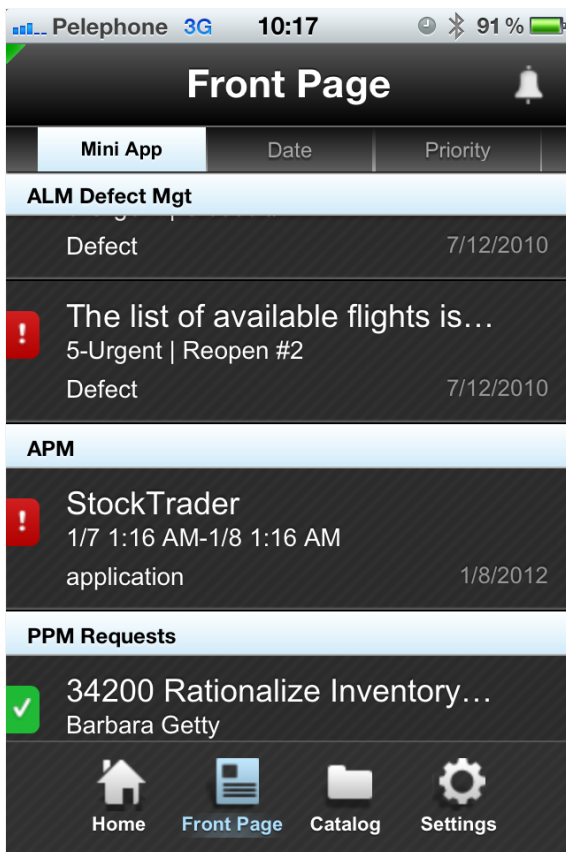
Chapter 7

End User Alerts

Alert Rules

Each end user can define rules for getting alerts about new/modified data items.

To create the rules, end users click on the “Create Alert” button on the Front Page of their mobile device, as shown in the example below:

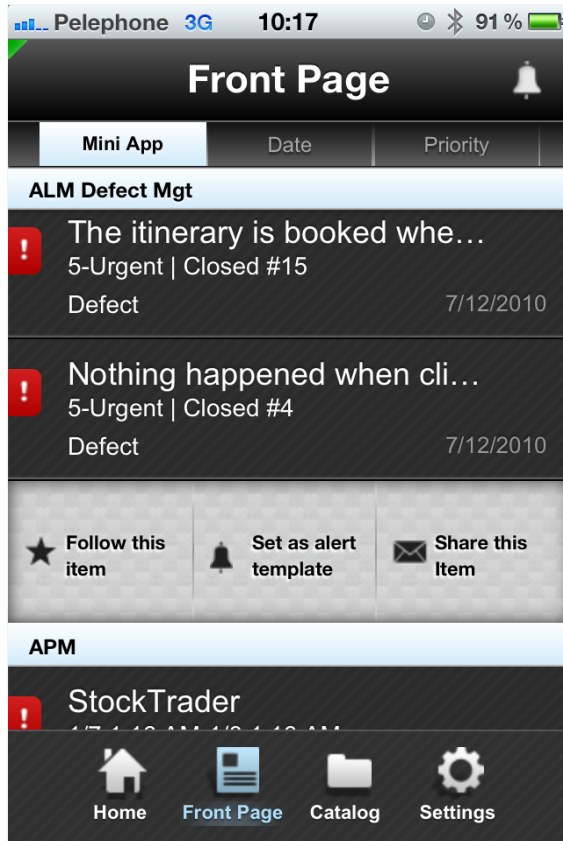


The alert is sent as a Push Notification to the user’s mobile device.

After the alert arrives, the user clicks the Push Notification message box and HP Anywhere opens with the relevant data.

Follow Items

When the user swipes on a Front Page item, a menu opens. From this menu, they can follow the Front Page item by selecting **Follow this item**.



The following rules are relevant when sending alerts:

1. Alerts are sent only on items that are returned in front page. If an item no longer appears on the Front Page, it will not be followed until it reappears on the Front Page.
2. Alerts (by rule or by followed items) are sent only when changes are made on specific properties that the user sees when creating an alert rule.
3. Alerts are sent only on enabled services.

