HP Anywhere

Windows

Software Version: 10.01

Administrator Guide

Document Release Date: May 2013

Software Release Date: May 2013

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

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

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

Chapter 1

Overview

This guide is intended for HP Anywhere administrators.

HP Anywhere is a next-generation mobility platform that introduces a new and innovative approach for developing, managing, and consuming enterprise applications. It is designed for developing granular applications (apps) that can be accessed on various types of media—desktop, tablet, and smartphone. This enables end users to consume only the information they need, wherever they may be.

In addition, HP Anywhere places collaboration at the heart of any successful workflow by combining structured processes with unstructured discussions into organized, context-specific activity streams.

You use the Administrator Console to manage your organization's apps, and to perform most administrator tasks.

This guide describes the Administrator Console and the tasks required to manage apps, the HP Anywhere platform backend, and HP Anywhere end users.

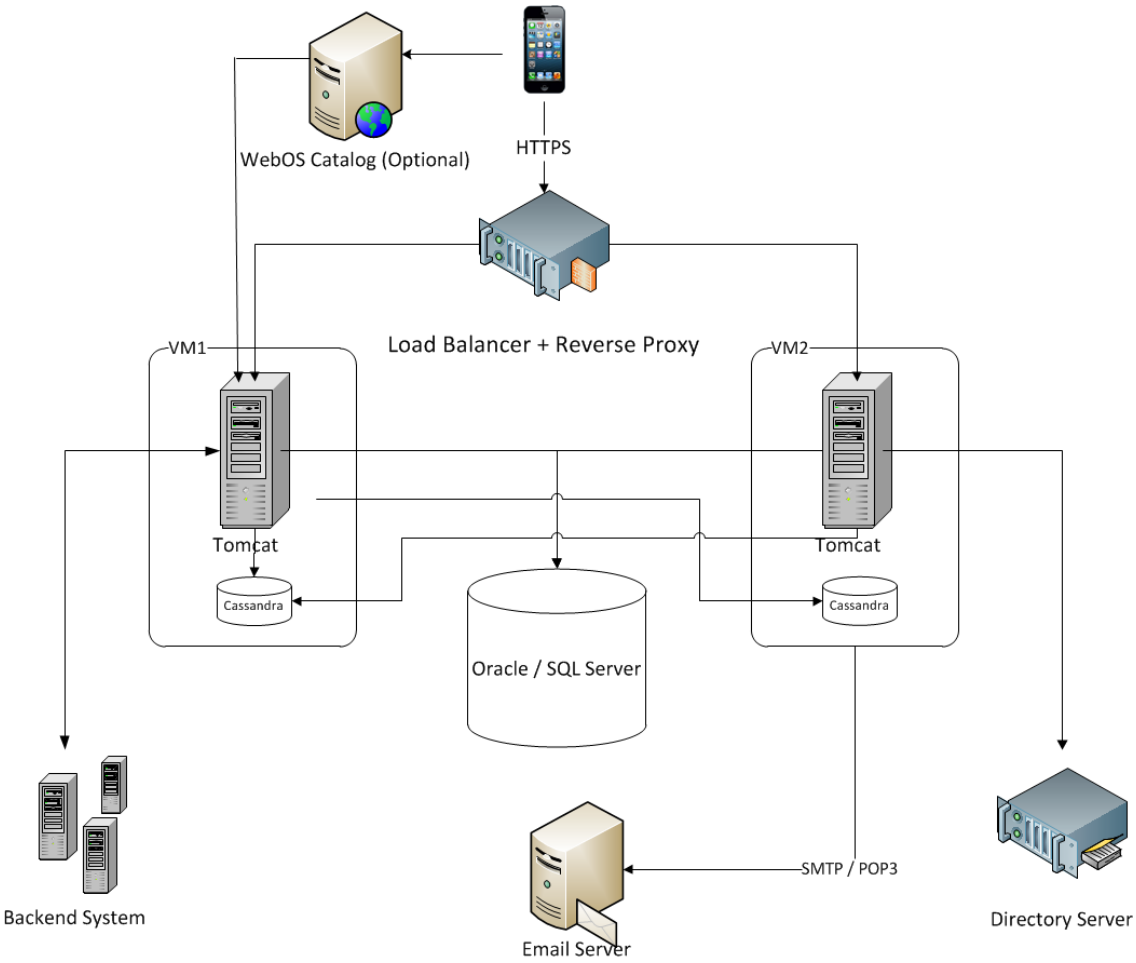
For details on defining a white list or black list for users and/or devices, see *HP Anywhere – Restricting User/Device Connections (Black/White List)* on the HP Software Product Manuals web site.

HP Anywhere Architecture

HP Anywhere architecture comprises:

- **Apps**:
  - **Client side.** The interface that the end user sees on a smartphone, tablet, or desktop.
  - **Server side.** The interface that act as a proxy between the client device and the backend.
- **HP Anywhere Runtime Server - Tomcat.** The platform for connecting to apps.
- **Backend System.** The data source for an app in an enterprise's system. (Not supplied with HP Anywhere)
- **Cassandra Database.** A highly scalable, distributed, structured, key-value store. HP Anywhere uses this store as a high-speed distributed caching layer.
- **Email Server.** The interface for sending and receiving emails from the Timeline. (Not supplied with HP Anywhere)
- **Load Balancer and Reverse Proxy.** Used to distribute load between the HP Anywhere runtime servers in high availability environments, and to provide failover for crashes. (Optional component. Not supplied with HP Anywhere)
- **Directory Server.** Stores the organization's users. (Not supplied with HP Anywhere)
- **Oracle/SQL Server.** Stores the HP Anywhere service data. (Not supplied with HP Anywhere)
- **Catalogs.** Store the client-side apps used by the enterprise. Developers provide the apps to administrators, who upload them to the relevant catalog. Apps are automatically transferred to the HP Anywhere runtime server from the catalog.

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

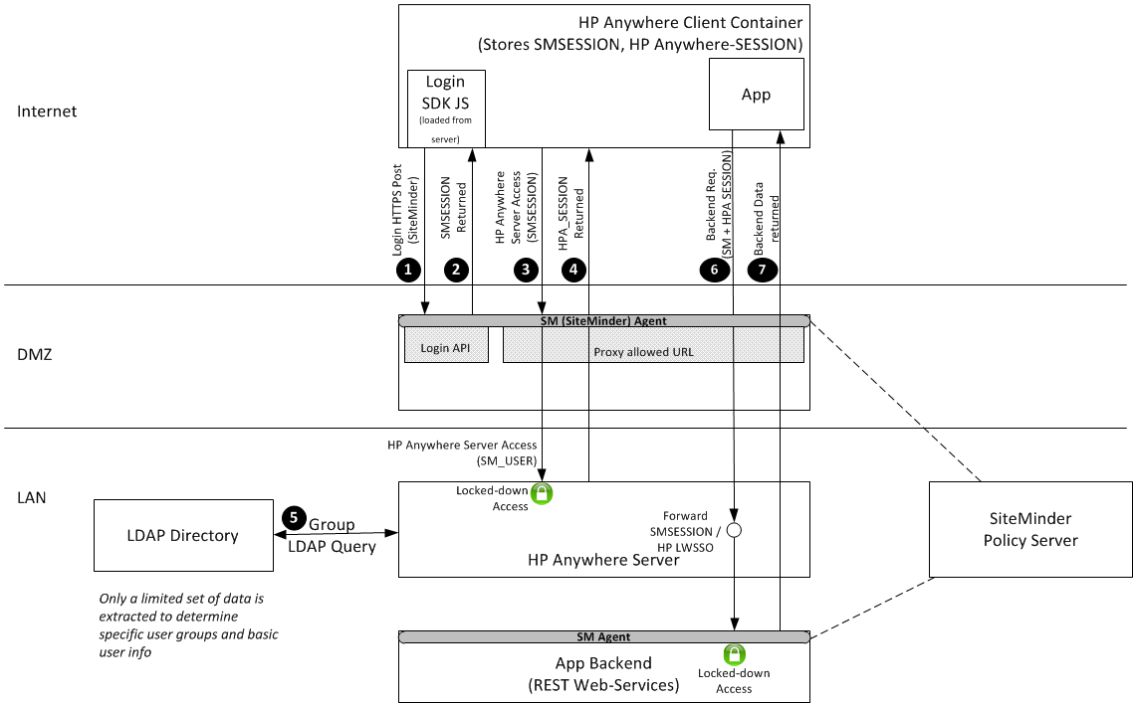


HP Anywhere Login Security with SiteMinder

The HP Anywhere client container contains:

- HP Anywhere screens and client side logic.
- Dynamically loaded apps.
- A JavaScript-based Login page and logic that creates the HTTPS POST request in order to initiate the login flow. This library is loaded dynamically from a public URL.

Security Design



The flow:

1 The client-side JavaScript connects to SiteMinder (or any other authentication provider) with a login request using HTTPS POST.

2 SiteMinder responds with an SMSESSION token upon successful login. From now until the token expires, the SMSESSION token is sent with every request to the server.

3 The client connects to HP Anywhere server with a login request that includes the SMSESSION token. The request passes this token to the DMZ for authentication with HP Anywhere. The request is sent to a single, public URL that allows login on HP Anywhere.

4 HP Anywhere sends a response to the client with the HPA_SESSION token to be used with any subsequent request.

5 HP Anywhere connects to the enterprise user repository (LDAP in the diagram) and requests basic user information and the LDAP group to which the user belongs. This information can be used later on the server side for authorization.

6 The client side of the app connects to the server side of the app with two tokens because the HP Anywhere client container adds these headers to every request. The server side of the app connects to the the backend and forwards SMSESSION (or HP-LWSSO if the backend is an HP software product).

7 The response from the backend is returned to the client side of the app.

Chapter 2

LDAP Configuration Prerequisites for HP Anywhere

HP Anywhere interacts with users via LDAP. Therefore, you must assign administrator privileges to at least one LDAP user before you can begin working with the HP Anywhere Administrator Console. You must also make sure that the HP Anywhere users in your organization are assigned to relevant LDAP groups.

For details, see:

- "LDAP Admin Users for HP Anywhere" below
- "Defining LDAP Groups for HP Anywhere" below

LDAP Admin Users for HP Anywhere

Before you can log on to the Administrator Console, you need to assign administrator privileges to at least one LDAP user. You can create as many administrators as needed.

To assign administrator privileges to an LDAP user:

1. Open a command-line interface and run the following:

   <HP Anywhere installation folder>\conf\population>assign-admin-role.bat <user name>

   For example:

   C:\HP\HPAnywhere\conf\population>assign-admin-role.bat alex@mycompany.com

2. Repeat for each LDAP user that needs administrator privileges.

Defining LDAP Groups for HP Anywhere

Any LDAP user in your organization can log in to HP Anywhere. However, only authorized LDAP users can view and access apps.

HP Anywhere uses LDAP groups to authorize app users. To enable users to view and access relevant apps in the catalog, you must associate each app with a dedicated LDAP group, and assign users to that group.

The first step is to define a root authorization group in LDAP. This group serves as a parent group for any sub-LDAP group that you may define. For example, you may want to create a dedicated sub-group for salespeople, and a dedicated sub-group for their managers.

LDAP groups are organized hierarchically, so that users can access any app that is associated with their assigned LDAP group or with a parent LDAP group.

After you define the root authorization group in LDAP, you instruct HP Anywhere to use that group by setting a parameter in the Administrator Console.

To define the root authorization group:

1. Define the root authorization group in LDAP.
2. Make sure that that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 17.
3. In the HP Anywhere Administrator Console, select **Settings > General Settings**.
4. In the Authorization section, enter the group name in the **Authorization groups root** text box.
   Note: The name is case-sensitive.

Note: If the expected path length from the root node to the furthest sub-node (leaf) is greater than 10, you must modify the value in the **Authorization groups tree max height** text box (in the Authorization section).

Chapter 3

Understanding the Administrator Console

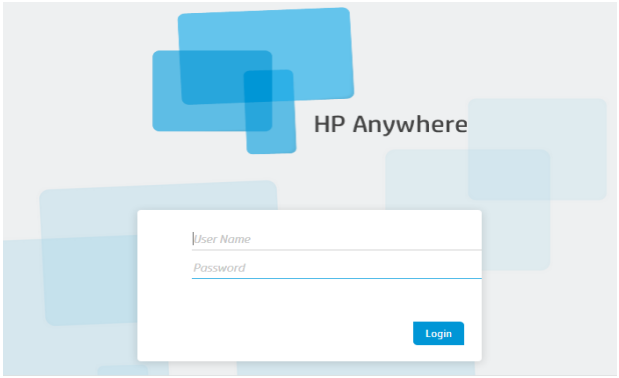
You use the Administrator Console to :

- Manage and configure your apps, including:
  - Installing apps on the HP Anywhere server
  - Viewing and enabling apps
  - Associating apps with authorized LDAP groups
  - Configuring backend data sources for your apps
- Configure system settings
- View the devices associated with end users that are currently logged in to HP Anywhere

Logging In and Out of the Administrator Console

To log into the Administrator Console:

1. Browse to **http(s)://<hostname>:<port>/admin/**. The login page opens.



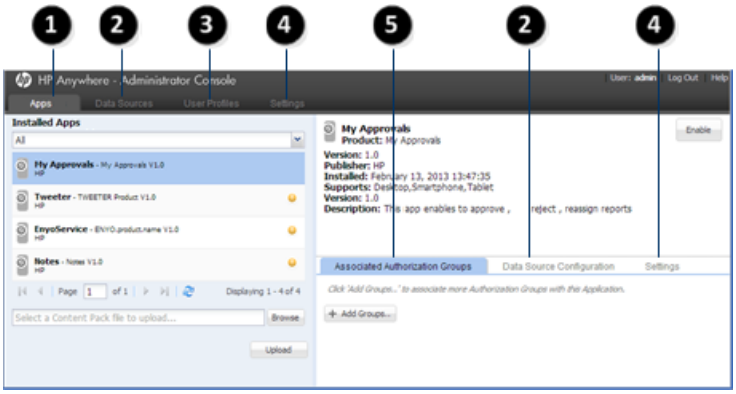
2. Enter your administrator login credentials (user name and password) and click **Login**.After your login is authenticated, the Administrator Console opens.

To log out of the Administrator Console:

In the top-right corner of the Administrator Console, click **Log Out**.

Administrator Console User Interface

You use the Administrator Console to manage various HP Anywhere components. This section provides an overview of the Administrator Console user interface.



1	**Apps**	• View and filter list of installed apps • Upload new apps and overwrite previous versions of installed apps • View the details for a selected app in the right pane • Manage LDAP group associations, data sources, and settings for apps For details, see "Uploading Apps to the Default Catalog" on page 62
2	**Data Sources / Data Source Configuration**	View and manage the data sources for a selected app For details, see"Defining a Data Source for an App" on page 68.
3	**User Profiles**	View and filter list of users that are logged into HP Anywhere, as well as their devices
4	**Settings**	View and configure: • App-specific settings • Global system settings For details, see "Defining Global and App-Specific Settings" on page 67.

5	**Associated Authorization Groups**	View and manage the associated LDAP authorization group for each app For details, see "Defining LDAP Groups for HP Anywhere" on page 15.

General Settings

This section describes many of the fields in the General Settings pane (Settings tab) of the Administrator Console.

For details on opening the Administrator Console, see "Logging In and Out of the Administrator Console" on page 17.

General Text Field Limitation

Field	Description
Max short text field length	The maximum number of characters allowed in a short text field. **Required:** Yes **Possible values:** Integer from 1 -4000 **Default:** 100
Max long text field length	The maximum number of characters allowed in a long text field. **Required:** Yes **Possible values:** Integer from 1-4000 **Default:** 2000
Max medium text field length	The maximum number of characters allowed in a medium length text field. **Required:** Yes **Possible values:** Integer from 1-4000 **Default:** 500

Email

Field	Description
Enable SSL when sending email	Specifies whether to send via HTTP or HTTPS. If HTTPS, requires a certificate for the server. When you install HP Anywhere, the installation automatically generates a certificate for the server. If you need to manually generate a certificate, go to the JMX-Console (**Host/diamond/jmx-console > diamond > CertificateJMX service > fetching certificate from trusted server**). Make sure to restart all of the HP Anywhere nodes to make the certificate available. (Requires restart) **Possible values:** True, False **Default:** False

Email, continued

Field	Description
Separator between emails (exact match)	Separator between email threads. **Default:** \r\n-----Original Message-----;\r\nFrom;\r\nSent from my;\r\n_____ _
HP Anywhere user name for sending email	The user name for the HP Anywhere email account that is used to send emails. **Default:** N/A **Example:** <*server*>@<*company.com*>
Prefix of email subject	The prefix to include in the subject line of the email (the title of the activity). **Default:** HPA **Example:** **From:** myserver@mycompany.com **Date:** Thursday, September 15, 2013 12:57 PM **To:** Lee.Johnson@mycompany.com **Subject: HPA:** An important activity
Email signature format to be removed	Specifies the format of the company email signature to remove from replies before sending the email. **Default:** ${email};${firstName} ${lastName}
Email subject prefix when failed to add participant	The prefix to include in the subject line of the email (the title of the activity). **Default:** Can't add participants -
Email sending host	The URL of the SMTP email server. You can either use the default port or you can specify a port, as follows: <*server*>:<*port*>
HP Anywhere user password for receiving email	The password for the HP Anywhere email account that is used for replies to emails. **Default:** N/A

Email, continued

Field	Description
Enable SSL when receiving email	Specifies whether to receive via POP3/IMAP or POP3S/IMAPS. If POP3S/IMAPS, requires a certificate for the server. When you install HP Anywhere, the installation automatically generates a certificate for the server. If you need to manually generate a certificate, go to the JMX-Console (**Host/diamond/jmx-console > diamond > CertificateJMX service > fetching certificate from trusted server**). Make sure to restart all of the HP Anywhere nodes to make the certificate available. (Requires restart) **Possible values:** • **True:** Receives emails via POP3S/IMAPS • **False:** Receives emails via POP3/IMAP **Default:** False
HP Anywhere user name for receiving email	The user name for the HP Anywhere email account that is used for replies to emails. **Default:** N/A
Allow adding participants by Email CC	Specifies whether HP Anywhere should add email email addresses that are in the CC of a reply to the activity as participants . **Default:** False
Send email from a general name	Specifies the email user ID. Possible values: • **True:** Email is sent from a general (fake) email address. • **False:** Email is sent from the email of the user that posted the message. Applicable only if supported by email server. **Default:** False
Prefix of Snooze/Wake up Email subject	The prefix to include in the subject line of the email (the title of the activity) when a snoozed activity times out. **Default:** HPA: Reminder-
HP Anywhere user password for sending email	The user password for the HP Anywhere email account that is used to send emails. **Default:** N/A

Email, continued

Field	Description
Maximum timeout until sending an email (in minutes)	The number of minutes from the last email that was sent until another email is sent to offline participants. **Default:** 20
Email receiving host	The URL of the receiving email server. You can either use the default port or you can specify a port, as follows: *<server>:<port>*
Email subject when activity ID is not found	Relevant for replies to email. Used only if HP Anywhere cannot match the incoming email to an activity. **Default:** RE: Message delivery problem

Activities

Field	Description
Maximum limitation of activity search results	The maximum number of activities to return when searching for an activity. **Required:** Yes **Possible values:** Integer from 1-2000 **Default:** 1000
Max number of activities to return on request	The maximum number of activities to display per page in the search results when searching for an activity. **Required:** Yes **Possible values:** 1-100 **Default:** 50

Activities, continued

Field	Description
Allow private activities only Activity visibility settings are privacy settings that specify whether activities are visible to all users in your organization or only to actual activity participants. Activities can be set to: **Private**. Only participants that are currently included in the activity can view the activity. Search results for private activities are displayed only to activity participants. **Public**. Any user can search for and view an activity that is defined as public.	Specifies whether end users can define activities as public. **Required:** Yes **Possible values:** • **True**. ▪ All activities that end users create are private and are accessible only to activity participants. ▪ End users cannot change private activities to public. • **False**. (Default) End users can set an activity to **public** or **private**. **Default:** False
Default number of activities to return on request	The default number of activities to display per page in the search results when searching for an activity. **Required:** Yes **Possible values:** 1-100 **Default:** 10
Activity indexing bulk size	The bulk size for indexing activities in index server. **Required:** Yes **Possible values:** 100-5000 **Default:** 500

Activities, continued

Field	Description
Default created activity visibility Activity visibility settings are privacy settings that specify whether activities are visible to all users in your organization or only to actual activity participants. Activities can be set to: • **Private**. Only participants that are currently included in the activity can view the activity. Search results for private activities are displayed only to activity participants. • **Public**. Any user can search for and view an activity that is defined as public. **Default:** PUBLIC	The default for all new activities. • **PRIVATE**. ▪ All new activities are set to private. ▪ If **Allow private activities only** is set to **False**, users can set an activity to public, if needed. • **PUBLIC**. ▪ All new activities are set to public. ▪ **Allow private activities only** (described above) must be set to **False**. ▪ Users can set an activity to private, if needed. **Default:** PUBLIC
Minimum interval for activity indexing (in minutes)	The minimum interval in minutes between activity indexing operations. **Default:** 1
What's next visibility	Specifies whether to show or hide What's Next in an activity workspace. **Default:** True

Profile

Field	Description
Maximum results for profile search	The maximum number of results to return when searching for a user. **Default:** 50
Profile thumbnail image width (in pixels)	The width in pixels of the image displayed for activity participants. **Default:** 60

Profile, continued

Field	Description
Take profile display name from LDAP	Specifies whether to display a participant's LDAP profile name, for example, *Smith, Alex*. If set to **False**, the email address of the participant is displayed instead, for example, *alex.smith@mycompany.com*. **Default:** False
Profile search fields priority	The priority of each search criterium **Default:** firstName,lastName,email
Max profile image upload size (in MB)	The maximum size of a profile image to upload. **Default:** 10
Non-person name regular expression (for search optimization)	The regular expression that can be used when searching for anything other than a user name. **Default:** ^[^0-9@!@#$%^&*()<>{}"?~.;:/]*$
Profile small image width (in pixels)	The size in pixels of a small profile image **Default:** 60
Minimum number of letters for profile search	The minimum number of characters to enter in a search for a user. **Default:** 3
Profile cache size	The number of users that are stored in the cache after a search **Default:** 1000
Profile large image width (in pixels)	The size in pixels of a large profile image **Default:** 200

Attachments

Field	Description
Maximum attachment description size (in characters)	Maximum number of characters that can be used in the description of an attachment. **Required:** Yes **Possible values:** 1-260 **Default:** 256

Attachments, continued

Field	Description
White list of allowed attachment types	Comma-separated list of attachment types (not extensions) that are allowed. **Required:** No **Possible values:** • image - All types of images • text - Text files (including logs) • application/x-tika-ooxml - Word documents (.doc and .docx formats) • application/xml - XML files • application/pdf - PDF files • application/x-tika-msoffice - Power point, Excel files (.ppt, .xls) • application/x-tika-ooxml - Power point, Excel files (.pptx, .xlsx) • application/x-rar-compressed - Archive (rar) • application/zip - Archive (zip) **Default:** image,text,application/pdf,application/zip,application/x-tika-ooxml,application/x-tika-msoffice,application/x-tika-ooxml
Maximum attachment size (in MB)	Maximum size of an attachment in megabytes. **Required:** Yes **Possible Values:** 1-1000 **Default:** 50
Maximum attachment file name size (in characters)	Maximum number of characters in file name. **Required:** Yes **Possible Values:** 1-260 **Default:** 256

Attachments, continued

Field	Description
Maximum amount of attachments per activity	Maximum number of attachments that can be included in an activity. **Required:** Yes **Possible values:** 1-100 **Default:** 50

Presence

Field	Description
Number of seconds from Comet disconnection to offline presence	Number of seconds after Comet disconnection after which user is considered offline. **Required:** Yes **Possible values:** 1-60 **Default:** 10

Foundation Settings

Field	Description
User repository type	The type of user repository **Possible values:** LDAP, SAAS, DB **Default:** ldap
Open the JMX to HTTP	Specifies whether HTTP access to JMX console is allowed. **Note:** If you set this to **False**, you must connect to JMX via the JConsole. To do this, you must set the remote connection to: **localhost:29601** **Possible values:** True, False **Default:** True
Enable audit logs	Specifies whether to write audit logs **Possible values:** True, False **Default:** True

Foundation Settings, continued

Field	Description
User repository case-sensitive	Specifies whether the user names in user repository are case-sensitive (is "Jack" and "jack" the same user or two different user names). **Note:** You must set this to **True** if your user repository is case-sensitive. **Possible values:** True, False **Default:** False
SAAS base URL	The URL of the SaaS server. **Possible values:** N/A **Default:** N/A

Apple Push Notifications (APNS)

Field	Description
SOCKS Proxy port	SOCKS proxy port for sending notifications to iOS devices. **Required:** No **Possible values:** Integer from 1 to 65535 **Default:** N/A
SOCKS Proxy URL	SOCKS proxy URLfor sending notifications to iOS devices. **Required:** No **Possible values:** *Enter a URL string* **Default:** N/A
APNS thread pool size	The maximum number of notifications that can be processed simultaneously on the HP Anywhere backend server for sending to iOS devices. **Required:** No **Possible values:** Integer from 1 to 500 **Default:** 20

Apple Push Notifications (APNS), continued

Field	Description
APNS certificate password	Apple's certificate password **Required:** No **Possible values:** *Enter a password* **Default:** N/A
APNS certification file path	The location where the Apple certificate is stored in the file system on the HP Anywhere server. **Required:** No **Possible values:** *Enter a file path on the HP Anywhere server* **Default:** N/A

Google Push Notifications (GCM)

Field	Description
HTTP Proxy port	The port number of the proxy server behind which the HP Anywhere backend server runs. **Default:** 8080
Google Cloud Messaging API Key	**Default:** N/A
HTTP Proxy URL	The host name of the proxy server behind which the HP Anywhere backend server runs. **Default:** N/A

Entry Points

Field	Description
Max entry point state size (in KB)	The maximum size of an entry point state to transfer to the server in kilobytes. **Default:** 100

Default Notification Channels

Field	Description
Default notification channels for app alerts	Specifies how to send notifications to participants. **Possible values**: FRONTPAGE, EMAIL, PUSH_NOTIFICATION, NONE **Default:** FRONTPAGE

Tenant Email

Field	Description
External white list for sending email	A list of approved domains for sending emails. Separate the domains using a semicolon (;) (for example: hp.com;google.com) **Default:** N/A
Email sending to external	Specifies whether to send email to external users (non-enterprise email addresses, for example, *John.Doe@gmail.com*). **Possible values:** True, False **Default:** True

Catalog Settings

Field	Description
Always Check Apps Authorization	When **Catalog flavor** (below) is set to NONE, defines if HP Anywhere should consider associated authorization groups when installing apps on end user devices.. **Possible values:** • **True** - Installs an app on an end user's devices only if the end user is listed in an LDAP authorization group that is currently associated with that app. • **False** - Installs all available apps on an end user's devices regardless of the authorization groups associated with each app. **Default:** False
Catalog integration resources location	The URL of the resources used by the integrated catalog. **Default:** N/A
Enable Installed Applications Sync	Enable the HP Anywhere catalog to synchronize the installed applications when users log in. **Possible values:** True, False **Default:** True
Catalog flavor	Defines the catalog to use for this HP Anywhere server. **Possible values:** WEB_OS, NONE, DEFAULT, INTEGRATED **Default:** Default
Catalog sync authorization interval (in minutes)	The time interval after which the HP Anywhere server synchronizes with the LDAP group structure. **Default:** 1440 (24 hours)

Server

Field	Description
External URL of HP Anywhere server	The URL for external users that need to access HP Anywhere from outside of the enterprise, for example, the URL for load balancers. **Default:** The URL of the HP Anywhere server
Application Name	The title that appears at the top of the HP Anywhere application. You can use this to set your own company name, for example.

Apps

Field	Description
Enable base URL	Not in use.
Common web context for apps	Used to simplify URL mapping for load balancer configuration, and so on. This enables multiple apps to run their calls under a single context. This also enables you to create a white list for your apps by blocking any app that does not contain the common web context in its URL. For example, if you set "OurApps" as the value in this field, the URL for your apps will change from: http://<server>:<port>/<AppName>/... to: http://<server>:<port>/OurApps/<AppName>/... The URL must be consistent with the reverse proxy / load balancer. **Important:** You must apply the common web context BEFORE deploying any apps. If apps are already deployed, you must redeploy them (with no data loss) to apply this functionality. **Possible values:** Context can include up to 20 characters (letters and digits only). **Default:** N/A

Single Sign-On Settings

Field	Description
Init string	Init string for the Single Sign-On that is used to connect to many HP products.

Authorization

Field	Description
Authorization groups root	The parent LDAP root group. For details, see "Defining LDAP Groups for HP Anywhere" on page 15. **Required:** Yes **Default:** N/A
Authorization groups retrieval size	The maximum number of groups that can be retrieved from LDAP. **Default:** 50
Authorization groups tree max height	The path length in LDAP from the root node to the furthest sub-node (leaf). **Default:** 10

Publish Channels

Field	Description
Push notifications	Specifies whether push notifications are allowed. **Possible values:**: True, False **Default:** True
Publish emails	Specifies whether email notifications are allowed. **Possible values:** True, False **Default:** False

Chapter 4

Catalogs - What Administrators Need to Know

The **catalog** contains a collection of apps that are available for your end users. The administrator is responsible for maintaining the catalog. Each HP Anywhere server works with one catalog.

There are several types of catalogs. This guide focuses on:

- "WebOS Catalog" on page 37.
- "Default Catalog" on page 59.

Chapter 5

WebOS Catalog

The HP Anywhere administrator is responsible for managing the HP Anywhere apps in the WebOS catalog and the HP Anywhere server (via the Administrator Console).

Although the Enterprise Portal supports multiple versions for the same app, HP Anywhere supports only one version for end users. Therefore, each time you upload a new version of an app to the Administrator Console, it overwrites the previous version, so that only the latest installed version is available.

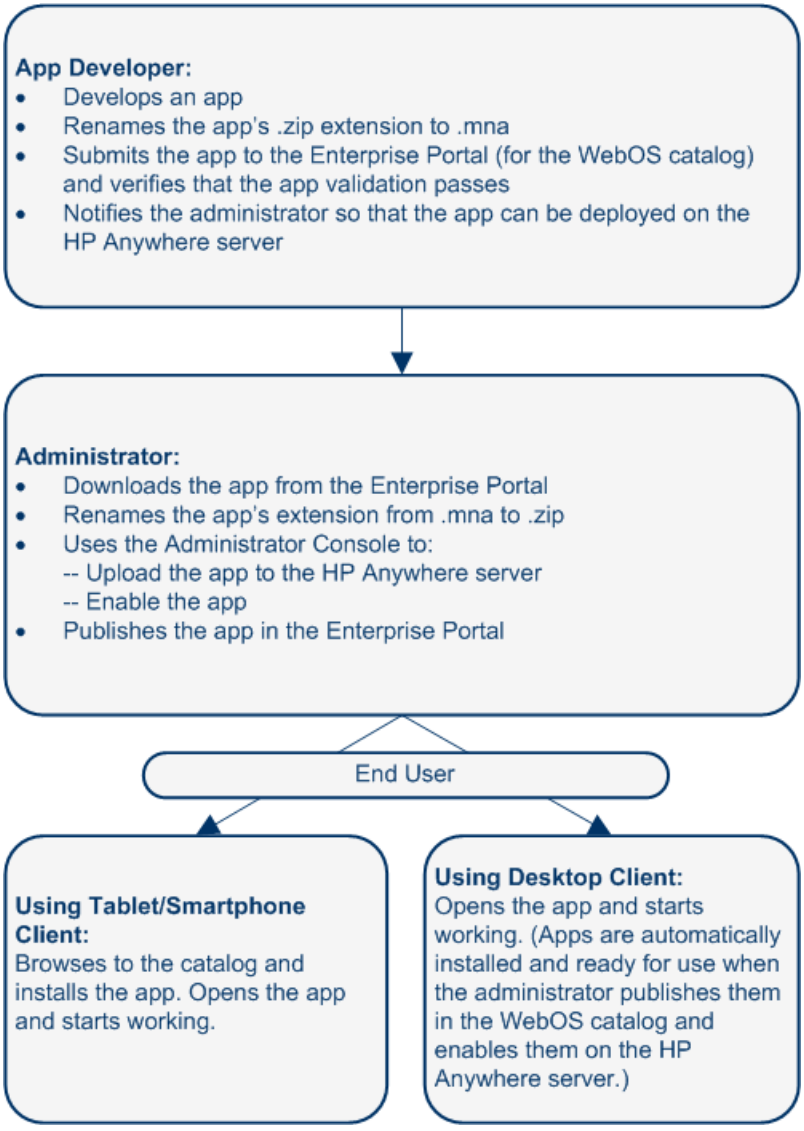
Note: HP Anywhere never uninstalls an app from the HP Anywhere server, only upgrades/updates it. However, you can suspend or disable it in your end users catalogs as required.

Apps in WebOS Catalog—from Developer to End User

The administrator manages the app lifecycle for end users via the HP Anywhere Administrator Console and the HP Enterprise Portal. This section describes the development-to-delivery flow for apps and the steps that you need to perform to provide your end users with access to each app.

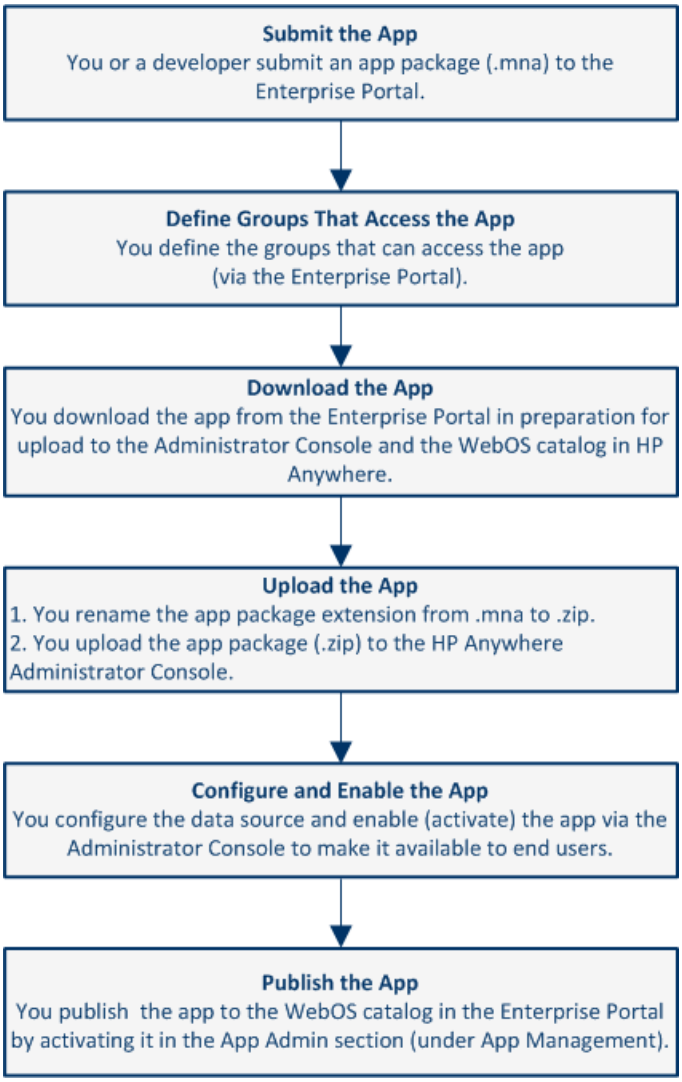
Development-to-Delivery

The following chart illustrates how your organization's apps reach end users.



Administrator Tasks for Delivering WebOS Apps to End Users

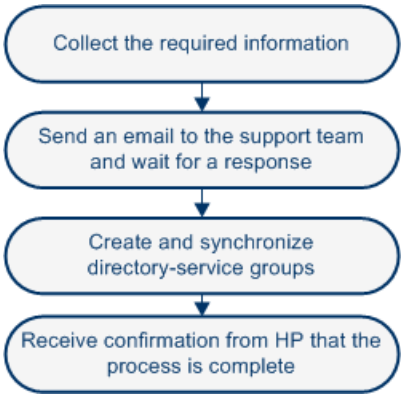
The following chart illustrates your role in enabling your organization's apps to reach end users.



For details, see "Deploying Apps to the WebOS Catalog" on page 45.

Prerequisites for Using the WebOS Catalog

Before you can add apps to the WebOS catalog and make these apps available to your users, you need to register your company with HP so that you can integrate your Enterprise Portal with HP Anywhere, as follows:



For a diagram illustrating the integration, see "How HP Anywhere Integrates with Your WebOS Catalog and Users" on page 44.

Step 1: Collect the Required Information for Integration with the Enterprise Portal

The first step is to prepare the information required to integrate the Enterprise Portal with HP Anywhere.

Company information:

Legal entity name:
Legal entity type:
DUNS (Data Universal Numbering System) number:
Company size:
Company Web site:
Phone number of the main switchboard:
Company logo: (Attach the file to the email message (step 2 below). The file type must be PNG or JPG, and the maximum dimensions are 200 pixels wide by 100 pixels high.)

Company address:

Country:

Street address:
City or town:
State or province:
Zip code or postal code

Contact information for the HP Anywhere representative at your company:

First and last name:
Department and title:
Phone number:
Email address:

Contact information for a representative in your company's legal department:

First and last name:
Title:
Phone number:
Email address:

Information about the identity provider (certificate authority) for HP Anywhere:

Name of the identity provider:
URL of the identity provider:
A SAML signing certificate (.crt file). (Zip the file and attach it to the email message. For details,see "Creating SAML Certificates for the WebOS Catalog" on page 53.)
Password for the certificate, if applicable:

Information about the top-level directory-service group that was created for HP Anywhere:

Group name for the enterprise administrators group: (Enterprise administrator permissions will be manually assigned to this group, so that members of the group can log in to the Enterprise Portal.)

Enterprise Portal login credentials for three Enterprise Portal users:

The following must be valid email addresses for user types..

User name (email address) of an enterprise administrator (for example, ep_enterprise_ admin@mycompany.com):
User name (email address) of a developer administrator (for example, ep_developer_ admin@mycompany.com):
User name (email address) of a developer (for example, ep_developer@mycompany.com):

Step 2: Send an Email Request for Integration with the Enterprise Portal

Send an email message containing the information in step 1 above to:
HPWS-HPASupport@hp.com

Tip: You can copy/paste the information in step 1 into an email.

- Include the word “Onboarding” in the subject line.
- Include the information listed in step 1 in the body of the email message.
- Include the attachments (the company logo and zipped certificate file).

A member of the support team will contact you if any additional information is required.

After receiving your email, the team creates instances of the software and database elements that run the Enterprise Portal, Account Services, and Application Catalog for your enterprise.

This process takes approximately three business days, after which .the team will contact you regarding the remaining steps needed to complete the integration process.

Step 3: Create and Synchronize the Directory-Service Groups

1. Create directory-service user groups for users that can view and access the apps to be stored in the WebOS catalog.
2. After these groups are synchronized with HP Anywhere, notify the person that contacted you that the groups are ready.

Step 4: Receive Confirmation that Three Enterprise Portal Users are Ready

After confirming a successful synchronization of the groups with HP Anywhere, the team creates the three Enterprise Portal users for which you provided usernames above.

Following the creation of the Enterprise Portal users, the team will contact you to say that the process is complete. You can now use the Enterprise Portal and Application Catalog.

How HP Anywhere Integrates with Your WebOS Catalog and Users

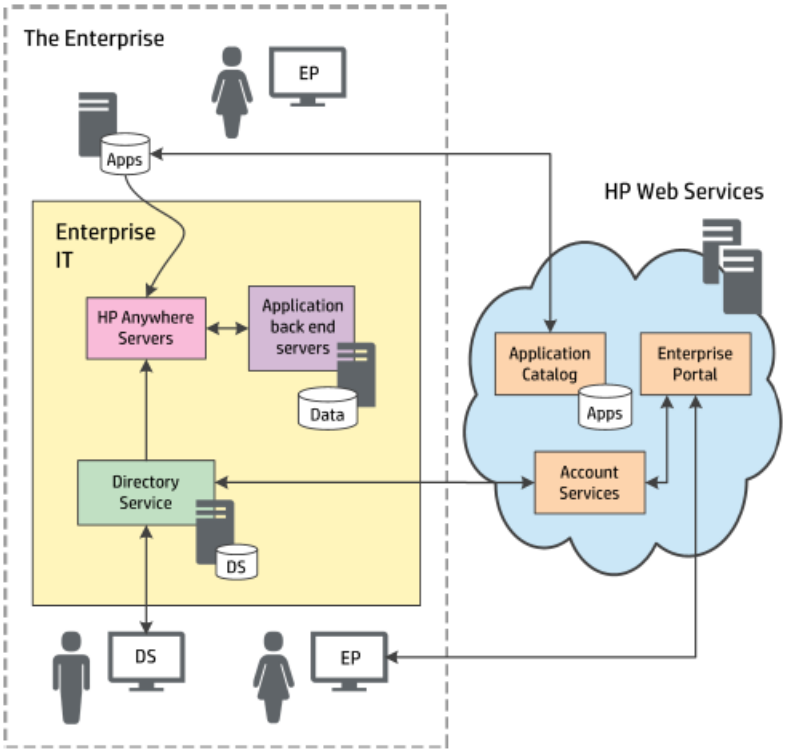
Registering your enterprise enables HP to integrate HP Anywhere with your company's apps and users:

Enterprise Portal. Your Enterprise Portal runs at HP and communicates with other parts of HP Anywhere running at HP.

Account Services. The Account Services communicate with your IT infrastructure to obtain information about group members and to authenticate Enterprise Portal users.

Application Catalog. The Application Catalog (WebOS Catalog) contains the apps that your enterprise has chosen to make available to enterprise users for use on their mobile devices.

The following diagram illustrates the integration between HP Anywhere are displayed in the cloud in the diagram below:



Deploying Apps to the WebOS Catalog

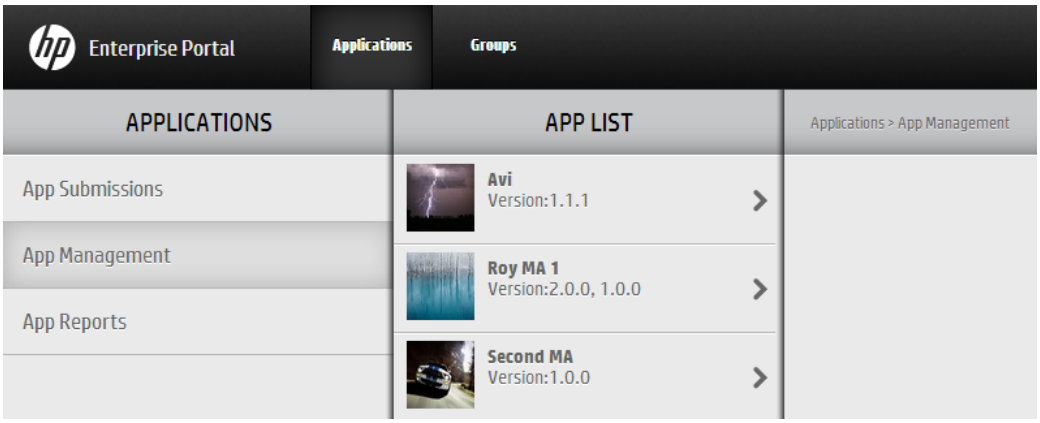
After you integrate the Enterprise Portal with HP Anywhere (as described in "WebOS Catalog" on page 37), you can deploy apps to the WebOS catalog and enable end users to access them.

To deploy an app to the WebOS Catalog:

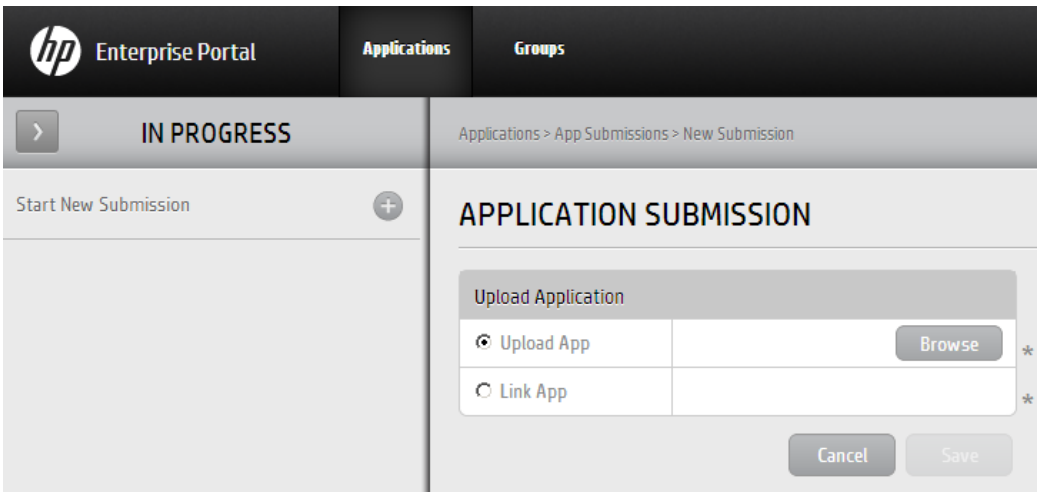
1. Submit the app to the Enterprise Portal.

   a. Log in to the Enterprise Portal using the credentials you received when setting up the integration between the Enterprise Portal and HP Anywhere.

   b. Click the **Applications** tab at the top of the window if it is not already open. The App Management tab opens by default.



   c. In the Applications pane, click the **App Submissions** tab. The Application Submission pane opens.



   d. Click the **+** button next to **Start New Submission**. Then select **Upload App** and click

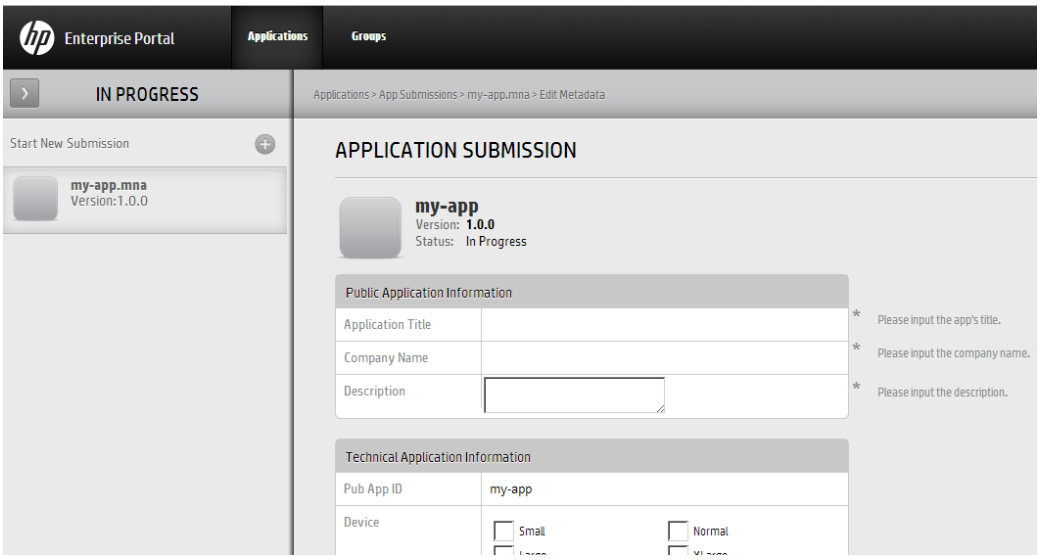
Browse to browse to the app package in the file system and upload it.

> **Note:** Make sure that the app name matches the naming conventions for app packages (see "Appendix A: Naming Conventions for Apps in the WebOS Catalog" on page 57) and that it has an **.mna** extension. (Rename the app in the file system prior to upload, if needed.)
>
> **Example:** *my-app.mna*

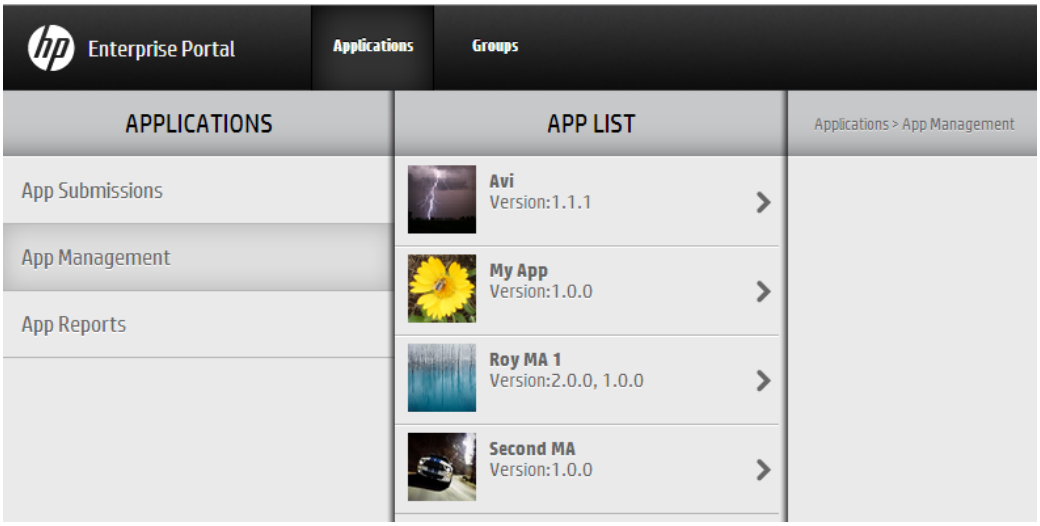
e. Click **Save**. Then click **Yes** in the confirmation box to begin the submission process. The Enterprise Portal validates the app and perfoms checks, such as:

- Verifies that the file type is MNA
- Verifies that the file structure and folders are valid
- Verifies that the app ID is unique in the Enterprise Portal

f. In the Application Submission pane, enter the relevant information.



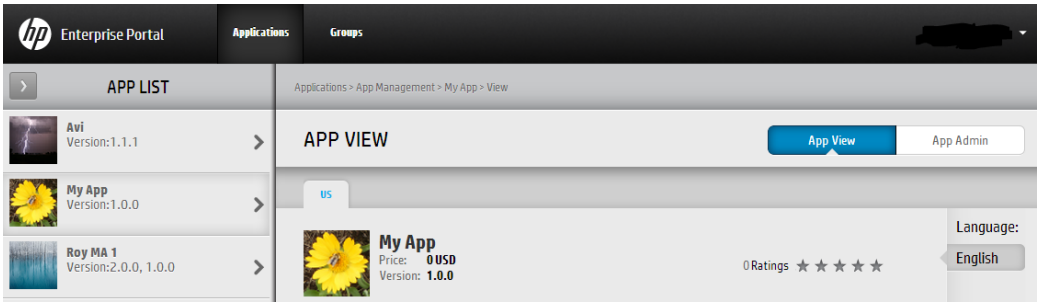
g. Click **Save**. Then click **Yes** in the confirmation box to complete the submission process. The app is added to the **App List** under **App Management**.



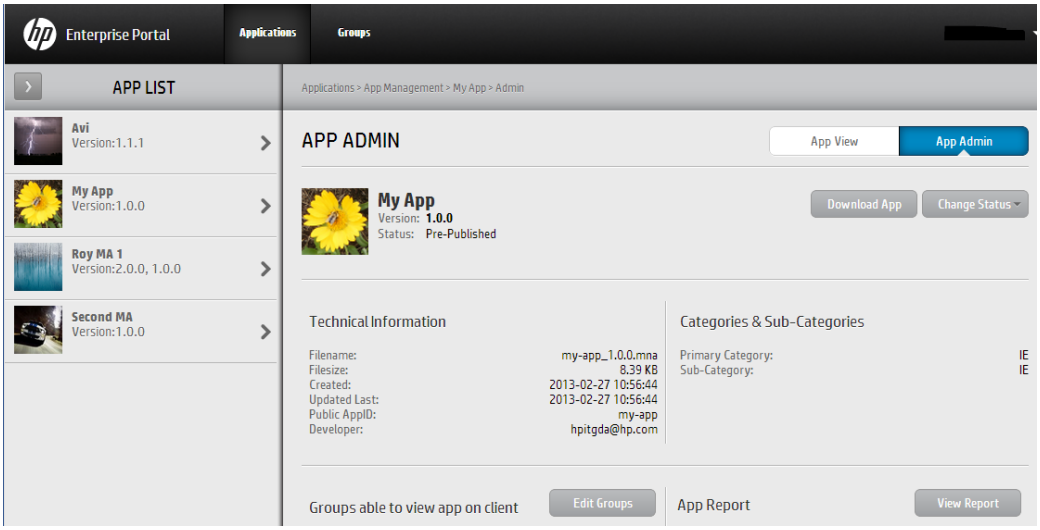
2. Define the groups that can access the app:

   a. In the Applications pane, select **App Management**.

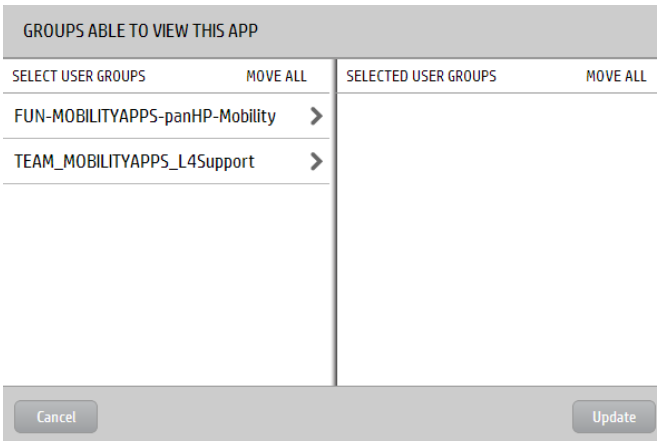
   b. In the App List pane, select the submitted app. The app is displayed in the App View pane.



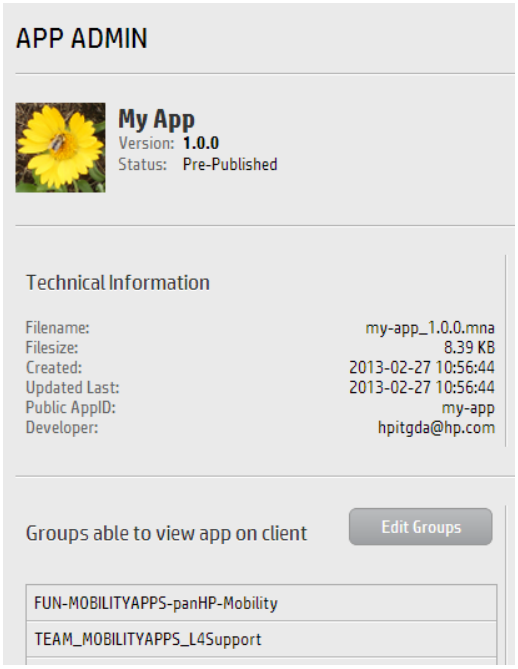
   c. In the App View pane, click **App Admin**. The App Admin pane opens.



d. Click **Edit Groups**. The **Groups Able to View This App** box opens displaying the list of user groups. This list is populated by HP Anywhere and is synchronized every 24 hours.



e. Move the relevant groups to the Selected User Groups pane on the right and click **Update**. The groups are added to the App Admin pane.

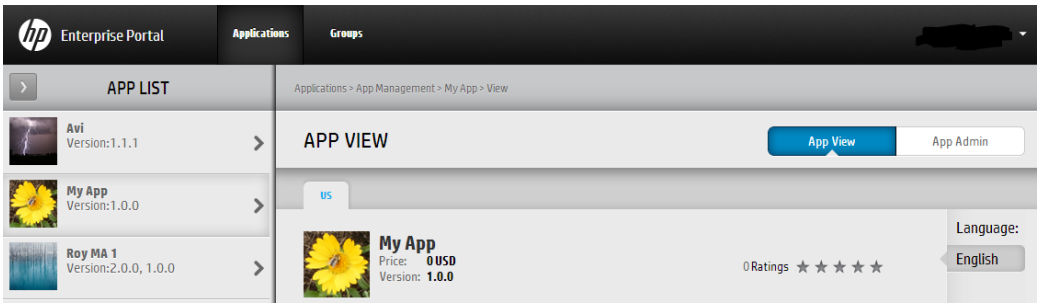


Note: If needed, notify the person responsible for adding apps to the HP Anywhere WebOS catalog that the app is ready to be deployed on HP Anywhere.

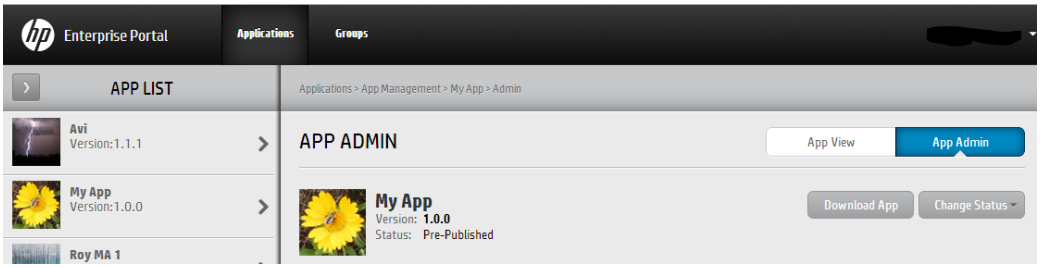
3. Download the app from the Enterprise Portal:

   a. In the Applications pane, select **App Management**.

   b. In the App List pane, select the submitted app. The app is displayed in the App View pane.



   c. In the App View pane, click **App Admin**. The App Admin pane opens.



d. Click **Download App** and save the app to a convenient location in the file system. The app is saved with an appended version number (as defined in the ***<app_name>*-descriptor.xml** file), for example, *my-app_1.0.0.mna*.

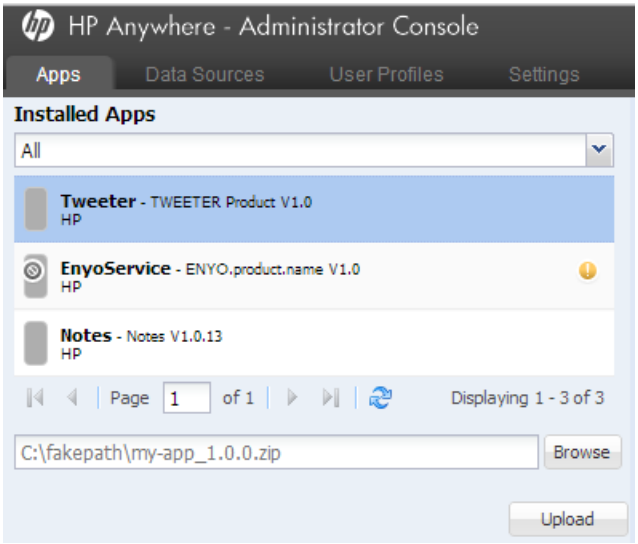
e. Rename the app's **.mna** extension to **.zip**.

4. Upload the app to the Administrator Console.

a. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 17.

b. **The first time you upload an app:** In the General Settings tab of the Administrator Console, navigate to **Catalog settings** and verify that **Catalog flavor** is set to **WEBOS**. If you change this value, you must restart the server for the change to take effect.

c. In the Apps tab of the Administrator Console, click the **Browse** button. In the Open dialog box, browse to and select the relevant *<app name>.zip* file and click **Open**.



d. Click **Upload**.

e. In the confirmation box, click **Yes**. The app uploads and is deployed automatically, and the new app is added to the list of **Installed Apps**

Note: If the deployment fails, check the **hpanywhere-stderr** log file in: <*HP Anywhere installation folder*>\tomcat\logs

5. Set the data source for the app, as described in "Defining a Data Source for an App" on page 68.

6. Define any app-specific settings:
   a. In the Apps pane of the Administrator Console, select the app you want to enable.

   b. In the right pane, select **Settings** and modify the values, as needed.

7. Enable the app in the HP Anywhere Administrator console:

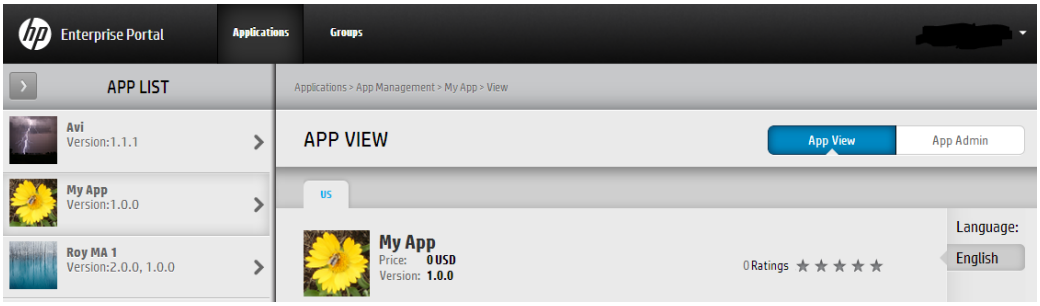
   a. In the Apps pane of the Administrator Console, select the app you want to enable.

   b. In the right pane, click **Enable**. The app is accessible to end users after the next synchronization between the Enterprise Portal and HP Anywhere.

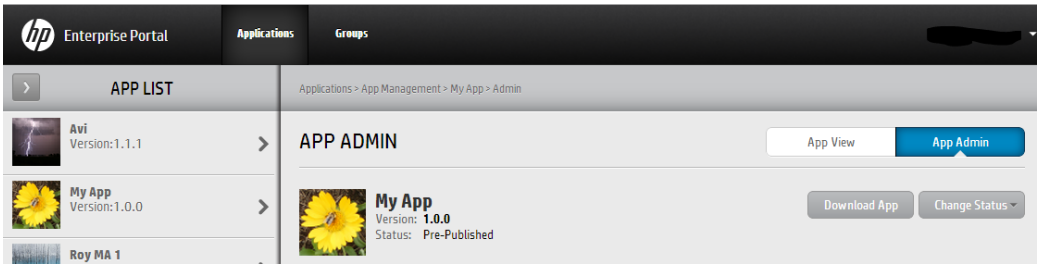
8. Publish the app to the WebOS catalog for end users via the Enterprise Portal.

   a. In the Applications pane of the Enterprise Portal, select **App Management**.

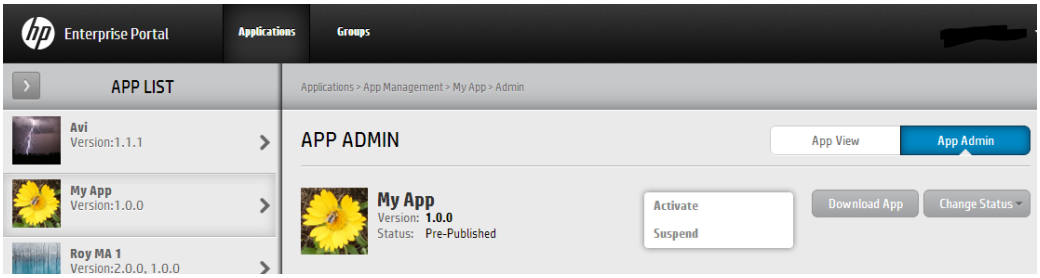
   b. In the App List pane, select the submitted app. The app is displayed in the App View pane.



   c. In the App View pane, click **App Admin**. The App Admin pane opens.



   d. Click **Change Status** and select **Activate**.



The app will be available on HP Anywhere after the next synchronization with HP Anywhere, which occurs every 24 hours.

Creating SAML Certificates for the WebOS Catalog

To work with a WebOS catalog, you need to use SAML certificates.

To create SAML certificates:

1. Run **CreateSamlSelfSignedCertificate.bat** from:
   <HP Anywhere installation folder>/scripts directory. This batch file creates two certificate files under **../jre/lib/security**:

   - keystore.jks - contains the full certificate (public/private peer)
   - hpapublic.cer (password – hpapwd) contains public key for WEBOS

2. To apply the newly generated certificate (or if you have your own certificates), set the relevant properties in **<HP Anywhere installation folder>/conf/saml.properties** file. For example:

```
keyStoreType=JKS
keystoreName= hpasaml
keyStorePassword=hpapwd
privateKeyPassword= hpapwd
algorithmName=http://www.w3.org/2000/09/xmldsig#rsa-sha1
lookForKeyStoreInClasspath=false
privateKeyDefaultAliasName=hpasaml
certificateDefaultAliasName=hpasaml
keyStorePath=../jre/lib/security/keystore.jks
recipient=https://token.palmws.com
audienceURI=https://www.palmws.com
issuer=https://HPAnywhere.com
```

Upgrading App Versions in the WebOS Catalog

You can update the WebOS catalog to include an upgraded (replacement) app version, when needed.

To upgrade an app version in the WebOS catalog:

1. Open the Enterprise Catalog, select the app you want to upgrade, and navigate to the App Admin pane. For details, see steps 1 and 2 in "Deploying Apps to the WebOS Catalog" on page 45

2. Click **Full Update**. (Available only if the app was activated (set to Published status) at least once.)

3. Submit the replacement version to the WebOS catalog. For details, see step 1 in "Deploying Apps to the WebOS Catalog" on page 45.

4. Download the app from the Enterprise Portal in preparation for upload to the Administrator Console and the WebOS catalog in HP Anywhere. For details, see step 4 in "Deploying Apps to the WebOS Catalog" on page 45.

5. In the HP Anywhere Administrator Console, disable the app by selecting it in the Apps tab, and, on the right side of the window, clicking **Disable**.

6. Remove files from the previous app version from the HP Anywhere server, as follows:
   a. Stop the HP Anywhere server.

   b. Browse to: ***<HP Anywhereinstallation folder>*/tomcat/webapps**

   c. Delete the following:

      - **<app_name> folder**
      - **<app_name>.WAR file**
      - **<app_name>.ZIP file**

   d. Start the HP Anywhere server.

7. Upload the app to the Administrator Console. For details, see step 5 in "Deploying Apps to the WebOS Catalog" on page 45.

   Note: Make sure the version of the app you are uploading is different from the previously uploaded version.

8. In the Administrator Console,enable the app by selecting it in the Apps tab, and, on the right side of the window, clicking **Enable**.

9. Publish the app in the Enterprise Portal if you suspended it. For details, see step 3 in "Deploying Apps to the WebOS Catalog" on page 45.

Remove an App from the End User WebOS Catalog

After you install an app on the HP Anywhere server or the Enterprise Portal, you cannot uninstall it, but you can make it unavailable to non-administrator end users in any of the following ways:

- **Disable the app for all end users simultaneously via the HP Anywhere Administrator Console.**

  a. In the Administrator Console, select the app in the Apps tab.

  b. On the right side of the window, click **Disable**.This removes the app from the My Apps page in the HP Anywhere client.

- **Disable the app for all end users simultaneously via the Enterprise Portal.**

  a. In the Applications pane, select **App Management**. Then, in the App List pane, select the app that you want to remove.

  b. On the right side of the window, click **Change Status** and then click **Suspend**.

- **Remove the association with specific user groups in the Enterprise Portal.**

  a. In the Applications pane, select **App Management**.

  b. In the App List pane, select the app that you want to remove.

  c. On the right side of the window, click **App Admin**.

  d. Click **Edit Groups**. Move the groups you want to remove to the left pane and click **Update**.

Note: When you disable an app, it is no longer available to end users. However, you can still see the app in the list of **Installed Apps** in the Administrator Console, and you can still access it. For example, you may want to test it or re-enable it.

Appendix A: Naming Conventions for Apps in the WebOS Catalog

This section lists the Enterprise Portal naming conventions for apps in the WebOS catalog.

Item	Naming Conventions
App Packages	• Must be unique in the Enterprise Portal and in the HP Anywhere Administrator Console's list of apps • Must not exceed 2048 characters • File name must be in the following format: <AppID>_<version>_*.mna • Can contain the following characters: lower-case letters (a-z), upper-case letters (A-Z), digits (0-9), period (.), and hyphen (-) • Can use an underscore (_) only to separate the public app ID and version
App Names	• Must be unique in the Enterprise Portal and in the HP Anywhere Administrator Console's list of apps • Must begin with a lower-case letter • Must not exceed 128 characters • Can contain the following characters: lower-case letters (a-z), upper-case letters (A-Z), digits (0-9), period (.), and hyphen (-)
Version Numbers	• Must contain three, period-separated sets of numbers, for example: 1.0.32 • Each set must contain between 1-4 digits, for example: 1.234.5678 • 0.0.0 is not allowed

Chapter 6

Default Catalog

The HP Anywhere administrator is responsible for managing the Default catalog, including:

- Uploading apps to the HP Anywhere server via the Administrator Console to add them to the catalog
- Enabling apps after configuring their required data sources and settings (if any)
- Associating apps with LDAP groups so that end users can access the apps
- Disabling any apps that you do not want end users to access

Each time you upload a new version of an app to add to the catalog, it overwrites the previous version, so that only the latest installed version is available.

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

To add an app to the default catalog:

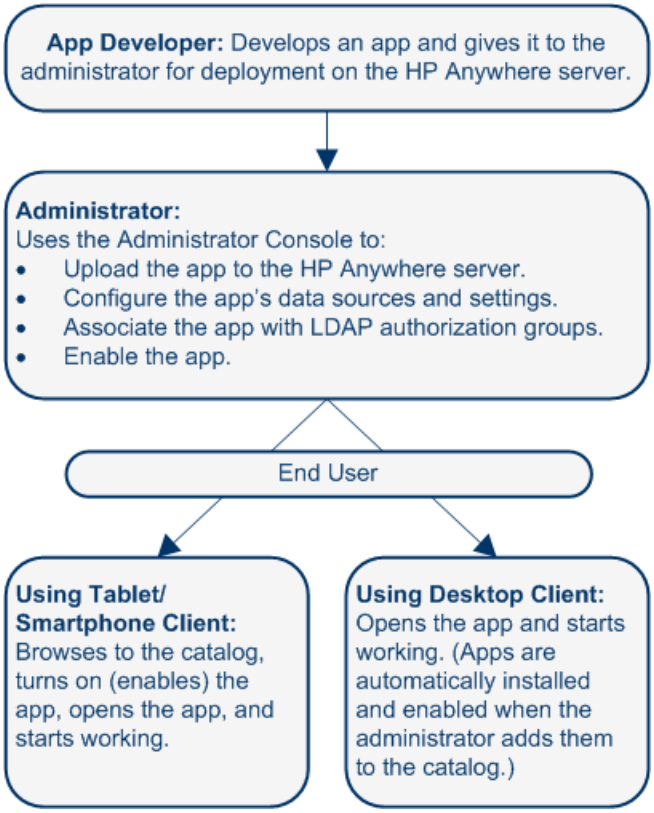
1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 17.
2. Install the app, as described in "Uploading Apps to the Default Catalog" on page 62.
3. Define a data source for the app, if needed. For details, see "Defining a Data Source for an App" on page 68.
4. Modify the app settings, if needed, as described in "Defining Global and App-Specific Settings" on page 67.
5. Associate LDAP authorization groups with each app,as described in "Defining LDAP Groups for HP Anywhere" on page 15
6. Enable the app, as described in "Enabling an App for End Users" on page 65.

Apps in Default Catalog—from Developer to End User

The administrator manages the app lifecycle for end users via the Administrator Console.This section describes the development-to-delivery flow for apps and the steps that you need to perform to provide your end users with access to each app.

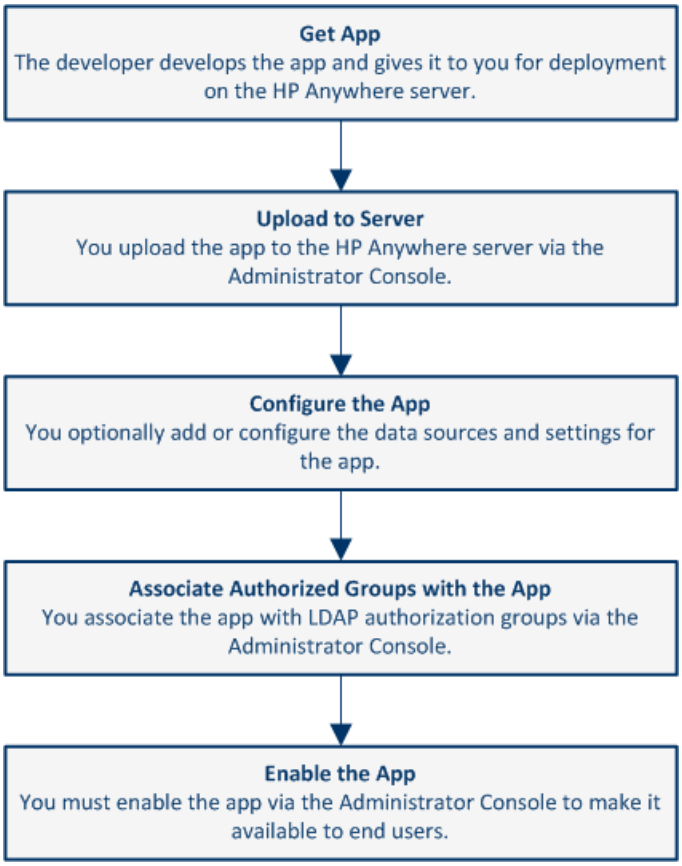
Development-to-Delivery

The following chart illustrates how your organization's apps reach end users.



Administrator Tasks for Delivering Apps to End Users

The following chart illustrates your role in enabling your organization's apps to reach end users.



For details, see:

- "Uploading Apps to the Default Catalog" on next page
- "Defining Global and App-Specific Settings" on page 67
- "Defining a Data Source for an App" on page 68
- "Associating LDAP Authorization Groups with Apps" on page 64
- "Enabling an App for End Users" on page 65

Uploading Apps to the Default Catalog

The first step in making apps available to end users is to upload them to the HP Anywhere server. You do this in the Administrator Console.

After you upload an app, it is immediately available to users with administrator privileges. This enables you to test it, or otherwise use the app before you enable it for other, non-administrator end users.

To upload an app to the HP Anywhere server:

1. Open the Administrator Console. For details, see "Logging In and Out of the Administrator Console" on page 17.

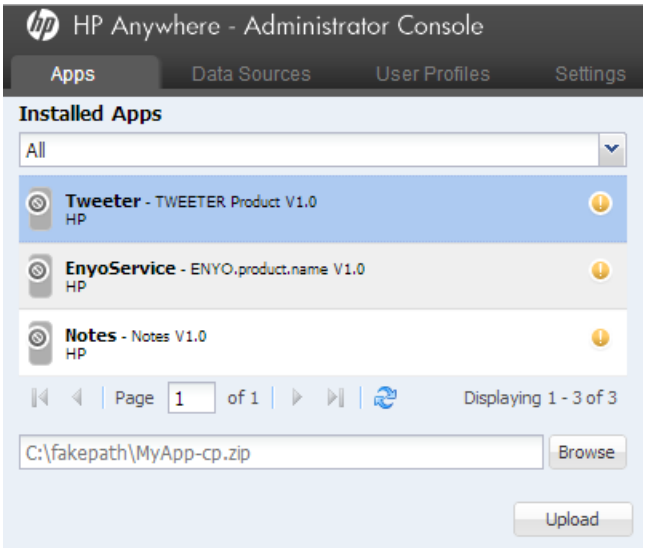
2. **The first time you upload an app:**

   a. In the General Settings tab of the Administrator Console, navigate to **Catalog settings** and verify that **Catalog flavor** is set to **DEFAULT**.

   b. Make sure that the LDAP prerequisites are met. For details, see "LDAP Configuration Prerequisites for HP Anywhere" on page 15.

3. Get the app .zip file from the developer.

4. In the Apps tab of the Administrator Console, click the **Browse** button. In the Open dialog box, browse to and select the relevant *<App name>.zip* file and click **Open**.



5. Click **Upload**.

6. In the confirmation box, click **Yes**. The app uploads and is deployed automatically, and the new app is added to the list of **Installed Apps**.

Tip: If the deployment fails, check the **hpanywhere-stderr** log file in <*HP Anywhere installation folder*>\tomcat\logs.

Upgrading App Versions in the Default Catalog

You can update the WebOS catalog to include an upgraded (replacement) app version, when needed.

To upload a different app version to the HP Anywhere server:

1. Stop the HP Anywhere server.
2. Browse to: ***<HP Anywhereinstallation folder>*/tomcat/webapps**
3. Delete the following:
   - **<app_name> folder**
   - **<app_name>.WAR file**
   - **<app_name>.ZIP file**
4. Start the HP Anywhere server.
5. Upload the replacement app, as described in "Uploading Apps to the Default Catalog" on page 62.

   Note: Make sure the version of the app you are uploading is different from the previously uploaded version.

Tip: If the deployment fails, check the **hpanywhere-stderr** log file in <*HP Anywhere installation folder*>\tomcat\logs.

Associating LDAP Authorization Groups with Apps

Apps are mapped to end users via LDAP authorization groups. This enables you to assign apps to end users according to their organizational roles or other relevant criteria, instead of assigning apps to end users individually.

For details on defining LDAP groups, see "Defining LDAP Groups for HP Anywhere" on page 15.

To associate one or more LDAP authorization groups with an app:

1. Make sure that that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 17.
2. In the Apps tab, select an app.
3. On the right-side of the window, select the **Associated Authorization Groups** tab and click **Add Groups**. The Add Authorization Groups dialog box opens.

4. Select the LDAP groups that you want to associate with the app and click **Add**.

> **Tip:** You can select multiple groups by pressing and holding the **Ctrl** key.

All users that are assigned to the groups you selected can access the app when it is set to **Enable**.

Enabling an App for End Users

When you enable an app, it becomes available to end users in any LDAP authorization group with which the app is associated.

Before enabling an app, you must ensure that the relevant configuration is set. For example, you may need to configure an app's data source or modify app-specific settings.

> **Note:** After you install an app on the HP Anywhere server, you cannot uninstall it, but you can make it unavailable to end users, as described below.

To enable an app so that users can access it from the default catalog:

1. Make sure that that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 17.
2. In the Apps pane of the Administrator Console, select the app you want to enable.
3. Make sure that all relevant app configurations are set. For example, you may need to:
   - Define any app-specific settings by modifying the values for the app in the **Settings** tab in the right pane.
   - Set the data source for the app, as described in "Defining a Data Source for an App" on page 68.
4. Make sure that the app is selected in the Apps tab. Then, in the right pane, click **Enable**.

To remove an app from a user's default catalog:

1. Make sure that that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 17.
2. Do one of the following:
   - Disable the association with the app for all end users simultaneously.
     i. In the Administrator Console, select the app in the Apps tab.
     ii. On the right side of the window, click **Disable**.This removes the app from the catalog and the My Apps page in the HP Anywhere client.

- Remove the association with any or all LDAP authorization groups.

  i. In the Apps tab of the Administrator Console, select the app that you want to remove.

  ii. On the right-side of the window, select the Associated Authorization Groups tab.

  iii. Position your mouse over an authorization group and click the **X** next to the group name. The LDAP authorization group is no longer associated with the app. This removes the app from the catalog and the My Apps page in the HP Anywhere client.

Note: When you disable an app, it is no longer available to end users. However, you can still see the app in the list of **Installed Apps** in the Administrator Console, and you can still access it. For example, you may want to test it or re-enable it.

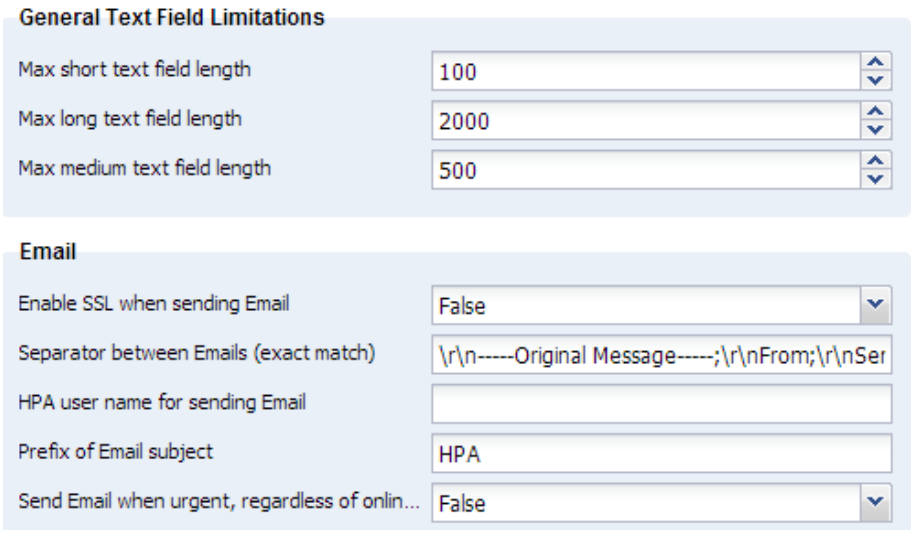
Defining Global and App-Specific Settings

Before you enable apps for end users, you must ensure that all required settings are defined. You do this in the Settings area of the Administrator Console, where you can view and define:

- **General Settings.** Global HP Anywhere settings that affect the entire system.
- **<App>.** Each app can have its own system settings, which are created by the app developer.

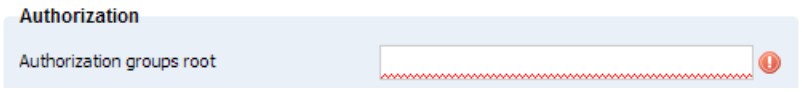
Settings are organized into group areas.

The following shows an example of some of the parameters for the HP Anywhere **General Settings**:



Each parameter displays a tooltip containing a description and an indication of when changes to this parameter take effect.

Mandatory parameters are shown in red. For example:



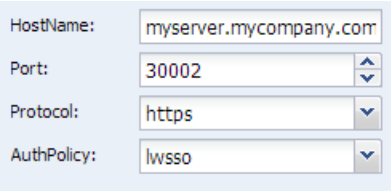
To update the value of a parameter:

1. Make sure that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 17.
2. Navigate to the relevant field and enter a value or select a value from the drop-down list.
3. Click **Save**.

Defining a Data Source for an App

Apps often need to access a server to retrieve and upload data. You can define one or more servers as the data source for an app.

A data source may include information such as: *Host Name*, *Port*, *Protocol*, and *Authentication Policy*. A data source instance defines a single occurrence of the information content. For example:



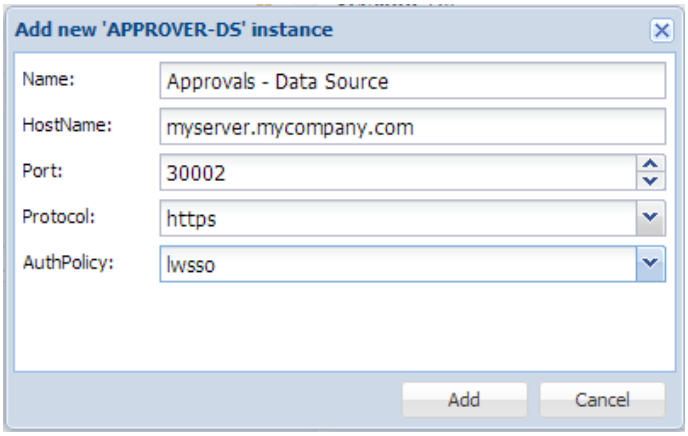
Developers define the data source requirements when they create an app.

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

Note: If no data source is defined for the app, a yellow exclamation point (!) is displayed next to the app name.

To add a new data source:

1. Make sure that that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 17.
2. In the Administrator Console, do one of the following:
   - In the Data Sources tab, select an app. Then, in the right pane, click the **Add Instance** button.
   - In the Apps pane, select an app. Then, in the right pane, select the **Data Source Configuration** tab and click the **Add Instance** button.
3. In the dialog box that opens, enter the parameter values, for example:



4. Click **Add**. The instance is displayed in the Data Source Configuration tab and is now available for the app's use.

Visibility Settings for Activities

Activity visibility settings are privacy settings that specify whether activities are visible to all users in your organization or only to actual activity participants. Activities can be set to:

Private. Only participants that are currently included in the activity can view the activity. Search results for private activities are displayed only to activity participants.

Public. Any user can search for and view an activity that is defined as public.

You set the global visibility settings for activities using the Administrator Console. You can specify the default visibility settings, and whether users are allowed to change the visibility settings for an activity.

To set the default visibility settings for all activities:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 17.
2. In the Settings tab of the Administrator Console, select **General Settings** (in the left pane).
3. In the right pane, navigate to the Activities group area and set the following:

Field	Description
Allow private activities only	Specifies whether end users can define activities as public. ▪ **True**. ○ All activities that end users create are private and are accessible only to activity participants. ○ End users cannot change private activities to public. ▪ **False**. (Default) End users can set an activity to **public** or **private**.

Field	Description
Default created activity visibility	The default for all new activities. ▪ **PRIVATE**. ○ All new activities are set to private. ○ If **Allow private activities only** is set to **False**, users can set an activity to public, if needed. ▪ **PUBLIC**. (Default) ○ All new activities are set to public. ○ **Allow private activities only** (described above) must be set to **False**. ○ Users can set an activity to private, if needed.

Sending Emails from HP Anywhere

HP Anywhere can send emails, for example, if a user is not connected to the HP Anywhere client, and someone invited that user to participate in an activity.

You set the default email settings from the Administrator Console.

To enable HP Anywhere to send emails:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 17.
2. In the **Settings tab > General Settings pane**, navigate to the various fields and set their values, as needed.

Mandatory Settings

Category: Publish Channels

Field	Description
Publish Emails	Specifies whether email notifications are allowed. **Possible values:** True, False **Default:** False

Category: Email

Field	Description
Email sending host	The URL of the SMTP email server. You can use the default port, or you can specify a port, as follows: *<server>:<port>*

Category: Email, continued

Field	Description
Enable SSL when sending email	Specifies whether to send via SMTP or SMTPS. If SMTPS, requires a certificate for the server. When you install HP Anywhere, the installation automatically generates a certificate for the server. If you need to manually generate a certificate, go to the JMX-Console (**Host/diamond/jmx-console > diamond > CertificateJMX service > fetching certificate from trusted server**). Make sure to restart all of the HP Anywhere nodes to make the certificate available. (Requires restart) **Possible values:** • True: Sends emails via SMTPS • False: Sends emails via SMTP **Default:** False
HP Anywhere user name for sending email	The user name for the HP Anywhere email account that is used to send emails. **Default:** N/A **Example:** <*server*>@<*company.com*>
HP Anywhere password for sending email	The user password for the HP Anywhere email account that is used to send emails. **Default:** N/A
Send email from a general name	Specifies the email user ID. **Possible values:** • True: Email is sent from a general (fake) email address. • False: Email is sent from the email of the user that posted the message. Applicable only if supported by email server. **Default:** False
Email receiving host	The URL of the receiving email server. You can either use the default port or you can specify a port, as follows: <*server*>:<*port*>

Category: Email, continued

Field	Description
Enable SSL when receiving email	Specifies whether to receive via POP3/IMAP or POP3S/IMAPS. If POP3S/IMAPS, requires a certificate for the server. When you install HP Anywhere, the installation automatically generates a certificate for the server. If you need to manually generate a certificate, go to the JMX-Console (**Host/diamond/jmx-console > diamond > CertificateJMX service > fetching certificate from trusted server**). Make sure to restart all of the HP Anywhere nodes to make the certificate available. (Requires restart) **Possible values:** • **True**: Receives emails via POP3S/IMAPS • **False**: Receives emails via POP3/IMAP **Default:** False
HPA user name for receiving email	The user name for the HP Anywhere email account that is used for replies to emails. **Default:** N/A
HPA user password for receiving email	The password for the HP Anywhere email account that is used for replies to emails. **Default:** N/A

Optional Settings

Category: Email

Field	Description
Prefix of email subject	The prefix to include in the subject line of the email (the title of the activity). **Default:** HPA **Example:** **From:** myserver@mycompany.com **Date:** Thursday, September 15, 2013 12:57 PM **To:** Lee.Johnson@mycompany.com **Subject: HPA:** An important activity

Category: Email, continued

Field	Description
Email subject prefix when failed to add participant	The prefix to include in the subject line of the email (the title of the activity). **Default:** Can't add participants -
Email subject when activity ID is not found	Relevant for replies to email. Used only if HP Anywhere cannot match the incoming email to an activity. **Default:** RE: Message delivery problem
Prefix of Snooze/Wake up email subject	The prefix to include in the subject line of the email (the title of the activity) when a snoozed activity times out. **Default:** HPA: Reminder-
Allow adding participants by email CC	Specifies whether HP Anywhere should add email email addresses that are in the CC of a reply to the activity as participants. **Default:** False
Email signature format to be removed	Specifies the format of the company email signature to remove from replies before sending the email. **Default:** ${email};${firstName} ${lastName}
Maximum timeout until sending an email (in minutes)	The number of minutes from the last email that was sent until another email is sent to offline participants. **Default:** 20

Category: Tenant Email

Email sending to external	Specifies whether to send email to external users (non-enterprise email addresses, for example, *John.Doe@gmail.com*). **Possible values:** True, False **Default:** True
External white list for sending email	A list of approved domains for sending email. Separate the domains using a semicolon (;) For example: hp.com;google.com **Default:** N/A

Email Logo Configuration

You can modify the default logo that is included in the email headers for notifications.

To change the default logo:

Replace **<*HP Anywhere installation folder*>\conf\email\logotop.jpg** with your logo (using the same name and JPG format, **logotop.jpg**).

Email Format Customization

You can modify the HP Anywhere email templates to customize the look and feel of the emails that HP Anywhere sends.

The following email templates are stored in **<*HP Anywhere installation folder*>\conf\email**:

- **Template.html**. Activity summary emails that are sent to participants.
- **replyTemplate.html**. System response email that is sent to someone that sends an email reply to a post, but the reply cannot be posted.
- **CantAddTemplate.html**. System response email that is sent when someone unsuccessfully tries to add a participant to an activity via email.

Load Balancer and Reverse Proxy Configurations

HP Anywhere integrates only with load balancers that are configured to use sticky sessions.

Note: When working with load balancers, the **Common web context for apps** field in the Administrator Console > General Settings pane (under Apps) must contain a value. For details, see "General Settings" on page 20.

Setting the Reverse Proxy

You must open the following URLs to access HP Anywhere via the reverse proxy (except as noted):

- *http(s)://<load_balancer_server_name>:<port>/onebox*
- *http(s)://<load_balancer_server_name>:<port>/diamond*
- *http(s)://<load_balancer_server_name>:<port>/bsf*
  (Mandatory for desktop mode)
- *http(s)://<load_balancer_server_name>:<port>/WebShell*
  (Optional)
- *http(s)://<load_balancer_server_name>:<port>/admin*
  (Relevant only if you want to access the Administrator Console via the reverse proxy URL)

"Alive" Indicator

You can configure the URL (status page) so that it provides a basic and limited "I'm Alive" indication for the load balancer, as follows:

http(s)://<host>:<port>/diamond/status.jsp

Note: This configuration is optional and is available only for load balancers that support it.

Modifying the Application URL (Via the HP Anywhere Administrator Console)

The application URL is configured automatically during post-installation. Sometimes, after completing the installation procedure, you may need to manually adjust the URL setting to match the load balancer URL for example, if you are working with High Availability.

To instruct HP Anywhere to use a different URL for the load balancer:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 17.
2. Select the **Settings** tab.
3. In the left pane, select **General Settings**.

4. Navigate to the Server group area and change the value of **The external URL of HPA server** to the URL of the load balancer server, for example:
   http(s)://<load_balancer_server_name>:<port>/onebox

Example of jvmRoute Configuration for AJP Protocol

If your load balancer uses the AJP protocol, you must ensure that a jvmRoute matching the worker name used in the **workers.properties** file is set.

Note: The **jvmRoute** name is case-sensitive.

For example, if you defined the following line in the load balancer:

workers.properties file

```
worker.<worker_A>.host=<node_A>
worker.<worker_B>.host=<node_B>
```

You must define the following in the server.xml file on each node (HP Anywhere server side):

server.xml in <node_A>:

```
<Engine defaultHost="localhost" jvmRoute="node_A">
[...]
</Engine>
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

server.xml in <node_B>:

```
<Engine defaultHost="localhost" jvmRoute="node_B">
[...]
</Engine>
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

HP Anywhere Lightweight Single Sign-On (LWSSO) Configuration

You can configure lightweight single sign-on for all of the HP applications installed on your server.

Note: If your enterprise does not use SiteMinder. or if you do not have any HP applications on your computer, skip to "Security Server Integration (SSI)" on page 81 instead.

To configure the HP Anywhere LWSSO init string on both the HP Anywhere Server and the backend:

1. Go to the Administrator Console, and select **Settings > Init String**.
2. Set the LWSSO init string and save the settings.

   The init string should be the same in all other applications that integrate with HP Anywhere and use the HP LWSSO.
3. Open the **%HPA_HOME%/HP/Anywhere/conf/lwssofmconf.xml** file.
4. If there are other servers integrated with HP Anywhere that use LWSSO with different domains, add a <DNSDomain> element for each such domain as follows and perform the remaining steps below:

```
<multiDomain>
  <trustedHosts>
     <DNSDomain>xxx.mycompany.com</DNSDomain>
     <DNSDomain>xxxs.mycompanyqcorp.net</DNSDomain>
     <DNSDomain>dddd.mycompany.com</DNSDomain>
  </trustedHosts>
</multiDomain>
```

5. If you have configured a Web server to have a different domain than the HP Anywhere server's domain, in the **<domain>** line marked below, change the domain to the domain of the Web server:

```
<webui>
 <validation>
   <in-ui-lwsso>
    <lwssoValidation id="ID000001">
      <domain>mywebserver.com</domain>
      <crypto cipherType="symmetricBlockCipher"
        engineName="AES" paddingModeName="CBC" keySize="256"
        encodingMode="Base64Url"
        initString="This string should be replaced"></crypto>
     </lwssoValidation>
 </validation>
```

Note: To initiate LWSSO on for all of the HP applications installed on your server, the init string must be identical in each application.

Security Server Integration (SSI)

Server Security Integration (SSI) is a framework that enables you to integrate HP Anywhere into your enterprise's SSO framework and to provide a unified sign-in experience from HP Anywhere to your enterprise's backend applications.

This section describes how to integrate your HP Anywhere server into your enterprise security infrastructure using the SSI interface. You do this by configuring your HP Anywhere server for IDM (identification management) and implementing the SSI interface.

To configure SSI:

1. Copy **idm-integration-api.jar** from **<HP Anywhere installation directory>/tomcat/lib** to your classpath.

2. Create a new class for the implementation. This class should implement the **IdentityManagementIntegration** interface. (You can optionally extend the **IdmIntegrationDefaultImpl** class in **idm-integration-api.jar**.)

3. Implement the required APIs. For details, see ***<HP_Anywhere_installation _ directory>*/Help/JavaDocs**.

4. If properties are required:

   - Add the necessary properties to **ssi-config.properties**, located in: **<HP Anywhereinstallation directory>/conf**

   - If your class extends the **IdmIntegrationDefaultImpl** class, this class already reads the properties file so you can just use these properties. Otherwise, it is your responsibility to read the properties file.

   - The first two properties in the **ssi-config.properties** file are mandatory. They determine how the token is stored in the request. Set the correct configuration for the cookie/header and the appropriate name.

5. Update the **lwssofmconf.xml**:

   Under the **webui validation** element, search for the **in-custom** element and verify that the following exists with your implementation (or add it):

```
<in-custom classname="com.hp.hpa.platform.security.integration.
                        handler.IdmIntegrationCustomHandler">
  <properties>
     <property>
        <name>idmIntegrationImplClassName</name>
         <value>add your IdentityManagementIntegration
```

```
              implementation full class name</value>
     </property>
  </properties>
</in-custom>
```

Example of validation element:

```
<validation>
  <in-ui-lwsso>
    <lwssoValidation id="ID000001">
        <domain/>
        <crypto cipherType="symmetricBlockCipher"
                    engineName="AES" paddingModeName="CBC"
                    keySize="256"
                    encodingMode="Base64Url"
                    initString="abc"/>
    </lwssoValidation>
  </in-ui-lwsso>
  <in-custom classname="com.hp.hpa.platform.security.
            integration.handler.IdmIntegrationCustomHandler">
    <properties>
        <property>
            <name>idmIntegrationImplClassName</name>
            <value>com.hp.hpa.platform.security.integration
                  .impl.IdmIntegrationSiteminderImpl
            </value>
        </property>
    </properties>
  </in-custom>
  <authenticationPoint refid="ID000002"/>
  <validationPoint refid="ID000002"
            validationPointID="validationPointID"
            authenicationPointServer="bsf.war"/>
</validation>
```

Example of Web Service inbound element:

```
<inbound>
  <restURLs>
       <url>.*/population.*</url>
       <url>.*/services/.*</url>
       <url>.*/rest/.*</url>
       <url>.*/populate/.*</url>
       <url>.*/api/tenant/.*</url>
```

```
      <url>.*/api/solution/.*</url>
  </restURLs>

  <default>
  </default>
  <service service-pattern=
   ".*/population.*" service-type="rest">
    <in-lwsso enabled="true" refid="ID000001"/>
    <remoteAuthentication
       classname="com.hp.sw.bto.ast.security.lwsso.ws.handlers.
        BSFBasicAuthenticationRemoteAuthenticationHandler">
        <properties>
           <property>
             <name>basicAuthenticationChallenge</name>
             <value>xBasic</value>
           </property>
        </properties>
     </remoteAuthentication>
                <in-lwssoAutoCreate enableAutoCookieCreation="true"
enableUserReplacement="true" refid="ID000002"/>
  </service>

  <service service-pattern=".*/services/.*"
           service-type="rest">
    <in-custom classname="com.hp.hpa.platform.security.
            integration.handler.IdmIntegrationCustomHandler">
        <properties>
           <property>
              <name>idmIntegrationImplClassName</name>
              <value>com.hp.hpa.platform.security.integration.
                      impl.IdmIntegrationSiteminderImpl</value>
           </property>
        </properties>
    </in-custom>
    <in-lwsso enabled="true" refid="ID000001"/>
    <remoteAuthentication
       classname="com.hp.sw.bto.ast.security.lwsso.ws.handlers.
        BSFBasicAuthenticationRemoteAuthenticationHandler">
        <properties>
           <property>
             <name>basicAuthenticationChallenge</name>
             <value>xBasic</value>
           </property>
        </properties>
     </remoteAuthentication>
```

```
   <in-lwssoAutoCreate enableAutoCookieCreation="true"
                       enableUserReplacement="true"
                       refid="ID000002"/>
</service>

<service service-pattern=".*/rest/.*" service-type="rest">
  <in-custom classname="com.hp.hpa.platform.security.
           integration.handler.IdmIntegrationCustomHandler">
      <properties>
         <property>
            <name>idmIntegrationImplClassName</name>
            <value>com.hp.hpa.platform.security.integration.
                   impl.IdmIntegrationSiteminderImpl</value>
            </property>
      </properties>
  </in-custom>
  <in-lwsso enabled="true" refid="ID000001"/>
  <remoteAuthentication classname=
       "com.hp.sw.bto.ast.security.lwsso.ws.handlers.
       BSFBasicAuthenticationRemoteAuthenticationHandler">
         <properties>
            <property>
               <name>basicAuthenticationChallenge</name>
               <value>xBasic</value>
            </property>
         </properties>
  </remoteAuthentication>
  <in-lwssoAutoCreate enableAutoCookieCreation="true"
                       enableUserReplacement="true"
                       refid="ID000002"/>
</service>

<service service-pattern=".*/populate/.*"
           service-type="rest">
  <in-custom classname="com.hp.hpa.platform.security.
           integration.handler.IdmIntegrationCustomHandler">
        <properties>
           <property>
              <name>idmIntegrationImplClassName</name>
              <value>com.hp.hpa.platform.security.integration.
                     impl.IdmIntegrationSiteminderImpl</value>
           </property>
        </properties>
  </in-custom>
  <in-lwsso enabled="true" refid="ID000001"/>
```

```
    <remoteAuthentication classname=
          "com.hp.sw.bto.ast.security.lwsso.ws.handlers.
          BSFBasicAuthenticationRemoteAuthenticationHandler">
    </remoteAuthentication>
    <in-lwssoAutoCreate enableAutoCookieCreation="true"
           enableUserReplacement="true" refid="ID000002"/>
  </service>

  <service service-pattern=
           ".*/api/tenant/.*" service-type="rest">
      <in-lwsso enabled="true" refid="ID000001"/>
      <in-validate/>
  </service>

  <service service-pattern=".*/api/solution/.*"
           service-type="rest">
     <in-lwsso enabled="true" refid="ID000001"/>
     <in-validate/>
  </service>
</inbound>
```

6. Create a .jar containing the implementation you created and any other resources you need.
7. Put this .jar in the **<*HP_Anywhere_installation_directory*>/tomcat/lib** directory.
8. Restart the HP Anywhere server for the changes to take effect.

Chapter 7

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 89

To use push notifications, you must 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)

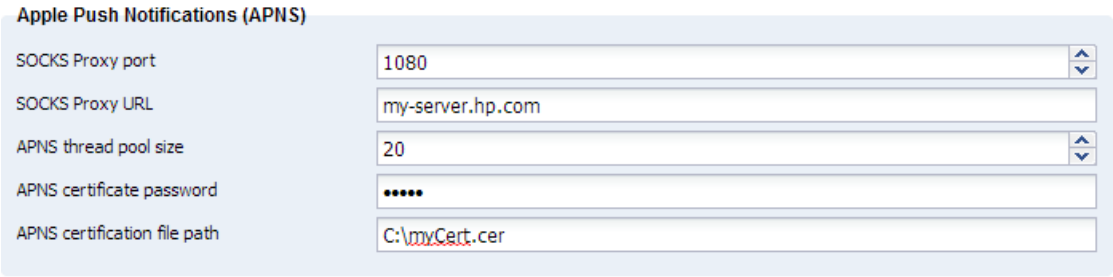
Before configuring push notifications for iOS devices, you must update the relevant settings in the Administrator Console.

To configure push notifications:

1. In the Administrator Console, select the **Settings** tab.
2. In the **General Settings pane > Publish Channels area**, set **Push Notifications** to **True**.
3. In the **General Settings pane > Apple Push Notifications (APNS) area**, set the value of the following fields:
   - **SOCKS Proxy port** (Optional)
   - **SOCKS Proxy URL** (Optional)
   - **APNS certificate password**
   - **APNS certification file path** – This is the full path to the file on the HP Anywhere server, for example “C:\myCert.cer”.

Note: Apple Push Notification Service requires an Internet connection. It uses SOCKS protocol with ports 2195 and 2196 for sending push notifications. You can either configure a proxy or open these ports in your firewall.

Example:



4. Use JMX to test the connection as follows:

   a. Go to: **http://<host>:<port>/diamond/jmx-console/HtmlAdaptor?action=inspectMBean&name=Diamond%3Aname%3DPushNotificationsJMX**.

   b. Click **Invoke**.

   c. Verify that you receive a success message.

If the connection test fails, try the troubleshooting tips in "Troubleshooting Push Notifications" on page 91.

Configure Push Notifications for Android Devices (Google)

Before configuring push notifications for Android devices, you must update the relevant settings in the Administrator Console.

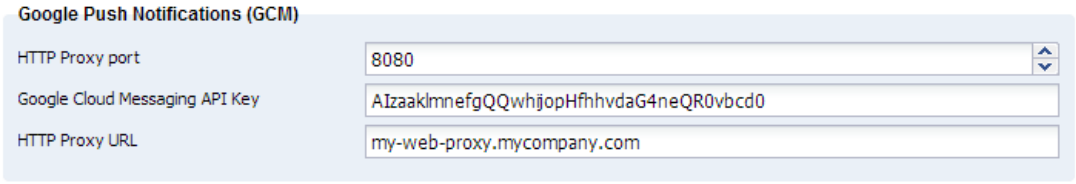
To configure push notifications:

1. In the Administrator Console, select the **Settings** tab.
2. In the **General Settings pane > Publish Channels area**, set **Push Notifications** to **True**.
3. In the **General Settings pane > Google Push Notifications (GCM)**, set the value of the following fields:

   - **HTTP Proxy port** (Optional). The port number of the proxy server behind which the HP Anywhere backend server runs.
   - **Google Cloud Messaging API Key**. API key for pushing device notifications with Google Cloud Messaging service.
   - **HTTP Proxy URL** (Optional). The host name of the proxy server behind which the HP Anywherebackend server runs.

Note: Google Cloud Messaging requires an Internet connection. It uses HTTPS protocol with port 443 for sending push notifications. You can either configure a proxy or open this port in your firewall.

Example:



Troubleshooting Push Notifications

Apple

Problem: APNS test connection fails

Solution 1: You may need to define a SOCKS proxy to get an 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 to reload the certificate. (HP Anywhere reads the certificate upon startup or when settings are updated.)

Android

Problem: GCM test connection fails

Solution: You may need to define an HTTP proxy to get an 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 receive push notifications only from apps on an Android device after a Google account is set.


Java™
COMPATIBLE