HP Anywhere

Windows

Software Version: 10.11

Administrator Guide

Document Release Date: January 2013

Software Release Date: December 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.

Apple and the Apple logo are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

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.

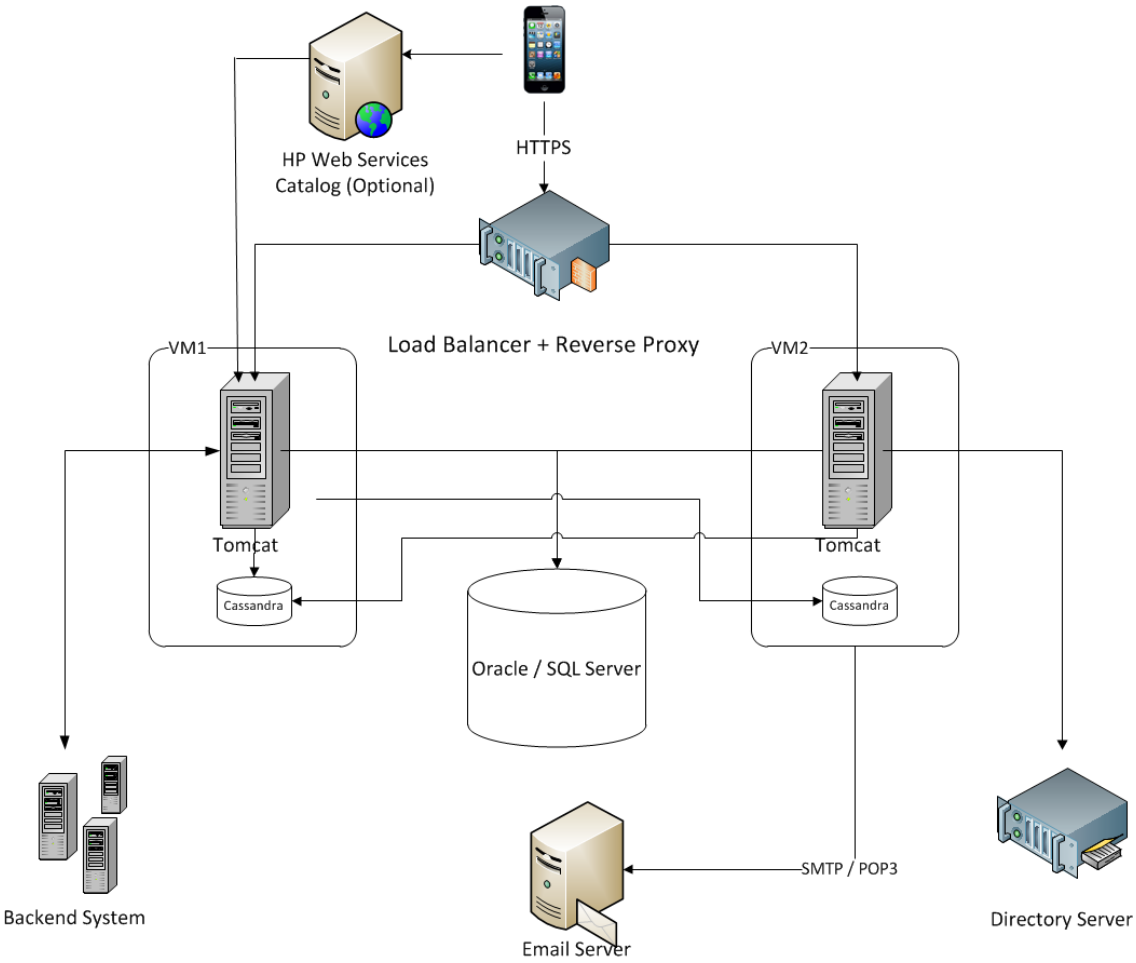
For details on defining a white list or black list for users and/or devices, see *HP Anywhere – Restricting User/Device Connections (Black/White List)* on the HP Software Product Manuals Web site.

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.

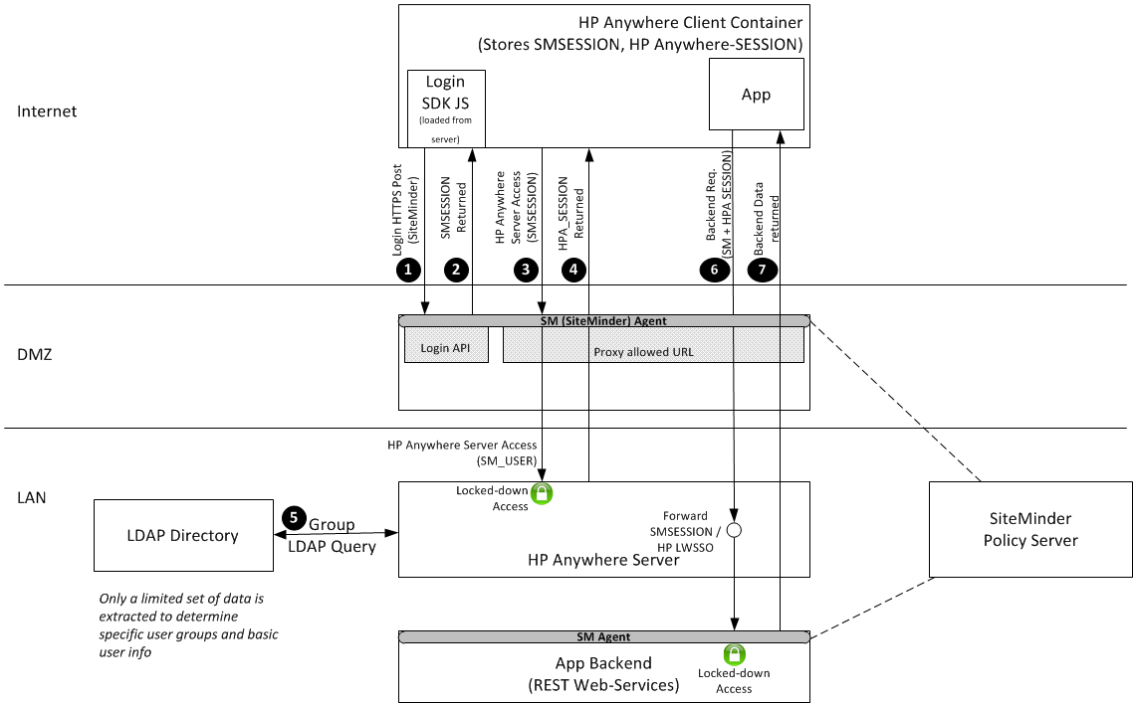


HP Anywhere Login Security with SiteMinder

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

This section describes how to configure LDAP for use with HP Anywhere. It contains the following topics:

Note:

- Many of LDAP the configuration steps require modifying the attributes in the **external-ldap.properties** file.

  You must be familiar with the LDAP structure to customize the attributes in the **external-ldap.properties** file.

  Role-related attributes in the **external-ldap.properties** file are not relevant and should be ignored.

- For details on creating LDAP administrators and defining LDAP groups for HP Anywhere, see "LDAP Configuration Prerequisites for HP Anywhere" in the HP Anywhere Administrator Guide.

LDAP Configuration and Authentication

This section describes how to configure the HP Anywhere server to authenticate users using LDAP.

To configure LDAP authentication, you need to:

1. Customize the LDAP Server as an External Repository.
2. In the HP Anywhere Administrator Console, change **User repository type** (in Foundation Settings) to **"ldap"**.
3. Assign the admin role to users.

   For details, see the "LDAP Groups for HP Anywhere" in the *HP Anywhere Administrator Guide*.

Customize the LDAP Server as an External Repository

The external-ldap.properties file contains the LDAP customization parameters.

To connect to the LDAP server, do the following:

> **Note:** This section describes how to work with Apache Directory Studio, but you can use any tool that displays the LDAP structure.

1. Download and install the Apache Directory Studio LDAP browser from http://directory.apache.org/studio/.
2. Open the LDAP browser and click the **New Connection** button from the Connections tab located at the bottom left hand side of the application window.
3. Enter the LDAP host name (**Hostname**) and port number (**Port**).
4. Select the appropriate encryption level (**Use SSL encryption (ldaps://)**).
5. Click **Check Network Parameters**.
6. Click **Next**.
7. Select one of the following authentication methods:
   - No Authentication - useAdministrator=false
   - Simple Authentication- useAdministrator=true
8. Click **Finish**. The connection is automatically tested.
9. Ift SSL is selected, the certificate trust window may open. If applicable, select **View Certificate**. Ensure that the certificate appears in the Java key store used by HP Anywhere.
10. Update the LDAP attributes in the **external-ldap.properties** file as follows:

Attribute	Description
ldapHost	LDAP host name
ldapPort	LDAP port number

Attribute	Description
enableSSL	You must set this parameter to True - Use SSL connection to LDAP. For details on the importing the SSL certificate, see "Configure LDAP Over SSL (LDAPS)" on page 23.
useAdministrator	True: Use simple authentication False: No authentication
ldapAdministrator	LDAP user distinguished name (defined if useAdministrator = True)
ldapAdministratorPassword	LDAP user password (defined if useAdministrator = True)
isAGroupAttribute	(Optional) Specifies the type of user management repository. By default, HP Anywhere expects **ou=groups**. If you know that your group's distinguished name (DN) is different from the default, you can add this attribute to the **external-ldap.properties** file. Recommended settings: ▪ Sun ONE: **isAGroupAttribute = ou=groups** ▪ Active Directory: Set according to the DN shared by all groups, for example: **isAGroupAttribute =cn=group** ▪ If you are not sure what the group's DN is, but you do know that it is not **ou=groups**, you can set a generic value, such as **isAGroupAttribute = cn =**. This may affect performance, though.

Configure the User Search Parameters

Update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties. This configures the connection to the LDAP server:

Attribute	Description
usersBase	LDAP Base Distinguished Name (DN) for users search specifying the location in the LDAP directory where the search begins.

Attribute	Description
usersScope	LDAP search scope. Defines how exactly the search under the usersBase location should be performed. • SCOPE_BASE: Searches the usersBase level only • SCOPE_ONE: Searches the direct children of the usersBase level only (does not search the usersBase level itself) • SCOPE_SUB: Searches the usersBase and its whole subtree
usersFilters	LDAP filter for users search

Configure the User Objects Class

The following parameters are used to define the LDAP vendor or customized implementation-specific objects that represent the users objects.

To map the users configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties.

Attribute	Description
usersObjectClass	LDAP object class representing users object.
usersUniqueIDAttribute	User's unique ID LDAP attribute name.
usersLoginNameAttribute	User's login name LDAP attribute name.
Optional Attribute	**Description**
usersDisplayNameAttribute	User's display name LDAP attribute name.
usersFirstNameAttribute	User's first name LDAP attribute name.
usersLastNameAttribute	User's last name LDAP attribute name.
usersEmailAttribute	User's email LDAP attribute name.
usersPreferredLanguageAttribute	User's preferred language LDAP attribute name.
usersPreferredLocationAttribute	User's preferred location LDAP attribute name.
usersTimeZoneAttribute	User's time zone LDAP attribute name.
usersDateFormatAttribute	User's date format LDAP attribute name.
usersNumberFormatAttribute	User's number format LDAP attribute name.
usersWorkWeekAttribute	User's work week LDAP attribute name.
usersTenantIDAttribute	User's tenant ID LDAP attribute name.
usersPasswordAttribute	User's password LDAP attribute name.

Group Search

The following properties define the search mechanism that is implemented on LDAP groups. There are two sets of properties: the first for regular groups and the second for root groups.

To display only a limited number of groups, restrict the root groups search criteria appropriately. The same search criteria for both root and non-root groups can also be used. This configuration is recommended when the overall number of groups is small.

Check Group Search Configuration Properties

To map the groups configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties.

Attribute	Description
groupsBase	LDAP Base Distinguished Name (DN) for groups search. Only groups under this DN in the LDAP hierarchy are returned from the search.
groupsScope	LDAP search scope for groups search. Defines how exactly the search under the groupsBase location should be performed. • SCOPE_BASE: search space contains a single entry pointed by the groupsBase • SCOPE_ONE: search space contains the groupsBase and its direct children only • SCOPE_SUB: search space contains the groupsBase and its whole sub tree
groupsFilter	LDAP filter for groups search. The only valid values are rootGroupsBase, rootGroupsScope, or rootGroupsFilter.
rootGroupsBase	LDAP Base Distinguished Name (DN) for groups search. Only groups under this DN in LDAP hierarchy are returned from the search
rootGroupsScope	LDAP search scope for groups search. Specifies how the search under the gropusBase location should be performed. • SCOPE_BASE: search space contains a single entry pointed to the rootGroupsBase • SCOPE_ONE: search space contains the rootGroupsBase and its direct children only • SCOPE_SUB: search space contains the rootGroupsBase and its whole sub tree
rootGroupsFilter	LDAP filter for groups search

Group Object Class (Vendor-Dependent LDAP)

The following properties are used to define the LDAP vendor or custom implementation-specific objects representing static groups. More than one comma-separated object class is supported. In this scenario, the user can define the appropriate corresponding comma-separated attribute names.

To map the groups configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties:

Attribute	Description
groupsObjectClass	LDAP object class representing the group object.
groupsMembersAttribute	Groups members LDAP attribute name. This multi-value attribute contains the full distinguished names (DNs) of static group members.
Optional Attribute	**Description**
groupsNameAttribute	Groups unique name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as groupsDisplayNameAttribute.
groupsDisplayNameAttribute	Groups display name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as groupsNameAttribute.
groupsDescriptionAttribute	Groups description LDAP attribute name. The attribute contains the groups' description.
enableDynamicGroups	Boolean attribute for enabling dynamic groups. If the value of this attribute is true, dynamic groups are searched. Note that enumerating members of very large dynamic groups may be time consuming. **Recommended:** False
dynamicGroupsClass	LDAP object class representing dynamic group object.
dynamicGroupsMemberAttribute	Dynamic group members LDAP attribute name. This attribute contains the LDAP search URL. The values returned by this LDAP search URL are considered dynamic group members.
dynamicGroupsNameAttribute	Dynamic group unique name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as dynamicGroupsDisplayNameAttribute.
dynamicGroupsDisplayNameAttribute	Dynamic group display name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as dynamicGroupsNameAttribute.
dynamicGroupsDescriptionAttribute	Dynamic group description LDAP attribute name. This attribute contains the groups description.

Groups Hierarchy

The Groups Hierarchy attributes defines whether HP Anywhere relates to LDAP server groups hierarchy information.

Attribute	Description
enableNestedGroups	Enable support of nested groups. If support of nested groups is disabled, subgroups of a group are not searched.
maximalAllowedGroups HierarchyDepth	Maximal allowed depth of groups hierarchy. No groups are searched beneath this level.

Advanced Configuration

The advanced configuration attributes are used for fine-tuning the LDAP connection.

Attribute	Description
ldapVersion	LDAP protocol version. Possible values are: • 3 (default) • 2 (for old versions of LDAP)
baseDistinguishNameDelimiter	**Base DN delimiter.** Symbol used in configuration when using multiple base DNs for users or groups or users search. Note that this symbol must not appear as part of the base DN used in this configuration. If it appears in the base DNs, change the default value to some other symbol.
scopeDelimiter	**Scope delimiter.** Symbol used in configuration when using multiple scopes for users or groups search. This symbol must not be including in the scope name used in this configuration. If it is included in the scope name, change the default value to some other symbol.
attributeValuesDelimiter	Symbol used in configuration when included in multiple attribute names of users or group. Make sure that this symbol does not appear as part of attributes used in this configuration. If it appears in attribute names, then change the default value to some other symbol.

Configure LDAP Over SSL (LDAPS)

For HP Anywhere to work with LDAP, you must enable it to run over SSL (LDAPS).

Import your LDAP server certificate into the keystore:

<*HP_Anywhere_installation_directory*>\jre\bin\keytool -import -file <path_of_certificate_file> -keystore "<*HP_Anywhere_installation_directory*>\jre\lib\security\cacerts"

1. In the HP Anywhere Administrator Console, change **User repository type** (in Foundation Settings) to **"ldap"**.
2. Restart the server.

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
- "LDAP Groups for HP Anywhere" on the facing page

LDAP Admin Users for HP Anywhere

HP Anywhere interacts with users via LDAP. 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

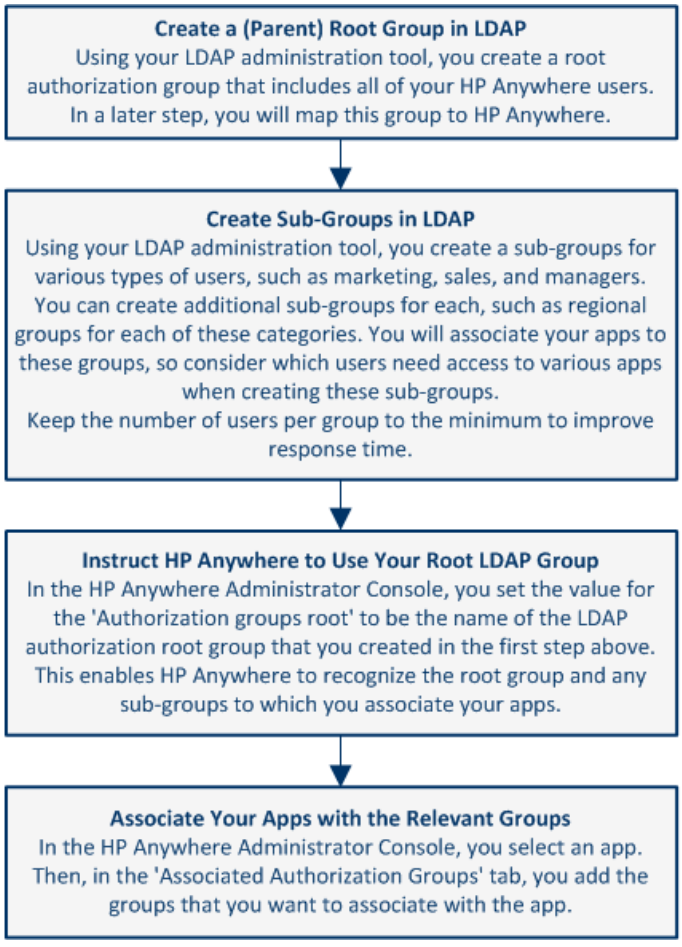
2. Repeat for each LDAP user that needs administrator privileges.

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. 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.

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. For example, suppose you create a parent LDAP group for all sales personnel, and you create sub-groups for various regions. If an app is associated with an LDAP group for a particular region, only users in that region's group can access the app. If you associate that same app with the parent group (for all sales personnel), then users in all regions can access the app.

The following chart illustrates the steps you need to perform to associate your HP Anywhere apps with LDAP groups.



Note: This section describes how to map an LDAP root authorization group to HP Anywhere. For details on associating apps with LDAP authorization groups, see "Associating LDAP Authorization Groups with Apps" on page 108.

To map an LDAP root authorization group to HP Anywhere:

1. In your LDAP administration tool, define the root authorization group. This is the root LDAP authorization group for all HP Anywhere users.

2. In your LDAP administration tool, create additional sub-groups that include the specific LDAP users to associate with each app. For example, for an expense report app, you may want to create a separate, region-specific sub-group for managers, for sales personnel, for technicians, and so on.

   Note: It is better to create multiple sub-groups with fewer users than fewer groups with many users.

3. In the HP Anywhere Administrator Console, do the following:
   (For details on opening the Administrator Console, see "Understanding the Administrator Console" on page 26.)

   a. Select **Settings > General Settings**.

   b. In the Authorization section, enter the case-sensitive, group name in the **Authorization groups root** text box. Use the CN value and not the full LDAP path. For example, if the group's LDAP path is *cn=hpanywhere, ou=Groups, dc=mycompany, dc=com*, enter only the value *hpanywhere*.

   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

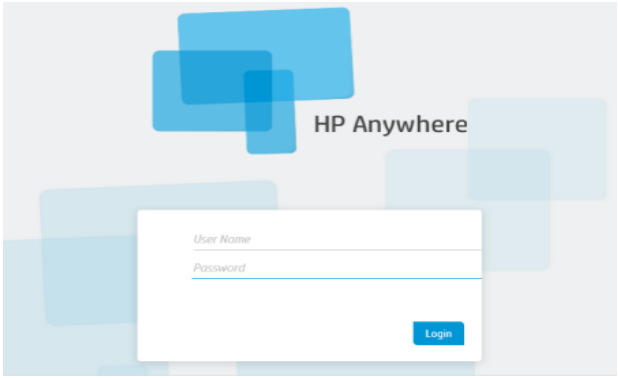
You use the Administrator Console to :

- 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
- Customize the look and feel of the HP Anywhere client app for your end users
- 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.



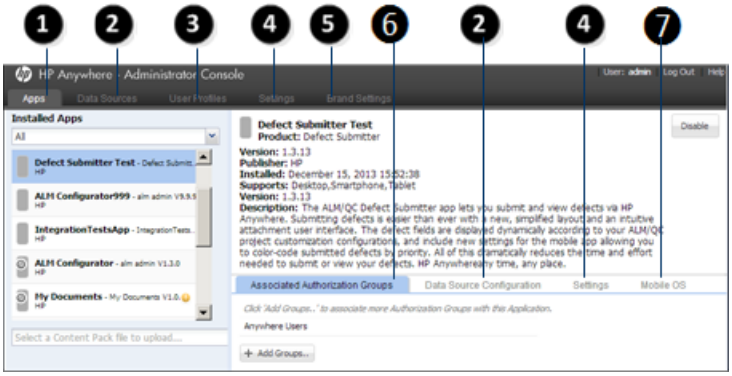
2. Enter your administrator login credentials (user name and password) and click **Login**.After your login is authenticated, the Administrator Console opens.

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 101.
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 51.
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 29.
5	**Brand Settings**	Customize the theme color and logo of the HP Anywhere client app for your end users.
6	**Associated Authorization Groups**	View and manage the associated LDAP authorization group for each app For details, see "LDAP Groups for HP Anywhere" on page 24.
7	**Mobile OS**	Select the mobile operating systems for each app in the Default catalog. For details, see "Specifying Supported Mobile Operating Systems for HP Anywhere Apps" on page 53.

Chapter 4

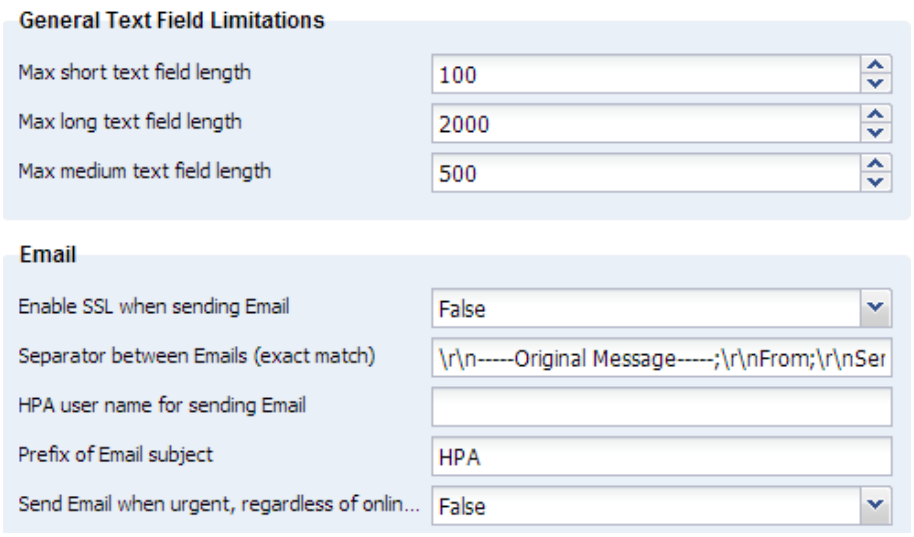
Defining Global and App-Specific Settings

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.

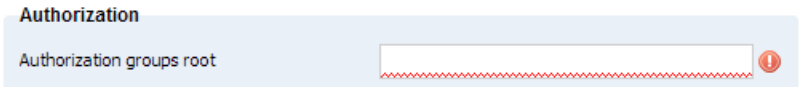
Settings are organized into group areas.

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 26.
2. Navigate to the relevant field and enter a value or select a value from the drop-down list.
3. Click **Save**.

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 26.

General Text Field Limitation

Field	Description
Max field length of short text	The maximum number of characters allowed in a short text field. **Required:** Yes **Possible values:** Integer from 1 -4000 **Default:** 100
Max field length of long text	The maximum number of characters allowed in a long text field. **Required:** Yes **Possible values:** Integer from 1-4000 **Default:** 2000
Max field length of medium text	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
Separator between emails (exact match)	Separator between email threads. **Default:** \r\n-----Original Message-----;\r\nFrom;\r\nSent from my;\r\n_____

Email, continued

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
Token expiration of email (in hours)	The time frame (in hours) during which a user can reply to an email. After the time elapses, the token expires and email replies are not accepted. Use **0** for an unlimited timeout. **Default:** 48
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 -
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
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, continued

Field	Description
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
Timeout from last post until sending an email in required mode (in minutes)	The number of minutes from the last post until an email is sent to offline participants. **Default:** 5
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
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
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>*

Email, continued

Field	Description
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 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
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
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-
Email receiving protocol	Protocol used for receiving emails. **Possible values:** imap, pop3 **Default:** pop3
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
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

Attachments

Field	Description
Maximum description length for an attachment (in characters)	Maximum number of characters that can be used in the description of an attachment. **Required:** Yes **Possible values:** 1-260 **Default:** 256
Maximum attachment size (in MB)	Maximum size of an attachment in megabytes. **Required:** Yes **Possible Values:** 1-1000 **Default:** 50
Maximum file name length for an attachment (in characters)	Maximum number of characters in file name. **Required:** Yes **Possible Values:** 1-260 **Default:** 256
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

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 total attachments size (in MB) per hour (for a user).	Maximum total size of attachments (in MB) that a user can upload for posts, profile pictures, and so on, per hour.

Profile

Field	Description
Maximum results for profile search	The maximum number of results to return when searching for a user. **Default:** 50
Profile thumbnail 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 criterion. **Default:** firstName,lastName,email
Max upload size (in MB) for profile image	The maximum size of a profile image to upload. **Default:** 10
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
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@!@#$%^&*()<>{}"?~.;:/]*$
Width of large profile image (in pixels)	The size in pixels of a large profile image **Default:** 200

Black/White List

Field	Description
Activate Black/White List	Specifies if HP Anywhere should apply a given black or white list to users and/or devices that attempt to connect to this HP Anywhere server. You manage the given list using the **provision-list** API. For details, see "User and Device Management - Restricting User/Device Connections (Black/White List)" on page 113. **Possible values:** • **True**. Activates a black or white list according to the **List Type** and **provision-list** API. This option enables you to allow or prevent specific users and/or devices from accessing HP Anywhere. If blocked users or devices try to access HP Anywhere, they receive an error message. • **False**. HP Anywhere does not consider a defined black/white list when users and/or devices attempt to log on to HP Anywhere. **Default:** False
List Type	Type of restriction list. **Possible values:** • **White**. Allows only specific users and/or devices to access HP Anywhere and its apps. Users and/or devices that are not on this list cannot access HP Anywhere. • **Black**. Prevents specific users and/or devices from connecting to HP Anywhere. All otherusers and/or devices in your organization can access HP Anywhere. **Default:** Black

Catalog Settings

Field	Description
Always check app 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**. Enables an end user to install an app on a device only if the end user is listed in an LDAP authorization group that is currently associated with that app. • **False**. Enables an end user to install an app on a device regardless of the authorization groups associated with that app. **Default:** False
URL for app details	URL for retrieving app details. If this field is blank, the default HP Web Services catalog URL is used. Relevant only when **Catalog flavor** is set to **WEB_OS**.
Enable installed app authorization	Specifies whether to filter apps by authorization groups. Relevant only when **Catalog flavor** is set to **WEB_OS**. **Possible values:** • **True** - Validates the user against the directory-service (authorization) group in the HP Web Services catalog to determine if the user is allowed to install the app. • **False** - Enables an end user to install an app on a device regardless of the directory-service groups associated with that app. **Default:** True
URL for catalog resources	URL of the resources used by the HP Web Services catalog. Relevant only when **Catalog flavor** is set to **WEB_OS**.
URL for synchronizing Authorization Groups	URL used for synchronizing authentication groups with the HP Web Services catalog. If this field is blank, the default HP Web Services catalog URL is used. Relevant only when **Catalog flavor** is set to **WEB_OS**.
Sync installed applications	Enable the HP Anywhere catalog to synchronize the installed applications when users log in. **Possible values:** True, False **Default:** True

Catalog Settings, continued

Field	Description
Catalog flavor	Defines the catalog to use for this HP Anywhere server. **Possible values:** WEB_OS, NONE, DEFAULT, INTEGRATED **Default:** Default
URL for retrieving list of installed apps	URL used for retrieving the installed apps from the HP Web Services catalog. If this field is blank, the default HP Web Services catalog URL is used. Relevant only when **Catalog flavor** is set to **WEB_OS**.
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)

Snapshots

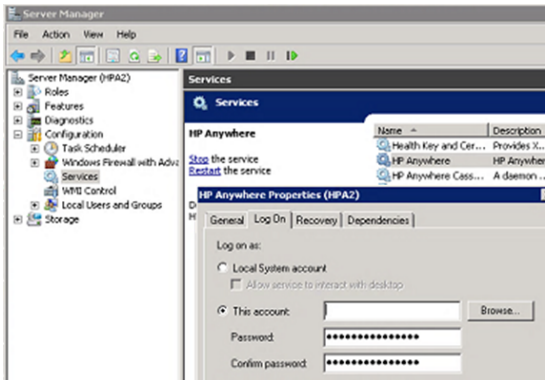
Field	Description
Diameter of small snapshots (in pixels)	Diameter of small snapshots (in pixels). **Default:** 200
Diameter of medium snapshots (in pixels)	Diameter of medium snapshots (in pixels). **Default:** 750
Diameter of snapshots for mobile (in pixels)	Diameter of snapshots for mobile (in pixels). **Default:** 50
Max snapshot image upload size (in KB)	Max snapshot upload size (in KB). **Default:** 5000
Max caching time for snapshot image in client side (in seconds)	Amount of time in seconds after which the client sends an HTTP request for the snapshot again. **Default:** 2592000
Diameter of snapshot thumbnails (in pixels)	Diameter of snapshot thumbnails (in pixels). **Default:** 100
Diameter of large snapshots (in pixels)	Diameter of large snapshots (in pixels). **Default:** 1500

Google Push Notifications (GCM)

Note: To enable push notifications to Android devices, you need a Google Cloud Messaging API key. For details on obtaining a key and instructions on enabling push notifications, see "Push Notifications for Android Devices (Google)" on page 65.

Field	Description
Google Cloud Messaging API Key	API key for pushing device notifications with the Google Cloud Messaging (GCM) service. This setting takes effect immediately after saving the settings. **Required:** No (Required when using GCM) **Default:** N/A
HTTP proxy port	The port number of the proxy server behind which the HP Anywhere backend server runs. This setting takes effect immediately after saving the settings. **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. **Required:** No (Optional when using GCM) **Possible values:** Integer from 1 to 65535 **Default:** N/A
HTTP proxy URL	The host name of the proxy server behind which the HP Anywhere backend server runs. This setting takes effect immediately after saving the settings. **Required:** No (Optional when using GCM) **Possible values:***Enter a URL string* **Default:** N/A

Logs

Field	Description
Client Log Path	The path where logs received from the client are stored. (These are the logs that users can send directly from their devices using the **Send Log** feature in the HP Anywhere client Settings.) **Default:** N/A If you leave this field blank (or if the path is not valid), received logs are automatically written to the <**HP Anywhere_installation_folder>/logs/userLog.log** file on the HP Anywhere server. Otherwise, if you specify a different path, the log file name is appended with the HP Anywhere server IP address, for example, *<HP_Anywhere_server_IP>_userLog.log*. This enables you to differentiate between logs in cases where multiple logs are written to the same location. **Note:** Validation is not performed on the path and no error message is displayed if the path is incorrect or invalid. **Tip:** When setting this field for multiple HP Anywhere servers, you may want to specify a single, accessible location on your network so that you can access logs for all servers in one central location. For example: *\\<Your_IP_address>\C$\hpa_logs\logs_from_clients\...* **Important:** Make sure that the **HP Anywhere Service** on the HP Anywhere server is run by a user that can access this file location, otherwise the logs are written to the default location. You set this in Windows, for example: **Start > Run >services.msc > HP Anywhere** service. 

Proxy Configuration

Field	Description
Scheme	Proxy server scheme for accessing HP Web Services catalog. Relevant only when **Catalog flavor** is set to **WEB_OS**.

Proxy Configuration, continued

Field	Description
Port	Proxy server port for accessing HP Web Services Catalog. Relevant only when **Catalog flavor** is set to **WEB_OS**.
Host	Proxy server host name or IP address for accessing HP Web Services Catalog. Relevant only when **Catalog flavor** is set to **WEB_OS**.

Apple Push Notifications (APNS)

Note: To enable push notifications to iOS devices, you need an APNS certificate. For details on obtaining a certificate and instructions on enabling push notifications, see "Push Notifications for iOS Devices (Apple)" on page 62.

Field	Description
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. This setting takes effect after restarting the HP Anywhere server. **Required:** No (Optional when using APNS) **Possible values:** Integer from 1 to 500 **Default:** 20
APNS certificate password	Apple's certificate password. This setting takes effect after restarting the HP Anywhere server. **Required:** No (Required when using APNS) **Possible values:***Enter a password* **Default:** N/A

Field	Description
SOCKS proxy port	SOCKS proxy port for sending notifications to iOS devices. This setting takes effect after restarting the HP Anywhere server. **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. **Required:** No (Optional when using APNS) **Possible values:** Integer from 1 to 65535 **Default:** N/A
SOCKS proxy URL	SOCKS proxy URLfor sending notifications to iOS devices. This setting takes effect after restarting the HP Anywhere server. **Required:** No (Optional when using APNS) **Possible values:***Enter a URL string* **Default:** N/A
APNS certification file path	The full path to the location where the Apple certificate is stored in the file system on the HP Anywhere server. For example “C:\myCert.cer” This setting takes effect after restarting the HP Anywhere server. **Required:** No (Required when using APNS) **Possible values:***Enter a file path on the HP Anywhere server* **Default:** N/A

Activities

Field	Description
What's Next visibility	Specifies whether to show or hide What's Next in an activity workspace. **Default:** True

Activities, continued

Field	Description
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
Minimum interval for activity indexing (in minutes)	The minimum interval in minutes between activity indexing operations. **Default:** 1
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 visibility for new 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. **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

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

Foundation Settings

Field	Description
Enable audit logs	Specifies whether to write audit logs **Possible values:** True, False **Default:** True
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
Base URL for SAAS	The URL of the SaaS server. **Possible values:** N/A **Default:** N/A
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

Server

Field	Description
Default application name	The title that appears at the top of the HP Anywhere client application. You can use this to set your own company name, for example. To customize the theme color and logo of the HP Anywhere client, use this in conjunction with Brand Settings.
Application login page	Path to the (HP Anywhere) login page on the local or remote server. You specify if the path is absolute or relative in the Relative path for application login page field. If the page is stored on a local server, the file must be under: **<HP_ Anywhere_installation_folder>\tomcat\webapps** Examples: **Relative path:** *HPALogin\js\HPALogin-build.js* **Absolute path:** *<HP_Anywhere_installation_ folder>\tomcat\webapps\HPALogin\js\HPALogin-build.js* *<myserverpath>:8080/HPALogin/js/HPALogin-build.js* *http://name.domain...../anycorrectpath/login.js*
Relative path for application login page	Specifies if the path to the application login page is relative (True) or absolute (False). Relative paths are relative to: **<HP_Anywhere_installation_ folder>\tomcat\webapps** Use this field in conjunction with Application login page.
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

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
Root authorization group	The parent LDAP root group. For details, see "LDAP Groups for HP Anywhere" on page 24. **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

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

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

Notifications

Field	Description
Comet sleep time (in seconds)	Maximum time (in seconds) that the server can delay sending a response to the client. **Default:** 22
Comet sleep time for iOS (in seconds)	Maximum time (in seconds) that the server can delay sending a response to the iOS client. **Default:** 8

Apps

Field	Description
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

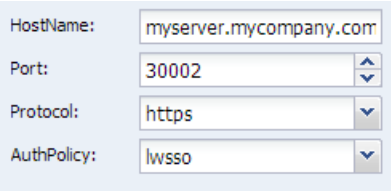
Offline Support

Field	Description
Allow HP Anywhere to work offline	Specifies whether a user can open HP Anywhere and work with HP Anywhere and any of its apps that provide offline support when there is no Internet connection. For more details, see "Enabling Offline Support" on page 55. Relevant only for smartphones and tablets. **Possible values:** True, False **Default:** True

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:

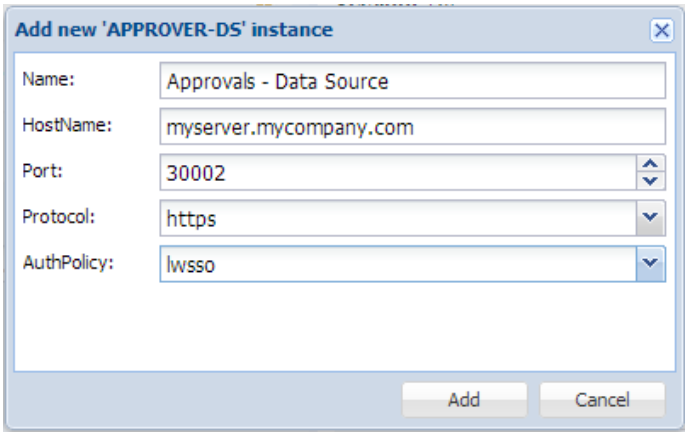
1. Make sure that that the Administrator Console is open. For details, see "Understanding the Administrator Console" on page 26.

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.

Specifying Supported Mobile Operating Systems for HP Anywhere Apps

Not all apps run on all mobile devices. This tab enables you to set the mobile operating systems that are supported for the selected app.

Note: This setting is applicable only to some catalog types. The availability of this setting depends on the selected 'Catalog flavor'.

To set the supported mobile operating systems for an app:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 26.
2. In the Apps pane, select an app.
3. In the right pane, select the **Operating System** tab. Then select the mobile operating systems for which this app is supported. You can select any, all, or none of the following:
   - iOS (selected by default)
   - Android (selected by default)
   - Windows 8 (cleared by default)
4. Click **Save** to save your changes to the server. End users see the changes to the catalog the next time they log on to HP Anywhere.

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 26.
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.

Enabling Offline Support

HP Anywhere enables you to determine if users can log on to HP Anywhere and work with their apps when their mobile devices (tablets and smartphones) are not connected to the Internet. (Only apps that provide offline support are available when there is no Internet connection. To verify which, if any, of your apps provide offline support, contact the app developer or other relevant party.)

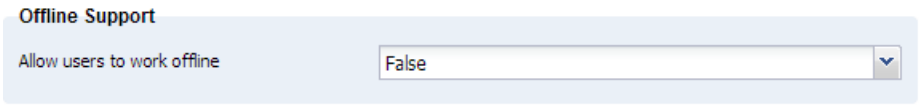
By default, offline support is not enabled.

If you enable offline support, users must set a PIN that replaces their user name and password when they log on to HP Anywhere. They set this PIN via the User Settings on their mobile devices. To ensure that users know that they need to define a PIN, an informative message opens the first few times they log on to HP Anywhere.

If you do not enable offline support, users cannot log on to HP Anywhere from their mobile devices when there is no Internet connection. Additionally, if they are already logged on to HP Anywhere and the Internet connection is lost, the device displays a message stating that there is no Internet connection when they to perform an action that requires an Internet connection, such as navigating between pages or submitting a post on the Timeline.

To enable/disable offline support:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 26.
2. In the **General Settings pane > Offline Support area**:
   - Set **Allow users to work offline** to **True** to enable offline support.
   - Set **Allow users to work offline** to **False** to disable offline support.



3. Click **Save** to save your changes.

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 26.
2. In the **Settings tab > General Settings pane**, navigate to the various fields and set their values, as needed.

Mandatory Email 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	
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

Category: Email	
Field	**Description**
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*>
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 Email 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
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	
Field	**Description**
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 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

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.

Note: For details on backing up and restoring customized email templates when upgrading the HP Anywhere server, see the section on upgrading in the HP Anywhere Installation, Configuration, and Upgrade Guide.

Push Notifications for iOS Devices (Apple)

Before configuring push notifications for iOS devices, you must obtain a an APNS certificate (iOS) and update the relevant settings in the Administrator Console.

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

To configure push notifications:

1. Open a **Service Request** from the HP Software Support Online web site (http://www.hp.com/go/hpsoftwaresupport). (Requires an HP Passport):

   a. Click **Service Request** to open the Service request manager.

   b. In the Service request manager, click **Submit a new service request** and follow the onscreen instructions.

   c. In the Service Request title, enter: **HP Anywhere Push Notification Certificate**

   d. In the description, specify whether you need a certificate for iOS, or both a certificate for iOS and a key for Android.

2. After you receive the certificate, set the required configurations in the Administrator Console.

   a. Open the Administrator Console. For details, see "Logging In and Out of the Administrator Console" on page 26.

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

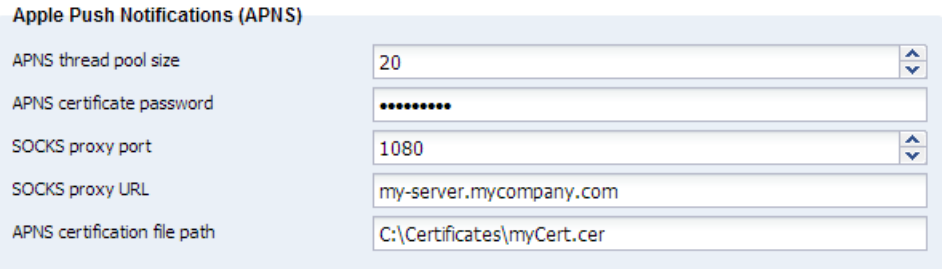
      - In the **General Settings** pane **> Publish Channels** area, set **Push Notifications** to **True**.

      - In the **General Settings** pane **> Apple Push Notifications (APNS)** area, set the value of the following fields:

Field	Description
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. This setting takes effect after restarting the HP Anywhere server. **Required:** No (Optional when using APNS) **Possible values:** Integer from 1 to 500 **Default:** 20
APNS certificate password	Apple's certificate password. This setting takes effect after restarting the HP Anywhere server. **Required:** No (Required when using APNS) **Possible values:***Enter a password* **Default:** N/A
SOCKS proxy port	SOCKS proxy port for sending notifications to iOS devices. This setting takes effect after restarting the HP Anywhere server. **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. **Required:** No (Optional when using APNS) **Possible values:** Integer from 1 to 65535 **Default:** N/A
SOCKS proxy URL	SOCKS proxy URLfor sending notifications to iOS devices. This setting takes effect after restarting the HP Anywhere server. **Required:** No (Optional when using APNS) **Possible values:***Enter a URL string* **Default:** N/A

Field	Description
APNS certification file path	The full path to the location where the Apple certificate is stored in the file system on the HP Anywhere server. For example “C:\myCert.cer” This setting takes effect after restarting the HP Anywhere server. **Required:** No (Required when using APNS) **Possible values:***Enter a file path on the HP Anywhere server* **Default:** N/A

Example:



Note: To enable an HP Anywhere app to implement push notifications:

- The app must call the Events REST API. (This is configured by the app developer.) For details, see the API Reference and the Events Sample App Cookbook.
- The HP Anywhere server must be connected to the Internet.

For a mobile device to receive push notifications from an HP Anywhere app:

- The mobile device must be configured to receive push notifications. For details, see the section on mobile notification settings in the HP Anywhere User Guide.
- The app sending the notification must be enabled on the mobile device.

Push Notifications for Android Devices (Google)

Before configuring push notifications for Android devices, you must obtain a Google Cloud Messaging API key and update the relevant settings in the Administrator Console.

To configure push notifications:

1. Open a **Service Request** from the HP Software Support Online web site (http://www.hp.com/go/hpsoftwaresupport). (Requires an HP Passport):
   a. Click **Service Request** to open the Service request manager.
   b. In the Service request manager, click **Submit a new service request** and follow the onscreen instructions.
   c. In the Service Request title, enter: **HP Anywhere Push Notification Certificate**
   d. In the description, specify whether you need a key for Android, or both a key for Android and a certificate for iOS.
2. After you receive the key, set the required configurations in the Administrator Console.

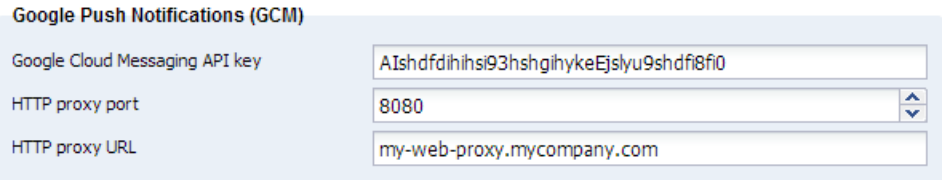
a. Open the Administrator Console. For details, see "Logging In and Out of the Administrator Console" on page 26.

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

   - In the **General Settings** pane **> Publish Channels** area, set **Push Notifications** to **True**.
   - In the **General Settings** pane **> Google Push Notifications (GCM)** area, set the value of the following fields:

Field	Description
Google Cloud Messaging API Key	API key for pushing device notifications with the Google Cloud Messaging (GCM) service. This setting takes effect immediately after saving the settings. **Required:** No (Required when using GCM) **Default:** N/A
HTTP proxy port	The port number of the proxy server behind which the HP Anywhere backend server runs. This setting takes effect immediately after saving the settings. **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. **Required:** No (Optional when using GCM) **Possible values:** Integer from 1 to 65535 **Default:** N/A
HTTP proxy URL	The host name of the proxy server behind which the HP Anywhere backend server runs. This setting takes effect immediately after saving the settings. **Required:** No (Optional when using GCM) **Possible values:***Enter a URL string* **Default:** N/A

Example:



Note: To enable an HP Anywhere app to implement push notifications:

- The app must call the Events REST API. (This is configured by the app developer.) For details, see the API Reference and the Events Sample App Cookbook.
- The HP Anywhere server must be connected to the Internet.

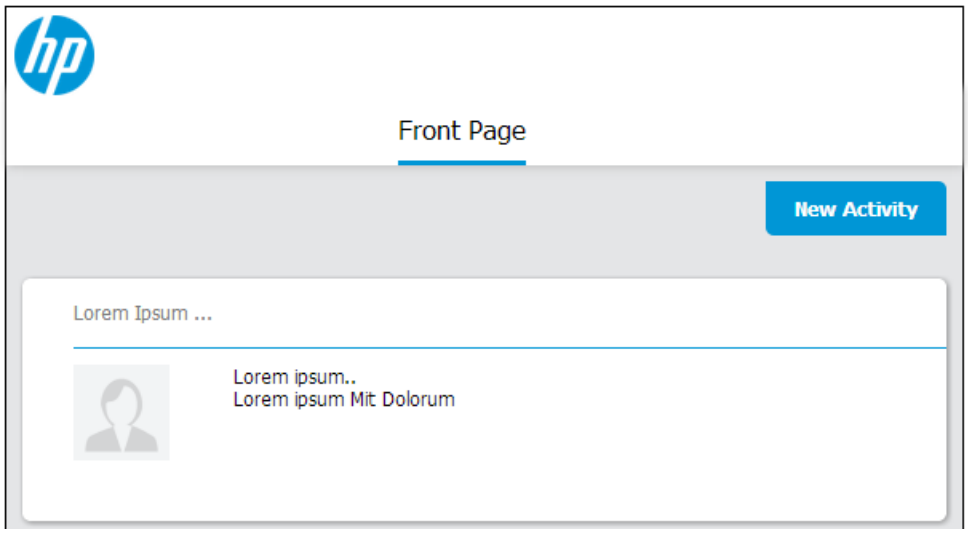
For a mobile device to receive push notifications from an HP Anywhere app:

- The mobile device must be configured to receive push notifications. For details, see the section on mobile notification settings in the HP Anywhere User Guide.
- The app sending the notification must be enabled on the mobile device.
- The mobile device must have access to a Google account.

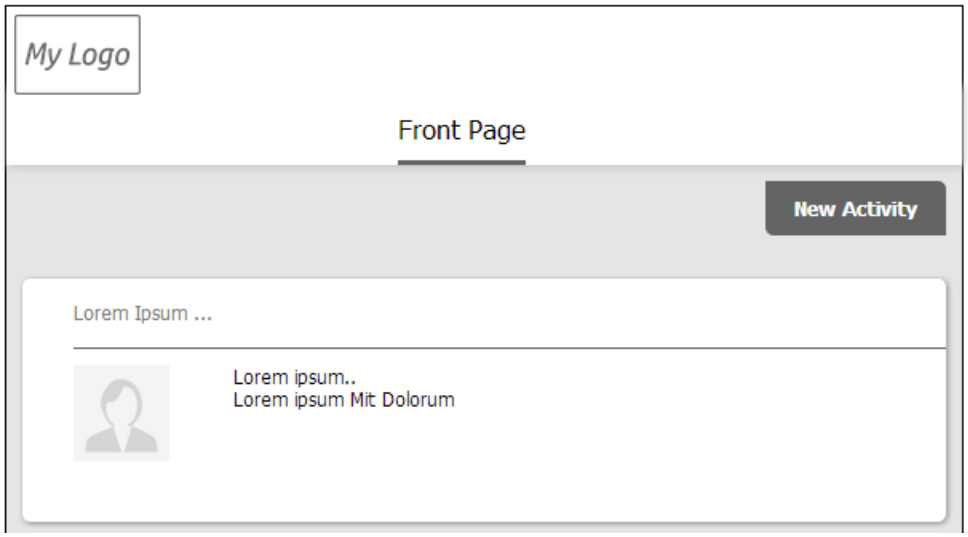
Customizing the HP Anywhere User Interface

You can customize the HP Anywhere look and feel to match your company's brand identity and align with your product set. You can apply your own logo, brand name, and theme color. (You can also design your own login page to replace the default one. For details, see "Applying Your Own Login Screen" on page 71.)

For example, you can change this:



to this:



Note: The brand name is not shown in the example above.

To customize the HP Anywhere user interface:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 26.
2. In the **Brand Settings** tab, navigate to the various fields and set their values, as needed.
3. At the bottom of the page, preview your changes to the logo and theme color, as applicable.

   Note: The **Application name** is not displayed in the preview.

4. Do one of the following:
   - Click **Save** to save your changes.
   - Click **Reset** to restore the factory settings.
   - Click **Cancel** to restore the last saved settings.

Brand Settings

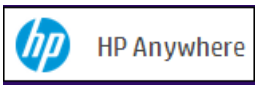
This section describes the fields in the Brand Settings pane of the Administrator Console.

For details on opening the Administrator Console, see "Logging In and Out of the Administrator Console" on page 26.

Brand Settings

Field	Description
Logo (.png)	A logo that replaces the default HP logo in the top-left corner of HP Anywhereon user devices. Logo requirements: • **File type:** .png • **Background:** Transparent • **Max height:** 57 pixels • **Max width:** 180 pixels **Note:** If the height or width exceeds the maximum allowed number of pixels, the image is resized proportionally to fit the allotted space. **Required:** No **Possible value:** File path for the logo image to upload **Default:** None **Note:** The HP logo is displayed in the preview until you select a different image file.
Theme Color (Hex)	A Hex color code, such as #000000 (black). The theme color replaces the default color of the lines and enabled buttons in HP Anywhere on user devices. **Required:** Yes **Possible value:** Any Hex color code value **Default:** #0096d6

Brand Settings, continued

Field	Description
Application name	The name of your brand/application/tag line to display to the right of the logo in HP Anywhere on user devices, for example:  **To define the application name:** 1. Browse to the **Settings** tab > **General Settings** pane. 2. Define the the value in the **Default Application Name** field. **To leave the application name blank:** 1. Browse to the **Settings** tab > **General Settings** pane. 2. Enter a space character in the **Default Application Name** field. (If you clear the field, the default application name, HP Anywhere, is displayed.) **Note:** • Relevant only for Desktop and Tablet. (The application name is not displayed on Smartphones.) • The application name is not displayed in the preview. **Required:** Yes **Possible values:** String **Default:** HP Anywhere

Applying Your Own Login Screen

By default, your users log on to HP Anywhere via the HP Anywhere login page. You can replace this login screen with your own by modifying settings in the Administrator Console.

Note: For details on creating a login page, see the documentation in the HP Anywhere Developer Zone's Resource Center .

To use your own login page:

1. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 26.
2. In the Settings tab, navigate to the **Server** section and set the values for:

- **"Relative path for application login page"** (For details, see "Relative path for application login page" on page 47.)
- **"Application login page"** (For details, see "Application login page" on page 47.)

3. Do one of the following:
   - Click **Save** to save your changes.
   - Click **Reset** to restore the factory settings.
   - Click **Cancel** to restore the last saved settings.

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 30.

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>/HPALogin*
- *http(s)://load_balancer_server_name:<port>/<common_web_context>*
  (Specify the **Common web context for apps** value from the Administrator Console > Settings > General Settings pane)
- *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 26.
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 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" />
```

Chapter 5

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:

- "HP Web Services Catalog" on page 76.
- "Default Catalog for HP Anywhere Apps" on page 98.

Chapter 6

HP Web Services Catalog

The HP Anywhere administrator is responsible for managing the HP Anywhere apps in the HP Web Services 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.

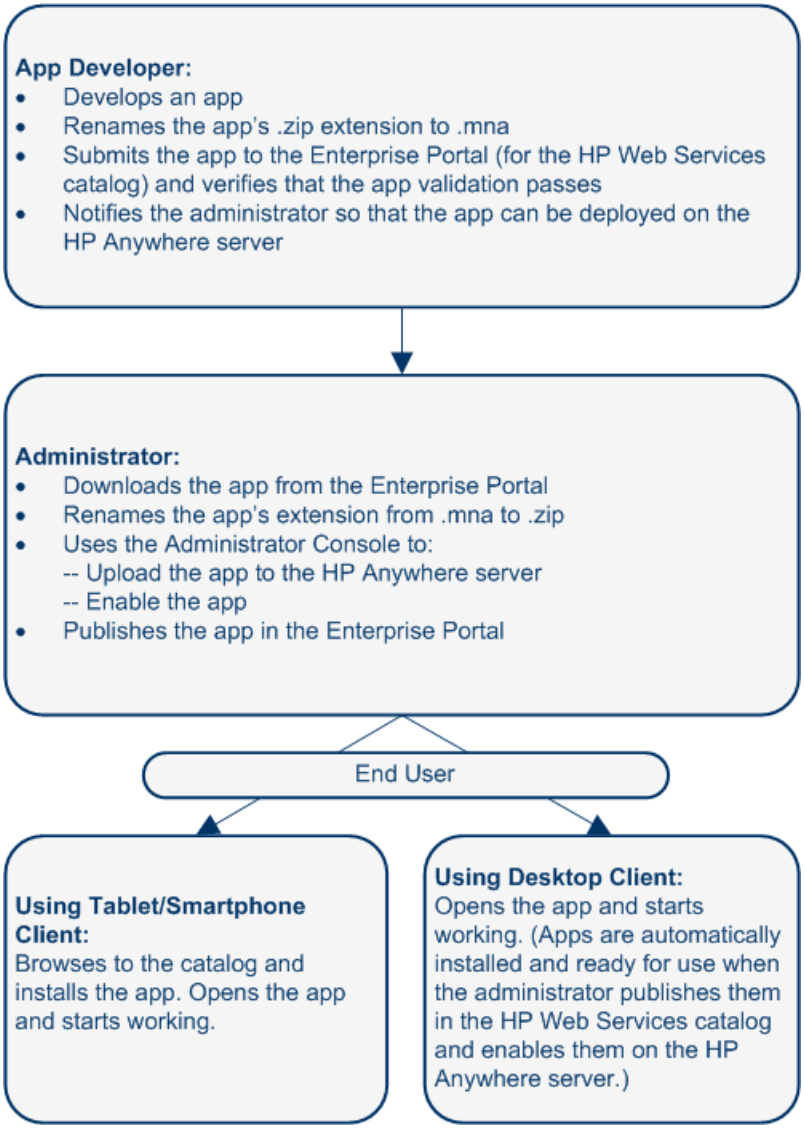
Note: HP Anywhere never uninstalls an app from the HP Anywhere server, only upgrades/updates it. However, you can suspend or disable it in your end users catalogs as required.

Apps in HP Web Services 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.

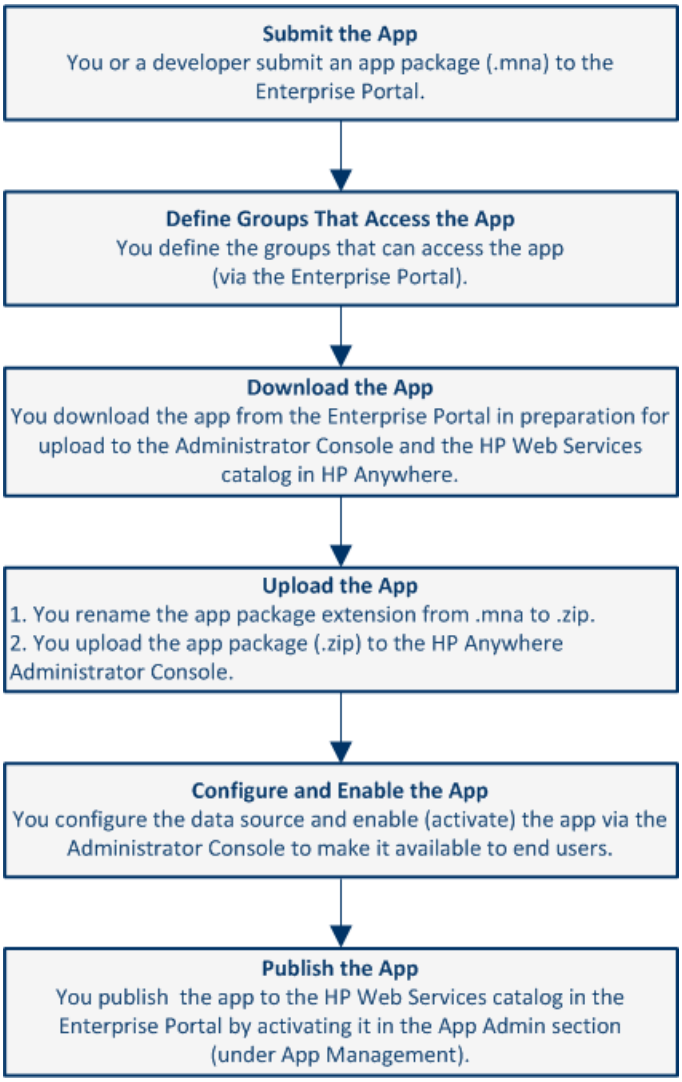
Development-to-Delivery

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



Administrator Tasks for Delivering HP Web Services Apps to End Users

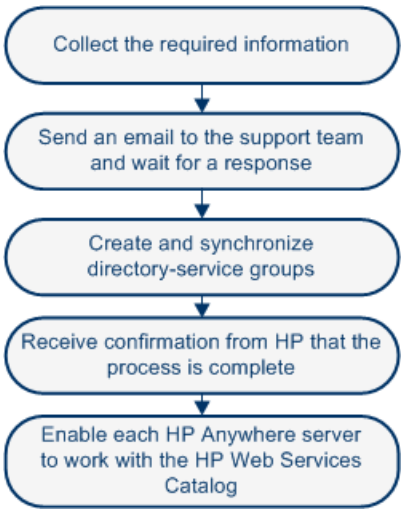
The following chart illustrates your role in enabling your organization's apps to reach end users.



For details, see "Deploying Apps to the HP Web Services Catalog" on page 85.

Prerequisites for Using the HP Web Services Catalog

Before you can add apps to the HP Web Services 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 HP Web Services Catalog and Users" on page 84.

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 HP Web Services Catalog" on page 93.)	
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

When you publish an app, you need to associate the app with groups in the enterprise directory service. This enables users in an associated group to view and download the app.

1. Create directory-service user groups for users that can view and access the apps to be stored in the HP Web Services catalog.

2. After these groups are synchronized with HP Anywhere, notify the person that contacted you that the groups are ready.

When you create directory-service groups, consider the following:

- By enabling access to enterprise applications, you are enabling access to proprietary and confidential information. Consider the groups used for app access and their changing membership carefully—as carefully as you consider groups for accessing other enterprise IT resources.

- Associations of apps with directory-service groups in the Enterprise Portal enable users in those groups to view and download the apps from the HP Web Services Catalog (if they have compatible devices).

- Before using existing groups, consider whether all apps to be associated with these groups are relevant for and should be accessible to all users in these groups.

- Set up groups for which app-related maintenance will be as “maintenance-free” as possible.

- If some enterprise apps enable access to more highly privileged enterprise information, for example, to financial or HR information, then management of the groups that give access to the apps should respect existing procedures for requesting access to more highly privileged information.

- Synchronization occurs every 24 hours and when the HP Anywhere server is restarted.

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.

Step 5: Set the HP Web Services Catalog in the HP Anywhere Administrator Console

Each HP Anywhere server works with one catalog type at time. To enable HP Anywhere to work with the HP Anywhere Web Services catalog, do the following:

1. In the General Settings tab of the Administrator Console, navigate to **Catalog settings**.
2. Set the **Catalog flavor** to **WEB_OS**.
3. Restart the HP Anywhere server for the change to take effect.

How HP Anywhere Integrates with Your HP Web Services Catalog and Users

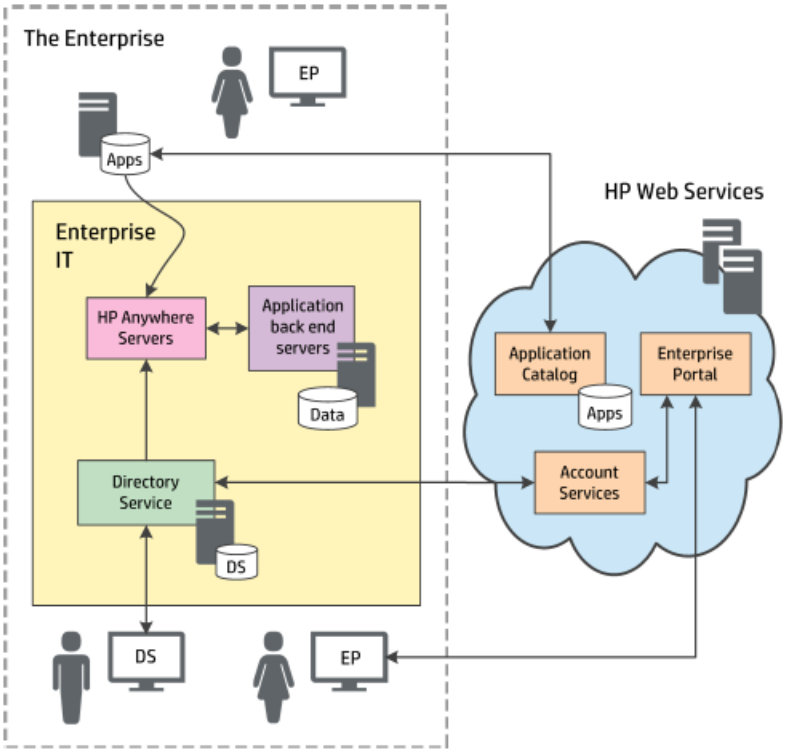
Registering your enterprise enables HP to integrate HP Anywhere with your company's apps and users:

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 (HP Web Services 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 HP Web Services Catalog

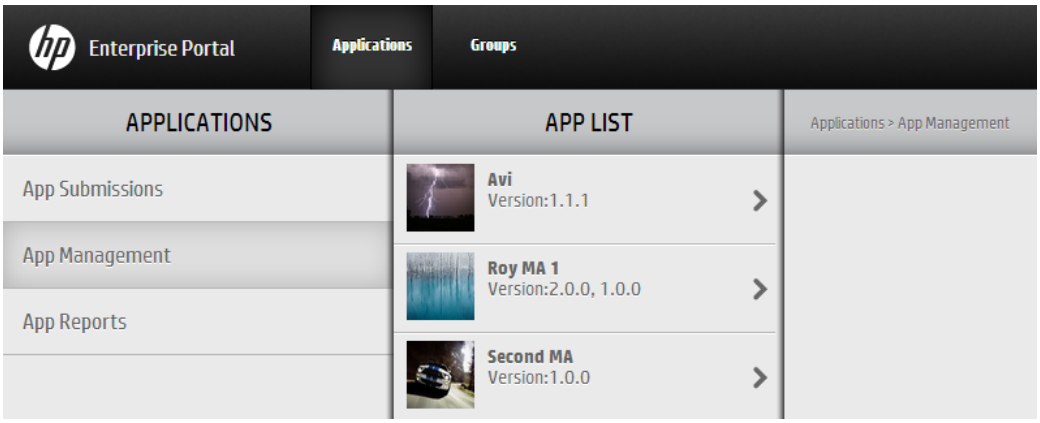
After you integrate the Enterprise Portal with HP Anywhere (as described in "HP Web Services Catalog" on page 76), you can deploy apps to the HP Web Services catalog and enable end users to access them.

To deploy an app to the HP Web Services Catalog:

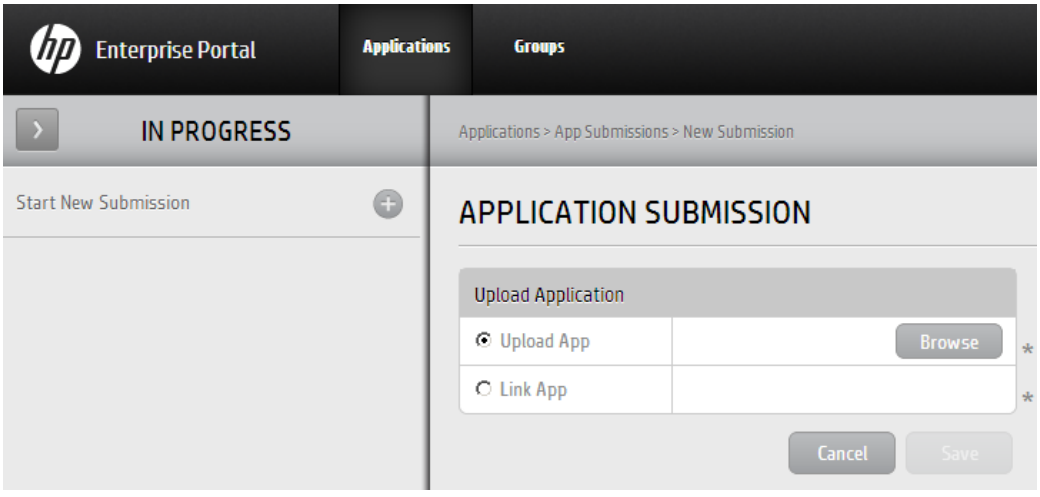
1. Submit the app to the Enterprise Portal.

   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.



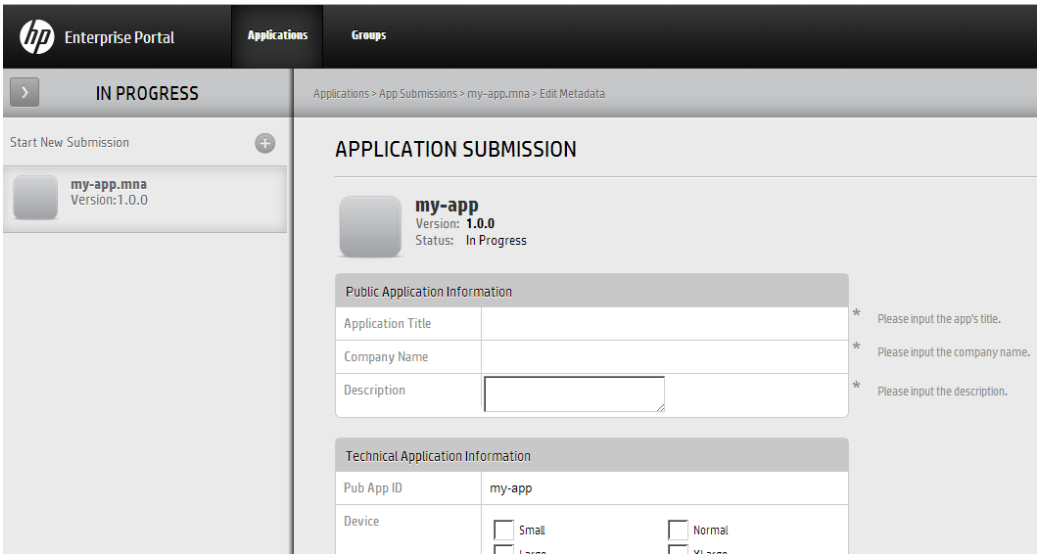
d. Click the **+** button next to **Start New Submission**. Then select **Upload App** and click **Browse** to browse to the app package in the file system and upload it.

> **Note:** Make sure that the app name matches the naming conventions for app packages (see "Appendix A: Naming Conventions for Apps in the HP Web Services Catalog" on page 97) and that it has an **.mna** extension. (Rename the app in the file system prior to upload, if needed.)
>
> **Example:** *my-app.mna*

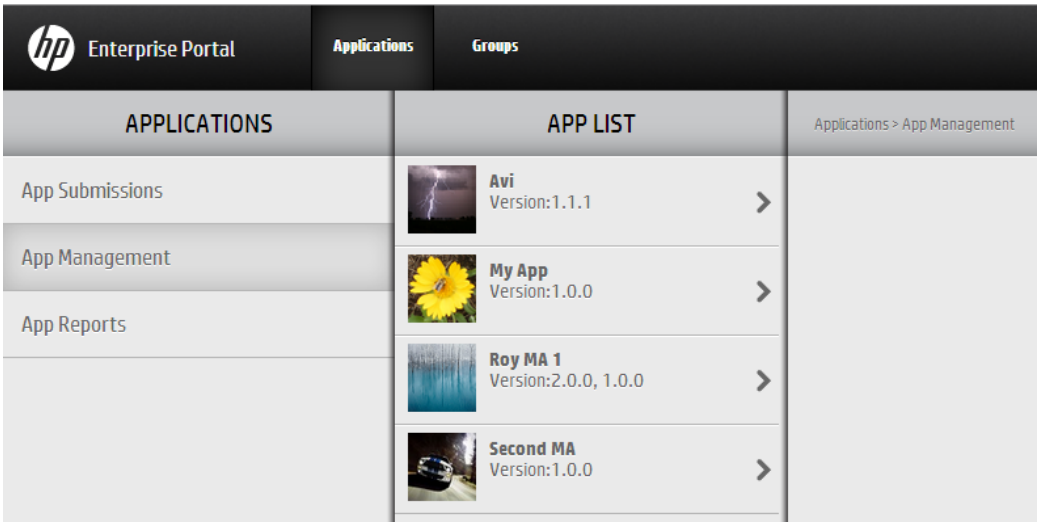
e. Click **Save**. Then click **Yes** in the confirmation box to begin the submission process. The Enterprise Portal validates the app and perfoms checks, such as:

- 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.



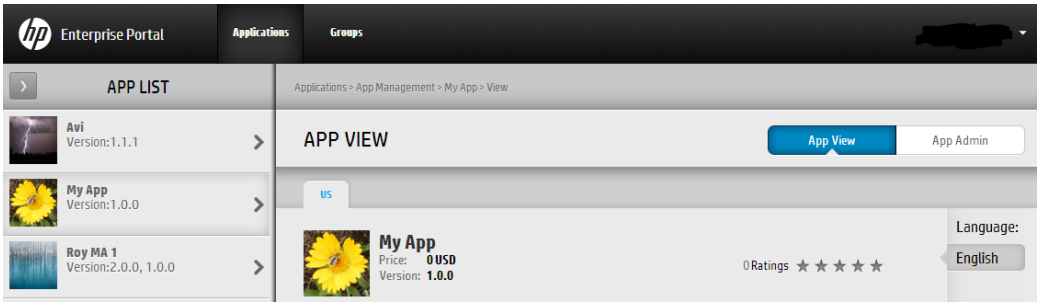
g. Click **Save**. Then click **Yes** in the confirmation box to complete the submission process. The app is added to the **App List** under **App Management**.



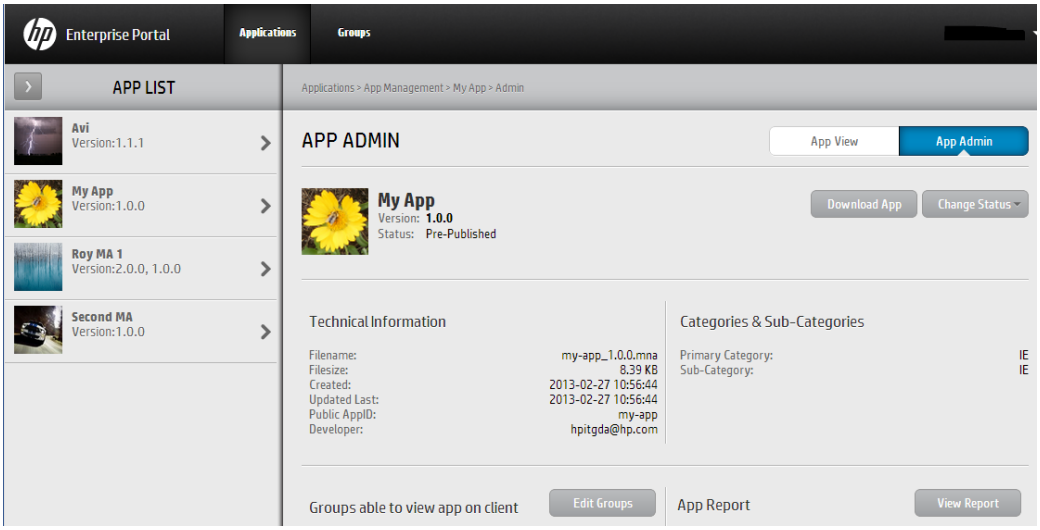
2. Define the groups that can access the app:

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

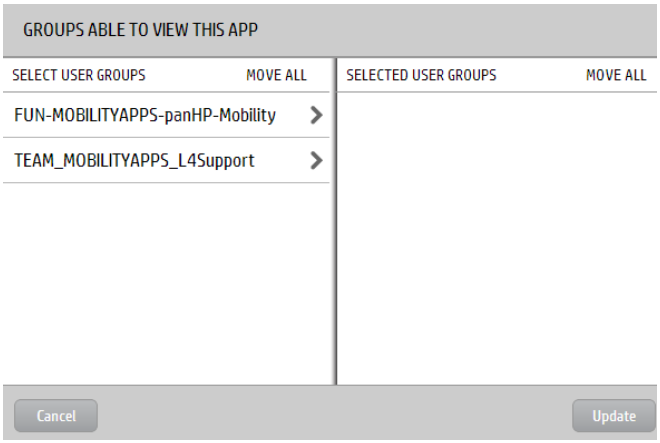
   b. In the App List pane, select the submitted app. The app is displayed in the App View pane.



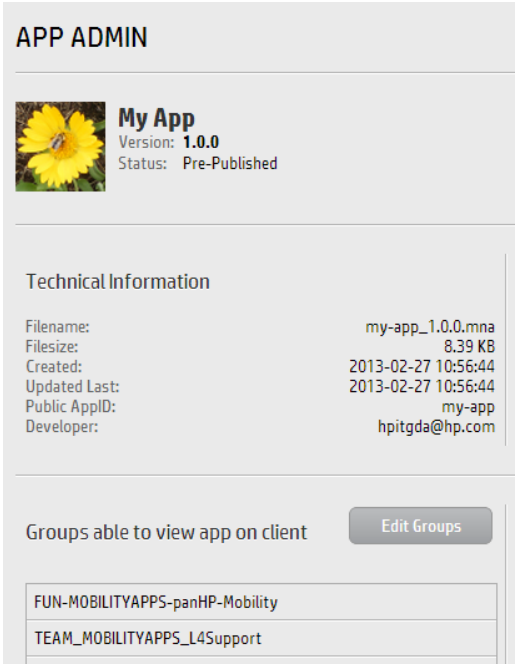
c. In the App View pane, click **App Admin**. The App Admin pane opens.



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.

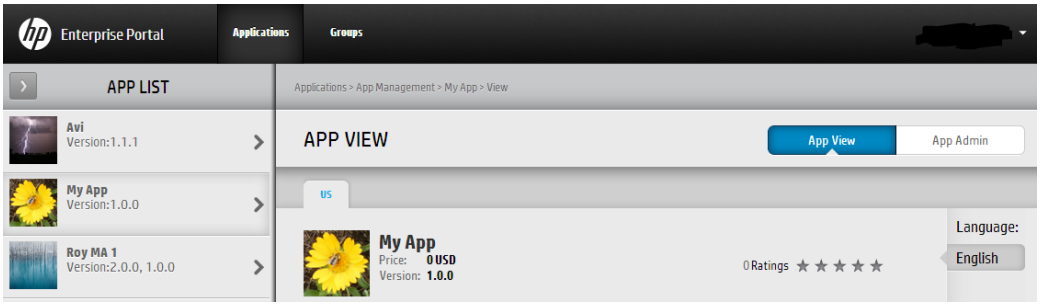


Note: If needed, notify the person responsible for adding apps to the HP Anywhere HP Web Services catalog that the app is ready to be deployed on HP Anywhere.

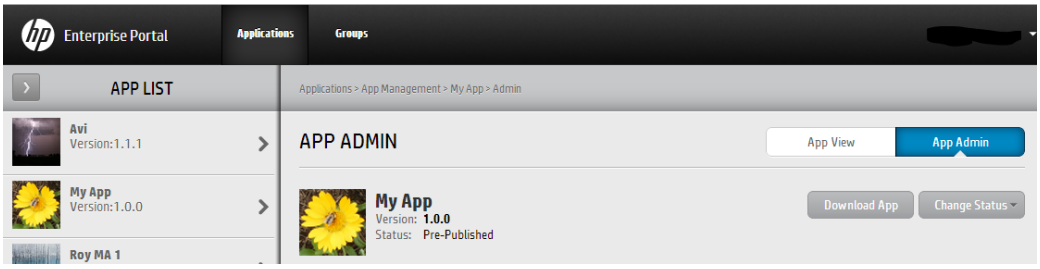
3. Download the app from the Enterprise Portal:

   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*.

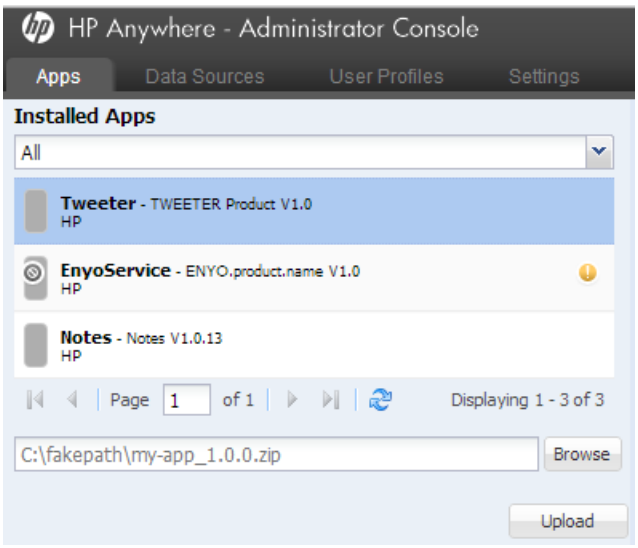
e. Rename the app's **.mna** extension to **.zip**.

4. Upload the app to the Administrator Console.

a. Open the Administrator Console. For details, see "Understanding the Administrator Console" on page 26.

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 **WEB_OS**. 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**

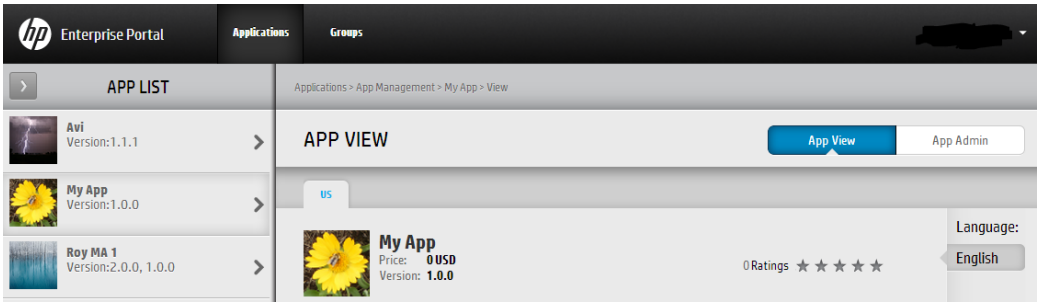
> **Note:** If the deployment fails, check the **hpanywhere-stderr** log file in: <*HP Anywhere installation folder*>\tomcat\logs

5. Set the data source for the app, as described in "Defining a Data Source for an App" on page 51.

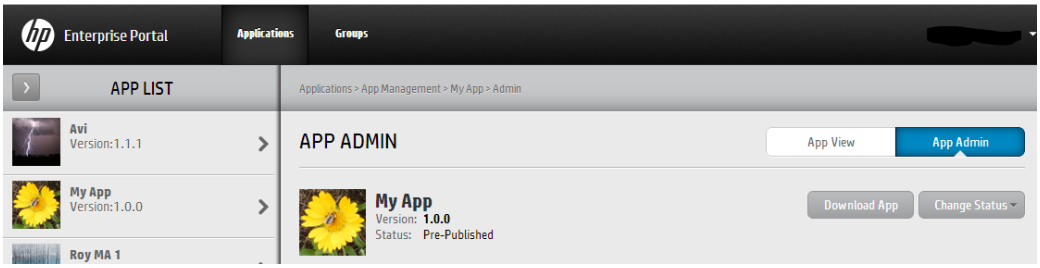
6. Define any app-specific settings:
   a. In the Apps pane of the Administrator Console, select the app you want to enable.
   b. In the right pane, select **Settings** and modify the values, as needed.

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.

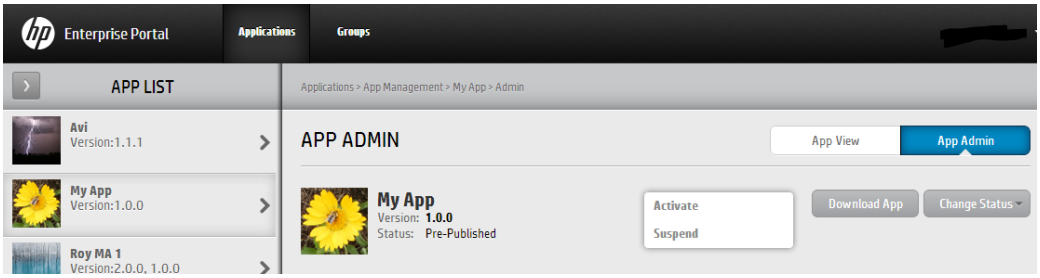
8. Publish the app to the HP Web Services catalog for end users via the Enterprise Portal.
   a. In the Applications pane of the Enterprise Portal, select **App Management**.
   b. In the App List pane, select the submitted app. The app is displayed in the App View pane.



   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 HP Web Services Catalog

To work with an HP Web Services catalog, you need to use SAML certificates.

To create SAML certificates:

1. In a text editor:
   a. Open **<HP_Anywhere_installation_folder>/scripts/CreateSamlSelfSignedCertificate.bat**.

   b. Replace **@btoaw.host.fqdn@** with the fully qualified domain name (FQDN) of the HP Anywhere server host. For example: Change *SET HOST_FQDN=@btoaw.host.fqdn@* to *SET HOST_FQDN=myserver.com*

2. Run **<HP Anywhere installation folder>/scripts/CreateSamlSelfSignedCertificate.bat**. 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 HP Web Services

3. In each HP Anywhere server, overwrite the existing **keystore.jks** file in **<*HP_Anywhere_installation_folder*>\conf\keystore.jks** with the newly generated file.

   Note: Make sure to back up the existing **keystore.jks** file before you overwrite it.

4. 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 HP Web Services Catalog

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

To upgrade an app version in the HP Web Services 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 HP Web Services Catalog" on page 85

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 HP Web Services catalog. For details, see step 1 in "Deploying Apps to the HP Web Services Catalog" on page 85.

4. Download the app from the Enterprise Portal in preparation for upload to the Administrator Console and the HP Web Services catalog in HP Anywhere. For details, see step 4 in "Deploying Apps to the HP Web Services Catalog" on page 85.

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 (**Start > HP > HP Anywhere > Stop HP Anywhere Server**).

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

   c. Delete the following:

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

   d. Start the HP Anywhere server (**Start > HP > HP Anywhere > Start HP Anywhere Server**).

7. Upload the app to the Administrator Console. For details, see step 5 in "Deploying Apps to the HP Web Services Catalog" on page 85.

   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 HP Web Services Catalog" on page 85.

Remove an App from the End User HP Web Services 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 HP Web Services Catalog

This section lists the Enterprise Portal naming conventions for apps in the HP Web Services 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 7

Default Catalog for HP Anywhere Apps

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:

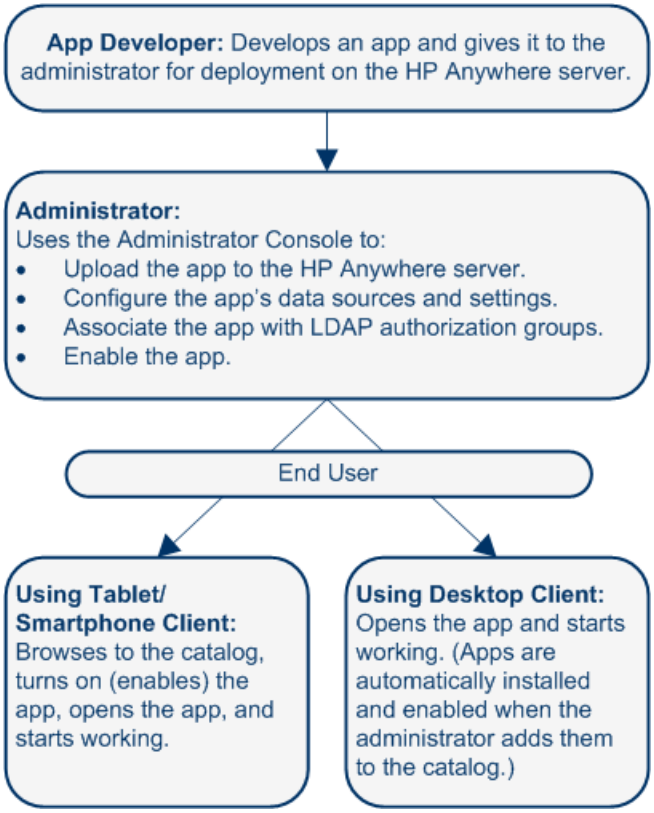
1. Open the Administrator Console. For details, see "Logging In and Out of the Administrator Console" on page 26.
2. Install the app, as described in "Uploading Apps to the Default Catalog" on page 101.
3. Define a data source for the app, if needed. For details, see "Defining a Data Source for an App" on page 51.
4. Modify the app settings, if needed, as described in "Defining Global and App-Specific Settings" on page 29.
5. Associate LDAP authorization groups with each app,as described in "LDAP Groups for HP Anywhere" on page 24.
6. Enable the app, as described in "Enabling an App for End Users" on page 109.

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.

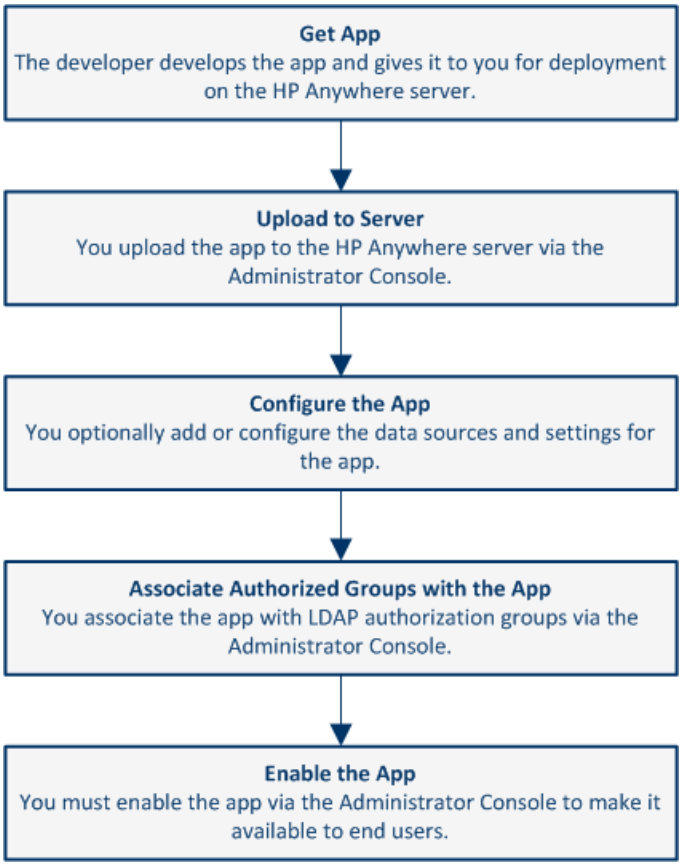
Development-to-Delivery

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 the next page
- "Defining Global and App-Specific Settings" on page 29
- "Defining a Data Source for an App" on page 51
- "Associating LDAP Authorization Groups with Apps" on page 108
- "Enabling an App for End Users" on page 109

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 26.

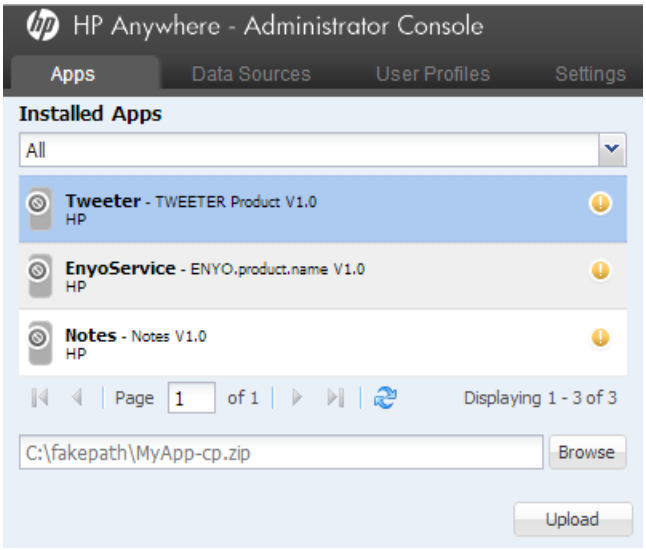
2. **The first time you upload an app:**

   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 relevant LDAP user groups for HP Anywhere exist. For details, see "LDAP Configuration Prerequisites for HP Anywhere" on page 23.

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 default 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 (**Start > HP > HP Anywhere > Stop HP Anywhere Server**).
2. Browse to: ***<HP Anywhere installation folder>*/tomcat/webapps**
3. Delete the following:
   - **<app_name> folder**
   - **<app_name>.WAR file**
   - **<app_name>.ZIP file**
4. Start the HP Anywhere server (**Start > HP > HP Anywhere > Start HP Anywhere Server**).
5. Upload the replacement app, as described in "Uploading Apps to the Default Catalog" on page 101.

   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.

For details on uploading apps to a cluster, see "Uploading Apps to a Cluster" below.

Uploading Apps to a Cluster

If you have direct access to each HP Anywhere server node's IP address, you can upload apps as described in "Uploading Apps to the Default Catalog" on page 101.

If you can access the HP Anywhere server nodes only via the load balancer, the upload process requires you to stop and start each server in rotation, as described in the example below. During the actual upload process, only one of the nodes should be up and running. After you upload an app, make sure to start the next node before stopping the current one to ensure high availability while uploading.

The following example describes how to upload an app to a cluster with two nodes.

Step	Node A	Node B
1	Make sure that the HP Anywhere server is running, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.	--
2	--	Stop the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.
3	--	Make sure that the node is down by verifying that the following services are stopped: • HPANYWHERE • HPANYWHERECASSANDRA
4	1. Upload your app via the Administrator Console (*https://<server-load-balancer>:<port>/admin*). 2. Verify that the correct app version of the app is displayed in the Administrator Console. 3. Enable the app.	--
5	--	Restart the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.
6	Stop the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.	--

Step	Node A	Node B
7	Make sure that the node is down by verifying that the following services are stopped: • HPANYWHERE • HPANYWHERECASSANDRA	--
8	--	1. Upload your app via the Administrator Console (*https://<server-load-balancer>:<port>/admin*). 2. Verify that the correct app version of the app is displayed in the Administrator Console. 3. Enable the app.
9	Restart the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.	

Uploading Replacement Apps to a Cluster

You may need to replace an app on a cluster, for example, when a new version is released. If you have direct access to each HP Anywhere server node's IP address, you can replace existing apps as described in "Upgrading App Versions in the Default Catalog" on page 103.

If you can access the HP Anywhere server nodes only via the load balancer, the app replacement process requires you to stop and start each server in rotation, as described in the example below. During the actual app replacement process, only one of the nodes should be up and running. After you upload a replacement app, make sure to start the next node before stopping the current one to ensure high availability while uploading.

The following example describes how to replace an app on a cluster with two nodes.

Step	Node A	Node B
1	--	Make sure that the HP Anywhere server is running, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.
2	Stop the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.	--
3	Delete the folder containing the uploaded apps and the .war file from **C:\HP\HPAnywhere\tomcat\webapps** **Example:** For an app named *MyApp* that is installed in the default location, delete: • C:\HP\HPAnywhere\tomcat\webapps\MyApp • C:\HP\HPAnywhere\tomcat\webapps\MyApp.war • C:\HP\HPAnywhere\tomcat\webapps\MyApp.zip	--
4	Start the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.	--
5	--	Stop the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.
6	--	Make sure that the node is down by verifying that the following services are stopped: • HPANYWHERE • HPANYWHERECASSANDRA

Step	Node A	Node B
7	--	Delete the folder containing the uploaded apps and the .war file from **C:\HP\HPAnywhere\tomcat\webapps** **Example:** For an app named *MyApp* that is installed in the default location, delete: • C:\HP\HPAnywhere\tomcat\webapps\MyApp • C:\HP\HPAnywhere\tomcat\webapps\MyApp.war • C:\HP\HPAnywhere\tomcat\webapps\MyApp.zip
8	1. Upload the replacement app via the Administrator Console (*https://<server-load-balancer>:<port>/admin*). 2. Verify that the correct app version of the app is displayed in the Administrator Console. 3. Enable the app.	
9	--	Start the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.
10	Stop the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.	--
11	Make sure that the node is down by verifying that the following services are stopped: • HPANYWHERE • HPANYWHERECASSANDRA	--

Step	Node A	Node B
12	--	1. Upload the replacement app via the Administrator Console (*https://<server-load-balancer>:<port>/admin*). 2. Verify that the correct app version of the app is displayed in the Administrator Console. 3. Enable the app.
13	Start the HP Anywhere server, as follows: From the **Start** menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.	--

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 "LDAP Groups for HP Anywhere" on page 24.

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 26.
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 26.
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 51.
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 26.
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.

Chapter 8

Managing Large-Scale App Deployment

This section describes how to configure your Java Virtual Machine (JVM) to support large-scale deployment of HP Anywhere apps (approximately 20-100 apps) on an HP Anywhere server. The configuration is based on tests performed on benchmark apps. For more details, see the supported server environments section of the Support Matrix.

For approximately 20-50 HP Anywhere apps

1. Create a backup copy of **<HP_Anywhere_installation_directory>\scripts\HPAnywhereServiceUtility.bat**.

2. In a text editor, open **<HP_Anywhere_installation_directory>\scripts\HPAnywhereServiceUtility.bat**, and locate and CAREFULLY change the following JVM parameters:

Replace:	With:
On the line that begins with **%EXECUTABLE%" //US//%SERVICE_NAME%**, replace: **-XX:MaxPermSize=512m** **Important:** This is the last instance in the file.	**-XX:MaxPermSize=1280m**
--JvmMx 3072	**--JvmMx 5120**

3. Stop the HP Anywhere server. (From the Start menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.)

4. Uninstall and re-install the HPA service by running the following commands:

   <HP_Anywhere_installation_directory>\scripts\uninstallAnywhereService.bat

   <HP_Anywhere_installation_directory>\scripts\installAnywhereService.bat

5. Start the HP Anywhere server. (From the Start menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.)

For approximately 51-100 HP Anywhere apps

1. Install the HP Anywhere server on a machine with 16 GB RAM (instead of the standard 8 GB RAM).

2. Create a backup copy of **<HP_Anywhere_installation_directory>\scripts\HPAnywhereServiceUtility.bat**.

3. In a text editor, open **<HP_Anywhere_installation_directory>\scripts\HPAnywhereServiceUtility.bat**.

   - Locate the following and change the following JVM parameters:

Replace:	With:
On the line that begins with **%EXECUTABLE%" //US//%SERVICE_NAME%**, replace: **-XX:MaxPermSize=512m** **Important:** This is the last instance in the file.	**-XX:MaxPermSize=2048m**
--JvmMx 3072	**--JvmMx 5120**

   - Add the following flags to the end of the same line in which you changed the JVM parameters listed above:

     - **-XX:ReservedCodeCacheSize=100m;**

     - **-XX:+UseCodeCacheFlushing;**

4. Stop the HP Anywhere server. (From the Start menu, select **HP**, right-click **Stop HP Anywhere**, and select **Run as administrator**.)

5. Uninstall and re-install the HPA service by running the following commands:

   <HP_Anywhere_installation_directory>\scripts\uninstallAnywhereService.bat

   <HP_Anywhere_installation_directory>\scripts\installAnywhereService.bat

6. Start the HP Anywhere server. (From the Start menu, select **HP**, right-click **Start HP Anywhere**, and select **Run as administrator**.)

Chapter 9

User and Device Management - Restricting User/Device Connections (Black/White List)

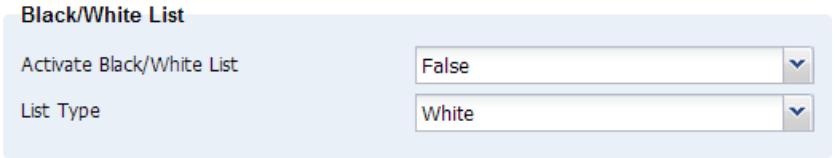
You can allow or prevent specific users and/or devices from accessing HP Anywhere by creating and implementing a:

- **White list** to allow only specific users and/or devices to connect to HP Anywhere.
- **Black list** to prevent specific users and/or devices from connecting to HP Anywhere.

By default, this restrictive functionality is disabled. When you enable this functionality, users or devices that are blocked receive an error message when they try to access HP Anywhere.

Prerequisites for using a Black List or White List:

1. Connect to the HP Anywhere database schema and run one of the following Create SQL commands according to your database type:
   - **Oracle:** <HP_Anywhere_installation_folder>\confwizard\conf\scripts\database\oracle\oracle_create_provisioning_entities.sql
   - **MSSQL:** <HP_Anywhere_installation_folder>\confwizard\conf\scripts\database\mssql\ mssql_create_provisioning_entities.sql
2. Set the **Black/White List** settings in the Administrator Console:
   a. Log in to the HP Anywhere Administrator Console (**http(s)://<HP_Anywhere Server_URL>:<port>/admin**).
   b. Click the **Settings** tab.
   c. Scroll to the **Black/White List** section and set
      - **Activate Black/White List** to **True**
      - **List Type** to **Black** or **White**



   d. Save the changes.

For details on working with Black and White lists, search http://support.openview.hp.com/selfsolve/manuals.

3. Apply restrictions using the provision-list API, described below.

provision-list API

You can apply restrictions to users and/or devices, using one of the following list types:

- **White list:** Allows only specific users and/or devices to access HP Anywhere and its apps. Users and/or devices that are not on this list cannot access HP Anywhere.
- **Black list:** Prevents specific users and/or devices from connecting to HP Anywhere. All other HP Anywhere users and/or devices in your organization can access HP Anywhere.

Each entry in a list can apply to:

- A user, for example: `{"userId": "user1"} or {"userId": "user1","deviceId": null}`
- A device, for example `{"deviceId": "device2"} or {"userId": null,"deviceId": "device2"}`
- A combination of the two to restrict a specific device for a specific user, for example: `{"userId": "user1","deviceId": "device2"}`

You can add as many entries to the list as needed.

URL

`http(s)://<host>:<port>/ diamond/rest/api/V2/provision-list`

Remarks

You set the list type using the **HP Anywhere Administrator Console > Settings tab > Black/White List** section **> List type**.

Note: The **List Type** does not affect the entries in the list—it affects only the restriction type.

HTTP Methods

GET

Description:	Retrieves the entries from the black or white list. **Note:** When using GET, you can: -- Use query parameters to specify a user and/or device ID to retrieve related entries. -- Leave the query string blank to retrieve all of the entries in the list.

Parameters:	**userId:**	The unique HP Anywhere login name.
	deviceId:	The device associated with a user, as defined in: HP Anywhere Administrator Console > User Profiles tab > Associated Devices tab > P/N
Examples:	**URLs:**	http (s)://<host>:<port>/diamond/rest/api/V2/provision-list?userId=user1 http (s)://<host>:<port>/diamond/rest/api/V2/provision-list?userId=user1&deviceId=device1 **Note:** This complex query example returns a single entry that contains both “user1” and “device1”.
	Headers:	Accept: application/json
	Response Body:	{"entries":[{"userId":"user1","deviceId":"device1"}, {"userId":"user1","deviceId":"device2"}, {"userId":"user1","deviceId":"device3"}]} {"entries": [{"userId":"user1","deviceId":"device1"}]}

DELETE

Description:	Deletes the specified entries from the black or white list. **Caution:** The entire list is DELETED if: --You do not add query parameters. --You misspell a query parameter (for example, deviceID instead of deviceId). **Note:** When using DELETE, you can: -- Use query parameters to specify a user and/or device ID to delete related entries. -- Leave the query string blank to delete all of the entries in the list.	
Parameters:	**userId:**	The unique HP Anywhere login name.
	deviceId:	The device associated with a user, as defined in: HP Anywhere Administrator Console > User Profiles tab > Associated Devices tab > P/N
Examples:	**URL:**	http(s)://<host>:<port>/diamond/rest/api/V2/provision-list?userId=user1
	Header:	X-CSRF-HPMEAP: HPA
	Status Code:	200 OK

PUT

Description:	Deletes the existing entries in the black or white list and replaces them with the given list of entries. **Note:** HP Anywhere validates entries before running PUT or POST to ensure that no conflicts exist, such as the following conflict: {"userId": "user1"}, /*Generic: Applies to all devices associated with this user */ {"userId": "user1","deviceId": "device2"} /*Specific: Restriction applies to this user when using this device */	
Examples:	**URL:**	http (s)://<host>:<port>/diamond/rest/api/V2/provision-list
	Header:	X-CSRF-HPMEAP: HPA Content-Type:application/json
	Body:	{"entries":[{"userId":"user1","deviceId":"device1"}, {"userId":"user1", "deviceId":"device2"}, {"userId":"user1","deviceId":"device3"}]}
	Status Code:	204 No Content

POST

Description:	Appends entries to the black or white list. If there is a conflict between entries in the existing list and the appended list, the appended list entries take precedence. For example, suppose a white list contains two entries for a specific user with two devices. {"userId": "user1","deviceId": "device1"}, {"userId": "user1","deviceId": "device2"} If you append the list with a generic entry for that user (without specifying a device), {"userId": "user1"} the appended entry overwrites the existing entries in the white list, allowing all devices for that user. Similarly, if a generic entry in a black list specifies only a user, and the appended list entry includes a device for that user, then the user that was previously blacklisted can now access HP Anywhere using any other registered device.

Examples:	**URL:**	http (s)://<host>:<port>/diamond/rest/api/V2/provision-list
	Header:	X-CSRF-HPMEAP: HPA Content-Type: application/json
	Body:	{"entries":[{"userId":"user1","deviceId":"device1"}, {"userId":"user1","deviceId":"device2"}, {"userId":"user1","deviceId":"device3"}]}
	Status Code:	204 No Content

Chapter 10

Cassandra—Backup and Restore

Cassandra is a NoSQL, peer-to-peer, database management system with its own backup utilities and restore process. The server nodes can be spread over multiple data centers and sites. Data is replicated between these nodes. Data restoration and recovery is usually needed only in cases where all replications of a data set are lost or corrupted data is written to the database.

When you back up your server nodes, you can either choose to take a base snapshot of the entire node, or you can combine base snapshots with incremental backups that include the changes made since the last base snapshot was taken.

Glossary of Cassandra terminology used in this section:

Cassandra	Relational Database Equivalent
column family	table
keyspace	database
SSTable	data file

Cassandra Backup Tools

Cassandra can take snapshots of the data in your keyspace whenever online operations are performed. This ensures that your data is continually backed up. These backups are hard links to the active data files in the parent keyspace (not actual file copies). Therefore, minimal disk space is used, and the processes are performed quickly.

Backups are usually stored in the Cassandra data directory, for example: *.../var/lib/cassandra/data/<keyspace_name>/<column_family_name>/snapshots/<optional_snapshot_name>*. This directory contains ***.db** files with data links, as they were captured by the snapshot.

To create base snapshots of the nodes:

1. On each node, run the **nodetool** utility with the following command:
   `$ nodetool -h localhost -p 7199 snapshot appStore -t <snapshot_name>`
   where <*snapshot_name*> is an optional parameter that enables you to manage your backups and where 7199 is the JMX port.

2. Repeat for additional nodes.

To delete snapshots:

1. On a node, run the **nodetool** utility with the following command:
   `$ nodetool -h localhost -p 7199 clearsnapshot –t <snapshot name>`
   where 7199 is the JMX port.

2. Repeat for each additional node.
3. (Optional) Compress and move snapshots to an external storage location for retention.

> **Note:** You may not be able to do delete snapshots when Cassandra is open due to known Windows issues. For details, see: https://issues.apache.org/jira/browse/CASSANDRA-4050?page=com.atlassian.jira.plugin.system.issuetabpanels:all-tabpanel

Incremental Backups

If you enable incremental backups, Cassandra hard-links each flushed SSTable to a **backups** directory under the keyspace data directory. This enables you to store incremental backups in an external location without performing snapshots of the entire keyspace.

To enable incremental backups:

1. In a text editor, open **cassandra.yaml**.
2. Change the value of **incremental_backups** to **true**.

> **Note:** Cassandra does not delete incremental backups. Therefore, you may want to set up an automatic process that clears incremental backups each time a new snapshot is taken.

Cassandra Recovery Process

When you perform a Cassandra keyspace recovery, you restore all of the keyspace SSTable files as they existed when the snapshots were taken. You must do this for each server node in the Cassandra cluster.

To restore a single node:

1. Make sure that Cassandra is shut down.
2. Delete all of the files in the **commitlog** directory, for example, *.../var/lib/cassandra/commitlog*.
3. Delete all ***.db** files in the **<data_directory_location>/<keyspace_name>/<column_family_name>** directory, but DO NOT delete the **/snapshots** and **/backups** subdirectories.
4. From the storage directory, copy the base snapshot to use for the recovery to the active keyspace: **$DATA_DIRECTORY/<keyspace>/**.
5. From the storage directory, copy the incremental snapshots to use for the recovery to the active keyspace: **$DATA_DIRECTORY/<keyspace>/**
6. Start Cassandra. (CPU resource usage spikes at this point due to a temporary peak of I/O activity.)


Java™
COMPATIBLE