HP PPM Apps for Smartphone

for the Android and iOS mobile operating systems

Software Version: PPM Requests for Smartphone 2.00, 1.01

TM Approval for Smartphone 2.00, 1.00

TM Submission for Smartphone 1.00

Configuration Guide

Document Release Date: August 2013

Software Release Date: August 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 Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

Java™ is a U.S. trademark of Sun Microsystems, Inc.

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

This manual's title page 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:

h20230.www2.hp.com/selfsolve/manuals

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

You can visit the HP Software Support Web site at:

hp.com/go/hpsoftwaresupport

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels, go to:

h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

h20229.www2.hp.com/passport-registration.html

Contents

1 Welcome to This Guide

Welcome to the *HP PPM Apps for Mobile Devices Configuration Guide*.

PPM Center now includes mobile capabilities, powered by HP Anywhere. Now, you can manage requests and timesheets from your iPhone and Android smartphones. With this new functionality, PMOs and managers can be more productive—working on the go in a secured, personalized and intuitive way.

Audience

This document is designed for administrators. Note that an administrator can be the HP Anywhere administrator or the PPM Center administrator or both roles can be combined.

System Requirements

Software Version:

- For PPM Requests for Smartphone 1.01, or PPM TM Approval for Smartphone 1.00:
  - HP Anywhere 9.00 or 9.01 (on the server and on the mobile device)
  - HP Project and Portfolio Management Center 9.13 or 9.14
- For PPM Requests for Smartphone 2.00 (HP Anywhere 10.x app for PPM Request Management), TM Approval for Smartphone 2.00 (HP Anywhere

10.x app for PPM Time Management Approval), or TM Submission for Smartphone 1.00 (HP Anywhere 10.x app for PPM Time Management Submission):

- HP Anywhere 10.00 (on the server and on the mobile device)
- HP Project and Portfolio Management Center 9.21

Supported devices:

- Smartphone

Device operating system (on recommended devices):

- For PPM Requests for Smartphone 1.01, or TM Approval for Smartphone 1.00:
  - iOS 4.0 and above
  - Android 2.2 and above
- For PPM Requests for Smartphone 2.00 (HP Anywhere 10.x app for PPM Request Management), TM Approval for Smartphone 2.00 (HP Anywhere 10.x app for PPM Time Management Approval), or TM Submission for Smartphone 1.00 (HP Anywhere 10.x app for PPM Time Management Submission):
  - iOS 5 (on iPhone 4/4S), or iOS 6 (on iPhone 5)
  - Android 2.3.5 (on Samsung Galaxy S2), or Android 4.0.4 (on Samsung Galaxy S3)

Mobile connectivity:

- Standard communication with the HP Anywhere Server, such as Wi-Fi or 3G

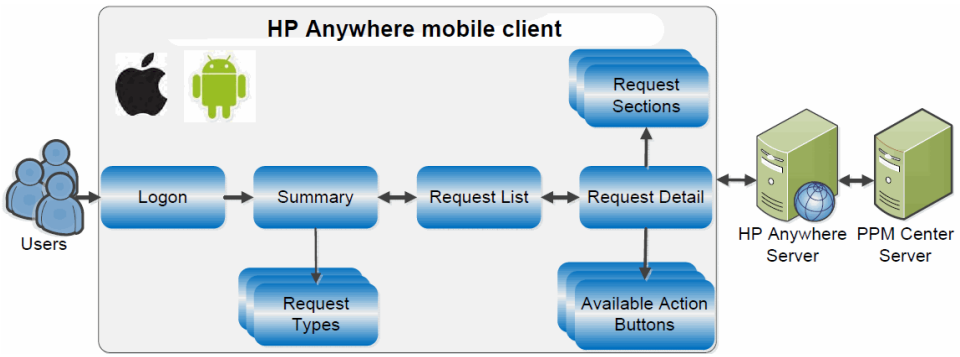
Overview of PPM Apps

PPM apps enable PPM Center users who are working outside of an office or without VPN access can act on available approval actions from their mobile devices, without having to log on to PPM Center.

PPM apps are powered by HP Anywhere. Before end users can use PPM apps from their mobile devices, administrators need to configure HP Anywhere server and PPM Server for apps to work properly.

Figure 1-1 illustrates how PPM Requests app works.

Figure 1-1. How PPM Requests app works



Supported Languages

PPM apps support all languages that PPM Center supports:

- English (en)
- Russian (ru)
- Portuguese (pt_BR)
- Spanish (es)
- Chinese (zh_CN)
- German (de)
- French (fr)

- Korean (ko)
- Turkish (tr)
- Italian (it)
- Japanese (ja)
- Dutch (nl)

HP Anywhere may not support some languages listed above. As a result, after logging on to HP Anywhere on a non-English language, you may see some screens with English words.

Related Information

The following documents include additional information related to HP Anywhere and the PPM apps for smartphone:

- *HP Anywhere Installation and Configuration Guide*
- *HP Anywhere Administrator Guide*
- *HP Anywhere Release Notes*

For information about how to configure or use HP Demand Management and HP Time Management, see the following PPM Center documents:

- *Release Notes*
- *HP Demand Management User's Guide*
- *HP Demand Management Configuration Guide*
- *Tracking and Managing IT Demand Configuration Guide*
- *Tracking and Managing IT Demand User's Guide*
- *Commands, Tokens, and Validations Guide and Reference*
- *HP Time Management User's Guide*
- *HP Time Management Configuration Guide*

- *Reports Guide and Reference*
- *Getting Started*
- *What's New and What's Changed*
- *HP Project Management User's Guide*
- *HP-Supplied Entities Guide* (includes descriptions of all HP Demand Management portlets, request types, and workflows)

2 Configuring PPM Apps on HP Anywhere Server

This chapter contains information that help administrators to configure PPM apps on HP Anywhere server.

This chapter includes:

- *Configuring PPM apps on HP Anywhere Server*
- *(Optional) Downloading HP Anywhere Limited*

Configuring PPM apps on HP Anywhere Server

Administrators can perform the following configuration tasks in the HP Anywhere – Administrator Console:

- (Optional) Install PPM apps on the HP Anywhere server.

You should follow the instructions if you use HP Anywhere 10.00 for PPM apps.

a. Go to HP Anywhere - Administrator Console page by entering the following address in your browser:

   - `http://<HPA_Server_IP>:<Port>/admin`, or,
     `http://<HPA_Server_Hostname>:<Port>/admin`
   - If HP Anywhere uses SSL:

     `https://<HPA_Server_IP>:<Port>/admin`, or,
     `https://<HPA_Server_Hostname>:<Port>/admin`

b. Click **Browse.**

c. Select the corresponding file for the app you want to install.

- For PPM Requests for Smartphone 2.00 (HP Anywhere 10.x app for PPM Request Management):

  Select the file `ppm-dm-runtime.<version_number>.zip` which you can download by entering the following address in the browser:

  `https://hpln.hp.com/node/8979/contentfiles`

- For TM Approval for Smartphone 2.00 (HP Anywhere 10.x app for PPM Time Management Approval):

  Select the file `ppm-tsapproval-hpa-runtime.<version_number>.zip` which you can download by entering the following address in the browser:

  `https://hpln.hp.com/node/10545/contentfiles`

- For TM Submission for Smartphone 1.00 (HP Anywhere 10.x app for PPM Time Management Submission):

  Select the file `ppm-tm-hpa-runtime.<version_number>.zip` which you can download by entering the following address in the browser:

  `https://hpln.hp.com/node/13228/contentfiles`

d. Click **Upload**.

The Confirmation prompt pops up.

e. Click **Yes**.

f. Wait for the deployment to finish.

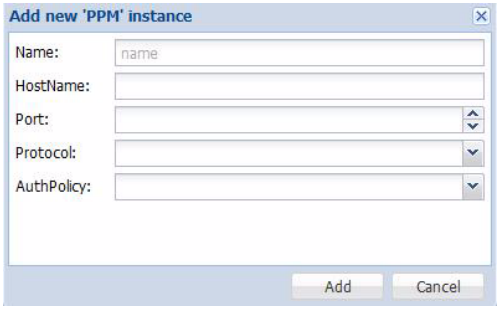
For details, see the *HP Anywhere Administrator Guide.*

- Enable or disable PPM apps.

  For details, see the *HP Anywhere Administrator Guide.*

- Configure PPM Center data source.

When you click Add Instance.. to add a new data source, the **Add new 'PPM' instance** dialog opens.



Provide values for the fields described in the table below:

Field	Description
Name	Specifies PPM Center data instance name. This name is visible to the app end users on their smartphones. You can provide a meaningful name that can be easily recognized by them.
HostName	Specifies a valid PPM Center instance host name or PPM Server instance web address.
Port	Specifies PPM Center instance port number.
Protocol	Specifies which protocol PPM Center should use. Valid values: `http, https` **Note:** If your protocol is `https`, you should have already imported a certificate from PPM Center when configuring LDAP over SSL. If you have not yet done so, import the certificate as described in the *Configure LDAP Over SSL section* in the *HP Anywhere: Installation and Configuration*.

Field	Description
AuthPolicy	Specifies which user authentication policy the PPM apps should use when end users log on HP Anywhere mobile client on their smartphones. Valid values include: • `BasicAuth` – Basic Authentication policy. If you select this value, end users must enter their PPM Center username and password. • `LWSSO` – Lightweight single sign-on authentication policy. Specifying this value requires configuring your PPM Center instance for LWSSO authentication support. Given the security provided by LWSSO, this authentication mode is recommended by HP. If you select this value, app end users do not need to set their PPM Center username and password on their mobile devices when they log in to HP Anywhere for the first time. For more information about user authentication and details about configuring LWSSO support, see *Configuring PPM Server* on page 19.

For more details about data source management, see the *HP Anywhere Administrator Guide.*

- Manage personas (roles). For details, see the *HP Anywhere Administrator Guide.*

(Optional) Downloading HP Anywhere Limited

HP Anywhere Limited version is only available for version 9.00. Follow the steps in this section if your organization choose to use the HP Anywhere Limited version that is available free of change for PPM apps only. Otherwise simply skip this section.

About HP Anywhere Limited

As a special flavor of the HP Anywhere Server product, HP Anywhere Limited is the single product license version of the product. It is provided to customers as part of app solution for a single HP Software product. HP Anywhere

Limited that bundled with PPM Center 9.10 is available free of charge for all PPM Center customers.

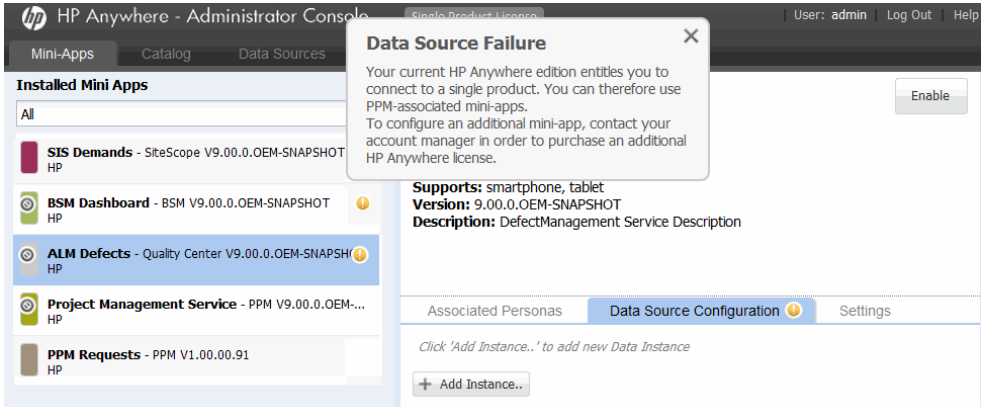
HP Anywhere Limited allows connection to a single product data source. Administrators can add multiple data instances to the associated product data source, then users can connect and retrieve data from the product data source.

For details about how to obtain HP Anywhere Limited, see *Download HP Anywhere Limited* on page 16.

For connection to data sources of multiple products, you need the full version of HP Anywhere server product. For more information, contact your HP Software sales representative.

The following are the differences between the limited version and full version of HP Anywhere:

- With HP Anywhere Limited installed, after logging into HP Anywhere – Administrator Console, you can find the "Single Product License" text in the top of the console window.
- If you try to add a data instance to a product other than PPM-associated app, a message pops up reminding you of the limitation.



For more information about configuring and using HP Anywhere and apps, see *HP Anywhere Administrator Guide* and *HP Anywhere Installation and Configuration Guide.* To download these guides, go to h20230.www2.hp.com/selfsolve/manuals.

Download HP Anywhere Limited

To obtain HP Anywhere Limited product and PPM app product,

1. Download HP Anywhere 9.00 Limited English (`T9468-15100.iso`).

   a. Go to Eval Portal and sign in:
   https://h20575.www2.hp.com/evalportal/index.do

   The Software Evaluations page appears.

   HP Passport is required to sign in. If you do not have one, click **New Users - please register** to register for an HP Passport ID.

   b. Go to **Product Center** section, click **HP Software > Project & Portfolio Management Center**.

   c. Locate **HP PPM 9.10 Eng SW E-Media** (Product Number `T5570EAE`), and click **Receive for Trial**.

   The Software downloads and licenses page appears.

   d. Click **Get Software**.

   e. In the **Electronic downloads** list, locate `Software, HP Anywhere 9.00 Limited English (T9468-15100.iso)`, and click **Download Directly**.

   If you are new to the PPM Center product, make sure to download `HP PPM 9.10 Media (T5570-15072.iso)` as well.

2. Download PPM Center 9.13 or 9.14 installation package.

   a. Go to HP Software Patches and Updates site.

   b. Click **Self-solve** tab, then in the left navigation pane, click **Software patches**.

   The Patches search page appears.

   c. Locate **Project and Portfolio Management** in the Product list, specify **9.13** or **9.14** for Product version, select your operating system, and then click **Search**.

d. In the search result section, click **PPMC_9.13** or **PPMC_9.14** and follow the instructions to download the patch.

3. Install the software.

   a. Install PPM Center 9.10 if you have not installed it. For detailed instructions, see the *Installation and Administration Guide* for PPM Center 9.10.

   b. Upgrade your PPM Center installation to version 9.13 or version 9.14. For detailed instructions, see *Release Notes for PPM Center 9.13* or *Release Notes for PPM Center 9.14*.

   c. Install HP Anywhere Limited, and connect to HP Live Network (http://www.hp.com/go/livenetwork) to retrieve available PPM apps.

      For detailed instructions, see *HP Anywhere Administrator Guide* and *HP Anywhere Installation and Configuration Guide.*

3 Configuring PPM Server

This chapter contains information that help administrators to configure PPM Server for PPM apps to work properly.

This chapter includes:

- *Deploying PPM app Hotfixes on PPM Server*
- *Configuring PPM Server for User Authentication Support*

Deploying PPM app Hotfixes on PPM Server

PPM Center versions 9.13 and 9.14 were released before the TM Approval version 1.00 and the MLU support for PPM Requests app are available. Therefore, the PPM app hotfixes contain the follows:

- TM Approval app version 1.00
- MLU support for PPM Requests app

If your organization plans to use the TM Approval app version 1.00, or the MLU support for PPM Requests app, or both, make sure to obtain and deploy the hotfixes as described below.

PPM Center version 9.14.0001 (or higher) contains the hotfixes mentioned here. If you already upgraded your PPM Center instances to version 9.14.0001 (or higher), you can simply ignore this section.

To obtain and deploy PPM app hotfix package,

1. Contact HP Software Support to obtain the app hotfix package for your version of PPM Center:

   - *For PPM Center version 9.13*
     HOTFIX_PPM_CENTER_9.1_SP3_TM_APPROVAL_MINIAPP_1.0.0
   - *For PPM Center version 9.14*
     HOTFIX_PPM_CENTER_9.1_SP4_TM_APPROVAL_MINIAPP_1.0.0

2. Use kDeploy to deploy the PPM app hotfix:

   kDeploy.sh -hotfix <*DEPLOYMENT_HOTFIX***>**

   where <*DEPLOYMENT_HOTFIX*> is the hotfix bundle name.

   For example:

   If the bundle name is

   - 913-debug-QCIM1L<*XXXX*>.jar, or
   - 913-debug-QCIM1L<*XXXX*>-QCIM1L<*XXXX*>.jar

   Then the corresponding deployment command is:

   - sh kDeploy.sh -hotfix 913-debug-QCIM1L<*XXXX*>.jar, or,
   - sh kDeploy.sh -hotfix 913-debug-QCIM1L<*XXXX*>-QCCR1L<*XXXX*>.jar

   kDeploy looks for the hotfix bundle file under <*PPM_HOME*>, so the hotfix bundle must be located in this directory.

For technical support, contact HP Software Support.

Configuring PPM Server for User Authentication Support

Overview of User Authentication

Authentication of HP Anywhere users is based on HP Software's Lightweight Single Sign-On (LW-SSO) framework. Once end users are authenticated by HP Anywhere's authentication framework, the authenticated users' security context information is transported from HP Anywhere to the backend system PPM Center using LW-SSO token in a REST Web Service call.

Starting from PPM Center version 9.13, the following line is added to the `websecurity.conf` file to enable RESTful web services:
`/rest=com.kintana.core.web.servlet.AllAccessURLSecurity`
Check and make sure whether the above line is already there. If not, simply copy and paste it to the `websecurity.conf` file.

For more information about RESTful web services, see the *Web Services Programmer's Guide*.

As a proxy to the PPM Center product, PPM apps support the following two user authentication modes that work with the HP Anywhere authentication framework:

- **Basic authentication** — No additional configuration work is required on the PPM Server side if you select this authentication mode in the HP Anywhere – Administrator Console. For more information, see *ENABLE_LW_SSO_WEB_SERVICE_IN* on page 22.
- **Web service lightweight single-on (LW-SSO)** — If you configure the PPM apps to use the LW–SSO authentication mode, you need to configure LW–SSO authentication support on PPM Server side. This is the only configuration task required on PPM Server side for the apps to work properly. For details, see *Configuring PPM Center for LW-SSO Support* on page 21.

Configuring PPM Center for LW-SSO Support

Read *LW-SSO Security Warnings* on page 25 before you configure the LW-SSO UI.

To configure PPM Center for LW-SSO authentication support,

1. Add the parameters described in the following table into the `server.conf` file and provide values for them.

Parameter	Description
ENABLE_LW_SSO_WEB_SERVICE_IN	Newly added for the PPM Requests app. Enables the LW-SSO web services and PPM Center supports LW-SSO authentication mode when set to `true`. When set to `false`, PPM Center supports basic authentication mode. Default: `false` **Note:** Setting the parameter value to `true` enables LW-SSO authentication mode and disables basic authentication on PPM Center.
LW_SSO_DOMAIN	Specifies LW-SSO domain, for example, `xyz.com`.
LW_SSO_INIT_STRING	Specifies the string value for the `initString` parameter. This should be consistent with the setting in the `lwssofmconf.xml` file from the HP Anywhere server. For more information about the `initString` parameter, see *LW-SSO Security Warnings* on page 25.
LW_SSO_EXPIRATION_PERIOD	Specifies LW-SSO token expiration period in minutes. For example, `60`.
LW_SSO_TRUSTED_DOMAIN	Specifies one or more LW-SSO trusted domains. Use semicolon (;) to separate multiple domains. For example, `xyz.come;abc.net`. Set this parameter value to your domain.
SINGLE_SIGN_ON_LWSSO_PLUGIN	Newly added. Specifies the plug-in that is used to authenticate users to PPM Center on incoming Web service request. Default: `com.kintana.sc.security.auth.WSRemoteUserSingleSignOn`.

If you configured LW-SSO support on PPM Center before, you might notice that the following parameters already exist. They are not required for the PPM Requests app, you may leave them as is so that LW-SSO support for other features are not interrupted.

- ENABLE_LW_SSO_UI
- LW_SSO_CLEAR_COOKIE
- ENABLE_LW_SSO_WEB_SERVICE

2. Run **`kUpdateHtml.sh.`**
3. Stop, and then restart the server.

LW-SSO Authentication - General References

This appendix contains information relating to Lightweight Single Sign-on (LW-SSO) Authentication, providing necessary LW-SSO concepts and references to PPM Center administrators.

This appendix includes:

LW-SSO Authentication Overview

LW-SSO is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The information in this section applies to LW-SSO version 2.2 and 2.3.

LW-SSO Token Expiration

The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.

Recommended configuration of the LW-SSO Token expiration

Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

GMT Time

All applications participate in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.

Multi-domain Functionality

Multi-domain functionality requires that all applications participating in LW-SSO integration configure the `trustedHosts` settings (or the `protectedDomains` settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the `lwsso` element of the configuration.

Get SecurityToken for URL functionality

To receive information sent as **SecurityToken for URL** from other applications, the host application should configure the correct domain in the `lwsso` element of the configuration.

LW-SSO System Requirements

The following table lists LW-SSO configuration requirements:

Product	Version	Comments
Java	1.5 and higher	
HTTP Servlets API	2.1 and higher	
Internet Explorer	6.0 and higher	The browser should enable HTTP session cookie and HTTP 302 Redirect functionality.
FireFox	2.0 and higher	The browser should enable HTTP session cookie and HTTP 302 Redirect functionality.
JBoss authentications	• JBoss 4.0.3 • JBoss 4.3.0	
Tomcat authentications	• Standalone Tomcat 5.0.28 • Standalone Tomcat 5.5.20	
Acegi authentications	• Acegi 0.9.0 • Acegi 1.0.4	
Spring Security Authentication	Spring Security 2.0.4	
Web Services engines	• Axis 1 - 1.4 • Axis 2 - 1.2 • AX-WS-RI 2.1.1	

LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

- **Confidential `initString` parameter in LW-SSO.** LW-SSO uses Symmetric Encryption to validate and create a LW-SSO token. The `initString` parameter within the configuration is used for initialization of

the secret key. An application creates a token, and each application that uses the same `initString` parameter validates the token.

- It is not possible to use LW-SSO without setting the `initString` parameter.
- The `initString` parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
- The `initString` should be shared only between applications integrating with each other using LW-SSO.
- The `initString` parameter should have a minimum length of 12 characters.

- **Enable LW-SSO only if required.** LW-SSO should be disabled unless it is specifically required.

- **Level of authentication security.** The Application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications, determines the level of authentication security for all the applications.

  It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

- **Symmetric encryption implications.** LW-SSO uses symmetric cryptography for issuing and validating LW-SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same `initString` parameter. This potential risk is relevant when an application sharing the `initString` either resides, or is accessible from, an untrusted location.

- **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. It is recommended that you share the same user registry (as LDAP/AD) among all integrated applications.

  Failure to map users may cause security breaches and negative application behavior. For example, the same user name may be assigned to different real users in the various applications.

  In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually

log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.

- **Identity Manager.** Used for authentication purposes, all unprotected resources in the Identity Manager must be configured as `nonsecureURLs` settings in the LW-SSO configuration file.
- **LW-SSO Demo mode**
  - The Demo mode should be used for demonstrative purposes only.
  - The Demo mode should only be used in unsecured networks.
  - The Demo mode must not be used in production. Any combination on the Demo mode with the production mode should not be used.

Troubleshooting and Limitations

Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

  Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

  Similarly, if the `IdM` token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

- **Multi domain logout functionality when using Internet Explorer 7.** Multi domain logout functionality may fail when using Internet Explorer 7 and when the application is invoking more then three consecutive HTTP 302 redirect verbs in the logout procedure.

In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an `Internet Explorer cannot display the webpage` error page instead.

As a workaround, we recommend that, if possible, you reduce the number of application redirect commands in the logout sequence.

Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client Access to the Application**

  If a domain is defined in the LW-SSO configuration:

  - The application's clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL. For example, http://myserver.**companydomain**.com/WebApp
  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp
  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp

  If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. Note that in this case a LW-SSO session cookie will be created specifically for a single machine without any domain information, and therefore will not be delegated by the browser to another, and will not pass to other computers located in the same DNS domain. This means that SSO will not work in the same Domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.

- **Multi domain support**

  - Multi domain functionality is based on the HTTP referer. Therefore, LW-SSO supports links from one application to another and does not

support typing a URL into a browser window, except when both applications are in the same domain.

- The first cross domain link using **`HTTP POST`** is not supported

  Multi domain functionality does not support the first **`HTTP POST`** request to a second application (only the **`HTTP GET`** request is supported). For example, if your application has an HTTP link to a second application, an **`HTTP GET`** request is supported, but an **`HTTP FORM`** request is not supported. All requests after the first can be either **`HTTP POST`** or **`HTTP GET`**.

- LW-SSO Token size

  The size of information that LW-SSO can transfer from one application in one domain to another application on another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

- Linking from Protected (HTTPS) to non protected (HTTP) in a Multi domain scenario

  Multi domain functionality does not work when linking from a protected (HTTPS) to a non protected (HTTP) page. This is a browser limitation where the referer header is not sent when linking from a protected to a non-protected resource. For an example, see http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- Third-Party cookie behavior in Internet Explorer:

  Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences (P3P) Project", meaning that cookies coming from a Third Party domain are blocked by default in the Internet security zone. Session cookies are also considered Third Party cookies by Internet Explorer, and therefore are blocked, causing LW-SSO to stop working. For details, see http://support.microsoft.com/kb/323752/en-us.

  To resolve this issue, add the launched application (or a DNS domain subset as ***.mydomian.com**) to the Intranet/Trusted zone on your computer (in Microsoft Internet Explorer, select **Menu > Tools >**

Internet Options > Security > Local Intranet > Sites > Advanced), which causes the cookies to be accepted.

The LW-SSO session cookie is only one of the cookies used by the Third Party applications that are blocked.

- **SAML2 token**
  - Logout functionality is not supported when the SAML2 token is used.

    Therefore, if the SAML2 token is used to access a second application, then a user who logs out in the first application will not be logged out in the second application.
  - The SAML2 token's expiration is not reflected in the application's session management.

    Therefore, if the SAML2 token is used to access a second application, then each application's session management will be handled independently of each other.
- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.
- **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

  It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the `common\classes` Tomcat folder.
- **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.
- **Demo mode.** In Demo mode, LW-SSO supports links from one application to another but does not support typing a URL into a browser window due to an HTTP **referer** header absence in this case.

A Troubleshooting

This chapter contains troubleshooting suggestions for issues relating to configuring and working with PPM Requests app.

This chapter includes:

Error Message List for Troubleshooting

Table A-1 lists all error messages administrators or end users might encounter as well as their possible causes.

Table A-1. Error message list for troubleshooting

Error Message	Possible Error Causes
Go to Settings	Data source deleted.
	BasicAuth, PPM user name/password changed.
This app is currently unavailable	PPM Server shutdown.
	LWSSO, PPM user does not exist.
No Data to Display (on Front Page)	Data source deleted.
	PPM Server shutdown.
	BasicAuth, PPM user name/password changed.
	LWSSO, PPM user does not exists.
	User loads front page, but the operation times out.
An error has occurred. Unable to connect to remote server, check server availability.	User refreshes request summary page, but the operation times out.
PPM not responding. Check your settings!	Data source deleted.
	PPM Server shutdown.
	BasicAuth, PPM user name/password changed.

Error Message	Possible Error Causes
Loading times out. Please try again later.	User taps into the request list page, but the operation times out.
	User refreshes the request list page, but the operation times out.
	User loads more requests, but the operation times out.
	User taps into the request detail page, but the operation times out.
	User taps **Notes** tab on the request detail page, but the operation times out.
	User loads more notes on Notes tab of the request detail page, but the operation times out.
Your request is being processed.	User approves a request, but the operation times out.
	User taps **Continue** on reconfirm page, but the operation times out.
Session Expired.	Session expired.
Validation failed: INTERNAL_ERROR	Data source deleted.
Validation failed: Wrong user name or password	BasicAuth, PPM user name/password changed.
	LWSSO, PPM user does not exist.
	PPM Server shutdown.
Validation failed: undefined	Validating data source, but the operation times out.
	Session expired while validating data source.

RESTful Web Services Not Enabled

Problem Description

- Nothing displays on the summary view after users logging in to HP Anywhere from their mobile devices. Or,
- No PPM Requests card displays after logging in to HP Anywhere from their mobile devices. Or,
- After users logging in to HP Anywhere and tapping 

on the quick launch bar, the Front Page displays "`No Data to Display`" message.

Troubleshooting

- RESTful web services on PPM Center side might not be configured.

  Check whether the following line is present in the `<PPM_Home>/conf/websecurity.conf` file:
  `/rest=com.kintana.core.web.servlet.AllAccessURLSecurity`

  If not, simply copy and paste the line into the `websecurity.conf` file to enable the RESTful web services.

- The PPM Request app is not installed on users' mobile devices.

  For details, see the *PPM Requests app User Guide*.

- Users have not specified their roles on their mobile devices.

  For details, see the *PPM Requests app User Guide*.

- If the PPM Requests card is still not visible after users having tried all the above solutions, the administrator shall check in the HP Anywhere — Administrator Console whether the PPM Requests app is available and enabled there.

Support

Bundle Cannot Be Started

Problem Description

While starting the HP Anywhere server, you may receive an error message ("`bundle can't be started`") in HP Anywhere — Administrator Console or found such error message in the server log.

Troubleshooting

1. Restart the HP Anywhere server, and then check whether the issue occurs again.
2. If the issue occurs again, stop the server and delete cache files in the following directories:
   - `<HPA_Server_Home>\glassfish\glassfish\domains\BTOA\generated`
   - `<HPA_Server_Home>\glassfish\glassfish\domains\BTOA\osgi-cache`

   For Windows users, also delete cache files in the following directory:
   - `C:\users\<username>\AppData\Local\Temp`

"Service Cannot Be Found" Error

Problem Description

When starting the HP Anywhere server, sometime you may receive an error message ("`service cannot be found`") in HP Anywhere — Administrator Console or found such error message in the server log. This service is JMS service, and you will also receive connection error info.

Workaround

Reinstall the HP Anywhere server into a fresh directory.

Test Connection Failed When Using LWSSO

Problem Description

After adding a PPM Server instance in the HP Anywhere — Administrator Console that uses LWSSO as the authentication policy, test connection fails when the administrator clicks **Test Connection**.

Troubleshooting

Check the `server.conf` file to see whether you have configured the following two parameters:

- `LW_SSO_DOMAIN`
- `LW_SSO_TRUSTED_DOMAIN`

Make sure that the values of the two parameters point to the same domain. Otherwise, HP Anywhere and PPM Center would be located in different domains.

Or, you can simply remove these two parameters from the `server.conf` file.

Notification Not Pushed Successfully

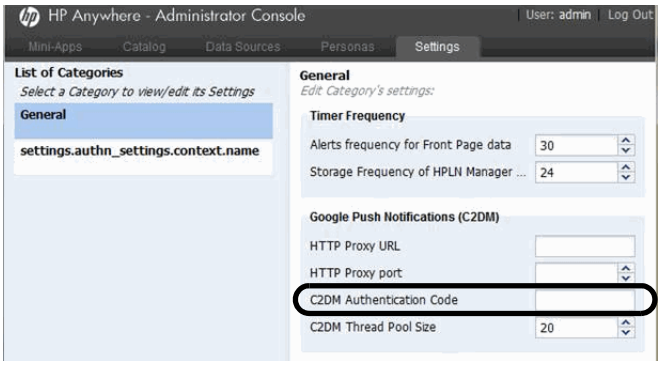
Problem Description

End users have created their alerts, but notifications were not pushed successfully.

Troubleshooting

Administrators should edit the C2DM setting in the HP Anywhere — Administrator Console: On the Settings tab, copy and paste the following value (no space) into the **C2DM Authentication Code** field:

```
DQAAAKoAAABFYMFxWfuY3hp5HAUQuEXYQ9G76xCLAE9hkthmvSvzdh_
kyBWgigudh5CmnHqpYWkaM05Tuyihlhmi_
ZI-pEDg24eroHXHXqtwyokQN06MNlOi9d-tecBe6rHl4o2eelYFbU0IsHrRngwN
1aXIsS4uoYFP-yo1SzFjrcMUJdEXCAc_
CYbhYPOnB7TGy25GAQizmnoyQcpMyMtVjM0D4hHALiMSFP-s_0i1XzGLznIixQ
```



Google may update the C2DM token periodically.

If the HP Anywhere server needs proxy to access the Internet, make sure to configure the **HTTP Proxy URL** and **HTTP Proxy port** fields as well.