HP Propel

Software Version 2.00
CentOS Operating System

Administration Guide

Document release date: July 2015

Software release date: July 2015

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

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.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

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 the following URL and sign-in or register: https://softwaresupport.hp.com/

Use the Search function at the top of the page to find documentation, whitepapers, and other information sources. To learn more about using the customer support site, go to: https://softwaresupport.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

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 https://softwaresupport.hp.com/

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

To learn more about using the customer support site, go to:

https://softwaresupport.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

Contents

Overview

This document provides information about administration tasks for HP Propel.

The following information is provided in this document:

Overview. Describes the audience for this guide and where to find additional HP Propel information**.**

HP Propel Tips. Provides miscellaneous information for HP Propel, including verification of the GPG code signing for the HP Propel OVA file, customizing the HP Propel Portal and Launchpad, manually changing the keystore password, changing the HP Service Manager port number, and understanding consumer and administrative roles.

Configuring SSL for HP Propel**.** Explains how to replace the previously generated HP Propel SSL certificates with Certificate Authority-signed SSL certificates.

HP Knowledge Management**.** Provides the instructions for the optional task of loading HP Knowledge Management documents into HP Service Manager and installing the Solr plugin for IDOL search**.**

Changing HP Propel Default User Accounts' Passwords**.** Provides the default passwords for the HP Propel user accounts and instructions for changing them, which HP recommends for increased security.

Audience

The person who administers HP Propel should have knowledge of or work with someone who has knowledge of the following:

- Configuring SSL certificates
- Executing Linux operating system commands with the Bash shell

Additional Information

Refer to the following guides for more information about HP Propel:

- HP Propel requirements: *HP Propel System and Software Support Matrix*
- HP Propel latest features and known issues: *HP Propel Release Notes*
- HP Propel installation and configuration: *HP Propel Installation and Configuration Guide*
- HP Propel troubleshooting tips: *HP Propel Troubleshooting Guide*
- HP Propel security considerations: *HP Propel Security Guide*

These guides are available from the HP Software Support website at https://softwaresupport.hp.com. (This website requires that you register with HP Passport.)

You need to sign in or register to use this site. Use the **Search** function at the top of the page to find documentation, whitepapers, and other information sources. To learn more about using the customer support site, go to:
https://softwaresupport.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

For more information or to track updates for all HP Propel documentation, refer to the *HP Propel Documentation List*.

To help us improve our documents, please send feedback to Propel_IE@hp.com.

HP Propel Tips

Verifying GPG Code Signing – HP Propel OVA File

Tip: If your system does not have the `gpg` tool, you can download it from
https://www.gnupg.org/download.

To verify that the HP Propel OVA file is signed with GNU Privacy Guard (GPG), you must download the
`.sig` file and the HP keys from https://softwaresupport.hp.com. Perform the following procedure on the
system that you downloaded the OVA file, the `.sig` file, and the HP keys.

1. Install HP's public keys:

   ```
   # gpg --import hpPublicKey.pub
   # gpg --import hpPublicKey2048.pub
   ```

2. Validate and verify the digital signature of the signed OVA file. The output from the command
   indicates the validity of the signature.

   ```
   # gpg --verify <OVA_FILE>.sig <OVA_FILE>
   ```

   If the level of trust on the key has not been set, you will see a trust level warning similar to this:

   ```
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg: There is no indication that the signature belongs to the owner.
   ```

3. If you do not want to see the warning in Step 2, edit the key to set the trust level of the key for proper
   verification:

   ```
   # gpg --edit-key "Hewlett-Packard Company"
   ```
   (Type the command "trust", select "5" for trusting the key, then confirm and quit.)

   Note: You can trust these public keys.

4. You must also trust the RSA key:

   ```
   # gpg --edit-key "Hewlett-Packard Company RSA"
   ```
   (Type the command "trust", select "5" for trusting the key, then confirm and quit.)

After performing the above procedure, you should not see the warning about an untrusted identity when
verifying the signature.

Here is an example of output from a verification:

```
# gpg --verify <OVA_FILE>.sig <OVA_FILE>
gpg: Signature made Thu 03 Jan 2013 04:48:47 PM UTC using RSA key ID 5CE2D476
gpg: Good signature from "Hewlett-Packard Company RSA (HP Codesigning Service)"
```

Customizing the HP Propel Portal

You can customize the display of the HP Propel Portal. For details about customizing the portal, themes,
and widgets, refer to the *HP Propel Customizing the Portal* whitepaper.

Customizing the HP Propel Launchpad

You can customize the display of the HP Propel Launchpad. For details about customizing the launchpad,
themes, and widgets, refer to the *HP Propel Customizing Launchpad* whitepaper.

Manually Changing the Keystore Password

The keystore password on the HP Propel is automatically changed to "propel2014" during the initial installation. Though not required, HP recommends that you change the default keystore password for the HP Propel VM. To change the keystore password, execute the following commands:

```
# <PROPEL_PORTAL_VM_JRE_DIR>/keytool –storepasswd –storepass propel2014
-new <NEW_KEYSTORE_PASSWORD> -keystore /opt/hp/propel/security/propel.truststore
# ./configureKeys.sh --setkspassword <NEW_KEYSTORE_PASSWORD>
```

Where *PROPEL_PORTAL_VM_JRE_DIR* is the JRE directory on the HP Propel VM and *NEW_KEYSTORE_PASSWORD* is the new keystore password that you specify.

Changing the HP Service Manager Port Number

During the HP Propel installation, a default port number for communication between HP Propel and HP Service Manager (HP SM) is specified in the `/opt/hp/propel/sx/WEB-INF/classes/config/sm/instances.json` file.

You may want to change this default port number for the following reasons:

- To avoid using web services over the HP SM LoadBalancer port, which is commonly set to port 13080.

- To change the port number for communication between HP Propel and HP SM from HTTP to HTTPS.

Perform the following procedure to change the port number used for communication between HP Propel and HP SM:

1. On the HP Propel VM, edit the `/opt/hp/propel/sx/WEB-INF/classes/config/sm/instances.json` file and revise the HP SM port number that is currently configured for HTTP. Note that an additional HP SM system can be added to the `instances.json` file to use HTTPS.

2. Restart the HP Propel services. See Restart HP Propel for instructions.

Important: If the HP SM port was changed from HTTP to HTTPS, SSL integration must be configured for HP SM. Refer to the *SSL Configuration for HP SM Integration* section in *HP Propel Installation and Configuration Guide* for instructions.

Understanding Administrative and Consumer Roles in HP Propel

Access to applications in HP Propel is controlled through HP Propel users. There are three types of HP Propel users:

- Administrator:
    - Logs in as the *admin* user with the *cloud* password at
      `$Propel_Hostname:9000/org/Provider`
    - Manages HP Propel settings across all of the organization. For example, managing organizations or content packs.
    - Has access to the Identity and Content Management applications.
- Organization Administrator:
    - Logs in as the *orgadmin* user with the *cloud* password at
      `$Propel_Hostname:9000/org/CONSUMER`
    - Manages the organization, aggregates and manages catalog items, manages catalogs and categories. Additionally can perform all Organization Consumer functions (for example shopping and support requests).
    - Has access to the Shop, Subscriptions, Knowledge, Request Support, Catalogs, Catalog Items, Categories, Policies, and Catalog Connect applications.
- Organization Consumer:
    - Logs in as the *consumer* user with the *cloud* password at
      `$Propel_Hostname:9000/org/CONSUMER`
    - Performs shopping, manages subscriptions, searches knowledge articles, and requests support.
    - Has access to the Shop, Subscriptions, Knowledge, and Request Support applications.

Where `$Propel_Hostname` is the fully qualified host name of the HP Propel VM.

Configuring SSL for HP Propel

HP Propel requires HTTPS (HTTP over SSL) for client browsers. HTTPS must be configured between HP Propel and any end-point systems (HP Cloud Service Automation and HP Service Manager).

Tip: Refer to the installation instructions in the *HP Propel Installation and Configuration Guide* for different methods of configuring SSL for HP Propel.

Replacing Generated HP Propel SSL Certificates with CA-Signed Certificates

This section explains how to replace the previously generated HP Propel SSL certificates with Certificate Authority-signed SSL certificates. (The generated HP Propel SSL certificates are created and configured by using the `/opt/hp/propel-install/propel-ssl-setup.sh auto` command when installing HP Propel.)

Although a self-signed certificate can be used in production, HP recommends that you replace this certificate by configuring a trusted certificate from a Certificate Authority (CA). Some organizations issue certificates that are signed by a corporate CA and some organizations get certificates from a trusted third-party CA, such as VeriSign.

Tips:

- In the following instructions, `$PROPEL_VM_HOSTNAME` represents the fully qualified hostname of the HP Propel VM. You can set this as an environment variable with the following command on the HP Propel VM:

  `# export PROPEL_VM_HOSTNAME=`*`mypropelhost.example.com`*

- The password is "changeit" for the HP Propel truststore (`/usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts`)

- The password is "propel2014" for the HP Propel keystore (`/opt/hp/propel/security/.keystore`)

Perform the following steps to replace the previously generated HP Propel SSL certificates with CA-signed SSL certificates:

Important: The following commands are run as `root` on the HP Propel VM. (The default password is "propel2015" for the `root` user.)

1. Stop the HP Propel services:

   `# propel stop`

2. Load the Certificate Authority (CA) into the global Java keystore. This file is in a PEM format, with extensions such as `.pem`, `.crt`, `.cer`, and `.key`.

   a. Copy the file to `/opt/hp/propel-install/ssl-tmp/CA.crt`. (The exact file name must be used.)

   b. Import the CA into the HP Propel keystore:

   `# keytool –import –file /opt/hp/propel-install/ssl-tmp/CA.crt –alias CA –trustcacerts –keystore /usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts`

3. Back up the existing SSL configuration:

   ```
   # cd /opt/hp/propel
   # cp –rp security security.backup
   ```

4. Initialize the SSL working directory:

    ```
    # cd /opt/hp/propel-install
    # ./propel-ssl-setup.sh init
    ```

    By default, the SSL working directory is `/opt/hp/propel-install/ssl-tmp`.

5. *Optional* – Only if your HP Propel VM needs multiple hostnames, all of these name must appear in the certificate. This is achieved by using the Subject Alternative Names (SAN) attribute. Edit the `/etc/pki/tls/openssl.cnf` file.

    Make sure it has entries like the following

    ```
    # This is required for TSA certificates.
    # extendedKeyUsage = critical, timeStamping

    [ v3_req ]

    # Extensions to add to a certificate request

    basicConstraints = CA:FALSE
    keyUsage = nonRepudiation, digitalSignature, keyEncipherment
    subjectAltName = @alt_names

    [alt_names}
    DNS.1 = server1.example.com
    DNS.2 = mail.example.com
    DNS.3 = www.example.com
    ```

    Important: the host name returned from the `hostname` command must also appear as one of the SAN entries in `openssl.cnf`.

6. Generate the Certificate Signing Request (CSR) and Server Private Key pair:

    ```
    # cd /opt/hp/propel-install
    # ./propel-ssl-setup.sh --password <PASSWORD> generateSigningRequest <SUBJECT>
    ```

    Where *PASSWORD* is the passphrase (default is "propel2014") used to encrypt the generated private key and *SUBJECT* is the signing request subject in the slash-separated form. "CN" must be the last field in the subject and contain the fully qualified hostname of the HP Propel VM. Enclose the subject in double quotes, such as:
    "/C=US/ST=CA/L=San Jose/O=StartUpCompany/OU=Software/CN=mypropelserver.example.com"

    This command creates two new directories and four new files
    `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/` directory
    `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/` directory
    `/opt/hp/propel-install/ssl-tmp/hostnames` file
    `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/private.key.pem` file
    `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/propel_host.key.csr` file
    `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.key.rsa` file

7. You can verify the content of your CSR by pasting the text in here:
    https://ssltools.websecurity.symantec.com/checker/views/csrCheck.jsp

8. Send the CSR containing the public key to your CA. This is a process specific to your company, and network administrators should know how to accomplish this. Ask for the certificate to be delivered in PEM format. If it is not, you can convert formats with the `openssl` command.

9. After the certificates have been received, copy the host certificate to:
    `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt`

10. Validate the certificate and the CA match:

```
# openssl verify –verbose –CAfile /opt/hp/propel-install/ssl-tmp/CA.crt
/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt
```

You should see the following message:
```
/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt: OK
```

Important: Do not proceed if you see any error messages. The CA and certificate must match. Restart this procedure if necessary.

11. Create the certificate and the key stores:

```
# /opt/hp/propel-install/propel-ssl-setup.sh finish
```

12. Move all the created files into their final locations:

```
# cd /opt/hp/propel-install/overlay/_ALL_HOSTS_/security
# cp –p * /opt/hp/propel/security
# cd /opt/hp/propel-install/overlay/$PROPEL_VM_HOSTNAME/security
# cp –p * /opt/hp/propel/security
# cp –p .keystore /opt/hp/propel/security
```

13. HP Operations Orchestration (HP OO) needs to be updated.

a. First, back up the existing configuration:

```
# cd /opt/hp/oo/central/var
# cp –rp security security.backup
```

b. Next, manually delete the old certificates from the HP OO stores and install the new certificates:

```
# keytool –delete –keystore
/opt/hp/oo/central/var/security/client.truststore –alias propel_host
- storepass changeit –noprompt

# keytool –importcert –keystore
/opt/hp/oo/central/var/security/client.truststore –file
/opt/hp/propel/security/propel_host.crt –alias propel_host –storepass changeit
–noprompt

# keytool –delete –keystore
/opt/hp/oo/central/var/security/client.truststore –alias
propeljboss_$PROPEL_VM_HOSTNAME –storepass changeit –noprompt

# keytool –importkeystore –noprompt –srcstoretype PKCS12 –srckeystore
/opt/hp/propel/security/propel_host.pfx –srcstorepass propel2014 –destkeystore
/opt/hp/oo/central/var/security/client.truststore –deststorepass changeit

# keytool –delete –keystore /opt/hp/oo/central/var/security/key.store –alias tomcat
–storepass changeit –noprompt

# keytool –importkeystore –noprompt –srcstoretype PKCS12 –srckeystore
/opt/hp/propel/security/propel_host.pfx –srcstorepass propel2014 –destkeystore
/opt/hp/oo/central/var/security/key.store –deststorepass changeit –srcalias
propeljboss_$PROPEL_VM_HOSTNAME –destalias tomcat

# keytool -keypasswd –new changeit –keystore
/opt/hp/oo/central/var/security/key.store –storepass changeit –alias tomcat
–keypass propel2014
```

14. Restart HP Propel:

    ```
    # propel start
    ```

15. Make sure you can log in to the HP Propel Launchpad.

HP Knowledge Management

This section provides instructions for installing HP Knowledge Management (KM), installing and configuring the Solr plugin for IDOL search, and loading KM documents into HP Service Manager (HP SM).

HP Knowledge Management Installation

Install HP Knowledge Management if it was not installed during HP Service Manager installation. The HP ITSM Deployment Manager (HP DM) simplifies setup of HP SM and its related components.

1. Access HP ITSM Deployment Manager from HP Live Network at: https://hpln.hp.com/group/itsm-deployment-manager. Note that you need to sign in to your HP Passport account. Download the following:

   a. *HP ITSM Deployment Manager Quick Start Guide* (https://hpln.hp.com/node/22326/attachment)

   b. The most recent version of HP DM (https://hpln.hp.com/node/18528/contentfiles)

2. Follow the instructions in the HP DM Quick Start Guide to install and configure HP DM.

3. In the HP DM **Environments** tab, click **More Wizards…**, then select **HP Service Manager – Knowledge Management**, and follow the instructions to install KM.

4. HP SM must be restarted for KM to become available for use.

For more information on the HP KM Search Engine, see the *HP Service Manager Release Notes* and *Service Manager Interactive Installation Guide* at https://softwaresupport.hp.com.

Note: Though optional, HP recommends that the HP SM Help Server is also installed. The HP SM Help Server includes the *Knowledge Management Search Engine Guide* as well as an extensive *Knowledge Management* help topic.

HP Knowledge Management Indexing

The `KMUpdate` process controls indexing. Use HP SM's **Update Indexes** form to stop and restart indexing, and to view the status statistics related to indexing. To access this form, from the HP SM navigator menu, select **Knowledge Management** -> **Configuration** -> **Update Indexes**.

For help with KM indexing, search the HP SM Help Server for the topic "**indexing the knowledgebases**".

Tip: A quick way to verify that `KMUpdate` is running s to type `status` in the Command window to display all processes currently running.

HP Knowledge Management Best Practices

- Rather than using the *falcon* operator as an integration account, create a copy of *falcon* using the HP SM **User Quick Add Utility (**from the HP SM navigator menu, select **System Administration** > **Ongoing Maintenance** > **User Quick Add Utility**). This simplifies analyzing the `sm.log` file. All possible integrations use *falcon* to log in, but after several integrations the operator's actions are more difficult to locate in the `sm.log` file.

- Before starting HP SM or HP SRC, start the KM Search Engine Service.

- HP Propel integration with SM's KM module will use both the KM Search Engine and an SM integration servlet to gather the documents and related attachments. Determine which port the master KM Search Engine uses as follows: from the HP SM navigator menu, select **Knowledge Management** > **Configuration** > **Configure Search Servers**, then click **Search**. By default, this will be port 8080.

  o Add the following lines to the HP SM's `sm.cfg` file. This configuration avoids using web services over the HP SM LoadBalancer port, which is often port 13080.

  ```
  # Propel: port used by Catalog Aggregation and Catalog microservices
  sm -httpPort:14090 -debugnode -log:../logs/propel_km_integration.log -
  ldapdisable:1 -ssl:0 -sslConnector:0 -trustedsignon:0 -querysecurity:0
  ```

  o Configure Propel's `setup.properties` file as follows:

  ```
  ### Knowledge Management
  km.url=http://sm_km_search_engine_solr_server.hp.com:8080
  km.attachUrl=http://sm_server.hp.com:14090
  km.user=INT-PROPEL
  km.password=password_for_the_km_integration_account
  ```

IDOL Search Installation and Configuration

To configure HP SM and KM to work with HP Propel Search, you must install the Solr plugin and configure it to send changes to HP Propel Search.
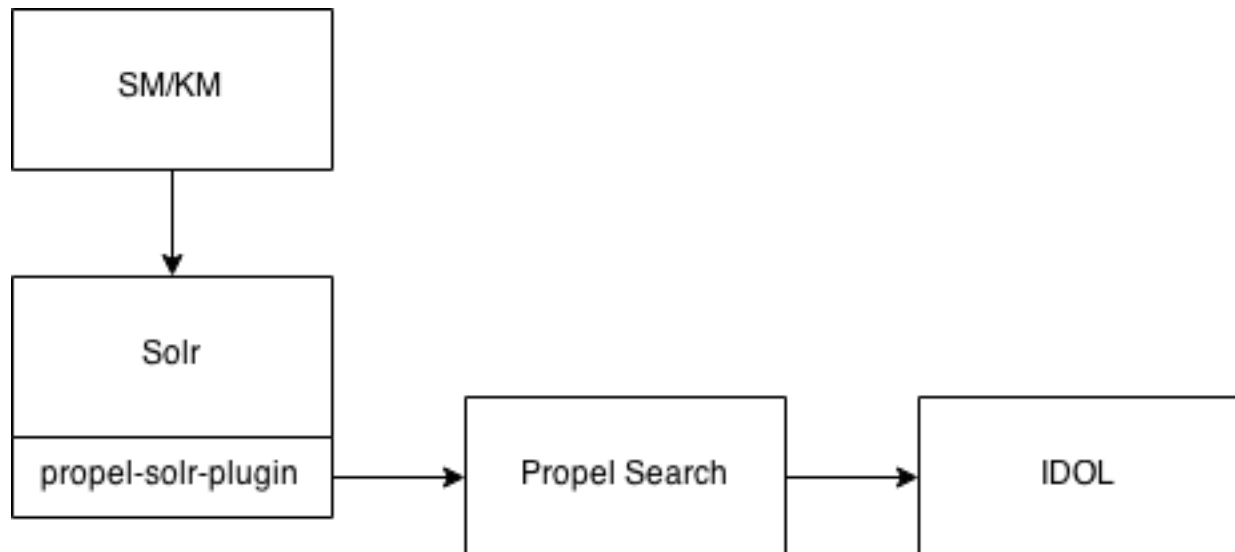

HP SM/KM indexes KM articles to Solr. HP Propel has a plugin to Solr, so all articles written to Solr are sent to HP Propel, which indexes it to IDOL.

Solr Plugin Installation Steps

1. On the HP Propel VM, copy the `/opt/hp/propel/search/propel-solr-plugin.zip` file to the HP SM/KM machine.

2. Unzip the `propel-solr-plugin.zip` file. The contents are:

   ```
   propel-solr-plugin-1.0-SNAPSHOT.jar
   jackson-mapper-asl-1.9.13.jar
   jackson-core-asl-1.9.13.jar
   jasypt-1.9.2.jar
   KMExtAccess.unl
   ```

3. Copy the `.jar` files to your primary search server. That is, copy `propel-solr-plugin-1.0-SNAPSHOT.jar`, `jackson-mapper-asl-1.9.13.jar`, `jackson-core-asl-1.9.13.jar`, and `jasypt-1.9.2.jar` to `<Primary_Search_Server>\Search_Engine\tomcat\webapps\KMCores\WEB-INF\lib\`
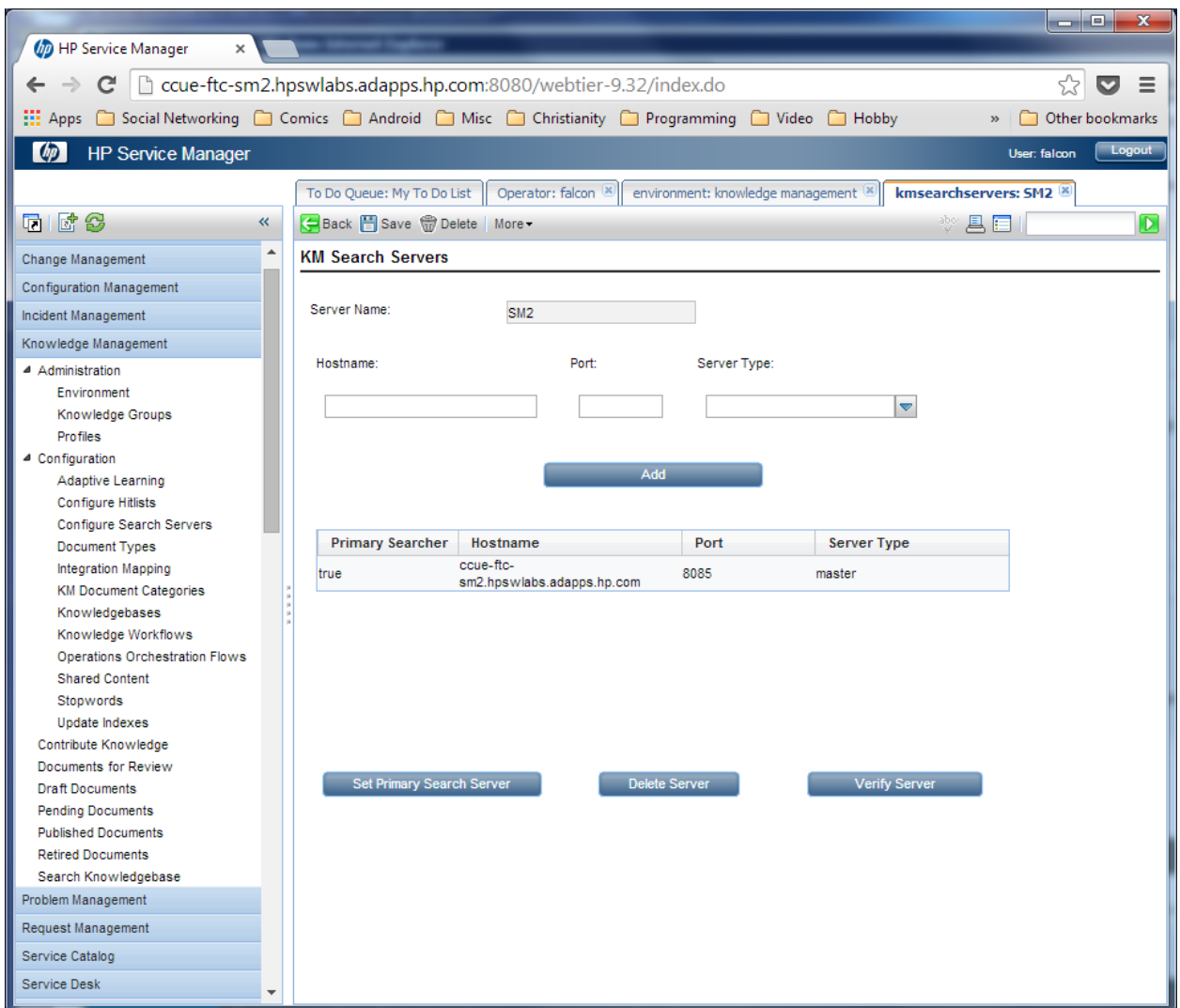
4. Edit the `<Primary_Search_Server_Home>`\Service Manager 9.30\Search_Engine\ kmsearchengine\KMCores\kmcore\conf\solrconf.xml file to add an updateRequestProcessorChain:

   Add `updateRequestProcessorChain` – solrconf.xml File Example

   ```
   <updateRequestProcessorChain name="propelSearch" default="true">
     <processor class="com.hp.propel.solr.plugin.PropelPushUpdateFactory">
       <str name="baseUrl">http://{Hostname:Port}/api/search/v1/article</str>
       <str name="username">searchTransportUser</str>
       <str name="password">{Password}</str>
       <str name="tenant">Provider</str>
     </processor>
     <processor class="solr.RunUpdateProcessorFactory"/>
   </updateRequestProcessorChain>
   ```

   Where *Hostname* is the hostname of HP Propel Search, *Port* is the port number of HP Propel Search, and *Password* is the password for searchTransportUser.

5. Update the same solrconf.xml and add the new updateRequestProcessorChain to the requestHandler.

   Add `updateRequestProcessorChain` to `requestHandler` – solrconf.xml File Example

   ```
   <requestHandler name="/update" class="solr.XmlUpdateRequestHandler">
     <lst name="defaults">
       <str name="update.processor">propelSearch</str>
     </lst>
   </requestHandler>
   ```

6. In the HP SM client, apply the KMExtAccess.unl unload file.

7. Restart KM.

8. Restart HP SM.

9. In the HP SM client, reindex KM.

    a. Select **Knowledge Management** -> **Administration** -> **Environment**.

    b. Check **SRC**.

    c. Select the **Search Server Name**.

    d. Click **Full Reindex**.
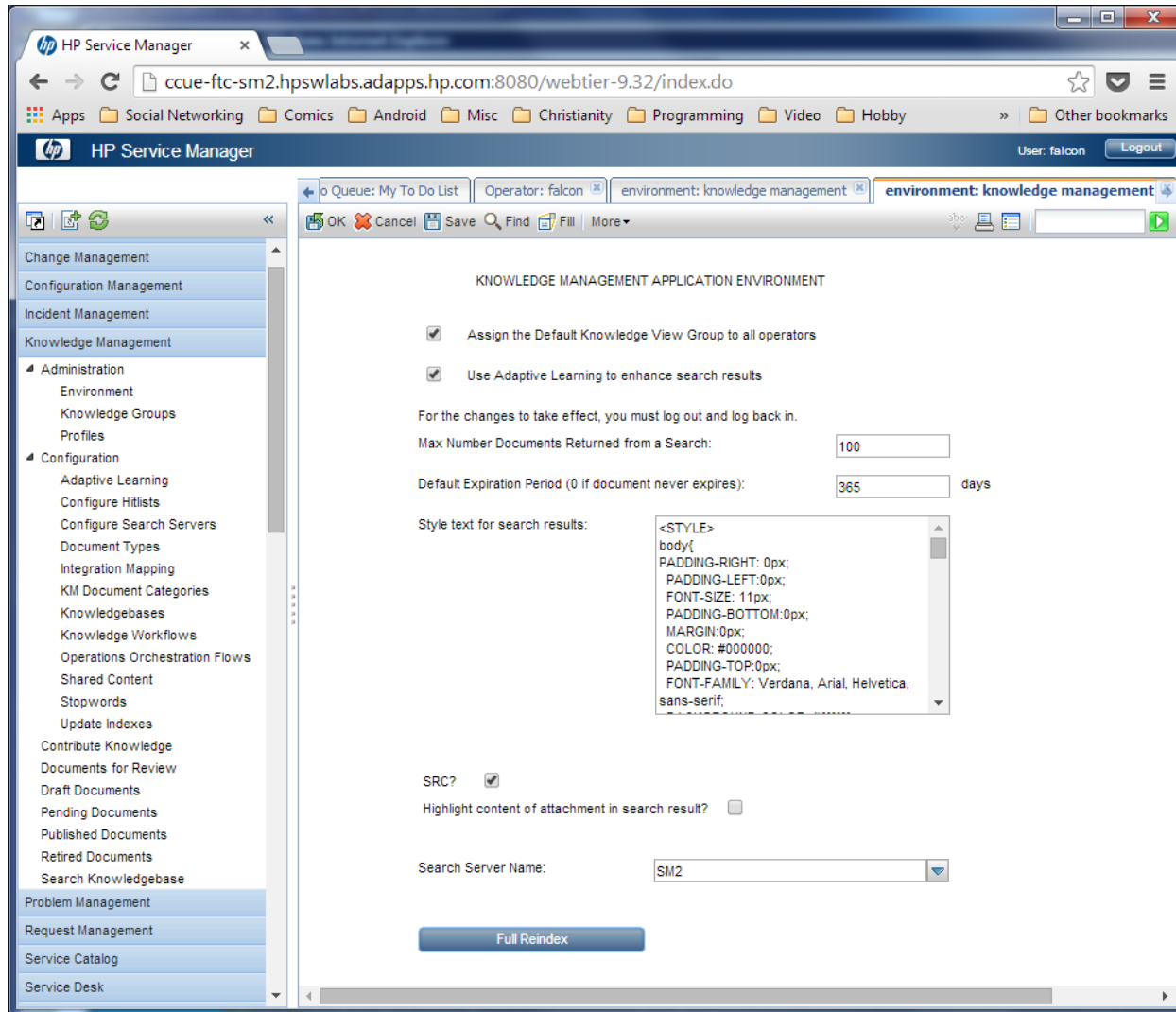
10. In the HP SM client, reindex the KM Libraries.

    a. Select **Knowledge Management** -> **Knowledgebases**.

    b. Click on each of the libraries, and then click **Full Reindex**.
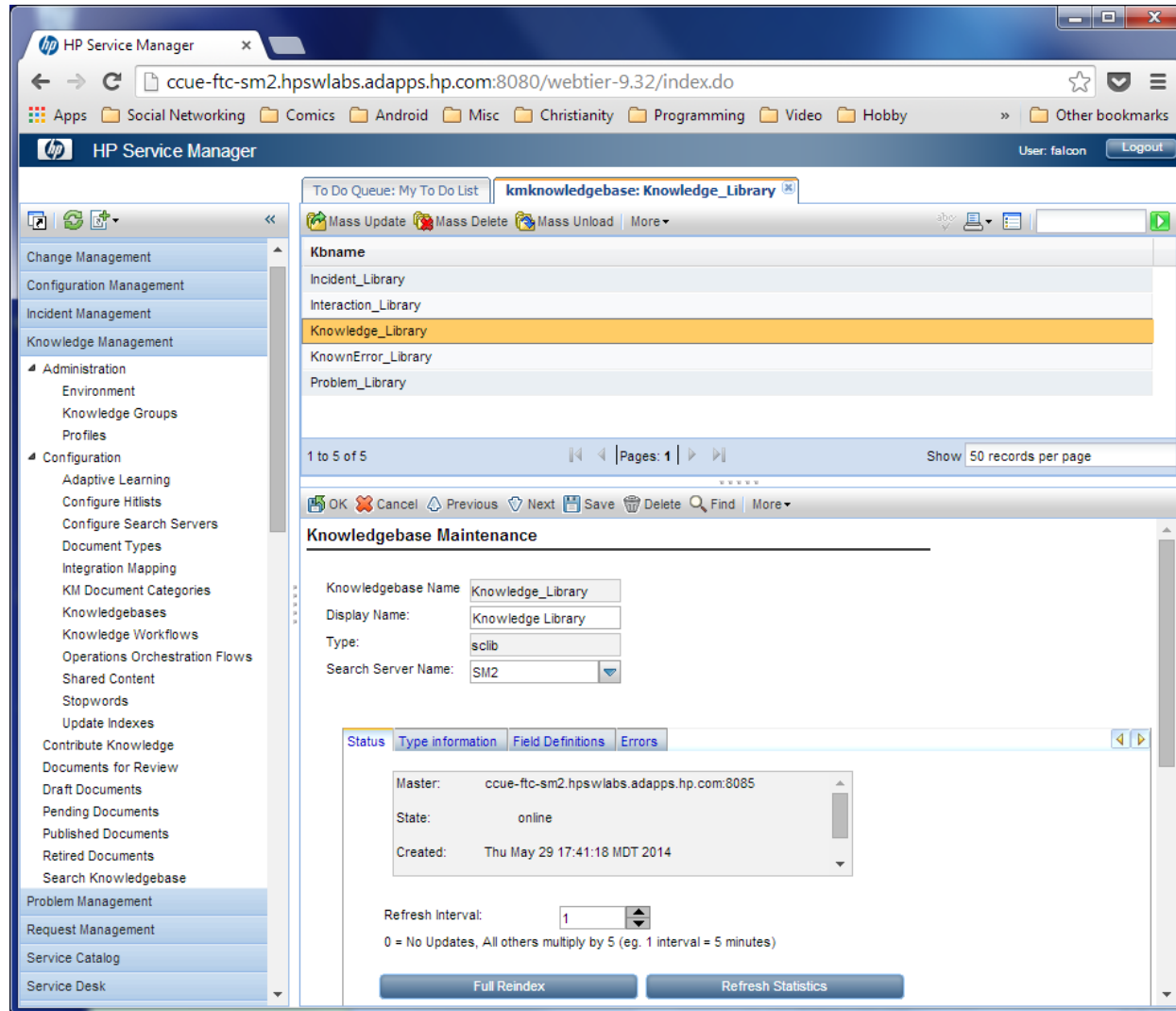
Load KM Documents into HP Service Manager

Note: The following instructions describe how to load sample KM documents into HP SM. Additional sample documents can be found in the KM installation directory. KM document packages can be purchased from companies such as KBI: http://www.kbi.com.

Pre-Requisites for Loading Documents

All documents loaded into HP SM have the following settings:

- Default status: **Externally Approved (external)**.
- docType: **Question/Answer (howto)**.
- Category: **Propel**.

Document Formats

Use the following formats for loading KM documents into HP SM:

- `<Title>`*propelKmImporter uses this text as the title and summary in HP SM*`</Title>`

- `<Introduction>`*propelKmImporter uses this text as the question in HP SM*`</Introduction>`

- `<Details>`*propelKmImporter uses this text as the answer in HP SM*`</Details>`

Sample KM Document

```
<? xml version="1.0" encoding="UTF-8"?>
<root><Title>Add an Email Account</Title>
<Introduction>&lt;div class="indent"&gt;&lt;span lang="es-cr"&gt;This page provides
steps for adding an email account.&lt;/span&gt;&lt;/div&gt;</Introduction>
<Details>&lt;div class="indent"&gt;&lt;ul&gt;&lt;li&gt;Follow these steps to add an
email account on your iOS device.&lt;/span lang="es-cr"&gt;:&lt;/span&gt;&lt;ol&gt
</Details>
<TrainingInfo><trainingRequirement>T</trainingRequiremen><imageItem></imageItem>
</TrainingInfo><SettingRequirement></SettingRequirement><title>This page has been
temporarily disabled</title></root>
```

KM Documents Directory Structure

The `Import` directory for the HP Propel Knowledge Importer must have the following structure:

- All folders that have documents to be imported must be in a folder named `products`.

- All folders that have images to be imported must be in a folder named `images`.

- The `products` and `images` folders must be located under the `Import` directory.

Figure 2 – Example Import Directory Structure
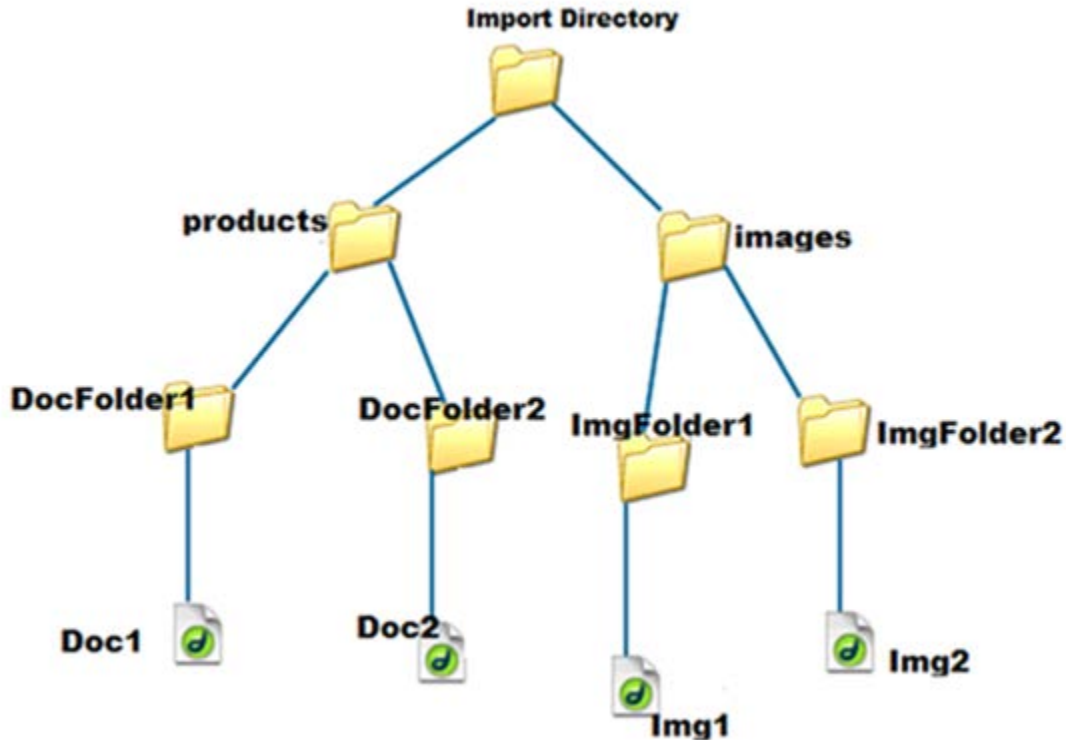
How to Load KM Documents

Follow this procedure to load KM documents with images into HP SM.

1. Import the HP Propel web services into HP SM:

   a. Transfer the `HPPropelKnowledge.unl` and `HPPropelKnowlegeAttachment.unl` web services files from the HP Propel VM to the HP SM system. The web services files are in the `/opt/hp/propel/km/webservices` directory on the HP Propel VM.

   b. Start HP SM, and in the HP SM left pane, navigate to: **System Administration** -> **Ongoing Maintenance** -> **Unload Manager** -> **Apply Unload.** The Unload Manager window is displayed.

   c. In the **Unload File** field, browse to the `HPPropelKnowledge.unl` web service file.

   d. In the **Backup To** field, type a name for the file to be stored as a backup. (This can be any name you choose.)

e. Click **Next**, and in the dialog that appears for applying the unload file, click **Yes**. A message appears confirming that the import was successful. The message text is: "Hotfix was successfully applied."

f. Click **Finish**.

g. Repeat Steps **b**. through **f**. for the `HPPropelKnowlegeAttachment.unl` web services file.

Note: Make sure the attachments flag is enabled in these two new HP SM web services.

2. To test the import process:

a. In HP SM, navigate to **Tailoring** -> **Web Services** -> **Web Service Configuration**.

b. Search for the **Service Name** `HPPropelKMAggregation`. If the HP Propel web services are configured correctly, `HPPropelKMAggregation` contains the `HPPropelKnowledge` and `HPPropelKnowlegeAttachment` objects.

3. (Optional) If you want to upload sample KM documents, they are available in the `documents.zip` file that is in the `/opt/hp/propel/km` directory on the HP Propel VM. Unzip the file and extract the sample documents by running the following commands as `root` on the HP Propel VM:

```
# cd /opt/hp/propel/km
# unzip documents.zip
```

A `documents` subdirectory is created and used as *DOCS_IMPORT_LOCATION* in step **5**.

4. Make sure the `/opt/hp/propel/km/PropelKMImporter.sh` file has execute permissions. If it does not, execute the following command as `root` on the HP Propel VM:

```
# chmod 755 /opt/hp/propel/km/PropelKMImporter.sh
```

5. Navigate to `/opt/hp/propel/km` on the HP Propel VM and execute the following command:

```
# PropelKMImporter.sh –pr <SM_PROTOCOL> -h <SM_HOSTNAME> -po <SM_PORT>
-u <NEW_SM_USER> -pa <NEW_SM_PASSWORD> -i <DOCS_IMPORT_LOCATION>
```

Where *NEW_SM_USER* and *NEW_SM_PASSWORD* are the user and the password for the new integration account you created as a copy of the *falcon* operator. (See Knowledge Management Best Practices for details.)

For example:

```
# ./PropelKMImporter.sh –pr http –h <my-sm-host.bel.hp.com> -po 14090
-u <INT-PROPEL> -pa <password> -i /home/INT-PROPEL/documents
```

Important: The integration user that is created as a copy of the *falcon* operator must have a password.

For help about this script:

```
# ./PropelKMImporter.sh –help
```

6. To verify that KM documents have been successfully loaded into HP SM (after receiving a success message):

   In HP SM, navigate to **Knowledge Management** -> **Search Knowledgebase**.
   (Using the Window client got to menu options [the black triangle at the right side] and select **Expert Search**. Using the web client, in the menu bar, click **More** and select **Expert Search**.)

   The Advanced Search form appears. Provide the following search criteria and perform the search:

   DocType: "Question/Answer"
   Status: "Externally Published"
   Category: "Propel"

Changing HP Propel Default User Accounts' Passwords

HP Propel has built-in user accounts. The user accounts are used to authenticate REST API calls and for initial setup and experimentation with the product. For security reasons, HP recommends that you change the default passwords associated with these accounts, however, do not change the user names.

Important Do not create users in your LDAP directory that match the users provided by HP Propel. The HP Propel users are: `admin`, `consumer`, `idmTransportUser`, `ooInbounduser`, and `sxCatalogTransportUser`. Creating an identical user in LDAP could allow an HP Propel user unintended access to the HP Propel Management Console or give the LDAP user unintended privileges.

Besides changing the passwords for the built-in HP Propel user accounts, HP recommends that you also change the default password for the `root` user on the HP Propel virtual machine (VM). For details about changing the `root` password, refer to the `passwd(1)` manpage.

Note: In the HP Propel 2.00 release, some default passwords have been updated, while others are the same as in prior releases. For example, the default `root` password has been updated to match the current calendar year; however, many of the default keystore passwords remain as they were in the 1.xx releases. If an updated default password does not work, try the prior release password.

In the following instructions, `$PROPEL_HOME` represents the `/opt/hp/propel` directory on the HP Propel VM. You can set this as an environment variable with the following command on the HP Propel VM:

```
# export PROPEL_HOME=/opt/hp/propel
```

HP Propel User Accounts – HP Propel Management Console

The following HP Propel user account is used to access the HP Propel Management Console.

admin User: HP Propel Management Console

Username	admin
Default Password	cloud
Usage	This Administrator account is used to log in to the HP Propel Management Console to manage HP Propel settings across all of the organization.

To Disable	Edit the `$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the `admin` property to disable this user account. For example, set `admin` to the following value. (This value should be encrypted.):
	
	`cloud,ROLE_REST,disabled`
	
	Note: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled.
	
	By default, the unencrypted value of this property is:
	`cloud,ROLE_REST,SERVICE_CONSUMER,enabled`
	
	See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value. The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`.

To Change Password	Edit the `$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password value of the `admin` property and encrypt the entire value, including the roles and the account status. (See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value.) The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`. You must also update and use the same password for every REST API call that uses the password. **Note**: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled. By default, the unencrypted value of this property is: `cloud,ROLE_REST,SERVICE_CONSUMER,enabled`

HP Propel Portal User Accounts

The following HP Propel user accounts are used to access the HP Propel Portal.

orgadmin User: HP Propel Portal

Username	orgadmin
Default Password	cloud
Usage	This Organization Administrator account is used to access both the HP Propel Portal and HP Propel administrative applications for an organization, such as Catalog Connect Policies. (LDAP does not have to be configured.) This user belongs to the "HP Propel consumer internal group" and is a member of the HP Propel Consumer organization. (Both the group and the user are provided as samples.)

To Disable	Edit the `$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/ csa-consumer-users.properties` file. Update the `orgadmin` property to disable this user account. For example, set `orgadmin` to the following value. (This value should be encrypted.):
	
	`cloud,SERVICE_CONSUMER,ROLE_REST,disabled`
	
	Note: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled.
	
	By default, the unencrypted value of this property is:
	`cloud,SERVICE_CONSUMER,ROLE_REST,enabled`
	
	See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value. The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`.

To Change Password	Edit the `$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/ csa-consumer-users.properties` file. Update the password value of the `orgadmin` property and encrypt the entire value, including the roles and the account status. (See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value.) The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`. **Note**: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled. By default, the unencrypted value of this property is: `cloud,SERVICE_CONSUMER,ROLE_REST,enabled`

consumer User: HP Propel Portal

Username	consumer
Default Password	cloud
Usage	This account is used to log in to the HP Propel Portal. (LDAP does not have to be configured.) This user belongs to the "HP Propel consumer internal group" and is a member of the HP Propel Consumer organization. (Both the group and the user are provided as samples.)

To Disable	Edit the `$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/` `csa-consumer-users.properties` file. Update the `consumer` property to disable this user account. For example, set `consumer` to the following value. (This value should be encrypted.):
	
	`cloud,SERVICE_CONSUMER,ROLE_REST,disabled`
	
	Note: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled.
	
	By default, the unencrypted value of this property is:
	`cloud,SERVICE_CONSUMER,ROLE_REST,enabled`
	
	See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value. The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`.

To Change Password	Edit the `$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/` `csa-consumer-users.properties` file. Update the password value of the `consumer` property and encrypt the entire value, including the roles and the account status. (See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value.) The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`. **Note**: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled. By default, the unencrypted value of this property is: `cloud,SERVICE_CONSUMER,ROLE_REST,enabled`

Encrypt a Password – HP Propel User Accounts

To encrypt a password for HP Propel user accounts:

1. Log in to the HP Propel VM as `root` and navigate to the `$PROPEL_HOME/cryptoUtil` directory.

2. Determine a new password for the user account: *New_Password*

3. Encrypt the password by running the following command:

   ```
   # $JAVA_HOME/bin/java –jar cryptoUtil-cli-1.0.4.jar encrypt <New_Password>
   ```

   Note: Some user accounts, such as `idmTransportUser`, require that values are also specified for the account roles and the account status. For example, the default password, roles, and status values for `idmTransportUser` are:

   ```
   idmTransportUser,PERM_IMPERSONATE,ROLE_ADMIN,enabled
   ```

4. The `java` command in step 3 returns encrypted text for the specified password. Use the encrypted text returned in step 3 to replace the user account's password information to the right of the equal sign ("=") in the corresponding file.

   The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. For example, to use the encrypted text as a replacement for the password value for the `idmTransportUser` in the `integrationusers.properties` file:

   ```
   idmTransportUser=ENC(<Encrypted_Text>)
   ```

   Where *<Encrypted_Text>* is the encrypted text returned from the `java` command in step 3.

Restart HP Propel

To restart services on the HP Propel VM, do the following:

1. Log in to the HP Propel VM as `root`, and navigate to the `$PROPEL_HOME/bin` directory.

2. Run the following commands:

   ```
   # propel stop
   ```

   ```
   # propel start
   ```

Change the HP Propel Master Password

HP Propel uses a master password (or Key Encryption Key – KEK) to encrypt passwords for user accounts that are in the `$PROPEL_HOME/mpp/conf/mpp.json` file, such as the `idmTransportUser` user account. HP recommends that you change the default master password for improved security.

The HP Propel master password is implemented using Shamir's Secret Sharing Scheme (SSSS) to split the master password into multiple cryptographically-secure KEK shares and store them in distributed file locations.

After you split a new master password into three encrypted values, you insert the values into three separate files and distribute the three files in distinct locations as KEK stores. For the HP Marketplace Portal the file locations are configured in the `$PROPEL_HOME/mpp/conf/mpp.json` file and for the HP Propel Launchpad the file locations are configured in the `$PROPEL_HOME/launchpad/app.json` file.

Important: Whenever the master password is changed, the following three things must be done:

- If a `keyfile*` file exists, delete it. The location of the `keyfile*` file is specified in the `keyfile` attribute in the `$PROPEL_HOME/mpp/conf/mpp.json` file and the `$PROPEL_HOME/launchpad/app.json` file.

- All encrypted passwords in the `$PROPEL_HOME/mpp/conf/mpp.json` file must be regenerated using the `passwordUtil.js` utility. For an example of updating a password in the `mpp.json` file, see Updating the password Attribute in mpp.json.

When you change the Master Password for an HP Propel instance, it is also good practice to change the JWT signing key. For more information on changing the signing key, see Change the JWT Signing Key.

The tasks to change the HP Propel master password are:

- Split the HP Propel Master Password

- If configuring the HP Marketplace Portal – Configure the mpp.json File

- If configuring the HP Propel Launchpad – Configure the app.json File

Split the HP Propel Master Password

Perform the following procedure to split the new master password:

1. Log in as `root` and navigate to the `/usr/bin` directory.

2. Run the `passwordUtil.js` command to split the new master password into three separate values:

```
# ./node /opt/hp/propel/launchpad/bin/passwordUtil.js --split
Please enter the password to split <hidden_password>
Please enter the File prefix or blank to skip file creation
Shares are (801d3c957e144c6a9d2725315,802b88f01df3c91dfb974a689,8036a46333e1457066b76f5fd)
```

3. Using the three encrypted values (KEK shares) from the output of step 2, create three new files in different locations that are relative to the `$PROPEL_HOME/mpp/conf` directory. For example, insert the corresponding encrypted values into newly created KEK share files: the first encrypted value into a `../masterpass1` file, the second encrypted value into a `../../security/masterpass2` file, and the third encrypted value into a `../../etc/masterpass3` file.

HP Marketplace Portal – Configure the `mpp.json` File

For the HP Marketplace Portal, after you have spilt the new master password into three unique KEK share files, you must configure the files in the `mpp.json` file, which is located in the `$PROPEL_HOME/mpp/conf` directory The `kekshare1`, `kekshare2`, and `kekshare3` attributes in the `mpp.json` file are used to reference the paths to the KEK share files.

If the `kekshare*` attributes are not specified in the `mpp.json` file, the default files for the KEK shares are `kekshare1`, `kekshare2`, and `kekshare3` and they are located in the `$PROPEL_HOME/mpp/conf` directory.

The following (partial) example of the `mpp.json` file shows how you can specify the paths to the KEK share files:

```
{
  "uid": "ccue_mpp",
  "port": 8089,
  "defaultOrganizationName": "CONSUMER",
  "defaultHelpLocate": "en_US",
  "defaultHelpPage": "MarketplacePortal_HELP_CSA.htm",
  "keyfile": "../conf/keyfile",
  "kekshare1": "../masterpass1",
  "kekshare2": "../../security/masterpass2",
  "kekshare3": "../../etc/masterpass3",
  "session": {
    "cookieSecret": "enc(dqmtAEFpkRd4DYpx4pDMzQ==)",
    "timeoutDuration": 1800,
    "cleanupInterval": 3600
  },
```

Important: When splitting a new HP Propel master password, you must configure one of the following in the `mpp.json` file:

- At least two KEK shares (`kekshare*` attributes)

- No KEK shares, so that the default `kekshare*` files in the `$PROPEL_HOME/mpp/conf` directory will be used

HP Propel Launchpad – Configure the `app.json` File

For the HP Propel Launchpad, after you have spilt the new master password into three unique KEK share files, you must configure the files in the `app.json` file, which is located in the `$PROPEL_HOME/launchpad` directory. The `kekshare1`, `kekshare2`, and `kekshare3` attributes in the `app.json` file are used to reference the paths to the KEK share files.

The default files for the KEK shares are `kekshare1`, `kekshare2`, and `kekshare3` and they are located in the `$PROPEL_HOME/launchpad/bin` directory.

The following (partial) example of the `app.json` file shows how you can specify the paths to the KEK share files:

```
"daemon": {
  "name": "launchpad",
  "port": 9000,
  "keyfile": "bin/keyfile",
  "kekshare1": "bin/kekshare1",
  "kekshare2": "bin/kekshare2",
  "kekshare3": "bin/kekshare3",
  "cluster_enabled": false,
  "num_cluster_instances": "max",
  "https_enabled": true,
  "configure_pfx": true,
  "pfx": "/opt/hp/propel/security/propel_host.pfx",
  "configure_passphrase": true,
  "passphrase": "enc()kdjfdKJJKDJkdjgjgdDKSHS==)",
  "rejectUnauthorized": false
  },
```

Important: When splitting a new HP Propel master password, you must configure one of the following in the `app.json` file:

- At least two KEK shares (`kekshare*` attributes)
- No KEK shares, so that the default `kekshare*` files in the `$PROPEL_HOME/launchpad` directory will be used

Change the JWT Signing Key

Important: After changing the password for the `idmTransportUser`, you should also change the JWT signing key. To accomplish this, you must update all of the following four properties with identical encrypted values:

JWT Signing Key - update locations

1) The `AUTHENTICATION.secretKey` JSON property in the `/opt/hp/propel/sx/WEB-INF/classes/config/infrastructure.json` file.
2) The `security.encryptedSigningKey` property in the `/opt/hp/propel/sx/WEB-INF/sx.properties` file.
3) The `idm.encryptedSigningKey` property in the `/opt/hp/propel/idm-service/idm-service.war/WEB-INF/spring/applicationContext.properties` file.
4) The `securityEncryptedSigningKey` property in the `/opt/hp/propel/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/csa.properties` file.

The first two JWT signing-key locations (items 1 and 2) are under the `sx.war` directory, and will get encrypted automatically if both of their properties have an unencrypted value. For the final two locations (items 3 and 4), you must encrypt the value manually. (See Encrypt a Password – HP Propel User Accounts for instructions on how to encrypt this value.)

Note: It is highly recommended that the signing key assigned by the HP Propel Administrator is strong and long enough to survive brute force attacks. Any user with an IDM token (even an expired token) and knowledge about the authentication method may use this knowledge to perform a brute force attack without any rate limits in search of the secret signing key. Example: a strong and long key should be composed of 25 characters (including letters, digits, and some symbols), but not containing any dictionary words.

After making these password changes, you must restart HP Propel for the changes to take effect. See Restart HP Propel for detailed information about how to restart HP Propel.