HP Propel

Software Version 1.10
CentOS

Administration Guide

Document Release Date: December 2014
Software Release Date: December 2014

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 Marketplace Portal, manually changing the keystore password, and changing the HP Service Manager port number.

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

Loading KM Documents. Provides the instructions for the optional task of loading Knowledge Management documents into HP Service Manager**.**

Changing Default 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 **csa_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 Marketplace Portal

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

To change the default port number (13080) that is used by HP Propel to communicate with HP Service Manager, perform the following procedure:

1. Add an HP Service Manager (type) adapter, which is done via the Aggregation tile in the HP Propel Management Console, and use the Add Adapter window to edit the port number value for the `service-manager-port` property. Refer to the *HP Propel Catalog Aggregation Help* for details.
2. On the HP Propel SX VM, specify the port number you want to use by revising the “13080” value in the `/opt/hp/propel/jboss-as/standalone/deployments/sx.war/WEB-INF/classes/config/sm/instances.json` file.

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 `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 “propel2014” for the HP Propel keystore and truststore.

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 in the `/opt/hp/propel-install` directory. (The default password is “propel2014” for the `root` user.)

1. Initialize the SSL working directory:

   ```
   # ./propel-ssl-setup.sh init
   ```

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

2. Generate the SSL certificate signing request (CSR) for the CA:

   ```
   # ./propel-ssl-setup.sh --password <PASSWORD> generateSigningRequest <SUBJECT>
   ```

   Where *PASSWORD* is the passphrase 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”

   A CSR is written to the `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME` directory and named `propel_host.key.csr`. The private secret is stored in the same directory and named `private.key.pem`, and converted to `propel_host.key.rsa` in the `out` subdirectory.

3. 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.

4. Add trust for the end-point server you want HP Propel to integrate with.

   The public keys of end-point systems that HP Propel integrates with (HP CSA and HP SM) must be added to the HP Propel truststore. For each of the end-point servers, run the following command:

   ```
   # ./propel-ssl-setup.sh addTrustedServer <END_POINT_HOSTNAME>:<END_POINT_PORT>
   ```

   Where *END_POINT_HOSTNAME* is the fully qualified end-point hostname and *END_POINT_PORT* is the end-point system's port that is used by the HP Propel VM for communication.

5. After the CA has returned the signed certificates, create the ZIP file:

   a. Make sure you have the following files under the `/opt/hp/propel-install/ssl-tmp` directory:
   - `CA.crt` – the PEM-encoded public X.509 certificate of the CA.
   - `$PROPEL_VM_HOSTNAME/out/propel_host.crt` – a certificate for the HP Propel server that is issued by the CA in X.509 format.

   b. Create the ZIP file:

   ```
   # .propel-ssl-setup.sh finish
   ```

6. Unpack the `/opt/hp/propel-install/res/ssl/$PROPEL_VM_HOSTNAME.zip` file into the `/opt/hp/propel/security` directory.

7. Stop the HP Propel services and the central HP Operations Orchestration services on the HP Propel VM:

   ```
   # propel stop
   # service central stop
   ```

8. Re-import the HP Propel truststore into HP Operations Orchestration with the following `keytool` commands:

   ```
   # 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
   ```

9. Start the HP Propel services and the central HP Operations Orchestration services on the HP Propel VM:

```
# propel start
# service central start
```

Loading Knowledge Management Documents into HP Service Manager

This appendix provides instructions for loading knowledge management (KM) documents into HP Service Manager (HP SM).

Pre-Requisites for Loading Documents

All documents that are loaded into HP SM have the following settings:

- The default status is set to **external**.
- The docType is set to **Question/Answer**.
- The category is set to **Propel**.

Document Format for Loading Documents

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

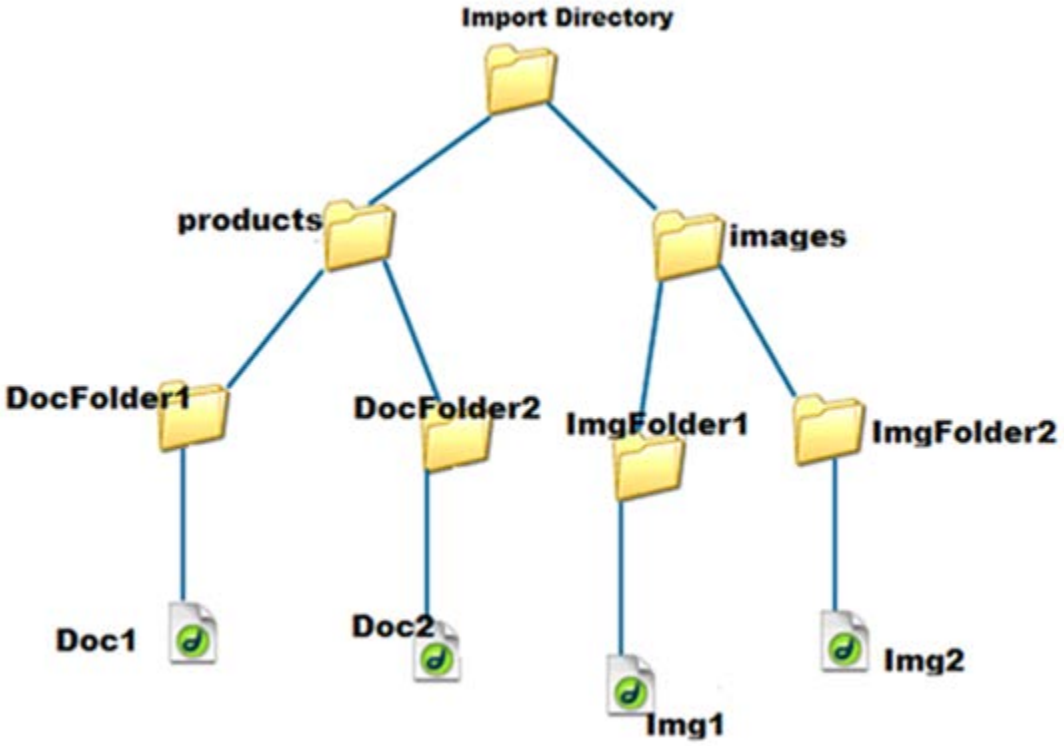
```
<? xml version=”1.0” encoding=”UTF-8”?>

<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.

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.

4. Make sure you have Java running in your environment.

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 <SM_USER> -pa <SM_PASSWORD> -i <DOCS_IMPORT_LOCATION>
   ```

   Note: If the password is not specified, you will be prompted to enter the password.

   For example:

   ```
   # ./PropelKMImporter.sh –pr http –h <smhost> -po 13080 –u <smuser>
   -pa <smpassword> -i /home/<myuser>/documents
   ```

   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):

   a. In HP SM, navigate to **Search Knowledge Base** -> **Advanced**.

   Provide the following search criteria and perform the search:

   DocType: “Question/Answer”

   Status: “External”

   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.

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.

Important: Do not create users in your LDAP directory that match the users provided by HP Propel. The HP Propel users are: `admin`, `consumer`, `CatalogAggregationTransportUser`, `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.

Note: 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 accounts are used to access the HP Propel Management Console.

admin User: HP Propel Management Console

Username	admin
Default Password	cloud
Usage	This account is used to initially log in to the HP Propel Management Console to configure the provider organization.

To Disable	Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/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,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/jboss-as/standalone/deployments/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,enabled`

catalogAggregationTransportUser User: HP Propel Management Console

Username	catalogAggregationTransportUser
Default Password	cloud
Usage	This account is used to authenticate REST_API calls.
To Disable	Do not disable this account.
To Change Password	Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/aggregation.war/WEB-INF/classes/aggregation-adapter.properties` file. Update the password value of the `catalogAggregationTransportUserPassword` property and encrypt the value. (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 any calls that use the Catalog Aggregation registration REST APIs. **Important**: If you change the password for the `catalogAggregationTransportUser` user, you must re-create the Catalog Aggregation adapters. (The existing adapters will no longer work due to the password change.) After modifying the `aggregation-adapter.properties` file, you must restart HP Propel. See **RESTART HP PROPEL** for detailed information about how to restart HP Propel.

idmTransportUser User: HP Propel Management Console

Username	idmTransportUser
Default Password	idmTransportUser
Usage	This account is used to authenticate REST API calls.
To Disable	Do not disable this account.
To Change Password	Prior to changing the password to the `idmTransportUser` account, you must first change the HP Propel master password. (The master password is used to encrypt and decrypt passwords in the `mpp.json` file.) After the master password has been changed, update identical values of the password in the `integrationusers.properties` file, the `org.authenticate.httpbasic.password` property in the `csa.properties` file, and the `password` attribute in the `idmProvider` section of the `mpp.json` file. You must also update and use the same password for every REST API call that uses the password. Additionally, the default values for the JWT signing key should also be changed. See **CHANGE THE JWT SIGNING KEY** for details. **Changing the HP Propel Master Password** For details of changing the HP Propel master password, see **CHANGE THE HP PROPEL MASTER PASSWORD**. **Updating the idmTransportUser Property in integrationusers.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/integrationusers.properties` file. Update the password value of the `idmTransportUser` property. Encrypt the entire value, including the roles and the account status. (See **ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS** for instructions on how to encrypt this value.) The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`. **Important**: The `idmTransportUser` property must always be enabled. This property not only determines if the account is enabled, it also contains the password and the roles that control access to HP Propel. By default, the unencrypted value of this property is: `idmTransportUser,ROLE_ADMIN,PERM_IMPERSONATE,enabled` **Updating the org.authenticate.httpbasic.password Property in csa.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/csa.properties` file. Update the password value of the `org.authenticate.httpbasic.password` property, using the same password that you used for the `idmTransportUser` property in the `integrationusers.properties` file. (See **ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS** for instructions on how to encrypt this value.) Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`.

	Updating the password Attribute in mpp.json Edit the `$PROPEL_HOME/mpp/conf/mpp.json` file. Update the value of the `password` property in the `idmProvider` section, using the same password that you used for the `idmTransportUser` property in the `integrationusers.properties` file. To encrypt the password, use the `passwordUtil.js` utility that is provided by the HP Propel Marketplace Portal: 1. Log in to the HP Propel VM as `root`, and navigate to the `$PROPEL_HOME/node/bin` directory. 2. Run the following command: `./node /$PROPEL_HOME/mpp/bin/passwordUtil.js` When prompted, enter the identical password that you used for the `idmTransportUser` property in the `integrationusers.properties` file. 3. An encrypted password is displayed. Copy the encrypted password to the `password` attribute value in the `idmProvider` section of the `mpp.json` file. An encrypted password 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)`.

ooInboundUser User: HP Propel Management Console

Username	ooInboundUser
Default Password	cloud
Usage	This account is used by HP Operations Orchestration to authenticate REST API calls with HP Propel.
To Disable	Do not disable this account
To Change Password	If you change the password to the `ooInboundUser` account, you must update identical values of the password in the `csa-provider-users.properties` file and the `securityOoInboundUserPassword` property in the `csa.properties` file. You must also update and use the same password for every REST API call that uses the password. **Important**: You must also update and use the same password for the CSA_REST_CREDENTIALS system account in HP Operations Orchestration (located in the Configuration folder of the Public Repository). **Updating the ooInboundUser Property in csa-provider-users.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password value of the `ooInboundUser` property and encrypt the entire value, including the roles and the account status. (See ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS for instructions on how to encrypt this value.) The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`. **Note**: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled. By default, the unencrypted value of this property is: `cloud,ROLE_REST,enabled` **Updating the securityOoInboundUserPassword Property in csa.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/csa.properties` file. Update the password value of the `securityOoInboundUserPassword` property and encrypt the value. (See ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS for instructions on how to encrypt this value.) Use the same encrypted password that you entered for the `ooInboundUser` property in the `csa-provider-users.properties` file. After modifying the `csa.properties` file, you must restart HP Propel. See RESTART HP PROPEL for detailed information about how to restart HP Propel.

sxCatalogTransportUser User: HP Propel Management Console

Username	sxCatalogTransportUser
Default Password	cloud
Usage	This account is used to authenticate REST API calls.
To Disable	Do not disable this account
To Change Password	If you change the password to the `sxCatalogTransportUser` account, you must update identical values of the password in the `csa-provider-users.properties` file and the `sx.authenticate.idm.user.password` property in the `sx.properties` file on the HP Propel VM. Additionally, you must also update and use the same password for the `catalog.notificationUserPassword` property in the `sx.properties` file on the HP Propel Service Exchange VM. You must also update and use the same password for every REST API call that uses the password. **Updating the sxCatalogTransportUser Property in csa-provider-users.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password value of the `sxCatalogTransportUser` property and encrypt the entire value, including the roles and the account status. (See **ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS** for instructions on how to encrypt this value.) The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value, for example: `ENC(54j5ngfki3i43A0=d)`. **Note**: This property not only contains the password, but also the roles that control access to HP Propel and if the account is enabled. By default, the unencrypted value of this property is: `cloud,ROLE_REST,enabled` **Updating the sx.authenticate.idm.user.password Property in sx.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/sx.properties` file. Update the password value of the `sx.authenticate.idm.user.password` property and encrypt the value. (See **ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS** for instructions on how to encrypt this value.) Use the same encrypted password that you entered for the `sxCatalogTransportUser` property in the `csa-provider-users.properties` file. **Updating the catalog.notificationUserPassword Property in sx.properties on the HP Propel Service Exchange Virtual Machine** On the HP Propel Service Exchange VM, edit the `$PROPEL_HOME/jboss-as/standalone/deployments/sx.war/WEB-INF/sx.properties` file. Update the password value of the `catalog.notificationUserPassword` property and encrypt the value. (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)`.

HP Propel Marketplace Portal User Accounts

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

consumer User: HP Propel Marketplace Portal

Username	consumer
Default Password	cloud
Usage	This account is used to initially log in to and experiment with the HP Propel Marketplace 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/jboss-as/standalone/deployments/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/jboss-as/standalone/deployments/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/jboss-as/standalone/deployments/idm-service.war/WEB-INF/lib` 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-1.0.3.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. The file locations are configured in the `mpp.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 `$PROPEL_HOME/mpp/conf/mpp.json` file.
- All encrypted passwords in the `$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
- CONFIGURE THE MPP.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 `$PROPEL_HOME/node/bin` directory.
2. Run the `passwordUtil.js` command to split the new master password into three separate values:

```
# ./node /opt/hp/propel/mpp/bin/passwordUtil.js --split
Please enter the password to split <hidden_password>
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 `../../node/masterpass3` file.

Configure the `mpp.json` File

After you have spilt the new master password into three unique KEK share files, you must configure the files in `mpp.json`, which is located in `$PROPEL_HOME/mpp/conf`. 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": "../../node/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

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/jboss-as/standalone/deployments/sx.war/WEB-INF/classes/config/infrastructure.json` file.
2) The `security.encryptedSigningKey` property in the `/opt/hp/propel/jboss-as/standalone/deployments/sx.war/WEB-INF/sx.properties` file.
3) The `idm.encryptedSigningKey` property in the `/opt/hp/propel/jboss-as/standalone/deployments/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.