HP Propel

HP Propel Installation Guide

For the CentOS Operating System

Software Version 1.01 (October 2014)

Contents

Overview

This document provides information on how to install HP Propel, which includes the HP Propel Portal virtual machine (VM) and the HP Propel Service Exchange VM.

The following information is provided in this document:

Overview. Describes the audience for this guide and where to find additional HP Propel information. Default passwords, contents of the HP Propel product, and HP Propel requirements are provided. Additionally, an HP Propel installation overview is provided**.**

Installation. Provides the detailed HP Propel Portal and HP Propel Service Exchange (HP Propel SX) installation steps. The end result is the instantiated HP Propel Portal VM and the HP Propel SX VM.

Configuration. Provides basic information for Catalog Aggregation configuration and the recommendation to improve the security of HP Propel.

Next Steps. Provides HP Propel SX configuration information necessary to complete the HP Propel configuration.

HP Propel Tips. This appendix provides miscellaneous information for HP Propel, including verification of the GPG code signing for the HP Propel OVA files, customizing the HP Marketplace Portal, manually changing the keystore password, and changing the HP Service Manager port number.

Configuring SSL Certificates. This appendix provides general information to configure the SSL certificates so that the HP Propel Portal, HP Propel SX, and an end-point system communicate successfully. Instructions for manually creating self-signed SSL certificates are also provided.

Loading KM Documents. This appendix provides the optional instructions for loading Knowledge Management documents into HP Service Manager**.**

Changing Default Passwords. This appendix provides the default passwords for the HP Propel user accounts and instructions for changing them, which HP recommends for increased security.

Revision History

Revisions for HP Propel Version 1.01 (October 2014)

- Revised the detailed installation instructions in **HP PROPEL INSTALLATION**, including the SSL certificates configuration.
- Added default passwords and requirements for end-point system integration and SSL certificates to **BEFORE YOU BEGIN**.
- Added **CHANGING THE HP SERVICE MANAGER PORT NUMBER**.
- Revised **APPENDIX B – CONFIGURING SSL FOR HP PROPEL**, including how to manually configure self-signed SSL certificates.
- Revised step 5 in **HOW TO LOAD KM DOCUMENTS**.
- Added **APPENDIX D – CHANGING HP PROPEL DEFAULT USER ACCOUNTS' PASSWORDS.**

Revisions for HP Propel Version 1.00 (July 2014)

- Initial release of the software

Audience

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

- Working with VMware ESX Server 5
- Installing OVA packages
- Deploying virtual machines (VMs), including configuration and administration
- Configuring VM networking
- Configuring SSL certificates

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 Service Exchange: *HP Propel Service Exchange Configuration Guide*
- HP Catalog Aggregation: *HP Propel Catalog Aggregation Help*
- HP Propel Marketplace Portal (MPP): *HP Propel Marketplace Portal Help*

These guides are available from the HP Software Support website at **http://h20230.www2.hp.com/selfsolve/manuals/**. (This website requires that you register with HP Passport.)

Before You Begin

HP Propel contains two OVA templates that are imported into a VMware ESX server environment and instantiated as virtual machines.

- HP Propel Portal OVA template: contains the HP Propel Marketplace Portal (MPP), the HP Catalog Aggregation, the HP Identity Manager, and the HP Micro Services (Knowledge Management and Ticket Management) products
- Service Exchange OVA template: contains the HP Propel Service Exchange product

You will need to use the following (default) passwords to install HP Propel:

- Use “propel2014”’ as the `root` user password on both the HP Propel Portal virtual machine (VM) and the HP Propel Service Exchange VM.
- Use “propel2014” as the keystore password on both the HP Propel Portal VM and the HP Propel Service Exchange VM.
- Default HP Propel user accounts’ passwords are provided in **APPENDIX D – CHANGING HP PROPEL DEFAULT USER ACCOUNT’S PASSWORDS**.

You will need the following for end-point system integration and SSL certificates:

- The hostname of the HP Service Manager system.
- The hostname of the HP Cloud Service Automation (CSA) system.
- The keystore password on the HP CSA system.
- The CSA system’s SSL certificate.

The following customized environment variables are used throughout this guide:

- $PROPEL_HOME = `/opt/hp/propel`
- $JAVA_HOME = `/usr/lib/jvm/java-1.7.0-openjdk.x86_64`
- $CSA_JRE_HOME is the directory where the JRE that is used by HP CSA is installed.

Preparing Your Environment for Virtual Machines

Before installing HP Propel, you need to make sure that your VMware environment has enough resources to instantiate the two VM templates that are included in the HP Propel product. Refer to the *HP Propel System and Software Support Matrix* for all HP Propel requirements.

HP Propel Software and Hardware Requirements

Software Requirements:

- VMware ESX Server 5 (or later)
- VMware vSphere Client (available for download from the VMware ESX server)

Hardware Requirements:

For each HP Propel VM (HP Propel Portal and HP Propel Service Exchange) in the VMware ESX Server environment:

- 8 GB memory
- 4 CPUs
- 160 GB of allocated disk space

HP Propel Product End-Point Integrations

- HP Cloud Service Automation (HP CSA) 4.1
- HP Service Manager (HP SM) 9.32, 9.33, 9.34

IMPORTANT: You must install and configure either the HP CSA product or the HP SM product for HP Propel to properly operate.

Installation Overview

The general procedure to install HP Propel is:

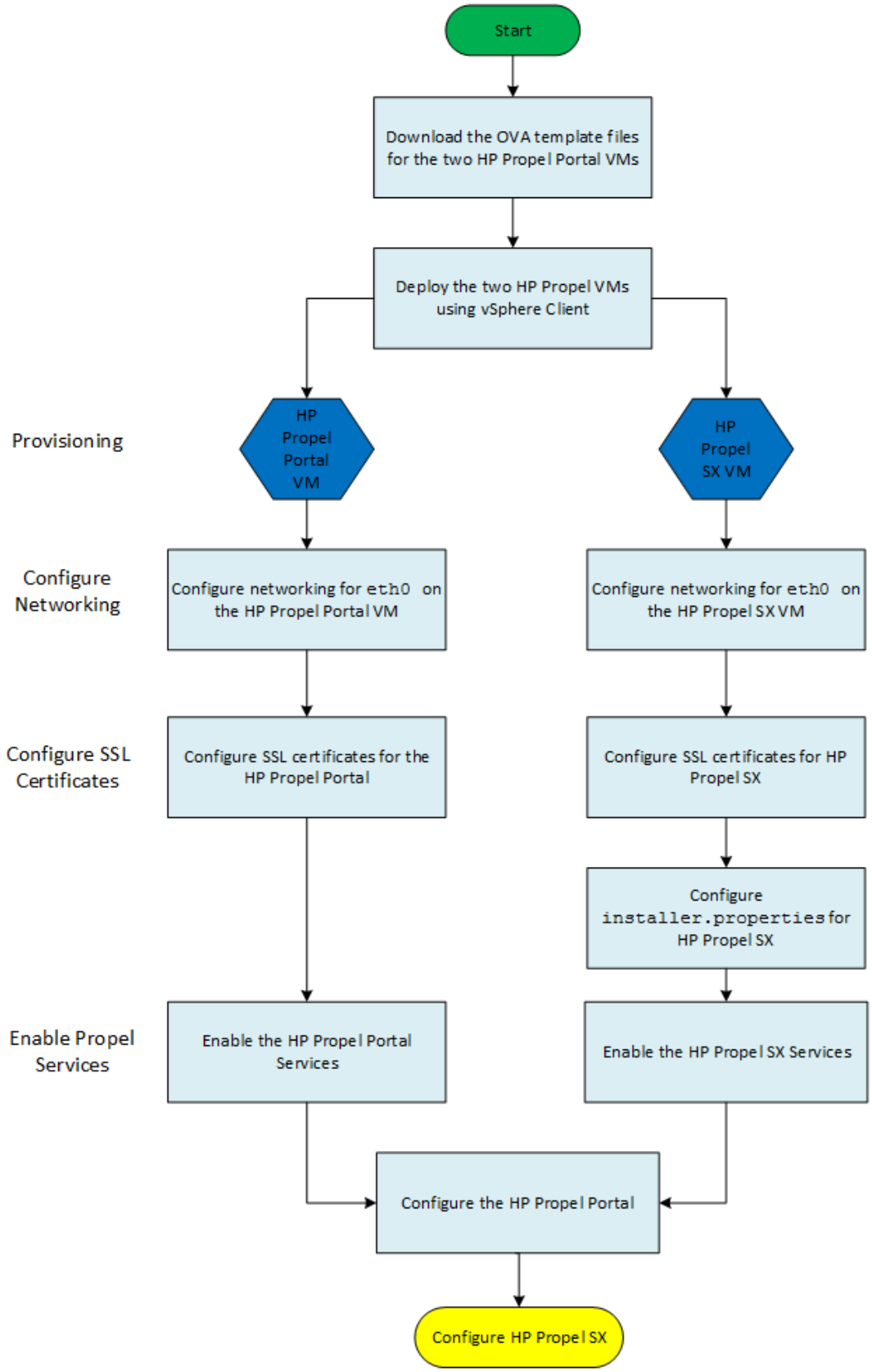
1. From the HP Propel website, download the two OVA templates:
   a. HP Propel Portal VM
   b. HP Propel SX VM
2. Using the VMware vSphere Client, deploy the two HP Propel VMs into the VMware ESX environment by importing the OVA templates:
   a. HP Propel Portal VM
   b. HP Propel SX VM
3. Using the VMware vSphere Client, configure the HP Propel Portal VM network adapter.
4. Specify the HP Propel Portal hostname and configure DHCP networking for `eth0`.
5. Using the VMware vSphere Client, configure the HP Propel SX VM network adapter.

6. Specify the HP Propel SX hostname and configure DHCP networking for `eth0`.
7. Configure Secure Socket Layer (SSL) communication.
8. Specify either an HP SM instance or an HP CSA instance, or both (`installer.properties` file).
9. Enable services on HP Propel SX.
10. Enable services on the HP Propel Portal.
11. Add an aggregation adapter on the HP Propel Portal, which is described in the *HP Propel Catalog Aggregation Help*.
12. Continue with configuring HP Propel SX, which is described in the *HP Propel Service Exchange Configuration Guide*.

Detailed HP Propel installation instructions are provided in **HP PROPEL INSTALLATION**.

Figure 1 shows the general procedure to install HP Propel and the initial configuration.

Figure 1 - HP Propel Installation Procedure



HP Propel Installation

Perform the following steps to install HP Propel:

1. Download the two HP Propel OVA template files from **HP PROPEL HOME**:
   a. HP Propel Portal VM
   b. HP Propel SX VM

   NOTE: To verify the GPG code signing of the two OVA files, download the two `.sig` files and the two HP public key files, then see **VERIFYING GPG CODE SIGNING – HP PROPEL OVA FILES** for details.
2. On the ESX server, use the VMware vSphere Client to deploy the two HP Propel VMs:
   a. HP Propel Portal VM
   b. HP Propel SX VM
3. After the HP Propel Portal VM has been deployed and is available, use VMware vSphere Client to edit the VM properties. Click the **Getting Started** tab, and then click **Edit virtual machine settings**. Click **Network adapter 1** in the Virtual Machine Properties window, and change the network label to the network configured for the ESX server.
4. Power on the HP Propel Portal VM.
5. Click the **Console** tab in VMware vSphere Client, and log in to the HP Propel Portal VM as `root`, using “propel2014” as the password.
6. Specify the HP Propel Portal hostname and configure DHCP networking for `eth0` on the HP Propel Portal VM:

   ```
   # cd /opt/hp/propel/bin
   # ./reconfigurePropelCat.sh –-hostname <PROPEL_PORTAL_VM_HOSTNAME> --configuredhcp
   ```

   Where *PROPEL_PORTAL_VM_HOSTNAME* is the fully qualified hostname you specify for the HP Propel Portal VM.

   IMPORTANT: The underscore character (“_”) cannot be used in the hostname of the HP Propel Portal VM.

   Reply “Y” to the prompt to configure DHCP networking and the prompt to reboot the VM.
7. After the HP Propel SX VM has been deployed and is available, use VMware vSphere Client to edit the VM properties. Click the **Getting Started** tab, and then click **Edit virtual machine settings**. Click **Network adapter 1**, and change the network label to the network configured for the ESX server.
8. Power on the HP Propel SX VM.
9. Click the **Console** tab in VMware vSphere Client, and log in to the HP Propel SX VM, log in as `root`, using “propel2014” as the password.
10. Specify the HP Propel SX hostname and configure DHCP networking for `eth0` on the HP Propel SX VM:

    ```
    # cd /opt/hp/propel/bin
    # ./reconfigurePropelSX.sh –-hostname <PROPEL_SX_VM_HOSTNAME> --configuredhcp
    ```

    Where *PROPEL_SX_VM_HOSTNAME* is the fully qualified hostname you specify for the HP Propel SX VM.

    IMPORTANT: The underscore character (“_”) cannot be used in the hostname of the HP Propel SX VM.

Reply “Y” to the prompt to configure DHCP networking and the prompt to reboot the VM.

11. The SSL certificates for an end-point system must be configured. For SSL certificates details, see **APPENDIX B – CONFIGURING SSL FOR HP PROPEL**. This step provides a method to configure self-signed SSL certificates with an HP CSA system.

    a. Copy the HP CSA system’s SSL certificate to the HP Propel Portal VM. The file on the HP Propel Portal VM must be named `propel_csa.cert` and copied to the `/opt/hp/propel/security` directory. For example, on the HP CSA system, navigate to the `/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration` directory and run the following command:

    ```
    # scp jboss.crt root@<PROPEL_PORTAL_HOSTNAME>:/opt/hp/propel/security/propel_csa.cert
    ```

    b. Copy the HP CSA system’s SSL certificate to the HP Propel SX VM. The file on the HP Propel SX VM must be named `propel_csa.cert` and copied to the `/opt/hp/propel/security` directory. For example, on the HP CSA system, navigate to the `/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration` directory and run the following command:

    ```
    # scp jboss.crt root@<PROPEL_SX_HOSTNAME>:/opt/hp/propel/security/propel_csa.cert
    ```

    c. On the HP Propel Portal VM, navigate to `/opt/hp/propel/bin` and run the following command as `root`:

    ```
    # ./wrapper_import_scripts.sh
    ```

    The `wrapper_import_scripts.sh` script prompts you for the fully qualified hostname of the HP SX VM and also prompts you multiple times for the default “propel2014” password. (At the time of publishing, some `keytool` errors are displayed, along with other warnings.) This script creates self-signed SSL certificates for the HP Propel Portal VM and the HP Propel SX VM. The script adds the CSA certificates, which were copied in steps **a** and **b**, to the truststores on both HP Propel VMs.

    d. On the HP Propel Portal VM, copy the `propel_catalog.cert` file to the HP CSA system. For example, run the following command on the HP Propel Portal VM in the `/opt/hp/propel/security` directory:

    ```
    # scp propel_catalog.cert root@<CSA_HOSTNAME>:/tmp
    ```

    e. On the HP Propel SX VM, copy the `propel_sx.cert` file to the HP CSA system. For example, run the following command on the HP Propel SX VM in the `/opt/hp/propel/security` directory:

    ```
    # scp propel_sx.cert root@<CSA_HOSTNAME>:/tmp
    ```

    f. On the HP CSA system, import the HP Propel Service Exchange’s self-signed certificate as a trusted certificate by running the following command:

    ```
    # $CSA_JRE_HOME/bin/keytool -importcert -alias propel_sx -file /tmp/propel_sx.cert
    –trustcacerts –keystore $CSA_CACERTS_HOME/cacerts
    ```

    Where `$CSA_CACERTS_HOME` is the directory that the `cacerts` keystore file is located. When prompted, type the keystore password. (The default password is `changeit` on the HP CSA system.) Reply `yes` when prompted to trust the certificate.

    g. On the HP CSA system, import the HP Propel Portal’s self-signed certificate as a trusted certificate by running the following command:

    ```
    # $CSA_JRE_HOME/bin/keytool -importcert -alias propel_portal -file
    /tmp/propel_catalog.cert –trustcacerts –keystore $CSA_CACERTS_HOME/cacerts
    ```

    Where `$CSA_CACERTS_HOME` is the directory that the `cacerts` keystore file is located. When prompted,

type the keystore password. (The default password is `changeit` on the HP CSA system.) Reply `yes` when prompted to trust the certificate.

12. On the HP CSA system, restart HP CSA so that the newly imported certificates will take effect:

```
# service csa restart
# service mpp restart
```

13. On the HP Propel SX VM, log in as `root`, using “propel2014” as the password.

14. On the HP Propel SX VM, edit the `installer.properties` file, entering your unique values for the integration sections. This file is located in the `/opt/hp/propel/bin` directory. See the example below.

    If an integration section is set to false (for example, “SM_ENABLED=false”), the corresponding lines in the section are ignored and do not need to be commented out.

    NOTE: Any additional instances must be added into the relevant `instances.json` file. For details of adding additional instances, see the *HP Propel Service Exchange Configuration Guide*.

```
# CCUE CATALOG INTEGRATION
CATALOG_HOSTNAME=catalog.example.com

#Do not modify LWSSO_ENABLED. Always set to false.
LWSSO_ENABLED=false

# SERVICE MANAGER INTEGRATION
SM_ENABLED=true
SM_HOSTNAME=smhost.example.com
SM_PORT=13444
SM_SSL=true
SM_USER=johndoe
SM_PASS=mypassword
# If SM_PD is true, the Process Designer engine is installed in your HP Service Manager
SM_PD=false

# CSA INTEGRATION
CSA_ENABLED=true
CSA_HOSTNAME=csahost.example.com
CSA_PORT=8444
CSA_SSL=true
CSA_USER=johndoe
CSA_PASS=mypassword
CSA_ORG=CSA_CONSUMER

# MAILING PROPERTIES
SMTP_SERVER=smtp.example.com
SMTP_PORT=25
MAIL_FROM=noreply@example.com
MAIL_BCC=archive@example.com
SMTP_USER=
SMTP_PASS=
```

15. On the HP Propel SX VM, start the HP Propel SX services:

```
# cd /opt/hp/propel/bin
# ./reconfigurePropelSx.sh –-configuresx –-enableservices
```

16. On the HP Propel Portal VM, log in as `root`, using “propel2014” as the password.

17. Start the HP Propel Portal services:

```
# cd /opt/hp/propel/bin
# ./reconfigurePropelCat.sh –-sxhostname <PROPEL_SX_VM_HOSTNAME>
--smhostname <SERVICE_MANAGER_HOSTNAME>
# ./reconfigurePropelCat.sh –-enableservices
```

Congratulations, you have successfully installed HP Propel and configured the SSL certificates between HP Propel and an end-point system. You can now display the HP Propel Portal by opening a browser window and entering the following URL:

`https://<PROPEL_PORTAL_VM_HOSTNAME>:8444`
(Use “consumer” as the user and “cloud” as the password.)

To display the HP Propel SX user interface, enter the following URL, and log in to HP Propel SX through the HP Propel Portal:

`https://<PROPEL_SX_VM_HOSTNAME>:8444/sx`
(Use “consumer” as the user and “cloud” as the password.)

HP Propel Portal Configuration

After you have successfully installed the HP Propel Portal, you must perform the following configuration tasks:

- Configure Catalog Aggregation and create a new catalog. For details, see *HP Propel Catalog Aggregation Help*. (If required, you can change the default port number (13080) used for communication with HP Service Manager. See CHANGING THE HP SERVICE MANAGER PORT NUMBER for details.)
- Improve security on the HP Propel Portal by changing the default user accounts’ passwords. Though this is an optional task, HP recommends that you change the default passwords. See APPENDIX D – CHANGING HP PROPEL DEFAULT USER ACCOUNTS’ PASSWORDS for details.

Additionally, if you have Knowledge Management documents that you need to load into HP Service Manager, see APPENDIX C – LOADING KNOWLEDGE MANAGEMENT DOCUMENTS INTO HP SERVICE MANAGER for details.

Next Steps

After the HP Propel Portal VM is installed and configured and the HP Propel Service Exchange VM is installed, you must configure the HP Propel Service Exchange VM. Refer to the *HP Propel Service Exchange Configuration Guide* for details about configuring the HP Propel Service Exchange VM.

Appendix A – HP Propel Tips

Verifying GPG Code Signing – HP Propel OVA Files

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

To verify that the two HP Propel OVA files are signed with GNU Privacy Guard (GPG), you must download the two `.sig` files and the HP keys from **HP SOFTWARE SUPPORT ONLINE (SSO)**. Perform the following procedure on the system that you downloaded the OVA files, the `.sig` files, 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 themes, widgets, and sections, refer to the *HP Propel Customizing the Marketplace Portal* whitepaper.

Manually Changing the Keystore Password

The keystore password on the HP Propel Portal 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 Portal 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 Portal 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.

Appendix B – Configuring SSL for HP Propel

The HP Propel Portal is configured to require https (http over SSL) for client browsers. For an SSL connection to be established, an SSL certificate must first be installed on the HP Propel Portal.

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.

HP Propel provides an automated script that configures self-signed SSL certificates on the HP Propel Portal VM and the HP Propel SX VM. For details of using the automated `wrapper_import_scripts.sh` script, see step 11 in HP PROPEL INSTALLATION.

SSL Certificates Overview

The HP Propel Portal VM, HP Propel Service Exchange (HP Propel SX) VM, and an end-point system—either the HP Cloud Service Automation (HP CSA) or the HP Service Manager (HP SM), or both—must have authorized SSL certificates that communicate with each system. There are multiple ways to configure the SSL certificates so that the HP Propel Portal and an end-point system communicate successfully:

- Use a third-party CA to sign both hosts' certificate signing requests (CSRs).
- Use an internal company CA to sign both hosts' CSRs, copy the company's internal `CA.crt` file to both systems, and install the certificates.
- Generate a self-signed CA to sign both hosts' CSRs and distribute the self-signed CA to all systems (HP Propel Portal, HP Propel SX, HP SM, and HP CSA).
- Generate a self-signed certificate for each system and transfer the certificates to every system that requires trust.

NOTE: Though HP does not recommend a specific SSL implementation, for an example of using self-signed certificates, see MANUALLY CONFIGURING SELF-SIGNED SSL CERTIFICATES FOR HP PROPEL.

HP Propel SSL Certificates

Use the following tables to configure SSL certificates for HP Propel.

Table 1 – HP Propel Portal SSL Configuration Locations

Component	Location	Line	SSL Entry Type
MPP	/opt/hp/propel/mpp/conf/mpp.json	23	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	33	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	40	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	47	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	52	propel_catalog.pfx
MSVC	/opt/hp/propel/msvc/conf/idm.json	8	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/knowledge.json	7	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/knowledge.json	14	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/ticket.json	7	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/server.json	13	propel_catalog.pfx
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/api.json	7	propel_catalog.cert
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/idm.json	10	propel_catalog.cert
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/server.json	18	propel_catalog.pfx
AGGREGATION	/opt/hp/propel/jboss-as/standalone/deployments/aggregation.war/WEB-INF/classes/aggregation-adapter.properties	9	propel.truststore
AGGREGATION	/opt/hp/propel/aggrAdmin/conf/aggregation.json	7	propel_catalog.cert
AGGREGATION	/opt/hp/propel/aggrAdmin/conf/api.json	7	propel_catalog.cert
AGGREGATION	/opt/hp/propel/aggrAdmin/conf/idm.json	10	propel_catalog.cert
AGGREGATION	/opt/hp/propel/aggrAdmin/conf/server.json	18	propel_catalog.pfx
CONSUMPTION	/opt/hp/propel/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/csa.properties	44	propel.truststore

Table 2 – HP Propel Service Exchange SSL Configuration Locations

Component	Location	Line	SSL Entry Type
RABBITMQ	/etc/rabbitmq/rabbitmq.config	6	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	7	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	8	sx_host.key.rsa
RABBITMQ	/etc/rabbitmq/rabbitmq.config	16	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	17	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	18	sx_host.key.rsa
SX	/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml	221	.keystore
SX	/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml	33	propel.truststore

Table 3 – HP Propel Truststore[1] Contents

Certificate Type	SSL Authentication Setup
propel_catalog.cert	Self-signed
propel_sx.cert	Self-signed
propel_csa.cert[2]	Self-signed or Certificate Authority
SM1.cert[2]	Self-signed or Certificate Authority
propelCA.cert	Certificate Authority

1 – `propel.truststore` is on both the HP Propel Portal and HP Propel Service Exchange under the `/opt/hp/propel/security` directory.

2 – The HP SM and HP CSA instances are the certificates for the end-point systems; there might be zero or more.

Table 4 – HP Propel SSL Descriptions

SSL Entry Type	Description
propel_catalog.cert	The certificate containing the hostname of the HP Propel Portal VM
propel_sx.cert	The certificate containing the hostname of the HP Propel SX VM
propel_catalog.pfx	The certificate and private key associated with the HP Propel Portal certificate
propel_sx.pfx	The certificate and private key associated with the HP Propel SX certificate
propel_sx.key.rsa	The unencrypted private key associated with the Propel SX certificate
propel.truststore	The container for certificates trusted by the HP Propel VMs (Portal and SX)
.keystore	The container for private keys associated with the Propel VMs (Portal and SX)

Manually Configuring Self-Signed SSL Certificates for HP Propel

This section provides instructions to manually configure self-signed SSL certificates to enable secure communication among the HP Propel Portal, HP Propel Service Exchange (HP Propel SX), HP Cloud Service Automation (HP CSA), and HP Service Manager (HP SM) systems.

CAUTION: Before attempting to configure SSL certificates, HP recommends that you backup your environment.

Create HP Propel Portal SSL Files

Perform the following steps on the HP Propel Portal to create the necessary SSL files for self-signed certificates:

1. Log in as `root`.
2. `# cd /opt/hp/propel/security`
3. `# openssl genrsa -des3 -out propel_catalog.key 2048`
4. `# openssl rsa -in propel_catalog.key -out propel_catalog.key.rsa`
5. `# openssl req -new -key propel_catalog.key.rsa -out propel_catalog.csr`
6. `# openssl x509 -req -days 365 -in propel_catalog.csr -signkey propel_catalog.key.rsa -out propel_catalog.cert`
7. `# openssl pkcs12 -export -in propel_catalog.cert -inkey propel_catalog.key.rsa -out propel_catalog.pfx`

Configure HP Propel Portal Keystore and Truststore

NOTE: The default keystore password is “propel2014” on the HP Propel Portal VM.

Perform the following steps on the HP Propel Portal in `/opt/hp/propel/security` to configure the keystore and truststore with the previously created SSL files:

1. `# keytool –delete –keystore .keystore –alias propel_catalog`
2. `# keytool -importkeystore -srckeystore propel_catalog.pfx -srcstoretype PKCS12 -destkeystore .keystore -srcalias 1 -destalias propel_catalog`
3. To make sure the key is in the keystore:

   `# keytool –list –keystore .keystore -v`
4. `# keytool -importcert -keystore propel.truststore -alias propel_catalog -file propel_catalog.cert -trustcacerts -noprompt`

Add or Update HP Propel Portal SSL Entries

Add or update the following SSL entries on the HP Propel Portal.

Table 5 – HP Propel Portal SSL Configuration Locations

Component	Location	Line	SSL Entry Type
MPP	`/opt/hp/propel/mpp/conf/mpp.json`	23	propel_catalog.cert
MPP	`/opt/hp/propel/mpp/conf/mpp.json`	33	propel_catalog.cert
MPP	`/opt/hp/propel/mpp/conf/mpp.json`	40	propel_catalog.cert
MPP	`/opt/hp/propel/mpp/conf/mpp.json`	47	propel_catalog.cert
MPP	`/opt/hp/propel/mpp/conf/mpp.json`	52	propel_catalog.pfx
MSVC	`/opt/hp/propel/msvc/conf/idm.json`	8	propel_catalog.cert
MSVC	`/opt/hp/propel/msvc/conf/knowledge.json`	7	propel_catalog.cert
MSVC	`/opt/hp/propel/msvc/conf/knowledge.json`	14	propel_catalog.cert
MSVC	`/opt/hp/propel/msvc/conf/ticket.json`	7	propel_catalog.cert
MSVC	`/opt/hp/propel/msvc/conf/server.json`	13	propel_catalog.pfx
IDM-ADMIN	`/opt/hp/propel/idmAdmin/conf/api.json`	7	propel_catalog.cert
IDM-ADMIN	`/opt/hp/propel/idmAdmin/conf/idm.json`	10	propel_catalog.cert
IDM-ADMIN	`/opt/hp/propel/idmAdmin/conf/server.json`	18	propel_catalog.pfx
AGGREGATION	`/opt/hp/propel/jboss-as/standalone/deployments/aggregation.war/WEB-INF/classes/aggregation-adapter.properties`	9	propel.truststore
AGGREGATION	`/opt/hp/propel/aggrAdmin/conf/aggregation.json`	7	propel_catalog.cert
AGGREGATION	`/opt/hp/propel/aggrAdmin/conf/api.json`	7	propel_catalog.cert
AGGREGATION	`/opt/hp/propel/aggrAdmin/conf/idm.json`	10	propel_catalog.cert
AGGREGATION	`/opt/hp/propel/aggrAdmin/conf/server.json`	18	propel_catalog.pfx
CONSUMPTION	`/opt/hp/propel/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/csa.properties`	44	propel.truststore

Create HP Propel SX SSL Files

Perform the following steps on HP Propel SX to create the necessary SSL files for self-signed certificates:

1. Log in as root.
2. `# cd /opt/hp/propel/security`
3. `# openssl genrsa -des3 -out propel_sx.key 2048`
4. `# openssl rsa -in propel_sx.key -out propel_sx.key.rsa`

5. `# openssl req -new -key propel_sx.key -out propel_sx.csr`
6. `# openssl x509 -req -days 365 -in propel_sx.csr -signkey propel_sx.key.rsa -out propel_sx.cert`
7. `# openssl pkcs12 -export -in propel_sx.cert -inkey propel_sx.key.rsa -out propel_sx.pfx`

Configure HP Propel SX and HP Operations Orchestration Keystore and Truststore

Perform the following steps on HP Propel SX in `/opt/hp/propel/security` to configure the HP Propel SX and HP Operations Orchestration keystores and truststores with the previously created SSL files:

1. `# keytool -delete -keystore .keystore -alias propel_sx`
2. `# keytool -importkeystore -srckeystore propel_sx.pfx -srcstoretype PKCS12 -destkeystore .keystore -srcalias 1 -destalias propel_sx`
3. To make sure the key is in the keystore:

   `# keytool -list -keystore .keystore –v`
4. `# keytool -importcert -keystore propel.truststore -file propel_sx.cert -alias propel_sx -trustcacerts –noprompt`
5. `# keytool -delete -keystore "/opt/hp/oo/central/var/security/key.store" -alias tomcat`
6. `# keytool -importkeystore -srckeystore propel_sx.pfx -srcstoretype PKCS12 -destkeystore "/opt/hp/oo/central/var/security/key.store" -srcalias 1 -destalias tomcat -destkeypass changeit -srckeypass propel2014 -deststorepass changeit -srcstorepass propel2014`
7. To make sure the key is in the keystore:

   `# keytool -list -keystore "/opt/hp/oo/central/var/security/key.store"  -v`
8. `# keytool -delete -keystore "/opt/hp/oo/central/var/security/client.truststore" -alias propelCA`
9. `# keytool -importcert -keystore "/opt/hp/oo/central/var/security/client.truststore" -alias propel_sx -file propel_sx.cert -trustcacerts -noprompt`

Add or Update HP Propel SX SSL Entries

Add or update the following SSL entries on HP Propel SX.

Table 6 – HP Propel Service Exchange SSL Configuration Locations

Component	Location	Line	SSL Entry Type
RABBITMQ	`/etc/rabbitmq/rabbitmq.config`	6	propel_sx.cert
RABBITMQ	`/etc/rabbitmq/rabbitmq.config`	7	propel_sx.cert
RABBITMQ	`/etc/rabbitmq/rabbitmq.config`	8	propel_sx.key.rsa
RABBITMQ	`/etc/rabbitmq/rabbitmq.config`	16	propel_sx.cert
RABBITMQ	`/etc/rabbitmq/rabbitmq.config`	17	propel_sx.cert
RABBITMQ	`/etc/rabbitmq/rabbitmq.config`	18	propel_sx.key.rsa
SX	`/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml`	221	.keystore
SX	`/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml`	33	propel.truststore

Exchange HP Propel Portal and HP Propel SX SSL Certificates

Perform the following steps on the HP Propel Portal and HP Propel SX in `/opt/hp/propel/security` to exchange the SSL certificates between the HP Propel Portal and HP Propel SX:

1. From `/opt/hp/propel/security` on the HP Propel Portal:

   a. `# scp propel_catalog.cert root@<SX_HOSTNAME>:/opt/hp/propel/security/`

   b. `# scp root@<SX_HOSTNAME>:/opt/hp/propel/security/propel_sx.cert .`

   c. `# keytool -importcert -keystore propel.truststore -alias propel_sx -file propel_sx.cert -trustcacerts –noprompt`

2. From `/opt/hp/propel/security` on HP Propel SX:

   ```
   # keytool -importcert -keystore propel.truststore -alias propel_catalog –file propel_catalog.cert -trustcacerts –noprompt
   ```

Appendix C – 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

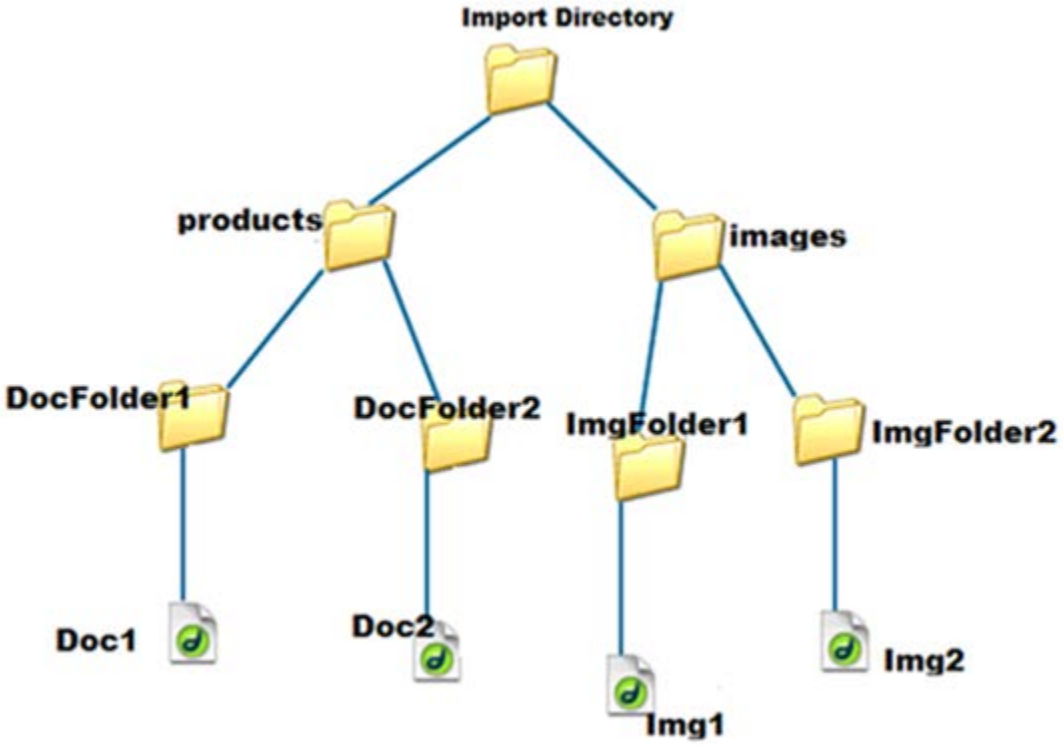
```
<? xml version=”1.0” encoding=”UTF-8”?>

<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 Portal VM to the HP SM system. The web services files are in the `/opt/hp/propel/aggregation/km/webservices` directory on the HP Propel Portal 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/aggregation/km` directory on the HP Propel Portal 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/aggregation/km` on the HP Propel Portal 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”

Appendix D – 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.

NOTE: 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.

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 THE HP PROPEL PORTAL** 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	If you change the password to the `idmTransportUser` account, you must update identical values of the password in the `integrationusers.properties` file, the `securityIdmTransportUserPassword` 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. **IMPORTANT**: After changing the password for the `idmTransportUser`, you should also change the JWT signing key. To accomplish this, update the value for the `idm.encryptedSigningKey` property in the `$PROPEL_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file. This value should be encrypted. **Updating the idmTransportUser Property in integrationusers.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/integrationusers.properties` file. Update the password value of the `idmTransportUser` property 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)`. **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 securityIdmTransportUserPassword Property in csa.properties** Edit the `$PROPEL_HOME/jboss-as/standalone/deployments/consumption.war/WEB-INF/classes/csa.properties` file. Update the password value of the `securityIdmTransportUserPassword` property and encrypt the value, (See **ENCRYPT A PASSWORD – HP PROPEL USER ACCOUNTS** for instructions on how to encrypt this value.) Use the same password that you entered for the `idmTransportUser` property in the `integrationusers.properties` file. After modifying the `csa.properties` file, you must restart HP Propel. See **RESTART THE HP PROPEL PORTAL** for detailed information about how to restart HP Propel. **Updating the password Attribute in mpp.json** Edit the `$PROPEL_HOME/mpp/conf/mpp.json` file. Update the value of the `password` attribute in the `idmProvider` section and the `keyfile` attribute. Use the same password that you entered for the `idmTransportUser` property in the `integrationusers.properties` file and encrypt this password using the utility that is provided by the HP Propel Marketplace Portal:

	1. Log in to the HP Propel Portal 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 THE HP PROPEL PORTAL** 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 Portal 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 Portal as `root` and navigate to the `/opt/hp/propel/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 –classpath cryptoUtil-1.0.2.jar:cryptoUtil-cli-1.0.2.jar
   com.hp.ccue.crypto.util.App 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. 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 the HP Propel Portal

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

1. Log in to the HP Propel Portal VM as `root`, and navigate to the `/opt/hp/propel/bin` directory.
2. Run the following commands:

   ```
   # ./reconfigurePropelCat.sh –-disableservices

   # ./reconfigurePropelCat.sh –-enableservices
   ```