



Propel

Software Version: 2.20.p2

Administration Guide

Document Release Date: December 2016

Software Release Date: December 2016



Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© 2014 - 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com>.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an account** on the HPE Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

Contents

Overview	5
Audience	5
Additional Information	6
HPE Propel Tips	7
Verifying GPG Code Signing – HPE Propel OVA File	7
Customizing the HPE Propel Portal	7
Customizing the HPE Propel Launchpad	7
Applying Custom HPE Propel Themes	8
Manually Changing the Keystore Password	8
Changing HPE Propel Requests Redeliveries for Unavailable HPE SM System	8
Managing Licensing	9
Understanding Administrative and Consumer Roles in HPE Propel	9
Using Common LDAP Server with HPE Propel and End-Point Systems	10
Viewing the SSL Certificate-Signing Algorithm	10
Filter HPE SM Search Results by Display Name	11
Attachment Size and File Types in HPE Propel	11
Configuring the Hot News application in HPE Propel	12
Running the RSS Interface in Launchpad Behind a Firewall	13
Exporting and Importing Business Processes	13
Export a Business Process	14
Import a Business Process	14
HPE Propel Custom Themes	15
Introduction to Themes	15
Apply the HPE Propel-Provided Dark Theme	15
Create and Apply a Custom Theme	16
Installing the HPE SAW Adapter in HPE Propel	17
Replacing HPE Propel-Generated SSL Certificates	19
Preparation	19
Replace HPE Propel-Generated SSL Certificates	20
Update RabbitMQ	26

Update HPE Operations Orchestration	27
Exchange SSL Certificates from HPE Propel VM and Suppliers	28
Final SSL Configuration Steps and Validation	29
HPE Knowledge Management	31
Installation	31
HPE Knowledge Management Indexing	32
HPE Knowledge Management Best Practices	32
HPE Knowledge Management Configuration Steps – After HPE Propel Installation	32
IDOL Search Installation and Configuration Using Solr	35
Solr Plugin Installation Steps	35
Search Installation and Configuration Using Smart Analytics (IDOL)	40
Connecting HPE Propel to HPE SM 9.41 for Smart Analytics	40
Setting Up Smart Analytics in HPE SM	41
Configuring HPE Propel for Smart Analytics (IDOL)	42
Load HPE KM Documents into HPE Service Manager	45
Changing HPE Propel Default User Accounts' Passwords	49
Change Passwords for HPE Propel Management Console User Accounts	50
Change Passwords for HPE Propel Portal User Accounts	51
Change Passwords for HPE Propel Transport User Accounts	53
Encrypt a Password - HPE Propel User Accounts	58
Change the HPE Propel Master Password	59
Split the HPE Propel Master Password	59
Update All KEK Share Files for an HPE Propel Application	60
Update all Encrypted Values for an HPE Propel Application	60
Change the JWT Signing Key	62
Restart HPE Propel	62
Send Documentation Feedback	64

Overview

This document provides information about administration tasks for HPE Propel.

The following information is provided in this document:

- **Overview:** Describes the audience for this guide and where to find additional HPE Propel information.
- ["HPE Propel Tips" on page 7](#): Provides miscellaneous information for HPE Propel, including verification of the GPG code signing for the HPE Propel OVA file, customizing the HPE Propel Portal and Launchpad, manually changing the keystore password, changing the HPE Service Manager port number, understanding consumer and administrative roles, using a common LDAP server, and viewing an SSL certificate signing algorithm
- ["HPE Propel Custom Themes" on page 15](#): Explains how to change the appearance of the HPE Propel Launchpad and applications in the HPE Propel Portal using color themes.
- ["Installing the HPE SAW Adapter in HPE Propel" on page 17](#): Provides the instructions to install the HPE Service Anywhere adapter in HPE Propel.
- ["Replacing HPE Propel-Generated SSL Certificates" on page 19](#): Explains how to replace the previously generated HPE Propel SSL certificates with Certificate Authority-signed SSL certificates.
- ["HPE Knowledge Management" on page 31](#): Provides the instructions for the optional task of loading HPE Knowledge Management documents into HPE Service Manager and installing the Solr plugin for IDOL search.
- ["Changing HPE Propel Default User Accounts' Passwords" on page 49](#): Provides the default passwords for the HPE Propel user accounts and instructions for changing them, which HPE recommends for increased security.

Audience

The person who administers HPE 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 HPE Propel:

- Requirements: *HPE Propel System and Software Support Matrix*
- Latest features and known issues: *HPE Propel Release Notes*
- Installation and configuration: *HPE Propel Installation and Configuration Guide*

These guides are available from the HPE Software Support website at <https://softwaresupport.hpe.com/group/softwaresupport>. (This website requires that you register with HPE 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.hpe.com/documents/10180/14684/HPE_Software_Customer_Support_Handbook/

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

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

HPE Propel Tips

Verifying GPG Code Signing – HPE Propel OVA File

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

The HPE Propel binary OVA file has been signed by Hewlett Packard Enterprise. The file signature is as follows:

```
-----BEGIN PGP ARMORED FILE-----
Version: GnuPG v2.0.22 (GNU/Linux)
Comment: Use "gpg --dearmor" for unpacking

iQEcBAABCAAGBQJXh6B1AAoJEMZ45pN/1bycWN4IAI8+2tknr9UwENRcRTWeGwYN
RDsEq2d0oRxksq+MNsIF91gGUJg9Qch7rR6Bmc/ad3oETLMX1zEY1GFsdfhKVK9
ZCNB7Yt8zM4KrQUuh9rA+pDUXMREXDW2HdAF5Xxv32oKT8Y5hqk3LNjUatQhSU8k
FyMsgFhCedW2WzO3FMCElhwpX+IL6wyEH3gs+M0FB9ABVCM+R7TOoFKLJidvYggS
72ab6kQoF/kW+BEHmaTtAurSAGvmrVJH49qPeCyOhfKMQUCAPx5ThbBM/w1lX1E3
IbupP0eey9UgvYUqlaJtDWIw4FuPISS96qlogGB9tx6cwvEw/ij0bIVjhmmDuAY=
=95ou
-----END PGP ARMORED FILE-----
```

To find the public GPG key, see

<https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>.

Customizing the HPE Propel Portal

You can customize the display of the HPE Propel Portal. For details about customizing the portal, refer to the *Manage Customizations* topic in the HPE Propel *Identity* online help.

Customizing the HPE Propel Launchpad

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

Applying Custom HPE Propel Themes

You can apply custom HPE Propel themes to change the appearance of the Launchpad and applications in the HPE Propel Portal. For details about applying custom themes, see ["HPE Propel Custom Themes" on page 15](#).

Manually Changing the Keystore Password

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

```
# keytool -storepasswd -storepass propel2014 -new <NEW_KEYSTORE_PASSWORD>  
-keystore /opt/hp/propel/security/propel.truststore
```

```
# ./configureKeys.sh --setkspassword <NEW_KEYSTORE_PASSWORD>
```

Where *NEW_KEYSTORE_PASSWORD* is the new keystore password that you specify.

Changing HPE Propel Requests Redeliveries for Unavailable HPE SM System

If HPE Service Manager is integrated with HPE Propel and the HPE SM system becomes unavailable for HPE Propel to deliver requests, the default number of attempted requests redeliveries is five and the interval is every 30 seconds.

You can configure these redelivery parameters in the `/opt/hp/propel/sx/WEB-INF/sx.properties` file on the HPE Propel VM:

```
sx.dlx.redelivery.interval.ms=30000  
sx.dlx.redelivery.max.count=5
```

Where the `interval` property is in milli-seconds.

Propel will automatically retry as configured in `/opt/hp/propel/sx/WEB-INF/sx.properties`. Failed requests are added to a manual retry list. The **Diagnostics** tab in the **Supplier Detail** view indicates a failed Synchronizations status for unsent requests. An `orgadmin` can use the **Manual Retry** tab on the **Supplier Detail** view where they can manually retry to sync a request with the **Retry** button. The list of

requests to be retried can be filtered such that one or more requests are retried. Upon submission, the automatic retry will start again from the beginning. If it fails again, failed requests will be re-added to the manual retry list.

To cancel failed requests in the retry list, the `orgadmin` can use the **Terminate** button in the **Manual Retry** view. The termination removes the failed requests from the retry list and the requests are displayed as failed in the HPE Propel Portal.

Managing Licensing

HPE Propel uses these license types:

- Instant-on licensing – implemented when installing HPE Propel and limited to 60 days.
- Permanent – either unlimited or limited duration.

Refer to the *HPE Propel Licensing Guide* for details of HPE Propel licensing.

Understanding Administrative and Consumer Roles in HPE Propel

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

- Administrator:
 - Logs in as the `admin` user with the "propel" password at `$PROPEL_VM_HOSTNAME:9000/org/Provider`
 - Manages HPE Propel settings across all of the organizations. For example, creating and managing organizations or content packs.
 - Has access to the Identity, Content Management, and Diagnostics applications.
- Organization Administrator:
 - Logs in as the `orgadmin` user with the "propel" password at `$PROPEL_VM_HOSTNAME:9000/org/CONSUMER`
 - Manages the organization, creates suppliers, aggregates and publishes catalog items, and manages catalogs, categories, and policies. Additionally can perform all Organization Consumer functions (for example shopping and support requests).

- Has access to the Shop, Subscriptions, Knowledge, Request Support, Catalogs, Catalog Items, Categories, Policies, Catalog Connect, and Suppliers applications.
- Organization Consumer:
 - Logs in as the consumer user with the "propel" password at
`$PROPEL_VM_HOSTNAME:9000/org/CONSUMER`
 - Performs shopping, manages subscriptions, searches knowledge articles, and requests support.
 - Has access to the Shop, Subscriptions, Knowledge, and Request Support applications.

Where `$PROPEL_VM_HOSTNAME` is the fully qualified host name of the HPE Propel VM.

Using Common LDAP Server with HPE Propel and End-Point Systems

To prevent errors in HPE Propel log files that are related to unknown users, HPE recommends that all integrated end-point systems (suppliers) share a common LDAP server with HPE Propel. Otherwise, identically named users need to be created on both the HPE Propel system and the integrated end-point system.

Viewing the SSL Certificate-Signing Algorithm

HPE recommends reviewing the certificate-signing algorithms used and ensuring that strong encryption is implemented. For example, SHA1 is sometimes used, and instead, stronger algorithms such as SHA256 should be used.

To view a certificate's signing algorithm, execute the following command:

```
# keytool -printcert -file <SSL-CERTIFICATE> | grep -i algorithm
```

For example:

```
# keytool -printcert -file /opt/hp/propel/security/propel_host.crt | grep algorithm
Signature algorithm name: SHA256withRSA
#
```

Filter HPE SM Search Results by Display Name

When adding an aggregation in the **Catalog Connect** application and using the `displayName` column in the **Query Filter** field, the query can return more results than expected.

Because `displayName` is part of an HPE SM information retrieval (IR) key, searching on a specified `displayName` value can return more results than expected. By removing `displayName` from the HPE SM IR key, you are able to correctly search on `displayName` values.

Before aggregating HPE SM items into HPE Propel, make the following HPE SM information retrieval (IR) configuration change to enable filtering by `displayName`.

1. From the HPE Service Manager Client, access the Table definitions as follows:
On the **System Navigator** tab, open **System Definition > Tables > svcDisplay**
2. Select the **Fields and Keys** tab (bottom of the display).
3. In the **Keys** content, select **IR key:description – displayName**.
4. Under **General**, select **displayName**, then click **Remove**.
5. Click **Save**.

Attachment Size and File Types in HPE Propel

You can control the size and allowable file types for attachments to HPE Propel Support Requests and Service and Support catalog items. Related properties are located in the `/opt/hp/propel/catalog/config.yml` file and their default values are:

```
blobstore
  fileLimit: 20971520
  fileExtensionWhiteList:
    - jpg
    - svg
    - png
    - ico
    - bmp
    - jpeg
    - doc
    - docx
    - ppt
    - pptx
    - xls
    -xlsx
    - xlt
```

```
- xml
- xsd
- uml
- pdf
- txt
- json
- yaml
- csv
whiteListEnabled: false
```

By default, 20971520 bytes (approximately 20 MB) is allowed per file and all file types are allowed, even if file extensions are already defined in the `fileExtensionWhiteList` property. The list of file extensions in the white list is not enabled by default.

To enable the white list of allowable file extensions, you need to specify the following in the `config.yml` file.

```
whiteListEnabled: true
```

After modifying the `config.yml` file, for the changes to take effect, you must restart the Catalog service with the following command on the HPE Propel VM:

```
# systemctl restart catalog
```

Note: Be careful when modifying YAML files. Use an online parser tool (for example, Online YAML Parser, <http://yaml-online-parser.appspot.com>) to check indentations.

Configuring the Hot News application in HPE Propel

The **Hot News** application in HPE Propel enables you to specify RSS feeds and view them in HPE Propel.

To configure **Hot News**:

1. Log in to the HPE Propel VM as `root` and navigate to the `/opt/hp/propel/launchpad/conf` directory.
2. Edit the `rss.json` file and add your RSS feeds, similar to the following:

```
[
  "http://investors.hpe.com/rss/news",
  "http://rss.cnn.com/rss/cnn_topstories.rss",
  "http://sports.espn.go.com/espn/rss/news"
```

]

Note: The feed must support RSS 2.0 format.

To configure organization-specific RSS feeds, create an `rss.ORG_NAME.json` file, where `ORG_NAME` is the name of the HPE Propel organization.

Running the RSS Interface in Launchpad Behind a Firewall

If HPE Propel is installed and running behind a firewall, then you need to configure a proxy so that the RSS interface in Launchpad can fetch the RSS feeds appropriately. Perform these instructions to configure the proxy for Launchpad:

1. Log in to the HPE Propel VM as `root`.
2. Create an `/etc/systemd/system/launchpad.service.d` directory.
3. Within the directory, create a `local.conf` file.
4. Edit the `local.conf` file and add the following entries, where `PROXY_HOST` and `PROXY_PORT` contain your proxy information:

```
[Service]
Environment=http_proxy=PROXY_HOST:PROXY_PORT
Environment=https_proxy=PROXY_HOST:PROXY_PORT
```

5. Run the following command to reload the new proxy configuration:

```
systemctl daemon-reload
```

6. Run following command to restart the HPE Propel Launchpad:


```
systemctl restart launchpad
```

After these steps are done, you should now see the RSS feeds load correctly.

Exporting and Importing Business Processes


Approvals in the **Business Processes** application can be exported and imported from one HPE Propel instance to another by the Organization Administrator.

Export a Business Process

1. Log in to the HPE Propel Portal as the `orgadmin` user.
2. Click the **Business Processes** application.
3. If the business process you want to export is not displayed, click the **All Processes** tab.
4. For the business process you want to export, click  and then select **Export**.
5. In the dialog that appears, save the zip file that contains the business process. Note the file name of the zip file for importing the business process into a different HPE Propel instance.

The business process' zip file is saved in your file system's **Downloads** folder. It can be imported into another HPE Propel instance via the **Business Processes** application.

Import a Business Process

1. Log in to the HPE Propel Portal as the `orgadmin` user.
2. Click the **Business Processes** application.
3. Click the business processes import  button.
4. In the **File Upload** dialog, select the zip file that contains the business process you want to import, and then click the **Open** button.

The business process is imported into the HPE Propel instance you are currently logged in to.

HPE Propel Custom Themes

Introduction to Themes

Each HPE Propel organization can have a unique color theme to change the appearance of the Launchpad and applications in the HPE Propel Portal.

The `themeName` attribute in the **Identity** application's **Customization** view for an organization specifies the color scheme.


You can change an organization's theme to an HPE Propel-provided theme or create your own custom theme and apply it to specific organizations.

- ["Apply the HPE Propel-Provided Dark Theme" below](#)
- ["Create and Apply a Custom Theme" on the next page](#)

Apply the HPE Propel-Provided Dark Theme

HPE Propel provides a color scheme with a dark background color for the Launchpad and applications in the HPE Propel Portal.

To configure the HPE Propel-provided dark theme for the Launchpad and HPE Propel Portal, specify "propel-dark-theme" in the `themeName` attribute in the **Identity** application's **Customization** view for a specific organization:

1. Log in to the HPE Propel Management Console as an administrator.
2. In the Launchpad, click the **Identity** application.
3. In the **Organization List** view, click the target organization.
4. In the **Organization Details** view, click **Customization**.
5. In the `themeName` attribute, click the edit  icon.
6. In the **Edit KeyPair** dialog, type "propel-dark-theme" in the **Value** field and click the **Save** button.

After specifying the *propel-dark-theme* for an organization, users who log in to the organization, via the organization's tenant, will see a dark background color for the Launchpad and applications in the HPE Propel Portal.

Create and Apply a Custom Theme

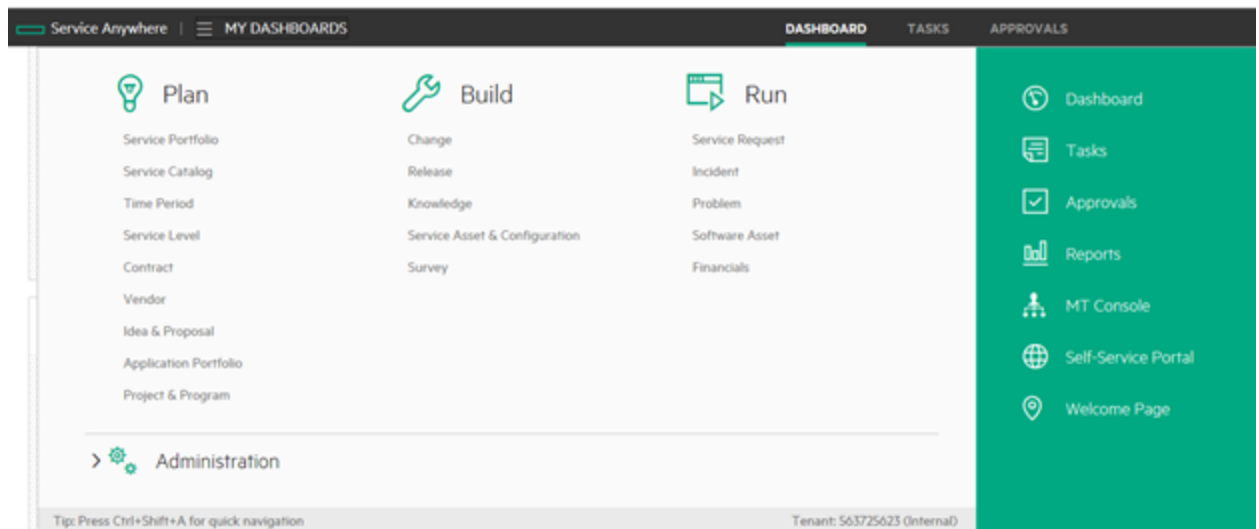
To create your own custom theme and apply it to a specific organization, refer to the *HPE Propel Theming Customization* whitepaper.

Installing the HPE SAW Adapter in HPE Propel

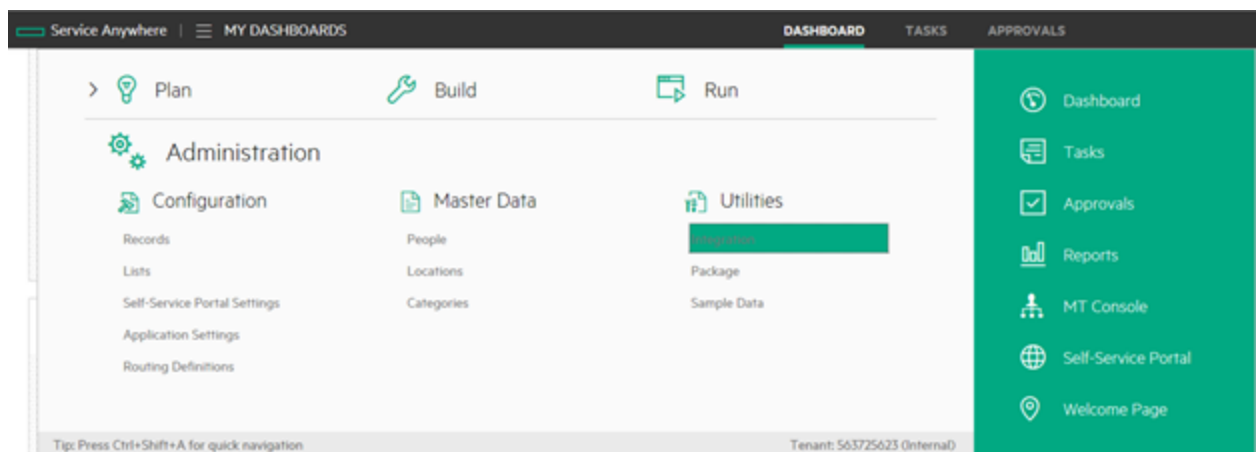
Beginning with the HPE Propel 2.20.p1 release, the HPE Service Anywhere adapter is not included for adding HPE SAW suppliers. The HPE SAW adapter is provided as a content pack that can be downloaded from the HPE Service Anywhere Download Center.

To download the content pack and install the HPE SAW adapter:

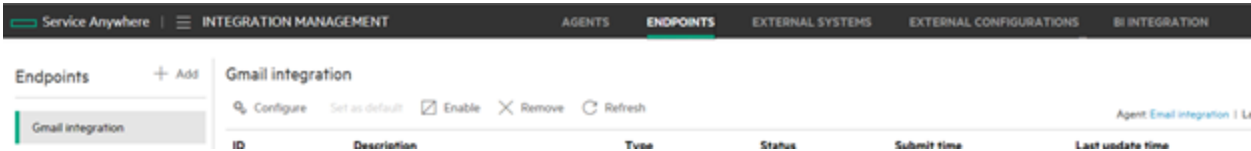
1. Navigate to the HPE Service Anywhere login page and log in as an Administrator.
2. In HPE Service Anywhere, click **My Dashboards**.



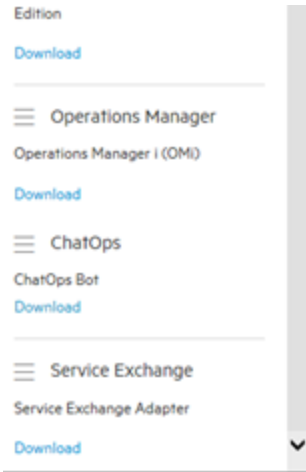
3. Click **Administration** to expand the **Administration** section and then click **Integration**, located in the **Utilities** section.



4. In the top menu, click **Endpoints**.



5. Scroll down to locate **Service Exchange** in the Download Center pane at the right side of the screen.



6. Under **Service Exchange Adapter**, click the **Download** link to download the adapter package (saw-sx-adapter.zip) and save it to the target location.
7. Navigate to the zip file downloaded in step 6 and extract it to the target location.
8. Follow the instructions provided in the `readme.pdf` file included in the zip archive to load the HPE SAW adapter content pack into HPE Propel.

After installing the HPE SAW adapter, **SAW** is available as a **Backend System Type** when creating a new Supplier in HPE Propel.

Replacing HPE Propel-Generated SSL Certificates

HPE Propel requires HTTPS (HTTP over SSL) for client browsers. HTTPS must be configured between HPE Propel and HPE Cloud Service Automation (HPE CSA) systems. HTTPS is optional for HPE Service Manager (HPE SM), however, HPE recommends configuring HTTPS between HPE Propel and HPE SM systems.

Important: Though HPE Propel-generated certificates can be configured during installation and used in production, HPE recommends that you configure trusted certificates 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.

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

Tips:

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

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

- The password is “changeit” for the HPE Propel global Java keystore (`/usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts`)
- The password is “propel2014” for the HPE Propel keystore (`/opt/hp/propel/security/.keystore`)

Preparation

Before performing these instructions and replacing the HPE Propel-generated certificates, make sure an SSL configuration between the HPE Propel VM and a supplier (end-point) system, such as HPE Cloud Service Automation or HPE Service Manager, works correctly. If you experience problems after replacing the SSL certificates, this will help you troubleshoot SSL issues.

To configure SSL and validate it works with suppliers, refer to the *Next Steps* chapter in the *HPE Propel Installation and Configuration Guide* for instructions.

Replace HPE Propel-Generated SSL Certificates

The instructions in this chapter are written for IT organizations that require both a CA-signed root certificate and an intermediate certificate. If your IT organization requires only a root certificate, you can simplify the instructions

Perform the following steps to replace the previously HPE Propel-generated SSL certificates with CA-signed SSL certificates. .

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

1. Stop the HPE Propel services:

```
# propel stop
```

2. Backup the current HPE Propel SSL directories:

```
# cp -rp /opt/hp/propel-install/ssl-tmp /opt/hp/propel-install/ssl-tmp.backup  
# cp -rp /opt/hp/propel/security /opt/hp/propel/security.backup
```

3. Initialize the SSL working directory:

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

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

Note: This re-creates the `/opt/hp/propel-install/ssl-tmp` directory and removes all previous files.

4. Obtain your IT organization's CA certificates for use by HPE Propel. Your IT organization can provide only a root certificate or both a root and an intermediate certificate. The instructions in this step are written for having both a root and an intermediate certificate. Considerations for the certificates are:

- They must be in PEM format.
- PEM certificates usually have extensions such as `.pem`, `.crt`, `.cer`, and `.key`.
- They must be Base64 encoded ASCII files and contain:

```
"-----BEGIN CERTIFICATE-----"
```

and

```
"-----END CERTIFICATE-----"
```

lines.

- a. Copy the root certificate as `CA.crt` and the intermediate certificate as `intermediate.crt` to the `/opt/hp/propel-install/ssl-tmp` directory.
- b. Merge both certificates in the `/opt/hp/propel-install/ssl-tmp` directory:

```
# cd /opt/hp/propel-install/ssl-tmp
# cat CA.crt intermediate.crt > rootPlusIntermediate.crt
```

5. Back up the existing HPE Propel global Java keystore:

```
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security
# cp cacerts cacerts.backup
```

6. Import the root certificate (`CA.crt`) into the HPE Propel global Java keystore

```
# keytool -importcert -file /opt/hp/propel-install/ssl-tmp/CA.crt
-alias <CA_ALIAS> -trustcacerts -keystore cacerts
```

Where `<CA_ALIAS>` is the CA alias you specify. The password is "changeit" for the global Java keystore.

7. Import the intermediate certificate (`intermediate.crt`) into the HPE Propel global Java keystore

```
# keytool -importcert -file /opt/hp/propel-install/ssl-tmp/intermediate.crt
-alias <INT_ALIAS> -trustcacerts -keystore cacerts
```

Where `<INT_ALIAS>` is the intermediate alias you specify.

Tip: You can verify that the global Java keystore contains your CA certificates:

```
# keytool -list -keystore cacerts -storepass changeit | grep <ALIAS>
```

Where `<ALIAS>` is either the CA alias or the intermediate alias you specified in steps 6 and 7.

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

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

Where `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 HPE 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"
```

Note: The private key password ("propel2014") is automatically created by the propel-ssl-setup.sh script.

This command creates two new directories and four new files

/opt/hp/propel-install/ssl-tmp/\$PROPEL_VM_HOSTNAME/ directory

/opt/hp/propel-install/ssl-tmp/\$PROPEL_VM_HOSTNAME/out/ directory

/opt/hp/propel-install/ssl-tmp/hostnames file

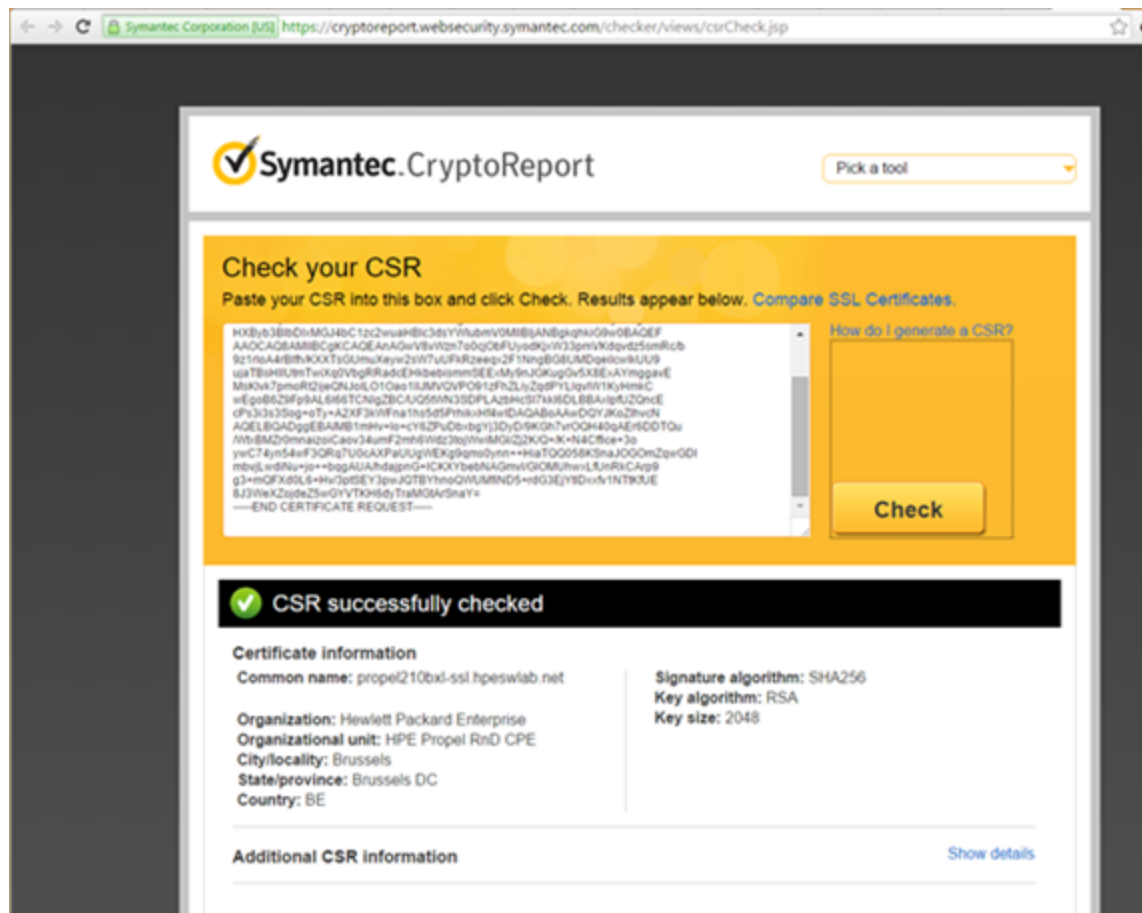
/opt/hp/propel-install/ssl-tmp/\$PROPEL_VM_HOSTNAME/private.key.pem file

/opt/hp/propel-install/ssl-tmp/\$PROPEL_VM_HOSTNAME/propel_host.key.csr file

/opt/hp/propel-install/ssl-tmp/\$PROPEL_VM_HOSTNAME/out/propel_host.key.rsa file

9. You can verify the content of your CSR by pasting its text in here:

<https://ssltools.websecurity.symantec.com/checker/views/csrCheck.jsp>



10. Send the CSR containing the public key to your CA. This is a process specific to your company, and network administrators should know how to accomplish this. Ask for the certificate to be delivered in PEM format. If it is not, you can convert formats with the `openssl` command.
11. After the certificate has been received from the CA, copy the new host certificate to:
`/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt`

If you need to extract the host certificate from a PEM file, you can extract the text beginning with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----"

```
[root@propel210bxi-ssl propel210bxi-ssl.hpeswlab.net]# cd out
[root@propel210bxi-ssl out]# ls -l
total 4
-rw-r--r--. 1 root root 1679 Feb  9 11:36 propel_host.key.rsa
[root@propel210bxi-ssl out]# vi propel_host.crt
[root@propel210bxi-ssl out]# ls -la
total 8
drwxr-xr-x. 2 root root  54 Feb  9 11:41 .
drwxr-xr-x. 3 root root  64 Feb  9 11:36 ..
-rw-r--r--. 1 root root 2358 Feb  9 11:41 propel_host.crt
-rw-r--r--. 1 root root 1679 Feb  9 11:36 propel_host.key.rsa
[root@propel210bxi-ssl out]# cat propel_host.crt
-----BEGIN CERTIFICATE-----
MIIGoDCCBYigAwIBAgIQEJHBerqery3i7oEBpBbM+TANBgkqhkiG9w0BAQUFADCB
nJEPMA0GA1UEChMGaHauY29tMR0wGAYDVQQLExFJVCBjb2ZyYXN0cnVjdHVyZTEL
MAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQtUGFja2FyZCBDb21wYW55MUAW
PgYDVQQDEZdIZXdsZXROLVBhY2thcmQgUHJpdmlF0ZSBDbGFzcyAyIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5MB4XDTE2MDIwOTAwMDAwMFoXDTE3MDIwODIzNTk1OVow
XDEGMB4GA1UEChQXSGV3bGV0dC1QYWNrYXJkIENvbnBhbnkxEDAOBgNVBASUB1Nl
cnZlcnMxJjAkBgNVBAMTHXByb3BlbDIxMGJ4bC1zc2wuaHBlc3dsYWIubmV0MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlt6vy02IEKJepCLI9XztgwZv
wqfncRuRHqTuEj+FTzfQ0NzB7i8RhcfEy598L/JQYel0CXWkh6xJm6TPmi4h1l/L
r82mlyoaCeNo8Zd0y8BG6k8fouX/xWESB0MlnyjlBhpCu5IQD/o8DmLV0RDyrCyX
jaHES6vOfPELxZWQMwp90/w355oPotEJcH1cRQ3sxfEGSyV5AJ0IpjTV2rkN9AiK
um2qi++SvmBTYcRPRKMqjyWdn+e08SXTT9k/dXu18UEI6RmQzqDlFgE+86C4KscM
Xzu27hU3FRH8b475cmrS30THD808u9I+7LLG9GqCSQ0RKV3UU5dH2FbXIOTjhwID
AQAB04IDGTCCAxUwDAYDVR0TAQH/BAIwADAObgNVHQ8BAf8EBAMCBLAWhwYDVR0j
BBgwFoAUN+33FXktMKWYmnW2XDfjiOoRatUwHQYDVR0OBBYEFDUjInZLav6d4gB9
-----
```

Important: HPE recommends reviewing the certificate-signing algorithm used and ensuring that strong encryption is used. For example, SHA1 is sometimes used, and instead, stronger algorithms such as SHA256 should be used. See [Viewing the SSL Certificate-Signing Algorithm](#) for more details.

12. Validate the host certificate and the CA match:

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

You should see the following message:

```
/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt: OK
```

Important: Do not proceed if you see any error messages. The CA and certificate must match. Restore the HPE Propel VM's files that were backed up in previous steps (2 and 5) and restart this procedure if necessary.

13. Create the certificate and the keystores:

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

The results of the `propel-ssl-setup.sh finish` script are:

```
[root@propel210b1-ssl propel-install]# ls -la /opt/hp/propel-install/overlay/*/security/  
/opt/hp/propel-install/overlay/_ALL_HOSTS_/security/:  
total 8  
drwxr-xr-x. 2 jetty jetty 43 Dec 9 02:30 .  
drwxr-xr-x. 3 jetty jetty 21 Dec 9 02:30 ..  
-rw-r--r--. 1 jetty jetty 1596 Feb 9 12:46 CA.crt  
-rw-r--r--. 1 jetty jetty 2932 Feb 9 12:46 propel.truststore  
  
/opt/hp/propel-install/overlay/${hostname}/security/:  
total 24  
drwxr-xr-x. 2 jetty jetty 4096 Dec 9 02:30 .  
drwxr-xr-x. 3 jetty jetty 21 Dec 9 02:30 ..  
-rw-r--r--. 1 jetty jetty 2141 Dec 9 02:30 .keystore  
-rw-r--r--. 1 jetty jetty 2433 Dec 9 02:30 propel_host.chain.crt  
-rw-r--r--. 1 jetty jetty 1099 Dec 9 02:30 propel_host.crt  
-rw-r--r--. 1 jetty jetty 1679 Dec 9 02:30 propel_host.key.rsa  
-rw-r--r--. 1 jetty jetty 2500 Dec 9 02:30 propel_host.pfx  
  
/opt/hp/propel-install/overlay/propel210b1-ssl.hpeswlab.net/security/:  
total 24  
drwxr-xr-x. 2 root root 4096 Feb 5 12:50 .  
drwxr-xr-x. 3 root root 21 Feb 5 12:50 ..  
-rw-r--r--. 1 root root 3089 Feb 9 12:46 .keystore  
-rw-r--r--. 1 root root 3954 Feb 9 12:46 propel_host.chain.crt  
-rw-r--r--. 1 root root 2358 Feb 9 11:41 propel_host.crt  
-rw-r--r--. 1 root root 1679 Feb 9 11:36 propel_host.key.rsa  
-rw-r--r--. 1 root root 3505 Feb 9 12:46 propel_host.pfx  
[root@propel210b1-ssl propel-install]#
```

14. Move all the created files, `intermediate.crt`, and `rootPlusIntermediate.crt` into their final locations:

Note: The yes commands preceding the cp commands automatically sends a "y" when prompted to overwrite an existing file.

```
# cd /opt/hp/propel-install/overlay/_ALL_HOSTS_/security
# yes | cp -p * /opt/hp/propel/security

# cd /opt/hp/propel-install/overlay/$PROPEL_VM_HOSTNAME/security
# yes | cp -p * /opt/hp/propel/security
# yes | cp -p .keystore /opt/hp/propel/security

# cp /opt/hp/propel-install/ssl-tmp/rootPlusIntermediate.crt
/opt/hp/propel/security/rootPlusIntermediate.crt

# cp /opt/hp/propel-install/ssl-tmp/intermediate.crt
/opt/hp/propel/security/intermediate.crt
```

```
[root@propel210b1-ssl propel-install]# cd /opt/hp/propel-install/overlay/_ALL_HOSTS_/security
[root@propel210b1-ssl security]# ls -la
total 8
drwxr-xr-x. 2 jetty jetty 43 Dec 9 02:30 .
drwxr-xr-x. 3 jetty jetty 21 Dec 9 02:30 ..
-rw-r--r--. 1 jetty jetty 1596 Feb 9 12:46 CA.crt
-rw-r--r--. 1 jetty jetty 2932 Feb 9 12:46 propel.truststore
[root@propel210b1-ssl security]# cp -p * /opt/hp/propel/security
cp: overwrite '/opt/hp/propel/security/CA.crt'? y
cp: overwrite '/opt/hp/propel/security/propel.truststore'? y
[root@propel210b1-ssl security]# cd /opt/hp/propel-install/overlay/propel210b1-ssl.hpeswlab.net/security/
[root@propel210b1-ssl security]# ls -la
total 24
drwxr-xr-x. 2 root root 4096 Feb 5 12:50 .
drwxr-xr-x. 3 root root 21 Feb 5 12:50 ..
-rw-r--r--. 1 root root 3089 Feb 9 12:46 .keystore
-rw-r--r--. 1 root root 3954 Feb 9 12:46 propel_host.chain.crt
-rw-r--r--. 1 root root 2358 Feb 9 11:41 propel_host.crt
-rw-r--r--. 1 root root 1679 Feb 9 11:36 propel_host.key.rsa
-rw-r--r--. 1 root root 3505 Feb 9 12:46 propel_host.pfx
[root@propel210b1-ssl security]# cp -p * /opt/hp/propel/security
cp: overwrite '/opt/hp/propel/security/propel_host.chain.crt'? y
cp: overwrite '/opt/hp/propel/security/propel_host.crt'? y
cp: overwrite '/opt/hp/propel/security/propel_host.key.rsa'? y
cp: overwrite '/opt/hp/propel/security/propel_host.pfx'? y
[root@propel210b1-ssl security]# cp -p .keystore /opt/hp/propel/security
cp: overwrite '/opt/hp/propel/security/.keystore'? y
[root@propel210b1-ssl security]# ls -la /opt/hp/propel/security
total 36
drwxr-xr-x. 2 propel root 4096 Feb 5 13:03 .
drwxr-xr-x. 33 propel root 4096 Feb 9 12:33 ..
-rw-r--r--. 1 jetty jetty 1596 Feb 9 12:46 CA.crt
-rw-r--r--. 1 root root 3089 Feb 9 12:46 .keystore
-rw-r--r--. 1 root root 3954 Feb 9 12:46 propel_host.chain.crt
-rw-r--r--. 1 root root 2358 Feb 9 11:41 propel_host.crt
-rw-r--r--. 1 root root 1679 Feb 9 11:36 propel_host.key.rsa
-rw-r--r--. 1 root root 3505 Feb 9 12:46 propel_host.pfx
-rw-r--r--. 1 jetty jetty 2932 Feb 9 12:46 propel.truststore
[root@propel210b1-ssl security]#
```

15. Make sure the CA.crt and intermediate.crt files are in the /opt/hp/propel/security directory on the HPE Propel VM. (They should have already been copied in step 14 above.)

16. Import the intermediate certificate (`intermediate.crt` file) into the HPE Propel truststore:

```
# cd /opt/hp/propel/security
```

```
# keytool -importcert -file intermediate.crt -keystore propel.truststore  
-trustcacerts
```

The password is "propel2014" for the HPE Propel truststore.

17. Update the `app.json` files on the HPE Propel VM with the following commands:

```
# cd /opt/hp/propel
```

```
# sed -i -e  
's!/opt/hp/propel/security/CA.crt!/opt/hp/propel/security/CA.crt,/opt/hp/propel  
/security/intermediate.crt!' $(find . -print | grep app.json)
```

18. Update the Identity Management (IdM) `*.json` files on the HPE Propel VM with the following commands:

```
# cd /opt/hp/propel/idmAdmin/conf
```

```
# sed -i -e  
's!/opt/hp/propel/security/CA.crt!/opt/hp/propel/security/CA.crt,/opt/hp/propel  
/security/intermediate.crt!' $(find . -print | grep endpoint.json)
```

```
# sed -i -e  
's!/opt/hp/propel/security/CA.crt!/opt/hp/propel/security/CA.crt,/opt/hp/propel  
/security/intermediate.crt!' $(find . -print | grep idm.json)
```

Update RabbitMQ

1. Edit the `/etc/rabbitmq/rabbitmq.config` file so that the `cacertfile` property has either the single root certificate (`CA.crt` file) or both the root and intermediate certificates (`rootPlusIntermediate.crt` file) specified. The following is an example of using both certificates:

```
[
  {rabbit, [
    {tcp_listeners, []},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/opt/hp/propel/security/rootPlusIntermediate.crt"},
      {certfile, "/opt/hp/propel/security/propel_host.crt"},
      {keyfile, "/opt/hp/propel/security/propel_host.key.rsa"},
      {verify, verify_none}}}
    ]},
  { rabbitmq_management, [
    {listener, [
      {port, 15672},
      {ssl, true},
      {ssl_opts, [
        {cacertfile, "/opt/hp/propel/security/rootPlusIntermediate.crt"},
        {certfile, "/opt/hp/propel/security/propel_host.crt"},
        {keyfile, "/opt/hp/propel/security/propel_host.key.rsa"}
      ]}
    ]}
  ]}
].
~
```

2. Restart RabbitMQ and clean up its log files

```
systemctl stop rabbitmq-server
```

```
rm -rf /var/log/rabbitmq/*
```

```
systemctl start rabbitmq-server
```

3. Make sure there are no errors in the

```
/var/log/rabbitmq/rabbit@<PROPEL_HOST_SHORTNAME>.log file.
```

Update HPE Operations Orchestration

Perform the following steps to update HPE Operations Orchestration (HPE OO) on the HPE Propel VM.

1. Stop the HPE OO service on the HPE Propel VM:

```
# systemctl stop central
```

2. Back up the existing HPE OO configuration:

```
# cd /opt/hp/oo/central/var
```

```
# cp -rp security security.backup
```

3. Manually delete the old certificates from the HPE OO stores and install the new certificates:

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

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

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

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

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

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

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

4. Restart HPE OO:

```
# systemctl start central
```

Exchange SSL Certificates from HPE Propel VM and Suppliers

The newly created SSL certificates on the HPE Propel VM and the supplier's certificates must be exchanged for SSL to work correctly. Refer to the *Configure SSL for a Supplier* chapter in the *HPE Propel Installation and Configuration Guide* for instructions.

Final SSL Configuration Steps and Validation

After exchanging SSL certificates on the HPE Propel VM and suppliers, clean up log files, configure file permissions, and restart the HPE Propel services:

```
# propel stop

# chmod 440 /opt/hp/propel/security/*

# chmod 440 /opt/hp/propel/security/.keystore

# chown propel:propel /opt/hp/propel/security/*

# chown propel:propel /opt/hp/propel/security/.keystore

# yes | rm -f /var/run/propel/*.pid

# yes | rm -rf /var/log/propel/*/*.*

# yes | rm -rf /opt/hp/propel/launchpad/.app/*.*

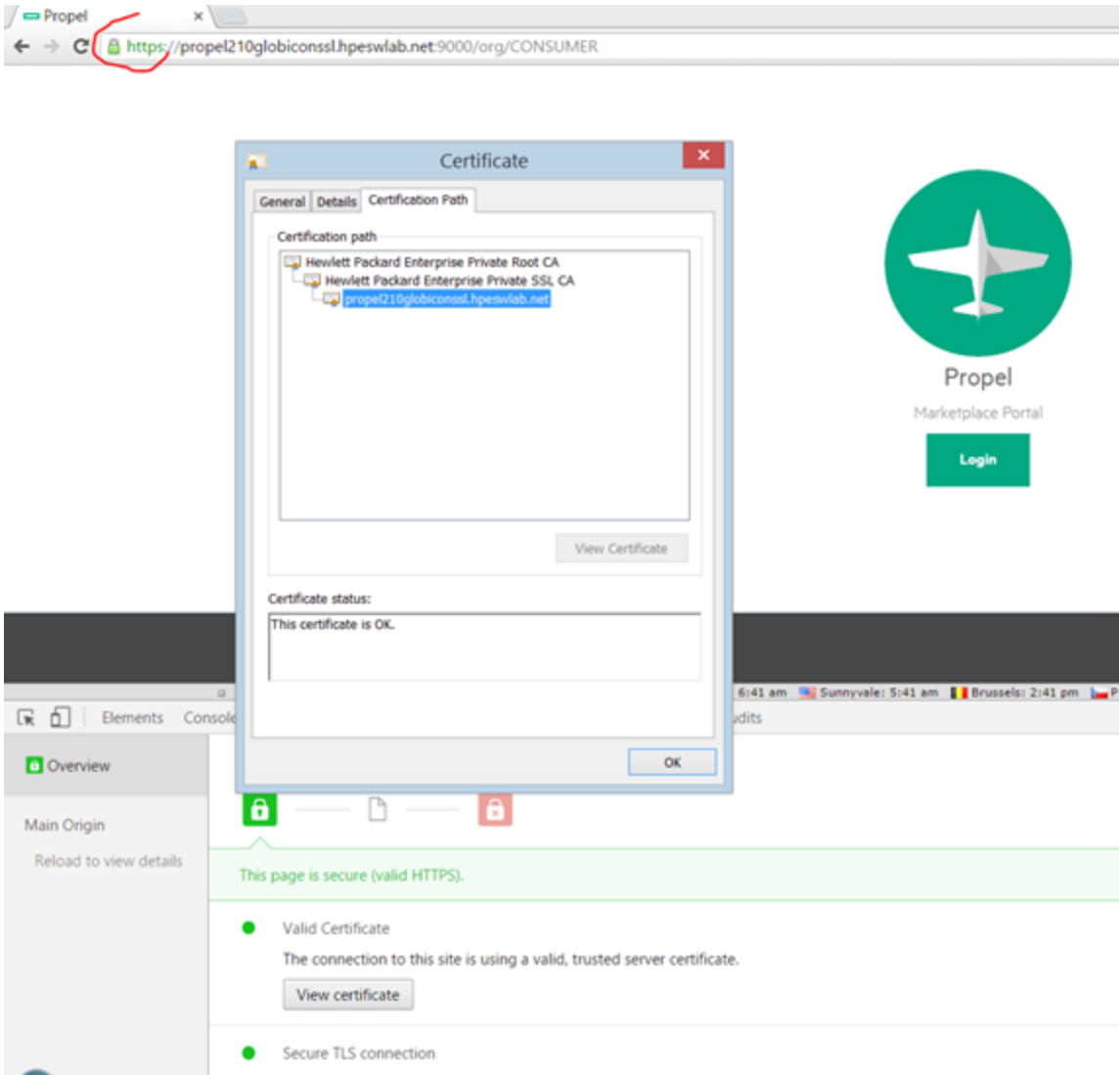
# propel start
```

Note: If the `jetty-sx` service does not start, inspect the `/var/log/messages` log file for errors. If an old `jetty-sx.pid` file is preventing `jetty-sx` from starting, remove the old `jetty-sx.pid` file and restart the `jetty-sx` service with the following command:

```
# systemctl restart jetty-sx
```

Make sure you can log in to the HPE Propel Launchpad and fulfill orders from the supplier systems.

To verify the new SSL certificate:



HPE Knowledge Management

This chapter provides instructions for installing HPE Knowledge Management (HPE KM) and configuring either the Solr plugin for IDOL as the search engine or the Smart Analytics (IDOL) search engine. Additional instructions are provided for loading HPE KM documents into HPE Service Manager (HPE SM).

These configuration instructions vary, depending on the search engine enabled in HPE SM:

- HPE SM uses the Solr search engine.
- HPE SM uses Smart Analytics (IDOL) as the search engine.

Installation

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

1. Access HPE DM from HPE Live Network at: <https://hpln.hpe.com/contentoffering/itsm-deployment-manager>. Note that you need to sign in to your HP Passport account. Download the following:
 - a. *HPE ITSM Deployment Manager Quick Start Guide* (<https://hpln.hpe.com/node/26347/attachment>)
 - b. HPE ITSM Deployment Manager Version 3.0 (From ITSM Deployment Manager home page <https://hpln.hpe.com/contentoffering/itsm-deployment-manager> **Downloads** tab, select **Deployment Manager Version 3.0**. Click **Download**, and select the latest version to download.)
2. Follow the instructions in the *HPE DM Quick Start Guide* to install and configure HPE DM.
3. In the HPE DM **Environments** tab, click **More Wizards...**, then select **HP Service Manager – Knowledge Management**, and follow the instructions to install HPE KM.
4. HPE SM must be restarted for HPE KM to become available for use.

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

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

HPE Knowledge Management Indexing

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

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

Tip: To quickly verify that KMUpdate is running, type `status` in the Command window to display all processes currently running.

HPE Knowledge Management Best Practices

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

HPE Knowledge Management Configuration Steps – After HPE Propel Installation

Perform the following steps to configure HPE KM after the HPE Propel installation.

1. On the HPE Propel VM, stop the HPE SX UI service:

```
# systemctl stop sx-client-ui
```

2. Add the following lines to the HPE SM's `sm.cfg` file. This configuration avoids using web services

over the HPE SM LoadBalancer port, which is often port 13080:

```
# Propel: port used by Catalog Aggregation and Catalog microservices
sm -httpPort:21090 -httpsPort:21493 -debugnode
-log:../logs/sm-propel-2.20.log -sslConnector:1 ssl:0
```

This configuration allows connecting either with SSL (port 21493) or without SSL (port 21090).

3. HPE Propel integration with HPE SM's KM module will use both the HPE KM Search Engine and an HPE SM integration servlet to gather the documents and related attachments. Determine which port the master HPE KM Search Engine uses as follows: from the HPE SM navigator menu, select **Knowledge Management > Configuration > Configure Search Servers**, then click **Search**. By default, this will be port 8080.
4. On the HPE Propel VM, modify the `/opt/hp/propel/sxClientUI/app.json` file. The following partial example shows modifications to the knowledge section:

```
}, "knowledge": {
  "mount": "/api/km",
  "kmUrl": "http://SM_SOLR_SERVER:8380",
  "kmContextPath": "/KMCores",
  "kmStrictSSL": true,
  "kmSecureProtocol": "TLSv1_method",
  "kmCa": "/opt/hp/propel/security/CA.crt",
  "kmAttachUrl": "https://SM_SERVER:21493",
  "kmAttachContextPath": "/SM/9/rest",
  "kmAttachStrictSSL": false,
  "kmAttachSecureProtocol": "TLSv1_method",
  "kmAttachCa": "/opt/hp/propel/security/CA.crt",
  "kmAttachUsername": "falcon",
  "kmAttachPassword": "",
},
```

Where `SM_SERVER` is the fully qualified hostname of the HPE SM server. Other considerations for configuring the knowledge section are:

- The `kmUrl` property contains the host and port of the HPE SM Solr server. The default HPE SM Solr port is 8380, but the port number can vary.
- The `kmAttachUrl` property can also use port 21090, but then `https` should be changed to `http`.
- The default value for the `kmAttachStrictSSL` property is `true`, but this needs to be set to `false` in case self-signed SSL certificates are used.

- The `kmAttachUsername` property contains the HPE SM integration account. This can be a clone of the `falcon` HPE SM user.
5. Load the HPE Propel VM's CA-signed certificate into the HPE SM system's keystore. The general steps to do this are:
- a. Copy the HPE Propel VM's `/opt/hp/propel/security/CA.crt` file to the HPE SM system's `/tmp` directory.
 - b. On the HPE SM system, import the HPE Propel CA-signed certificate:

```
# keytool -import -file /tmp/CA.crt -alias Propel_CA -trustcacerts -keystore <SM-KEYSTORE-PATH>/cacerts
```

Where `SM-KEYSTORE-PATH` is the location of the `cacerts` file on the HPE SM system.
 - c. On the HPE SM system, restart HPE SM:

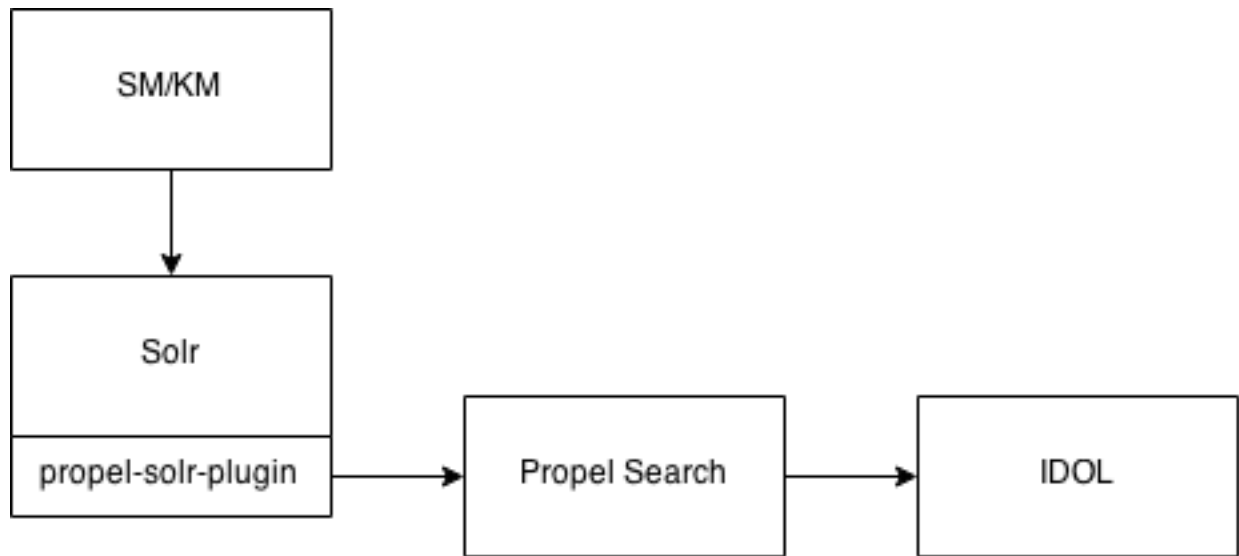
```
# service sm restart
```
6. Load the HPE SM system's CA-signed certificate into the HPE Propel VM's keystore. The general steps to do this are:
- a. Copy the HPE SM system's `CA.crt` file to the HPE Propel VM's `/tmp` directory.
 - b. On the HPE Propel VM, import the HPE SM CA-signed certificate:

```
# keytool -import -file /tmp/CA.crt -alias SM_CA -trustcacerts -keystore /usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts
```
 - c. On the HPE Propel VM, start the HPE SX UI service:

```
# systemctl restart sx-client-ui
```
7. Depending on the search engine enabled in HPE SM:
- If HPE SM uses the Solr search engine, continue with ["IDOL Search Installation and Configuration Using Solr"](#) on the next page.
 - If HPE SM uses Smart Analytics (IDOL) as the search engine, continue with ["Search Installation and Configuration Using Smart Analytics \(IDOL\)"](#) on page 40.

IDOL Search Installation and Configuration Using Solr

Most HPE SM installations prior to 9.41 use the Solr search engine. To configure HPE SM and HPE KM to work with HPE Propel Search, you must install the Solr plugin and configure it to send changes to HPE Propel Search.



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

Solr Plugin Installation Steps

1. On the HPE Propel VM, copy the `/opt/hp/propel/search/propel-solr-plugin.zip` file to the HPE SM/HPE KM machine.
2. Unzip the `propel-solr-plugin.zip` file. The contents are:
jackson-core-asl-1.9.13.jar
jackson-mapper-asl-1.9.13.jar
jasypt-1.9.2.jar
KMExtAccess.unl
propel-solr-plugin-1.1.0.jar
3. Copy the `.jar` files to your primary search server. That is, copy `propel-solr-plugin-1.1.0.jar`, `jackson-mapper-asl-1.9.13.jar`, `jackson-core-asl-1.9.13.jar`, and `jasypt-`

1.9.2.jar to <Primary_Search_Server>\Search_Engine\tomcat\webapps\KMCores\WEB-INF\lib\.

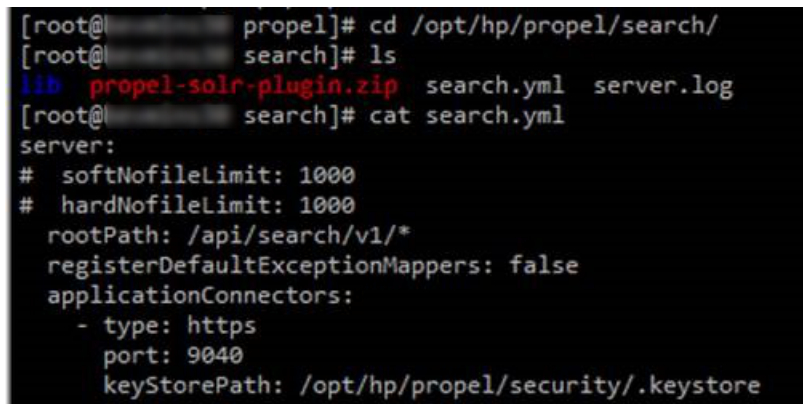
4. Edit the <Primary_Search_Server_Home>\Service Manager 9.30\Search_Engine\kmsearchengine\KMCores\kmcore\conf\solrconfig.xml file to add an updateRequestProcessorChain:

Add updateRequestProcessorChain to solrconfig.xml File Example

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

Where:

- *Hostname* is the hostname of the HPE Propel server.
- *Port* is the port defined for the search.endpoint parameter in the /opt/hp/propel-install/setup.properties file on the HPE Propel server. The port number is visible in the HPE Propel Search services /opt/hp/propel/search/search.yml configuration file, and is 9040 by default.



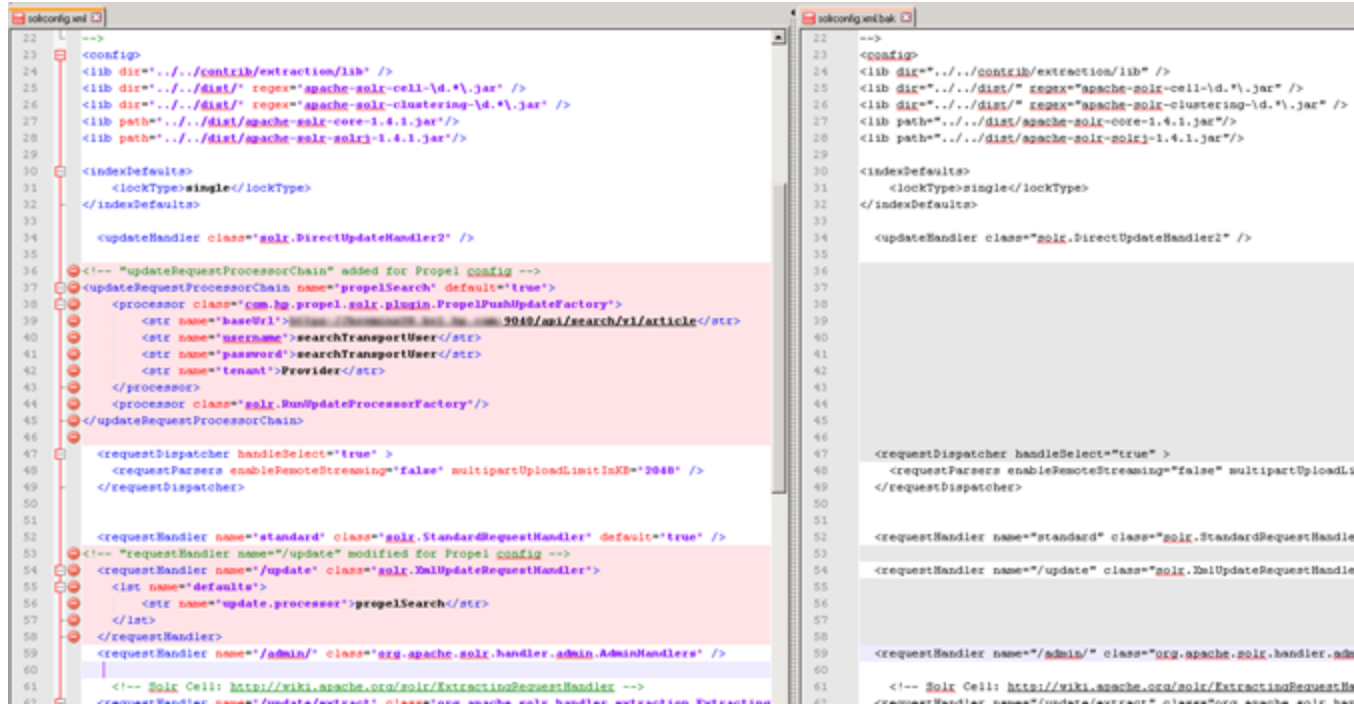
```
[root@propel]# cd /opt/hp/propel/search/
[root@propel]# ls
lib propel-solr-plugin.zip search.yml server.log
[root@propel]# cat search.yml
server:
#  softNofileLimit: 1000
#  hardNofileLimit: 1000
rootPath: /api/search/v1/*
registerDefaultExceptionMappers: false
applicationConnectors:
- type: https
  port: 9040
  keyStorePath: /opt/hp/propel/security/.keystore
```

- *Password* is the password for searchTransportUser. (The default password is searchTransportUser.)
5. Update the same solrconfig.xml and modify the requestHandler.

Modify requestHandler in solrconfig.xml File Example


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

Example content for steps 4 and 5 (compared with an out-of-the-box solrconfig.xml file):



6. In the HPE SM client, apply the `KMExtAccess.unl` unload file.
7. Restart HPE KM.
8. Restart HPE SM.
9. In the HPE SM client, reindex HPE KM.
 - a. Select **Knowledge Management** -> **Administration** -> **Environment**.
 - b. Check **SRC**.
 - c. Select the **Search Server Name**.

- d. Click **Full Reindex**.

HP Service Manager

To Do Queue: My To Do List environment: knowledge management

KNOWLEDGE MANAGEMENT APPLICATION ENVIRONMENT

☒ Assign the Default Knowledge View Group to all operators

☒ Use Adaptive Learning to enhance search results

For the changes to take effect, you must log out and log back in.

Max Number Documents Returned from a Search: 100

Default Expiration Period (0 if document never expires): 365 days

Style text for search results:

```
<STYLE>
body{
  PADDING-RIGHT: 0px;
  PADDING-LEFT: 0px;
  FONT-SIZE: 11px;
  PADDING-BOTTOM: 0px;
  MARGIN: 0px;
  COLOR: #000000;
  PADDING-TOP: 0px;
  FONT-FAMILY: Verdana, Arial, Helvetica, sans-serif;
  BACKGROUND-COLOR: #ffffff;
  BORDER-top: 0px none #ffffff;
  BORDER-bottom: 1px solid #999999;
}
```

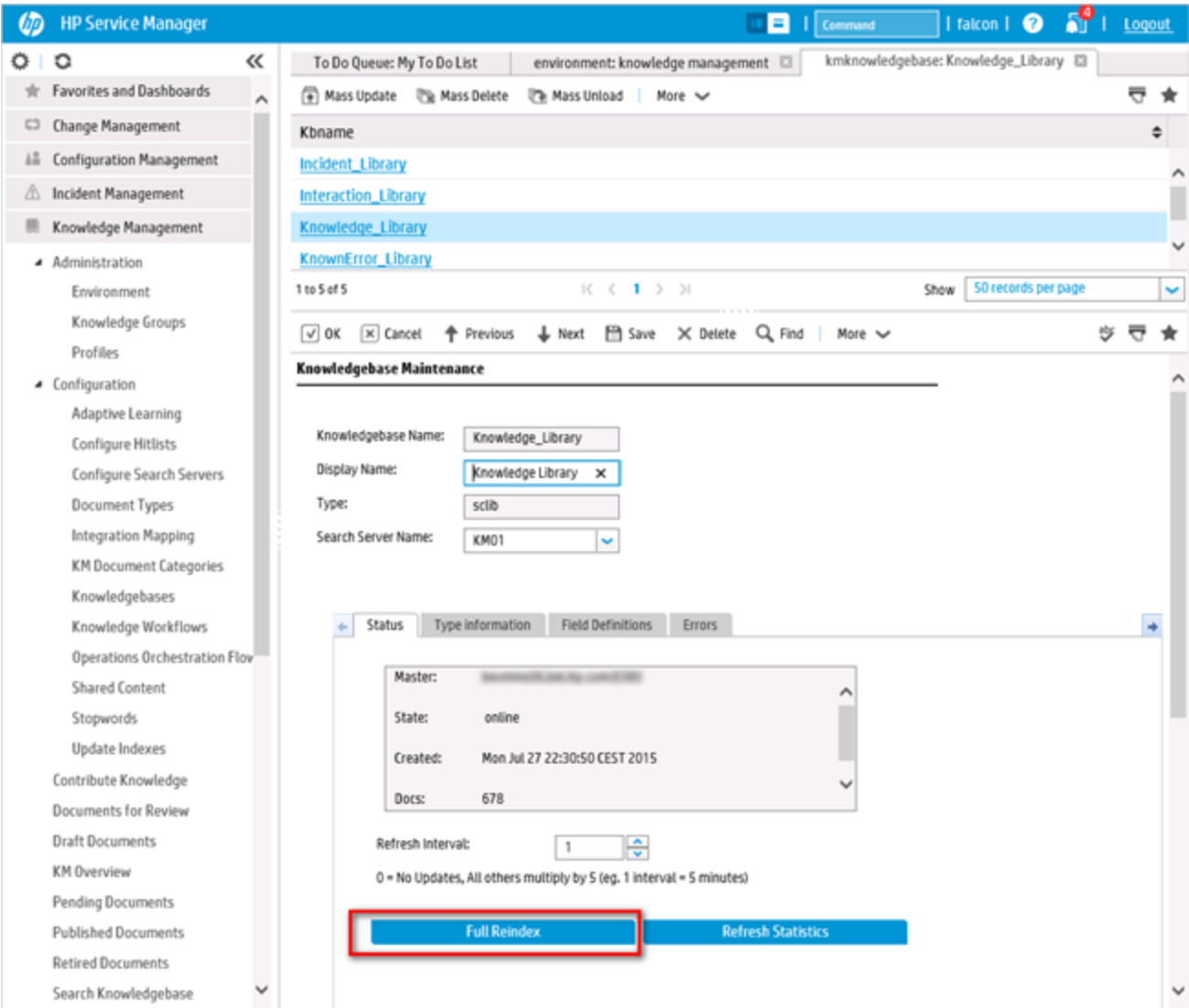
SAC? ☒

Highlight content of attachment in search result? ☒

Search Server Name: KNO1

Full Reindex

10. In the HPE SM client, reindex the HPE KM Libraries:
- Select **Knowledge Management -> Knowledgebases**.
 - Click on each of the libraries, and then click **Full Reindex**.



You have completed the procedure for configuring IDOL search to use the Solr plugin. For instructions to load HPE KM documents into HPE SM, see ["Load HPE KM Documents into HPE Service Manager" on page 45](#)

Search Installation and Configuration Using Smart Analytics (IDOL)

Most HPE SM 9.41 and later installations use the Smart Analytics (IDOL) search engine. This section provides instructions for enabling HPE KM search in HPE Propel when Smart Analytics is enabled in HPE SM.

Connecting HPE Propel to HPE SM 9.41 for Smart Analytics

If you use HPE Propel to connect to HPE SM 9.41, follow these steps; otherwise, continue to ["Setting Up Smart Analytics in HPE SM" on the next page.](#)

1. Import the `/opt/hp/propel/sx/contentStorage/sm-base/sm/SupportSingleIDOL.unl` unload file in the adaptor package.
2. If Smart Analytics is already enabled in HPE SM 9.41, upgrade Smart Analytics to 9.50 by using the Smart Analytics 9.50 installer; if Smart Analytics has not been enabled in HPE SM 9.41, install Smart Analytics 9.50 directly. For installation or upgrade instructions, see the *Service Manager 9.50 Smart Analytics Administrator and User Guide*.
3. Install Content-Propel and QMS, and specify the QMS and Content-Propel ports during the installation process.
4. Edit the `<Smart Analytics upgraded to Smart Analytics 9.50>/IDOL/IDOLServer.cfg` file:

- a. Increase the `Number` value in the `DistributionIDOLServers` section from `X` to `X+1`:

```
[DistributionIDOLServers]
#Number=3
Number=4
```

- b. Increase the `VirtualDatabases` value in the `Server` section from `N` to `N+4`:

```
[Server]
...
#VirtualDatabases=25
VirtualDatabases=29
```

- c. Add the following information. The IDOL server number needs input `X`.

```
[IDOLServer3]
Name=Content-Propel
Host=127.0.0.1
```

```
Port=10020  
DistributeByFieldsValues=PROPEL
```

- d. Add the following information. The `vdb#` is increased from `N` to `N+3`. The `mapsto` number is `X`, which means the information from the HPE Propel side will index into this content.

```
[vdb25]  
dbname=Offerings  
type=combinator  
mapsto=3:Offerings
```

```
[vdb26]  
dbname=Article  
type=combinator  
mapsto=3:Article
```

```
[vdb27]  
dbname=Services  
type=combinator  
mapsto=3:Services
```

```
[vdb28]  
dbname=Support  
type=combinator  
mapsto=3:Support
```

5. Restart `IDOLServer.exe` in the IDOL folder.
6. Continue with ["Configuring HPE Propel for Smart Analytics \(IDOL\)" on the next page](#).

Setting Up Smart Analytics in HPE SM

Make sure that you complete the following tasks in HPE SM to enable Smart Search for HPE KM.

1. Install and configure Smart Analytics. Make sure to select *SMA for Service Portal*.
2. Enable Smart Analytics.
3. Configure the knowledge library for Smart Search and complete a full indexing.

Note: Refer to the *Service Manager Smart Analytics Administrator and User Guide* for detailed instructions.

After you finish the full indexing in HPE SM and HPE SM can search from the knowledge library by using Smart Search, continue with "[Configuring HPE Propel for Smart Analytics \(IDOL\)](#)" below.

Configuring HPE Propel for Smart Analytics (IDOL)

To configure HPE Propel to use Smart Analytics as the search engine, follow these steps on the HPE Propel VM that contains the search and `sx-client-ui` services:

1. Log in to the HPE Propel VM as `root`.
2. Stop the search and `sx-client-ui` services:

```
# systemctl stop search
# systemctl stop sx-client-ui
```

3. Edit the `/opt/hp/propel/search/search.yml` file:

- a. Set the `"smaEnabled"` parameter to `"true"` as displayed in the following partial example:

```
...
idol:
...
smaEnabled: true
...
```

- b. For each IDOL component, change the `hostname` value to the address of the single IDOL server (Smart Analytics) and update the port accordingly:

```
...
query:
  hostname: localhost
  port: 14000
...
index:
  hostname: localhost
  port: 14001
...
attach:
  hostname: localhost
  port: 7000
...
qms:
  hostname: localhost
  port: 16000
...
agentStore:
  hostname: localhost
```

port: 14051
...

The following table lists the locations of the port numbers for each component in Smart Analytics.

Component	Where to locate the port number
query	Location: <Smart Analytics installation>/IDOL/IDOLServer.cfg [Server] //SecurityDebugLogging=true Port=9000 IndexPort=9001
index	Location: <Smart Analytics installation>/IDOL/IDOLServer.cfg [Server] //SecurityDebugLogging=true Port=9000 IndexPort=9001
attach	Location: <Smart Analytics installation>/CFS/CFS.cfg [Server] Port=7000 QueryClients=*,127.0.0.1,::1 AdminClients=*,127.0.0.1,::1
qms	Location: <Smart Analytics installation>/QMS/QMS.cfg [Server] Port=16000 AdminClients=*,127.0.0.1,::1 QueryClients=*,127.0.0.1,::1
agentStore	Location: <Smart Analytics installation>/IDOL/agentstore/portinfo.dat [Ports] ACIPort=9050 IndexPort=9051 QueryPort=9052 ServicePort=9053

4. Start the search service:

```
# systemctl start search
```

5. Open the /opt/hp/propel/sxClientUI/app.json file, and then add the smaEnabled flag and configure kmAttachUrl as displayed in the following partial example:

```
...  
"knowledge": {  
  "mount": "/api/km",  
  "smaEnabled": true,  
  "kmAttachUrl": "https://SM_SERVER:13080",  
  ...  
}
```

6. Start the `sx-client-ui` service:

```
# systemctl start sx-client-ui
```

7. Set the HPE SM user with the RESTful API capability in `/opt/hp/propel/sxClientUI/app.json`. The user in `/opt/hp/propel/sxClientUI/app.json`, such as `falcon` in the following configuration example, should have the RESTful API capability added in HPE SM. By doing so, the HPE Propel consumer users can drill down to the KM article detail page.

```
}, "knowledge": {  
  "mount": "/api/km",  
  "smaEnabled": true,  
  "kmUrl": "",  
  "kmContextPath": "/KMCores",  
  "kmStrictSSL": true,  
  "kmSecureProtocol": "TLSv1_method",  
  "kmCa": "/opt/hp/propel/security/CA.crt",  
  "kmAttachUrl": "https://SM_SERVER:13080",  
  "kmAttachContextPath": "/SM/9/rest",  
  "kmAttachStrictSSL": true,  
  "kmAttachSecureProtocol": "TLSv1_method",  
  "kmAttachCa": "/opt/hp/propel/security/CA.crt",  
  "kmAttachUsername": "falcon",  
  "kmAttachPassword": ""  
},
```

You have completed the procedure for configuring IDOL search to use Smart Analytics. For instructions to load HPE KM documents into HPE SM, see ["Load HPE KM Documents into HPE Service Manager" on the next page](#).

Load HPE KM Documents into HPE Service Manager

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

Pre-Requisites for Loading Documents

All documents loaded into HPE SM have the following settings:

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

Document Formats

Use the following formats for loading HPE KM documents into HPE 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 HPE 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</trainingRequirement><imageItem></imageItem>
</TrainingInfo><SettingRequirement></SettingRequirement><title>This page has been
temporarily disabled</title></root>
```

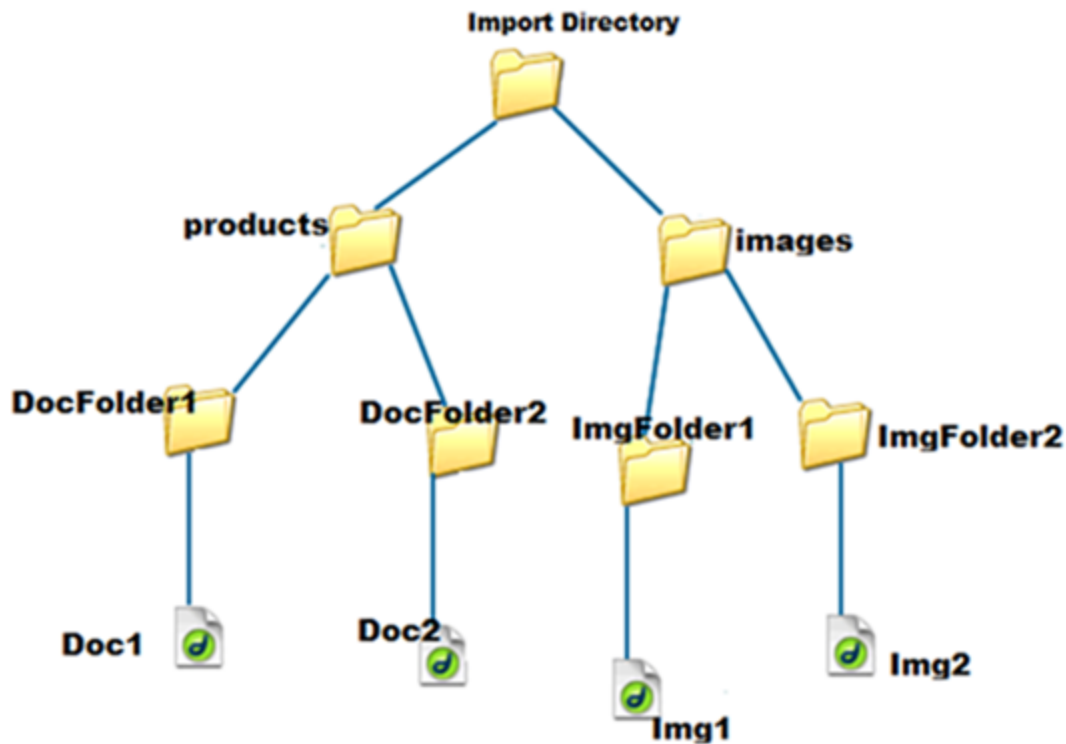
HPE KM Documents Directory Structure

The Import directory for the HPE 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.

Example Import Directory Structure



How to Load HPE KM Documents

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

1. Import the HPE Propel web services into HPE SM:
 - a. Transfer the `HPPropelKnowledge.unl` and `HPPropelKnowledgeAttachment.unl` web services files from the HPE Propel VM to the HPE SM system. The web services files are in the `/opt/hp/propel/km/webservices` directory on the HPE Propel VM
 - b. Start HPE SM, and in the HPE 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 `HPPropelKnowledgeAttachment.unl` web services file.

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

2. To test the import process:
 - a. In HPE SM, navigate to **Tailoring -> Web Services -> Web Service Configuration**.
 - b. Search for the **Service Name** `HPPropelKMAggregation`. If the HPE Propel web services are configured correctly, `HPPropelKMAggregation` contains the `HPPropelKnowledge` and `HPPropelKnowledgeAttachment` objects.
3. *Optional* - If you want to upload sample HPE KM documents, they are available in the `documents.zip` file that is in the `/opt/hp/propel/km` directory on the HPE Propel VM. Unzip the file and extract the sample documents by running the following commands as `root` on the HPE Propel VM:

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

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

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

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

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

For help about this script:

```
# ./PropelKMImporter.sh -help
```

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

In HPE SM, navigate to **Knowledge Management -> Search Knowledgebase**.

(Using the Window client got to menu options [the black triangle at the right side] and select **Expert Search**. Using the web client, in the menu bar, click **More** and select **Expert Search**.)

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

DocType: "Question/Answer"

Status: "Externally Published"

Category: "Propel"

Changing HPE Propel Default User Accounts' Passwords

HPE 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, HPE recommends that you change the default passwords associated with these accounts, however, do not change the user names. You can also disable the `admin`, `orgadmin`, and `consumer` user accounts and create your own users with identical roles.

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

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

Note: In the HPE Propel 2.20 release, some default passwords have been updated, while others are the same as in prior releases. Many of the default keystore passwords remain as they were in the 1.xx releases. If an updated default password does not work, try the prior release password.

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

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

Important: When changing default passwords, use strong passwords consisting of at least six characters. The more characters the stronger the password. Use a combination of letters, numbers, and symbols.

Change Passwords for HPE Propel Management Console User Accounts

The following HPE Propel user account is used to access administrative applications in the HPE Propel Management Console.

admin User: HPE Propel Management Console

Username	admin
Default Password	propel
Usage	This Administrator account is used to log in to the HPE Propel Management Console to manage HPE Propel settings across all of the organizations.
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Administrator role in the HPE Propel Management Console.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/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.):</p> <pre>propel,ROLE_REST,disabled</pre> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> </div> <p>By default, the unencrypted value of this property is:</p> <pre>propel,DIAGNOSTICS_ADMIN,SUPPLIER_VIEWER,CONTENT_ADMIN,LICENSE_ADMIN,SUPER_IDM_ADMIN,ROLE_REST,enabled</pre> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p>
To Change Password	<p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/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 - HPE Propel User Accounts" on page 58 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).</p> <p>You must also update and use the same password for every REST API call that uses</p>

admin User: HPE Propel Management Console, continued

	<p>the password.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p> </div> <p>By default, the unencrypted value of this property is: propel,DIAGNOSTICS_ADMIN,SUPPLIER_VIEWER,CONTENT_ADMIN,LICENSE_ADMIN, SUPER_IDM_ADMIN,ROLE_REST,enabled</p>
--	---

Change Passwords for HPE Propel Portal User Accounts

The following HPE Propel user accounts are used to access applications in the HPE Propel Portal.

orgadmin User: HPE Propel Portal

Username	orgadmin
Default Password	propel
Usage	<p>This Organization Administrator account is used to access both the HPE Propel Portal and HPE Propel administrative applications for an organization, such as Catalog Connect and Policies. (LDAP does not have to be configured.) This user belongs to the "HPE Propel consumer internal group" and is a member of the HPE Propel Consumer organization. (Both the group and the user are provided as samples.)</p>
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Organization Administrator role in the HPE Propel Portal.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/consumer-users.properties file. Update the orgadmin property to disable this user account. For example, set orgadmin to the following value. (This value should be encrypted.):</p> <p>propel,SERVICE_CONSUMER,ROLE_REST,disabled</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> </div> <p>By default, the unencrypted value of this property is: propel,IDM_ADMIN,CATALOG_ADMIN,AGGREGATION_ADMIN,CONSUMER,SUPPORT, SUBSCRIPTION_ADMIN,SUPPLIER_ADMIN,ROLE_REST,enabled</p> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p>

orgadmin User: HPE Propel Portal, continued

To Change Password	<p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/consumer-users.properties file. Update the password value of the orgadmin property and encrypt the entire value, including the roles and the account status. (See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p> <div data-bbox="391 520 1370 632" style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p> </div> <p>By default, the unencrypted value of this property is: propel, IDM_ADMIN, CATALOG_ADMIN, AGGREGATION_ADMIN, CONSUMER, SUPPORT, SUBSCRIPTION_ADMIN, SUPPLIER_ADMIN, ROLE_REST, enabled</p>
---------------------------	---

consumer User: HPE Propel Portal

Username	consumer
Default Password	propel
Usage	<p>This consumer account is used to log in to the HPE Propel Portal. (LDAP does not have to be configured.) This user belongs to the "HPE Propel consumer internal group" and is a member of the HPE Propel Consumer organization. (Both the group and the user are provided as samples.</p>
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Consumer role in the HPE Propel Portal.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/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.):</p> <p>propel, CONSUMER, SUPPORT, ROLE_REST, disabled</p> <div data-bbox="391 1501 1370 1612" style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> </div> <p>By default, the unencrypted value of this property is: propel, CONSUMER, SUPPORT, ROLE_REST, enabled</p> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p>

consumer User: HPE Propel Portal, continued

To Change Password	<p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/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 - HPE Propel User Accounts" on page 58 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).</p> <div data-bbox="391 520 1365 632"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p> </div> <p>By default, the unencrypted value of this property is: propel,CONSUMER,SUPPORT,ROLE_REST,enabled</p>
---------------------------	--

Change Passwords for HPE Propel Transport User Accounts

The following HPE Propel user accounts are used as transport users.

idmTransportUser User: HPE Propel Transport User

Username	idmTransportUser
Default Password	idmTransportUser
Usage	This transport user is an integration user for the Provider organization.
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Organization Administrator role in the HPE Propel Portal.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/integrationusers.properties file. Update the idmTransportUser property to disable this user account. For example, set idmTransportUser to the following value. (This value should be encrypted.):</p> <p>idmTransportUser,ROLE_ADMIN,PERM_IMPERSONATE,disabled</p> <div data-bbox="391 1570 1365 1682"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> </div> <p>By default, the unencrypted value of this property is: idmTransportUser,ROLE_ADMIN,PERM_IMPERSONATE,enabled</p> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 for instructions on how to encrypt this value. The encrypted value is preceded by ENC without any</p>

idmTransportUser User: HPE Propel Transport User, continued

	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	<p>Edit the \$PROPEL_HOME/idm-service/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 - HPE Propel User Accounts" on page 58 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).</p> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p> <p>By default, the unencrypted value of this property is: idmTransportUser,ROLE_ADMIN,PERM_IMPERSONATE,enabled</p>

sxCatalogTransportUser User: HPE Propel Transport User

Username	sxCatalogTransportUser
Default Password	sxCatalogTransportUser
Usage	This transport user is a seeded user for the Provider organization.
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Consumer role in the HPE Propel Portal.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/provider-users.properties file. Update the sxCatalogTransportUser property to disable this user account. For example, set sxCatalogTransportUser to the following value. (This value should be encrypted.):</p> <p>sxCatalogTransportUser,CONSUMER,SUPPORT,ROLE_REST,disabled</p> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> <p>By default, the unencrypted value of this property is: sxCatalogTransportUser,CONSUMER,SUPPORT,ROLE_REST,enabled</p> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p>

sxCatalogTransportUser User: HPE Propel Transport User, continued

To Change Password	<p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/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 - HPE Propel User Accounts" on page 58 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).</p> <div data-bbox="407 541 1336 606"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p> </div> <p>By default, the unencrypted value of this property is: sxCatalogTransportUser,CONSUMER,SUPPORT,ROLE_REST,enabled</p>
---------------------------	--

searchTransportUser User: HPE Propel Transport User

Username	searchTransportUser
Default Password	searchTransportUser
Usage	This transport user is a seeded user for the Provider organization.
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Consumer role in the HPE Propel Portal.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/provider-users.properties file. Update the searchTransportUser property to disable this user account. For example, set searchTransportUser to the following value. (This value should be encrypted.):</p> <p>searchTransportUser,CONSUMER,SUPPORT,ROLE_REST,disabled</p> <div data-bbox="407 1388 1336 1453"> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> </div> <p>By default, the unencrypted value of this property is: searchTransportUser,CONSUMER,SUPPORT,ROLE_REST,enabled</p> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p>
To Change Password	Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/provider-users.properties file. Update the password value of the searchTransportUser property and encrypt the entire value, including the roles and

searchTransportUser User: HPE Propel Transport User, continued

	<p>the account status. (See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p> <p>By default, the unencrypted value of this property is: searchTransportUser,CONSUMER,SUPPORT,ROLE_REST,enabled</p>
--	---

externalLinkTransportUser User: HPE Propel Transport User

Username	externalLinkTransportUser
Default Password	externalLinkTransportUser
Usage	This transport user is a seeded user for the Provider organization.
To Disable	<p>You should disable this account only after you have set up and verified a user with the HPE Propel Consumer role in the HPE Propel Portal.</p> <p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/provider-users.properties file. Update the externalLinkTransportUser property to disable this user account. For example, set externalLinkTransportUser to the following value. (This value should be encrypted.):</p> <p>externalLinkTransportUser,CONSUMER,SUPPORT,ROLE_REST,disabled</p> <p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled</p> <p>By default, the unencrypted value of this property is: externalLinkTransportUser,CONSUMER,SUPPORT,ROLE_REST,enabled</p> <p>See "Encrypt a Password - HPE Propel User Accounts" on page 58 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).</p>
To Change Password	<p>Edit the \$PROPEL_HOME/idm-service/idm-service.war/WEB-INF/classes/provider-users.properties file. Update the password value of the externalLinkTransportUser property and encrypt the entire value, including the roles and the account status. (See "Encrypt a Password - HPE Propel User Accounts" on page 58 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</p>

externalLinkTransportUser User: HPE Propel Transport User, continued

	<p>no blank space at the end of the value, for example: ENC(54j5ngfki3i43A0=d).</p> <div><p>Note: This property not only contains the password, but also the roles that control access to HPE Propel and if the account is enabled.</p></div> <p>By default, the unencrypted value of this property is: externalLinkTransportUser,CONSUMER,SUPPORT,ROLE_REST,enabled</p>
--	---

Encrypt a Password - HPE Propel User Accounts

To encrypt a password for HPE Propel user accounts:

1. Log in to the HPE Propel VM as root and navigate to the `$PROPEL_HOME/cryptoUtil` directory.
2. Determine a new password for the user account: *New_Password*
3. Encrypt the password by running the following command:

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

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

```
propel, IDM_ADMIN, CATALOG_ADMIN, AGGREGATION_ADMIN, CONSUMER, SUPPORT,  
SUBSCRIPTION_ADMIN, SUPPLIER_ADMIN, ROLE_REST, 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 `orgadmin` user in the `consumer-users.properties` file.

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

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

Change the HPE Propel Master Password

HPE Propel uses a master password (or Key Encryption Key – KEK) to encrypt sensitive data, such as passwords for integration accounts and database connections. HPE recommends that you change the default master password for improved security.

The HPE 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.

The master password for individual HPE Propel applications can be changed, and not all HPE Propel applications need to have the master password changed.

The following must be done to change the HPE Propel master password:

- ["Split the HPE Propel Master Password" below](#)
- ["Update All KEK Share Files for an HPE Propel Application" on the next page](#)
- ["Update all Encrypted Values for an HPE Propel Application" on the next page](#)

Split the HPE Propel Master Password

Perform the following procedure to split the new master password:

1. On the HPE Propel VM, log in as root and navigate to the `/usr/bin` directory.
2. Run the `passwordUtil.js` command to split the new master password into three separate values:

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

3. Save the three encrypted values (KEK shares) from the output of step 2. They will be used to update the KEK share files in an HPE Propel application.

Update All KEK Share Files for an HPE Propel Application

After you split a new master password into three encrypted values, you insert the values into all of the KEK share files (KEK stores) under the parent directory of an HPE Propel application. The various HPE Propel applications have copies of these KEK stores with files named: `kekshare1`, `kekshare2`, and `kekshare3`. The following application directories under the `/opt/hp/propel` parent directory contain the `kekshare*` files: `catalog-ui`, `subscription-ui`, `idmAdmin`, `msvc`, `sxUI`, `sxClient`, `launchpad`, `autopassUI`, `portal`, `mpp`, and `diagnostics-ui`.

Important: When resetting the master password, all KEK share files in an HPE Propel application must have their KEK stores updated and sensitive data re-encrypted. However, you can reset the master password for individual HPE Propel applications, and not all applications must be done immediately. For each application:

- If a `keyfile*` file exists, delete it. The location of the `keyfile*` file is specified in the `keyfile` attribute of an application's configuration file. For example, inspect the `$PROPEL_HOME/launchpad/app.json` configuration file for the location of the Launchpad application's keyfile.
- Locate and update every KEK store file with the newly encrypted values (from splitting the master password). That is, using the first encrypted value from the master password split, update the `kekshare1` file. Update all `kekshare1`, `kekshare2`, and `kekshare3` files with the three corresponding encrypted values from the master password split. For example, locate and update all `kekshare*` files under the `/opt/hp/propel/launchpad` parent directory when splitting the master password for the Launchpad application.

Update all Encrypted Values for an HPE Propel Application

After updating all KEK share files for an HPE Propel application, all of the application's encrypted passwords must be regenerated using the `passwordUtil.js` utility. In the following example, all encrypted values for the Launchpad application are regenerated.

1. Encrypt a new value for a password with the following commands:

```
# cd /usr/bin
# ./node /opt/hp/propel/launchpad/bin/passwordUtil.js
Please enter the password to encrypt
Encrypted password is enc(4W6uYbNm6uWsaptPzjxPGQ==)
```


2. Using the encrypted value from step 1, Edit the `$PROPEL_HOME/launchpad/app.json` file and update all encrypted values for the following attributes: `idmPassword`, `passphrase`, `sessionCookieSecret`, and `connectionPassword`.

Tip: When you change the master password for an HPE 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"](#) on page 62.

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 properties with identical encrypted values.

JWT Signing Key - Update Locations

1. The `AUTHENTICATION.secretKey` JSON property in the `/opt/hp/propel/sx/WEB-INF/classes/config/infrastructure.json` file.
2. The `security.encryptedSigningKey` property in the `/opt/hp/propel/sx/WEB-INF/sx.properties` file.
3. The `idm.encryptedSigningKey` property in the `/opt/hp/propel/idm-service/idm-service.war/WEB-INF/spring/applicationContext.properties` file.

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 location (item 3), you must encrypt the value manually. (See ["Encrypt a Password - HPE Propel User Accounts" on page 58](#) for instructions on how to encrypt these values.).

Note: It is highly recommended that the signing key assigned by the HPE 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 HPE Propel for the changes to take effect. (See ["Restart HPE Propel" below](#) for information to restart HPE Propel.)

Restart HPE Propel

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

1. Log in to the HPE Propel VM as `root`, and navigate to the `$PROPEL_HOME/bin` directory.
2. Run the following commands:

```
# propel stop
```

```
# propel start
```

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Administration Guide (Propel 2.20.p2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Propel_IE@hpe.com.

We appreciate your feedback!

