Propel

Software Version: 2.20

Installation and Configuration Guide

Document Release Date: December 2016
Software Release Date: July 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

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.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Overview

HPE Propel enables IT departments to offer their services in an online shopping experience, similar to what users experience today at popular online retailers. Users may select from a variety of service providers, giving back IT a level of control over the computing environment while allowing their consumers to choose from a wide variety of sources.

This document provides information on how to install and configure HPE Propel, which includes the HPE Propel virtual machine (VM).

Audience

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

- Working with VMware ESX Server 5
- Installing OVA packages
- Deploying VMs, including configuration and administration
- Configuring VM networking
- Configuring SSL certificates
- Executing Linux operating system commands with the Bash shell
- Using a text editor, such as `vi` or `vim`, to edit files

Additional Information

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

- HPE Propel requirements: *HPE Propel System and Software Support Matrix*
- HPE Propel latest features and known issues: *HPE Propel Release Notes*
- HPE Propel system administration: *HPE Propel Administration Guide*
- HPE Propel administration-related help: *HPE Propel Admin Help*
- HPE Propel consumer-related help: *HPE Propel Consumer Help*

These guides are available from the HPE Software Support website at: https://softwaresupport.hpe.com/group/softwaresupport.

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 about using the customer support site, go to : https://softwaresupport.hpe.com/documents/10180/14684/HP_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.

Before You Begin

HPE Propel contains an OVA template that is imported into a VMware ESX server environment and instantiated as a VM.

The HPE Propel OVA template contains the HPE Propel applications, such as Shop, Services, Knowledge Management, Catalogs and Identity.

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

- Use "propel2015" as the `root` user password on the HPE Propel VM.
- Use “propel2014” as the keystore password on the HPE Propel VM.
- Default HPE Propel user accounts passwords are provided in the *HPE Propel Administration Guide*

Note: When working with an HPE Propel installation, some default passwords are the same as in prior releases. For example, the default keystore password remains as it was in the 1.xx releases. If an updated default password does not work, try the prior release password.

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

- If you are integrating HPE Service Manager (HPE SM) with HPE Propel and using HTTPS: the hostname, the `root` or administrator password, and the keystore password for the HPE SM system.
- If you are integrating HPE Cloud Service Automation (HPE CSA) with HPE Propel: the hostname, the `root` or administrator password, and the keystore password for the HPE CSA system .

Preparing Your ESX Server Environment

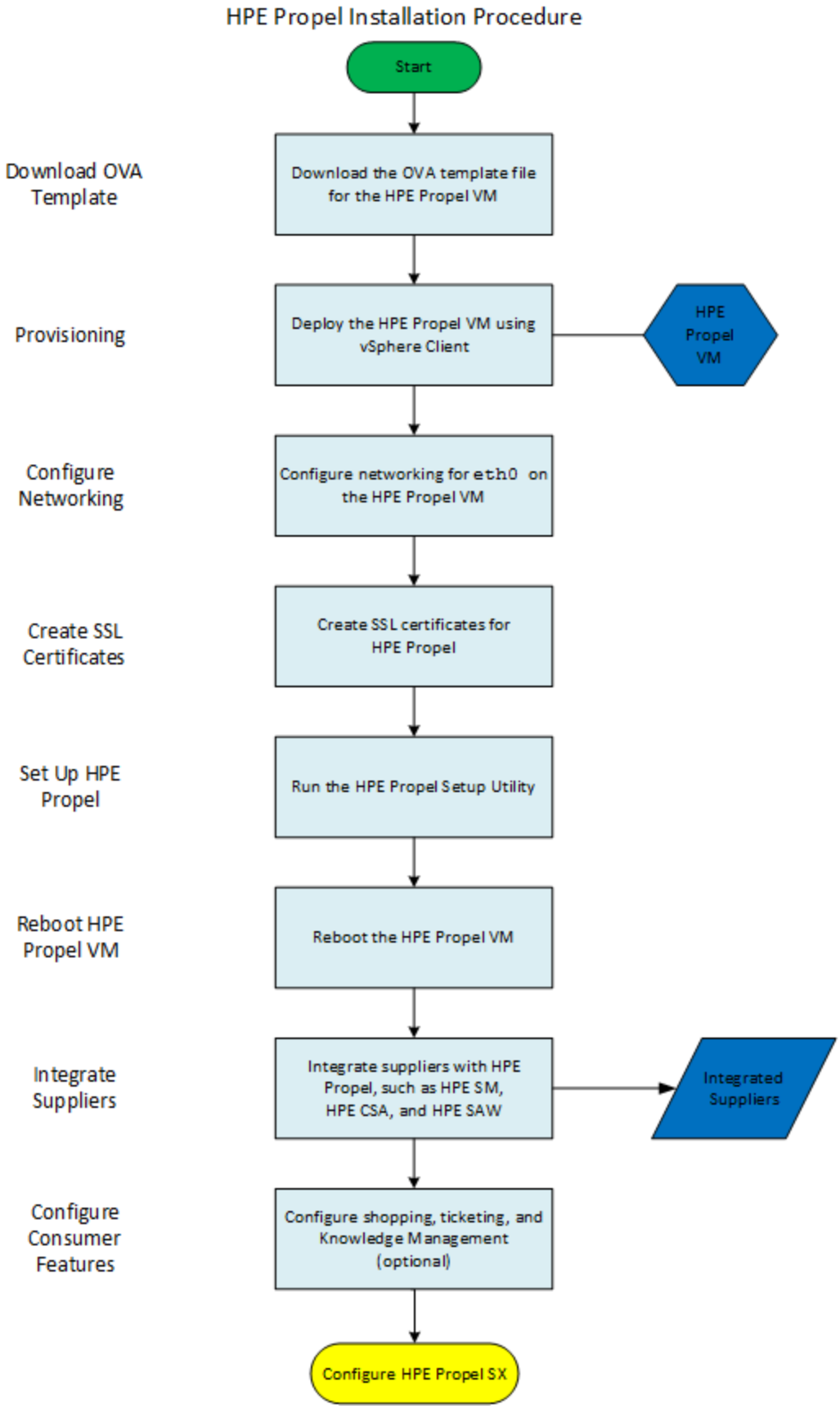
Before installing HPE Propel, you need to make sure your VMware environment has enough resources to instantiate the VM template that is included in the HPE Propel product. Refer to the *HPE Propel System and Software Support Matrix* for all HPE Propel requirements.

Installation Overview

The general procedure to install HPE Propel is:

1. From the HPE Software Support website, download the HPE Propel OVA template.
2. Using the VMware vSphere Client, deploy the HPE Propel VM into the VMware ESX environment by importing the OVA template.
3. Using the VMware vSphere Client, configure the HPE Propel VM network adapter.
4. Specify the HPE Propel VM hostname and configure networking for `eth0`. You can use the provided HPE Propel networking utility and specify either a static IP address or DHCP.
5. Create the HPE Propel Secure Socket Layer (SSL) certificates.
6. Run the HPE Propel setup tool.
7. Reboot the HPE Propel VM.
8. Integrate suppliers (such as HPE SM and HPE CSA) with HPE Propel.
9. Configure shopping, ticketing, and Knowledge Management (if required).

The following figure shows the general HPE Propel installation process.


HPE Propel Installation Procedure
Start
Download OVA Template
Download the OVA template file for the HPE Propel VM
Provisioning
Deploy the HPE Propel VM using vSphere Client
HPE Propel VM
Configure Networking
Configure networking for eth0 on the HPE Propel VM
Create SSL Certificates
Create SSL certificates for HPE Propel
Set Up HPE Propel
Run the HPE Propel Setup Utility
Reboot HPE Propel VM
Reboot the HPE Propel VM
Integrate Suppliers
Integrate suppliers with HPE Propel, such as HPE SM, HPE CSA, and HPE SAW
Integrated Suppliers
Configure Consumer Features
Configure shopping, ticketing, and Knowledge Management (optional)
Configure HPE Propel SX

HPE Propel Installation

Tip: To assist copying and pasting commands from these installation instructions into your HPE Propel virtual machine's (VM) terminal window, set the `$PROPEL_VM_HOSTNAME` environment variable to the HPE Propel VM's fully qualified hostname. For example:

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

Where *mypropel.example.com* is the fully qualified hostname that you will use for your HPE Propel VM. (This environment variable is temporary and needs to be set after rebooting the HPE Propel VM.)

Perform the following steps to install HPE Propel:

1. Download the HPE Propel OVA template file from HPE Software Support.

   Tip: To verify the GPG code signing of the OVA file, refer to the *HPE Propel Administration Guide* for details.

2. On the ESX server, use the VMware vSphere Client to deploy the OVA image into the HPE Propel VM:

   a. Click **File->Deploy OVF Template...**

   b. Select the HPE Propel OVA file that you downloaded.

   c. Specify a name and location for the HPE Propel VM and deploy.

3. After the HPE Propel VM has been deployed and is available, verify that the correct network is specified for `eth0`. In the VMware vSphere Client:

   a. Click the **Getting Started** tab, and then click **Edit virtual machine settings**.

   b. In the **Edit Settings** window, verify that the correct network is specified for **Network adapter 1**. If it is not correct, select the network configured for the ESX server.

4. Power on the HPE Propel VM.

5. In the VMware vSphere Client:

   a. Click **Actions** and then select **Open Console**.

   b. Log in to the HPE Propel VM as `root`, using "propel2015" as the password.

6. Specify the HPE Propel hostname and configure networking for `eth0` on the HPE Propel VM. You can use the `/opt/hp/propel-install/configureNetwork.sh` utility to accomplish this. In the following example, DHCP is specified; however, you can also use the `--configurestatic` option to configure a static IP address for the HPE Propel VM. When using the `--configurestatic` option, values for the netmask, gateway, domain, primary DNS server, and backup DNS server must be provided.

   Tip: Before running the `configureNetwork.sh` utility with the `--configuredhcp` option, use the `--help` option for information about whether to use the short or fully qualified hostname for the HPE Propel VM.

   ```
   # cd /opt/hp/propel-install
   # ./configureNetwork.sh --hostname $PROPEL_VM_HOSTNAME --configuredhcp
   ```

   Where `$PROPEL_VM_HOSTNAME` is the hostname you specify for the HPE Propel VM.

   Important: The hostname of the HPE Propel VM must contain only valid characters under DNS. Characters such as the underscore character ("_"), which are used in resolution algorithms, and mixed-case hostnames cannot be used. For more information, refer to RFC 1178 and RFC 2872.

   Reply "Y" to the prompt to configure networking and the prompt to reboot the VM.

7. Verify that you have a configured IP address on `eth0` for the HPE Propel VM. You can accomplish this with the `nslookup` and `ifconfig` commands.

   Note: If either of the following conditions exist, take corrective action to resolve the problem:

   - If the HPE Propel VM does not have a configured IP address.
   - If the IP address listed by the `ifconfig` command does not match the IP address listed by the `nslookup` command.

8. On the HPE Propel VM, log in as `root` and navigate to the `/opt/hp/propel-install` directory, and then create the HPE Propel-generated SSL certificates:

   Important Third-party or corporate CA-signed certificates should be used in production systems; however, self-signed certificates generated by HPE Propel can be used in non-production systems.

```
# cd /opt/hp/propel-install
# ./propel-ssl-setup.sh auto --hostname $PROPEL_VM_HOSTNAME [<CA_SUBJECT>] 2>&1
| tee ssl-setup.log
```

Where `$PROPEL_VM_HOSTNAME` is the fully qualified HPE Propel VM hostname and *CA_SUBJECT* is the optional CA subject. By default the string "`/CN=Generated Propel CA`" is used. If you specify the *CA_SUBJECT* option:

- The "`CN`" field must be present and in uppercase. The value for "`CN`" can be any string.
- This is the subject of your private HPE Propel CA, not your HPE Propel VM; it is not used for the hostname.
- All fields must be separated with a slash ("/").

9. Run the HPE Propel setup utility:

```
# ./setup.sh install $PROPEL_VM_HOSTNAME 2>&1 | tee install.log
```

Where `$PROPEL_VM_HOSTNAME` is the fully qualified hostname you specify for the HPE Propel VM. The output and any errors from the `setup.sh` utility are captured in the `install.log` file .

10. Reboot the HPE Propel VM:

```
# reboot
```

Congratulations, you have successfully installed HPE Propel. After the HPE Propel VM completes the reboot, you can now log in to HPE Propel by opening a browser window and entering any of the following URLs for the three HPE Propel roles:

- HPE Propel Administrator: `https://$PROPEL_VM_HOSTNAME:9000/org/Provider`
  (Use "admin" as the user and "propel" as the password.)
- Organization Administrator: `https://$PROPEL_VM_HOSTNAME:9000/org/CONSUMER`
  (Use "orgadmin" as the user and "propel" as the password.)
- Consumer: `https://$PROPEL_VM_HOSTNAME:9000/org/CONSUMER`
  (Use "consumer" as the user and "propel" as the password.)

Tip: If the HPE Propel installation is unsuccessful and you need to repeat the installation, use the `/opt/hp/propel-install/setup.sh purge` command to remove the installed HPE Propel software, including the Postgres databases. After re-installation, some HPE Propel files are owned by the initial Linux `propel`user and need to be modified so that they are owned by the new `propel`user. Notice that the purge command does not work with distributed Propel.

Continue with "Next Steps" on page 14 to begin the HPE Propel configuration for your specific environment.

Next Steps

Tip: To prevent errors in HPE Propel log files that are related to unknown users, HPE recommends that all integrated end-point systems 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.

After you have successfully installed HPE Propel, the next step is to integrate suppliers, which are end-point systems such as HPE Service Manager (HPE SM) and HPE Cloud Service Automation (HPE CSA).

Integrate Suppliers with HPE Propel

Suppliers represent end-point systems that are integrated with HPE Propel. Examples of suppliers are: provider systems, fulfillment systems, and ticketing systems.

Suppliers are associated with organizations, and the Organization Administrator manages the supplier systems for his organization.

The Organization Administrator can create new suppliers in HPE Propel. To create a new supplier:

1. Log in to the HPE Propel Launchpad as the `orgadmin` user by opening a browser and specifying the following URL:

   `https://<PROPEL_VM_HOSTNAME>:9000/org/CONSUMER`

   Where *PROPEL_VM_HOSTNAME* is the fully qualified hostname of the HPE Propel VM.
2. From the Launchpad in HPE Propel, click the **Suppliers** application.
3. In the **Suppliers** view, click **Add Supplier**.
4. In the **Add Supplier** dialog, fill in and select the **Basic Supplier Properties**:
   a. Type the **Name** of the new supplier.
   b. Select the **Backend System Type**.
5. After the **Backend System Type** is selected, additional **General** fields are displayed, such as integration account credentials and end-point URLs. Fill in and select the required **General** fields.
6. Click **Create** in the **Add Supplier** dialog to finish and save your changes. The new supplier and its properties are displayed.

7. *Optional, only for HPE SM suppliers* - if an HPE SM supplier has been added and LWSSO has been specified, see "Setting up HPE SX to use LWSSO" on page 31 for instructions.
8. Validate connectivity between HPE Propel and the supplier. Run the HPE Propel **Diagnostics** application to verify the supplier is configured and connected correctly. See "Verify HPE SX Configuration" for details.

Important: If HTTPS is used for communication between HPE Propel and the new supplier, then HTTPS must be configured. See "Configure SSL for a Supplier" on page 90 for instructions.

Configure Shopping, Ticketing, KM, and Hot News

After you have successfully installed HPE Propel and added suppliers, the next steps are to configure shopping, ticketing, knowledge management, and Hot News, depending on the needs of the consumers using the HPE Propel Portal.

- **Shopping** – To configure shopping for HPE Propel, the following needs to be completed:
  a. *Create an aggregation*. Offerings from end-point systems are initially imported into an HPE Propel aggregation. For instructions to create an aggregation, refer to the *HPE Propel Catalog Connect Help*.
  b. *Create a new catalog*. Offerings from end-point systems are contained in HPE Propel catalogs as catalog items. For instructions to create a catalog and configure which users can access the catalog, refer to the *HPE Propel Catalogs Help*.
  c. *Publish catalog items*. Catalog items must be published in an HPE Propel catalog for consumer fulfillment. For instructions to publish catalog items in catalogs, refer to the *HPE Propel Catalog Items Help*.
- **Ticketing** – The HPE Propel ticketing features are available after a successful installation has been completed.
- **Knowledge Management** – If you have Knowledge Management documents that you need to load into HPE SM, refer to the *HPE Propel Administration Guide* for instructions.
- **Hot News** – To configure RSS feeds in the HPE Propel Hot News application, refer to the *HPE Propel Administration Guide* for instructions.

Caution: The default passwords for the `consumer`, `orgadmin`, and `admin` users are listed in this guide. To prevent access to your HPE Propel installation via these default passwords, they must be changed. Refer to the *HPE Propel Administration Guide* for instructions.

Important: HPE Service Exchange (HPE SX) must be configured. Continue to "HPE SX Configuration after VM install" on page 17.

HPE SX Configuration after VM install

HPE Service Exchange (HPE SX) is the component that brings the HPE Propel experience together, integrating the portal, catalog, and end-point fulfillment engines to enable functional integration with multiple providers. HPE SX features built-in content that exchanges service messages and orchestrates and dramatically simplifies the integration of new and existing products, services and solutions.

To run the complex tasks it is capable of, HPE SX needs some configuration. This involves some or all of the following, depending on the integrations with your HPE Propel installation:

- Examine and edit the two configuration files that HPE SX needs in order to run correctly, see "HPE SX Basic configuration" for details.
- Add any additional HPE CSA and HPE SM instances you wish connected to HPE Propel, see "Adding additional HPE CSA instances " and "Adding additional HPE SM instances".
- Add any HPE SAW instances you wish connected to HPE Propel, see "Connecting HPE SAW to HPE SX".
- Set HPE SX user roles and organizations to allow viewing of HPE SX management and Testing UIs "Setting User roles and Organizations".
- Run the HPE Propel **Diagnostics** application to verify that components are configured and connected correctly. It alerts administrators to any problems connecting to essential components, or with out-dated versions of customized files. **Diagnostics** is located on the HPE Propel Launchpad. See "Verify HPE SX Configuration" for details.
- If you are using HPE CSA, check through "Connecting HPE CSA to HPE SX" for any necessary LDAP and Approval configuration required.
- If you are using HPE SM, check for further configuration steps required both in your HPE SM instance and in HPE SX. See "Connecting HPE SM to HPE SX" for details.
- If you want to enable Case Exchange (CX) functionality see "Configuring Case Exchange".
- View and manage HPE SX content packs ("HPE SX Content Management") and adapters ("HPE SX Adapters").

Note: Throughout this guide, `[%SX_HOME%]` is used as a shortcut for the path: `/opt/hp/propel/sx`

HPE SX Basic configuration

There are a few basic configuration files that HPE SX needs in order to start and run correctly:

- "infrastructure.json"
- "sx.properties"

infrastructure.json

This file is located on a classpath in the `[%SX_HOME%]/WEB-INF/classes/config` directory. It contains information about HPE SX components like RabbitMQ and OO.

```
{
    "OO": { // Operation Orchestration connection information
        "endpoint": "http://localhost:8080/oo/rest",
        "loginName": "admin",
        "password": "changeit"
    },
    "JMS_BROKER": {
        "endpoint": "localhost",
        "loginName": "rabbit_sx",
        "password": "propel2014"
    },
    "REST": {
        "endpoint": "http://${env.HOSTNAME}:8080/sx/api/request",
        "operationEndpoint": "http://${env.HOSTNAME}:8080/sx/api/operation",
        "bundleCallbackEndpoint": "http://${env.HOSTNAME}:8080/sx/api/bundle",
        "csaNotificationEndpoint": "http://${env.HOSTNAME}:8080/sx/api/csa",
        "emailCallbackEndpoint": "http://${env.HOSTNAME}:8080/sx/api/email"
    },
    "SERVICE_CATALOG": {
        "catalogApprovalPageLink": "http://localhost:8080/sx/notifications.jsp",
```

```
        "requestCallbackEndpoint": "",
        "subscriptionCallbackEndpoint": "",
        "internalCallbackEndpoint": "http://localhost:8080/sx/api/catalog"
  },
    "AUTHENTICATION": {
        "secretKey": "propel"
    }
}
```

sx.properties

The `sx.properties` file is located in the `[%SX_HOME%]/WEB-INF` directory and contains configuration for the HPE SX web application.

```
catalog.notificationMaxEntries=50
catalog.notificationUser=sxCatalogTransportUser
catalog.notificationUserOrganization=Provider
catalog.notificationUserPassword=ENC(B/vX8k7pZkln2VxV2HaDiPesUUkF0hc3ZVLIAtGzG28\=)
db.dialect=org.hibernate.dialect.PostgreSQLDialect
db.driverClassName=org.postgresql.Driver
db.maxConnections=16
db.password=ENC(4w0oS736xObjhMmJTCq87Q\=\=)
db.url=jdbc\:postgresql\://localhost\:5432/sx
db.username=sxuser
diagnostics.transportUser=diagnosticsTransportUser
diagnostics.transportUserPassword=ENC
(aBT5iNIuAhermpyFtg+zdKj5FT1US6sbbgOo6t6Gil/y2fvnw14L5g\=\=)
security.encryptedSigningKey=propel
security.idmHostname=mpavmcsa05.hpswlabs.adapps.hp.com
security.idmPath=idm-service
security.idmPort=9600
security.idmProtocol=https
security.idmTenant=Provider
security.idmTransportUser=idmTransportUser
```

```
security.idmTransportUserPassword=ENC
(8ZHTqNTKpZn4+lbfFnkrPrRebZeUUu99yCXkT6N4DHQ\=)

security.returnUrl=${sx.url}

skipCertificateValidation=false

sx.catalog.notifications.queue=CN

sx.catalogPollingPeriodSeconds=10

sx.content.oo.delete=true

sx.content.oo.init=checkVersion

sx.content.oo.upload=always

sx.cx.backendEntityLockExpirationSeconds=300

sx.cx.lockExpirationSeconds=300

sx.disableCatalogPolling=false

sx.dlx.delay.queue=DELAY

sx.dlx.exchange=sx.dlx

sx.dlx.fail.queue=FAIL

sx.dlx.redelivery.interval.ms=30000

sx.dlx.redelivery.max.count=5

sx.dlx.retry.queue=RETRY

sx.http.connectionTimeout = 600000

sx.maxConcurrentConnectionPerSeparatedPool=2

sx.maxSeparatedPoolTotal=500

sx.mock.requests.queue=MOCK

sx.oo.callback.queue=OC

sx.oo.configuration=oo/properties

sx.oo.invocations.queue=OO

sx.organizationCache=300

sx.queue.main=SX

sx.queue.prefix=${PROPEL_HOSTNAME}

sx.queue.selftest=SELFTEST

sx.removeExistingSmChangesOnBoot=false

sx.serviceInstance.disableOnboarding=true

sx.storage.location=/datastorage
```

```
sx.sync.delay.queue=SYNC_DELAY

sx.sync.queue=SYNC

sx.sync.redelivery.interval.ms=5000

sx.ticket.disableOnboarding=false

sx.ticket.disableSmPolling=false

sx.url=https\://${PROPEL_HOSTNAME}\:9444/sx
```

Parameters for HPE SX internal database configuration

Property name	Description
db.dialect	Configuration of db connection. Dialect for HPE SX db. Possible values are `http://docs.jboss.org/hibernate/orm/3.5/javadocs/org/hibernate/dialect/package-summary.html`
db.driverClassName	Configuration of db connection. JDBC driver class name.
db.password	DB password in plain text.
db.url	JDBC db url. Key for IDM token validation.
db.username	Username of DB user.

Parameters for HPE SX security configuration

Property name	Description
security.encryptedSigningKey	It will be encrypted at first start of HPE SX.
security.idmHostname	Hostname part of IDM url.
security.idmPort	Port part of IDM url.
security.idmProtocol	Protocol part of IDM url.
security.idmTenant	Tenant user wants to log in.
security.idmTransportUser	Username of integration accout for communicating with IDM.
security.idmTransportUserPassword	Password in plain text of integration account. It will be encrypted once HPE SX starts.
skipCertificateValidation	Whether HPE SX should validate SSL certificates.

Parameters for HPE SX internal configuration

Property name	Description
sx.catalog.notifications.queue	Name of RabbitMQ queue for notifications.
sx.content.oo.delete	Tells if content management should delete content pack from OO during HPE SX content pack deletion. Values are true or false.
sx.content.oo.init	Defines strategy of checking if content packs in OO are up to date during HPE SX start. • checkName - check if content pack with given name is already uploaded, no version check, if content pack with given name is not uploaded it uploads. • checkVersion - check for latest version, if OO contains obsolete or no version it uploads. • always - always upload new content pack. • never - never upload.
sx.content.oo.upload	Defines strategy of checking if content packs are up to date in OO during HPE SX content pack upload. Possible values are same as for `sx.content.oo.init`.
sx.dlx.delay.queue	See DLX Queues.XXXX
sx.dlx.exchange	Name of dlx exchange. See DLX Queues.XXXX
sx.dlx.fail.queue	See DLX QueuesXXXX.
sx.dlx.redelivery.interval.ms	Time after that will be failing message redelivered to HPE SX. In ms.
sx.dlx.redelivery.max.count	Maximum count of retries.
sx.dlx.retry.queue	See DLX QueuesXXXX
sx.http.connectionTimeout	Connection timeout for HTTP connections. In ms.
sx.oo.configuration	Path to file with OO configuration.
sx.queue.prefix	Prefix that will be used in all queue names. Can be used for separation of multiple HPE SX instances so that they use their own queues.
sx.queue.main	Main HPE SX RabbitMQ queue.
sx.url	HPE SX URL.
sx.ticketing.maxAttachmentSize	Maximum size for ticket attachments.
sx.ticketing.forbidAttachmentExtensions	Comma separated list of forbidden file extensions for ticket attachements.

Verify HPE SX Configuration

Use the HPE Propel **Diagnostics** application to view the health status of HPE SX.

To use the **Diagnostics** application, log in to HPE Propel as the `admin` user (`https://$PROPEL_VM_HOSTNAME:9000/org/Provider`), then click the **Diagnostics** application.

Refer to the **Diagnostics** help for details.

For HPE SM instances, **Diagnostics** also checks versions of all installed unload files and lists them. In **Diagnostics**, click **Configuration Check** in the **Supplier Detail** view for an HPE SM instance.

Connecting HPE CSA to HPE SX

Adding additional HPE CSA instances

Additional HPE CSA instances are added as suppliers in the HPE Propel **Suppliers** application. See the *Integrate Suppliers with HPE Propel* instructions in "Next Steps" on page 14.

Important: When adding an HPE CSA supplier, HTTPS communication between HPE Propel and the HPE CSA supplier must be configured. See "Configure SSL for a Supplier" on page 90 for instructions.

LDAP and Approval settings

For HPE CSA to integrate with HPE SX, LDAP and Approval settings need to be configured. If these are already set, further action is not required. If not, see:

- "Configure HPE CSA to use LDAP" on page 27
- "Configure HPE CSA Approval settings" on page 28

Configure HPE CSA to use LDAP

1. Log in to HPE CSA.
2. Select **Organizations**.
3. Select **HP CSA Consumer**.
4. Select the **LDAP** section.
5. Fill in your LDAP server information and click **Save**.
6. Select the **Access Control** section.
7. Click **Add On**.
8. Fill in the AC Config and click **Update**.

Configure HPE CSA Approval settings

1. Log in to HPE CSA.
2. Select **Catalogs**.
3. Create a new catalog.
4. Go to the **Approval Policies** section of the new catalog.
5. Fill in **Name**, select a **Template** (for example, Named Approver Template) and add **Approver**.
6. Save the policy.

Connecting HPE SM to HPE SX

Setting up HPE SX to work with HPE SM

Adding additional HPE SM instances

Additional HPE SM instances are added as suppliers in the HPE Propel **Suppliers** application. See the *Integrate Suppliers with HPE Propel* instructions in "Next Steps" on page 14.

Important: When adding an HPE SM supplier, if you are using HTTPS communication between HPE Propel and the HPE SM supplier, HTTPS must be configured. See "Configure SSL for a Supplier" on page 90 for instructions.

Setting up HPE SX to use LWSSO

If an HPE SM supplier has been added to HPE Propel and LWSSO has been specified, to enable the LWSSO communication, the `/opt/hp/propel/sx/WEB-INF/classes/config/lwssofmconf.xml` file must contain the proper LWSSO configuration that matches the target HPE SM instance.

To configure HPE Propel to use LWSSO, the following must be done:

1. On the target HPE SM instance, inspect the `<SM_SERVER_INSTALL_PATH>/RUN/lwssofmconf.xml` file and obtain the domain value from the `domain` element.
2. On the HPE Propel VM, edit the `/opt/hp/propel/sx/WEB-INF/classes/config/lwssofmconf.xml` file and make the following revisions:
   a. The `domain` element must contain the domain of the HPE SM instance, which was obtained in step 1.
   b. The `initString` attribute of the `crypto` element must contain the same passphrase as the HPE SM instance.
3. On the HPE Propel VM, restart HPE SX:

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

Configure for ticketing

Users of a particular organization are only able to manage tickets on systems configured for that organization.

For ticketing REST API to use a certain instance, edits need to be made to the following file:

`[%SX_HOME%]/WEB-INF/classes/config/tenantInstanceMappings.json`

In `tenantInstanceMappings.json`:

- The `backendSystemType` and `instanceName` field values have to be set in the file for each organization.
- The DEFAULT values need to be added for all users whose organization is not specifically defined elsewhere in the file.

Example:

```
{
    <ORGANIZATION_NAME>: {
        "backendSystemType": "SM",
        "instanceName": "SMInstance1"
    },
    "DEFAULT": {
        "backendSystemType":"SM",
        "instanceName":"SMInstance2"
    }
}
```

In this example, SMInstance1 and SMInstance2 need to be the unique names previously defined in `instances.json`, and used for identifying these HPE SM instances in other configuration files.

Configure Case Exchange

To set up Case Exchange functionality, there are a number of configuration steps necessary.

See "Configure HPE SX" on page 72 for further details.

Setting up HPE SM to work with HPE SX

HPE SX requires the HPE SM instances to have specific customizations applied in order to enable HPE SX functionality.

Import HPE SX Unload scripts

Necessary customizations of HPE SM are performed by HPE SM unload files. To import unload files into HPE SM:

1. In your HPE SM instance, go to **System Administration > Ongoing Maintenance > Unload Manager > Apply Unload**.
2. Select the **Unload File**: e.g. {*path-to-unload-file*}
3. Select **Backup To**: e.g. {*path-to-unload-file*}.backup
4. Click **Next**.

If there is a conflict with an entry, double-click that entry to see details, and look at "Manual configuration for Case Exchange" on page 38 to understand what customizations each HPE SM unload pack contains. Consider checking all the changes made by the unload scripts to verify your HPE SM configuration is correct.

HPE SX Unload files

The following unload files contain fundamental HPE SM customizations that are needed for HPE SX to integrate with your HPE SM instance.

SXBaseDB.unl

Description: The triggers in the following entities:

- **cm3r (changes)**
- **subscription**
  - SX.subscription.delete
- **incidents**
  - SX.incidents.after.add
  - SX.incidents.after.update
  - SX.incidents.after.delete

Use the included scripts:

- SX_EntityChangeV2
- SX_SubscriptionDelete

To write the triggered changes into the next tables (newly created):

- SxEntityChangesV2
- SxRegisteredEntitiesV2

SXBaseExtAccess.unl

Description: Provides remote interfaces (SOAP/REST) for the following tables:

- Change detection (see SXBaseDB.unl) - SxEntityChanges (read changes from SxEntityChangesV2 table), SxRegisteredEntities (write into SxRegisteredEntitiesV2 table when it's necessary to be informed about changes in HPE SM. These are then written into the SxEntityChangesV2 table.)
- Other functionality that is shared for Quotes, Changes, and Ticketing features - for example, providing remote access to the following HPE SM objects for HPE SX: Relation (screlation),

Cart Item (svcCartItem), Interaction (incidents), svcCatalog, Approval, operator, and Attachment (SYSATTACHMENTS).

SXUnloadChecker.unl

Description: Provide remote interface (REST) to the table of applied unloads.

SXCaseExchange.unl

Description: Changes for Case Exchange feature support: adding REST endpoints and table triggers.

- Adds new REST endpoint SX/SXCE_Incident - providing remote access to probsummary HPE SM object for HPE SX.
- Adds new REST endpoint SX/SXCE_IncidentActivity - providing remote access to activity HPE SM object for HPE SX.
- Adds triggers for tables:
    - **probsummary** - writes **Incident** changes into SxEntityChangesV2 table. (See SXBaseDB.unl.)
    - **activity** - writes **Activity** changes into SxEntityChangesV2 table. (See SXBaseDB.unl.)
    - **SYSATTACHMENTS** - writes **Attachment** changes into SxEntityChangesV2 table. (See SXBaseDB.unl.)

SXExtRefTable.unl

Description Adds ExternalReferences table for Case Exchange integration. Necessary only in HPE SM 9.33 and older. For newer versions of HPE SM, the table is present out of the box.

SXPDCaseExchange.unl

Description: Triggers and APIs Task supporting Task case exchange use case. This unload script is intended exclusively for HPE SM with Process Designer. Note that both this file and `SXCaseExchange.unl` are mandatory for HPE SM with Process Designer.

Apply general unloads

Apply the following general unload files. Their locations are relative to the `/opt/hp/propel/sx/contentStorage` path:

- `./sx-base/sm/SXBaseCustomizations.unl`
- `./sx-base/sm/SXBaseDB.unl`
- `./sx-base/sm/SXEntityChangesV2.unl`
- `./sx-base/sm/SXBaseExtAccess.unl`
- `./sx-base/sm/SXUnloadChecker.unl`

- `./case-exchange/sm/SXExtRefTable.unl` – **Only for HPE SM 9.33 and older**
- `./case-exchange/sm/SXCaseExchange.unl`
- `./case-exchange/sm/SXPDCaseExchange.unl` – **Only for HPE SM with Process Designer**

Apply the following Knowledge Management unload files. Their locations are relative to the `/opt/hp/propel` path:

- `./km/webservices/HPPropelKnowledgeAttachment.unl`
- `./km/webservices/HPPropelKnowledge.unl`

Manual configuration for Case Exchange

Add **Add** activity privileges to the user account HPE SX will use:

1. Go to **Tailoring > Format Control**.
   a. In the **Name** field add the string `activity` and click **Search**. The activity unload file contents will load.
   b. Open the tab (click the button) **Privileges**.
2. Change "false" to "true" for operation **Add**.
3. Click **Save**.

HPE SM Process Designer - additional manual configuration

Configuration for Ticketing (for HPE SM with Process Designer only)

Remove the `$G.ess=true` line from the Expressions tab of SXTicketInteraction Web Service:

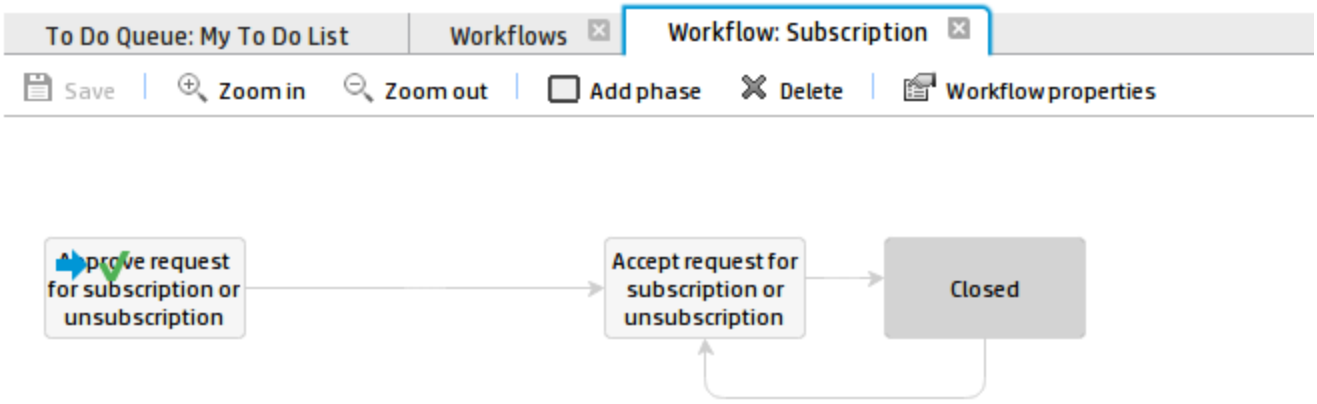
1. Go to **Tailoring > Web Services > Web Service Configuration**
   a. In the **Object Name** field add the string "SXTicketInteraction" and click **Search**. The SXTicketInteraction settings will load.
   b. Open the tab (click the button) **Expressions**.
2. Remove the string `$G.ess=true`.
3. Click **Save**.

Configuration for Change R2F (for HPE SM with Process Designer only)

1. Log in to your web client.
2. Go to **Change Management > Configuration > Change Workflows**.
3. Select **Subscription** from the list.
4. Remove the second phase from the diagram.
5. Connect the first and third phases by relation.
6. Click to the new relation.
7. Fill the Command Name with "nextphase".

NOTE: Be careful not to remove anything beyond this.

The result of this step should look like this:


To Do Queue: My To Do List
Workflows
Workflow: Subscription
Save
Zoom in
Zoom out
Add phase
Delete
Workflow properties
Approve request for subscription or unsubscription
Accept request for subscription or unsubscription
Closed

Apply R2F unload scripts

Apply the following request-to-fulfillment (R2F) unload scripts. Their locations are relative to the `/opt/hp/propel/sx/contentStorage` path:

- `./sm-r2f/sm/SXLineItemApproval940.unl` – **Only for HPE SM 9.40**
- `./sm-r2f/sm/SXR2FExtAccess.unl` – also contains Aggregation web services
- `./sm-r2f/sm/SXR2F940ExtAccess.unl` – **Only for HPE SM 9.40**
- `./sm-r2f/sm/SXR2FDB.unl`
- `./sm-r2f/sm/SXLineItemApproval.unl`
- `./sm-r2f/sm/SXR2FCustomizations.unl`

Manual configuration

1. **Customize the approval process/lifecycle of Quotes.**
    a. Go to **Request Management > Quotes > Quote Categories**, click **Search** and select the **Customer** record.
    b. Click the first phase box (**Front Line Management Approval**) and remove 'Financial Approval' on the **Approvals** tab. Click **OK**. If the tab "Select Event For New Phase" opens, click the **Back** button.
    c. Click the last phase (**Customer Approves Delivery of Item**) and remove 'Manager Approval' on the **Approvals** tab. Click **OK**. If the tab "Select Event For New Phase" opens, click the **Back** button.
2. **Rebuild the "Extaccess Actions" Global List.**

    Note: Use the HPE SM client directly.

    a. Go to **System Definition > Tables > globallist** and open it.
    b. Click **View all records in the table**.
    c. Select the line **Extaccess Actions**.
    d. Right click anywhere in the bottom part of the screen (the Item View panel), and select **Rebuild Global List**.
    e. Click **Save**.
3. **Modify the DEFAULT profile.**

Note: This step will not work if you have Process Designer installed.

a. Go to **System Administration > Ongoing Maintenance > Profiles > Service Desk Profiles** (Request Management Profiles on SM with PD.)

b. Click **Search** and select the **DEFAULT** profile.

c. Check the **Close** check-box.

d. Click **Save**.

Manual configuration - Approvals

NOTE: The following configuration is **not needed** if the HPE SM instance is accessed via LWSSO.

Modify Change and Request profiles used by your Approvers

1. Log in as Admin.
2. Go to **System Administration > Ongoing Maintenanace > Operators**.
3. Enter the login name and click **Search**.
4. Click the magnifying glass icon beside **Change Profile**.
5. Select the **Approvals/Groups** tab.
6. Check **Can Delegate Approvals**.
7. Click **OK**.
8. Click the magnifying glass icon beside **Request Profile**.
9. Change to **Alert/Approval** tab.
10. Check **Delegate Approvals**.
11. Click **OK**.
12. Select the **Startup** tab.
13. Change the parameter values in the first table in this way:
    1. name = MAIN MENU
    2. prompt =
    3. string1 = HOME
14. Click **OK**.

Delegate Change approving

NOTE: This step is only necessary if you have Process Designer installed.

1. Go to **System Administration > Operators**.
2. Fill **Login Name**: as "joe.manager", and click **Search**.
3. Add the "change approver" **Security Role** to joe.manager.

4. Click **Save**.
5. Go to **System Administration > Security > Roles**.
6. Select the change approver and click **Search**
7. Click the **Change** row.
8. Check **Can Delegate Approvals** under **Settings**.
9. Click **Save**.

Setup approval delegation for each Approver

1. Log in as the Approver.
2. Go to **Miscellaneous > Approval Delegation**.
3. Click **Add New Delegation**.
4. Select **Delegate Selected Approvals**.
5. Click **Next**.
6. Select the module **Request Management**.
7. Click **Next**.
8. Move "jane.doe" to the right column.
9. Click **Next**.
10. Delegate to: johndoe. Fill in the Start and End dates.
11. Click **Next**.
12. Click **Finish**.
13. Repeat for the the **Change Management** module.

Manual configuration for Ticketing

NOTE: This is only necessary for Process Designer-enabled HPE SM.

1. Log in as Admin.
2. Go to **Tailoring > Tailoring Tools > Display Options**.
3. Enter `db.view_add` into the **Unique ID** field.
4. Change the condition from

   ```
   evaluate(add in $L.env) and filename($L.filed)~="dbdict" and
   nullsub($L.io.cond.flag, true)
   ```

   to

   ```
   (evaluate(add in $L.env) or evaluate(new in $L.env)) and
   filename($L.filed)~="dbdict" and nullsub($L.io.cond.flag, true)
   ```
5. Click **Save**.

Import Certificates

On the HPE Propel VM

1. Download the HPE SM certificate, for example by using the following command:

   ```
   openssl s_client -connect <SM-HOST>:8443 </dev/null | sed -ne '/-BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p' >sm.crt
   ```

2. ```
   keytool -importcert -file sm.crt -keystore
   /opt/hp/propel/security/propel.truststore -alias sm_host
   ```

3. Enter the password *propel2014*.

4. Enter *yes*.

Setup LDAP

When LDAP has been configured in HPE SM:

1. Identify the operator template used, by:
   - Go to **System Administration > Base System Configuration > Miscellaneous > System Information Record**, and note the **Operator Template** field. Follow this method if you used the second approach from the *LDAP Configuration Guide*.
   - Otherwise, go to **System Administration > Ongoing Maintenance > Operators** and search for the operator template, for example in LDAP.template or Operator.General

   If there is a value for **Contact ID**, remove it.

2. For non-Process Designer installations: add **Change manager** to the **Change Profiles**.
   For Process Designer-enabled installations: add **Change manager** to the **Security Roles**.

3. Switch to the **Startup** tab.

4. Into **Execute Capabilities** add **SOAP API** and **RESTful API**.

5. Click **Save**.

Temporarily, for every LDAP user perform the following:

1. Log in to HPE SM.

2. Log out.

3. Log in as Admin.

4. Go to **System Administration > Ongoing Maintenance > Operators** and find your user.
   ```

5. Click **Create Contact**.
6. Select a contact to clone.
7. Click **Finish**.

Create and apply new unload files

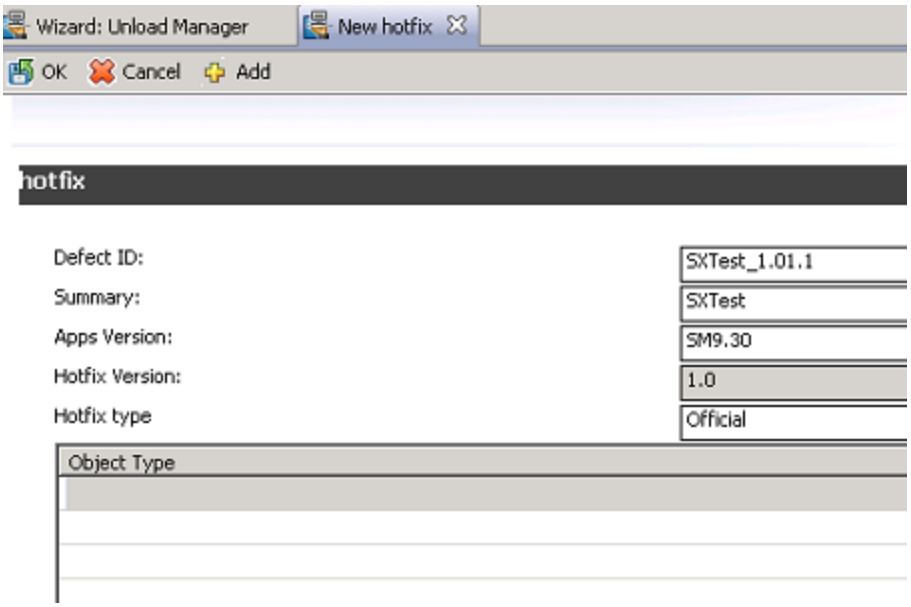
To enable HPE SX to communicate with your HPE SM instance, you may need to customize the out-of-the-box unload files, or create new ones.

If you develop your own HPE SX content and make modifications to your HPE SM instance, you will need to export these modifications into your own new unload file, or create a new version of an unload file. Using unload files enables you to backup changes and transfer them to other HPE SM instances.

Note: After creating a new unload file, run **Diagnostics** to check that you have all the latest versions of files installed, see "Using Diagnostics to check unload files" on page 51.

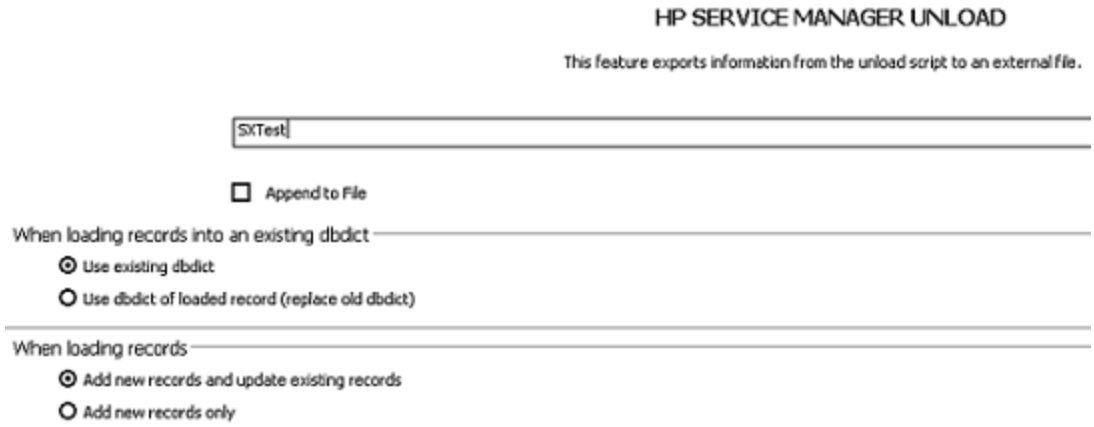
Creating unloads in HPE SM Unload manager

1. In **System Administration > Ongoing maintenance > Unload manager** select **Create Unload**.
   - **Defect ID** - Use this field to hold the version of the unload file. Versions must be unique and follow this format: <*unl_file_name*>_<*version*>. For example: *SXBaseCustomizations_1.01.1*.
   - **Summary** - Enter a name for the unload file, without file extension.
   - **Apps version** and **Hotfix type** are not currently used. *SM9.30* and *Official* are chosen in the example below.



NOTE: the unload object does not need to be in the unload when using Unload manager.

2. Click **Add**.
3. The unload is created. The next step is to export it into a file. Click **Proceed**.
4. Export the unload to a file with the same value as entered in **Summary**.



5. Click **Proceed** and your new unload file is complete.

Apply unload in HPE SM Unload manager

In **System Administration > Ongoing maintenance > Unload manager** select **Apply Unload** and follow the wizard instructions. After you finish you will see your unload with its version under **View Unload**.

Note: The table of applied unloads under **View Unload** is not updated automatically. Close and then reopen Unload manager to view your new unload.

Creating and updating version numbers

After implementing a change you may want to create a new version number for your unload.

To do so:

1. Double click your unload in **Unload manager > View Unload**.
2. Increment the version in the **Defect ID** field.
3. Export the unload into a file, see Step 4 above.
4. Apply the unload, see "Apply general unloads" on page 37.

Using Diagnostics to check unload files

As well as checking for correct connections and configurations, HPE Propel **Diagnostics** checks unload files for an HPE SM instance and lists their status. For this to happen, `SXUnloadChecker.unl` must be applied, and `metadata.json` edited to include all current unload file versions.

Before using **Diagnostics** to check versions:

1. Apply `SXUnloadChecker.unl` to your HPE SM instance.
2. Edit your `metadata.json` file, specifying any new unload files, and any new version numbers of unload files.

   For example:

```
{
    "id": "sx-base"
    "name": "Service Exchange base content",
    "description": "",
    "version": "1.0.0",
    "adapter": "SX",
    "features": [
    ],

    "files": [
        {
            "path": "sm/SXBaseDB.unl",
            "version": "1.01.1",
            "type": "sm_unload"
        },

        {
            "path": "sm/SXBaseExtAccess.unl",
            "version": "1.01.1",
            "type": "sm_unload"
        }

    ]

}
```

3. View **Configuration Check** in the **Diagnostics** application:
   a. Log in to HPE Propel as the `admin` user (`https://$PROPEL_VM_HOSTNAME:9000/org/Provider`), then click the **Diagnostics** application.
   b. Click **Suppliers**, and then click the circle that represents the HPE SM instance.
   c. Click **Configuration Check**.

The unload files and their status are listed.

Connecting HPE SAW to HPE SX

This topic describes the steps required to have an HPE SAW instance participate in HPE SX Case Exchange.

NOTE: Any HPE SAW instance to be integrated into HPE Propel needs to be added to the

`[%SX_HOME%]/WEB-INF/classes/config/saw/instances.json` file.

The settings required are outlined in the **instances.json** section of "HPE SX Basic configuration".

HPE SAW Setup for Case Exchange

First it is necessary to add a definition of an External System into HPE SAW. The name of this External System is the name that will be used to identify the HPE SAW system in the necessary HPE SX CX configuration (`external-systems.json`). Second, the defined External System must be added to a Group that has the integration account assigned as the Authorized user.

Follow these steps:

1. In the HPE SAW UI, from the **Administration** menu select **Administration > Integration Management**.
2. Open the **External Systems** tab.
3. Click the **+Add** button. Choose a name and enter it as the System ID, for example <*YOUR_SYSTEM_ALIAS*>. Set your desired Authorized user.
4. Open the **Administration** menu again, select **Administration > People**.
5. Open the **Groups** tab.
6. Click the **+ New** button and enter the following in the appropriate fields:
    - **Name**: <*YOUR_GROUP_NAME*>. Enter any value for your group name.
    - **Upn**: <*YOUR_GROUP_UPN_NAME*>. Enter any value for your group Upn.
    - **External system**: <*YOUR_SYSTEM_ALIAS*>. IMPORTANT: This is used when sending incidents from HPE SAW to HPE SM and so must match the system ID you chose in Step 3.
    - **Authorized user**: Enter the integration user set in the `instances.json` file.

How to connect two HPE SAW systems

In this section the previous procedure is described again, but this time for two systems called *sawA* and *sawB*, to demonstrate how to set up two HPE SAW systems to work with HPE SX.

IMPORTANT: All names in these examples are just for example purposes. In your configurations they must be the unique names you choose and define.

Add connections for both HPE SAW systems to HPE SX in:

`[%SX_HOME%]/WEB-INF/classes/config/saw/instances.json`

Note: The instance (for example, `sawA` below) in the `instances.json` file must not exceed 50 characters.

1. Add the endpoint.
2. Add the integration user.
3. Enter the correct **Organization**. You can find it in the HPE SAW UI:
    - From the menu in the top right corner select **About > Tenant Id**.
4. Enter the default **Service**, as a number. You can find this in the HPE SAW UI by following these steps:
    - Open an incident.
    - Click to view the Service list.
    - Choose any service from the list.
    - Make a note of the Column Id number.
5. Enter the default **Category**, as a number. You can find it in the HPE SAW UI by following these steps:
    - Open an incident.
    - Open the browser developer console (click F12.)
    - Start a network log in the developer console.
    - Click the category list in the HPE SAW UI.
    - Look at the REST request body in the developer console - the category IDs will be there in JSON format.
    - Choose a category ID.

WARNING: Organization, Service and Category have different IDs in different HPE SAW instances, even though the names are the same.

Example:

```
{
        "sawA":{
                "endpoint":"https://sawA.saas.hp.com",
                "user":{
                        "loginName":"user.XXX@hp.com",
                        "password":"12345"
                },
                "organization":"689550538",
                "defaultRegisteredForActualService":"21219",
                "defaultCategory":"20719"
        },
        "sawB":{
                "endpoint":"https://sawB.saas.hp.com",
                "user":{
                        "loginName":"user.YYY@hp.com",
                        "password":"12345"

                 },
                "organization":"698114386",
                "defaultRegisteredForActualService":"21200",
                "defaultCategory":"20583"
        }
}
```

Configure CX for both HPE SAWs:

`sw.war/WEB-INF/classes/config/caseexchange/external-systems.json`

Example:

```
{
        "externalSystems": [
                {
                        "instanceType": "SAW",
                        "instance": "sawA",
                        "registeredEventGroups": [
                                "IncidentCaseExchangeEvents"
                        ]
                },

                {
                        "instanceType": "SAW",
                        "instance": "sawB",
                        "registeredEventGroups": [
                                "IncidentCaseExchangeEvents"
```

```
                        ]
                }
        ],
        "externalSystemAliases": [
                {
                        "sourceInstanceType": "SAW",
                        "sourceInstance": "sawA",
                        "targetInstanceType": "SAW",
                        "targetInstance": "sawB",
                        "targetAlias": "sawB"
                },
                {
                        "sourceInstanceType": "SAW",
                        "sourceInstance": "sawB",
                        "targetInstanceType": "SAW",
                        "targetInstance": "sawA",
                        "targetAlias": "sawA"
                }
        ]
}
```

Configuration in sawA

1. In the HPE SAW UI, from the top pop-up menu go to **Administration > Integration Management**.
2. Go to the **External Systems** tab.
3. Click the **+Add** button, enter *sawB* as System ID, and set your desired Authorized user (for example, *user.XXX@hp.com*.)
4. From the same menu, go to **Administration > People**.
5. Go to the **Groups** tab.
6. Click the **+ New** button and set the following in the dialog:
    - **Name**: <*sawB group*>. Enter any value for your group name.
    - **Upn**: <*sawB_group*>. Enter any value for your group Upn.
    - **External system**: *sawB* IMPORTANT: This is used when sending incidents from sawA to sawB and must match the system ID given in Step 3.
    - **Authorized user**: This must be the integration user (*user.XXX@hp.com*.)

IMPORTANT: Check that the integration user (*user.XXX@hp.com*) has the **Tenant Admin Role**.

Configuration in sawB

1. In the HPE SAW UI, from the top pop-up menu go to **Administration > Integration Management**.
2. Go to the **External Systems** tab.
3. Click the **+Add** button, enter *sawA* as System ID, and set your desired Authorized user (*user.YYY@hp.com*).
4. From the same menu, go to **Administration > People**.
5. Go to the **Groups** tab.
6. Click the **+ New** button and set the following in the dialog:
    - **Name**: <*sawA group*>. Enter any value for your group name.
    - **Upn**: <*sawA_group*>. Enter any value for your group Upn.
    - **External system**: *sawA* IMPORTANT: This is used when sending incidents from sawB to sawA and must match the system ID given in Step 3.
    - **Authorized user**: This must be an integration user (*user.YYY@hp.com*).

IMPORTANT: Check that the integration user (*user.YYY@hp.com*) has the **Tenant Admin Role**.

Setting User roles and Organizations

HPE SX has both some management pages and a Testing UI. The management pages include the Content Management UI, the Testing UI includes for example the order wizard.

The two UIs have a similar configuration but the Testing UI is shipped separately as a part of the SDK package. See the HPE SX SDK package documentation for details on how to install it.

These UIs are only accessible by users having certain roles. The roles recognized by HPE SX are described below.

The roles valid for the HPE SX **management pages** are:

- ADMINISTRATOR – An administrative User.
- CONSUMPTION – Used for the transport User and shared with the consumption component.

The roles valid for the HPE SX **testing UI** are:

- ADMINISTRATOR – An administrative User.
- UI – The role used for development and testing.

A user needs to be assigned an ADMINISTRATOR or UI role to access any of the HPE SX UI pages.

To assign or change HPE SX user roles, see "Role association" on page 59.

Role association

Users are associated with roles in the `users.json` configuration file, located at `[%SX_HOME%]/WEB-INF/config/users.json`

A simple example configuration:

```
{
    "Provider": {
        "sxCatalogTransportUser": {
            "roles": [
                "CONSUMPTION"
            ]
        },
        "admin": {
            "roles": [
                "ADMINISTRATOR"
            ]
        }
    }
}
```

The file structure reflects the organization structure. In this example the Provider is at the top level, with two users with their roles underneath. A user name can also be * which means all users within the organization will have the same roles. When multiple entries match a user all their roles are merged together.

A more complex example:

```
        {
            "CONSUMER": {
               "admin" : {
                  "roles": [
                    "ADMINISTRATOR"
                  ]
                },
                "*": {
                     "roles": [
                        "UI"
                     ]
                  }
          },
             "Provider": {
                "sxCatalogTransportUser": {
                    "roles": [
                       "CONSUMPTION"
                    ]
                }
             }
```

```
}
```

In this example all the users of the CONSUMER organization have access to the testing UI for creating orders, and the admin user also has access to the administration section.

Selecting the Organization

When a user logs in to the HPE Propel Portal using `https://$PROPEL_VM_HOSTNAME:9000/org/CONSUMER` they have a default organization specified.

To change the default organization:

- Open the `sx.properties` file at `[%SX_HOME%]/WEB-INF/sx.properties`
- Change the `security.idmTenant` property to match your organization name.

HPE SX Content Management

Content packs are extension points to HPE Service Exchange (HPE SX). In collaboration with adapters, content packs enable HPE SX to communicate with end-point systems such as HPE SM or HPE CSA. A content pack is a ZIP or JAR file that can contain operation definitions, FreeMarker templates, HPE OO flows and/or other configuration files. Content packs contain the order message lifecycle modeled in HPE OO flows in request-to-fulfill (R2F) use cases. They can be installed or uninstalled on the running HPE SX server.

Content packs can be deployed into HPE SX at run-time. They provide business logic to the specific adapter. For example, the approval process of an order is modeled in OO Flow. The create order, approve operations, etc. must be defined. OO Flow implementation and the operations that have to be defined depend on the specific features the content pack supports.

Operations are defined in HPE SX JSON notation that is interpreted by the operation executor component of the adapter. The operations typically define a set of calls to the end-point systems' APIs. These calls (steps of the operation) are executed sequentially. The operation definition framework uses Freemarker templates to compose URLs, request bodies, transform responses, and other actions.

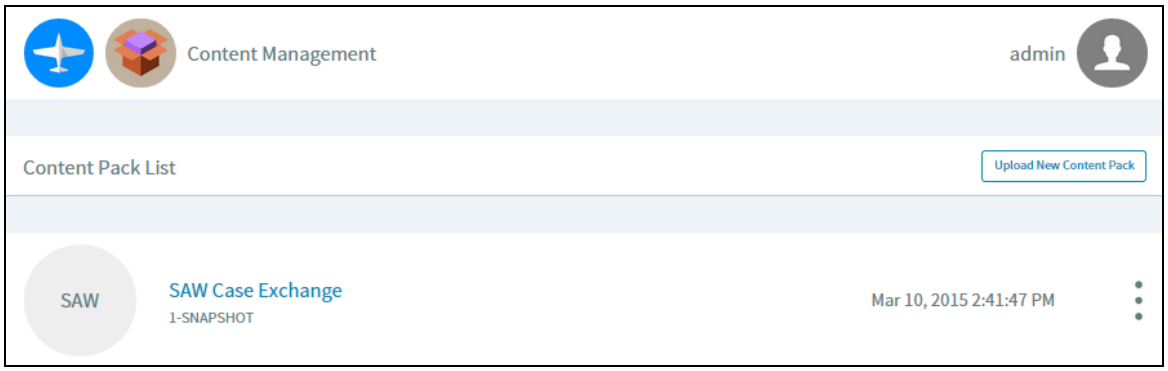
HPE SX offers out-of-the-box functionality through content packs that can be used as-is or customized. The HPE SX Content Management user interface allows you to view, download, upload and delete content packs in HPE SX. Access to this UI is limited to users with the appropriate user roles, see "Setting User roles and Organizations" on page 58. Upload and delete operations include upload or removal of relevant HPE Operation Orchestration JAR files (HPE OO content packs), and the merging of HPE SX customizations into the running HPE SX server.

"Content Packs and their contents" for the out-of-the-box content packs, and the *HPE Propel Service Exchange SDK* for details on how to customize a content pack or create a new one.

Using the Content Management UI

1. Log in to HPE Propel as the `admin` user at `https://$PROPEL_VM_HOSTNAME:9000/org/Provider`.
2. Click the **Content Management** application from the HPE Propel Launchpad.
3. In the **Content Management** application, view the available content packs and click a specific content pack to view its details:
   - Content Pack ID
   - Version numbers
   - Which adapter they connect to
   - Features
   - The relevant OO content pack name.

Example section of the **Content Management** application:



Downloading content packs

1. Click **Download** from the drop-down list in the row of the content pack you want to download.
2. When prompted, **Save** the <*contentpack*>.zip. Depending on your browser settings you might need to specify where to save the file, or you might find it in your **Downloads** folder.
3. View and customize the files.

Deleting content packs

To delete a content pack:

1. Click **Delete** from the drop-down list in the row of the content pack you want to delete.
2. A confirmation will be displayed.

Uploading content packs

To upload a content pack:

1. Click the **Upload New Content Pack** button.
2. Locate the `.zip` or `.jar` to be uploaded, for example, the `sm-case-exchange.jar` containing a customized `case-exchange.json` file.
3. Click **Open**.
4. When the upload is complete, a confirmation appears near the top of the Content Management UI. The upload time for the content pack is updated.

NOTE:When uploading a content pack that was previously loaded, HPE SX replaces the existing version. Content packs are identified by an ID attribute provided in their metadata file.

Content Packs and their contents

HPE Propel contains the following out-of-the-box content packs:

- *SM request to fulfillment* (**sm-r2f**) - the content pack providing files for HPE SM requests to fulfillment.
- *Service Exchange base content* (**sx-base**) - the base content for HPE SX. This content pack is required and cannot be removed.
- *Support for test UI (SM)* (**sm-test-ui-support**) - the content pack providing files for HPE SM-related functions of the HPE SX UI.
- *SAW Case Exchange* (**saw-case-exchange**) - the content pack providing files for HPE SAW Case Exchange customizations.
- *SAW Ticketing* (**saw-ticketing**) - the content pack providing files for HPE SAW ticketing.
- *SM Case Exchange* (**sm-case-exchange**) - the content pack providing files for HPE SX Case Exchange customizations.
- *SM Ticketing* (**sm-ticketing**) - the content pack providing files for HPE SM ticketing.
- *Case Exchange* (**case-exchange**) - the content pack providing files for HPE Propel Case Exchange.
- *MOCK request to fulfillment* (**mock-r2f**) - an empty content pack.
- *Support for test UI (SAW)* (**saw-test-ui-support**) - the content pack providing files for HPE SAW-related functions of HPE SX UI.
- *CSA request to fulfillment* (**csa-r2f**) - the content pack providing files for HPE CSA requests to fulfillment (r2f).
- *EMAIL request to fulfillment* (**email-r2f**) - files to enable Email requests to fulfillment of native offerings.
- *Support for test UI (CSA)* (**csa-test-ui-support**) - the content pack providing files for HPE CSA related functions of HPE SX UI.
- *OO request to fulfillment* (**oo-r2f**) - the content pack providing files for HPE OO requests to fulfillment (r2f).
- *SAW request to fulfillment* (**saw-r2f**) - the content pack providing files for HPE SAW requests to fulfillment (r2f).

HPE SX Case Exchange (CX)

CX is a subsystem of HPE SX, designed for exchanging entity data between two or more external systems. The aim is to have some entity data, for example Incidents, automatically synchronized between two different systems without the need for human intervention.

CX does all the work of data transformation including connecting systems of different types, for example HPE SM and HPE SAW. In addition, CX removes the need to setup the two systems to communicate directly with each other, which helps simplify the security and environment setup. Instead of having to provide an adapter for each possible system type pair combination, it is sufficient to implement CX between system A and HPE SX, and system B and HPE SX.

CX works in the following way:

1. A pairing between source and target system is defined.
2. The source system is observed for changes CX is interested in.
3. Once an interesting entity change is detected (Creation, Update, Status change), CX performs the following:
   a. Retrieves any important entity data from the source system.
   b. Transforms the entity data to the canonical model representation.
   c. Changes the data of a connected entity on a target system in a way defined by the configuration

Example:

There is an HPE SM instance called SM03 and an HPE SAW instance called SAW02.

To set up CX to clone any new Incident created on SM03 to SAW02 systems:

1. Create a CX pairing (XXXXsee External systems and entities pairing) between SM03 and SAW02, where SM03 is a source system and SAW02 is the target system.
2. Set up cloning of new incidents for the pairing. External systems and entities pairing

Once finished with the configuration, any new Incident created on SM03 is automatically cloned to SAW02.

When a new system type adapter (for example, Remedy) is being written, the adapter can be implemented to support Case Exchange, see the *HPE Propel Service Exchange SDK* for details on how to do this.

When configured, Case Exchange can listen out for entity changes where an entity in one HPE SM instance is referring to an entity in another HPE SM instance. If a referring entity is changed in one HPE SM instance, HPE SX is notified and registers a listener for entity changes in the other (referred) HPE SM instance.

Examples of HPE SX Case Exchange supported use cases:

1. An administrator can configure HPE SX to be notified:
    - If an entity of type {entityType} complying with filter condition {entityFilterExpr} in external system {instance} is created/updated/deleted.
    - If an entity of type {entityType} with id {entityId} in external system {instance} is created/updated/deleted.
2. An administrator can configure HPE SX to be notified about an entity change in an external system then:
    - Execute a custom OO flow.
    - Execute a custom SX operation.
3. OO flows can call custom (Case Exchange specific) HPE SX operations to:
    - Register or unregister a new entity-change listener in external systems.
    - Store mapping from entity {instanceTypeA}:{instanceA}:{entityTypeA}:{entityIdA} to {instanceTypeB}:{instanceB}:{entityTypeB}:{entityIdB}.
    - Remove mapping from or to entity {instanceType}:{instance}:{entityType}:{entityId}.

Configuring Case Exchange

This requires two procedures:

- "Configure HPE SM" on page 71
- "Configure HPE SX" on page 72

Configure HPE SM

1. Apply unload script SXCaseExchange.unl

Find the SXCaseExchange.unl unload script inside the sm-case-exchange content pack.

To apply the SXCaseExchange.unl script into each of your HPE SM instances, follow these steps:

1. Go to **System Administration > Ongoing Maintenance > Unload Manager > Apply Unload**.
2. Select **SXCaseExchange.unl**.
3. Select **Backup To:** and enter or select a backup location.
4. Click **Next**.
5. If there is a conflict with an entry, double-click that entry and manually resolve the conflict based on the description of what the unload script should do.
6. Click **Next**.

The unload script contains the following customizations:

- Adds new REST endpoint SX/SXCE_Incident
- Adds new REST endpoint SX/SXCE_IncidentActivity
- Adds triggers for the following tables:
    - probsummary
    - activity

2. Configure Activity privileges

Add activity privileges:

1. Open the HPE SM client.
2. Go to **Tailoring > Format Control > <Name: activity> > Privileges**.
3. Change false to true for operation **Add**.
4. Click **Save**.

Configure HPE SX

This configuration section describes how the Case Exchange (CX) framework is configured to communicate with end-point systems and to perform entity data exchange from one system to another. It includes:

- Which configuration files are involved in setting up CX operations.
- How various concepts of CX (like Events and Event Groups) are set up, including real-life examples of JSON configuration to illustrate what is being described.

Configuration Files

There are two configuration files involved in CX configuration: `external-systems.json` and `case-exchange.json`.The data format of both files is JSON.

external-systems.json

There is one `external-systems.json` file in the HPE SX war. In its first section, externalSystems, it contains the definitions for individual **external systems** one by one in an array. In the second section, **externalSystemAliases**, it contains definitions of external system pairs.

Here is an example from the `external-systems.json` file.

external-systems.json

```
{
    "externalSystems": [ // definitions of external systems, each item of the array
defines
      // one external system instance
    { // the first external system instance
         "instanceType" : "SAW", / the type of the defined system
         "instance": "msalb003sngx", // the name of the external system
         "registeredEventGroups": [ // the array of event groups that should be
           // observed on the external system
             "IncidentCaseExchangeEvents"
         ]
    },
    { // the second external system instance
         "instanceType" : "SM",
         "instance": "mpavmsm08",
         "registeredEventGroups": [
           // the external system
             "IncidentCaseExchangeEvents"
         ]
    }
    ],
```

```
    "externalSystemAliases": [ // definitions of external system pairs, each item
     // of the array defines one external system pair"
        { // first external system pair
           "sourceInstanceType": "SM", // the type of source external system of the
pair
           "sourceInstance": "mpavmsm08", // the name of the source external system
instance
           "targetInstanceType": "SAW", // the target external system type
           "targetInstance": "msalb003sngx", // the target external system name
           "targetAlias": "saw" // the target alias used in source external system
        },
        { // second external system pair
           "sourceInstanceType": "SAW",
           "sourceInstance": "msalb003sngx",
           "targetInstanceType": "SM",
           "targetInstance": "mpavmsm08",
           "targetAlias": "SM08"
        }
      ]
}
```

case-exchange.json

While there is only one `external-systems.json` file, there are typically multiple `case-exchange.json files`. Their content is combined as if there was a single file:

> **Note**: If some `case-exchange.json` files contain incompatible content, the resulting configuration is non-deterministic and may cause problems.

Each case-exchange.json file may contain the following sections:

1. **events**. Events are defined on the level of the external system type, for example, HPE SM. The events recognized by the CX framework are defined in this section:

events section

```
 "events: { // the "events" section
    "SM": { // the identifier of the external system whose events we are defining
        "incidentExternalReferenceCreated": { // the name of the defined event
            "entityType": "probsummary", // the native (external system specific)
entity type
            "entityFilter": "RECORD['vendor']!=null && RECORD['reference.no']==null
&& (ISCREATE || ISUPDATE && OLDRECORD['vendor']!=NEWRECORD['vendor'])", // the
filter defining event trigger condition
            "changeType": [ "create", "update" ] // optional Service manager
specific field
        },
        "incidentUpdated": {
```

```
            "entityType": "probsummary",
            "entityFilter": "RECORD['vendor']!=null && OLDRECORD['vendor']
==NEWRECORD['vendor'] && (OLDRECORD['brief.description']!=RECORD
['brief.description'] || OLDRECORD['action'].toString() || OLDRECORD
['severity']!=RECORD['severity'] || OLDRECORD['initial.impact']!=RECORD
['initial.impact'])",
            "change Type": [ "update" ]
        }
      ...
}
```

2. **eventGroups**. In this section, event groups are defined by specifying a list of contained events for each of them:

eventGroups section

```
 "eventGroups: { // the "eventGroups" section
    "IncidentCaseExchangeEvents": [ // the name of the event group being defined
        "incidentExternalReferenceCreated", // the name of the first event
belonging to the group
        "incidentUpdated", // the name of the second event belonging to the group
        "incidentResolved", // ...
        "incidentReopened",
        "incidentClosed",
        "incidentOwnershipAssigned",
        "incidentOwnershipAccepted",
        "incidentRejected",
        "incidentCancelled"
     ],
     "TaskCaseExchangeEvents": [ // the name of another event group
          "taskExternalReferenceCreated" // this group only contains one event
      ]
}
```

3. **eventActions**.The action or sequence of actions to be performed once an event is triggered. The order of execution when merging event actions from multiple configuration files is not defined. Each Action represents one of two currently supported action types:

- **executeOperation** – An HPE SX operation is executed. Based on the value of the `backendSystemType` property, the operation definition is searched for in content packs associated with the respective backend system type.
- **executeOoFlow** – An OO Flow is executed. Based on the value of the `backendSystemType` property, the flow is executed on behalf of the corresponding backend system. The flow to be executed is determined by the value of the `messageType` property. The message type is used to search for flow information in the `flows.json` file.

eventActions section

```
 "eventActions: { // the "eventActions" section
      "incidentClosed": { // the event we're defining actions for
           { // the first action to be executed when the event is triggered
                "action": "executeOperation", // action = execute operation
                "backendSystemType": "SM" // the backend system to be searched for
the operation
                "operationName": "retrieveIncident" // the name of the operation to
be executed
           }
           { // the second action to be executed when the event is triggered
                "action": "executeOperation",
                "backendSystemType": "SX"
                "operationName": "convertAssignmentGroupToInstance"
           }
           { // the third action to be executed when the event is triggered
                "action": "executeOoFlow", // action = execute OO flow
                "backendSystemType": "SX", // the backend system on whose behalf
the OO flow will be executed
                "messageType": "IncidentCaseExchangeFlow" // the type of the
message to be sent to the OO flow
           }
  }
```

4. **eventGroupActions**.The action or sequence of actions to be performed once an event from the given event group is triggered. The order of execution between event actions and event group actions is not deterministic, so it is not recommended to mix event actions and event group actions together when the order of execution is important. Both the syntax and semantics of the eventGroupActions is the same as for the eventActions:

*-mappings.json

Each external system type participating in CX has its own set of entities, its own vocabulary, and its own property names and values. To allow CX to communicate between different types of systems, the vocabulary, entities and properties, and their values, have to be unified. The CX implementation uses a common data format for the exchanged data called the Canonical Model. As a helper for data transformation between the canonical model and the external system native data model, each external system can provide a mapping file to aid the translations.

The name of the mapping file is in the form of **<external_system_type>-mappings.json**, for example sm-mappings.json. It may contain translation tables for entity names and property values. The translation tables can be used by content packs to make easy transformations, most importantly in Free Marker templates. Property names are not typically translated via translation table as it is much easier to perform their translation directly in Free Marker templates. In the next paragraphs, we will show an example of each of the mappings.

Entity Name Mappings

In this section of the mapping file, the native entity names are mapped to canonical model entity names:

Entity Name Mappings section

```
 "entityType: { // the section start
      "Incident": "probsummary", // pair of Canonical Model/native external system
entity name
      "IncidentTask": "imTask" // another pair for another entity
 }
```

Property Value Mappings

For each entity, a mapping for some of its property values between the Canonical Model and the native external system values may be provided:

Property Value Mappings

```
 "Incident: { // the name of the entity
         "Status": { // the name of the property in Canonical Model whose values
will be translated via this table
             "Open": "Ready", // pair of Canonical Model/native external system
property value
             "WorkInProgress": "InProgress", // another pair
             "PendingChange": "Pending",
             "PendingOther": "Suspended",
             "Complete": "Complete"
          }
          "Urgency": { // another property whose values will be translated
              "U4": "NoDisruption",
              "U3": "SlightDisruption", executed
              "U2": "SevereDisruption",
              "U1": "TotalLossOfService",
           }
  }
```

Free Marker Code

Once the mapping is defined in the mapping file, the mapping can be used to translate the value within a Free Marker template:

Free Marker Code

```
<#assign
findKey='com.hp.ccue.serviceExchange.adapter.freemarker.FindKeyForValue'?new()/>
// declare the findKey function defined in Java code of SX API for Adapters
<#assign sawMapping=loadConfig(context.contentStorage, "saw-case-exchange/saw-
mappings") />

{
```

```
       "properties": {
           "Urgency": "${findKey(sawMapping.Incident.Urgency,
entityProperties.Urgency)}",
            // use the Service Exchange provided findKey() function to perform
            // the translation of Urgency to Canonical Model specific value
           "Status": "${findKey(sawMapping.Incident.Status,
entityProperties.Status)}"
            // use the Service Exchange provided findKey() function to perform
            // the translation of Status to Canonical Model specific value
       }
  }
```

Configuration Concepts

When configuring a CX framework for HPE SX content, the following items need to be configured:

- External Systems
- External System Pairs
- Entity Types to be Case Exchanged
- Events
- Event Filters
- Event Groups
- Event and Event Group Actions

External Systems

In order to have an external system participate in CX, it must be present in the external system configuration. The configuration entry must contain:

- The system type (for example HPE SM, JIRA), the name of the system instance (corresponding to the name assigned to it in the `instances.json` configuration file for the respective external system type.)
- The array of event groups CX will handle for this particular external system.

Here is an example of an external system configuration:

External System

```
 {
      "instanceType": "SM", // the type of the external system
      "instance": "mpavmsmapp01", // the name of the concrete external system
instance
```

```
      "registeredEventGroups": [ // the event groups activated for this system
instance
           "TaskCaseExchangeEvents",
           "TaskCaseExchangeIncidentEvents"
      ]
  }
```

External System Pairs

To configure CX to perform entity data exchange between two particular systems, it is necessary to create an external system pair for them. In the pair definition:

- Source system must be specified by its type and name
- Target system must be specified by its type and name
- An alias to be used by users in the source system to identify the target system

Here is an example of an external system pair configuration:

External System Pair

```
{
    "sourceInstanceType": "SM", // the source external system type
    "sourceInstance": "mpavmsm08", // the source external system name
    "targetInstanceType": "JIRA", // the target (receiving) external system type
    "targetInstance": "mpavmint01", // the target (receiving) external system name
    "targetAlias": "jira" // the alias used for the target system instance in
      //the source system
}
```

Entity Types to be Case Exchanged

The entity types to be case exchanged are not specified directly. Instead, for each external system, an array of event groups is specified to be watched for in the system. See the **External Systems** section for an example of such a configuration. Each event group consists of several individual events, typically all associated with a specific entity type. See the **Event Groups** section for an example of an Event Group configuration and the Events section for an event configuration example. In this way, this indirect specification determines which entities are processed for the particular external system.

Events

The operation of the CX framework is based on events. Depending on the external system type and the changed entity type, the set of potential events that can occur is defined. The source external system is being watched for changes. Once an entity change occurs, CX is notified by the external system Change Observer. For each applicable event, its filter is checked and if its filter condition is satisfied by

the entity change, the corresponding event is triggered. See the Event Filters section for more detail. As a result, each entity change can trigger one or more events.

Here is an example event definition:

Event

```
"incidentUpdated": { // the name of the event being defined
     "entityType": "probsummary", // the native type of the entity the event is
defined for;
        // probsummary is Service Manager's type for Incident
      "entityFilter": "RECORD['vendor']!=null && OLDRECORD['vendor']==NEWRECORD
['vendor'] && (OLDRECORD['brief.description']!=RECORD['brief.description'] ||
OLDRECORD['action'].toString()!=RECORD['action'].toString() || OLDRECORD
['severity']!=RECORD['severity'] || OLDRECORD['initial.impact']!=RECORD
['initial.impact'])",
      "changeType": [ "update" ] // this field is optional
}
```

Event Filters

The definition of each event contains one or more filters. The filters are conditional expressions operating over changed entity data, written in Javascript syntax. Once an entity change is being processed by the CX framework, the filters for each potential event are evaluated. If at least one of them is evaluated to true, the respective event is triggered, ready for further processing. The input parameters for the condition vary between external system types because they are heavily depending on the entity change data, which in turn is generated by the system's Change Observer, and their format and content are not standardized.

Here is an example of an event filter definition for HPE SM:

Filter Expression

```
"RECORD['assignment']!=null && (ISCREATE || ISUPDATE && OLDRECORD
['assignment']!=NEWRECORD['assignment'])"
```

Event Groups

Events may be grouped together to form an Event Group. All the events in a group need to be applicable to the same entity. Event groups have two purposes:

- To allow assigning a common action to a set of events.
- To configure which events should be observed on a particular system.

Only event groups may be assigned to a target external system. Therefore, the only way to observe an event on a particular external system is to create an event group containing that event and add the

event group to the `registeredEventGroups` property array in the external system configuration. An event may be part of different Event Groups.

Here is an example of an Event Group definition:

Event Group

```
 "IncidentCaseExchangeEvents": [ // the name of the Event Group
      "incidentExternalReferenceCreated", // an array of individual Events
       // to be part of the Event Group, identified by their name
      "incidentUpdated",
      "incidentResolved",
      "incidentReopened",
      "incidentClosed",
      "incidentOwnershipAssigned",
      "incidentOwnershipAccepted",
      "incidentRejected",
      "incidentCancelled"
 ]
```

Here is an example of how to assign the Event Group to an external system instance:

Event Group Assignment

```
{
    "instanceType": "SM", // the External System type
    "instance": "mpavmsm09", // the External System name
    "registeredEventGroups": [ "problem.ReferringEntityEvents" ]
     // an array of Event Groups to be observed for this External System instance
}
```

Event and Event Group Actions

The last piece of the configuration is to define what the CX framework should perform after an Event is triggered. The execution units in HPE SX are called operations. For each event, the user can define a set of operations to be executed once the Event is triggered. Another set of operations can be configured for a whole event group. If operations are defined for the Event Group and for an Event from such a group, the group operations execute first, and then the event operations execute.

Here is an example of an Event operation definition:

Event Group Actions

```
"IncidentCaseExchangeEvents": [
{
     "action": "executeOperation",
     "operationName": "retrieveIncident"
},
{
```

```
     "action": "executeOperation",
     "operationName": "convertIncidentToCanonicalModel"
},
{
     "action": "executeOoFlow",
     "backendSystemType": "SX",
     "messageType": "IncidentCaseExchangeFlow"
}]
```

The same block of configuration can be used to configure operations for an Event Group.

HPE SX Adapters

HPE SX adapters interact with underlying (end-point) systems, making them accessible to HPE SX processes. Examples of end-point systems are HPE SM, HPE CSA, and HPE SAW. An adapter is required for an end-point system to be accessed by HPE SX. In this way the adapters make the functionality of the end-point systems available to HPE SX clients.

HPE Propel contains the following OOB adapters, located in the `/opt/hp/propel/sx/WEB-INF/lib` directory:

- HPE SX adapter - the internal HPE SX adapter. This is always the first adapter and implements the HPE SX CX functionality.
- HPE SM adapter - specifically for HPE SM end-point systems.
- HPE CSA adapter - specifically for HPE CSA end-point systems.
- EMAIL adapter - this adapter enables the fulfillment by email of offerings created independent of third-party products.
- MOCK adapter - for testing.

Note: To create your own adapter, see detailed procedures in the *HPE Propel Service Exchange SDK*.

Enabling an HPE SX adapter

To connect HPE Propel with end-point systems that do not have an OOB adapter provided by HPE Propel, you must install the appropriate adapter.

Install an adapter:

This example uses JIRA. Replace *jira* with your chosen adapter:

1. Stop the HPE SX service:

   ```
   # service jetty-sx stop
   ```

2. Copy the `sx-adapter-jira-version.jar` file to the `/opt/hp/propel/sx/WEB-INF/lib` directory.

3. Start the HPE SX service:

   ```
   # service jetty-sx start
   ```

Manually configure HPE SX-required files

Note: If you followed the HPE Propel installation procedure and have a functional system up and running, these configurations are already in place.

Use the following instructions to check, troubleshoot or customize configurations:

Configuring for OO server

To set an internal connection to a specific OO server, add the OO entry into the JSON file:

`[%SX_HOME%]/WEB-INF/classes/config/infrastructure.json`

Required fields: `endpoint`, `loginName`, and `password`

Example:

```
{
    "OO": {
        "endpoint": "http://oo.example.com:8080/oo/rest",
        "loginName": "oouser",
        "password": "oopassword"
    }
}
```

Note: Change the `endpoint`, `loginName`, and `password` to your unique values.

To enable the OO server to send email messages, change values in the JSON file:

`[%SX_HOME%]/WEB-INF/classes/config/oo/properties.json`

Example:

```
{
   "smtpServer": "smtp3.example.com",
   "smtpPort": "25",
   "mailFrom": "noreply@example.com",
   "smtpUser": "john.doe@example.com",
   "smtpPassword: "",
   "emailBcc": "joe.doe@example.com"
}
```

After you make changes to the `properties.json` file, for the changes to take effect, you must restart the HPE SX service with the following command:

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

Configuring for RabbitMQ Server

To set an internal connection to a specific RabbitMQ server add/edit the `JMS_BROKER` entry in the JSON file:

`[%SX_HOME%]/WEB-INF/classes/config/infrastructure.json`

Required field: `endpoint`

Example:

```
{
    "JMS_BROKER": {
          "endpoint": "oo.example.com"
    }
}
```

Note: Change the endpoints to those for your organization.

Configuring for the HPE Propel Portal

To enable communication with the HPE Propel Portal, entry `SERVICE_CATALOG` has to be added/edited in the JSON file:

`[%SX_HOME%]/WEB-INF/classes/config/infrastructure.json`

Example:

```
{
  "SERVICE_CATALOG": {
    "catalogApprovalPageLink": "https://<PROPEL_HOSTNAME>:9010/approval",
    "internalCallbackEndpoint": "https://<PROPEL_HOSTNAME>:9444/sx/api/catalog",
    "requestCallbackEndpoint": "https://<PROPEL_HOSTNAME>:9510/sx-
callback/request",
    "subscriptionCallbackEndpoint": "https://<PROPEL_
HOSTNAME>:9595/api/subscription/v1/sub"
    }
}
```

Note: Change the endpoints to those for your organization.

It is possible to use the string `${hpIPAddress}` instead of a specific IP address of the HPE Propel system, but it is still required to add the server port manually.

Configuring for IdM

To use Identity Manager, the entry `AUTHENTICATION` has to be added/edited in the JSON file:

`[%SX_HOME%]/WEB-INF/classes/config/infrastructure.json`

Example:

```
{
    "AUTHENTICATION": {
        "secretKey": "<YourSecretKey>"
    }
```

Required field: `secretKey`

Endpoint and other information has to be set in the properties file:

`[%SX_HOME%]/WEB-INF/sx.properties`

Required lines contain the prefix **security**.

Configuring for PostgreSQL

To use your PostgreSQL installation, change properties with the prefix 'db' in the properties file:

`[%SX_HOME%]/WEB-INF/sx.properties`

Preset values:

- `db.dialect=org.hibernate.dialect.PostgreSQLDialect`
- `db.driverClassName=org.postgresql.Driver`
- `db.password=`*`Password`*
- `db.url=jdbc\:postgresql\://localhost\:5432/sxdb`
- `db.username=sxuser`

Configure SSL for a Supplier

If HTTPS is used for communication between HPE Propel and a supplier, then HTTPS must be configured.

Important: Third-party or corporate CA-signed certificates should be used in production systems; however, self-signed certificates generated by HPE Propel can be used in non-production systems.

Configure SSL for a supplier by performing the instructions in one of the following sections, depending on whether you need to configure one-way SSL or two-way SSL for the supplier:

- "Configure One-Way SSL" below
- "Configure Two-Way SSL" on the next page

Configure One-Way SSL

To configure one-way SSL for a supplier, perform the following steps:

1. Import the HPE Propel VM's CA-signed certificate into the supplier'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 supplier's `/tmp` directory.
   b. On the supplier's system, import the CA-signed certificate:

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

      Where *SUPPLIER-KEYSTORE-PATH* is the location of the `cacerts` file on the supplier's system. Examples of `cacerts` file locations are:

      - HPE SM on Windows:
        `<HPE-ServiceManager-installation-path>\Server\RUN\cacerts`
      - HPE SM on Linux:
        `/<HPE-ServiceManager-installation-path>/Server/RUN/cacerts`
      - HPE CSA on Windows:
        `<HPE-CSA-installation-path>\openjre\lib\security\cacerts`

- HPE CSA on Linux:
  `<HPE-CSA-installation-path>/openjre/lib/security/cacerts`

c. On the supplier's system, restart the supplier's services.

2. Import the supplier's CA certificate into the HPE Propel VM's truststore. The general steps to do this are:

   a. Obtain the supplier's CA certificate, and then copy it to the HPE Propel VM's `/tmp` directory. For examples of obtaining a supplier's certificate, see "SSL Tips" on page 93. In the following step, the supplier's CA certificate is in a `CA.crt` file.

   b. On the HPE Propel VM, import the supplier's CA-signed certificate:

   ```
   # keytool -importcert -file /tmp/CA.crt -alias Supplier_CA -trustcacerts
   -keystore /opt/hp/propel/security/propel.truststore
   ```

   (The default password is "propel2014" for the HPE Propel truststore.)

3. On the HPE Propel VM, restart the HPE Service Exchange (HPE SX) services:

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

Tip: To verify that HTTPS is correctly configured between HPE Propel and the supplier, view the supplier details in the HPE Propel **Suppliers** application, and then click the **Diagnostics** tab. The status should indicate there are no connection issues.

Configure Two-Way SSL

In addition to authentication by SSO, HPE Propel requires the request coming from the HPE SM instance to be authenticated. Similarly, to establish a two-way connection, HPE SM also requires the request from HPE Propel to be authenticated. To configure two-way SSL for a supplier, perform the following steps:

1. Import the HPE Propel VM's CA-signed certificate into the supplier'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 supplier's `/tmp` directory.

   b. On the supplier's system, import the CA-signed certificate:

> **Note:** If the system requires both a CA-signed root certificate and an intermediate certificate, import the `CA.crt` and `intermediate.crt` files into the `cacerts` file.

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

Where *SUPPLIER-KEYSTORE-PATH* is the location of the `cacerts` file on the supplier's system. Examples of `cacerts` file locations are:

- HPE SM on Windows:
  `<HPE-ServiceManager-installation-path>\Server\RUN\cacerts`
- HPE SM on Linux:
  `/<HPE-ServiceManager-installation-path>/Server/RUN`
- HPE CSA on Windows:
  `<HPE-CSA-installation-path>\openjre\lib\security\cacerts`
- HPE CSA on Linux:
  `<HPE-CSA-installation-path>/openjre/lib/security/cacerts`

c. On the supplier's system, restart the supplier's services.

2. Import the HPE Propel host's certificate (`/opt/hp/propel/security/propel_host.crt`) into the supplier's trusted clients keystore:

```
keytool -importcert -file /tmp/propel_host.crt -alias propel_host -trustcacerts
-keystore <SUPPLIER-KEYSTORE-PATH>/cacerts
```

3. Import the supplier's CA certificate into the HPE Propel VM's truststore. The general steps to do this are:

   a. Obtain the supplier's CA certificate, and then copy it to the HPE Propel VM's `/tmp` directory. For examples of obtaining a supplier's certificate, see "SSL Tips" on the next page. In the following step, the supplier's CA certificate is in a `CA.crt` file.

   b. On the HPE Propel VM, import the supplier's CA-signed certificate:

```
# keytool -importcert -file /tmp/CA.crt -alias Supplier_CA -trustcacerts
-keystore /opt/hp/propel/security/propel.truststore
```

   (The default password is "propel2014" for the HPE Propel truststore.)

4. Enable sending the client certificate in HPE Propel.

   a. In the `sx.properties` file in the `/opt/hp/propel/sx/WEB-INF` directory, make sure that the `skipCertificateValidation` property is set to `false` (default).

b. Update the `jetty-ssl.xml` file.

> **Note:** If you are using the default keystore (`propel_host.pfx`), ignore this step.

In the `/opt/hp/propel/jetty-sx/etc/jetty-ssl.xml` file, set the `javax.net.ssl.keyStore`, `javax.net.ssl.keyStorePassword`, and `javax.net.ssl.keyStoreType` properties (by replacing the default values) as shown below:

```
<Call name="setProperty">
    <Arg>javax.net.ssl.keyStore</Arg>
    <Arg>/opt/hp/propel/security/propel_host.pfx</Arg>
</Call>
<Call name="setProperty">
    <Arg>javax.net.ssl.keyStorePassword</Arg>
    <Arg>${STORE_PASSWORD}</Arg>
</Call>
<Call name="setProperty">
    <Arg>javax.net.ssl.keyStoreType</Arg>
    <Arg>${STORE_TYPE}</Arg>
</Call>
```

Where:

- ${STORE_PASSWORD} is the password of your own `propel_host.pfx` keystore.
- ${STORE_TYPE} is the certificate type of the keystore: either **jks** or **pkcs12**.

5. On the HPE Propel VM, restart the HPE Service Exchange (HPE SX) services:

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

> **Tip**: To verify that HTTPS is correctly configured between HPE Propel and the supplier, view the supplier details in the HPE Propel **Suppliers** application, and then click the **Diagnostics** tab. The status should indicate there are no connection issues.

SSL Tips

If you do not have an SSL certificate from the supplier's system, you can manually create a certificate. Examples of creating a supplier's SSL certificate are:

- "Export SSL Certificate from Supplier's Truststore" on the next page
- "Create Supplier's Host Certificate" on the next page

Export SSL Certificate from Supplier's Truststore

Use the following command on the supplier's system to export an SSL certificate from the supplier's truststore:

```
# keytool -exportcert -file <CERT-OUTPUT-FILE> -keystore
<SUPPLIER-KEYSTORE-PATH>/cacerts -alias <SUPPLIER-ALIAS>
```

Where: :

- *CERT-OUTPUT-FILE* is the output file that will contain the exported certificate.
- *SUPPLIER-KEYSTORE-PATH* is the location of the `cacerts` file on the supplier's system.
- *SUPPLIER-ALIAS* is the alias used in the supplier's truststore to identify the supplier's certificate.

Create Supplier's Host Certificate

Use the following procedure to create a supplier's host certificate:

1. On the HPE Propel VM, execute the following command:

   ```
   # openssl s_client -connect <SUPPLIER-HOST>:<PORT> > supplier.crt
   ```

2. Edit the `supplier.crt` file and retain only the lines beginning with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----", deleting all other lines.

You can verify that the supplier's host certificate is valid with the following command:

```
# keytool -printcert -file supplier.crt
```

The output of the `keytool` command should identify the certificate owner and issuer.

Troubleshooting

This section offers some general recommendations and troubleshooting tips for HPE Propel.

General recommended steps

1. As the HPE Propel administrator, run the **Diagnostics** application from the HPE Propel Launchpad to check your connections are working and your configuration is correct, see "Verify HPE SX Configuration" on page 23.
2. When a problem happens, first inspect the relevant log files (for locations see "HPE Propel log files" on page 97), and look for any sign of an error.
2. If no error is found, look into the OO Flows input parameters (see "Where to find help " below.) For example, look for wrongly set notification email addresses etc.
3. If you can access it, use the HPE SX Debug UI. If the functionality you tried to perform through the is available in the HPE SX Debug UI, try to run it there. If it is successful, it is an important point to note in any defect report logged to HPE Support. If it still does not work, check the UI error messages and see the log files for any changes in the error printouts, when compared with the HPE Propel Portal execution.

Where to find help

OO Flows

If a problem occurs and you suspect the OO Flows did not execute properly:

1. Navigate to OO.

   The URL of the OO used for HPE SX will look similar to this:

   ```
   http://oo_server_hostname:8080/oo/#/runtimeWorkspace/runs
   ```

2. Check the following:

   a. Check that there is an entry in the **Run Management** section that corresponds to your request. View it.

   b. Check that the Flow was executed properly. It is fine that it goes through failure transitions, but the Flow should not end in an error state.

   c. If the flow ends in an error state, follow these steps to look for details in the Flow Input parameters:

      i. When viewing the Flow, click on its header (where the Flow name is displayed together with a down-expand arrow.)

      ii. You will see all the input parameters for the flow. Look for any suspicious or incorrect values, and make a note of them in case you need to report the issue later.

HPE Propel log files

Diagnostic context

Each request to a service is associated with a unique correlation ID (also called *diagnostic context*):

```
ERROR [2016-07-07T05:43:24.041-06:00] [AmBmvyoi] [msvc-util] received an error in response ...
```

In this example, `[AmBmvyoi]` is the unique correlation ID. You can use the ID to track execution of a request across multiple services.

HPE SX log files

HPE SX uses Apache Log4j logging framework. The Log4j configuration file can be found at the following location:

```
/opt/hp/propel/sx/WEB-INF/classes/log4j.xml
```

> **Tip**: You can modify the configuration file when implementing your own adapter and create a unique log file.

HPE SX log files are located in the HPE Propel log directory, at:

```
/var/log/propel/jetty-sx
```

The following important HPE SX log files are present out of the box.

Jetty server log file

File Name	Content Description
`console.log`	Standard Jetty log. HPE SX actions are logged in separate file. Use to check war file deployment status and fatal errors.

HPE SX log files

File Name	Content Description

autopass.log	HPE Propel license management (coordinated by HPE SX).
sx-messages.log	HPE SX REST endpoint (/operation, /ticket, /request) events.
sx.log	General HPE SX log in info level: • Messages on REST endpoints • OO flow execution • JMS messages • Pipeline execution • Operation execution (FTL transformations) – information about execution and error states
sx-trace.log	All the events logged in sx.log in trace level. FTL transformations logged with their input and output.
notification.log	HPE SX notifications to HPE Propel Portal (request and subscriptions state notifications)
sx-aggregation.log	Aggregation runs and errors in aggregating catalog items.
adapter-messages.log	Adapters boot, shutdown, pipeline execution, operation execution, change observer actions, and CX event evaluation across all the adapters deployed in HPE SX.
case-exchange.log	HPE SX case exchange-related log, HPE CX adapter boot and shutdown, case-exchange content pack reload, entity-change listening registration, and HPE SM case-exchange events.

HPE SX adapter-specific log files

Some of the adapters create specific log files. These log files contain the same information as sx.log but are restricted to a specific adapter. You may find it useful to use the same approach with your own adapter.

File Name	Content Description
csa-messages.log	HPE CSA general log file.
saw-messages.log	HPE SAW general log file.
sm-messages.log	HPE SM general log file.

HPE OO log files

Use to troubleshoot HPE OO problems. Located in:

/opt/hp/oo/central/var/logs

File Name	Content Description
wrapper.log	HPE OO general log file.
general.log	HPE OO general log file.

Catalog log files

Located in:

/var/log/propel/catalog

File Name	Content Description
catalog.log	Catalog items, catalogs, and organization management-related actions. May provide information on failed item aggregation.
console.log	Catalog items, catalogs, and organization management-related actions. May provide information on failed item aggregation.

Identity service log files

Located in:

/var/log/propel/idm

File Name	Content Description
console.log	Authentication events.
idm.log	Authentication events.

UI services logs

Each UI service (for example, portal and launchpad) logs into a single log file named after the service:

- /var/log/propel/launchpad/launchpad.log
- /var/log/propel/portal/portal.log
- /var/log/propel/catalog-ui/catalog-ui.log
- ...

You can configure logging in service configuration (app.json):

- **consoleJson** - If `true`, log messages are logged in JSON format. The default value is `false`.
- **consoleLevel** - Sets logging level. Change this to `debug` or `trace` to get more information about service activity. The default value is `info`.

Note: 1. Starting with HPE Propel 2.20, logging is handled at the `systemd` service level. Each UI service is expected to output all log messages into the standard output, from where it's being redirected to a log file named after the service. Two considerations are:

- Make sure you use `systemctl` to start the service, otherwise, logs will not be persisted anywhere.
- Before HPE Propel 2.20, each service logged into two files - `server.log` and `console.log`. Starting with HPE Propel 2.20 these two log files are merged into one.

Note: 2. In HPE Propel 2.20, the log format is changed from JSON to plain-text. Set **consoleJson** to `true` to change back to JSON, if needed.

List of UI services

- `apidoc` - API Documentation
- `autopass-ui` - License
- `bpm-ui` - Business Processes
- `catalog-ui` - Catalogs, Catalog Items, Categories, and Policies
- `diagnostics-ui` - Diagnostics
- `idm-admin` - Identity Management
- `launchpad` - Launchpad
- `portal` - Shop, Requests, Orders
- `subscription-ui` - Services
- `sx-client-ui` - Request Support and Knowledge Management
- `sx-ui` - Catalog Connect, Content Management, and Suppliers

HPE SM item types supported by HPE SX

Two HPE Service Manager (HPE SM) item types are supported by the current version of HPE SX: Changes and Quotes. See the following for details:

- How to discern supported items in HPE SM
- Quotes order processing in HPE SM
- Changes order processing in HPE SM

How to discern supported items in HPE SM

Look at the item in HPE SM, and view the details in the **Service Catalog > Administration > Manage Catalog** section under the **Connector Details** tab. To function correctly with HPE SX, an item should have the following attributes:

Changes:

- **Interface Type**: Open a Change
- **Create Subscription**: Checked

Quotes:

- **Interface Type**: Open New Request
- **Create Subscription**: *NOT* checked

Quotes order processing in HPE SM

The expected process advancement of a Quote Offering order in HPE SM is:

1. The Offering Item order is started and an Interaction is created in HPE SM.
2. An interaction starts in **Open - Idle** status.
3. It then moves to the **Open - Linked** state, which indicates a Quote was created for the Item and it is now linked with the Interaction.
4. The Quote starts in the **Initial** state and its Approval Status is set to **Manager Approval**.
5. After an Approval, the Quote's status changes to **Ordering**.
6. Now all Line Items defined for this Quote (if any) need to be solved.
7. When all Line Items are solved, the Quote moves to the **Customer Follow-up** state.

8. When the Item is received by the Requester, he acknowledges receipt and the Quote moves to the **Closed** state.

- Find the **Interactions** in HPE SM under **Service Desk > Interaction Queue > Search**.
- Find **Quote** details in HPE SM under **Request Management > Quotes > Search Quotes**.

Changes order processing in HPE SM

The Changes ordering functionality is similar to that for Quotes (see above), minus a few steps. See the process description in the following table:

	Change	**Interaction**	**Subscription**
Order by requester		Status: **Open - Idle** Approval Status: **Approved**	
After 30 - 60 seconds	Phase: **Subscription Approval** Status: **Initial** Approval Status: **Pending**	Status: **Open - Linked** Approval Status: **Approved**	Status: **Requested**
Approve by manager	Phase: **Subscription Acceptance** Status: **Initial** Approval Status: **Approved**		
Approve by requester	Phase: **Subscription Acceptance** Status: **Closed** Approval Status: **Approved**	Status: **Closed** Approval Status: **Approved**	Status: **Active**

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 Installation and Configuration Guide (Propel 2.20)

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!

Hewlett Packard
Enterprise