HP Propel

Software Version: 2.01

Installation and Configuration Guide

Document Release Date: September 2015
Software Release Date: September 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

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: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

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

HP 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 HP Propel, which includes the HP Propel virtual machine (VM).

Audience

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

- Working with VMware ESX Server 5
- Installing OVA packages
- Deploying 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 HP Propel:

- HP Propel requirements: *HP Propel System and Software Support Matrix*
- HP Propel latest features and known issues: *HP Propel Release Notes*
- HP Propel system administration: *HP Propel Administration Guide*
- HP Propel Catalog Aggregation: *HP Propel Catalog Connect Help*
- HP Propel Portal: *HP Propel Portal Help*
- HP Propel troubleshooting tips: *HP Propel Troubleshooting Guide*
- HP Propel security considerations: *HP Propel Security Guide*

These guides are available from the HP Software Support website at: https://softwaresupport.hp.com.

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.hp.com/documents/10180/14684/HP_Software_Customer_Support_Handbook/

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

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

Before You Begin

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

The HP Propel OVA template contains HP Propel Portal, HP Catalog Aggregation, HP Identity Manager, HP Micro Services (Knowledge Management and Ticket Management), and HP Propel Service Exchange components.

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

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

Note: When working with an HP Propel installation, some default passwords have been updated, while others are the same as in prior releases. For example, the default `root` password has been updated to match the current calendar year. However, the default keystore password remains as it was in the 1.xx releases. If the 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 HP Service Manager (HP SM) with HP Propel and using HTTPS: the hostname, the `root` password, and the keystore password for the HP SM system.
- If you are integrating HP Cloud Service Automation (HP CSA) with HP Propel: the hostname, the `root` password, and the keystore password for the HP CSA system .

Preparing Your ESX Server Environment

Before installing HP Propel, you need to make sure your VMware environment has enough resources to instantiate the VM template that is included in the HP Propel product. Refer to the *HP Propel System*

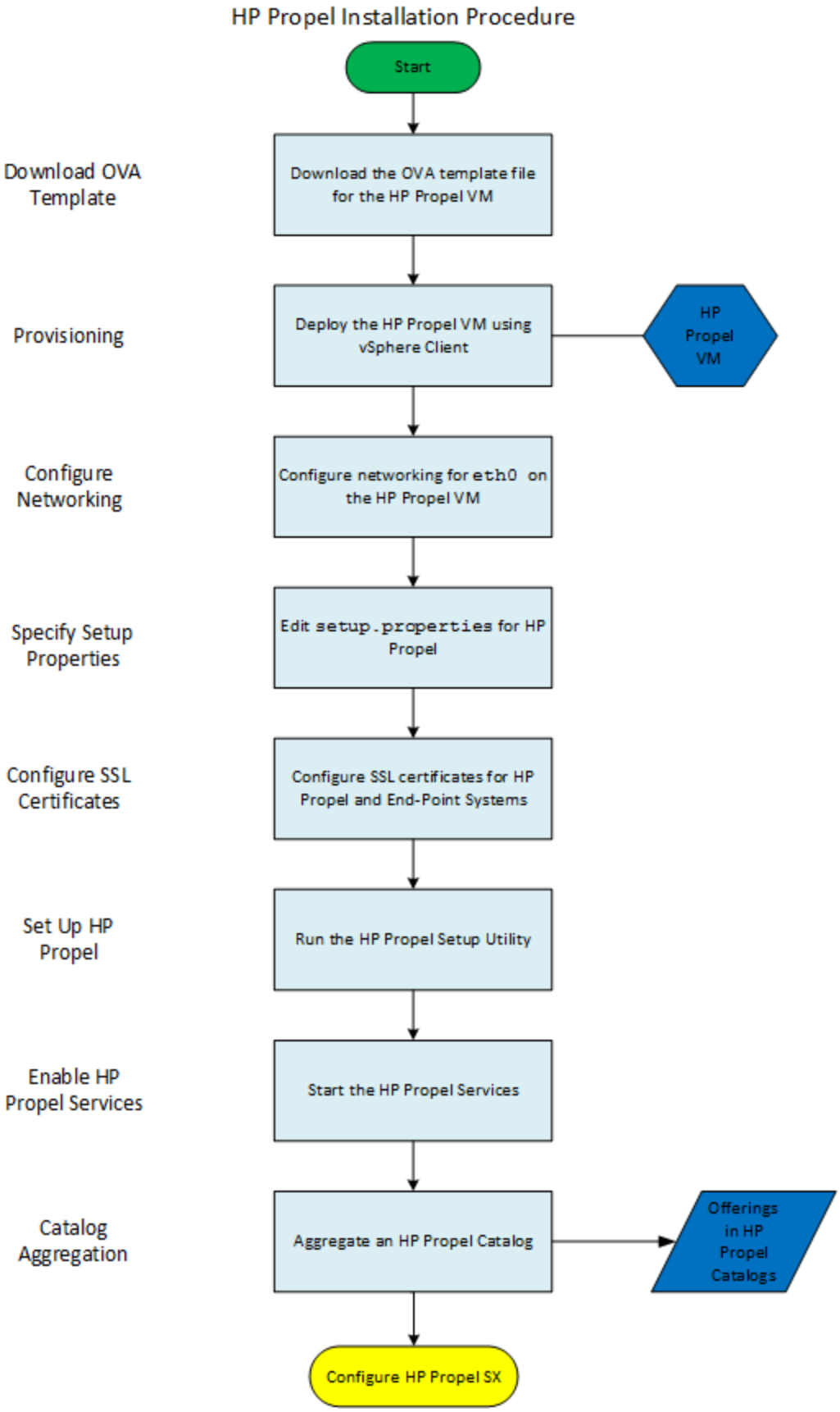
and Software Support Matrix for all HP Propel requirements.

Installation Overview

The general procedure to install HP Propel is:

1. From the HP Software Support website, download the HP Propel OVA template.
2. Using the VMware vSphere Client, deploy the HP Propel VM into the VMware ESX environment by importing the OVA template.
3. Using the VMware vSphere Client, configure the HP Propel VM network adapter.
4. Specify the HP Propel VM hostname and configure networking for `eth0`.
5. Edit the `setup.properties` file for your HP Propel environment and end-point systems.
6. Configure Secure Socket Layer (SSL) communication.
7. Run the HP Propel setup tool.
8. Start the HP Propel services.

The following figure shows the general HP Propel installation process.


HP Propel Installation Procedure
Start
Download OVA Template
Download the OVA template file for the HP Propel VM
Provisioning
Deploy the HP Propel VM using vSphere Client
HP Propel VM
Configure Networking
Configure networking for eth0 on the HP Propel VM
Specify Setup Properties
Edit setup.properties for HP Propel
Configure SSL Certificates
Configure SSL certificates for HP Propel and End-Point Systems
Set Up HP Propel
Run the HP Propel Setup Utility
Enable HP Propel Services
Start the HP Propel Services
Catalog Aggregation
Aggregate an HP Propel Catalog
Offerings in HP Propel Catalogs
Configure HP Propel SX

HP Propel Installation

Tip: To assist copying and pasting commands from these installation instructions into your HP Propel virtual machine's (VM) terminal window, set the `$PROPEL_VM_HOSTNAME` environment variable to the HP 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 HP Propel VM. (This environment variable is temporary and needs to be set after rebooting the HP Propel VM.)

Perform the following steps to install HP Propel:

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

   Tip: To verify the GPG code signing of the OVA file, download the `.sig` file and the two HP public key files, then refer to the *HP Propel Administration Guide* for details.

2. On the ESX server, use the VMware vSphere Client to deploy the OVA image into the HP Propel virtual machine (VM):
   - Click **File->Deploy OVF Template...**
   - Select the HP Propel OVA file that you downloaded.
   - Specify a name and location for the HP Propel VM and deploy.
3. After the HP Propel VM has been deployed and is available, use the VMware vSphere Client to edit the VM properties. Click the **Getting Started** tab, and then click **Edit virtual machine settings**. Click **Network adapter 1** in the Virtual Machine Properties window, and change the network label to the network configured for the ESX server.
4. Power on the HP Propel VM.
5. Click the **Console** tab in the VMware vSphere Client, and log in to the HP Propel VM as `root`, using "propel2015" as the password.
6. Specify the HP Propel hostname and configure networking for `eth0` on the HP 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 HP Propel VM. When using the `--configurestatic` option, values for the netmask, gateway, domain, primary DNS server, and backup DNS server

must be provided.

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

Where `$PROPEL_VM_HOSTNAME` is the fully qualified hostname you specify for the HP Propel VM.

Important: The hostname of the HP 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.

Note: A `Host SMBus controller not enabled!` message might appear for a few minutes in the console with no apparent reboot progress. This is due to the output of the reboot being in quiet mode. Wait at least 10 minutes for the reboot to complete and a login prompt to appear in the console.

7. Verify that you have a configured IP address on `eth0` for the HP Propel VM. You can accomplish this with the `nslookup` and `ifconfig` commands. If the HP Propel VM does not have a configured IP address, take corrective action to resolve the problem.

8. To resolve an issue with the missing Apache `mod_ssl` package, perform the following steps on the HP Propel VM:
   a. Edit the `/etc/yum.conf` file and add a proxy server. For example, add lines similar to:
   ```
   proxy=http://your-proxy-server.example.com:8080
   # The account details for yum connections, if required:
   #proxy_username=yum-user
   #proxy_password=querty
   ```
   b. Run the following command to install the Apache `mod_ssl` package:
   ```
   # yum install mod_ssl
   ```
   (Reply "y" to confirm the package installation.)

9. On the HP Propel VM, edit the `setup.properties` file, entering your unique values for the end-point systems that need to be integrated with HP Propel. This file controls the setup process and is located in the `/opt/hp/propel-install` directory. It has the format of Java properties, supports comments (lines beginning with "#"), and allows simple property assignments. See the example below.

   Important considerations for the `setup.properties` file are:

   - The `setup.properties` file can contain only one instance of HP SM and HP CSA (end-point) systems. Any additional instances must be added into the relevant `instances.json` file. For

details of adding additional instances, see "Adding additional HP CSA instances " on page 29 and "Setting up HP SX to work with HP SM" on page 34.

- HP recommends that HTTPS is configured in the `setup.properties` file for both HP SM and Knowledge Management integration. Note that the HTTPS port used for HP SM integration must also be added to the `sm.cfg` file (`httpsPort` parameter) on the HP SM system.

Example `setup.properties` File

```
require=postgresql,nodejs,sxWar,idmService,catalog-ui,subscription-ui,
subscription,idmAdmin,msvc,oo,km,sxUI,sxClientUI,launchpad,autopassUI,
portal,mpp,catalog,search,eula,osrb,cryptoUtil-cli,
diagnostics,diagnosticsUI,ganglia,hystrixDashboard,centos

### Knowledge Management
# km.url=
# km.attachUrl=
# km.user=
# km.password=

### LWSSO properties
## will use domain from sx.endpoint if not set
#sx.lwssoDomain=
sx.lwssoInitString=LWSSO_INIT_STRING

### whether certificates should be validated or not.
sx.skipCertificateValidation=false

### oo/properties.json
## Setting the mail properties is mandatory for proper sx functionality.
sx.smtpHost=localhost
sx.smtpPort=25
sx.smtpFrom=${hostname}@propel.hp.com
sx.emailBcc=
sx.smtpUser=
sx.smtpPassword=

### sm/instances.json
## If HP Service Manager is used uncomment and set sx.sm properties
## accordingly.
# sx.sm.url=https://smHostname:13443/SM
# sx.sm.user=
# sx.sm.password=
# sx.sm.withProcessDesigner=false

### csa/instances.json
## If HP Cloud Service Automation is used uncomment and set sx.csa
## properties accordingly.
# sx.csa.url=https://csaHostname:8444/csa
```

```
# sx.csa.organization=
# sx.csa.user=
# sx.csa.password=


### infrastructure.json
## Don’t change (uncomment) oo.* properties unless an external
## HP Operation Orchestration server is used
## Set your own credentials only if they have been changed in OO accordingly
# oo.user=admin
# oo.password=changeit

## When using external rabbitmq-server change all rabbit.*
## properties accordingly.
## If local rabbitmq-server is used don’t change rabbit.host value
## (credentials will be created during installation)
rabbit.host=localhost
rabbit.user=rabbit_sx
rabbit.password=propel2014

### default configuration for single OVA mode
## parameter value from installer will be used (--hostname).
## Do not change unless you know what you are doing.
oo.endpoint=http://${hostname}:8080/oo
launchpad.endpoint=https://${hostname}:9000
autopassUI.endpoint=https://${hostname}:9300
sxUI.endpoint=https://${hostname}:9400
sxClientUI.endpoint=https://${hostname}:9410
sx.endpoint=https://${hostname}:9444/sx
autopass.endpoint=https://${hostname}:9444/autopass
idmAdmin.endpoint=https://${hostname}:9200
idm.endpoint=https://${hostname}:9600/idm-service
mpp.endpoint=https://${hostname}:8089
portal.endpoint=https://${hostname}:9010
msvc.endpoint=https://${hostname}:9100
catalog.endpoint=https://${hostname}:9510
catalogUI.endpoint=https://${hostname}:9500
subscription.endpoint=https://${hostname}:9595
subscriptionUI.endpoint=https://${hostname}:9700
search.endpoint=https://${hostname}:9040
diagnostics.endpoint=https://${hostname}:9810
diagnosticsUI.endpoint=https://${hostname}:9800
ganglia.endpoint=https://${hostname}:443/ganglia
hystrixDashboard.endpoint=https://${hostname}:9444/hystrix-dashboard

autopass.allowASPCLicenses=true
```

10. SSL configuration is required for HP Propel. Perform one of the SSL alternatives in this step.

    HP recommends that HTTPS is configured for communication between HP Propel and end-point systems. Important considerations for HP Propel SSL configuration are:

    - HTTPS is required for integration with HP Cloud Service Automation (HP CSA), and though it is not required for HP Service Manager (HP SM), HTTPS is recommended for security.
    - When working with SSL certificates, HP recommends reviewing the certificate-signing algorithms used and ensuring that strong encryption is implemented. For example, SHA1 is sometimes used, and instead, stronger algorithms such as SHA256 should be used. (For details of additional SSL considerations, refer to the *HP Propel Administration Guide*.)
    - You can use your own Certificate Authority-signed certificates or HP Propel's generated Certificate Authority-signed certificates.

    a. There are three alternatives for configuring SSL for HP Propel. Choose one of the following methods:

        - Use the HP Propel utility that generates HP Propel CA-signed SSL certificates. This alternative is recommended if you do not have CA-signed certificates and you want to get HP Propel quickly operating. Continue with **step 9b** to use the automated utility.
        - Use SSL certificates from an existing CA. Use this alternative if you already have the SSL certificates from the CA or if you are submitting a certificate signing request (CSR) to a CA for CA-signed SSL certificates. Perform the instructions in "SSL Configuration Using Existing Certificate Authority" on page 92, then continue with step 10 below.
        - Manually create and configure the SSL certificates. Perform the instructions in "Manual SSL Configuration" on page 94, then continue with step 10 below.

    b. To configure HP Propel with SSL certificates that are generated by HP Propel, use the `propel-ssl-setup.sh` utility. Important considerations for the `auto` option of the `propel-ssl-setup.sh` utility are:

        - By default, a host certificate that is signed using the SHA1 signing algorithm is generated. For environments requiring stronger security, consider generating certificates manually with stronger signing algorithms, such as SHA256
        - The HP CSA and HP SM URLs that are configured in the `setup.properties` file are used to retrieve the end-point systems' SSL certificates, and then import the end-point systems' SSL certificates into the HP Propel's truststore (`propel.truststore`).
        - You can specify the fully qualified hostname of the HP Propel VM in either of the following ways:
            - Specify the hostname with the `--hostname` option.
            - Manually replace all occurrences of `${hostname}` in the `setup.properties` file prior to running the `propel-ssl-setup.sh` utility.

To configure HP Propel with SSL certificates that are generated by HP Propel, log in to the HP Propel VM as `root`, and run the following command from the `/opt/hp/propel-install` directory:

```
# ./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 HP 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 HP Propel CA, not your HP Propel VM; it is not used for the hostname.
- All fields must be separated with a slash ("/").

11. On the HP Propel VM, navigate to the `/opt/hp/propel-install` directory and run the HP Propel setup utility as `root`:

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

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

12. Start the HP Propel services:

    ```
    # propel start
    ```

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

- HP 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 HP 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 HP Propel software, including the Postgres databases.

Continue with "Next Steps" on page 17 to begin the HP Propel configuration for your specific environment.

Next Steps

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

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

- **Shopping** – To configure shopping for HP Propel, the following needs to be completed:
  a. *Configure SSL trust with the end-point system*. HP Propel integrates with multiple end-point systems so that their offerings can be aggregated into catalogs and fulfilled by HP Propel consumers. During fulfillment, end-point systems may send notifications via HTTPS; therefore, these end-point systems must trust the HP Propel system.
     - An HP Cloud Service Automation (HP CSA) system requires SSL trust. To integrate HP Propel with an HP CSA system, see "SSL Configuration for HP CSA Integration" on page 96 for instructions to import the HP Propel certificate into the HP CSA system's truststore.
     - HP recommends that you configure HTTPS for HP Propel integration with HP Service Manager (HP SM). To integrate HP Propel with HP SM, see "SSL Configuration for HP SM Integration" on page 97 for instructions to import the HP Propel certificate into the HP SM system's truststore.

  b. *Configure Catalog Aggregation and create a new catalog*. Offerings from end-point systems are contained in catalogs in HP Propel. For instructions to aggregate offerings into catalogs, refer to the *HP Propel Catalog Aggregation Help* in the HP Propel Management Console.

- **Ticketing** – The HP 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 HP Service Manager, refer to the *HP Propel Administration Guide* for instructions.

Additionally, you can improve HP Propel security by changing the default user accounts' passwords. Though this is an optional task, HP recommends that you change the default passwords. Refer to the *HP Propel Administration Guide* for instructions.

Important: HP Propel Service Exchange must be configured. Continue to "HP SX Configuration after VM install" on page 18.

HP SX Configuration after VM install

HP Propel Service Exchange (HP SX) is the component that brings the Propel experience together, integrating the portal, catalog, and end-point fulfillment engines to enable functional integration with multiple providers. HP 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, HP SX needs some configuration. This involves some or all of the following:

- Examine and edit the three configuration files that HP SX needs in order to run correctly, see "HP SX Basic configuration" for details.
- Add any additional HP CSA and HP SM instances you wish connected to HP Propel, see "Adding additional HP CSA instances " and "Adding additional HP SM instances".
- Add any HP SAW instances you wish connected to HP Propel, see "Connecting HP SAW to HP SX".
- Set HP SX user roles and organizations to allow viewing of HP SX management and Testing UIs "Setting User roles and Organizations".
- Run HP SX Self-test 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. **Self-test** is located on the top level of the HP SX management UI, see "Self-test HP SX configuration" for details.
- If you are using HP CSA, check through "Connecting HP CSA to HP SX" for any necessary LDAP and Approval configuration required.
- If you are using HP SM, check for further configuration steps required both in your HP SM instance and in HP SX, see "Connecting HP SM to HP SX".
- If you want to enable Case Exchange (CX) functionality see "Configuring Case Exchange".
- View and manage HP SX content packs ("HP SX Content Management") and adapters ("HP SX Adapters").

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

HP SX Basic configuration

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

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

instances.json

Each adapter needs its own `instances.json` file. These files are located on a classpath in the `[%SX_HOME%] /WEB-INF/classes/config/{adapterType}/` directory. They contain connection information for the remote systems and how they will integrate with HP SX.

The structure varies for different system types. See the sections that cover the specific system's setup for details.

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

A few examples:

CSA

```
  {

        "CSA-instance": {

            "endpoint": "https://mpavm0011.wren4labs.adapps.wren4.com:8444/csa", //
url to remote system's API

            "user": { // login information

            "loginName": "admin",

            "password": "propel"

          },

          "organization": "CSA_CONSUMER"

      }
  }
```

JIRA

```
  {

         "JIRA-instance": {
```

```
            "endpoint": "http://mpavmint01.wren4labs.adapps.wren4.com:8080", //
url to remote system's API
            "user": { // login information
                 "loginName": "System.admin",
                 "password": "noname"
            }
         }
   }
```

SAW

```
  {
        "SAW-instance": {
             "endpoint": "https://wren4003sngx.saas.wren4.com", // url to remote
system's API
             "user": { // login information
                   "loginName": "robin.friend@wren4.com",
                   "password": "1Q2w3e4r5t6y"
         },
         "r2fEnabled": "true",
         "organization": "689570538"
     }
  }
```

SM

```
  {
     "SM-instance": {
          "endpoint": "http://mpavmsmapp05.wren4labs.adapps.wren4.com:13080/SM",
// url to remote system's API
          "user": { // login information
              "loginName": "falcon",
              "password": "changeit"
         },
         "withProcessDesigner": true, // has this instance Process Designer
extension installed or not?
         "useLwsso": true // should SX use Lightweight SSO to login to SM?
      }
  }
```

infrastructure.json

This file is located on a classpath in the [%SX_HOME%]/WEB-INF/classes/config directory. It contains information about HP 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 HP 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.password=ENC(4w0oS736xObjhMmJTCq87Q\=\=)

db.url=jdbc\:postgresql\://localhost\:5432/sx

db.username=sxuser

security.encryptedSigningKey=propel

security.idmHostname=mpavmcsa05.hpswlabs.adapps.hp.com

security.idmPort=9600

security.idmProtocol=https

security.idmTenant=CONSUMER

security.idmTransportUser=idmTransportUser

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

skipCertificateValidation=false

sx.catalog.notifications.queue=CN

sx.content.oo.delete=true

sx.content.oo.init=checkVersion

sx.content.oo.upload=always

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.mock.requests.queue=MOCK
sx.oo.callback.queue=OC
sx.oo.configuration=oo/properties
sx.oo.invocations.queue=OO
sx.oo.organizationCache=300
sx.queue.main=SX
sx.queue.prefix=${PROPEL_HOSTNAME}
sx.queue.selftest=SELFTEST
sx.storage.location=/datastorage
sx.ticketing.forbidAttachmentExtensions=exe,bat,cmd,com
sx.ticketing.maxAttachmentSize=50000000
sx.url=https\://${PROPEL_HOSTNAME}\:9444/sx
```

Parameters for HP SX internal database configuration

Property name	Description
db.dialect	Configuration of db connection. Dialect for 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 HP SX security configuration

Property name	Description
security.encryptedSigningKey	It will be encrypted at first start of 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 SX starts.
skipCertificateValidation	Whether SX should validate ssl certificates.

Parameters for HP 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 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 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 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 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 SX instances so that they use their own queues.
sx.queue.main	Main SX RabbitMQ queue.
sx.url	SX URL.
sx.ticketing.maxAttachmentSize	Maximum size for ticket attachements.
sx.ticketing.forbidAttachmentExtensions	Comma separated list of forbidden file extensions for ticket attachements.

Self-test HP SX configuration

Use the **Self-test** utility to check for correct configurations, connections and file version details.

Log in to the HP SX administrator's UI (`https://$PROPEL_VM_HOSTNAME:9444/sx`), then click **Self-test**. A script runs, checking the connections with:

- HP SX url
- HP IdM
- HP Propel catalog
- HP SM and HP CSA instances
- OO mappings
- AMQP configuration

For HP SM instances, **Self-test** also checks versions of all installed unload files, and lists them.

> **Tip**: Additionally, the **Propel Component Versions** utility on the HP SX administrator's UI can provide helpful component information when working with HP Support.

The following example shows **Self-test** results, including an error:

Check AMQP configuration
Check AMQP connection : **OK**
Check message listeners : **OK**

Check configuration: csa/instances.json
Check instance badcop_hpswlabs_adapps_hp_com : **OK**

Check configuration: sm/instances.json
----------**ccue-qa-sm3_hpswlabs_adapps_hp_com**----------
Check instance ccue-qa-sm3_hpswlabs_adapps_hp_com is accessible : **OK**
Check instance ccue-qa-sm3_hpswlabs_adapps_hp_com - checking unload files ... :
Unload 'SXR2FCustomizations' in version '1.01.2' ... **OK**
Unload 'SXR2FDB' in version '1.01.3' ... **OK**
Unload 'SXR2FExtAccess' in version '1.11.6' ... **OK**
Unload 'SXBaseCustomizations' in version '1.01.1' ... **OK**
Unload 'SXBaseDB' in version '1.01.13' ... **OK**
Unload 'SXBaseExtAccess' in version '2.00.1' ... **OK**
Unload 'SXUnloadChecker' in version '1.01.1' ... **OK**
Unload 'SXTicketing' in version '1.01.3' ... **OK**
Unload 'SXCaseExchange' in version '1.01.11' ... **OK**
Unload 'SXPDCaseExchange' in version '1.01.3' ... **OK**

Check configuration: sx.properties
Check security.idm : **OK**
Check catalog.notification : **OK**
Check sx.url : **OK**

Check configuration: oo/properties.json
Check properties : **OK**
Check SMTP connection : **OK**

Check configuration: tenantInstanceMappings.json
Check DEFAULT.instanceName : **OK**

Check configuration: infrastructure.json
Check OO.endpoint : **OK**
Check REST.endpoint : **OK**
Check REST.operationEndpoint : **OK**
Check REST.csaNotificationEndpoint : **OK**
Check SERVICE_CATALOG.requestCallbackEndpoint : **OK**
Check SERVICE_CATALOG.subscriptionCallbackEndpoint : **ERROR:** Invalid credentials
Check SERVICE_CATALOG.internalCallbackEndpoint : **OK**

Note: See the *HP Propel Troubleshooting Guide* for troubleshooting recommendations and tips for the entire HP Propel product.

Connecting HP CSA to HP SX

Adding additional HP CSA instances

During install, the `setup.properties` file adds one HP CSA instance to the appropriate configuration JSON file. However, it is possible to connect any number of instances of HP CSA to HP SX. To add additional HP CSA instances the following file must be edited manually:

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

Required fields: endpoint, loginName and password

> **Note**: The instance (for example, `CSAEurope1` below) in the `instances.json` file must not exceed 50 characters.

Assuming CSAEurope1 was added through the `setup.properties` file during install, add additional instances as in the *CSAEurope2* example below.

NOTE: Enter your unique instance names, URLs, loginNames and passwords in place of the values in italics in the CSAEurope2 section below.

Example:

```
{
    "CSAEurope1": {
        "endpoint": "https://example1.com:8444/csa",
        "user": {
            "loginName": "johndoe",
            "password": "mypassword"
        },
        "organization": "CSA_CONSUMER"
    },

    "CSAEurope2": {
        "endpoint": "https://example2.com:8444/csa",
        "user": {
            "loginName": "janedoe",
            "password": "my2password"
        },
        "organization": "CSA_CONSUMER"
    }
```

IMPORTANT: For a specific module to use the correct instance, relevant configuration files must be edited to include the appropriate HP CSA instance names.

LDAP and Approval settings

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

- "Configure HP CSA to use LDAP" on page 31
- "Configure HP CSA Approval settings" on page 32

Configure HP CSA to use LDAP

1. Login to HP 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 HP CSA Approval settings

1. Login to 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** (ie. Named Approver Template) and add **Approver**.
6. Save the policy.

Connecting HP SM to HP SX

Setting up HP SX to work with HP SM

Adding additional HP SM instances

During install, the `setup.properties` file adds one HP SM instance to the appropriate configuration JSON file. However, it is possible to connect any number of instances of HP SM to HP SX. To add additional HP SM instances the following file must be edited manually:

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

Required fields: endpoint, loginName and password

> **Note**: The instance (for example, `SMEurope1` below) in the `instances.json` file must not exceed 50 characters.

Considerations for the `instances.json` file:

- In version 1.0 there was a 'db' section in this file for direct JDBC connection. This is no longer supported and needs to be removed from the configuration file.
- Instances of HP SM with Process Designer installed must have the `withProcessDesigner` parameter set to **true**.
- The example below uses the default port number that HP Propel uses to communicate with HP SM. If you changed the port number, specify yours in the endpoint address in place of *13080.*
- See "Setting up HP SX to use LWSSO" on page 36 concerning the `"useLwsso": true` line in the example.

Assuming SMEurope1 was added through the `setup.properties` file during install, add any additional HP SM instances as in the *SMEurope2* example below. Replace the values in italics with your unique urls, names and passwords.

Example:

```
{
    "SMEurope1":{
        "endpoint":"http://sm1.example.com:13080/SM",
        "user": {
            "loginName": "johndoe",
            "password": ""
```

```
        },
        "withProcessDesigner": true
    },
    "SMEurope2":{
        "endpoint":"http://sm2.example.com:13080/SM",
        "user": {
            "loginName": "janedoe",
            "password": ""
        },
        "useLwsso": true
    }
}
```

Important: For a specific module to use the correct instance, relevant configuration files must be edited to include the appropriate HP SM instance names.

Setting up HP SX to use LWSSO

The above example shows that HP SX is configured to access the SMEurope2 instance via LWSSO. Note that it is not necessary to supply the password in this case. However, to make the LWSSO communication work, it is necessary that the file `[%SX_HOME%]/WEB-INF/classes/config/lwssofmconf.xml` contains proper LWSSO configuration that matches the target HP SM instance. In particular:

- The domain element must contain the common domain for HP SX and the target HP SM instance.
- The initString attribute of the crypto element must contain the same passphrase as the HP SM instance.

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 HP 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 HP SX" on page 75 for further details.

Setting up HP SM to work with HP SX

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

Import SX Unload scripts

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

1. In your HP 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 43 to understand what customizations each HP SM unload pack contains. Consider checking all the changes made by the unload scripts to verify your HP SM configuration is correct.

HP SX Unload files

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

SXTicketing.unl

Description: Changes for Ticketing feature. Customizes SOAP/REST interfaces:

- **SXGlobalLists** - provides access (add, delete, save) to globallists for HP SX.
- **SXActivityServiceMgt** - provides access (add) to activityservicemgt HP SM item for HP SX - exposes Activity Lines in Interaction Items. It is used for storing comments in Tickets.
- **SXTicketInteraction** - provides remote access to Interaction (incidents) HP SM items for HP SX - this is a duplicate of SXInteraction remote interface (with a line added to Expressions tab: *$G.ess=true*). This is needed ONLY to escalate Tickets in HP SM.

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 HP SM object for HP SX.
- Adds new REST endpoint SX/SXCE_IncidentActivity - providing remote access to activity HP SM object for HP 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 HP SM 9.33 and older. For newer versions of HP 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 HP SM with Process Designer. Note that both this file and `SXCaseExchange.unl` are mandatory for HP 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/SXBaseDB.unl`
- `./sx-base/sm/SXBaseExtAccess.unl`
- `./sx-base/sm/SXUnloadChecker.unl`

- `./sm-ticketing/sm/SXTicketing.unl`

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

Manual configuration for Case Exchange

Add **Add** activity privileges to the user account HP 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**.

HP SM Process Designer - additional manual configuration

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

1. Login 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.

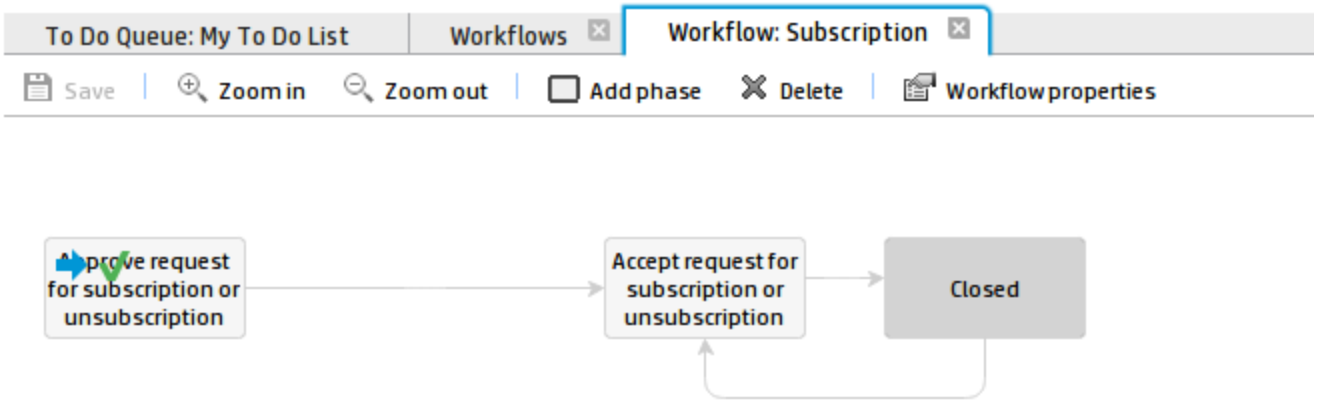
5. Connect the first and third phases by relation.

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

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 HP 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 HP SM instance is accessed via LWSSO.

Modify Change and Request profiles used by your Approvers

1. Login 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. Login 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 HP SM.

1. Login 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 HP Propel VM

1. Download the HP 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 --import -file sm.crt -keystore /usr/lib/jvm/java-1.8.0/jre/lib/security/cacerts -alias sm_host`

3. Enter the password *changeit*.

4. Enter *yes*.

Setup LDAP

When LDAP has been configured in HP 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. Login into HP SM.

2. Logout.

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

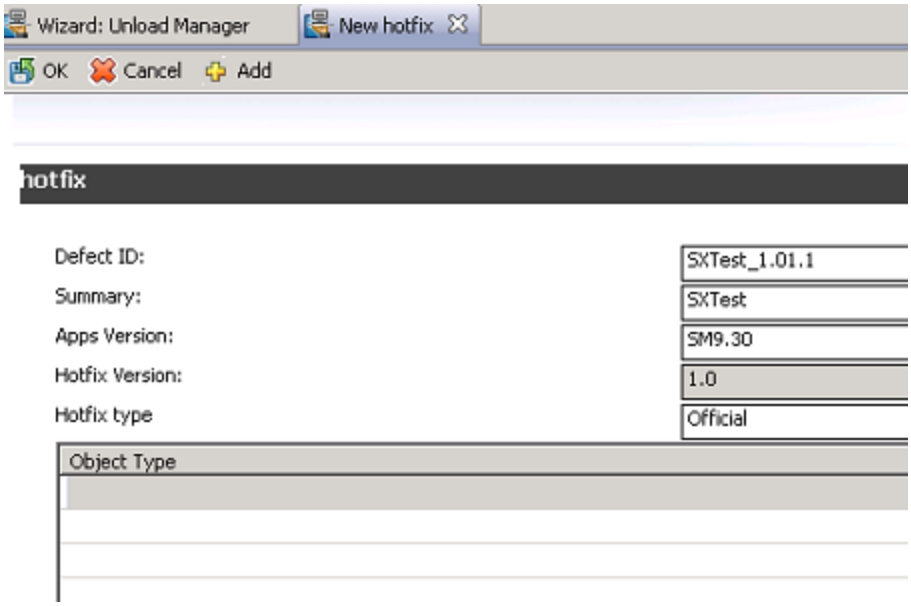
If you develop your own HP SX content and make modifications to your HP SM instance, you will need to export these modifications into your own new unload file, or create a new version of an unload file. Using unload files enables you to backup changes and transfer them to other HP SM instances.

NOTE: After creating a new unload file, edit and then run **Self-test** to check that you have all the latest versions of files installed, see "Using Self-test to check unload versions " on page 55.

Creating unloads in HP SM Unload manager

1. In **System Administration > Ongoing maintenance > Unload manager** select **Create Unload**.

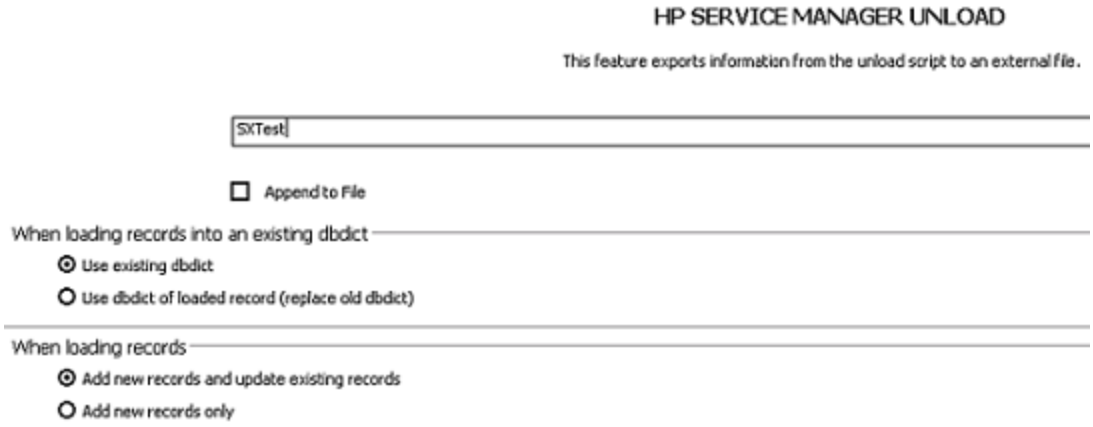
   - **Defect ID** - Use this field to hold the version of the unload file. Versions must be unique and follow this format: <*unl_file_name*>_<*version*>. For example: *SXBaseCustomizations_1.01.1*.
   - **Summary** - Enter a name for the unload file, without file extension.
   - **Apps version** and **Hotfix 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 HP 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 42.

Using Self-test to check unload versions

As well as checking for correct connections and configurations, HP SX Self-test checks the current versions of unload files, listing them in the output file. For this to happen, `SXUnloadChecker.unl` must be applied, and `metadata.json` edited to include all current unload file versions.

Before using the SX Self-test to check versions:

1. Apply `SXUnloadChecker.unl` to your HP 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. Run the HP SX Self-test, see "Self-test HP SX configuration" on page 26.
4. Verify that the versions of unload files listed are your latest.

Connecting HP SAW to HP SX

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

NOTE: Any HP SAW instance to be integrated into HP 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 "HP SX Basic configuration".

HP SAW Setup for Case Exchange

First it is necessary to add a definition of an External System into HP SAW. The name of this External System is the name that will be used to identify the HP SAW system in the necessary HP 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 HP 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 HP SAW to HP 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 HP 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 HP SAW systems to work with HP 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 HP SAW systems to HP 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 HP 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 HP 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 HP 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 HP 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 HP 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 HP 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 HP 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 HP 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

HP 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 HP 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 HP SX are described below.

The roles valid for the HP 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 HP 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 HP SX UI pages.

To assign or change HP SX user roles, see "Role association" on page 62.

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 HP 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.

HP SX Content Management

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

Content packs can be deployed into HP 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 HP 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.

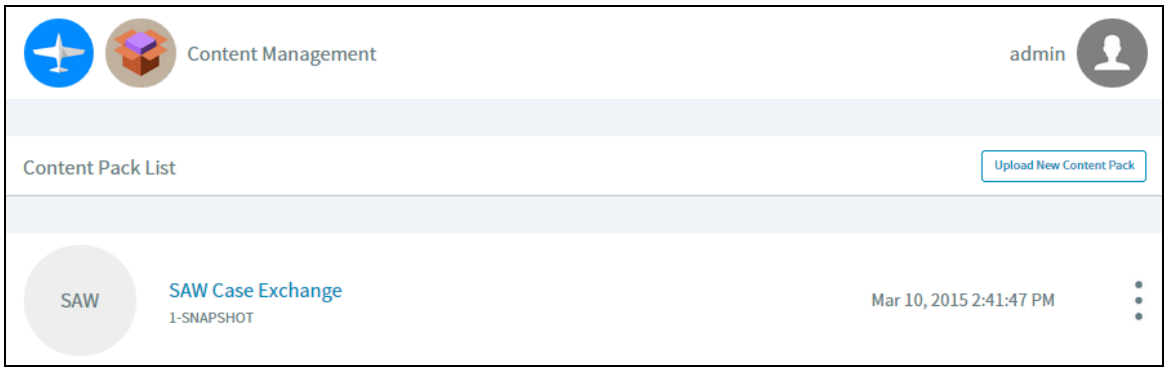
HP SX offers out-of-the-box functionality through content packs that can be used as-is or customized. The HP SX Content Management user interface allows you to view, download, upload and delete content packs in HP SX. Access to this UI is limited to users with the appropriate user roles, see "Setting User roles and Organizations" on page 61. Upload and delete operations include upload or removal of relevant HP Operation Orchestration JAR files (HP OO content packs), and the merging of HP SX customizations into the running HP SX server.

"Content Packs and their contents" for the out-of-the-box content packs, and the *HP 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 HP Propel as the `admin` user at `https://$PROPEL_VM_HOSTNAME:9000/org/Provider`.
2. Click the **Content Management** application from the HP 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, HP SX replaces the existing version. Content packs are identified by an ID attribute provided in their metadata file.

Content Packs and their contents

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

- *SM request to fulfillment* (**sm-r2f**) - the content pack providing files for HP SM requests to fulfillment.
- *Service Exchange base content* (**sx-base**) - the base content for HP 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 HP SM-related functions of HP SX UI.
- *SAW Case Exchange* (**saw-case-exchange**) - the content pack providing files for HP SAW Case Exchange customizations.
- *SAW Ticketing* (**saw-ticketing**) - the content pack providing files for HP SAW ticketing.
- *SM Case Exchange* (**sm-case-exchange**) - the content pack providing files for HP SX Case Exchange customizations.
- *SM Ticketing* (**sm-ticketing**) - the content pack providing files for HP SM ticketing.
- *Case Exchange* (**case-exchange**) - the content pack providing files for HP 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 HP SAW-related functions of HP SX UI.
- *CSA request to fulfillment* (**csa-r2f**) - the content pack providing files for HP 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 HP CSA related functions of HP SX UI.
- *OO request to fulfillment* (**oo-r2f**) - the content pack providing files for HP OO requests to fulfillment (r2f).
- *SAW request to fulfillment* (**saw-r2f**) - the content pack providing files for HP SAW requests to fulfillment (r2f).

HP SX Case Exchange (CX)

CX is a subsystem of HP 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 HP SM and HP 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 HP SX, and system B and HP 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 HP SM instance called SM03 and an HP 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 for Remedy) is being written, the adapter can be implemented to support Case Exchange, see the *HP 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 HP SM instance is referring to an entity in another HP SM instance. If a referring entity is changed in one HP SM instance, HP SX is notified and registers a listener for entity changes in the other (referred) HP SM instance.

Examples of SX Case Exchange supported use cases:

1. An administrator can configure 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 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) SX operations to:
    - register/unregister new entity change listener in external systems
    - store mapping from entity {instanceTypeA}:{instanceA}:{entityTypeA}:{entityIdA} to {instanceTypeB}:{instanceB}:{entityTypeB}:{entityIdB}
    - remove mapping from/to entity {instanceType}:{instance}:{entityType}:{entityId}

Configuring Case Exchange

This requires two procedures:

- "Configure HP SM" on page 74
- "Configure HP SX" on page 75

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

Configure HP 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 HP 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, HP 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 HP 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 HP 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 HP 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 HP 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 HP 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.

HP SX Adapters

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

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

- SX adapter - the internal SX adapter. This is always the first adapter and implements the HP SX CX functionality.
- SM adapter - specifically for HP SM end-point systems.
- CSA adapter - specifically for HP 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 *HP Propel Service Exchange SDK*.

Enabling an HP SX adapter

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

Install an adapter:

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

1. Stop HP SX:

   ```
   # 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 HP SX:

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

Manually configure HP SX-required files

Note: If you followed the HP 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" on page 87
- "Configuring for RabbitMQ Server" on page 88
- "Configuring for the HP Propel Portal " on page 89
- "Configuring for IdM" on page 90
- "Configuring for PostgreSQL" on page 91

Configuring for OO server

To set an internal connection to a specific OO server add/edit the OO entry in 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",
   "emailBcc": "joe.doe@example.com"
}
```

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 HP Propel Portal

To enable communication with the HP 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 HP 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`

SSL Configuration Using Existing Certificate Authority

Perform the following steps to configure HP Propel with SSL certificates from an existing Certificate Authority.

Note: The following commands must be executed as `root` on the HP Propel VM.

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

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

   b. Import the CA into the HP Propel keystore:

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

2. Initialize the SSL working directory:

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

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

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

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

   Where

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

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

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

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

5. After you have the certificates from the CA, copy the host certificate to:
`/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt`

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

6. Validate the certificate and the CA match::

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

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

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

7. Create the certificate and the key stores:

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

Important: After you complete this procedure, run the setup tool by continuing with step 10 in the HP Propel installation instructions.

Manual SSL Configuration

This section describes how to manually configure SSL for HP Propel and end-point systems, such as HP Cloud Service Automation (HP CSA) and HP Service Manager (HP SM). These instructions replace the `propel-ssl-setup.sh auto` command, in which HP Propel CA-signed SSL certificates are automatically generated. To manually configure your own SSL certificates:

1. Create the following files:

   - `CA.crt` – the PEM-encoded public X.509 certificate of the CA.
   - `.keystore` – the HP Propel keystore in JKS format that contains the private key for SSL use by the HP Propel VM. (The "CN" field in the subject must contain the fully qualified hostname of the HP Propel VM.) The private key must be certified by the CA, stored with an alias of the form `propeljboss_$PROPEL_VM_HOSTNAME`, and encrypted with the "propel2014" keystore password.
   - `propel.truststore` – the HP Propel truststore in JKS format. It must contain the public keys of all other machines that are trusted by HP Propel (HP CSA and HP SM), the certificate for the Propel VM, and the certificate of the CA that signed it. The certificates must be encrypted with the "propel2014" keystore password.
   - `propel_host.crt` – the PEM-encoded public X.509 certificate for the HP Propel VM that is issued by the CA.

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

   - `propel_host.key.rsa` – a RSA private key (2048-bit by default, in SSLeay format) for the HP Propel VM.
   - `propel_host.pfx` – a cryptography object archive in PKCS#12 format, protected by the "propel2014" password that contains two items:
     (= `propel_host.key.rsa` + `propel_host.crt`).

   These files are used in the following way by HP Propel:

   - Java/Jetty-based components of HP Propel use the `.keystore` and the `propel.truststore` files.
   - Nodejs-based components use the `CA.crt` and the `propel_host.pfx` files.
   - RabbitMQ uses all `propel_host.*` files.

- HP Operations Orchestration Central uses the `propel_host.crt` and the `propel_host.pfx` files.

2. Load the Certificate Authority (CA) into the global Java keystore. This file is in a PEM format, with extensions such as `.pem`, `.crt`, `.cer`, and `.key`.
   a. Copy the file to `/opt/hp/propel-install/ssl-tmp/CA.crt`. (The exact file name must be used.)
   b. Import the CA into the HP Propel keystore:

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

3. Initialize the SSL working directory

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

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

4. Copy the host certificate to `/opt/hp/propel-install/ssl-tmp/$PROPEL_VM_HOSTNAME/out/propel_host.crt`.

   Where `$PROPEL_VM_HOSTNAME` is the fully qualified hostname of the HP Propel VM.

5. Validate the certificate and the CA match:

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

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

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

6. Create the certificate and the key stores:

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

Important: After you complete the manual SSL configuration, run the setup tool by continuing with step 10 in the HP Propel installation instructions.

SSL Configuration for HP CSA Integration

If you are integrating HP Propel with an HP Cloud Service Automation (HP CSA) system, the HP Propel certificate must be imported into the HP CSA system's truststore. Perform the following steps to import the HP Propel CA certificate into the HP CSA truststore:

Note: The following instructions are an example for an HP CSA system on Linux. For an HP CSA system on Windows, file locations and commands are different.

1. On the HP Propel VM, copy the `CA.crt` file to the HP CSA system. For example, run the following command on the HP Propel VM in the `/opt/hp/propel-install/ssl-tmp` directory:

   ```
   # scp CA.crt root@$HP_CSA_HOSTNAME:/tmp
   ```

2. On the HP CSA system, import the HP Propel certificate as a trusted certificate by running the following command:

   ```
   # $HP_CSA_JRE_HOME/bin/keytool -importcert -alias propel_ca -file /tmp/CA.crt
   –trustcacerts –keystore $HP_CSA_CACERTS_HOME/cacerts
   ```

   Where `$HP_CSA_JRE_HOME` is the directory that contains the JRE for the HP CSA system and `$HP_CSA_CACERTS_HOME` is the directory that the `cacerts` keystore file is located. When prompted, type the keystore password. (The default password is "changeit" for the HP CSA keystore.) Reply "*yes*" when prompted to trust the certificate.

3. On the HP CSA system, restart HP CSA so that the newly imported HP Propel certificate will take effect:

   ```
   # service csa restart
   ```

SSL Configuration for HP SM Integration

If you are integrating HP Propel with an HP Service Manager (HP SM) system and using HTTPS, the HP Propel certificate must be imported into the HP SM system's truststore. Perform the following steps to import the HP Propel CA certificate into the HP SM truststore:

Note: The following instructions are an example for an HP SM system on Linux. For an HP SM system on Windows, the `cacerts` file location and the command (or method) to copy the `CA.crt` file are different.

1. On the HP Propel VM, copy the `CA.crt` file to the HP SM system. For example, run the following command on the HP Propel VM in the `/opt/hp/propel-install/ssl-tmp` directory:

   ```
   # scp CA.crt root@$HP_SM_HOSTNAME:/tmp
   ```

   Where `$HP_SM_HOSTNAME` is the fully qualified hostname of the HP SM system.

2. On the HP SM system, import the HP Propel certificate as a trusted certificate by running the following command:

   ```
   # $HP_SM_JRE_HOME/bin/keytool -importcert -alias propel_ca -file /tmp/CA.crt
   –trustcacerts –keystore $HP_SM_CACERTS_HOME/cacerts
   ```

   Where `$HP_SM_JRE_HOME` is the directory that contains the JRE for the HP SM system and `$HP_SM_CACERTS_HOME` is the directory that the `cacerts` keystore file is located, which by default is the HP SM system's `RUN` directory. When prompted, type the keystore password. (The default password is "changeit" for the HP SM keystore.) Reply "*yes*" when prompted to trust the certificate.

3. On the HP SM system, restart HP SM so that the newly imported HP Propel certificate will take effect:

   ```
   # service sm restart
   ```

   Note: For proper HTTPS communication between HP Propel and an HP SM system, make sure that the HP SM system is configured to run in SSL modus. The `cacerts` and other certificates should be configured in the HP SM system's `sm.ini` file.

Troubleshooting

This section offers some general recommendations and troubleshooting tips for HP Propel Service Exchange. See the *HP Propel Troubleshooting Guide* for a more comprehensive listing of troubleshooting recommendations for the entire HP Propel product.

General recommended steps

1. Run Self-test from the HP SX admin UI to check your connections are working and your configuration is correct, see "Self-test HP SX configuration" on page 26.
2. When a problem happens, go first to the relevant log files (for locations see "HP Propel log files" on the next page), and look for any sign of an error.
2. If no error is found, look into the OO Flows input parameters (see "OO Flows" below.) For example, look for wrongly set notification email addresses etc.
3. If you can access it, use the SX Debug UI. If the functionality you tried to perform through the HP Propel Portal is available in the 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 HP 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 HP Propel Portal execution.

Where to find help

- OO Flows
- Log files
- SX Debug UI
- HP SM item types supported by HP SX

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 HP 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.

HP Propel log files

HP SX log files

HP 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.

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

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

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

Jetty server log file

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

HP SX log files

File Name	Content Description
`autopass.log`	HP Propel license management (coordinated by HP SX).

sx-messages.log	HP SX REST endpoint (/operation, /ticket, /request) events.
sx.log	General HP 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	HP SX notifications to HP 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 HP SX.
case-exchange.log	HP SX case exchange-related log, HP CX adapter boot and shutdown, case-exchange content pack reload, entity-change listening registration, and HP SM case-exchange events.

HP 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	HP CSA general log file.
saw-messages.log	HP SAW general log file.
sm-messages.log	HP SM general log file.

HP OO log files

Use to troubleshoot HP OO problems. Located in:

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

File Name	Content Description

wrapper.log	HP OO general log file.
general.log	HP 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.

HP Propel Portal log file

Located in:

/opt/hp/propel/portal/logs

File Name	Content Description
server.log	HP Propel Portal log.

Knowledge Management log file

Note: Starting with HP Propel 2.00, the legacy Marketplace Portal component is used only for Knowledge Management (KM). For HP Propel Portal issues, refer to the HP Propel Portal log file.

Located in:

/opt/hp/propel/mpp/logs

File Name	Content Description
mpp.log	HP Propel KM (previously the MPP) log.

Catalog UI log files

Located in:

`/var/log/propel/catalog-ui/`

File Name	Content Description
`console.log`	HP Propel Catalog UI log.
`server.log`	HP Propel Catalog UI log.

Subscription log files

Located in:

`/var/log/propel/subscription`

File Name	Content Description
`console.log`	HP Propel Subscription log.
`subscription.log`	HP Propel Subscription log.

Subscription UI log files

Located in:

`/var/log/propel/subscription-ui`

File Name	Content Description
`console.log`	HP Propel Subscription UI log.
`server.log`	HP Propel Subscription UI log.

Identity Management log files

Located in:

`/opt/hp/propel/idmAdmin/bin/.idm`

File Name	Content Description
`idm.log`	HP Propel Identity Management log.

Located in:

`/opt/hp/propel/idmAdmin/logs`

File Name	Content Description
`server.log`	HP Propel Identity Management log.

Catalog Connect UI log files

Located in:

/var/log/propel/sx-ui

File Name	Content Description
console.log	HP Propel Catalog Connect UI log.

Located in:

/opt/hp/propel/sxUI/logs

File Name	Content Description
server.log	HP Propel Catalog Connect UI log.

HP Propel SX Client UI log files

Located in:

/opt/hp/propel/sxClientUI/logs

File Name	Content Description
server.log	HP Propel SX Client UI log.

Located in:

/var/log/propel/sx-client-ui

File Name	Content Description
console.log	HP Propel SX Client UI log.
server.log	HP Propel SX Client UI log.

Launchpad log files

Located in:

/opt/hp/propel/launchpad/logs

File Name	Content Description
server.log	HP Propel Launchpad log.

Located in:

/var/log/propel/launchpad

File Name	Content Description
console.log	HP Propel Launchpad log.

Autopass UI log files

Located in:

/var/log/propel/autopass-ui

File Name	Content Description
console.log	HP Propel Autopass UI log.
server.log	HP Propel Autopass UI log.

Diagnostics log file

Located in:

/var/log/propel/diagnostics

File Name	Content Description
console.log	HP Propel Diagnostics log.

Diagnostics UI log files

Located in:

/opt/hp/propel/diagnostics-ui/logs

File Name	Content Description
server.log	HP Propel Diagnostics UI log.

Located in:

/var/log/propel/diagnostics-ui

File Name	Content Description
console.log	HP Propel Diagnostics UI log.

HP Propel Micro Services node server log file

Located in:

/var/log/propel/msvc

File Name	Content Description
console.log	HP Micro Services node server log.

HP SM item types supported by HP SX

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

- How to discern supported items in HP SM
- Quotes order processing in HP SM

- Changes order processing in HP SM

How to discern supported items in HP SM

Look at the item in HP SM, and view the details in the **Service Catalog > Administration > Manage Catalog** section under the **Connector Details** tab. To function correctly with HP 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 HP SM

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

1. The Offering Item order is started and an Interaction is created in HP 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 HP SM under **Service Desk > Interaction Queue > Search**.
- Find **Quote** details in HP SM under **Request Management > Quotes > Search Quotes**.

Changes order processing in HP 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 2.01)

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@hp.com.

We appreciate your feedback!


Java™
COMPATIBLE