

HP Propel

HP Propel Installation and Configuration Guide



For the CentOS Operating System

Software Version 1.00 (July 2014)

Contents

Overview	3
Audience	3
Additional Information	3
Before You Begin	4
Preparing Your Environment for Virtual Machines	4
HP Propel Software and Hardware Requirements	4
HP Propel Product End-Point Integrations	4
Installation Overview	4
HP Propel Installation	7
Configure SSL for HP Propel	9
SSL Certificates Overview	9
HP Propel SSL Certificates	10
HP Propel Portal Configuration	11
Configure HP Identity Management Security	11
Next Steps.....	11
Appendix A – Loading Knowledge Management Documents into HP Service Manager	12
Pre-Requisites for Loading Documents.....	12
Document Format for Loading Documents	12
KM Documents Directory Structure.....	12
How to Load KM Documents	13

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. 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.

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.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. AMD is a trademark of Advanced Micro Devices, Inc. Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries. Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Appendix B – HP Propel Tips	15
Verifying GPG Code Signing – HP Propel OVA Files	15
Customizing the HP Marketplace Portal.....	15
Manually Changing the Keystore Password.....	16
Appendix C – Configuring HP Propel with Self-Signed SSL Certificates	17
Create HP Propel Portal SSL Files	17
Configure HP Propel Portal Keystore and Truststore.....	17
Add or Update HP Propel Portal SSL Entries	18
Create HP Propel SX SSL Files.....	18
Configure HP Propel SX and HP Operations Orchestration Keystore and Truststore.....	18
Add or Update HP Propel SX SSL Entries	19
Exchange HP Propel Portal and HP Propel SX SSL Certificates.....	19

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. 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.

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.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. AMD is a trademark of Advanced Micro Devices, Inc. Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries. Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Overview

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

The following information is provided in this document:

Overview. Describes the contents of the HP Propel product and its requirements. Additionally, an HP Propel installation overview is provided.

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

SSL Configuration. Provides general information to configure the SSL certificates so that the HP Propel Portal, HP Propel SX, and an end-point system communicate successfully.

Configuration. Provides information for Catalog Aggregation configuration and the procedure to improve the security of HP Identity Management.

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

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

HP Propel Tips. This appendix provides miscellaneous information for HP Propel, including verification of the GPG code signing for the HP Propel OVA files and customizing the HP Marketplace Portal.

Configuring Self-Signed SSL Certificates for HP Propel. This appendix provides instructions to configure self-signed SSL certificates to enable secure communication among the HP Propel Portal, HP Propel SX, HP Cloud Services Automation, and HP Service Manager systems.

Audience

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

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

Additional Information

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

- HP Propel Requirements: *HP Propel 1.00 Support Matrix*
- HP Propel Service Exchange: *HP Propel 1.00 Service Exchange Installation and Configuration Guide*
- HP Catalog Aggregation: *HP Propel 1.00 Catalog Aggregation Help*

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

Before You Begin

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

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

Preparing Your Environment for Virtual Machines

Before installing HP Propel, you need to make sure that your VMware environment has enough resources to instantiate the two VM templates that are included in the HP Propel product.

HP Propel Software and Hardware Requirements

Software Requirements:

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

Hardware Requirements:

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

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

HP Propel Product End-Point Integrations

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

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

Installation Overview

The general procedure to install HP Propel is:

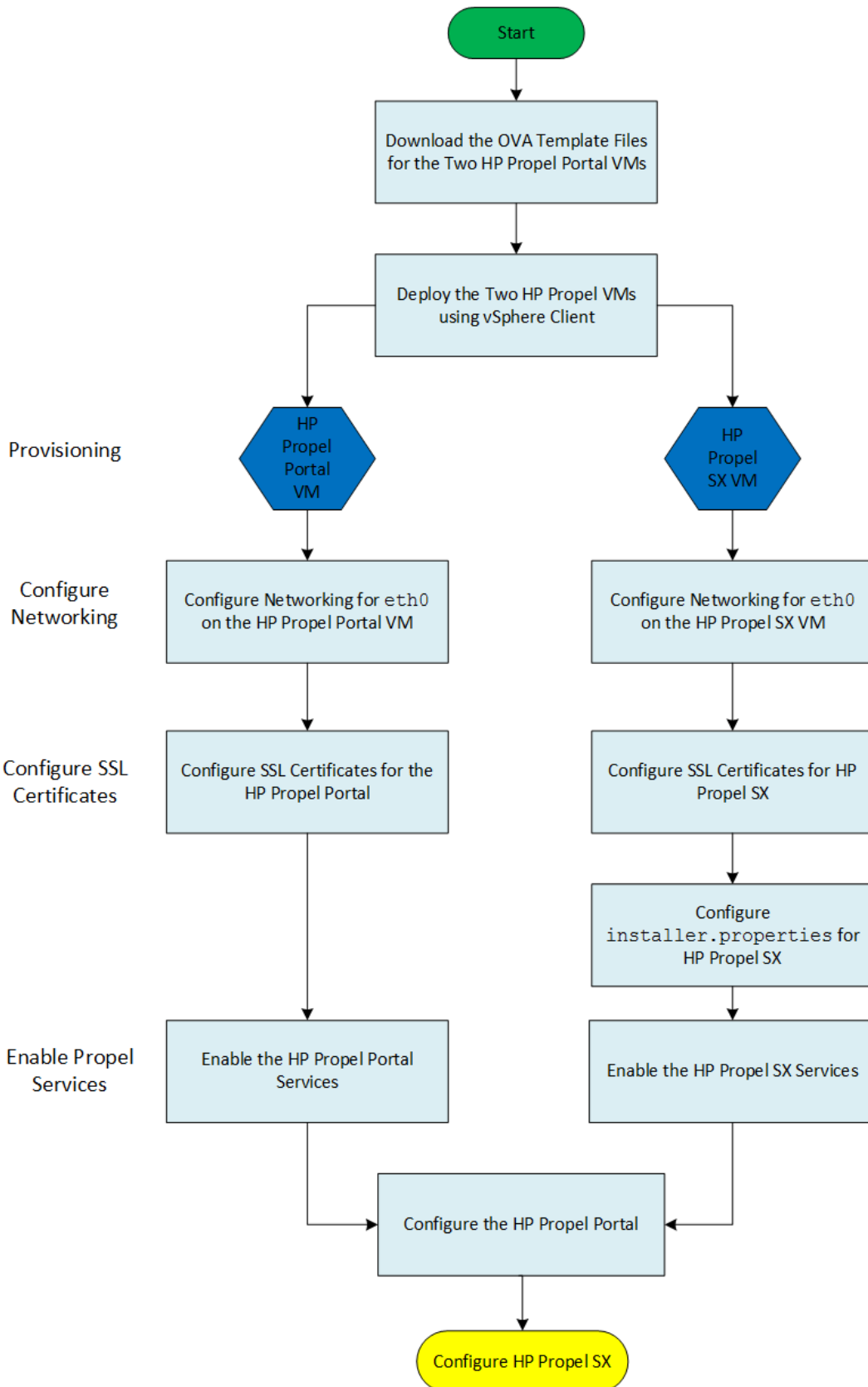
1. From the HP Software Support Online website, download the two OVA templates:
 - a. HP Propel Portal VM
 - b. HP Propel SX VM
2. Using the VMware vSphere Client, deploy the two HP Propel VMs into the VMware ESX environment by importing the OVA templates:
 - a. HP Propel Portal VM
 - b. HP Propel SX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

5. Using the VMware vSphere Client, configure the HP Propel SX VM network adapter.
6. Specify the HP Propel SX hostname and configure DHCP networking for `eth0`.
7. Configure Secure Socket Layer (SSL) communication.
8. Specify an HP SM instance and an HP CSA instance.
9. Enable services on HP Propel SX.
10. Enable services on the HP Propel Portal.
11. Configure the HP Propel Portal.
12. Continue with configuring HP Propel SX, which is described in the *HP Propel 1.00 Service Exchange Installation and Configuration Guide*.
 - a. Configure Ticketing
 - b. Configure Case Exchange

Detailed HP Propel installation instructions are provided in [HP PROPEL INSTALLATION](#).

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

Figure 1 - HP Propel Installation Procedure



HP Propel Installation

Perform the following steps to install HP Propel:

1. Download the two HP Propel OVA template files from [HP SOFTWARE SUPPORT ONLINE \(SSO\)](#):
 - a. HP Propel Portal VM
 - b. HP Propel SX VM

NOTE: To verify the GPG code signing of the two OVA files, download the two `.sig` files and the two HP public key files, then see [VERIFYING GPG CODE SIGNING – HP PROPEL OVA FILES](#) for details.

2. On the ESX server, use the VMware vSphere Client to deploy the two HP Propel VMs:
 - a. HP Propel Portal VM
 - b. HP Propel SX VM
3. Using the VMware vSphere Client, navigate to the VM properties for the newly created HP Propel Portal VM, select **Network Adapter**, and change the network label to the network configured for the ESX server.
4. After the HP Propel Portal VM has been deployed and is available, power on the VM.
5. On the HP Propel Portal VM, log in as `root`, using “propel2014” as the password.
6. Specify the HP Propel Portal hostname and configure DHCP networking for `eth0` on the HP Propel Portal VM:

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

Where `PROPEL_PORTAL_VM_HOSTNAME` is the hostname you specify for the HP Propel Portal VM.

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

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

7. Using the VMware vSphere Client, navigate to the VM properties for the newly created HP Propel SX VM, select **Network Adapter**, and change the network label to the network configured for the ESX server.
8. After the HP Propel SX VM has been deployed and is available, power on the VM.
9. On the HP Propel SX VM, log in as `root`, using “propel2014” as the password.
10. Specify the HP Propel SX hostname and configure DHCP networking for `eth0` on the HP Propel SX VM:

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

Where `PROPEL_SX_VM_HOSTNAME` is the hostname you specify for the HP Propel SX VM.

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

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

11. The SSL certificates for HP Propel and an end-point system must be configured. See [CONFIGURE SSL FOR HP PROPEL](#) for details.
12. On the HP Propel SX VM, log in as `root`, using “propel2014” as the password.

13. On the HP Propel SX VM, edit the `installer.properties` file, entering your unique names, passwords, and URLs. This file is located in the `/opt/hp/propel/bin` directory. See the example below.

NOTE: An HP SM instance and an HP CSA instance must be specified in this file. Only one instance of each product can be specified. Any additional instances must be added into the relevant `instances.json` file. For details of adding additional HP CSA instances, see the *HP Propel 1.00 Service Exchange Installation and Configuration Guide*.

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

```
# SERVICE MANAGER INTEGRATION
SM_HOSTNAME=sm.example.com
SM_PORT=13444
SM_SSL=true
SM_USER=johndoe
SM_PASS=myspassword
SM_DB_HOSTNAME=smdb.example.com
SM_DB_PORT=1433
SM_DB_USER=smuser
SM_DB_PASS=smpassword
```

```
# CSA INTEGRATION
CSA_HOSTNAME=csa.example.com
CSA_PORT=8444
CSA_SSL=true
CSA_USER=johndoe
CSA_PASS=myspassword
CSA_ORG=CSA_CONSUMER
```

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

14. Start the HP Propel SX services:

```
#: cd /opt/hp/propel/bin
#: ./reconfigurePropelSX.sh --configuresx --enableservices
```

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

16. Start the HP Propel Portal services:

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

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

```
https://<PROPEL_PORTAL_VM_HOSTNAME>:8444
```

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

```
https://<HP_PROPEL_SX_HOSTNAME>:8444/sx
```


Configure SSL for HP Propel

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

Although a self-signed certificate can be used in production, HP recommends that you replace this certificate by configuring a trusted certificate from a Certificate Authority (CA). Some organizations issue certificates that are signed by a corporate CA and some organizations get certificates from a trusted third-party CA, such as VeriSign.

SSL Certificates Overview

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

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

NOTE: Though HP does not recommend a specific SSL implementation, for an example of using self-signed certificates, see [APPENDIX C – CONFIGURING HP PROPEL WITH SELF-SIGNED SSL CERTIFICATES](#).

HP Propel SSL Certificates

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

Table 1 – HP Propel Portal SSL Configuration Locations

Component	Location	Line	SSL Entry Type
MPP	/opt/hp/propel/mpp/conf/mpp.json	24	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	34	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	41	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	48	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	53	propel_catalog.pfx
MSVC	/opt/hp/propel/msvc/conf/idm.json	8	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/knowledge.json	7	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/knowledge.json	14	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/ticket.json	7	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/server.json	14	propel_catalog.pfx
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/api.json	7	propel_catalog.cert
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/idm.json	10	propel_catalog.cert
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/server.json	19	propel_catalog.pfx
AGGREGATION	/opt/hp/propel/jboss-as/standalone/ deployments/aggregation.war/WEB-INF/ classes/aggregation-adapter.properties	9	propel.truststore
CONSUMPTION	/opt/hp/propel/jboss-as/standalone/ deployments/consumption.war/WEB-INF/ classes/csa.properties	46	propel.truststore

Table 2 – HP Propel Service Exchange SSL Configuration Locations

Component	Location	Line	SSL Entry Type
RABBITMQ	/etc/rabbitmq/rabbitmq.config	6	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	7	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	8	propel_sx.key.rsa
RABBITMQ	/etc/rabbitmq/rabbitmq.config	16	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	17	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	18	propel_sx.key.rsa
SX	/opt/hp/propel/jboss-as/standalone/configuration/ standalone.xml	231	.keystore
SX	/opt/hp/propel/jboss-as/standalone/configuration/ standalone.xml	33	propel.truststore

Table 3 – HP Propel Truststore¹ Contents

Certificate Type	SSL Authentication Setup
propel_catalog.cert	Self-signed
propel_sx.cert	Self-signed
CSA1.cert ²	Self-signed or Certificate Authority
SM1.cert ²	Self-signed or Certificate Authority
propelCA.cert	Certificate Authority

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

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

Table 4 – HP Propel SSL Descriptions

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

HP Propel Portal Configuration

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

- Configure Catalog Aggregation and create a new catalog. For details, see *HP Propel 1.00 Catalog Aggregation Help*.
- Configure security on HP Identity Management. See [CONFIGURE HP IDENTITY MANAGEMENT SECURITY](#) for details.

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

Configure HP Identity Management Security

HP recommends the following actions to improve the security of HP Identity Management (HP IdM):

1. Change the CSA integration account password in the `integrationusers.properties` file and encrypt the password:
 - a. On the HP Portal VM, log in as `root`.
 - b. #: `cd /opt/hp/propel/boss-as/standalone/deployments/idm-service.war/WEB-INF/\classes`
 - c. Change the default “idmTransportUser” password in the `integrationusers.properties` file.
 - d. Encrypt the new password:

```
#: <PROPEL_PORTAL_JRE>/java -jar cryptoutil.jar encrypt <PASSWORD>
```
2. Create a new JWT signing key in the `applicationContext.properties` file and encrypt the new signing key, using a similar `java` command as in Step 1.

Next Steps

After the HP Propel Portal VM is installed and configured and the HP Propel Service Exchange VM is installed, you must configure the HP Propel Service Exchange VM. Refer to the *HP Propel 1.00 Service Exchange Installation and Configuration Guide* for details about configuring the HP Propel Service Exchange VM.

Appendix A – Loading Knowledge Management Documents into HP Service Manager

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

Pre-Requisites for Loading Documents

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

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

Document Format for Loading Documents

Use the following formats for loading KM documents into HP SM:

- `<Title>propelKmImporter uses this text as the title and summary in HP SM</Title>`
- `<Introduction>propelKmImporter uses this text as the question in HP SM</Introduction>`
- `<Details>propelKmImporter uses this text as the answer in HP SM</Details>`

Sample KM Document

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

<root><Title>Add an Email Account</Title>

<Introduction>&lt;div class="indent"&gt;&lt;span lang="es-cr"&gt;This page provides
steps for adding an email account.&lt;/span&gt;&lt;/div&gt;</Introduction>

<Details>&lt;div class="indent"&gt;&lt;ul&gt;&lt;li&gt;Follow these steps to add an
email account on your iOS device.&lt;/span lang="es-
cr"&gt;:&lt;/span&gt;&lt;ol&gt;</Details>

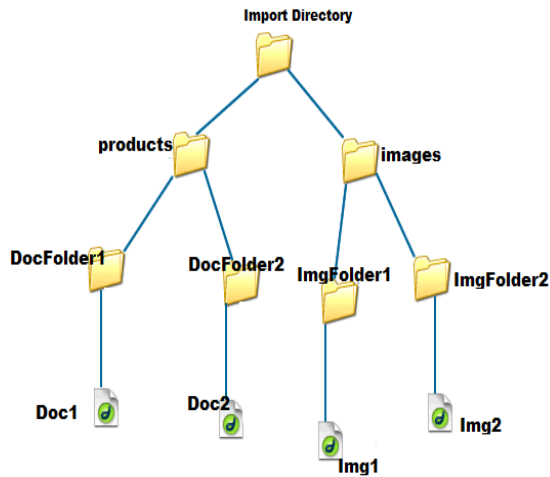
<TrainingInfo><trainingRequirement>T</trainingRequiremen><imageItem></imageItem>
</TrainingInfo><SettingRequirement></SettingRequirement><title>This page has been
temporarily disabled</title></root>
```

KM Documents Directory Structure

The `Import` directory for the HP Propel Knowledge Importer must have the following structure:

- All folders that have documents to be imported must be in a folder named `products`.
- All folders that have images to be imported must be in a folder named `images`.
- The `products` and `images` folders must be located under the `Import` directory.

Figure 2 – Example Import Directory Structure



How to Load KM Documents

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

1. Import the HP Propel Web Services into HP SM:
 - a. Start HP SM and transfer the `HPPropelKnowledge` and `HPPropelKnowledgeAttachment` Web Services files from the HP Propel Portal VM to the HP SM system. The Web Services files are in the `/opt/hp/propel/aggregation/km` directory on the HP Propel Portal VM.
 - b. In the HP SM left pane, navigate to: **System Administration -> Ongoing Maintenance -> Unload Manager -> Apply Unload**. The **Unload Manager** window is displayed.
 - c. In the **Unload File** field, browse to the `HPPropelKnowledge` file.
 - d. In the **Backup To** field, type a name for the file to be stored as a backup. (This can be any name you choose.)
 - e. Click **Next**, and in the dialog that appears for applying the unload file, click **Yes**. A window appears verifying that the hotfix was successfully applied.
 - f. Click **Finish**.
 - g. Repeat Steps **b.** through **f.** for the `HPPropelKnowledgeAttachment` Web Services file.

2. To test the import process:
 - a. In HP SM, navigate to **Tailoring -> Web Services -> Web Service Configuration**.
 - b. Search for the **Service Name** HPPropelKMAggregation. If the HP Propel Web Services are configured correctly, HPPropelKMAggregation contains the HPPropelKnowledge and HPPropelKnowledgeAttachment objects.
3. (Optional) If you want to upload sample KM documents, they are available in the documents.zip file that is in the /opt/hp/propel/aggregation/km directory on the HP Propel Portal VM. Unzip the file and extract the sample documents.
4. Make sure you have Java running in your environment.
5. Navigate to /opt/hp/propel/aggregation/km on the HP Propel Portal VM and execute the following command:

```
#: PropelKMImporter.sh <smSoapProtocol> <smhostname> <smport> <smuser> \  
<smpassword> <location_of_propelImportDOCS>
```

For example:

```
#: PropelKMImporter.sh http <mysmhost> 13080 <myuser> <mypass> \  
/home/<myuser>/documents
```

6. To verify that KM documents have been successfully loaded into HP SM (after receiving a success message):
 - a. In HP SM, navigate to **Search Knowledge Base -> Advanced**.
- Provide the following search criteria and perform the search:

DocType: "Question/Answer"

Status: "External"

Category: "Propel"

Appendix B – HP Propel Tips

Verifying GPG Code Signing – HP Propel OVA Files

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

To verify that the two HP Propel OVA files are signed with GNU Privacy Guard (GPG), you must download the two `.sig` files and the HP keys from [HP SOFTWARE SUPPORT ONLINE \(SSO\)](#). Perform the following procedure on the system that you downloaded the OVA files, the `.sig` files, and the HP keys.

1. Install HP's public keys:

```
#: gpg --import hpPublicKey.pub
#: gpg --import hpPublicKey2048.pub
```

2. Validate and verify the digital signature of the signed OVA file. The output from the command indicates the validity of the signature.

```
#: gpg --verify <OVA_FILE>.sig <OVA_FILE>
```

If the level of trust on the key has not been set, you will see a trust level warning similar to this:

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
```

3. If you do not want to see the warning in Step 2, edit the key to set the trust level of the key for proper verification:

```
#: gpg --edit-key "Hewlett-Packard Company"
(Type the command "trust", select "5" for trusting the key, then confirm and quit.)
```

NOTE: You can trust these public keys.

4. You must also trust the RSA key:

```
#: gpg --edit-key "Hewlett-Packard Company RSA"
(Type the command "trust", select "5" for trusting the key, then confirm and quit.)
```

After performing the above procedure, you should not see the warning about an untrusted identity when verifying the signature.

Here is an example of output from a verification:

```
#: gpg --verify <OVA_FILE>.sig <OVA_FILE>
gpg: Signature made Thu 03 Jan 2013 04:48:47 PM UTC using RSA key ID 5CE2D476
gpg: Good signature from "Hewlett-Packard Company RSA (HP Codesigning Service)"
```

Customizing the HP Marketplace Portal

You can customize the display of the HP Marketplace Portal Dashboard. For details about customizing the themes, widgets, and sections, refer to the *HP Propel 1.00 Customizing the Marketplace Portal* whitepaper.

Manually Changing the Keystore Password

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

```
#: <PROPEL_PORTAL_VM_JRE_DIR>/keytool -storepasswd -storepass propel2014 \  
-new <NEW_KEYSTORE_PASSWORD> -keystore /opt/hp/propel/security/propel.truststore  
#: ./configureKeys.sh --setkspassword <NEW_KEYSTORE_PASSWORD>
```

Where *PROPEL_PORTAL_VM_JRE_DIR* is the JRE directory on the HP Propel Portal VM and *NEW_KEYSTORE_PASSWORD* is the new keystore password that you specify.

Appendix C – Configuring HP Propel with Self-Signed SSL Certificates

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

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

Create HP Propel Portal SSL Files

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

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

Configure HP Propel Portal Keystore and Truststore

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

1. #: `keytool -delete -keystore .keystore -alias propel_catalog`
2. #: `keytool -importkeystore -srckeystore propel_catalog.pfx -srcstoretype PKCS12 \ -destkeystore .keystore -srcaalias 1 -destalias propel_catalog`
3. To make sure the key is in the keystore:
#: `keytool -list -keystore .keystore -v`
4. #: `keytool -importcert -keystore propel.truststore -alias propel_catalog \ -file propel_catalog.cert -trustcacerts -noprompt`

Add or Update HP Propel Portal SSL Entries

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

Table 5 – HP Propel Portal SSL Configuration Locations

Component	Location	Line	SSL Entry Type
MPP	/opt/hp/propel/mpp/conf/mpp.json	24	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	34	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	41	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	48	propel_catalog.cert
MPP	/opt/hp/propel/mpp/conf/mpp.json	53	propel_catalog.pfx
MSVC	/opt/hp/propel/msvc/conf/idm.json	8	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/knowledge.json	7	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/knowledge.json	14	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/ticket.json	7	propel_catalog.cert
MSVC	/opt/hp/propel/msvc/conf/server.json	14	propel_catalog.pfx
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/api.json	7	propel_catalog.cert
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/idm.json	10	propel_catalog.cert
IDM-ADMIN	/opt/hp/propel/idmAdmin/conf/server.json	19	propel_catalog.pfx
AGGREGATION	/opt/hp/propel/jboss-as/standalone/ deployments/aggregation.war/WEB-INF/ classes/aggregation-adapter.properties	9	propel.truststore
CONSUMPTION	/opt/hp/propel/jboss-as/standalone/ deployments/consumption.war/WEB-INF/ classes/csa.properties	46	propel.truststore

Create HP Propel SX SSL Files

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

1. Log in as root.
2. #: cd /opt/hp/propel/security
3. #: openssl genrsa -des3 -out propel_sx.key 2048
4. #: openssl rsa -in propel_sx.key -out propel_sx.key.rsa
5. #: openssl req -new -key propel_sx.key -out propel_sx.csr
6. #: openssl x509 -req -days 365 -in propel_sx.csr -signkey propel_sx.key.rsa \

-out propel_sx.cert
7. #: openssl pkcs12 -export -in propel_sx.cert -inkey propel_sx.key.rsa \

-out propel_sx.pfx

Configure HP Propel SX and HP Operations Orchestration Keystore and Truststore

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

1. #: keytool -delete -keystore .keystore -alias propel_sx
2. #: keytool -importkeystore -srckeystore propel_sx.pfx -srcstoretype PKCS12 \

-destkeystore .keystore -srccalias 1 -destalias propel_sx
3. To make sure the key is in the keystore:


```
#: keytool -list -keystore .keystore -v
```

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


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

Add or Update HP Propel SX SSL Entries

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

Table 6 – HP Propel Service Exchange SSL Configuration Locations

Component	Location	Line	SSL Entry Type
RABBITMQ	/etc/rabbitmq/rabbitmq.config	6	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	7	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	8	propel_sx.key.rsa
RABBITMQ	/etc/rabbitmq/rabbitmq.config	16	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	17	propel_sx.cert
RABBITMQ	/etc/rabbitmq/rabbitmq.config	18	propel_sx.key.rsa
SX	/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml	231	.keystore
SX	/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml	33	propel.truststore

Exchange HP Propel Portal and HP Propel SX SSL Certificates

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

1. From /opt/hp/propel/security on the HP Propel Portal:
 - a. #: scp propel_catalog.cert root@<SX_HOSTNAME>:/opt/hp/propel/security/
 - b. #: scp root@<SX_HOSTNAME>:/opt/hp/propel/security/propel_sx.cert .
 - c. #: keytool -importcert -keystore propel.truststore -alias propel_sx \
 -file propel_sx.cert -trustcacerts -noprompt
2. From /opt/hp/propel/security on HP Propel SX:


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