HP Propel

Software Version: 1.10
CentOS

Security Guide

Document Release Date: December 2014
Software Release Date: December 2014

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

Welcome to the HP Propel Secured Deployment and Configuration White Paper.

This document provides information for working with HP Propel in a secure environment.

This document is designed to help IT professionals who deploy and manage HP Propel instances in a secure manner in the modern enterprise. Our objective is to help you make well-informed decisions about the various capabilities and features that HP Propel provides to meet modern enterprise security needs. The HP Propel platform is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it could potentially be exposed.

Security requirements for the enterprise are constantly evolving and this paper should be viewed as HP's best effort to meet those stringent requirements. If there are additional security requirements that are not covered by this paper, please open a support case with the HP support team to document them and we will include them in future editions of this paper.

Related Documents

The following HP Propel documents 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.)

HP Propel 1.x Documents

HP PROPEL INSTALLATION GUIDE

HP PROPEL ADMINISTRATION GUIDE

HP PROPEL SERVICE EXCHANGE CONFIGURATION GUIDE

HP PROPEL SYSTEM AND SOFTWARE SUPPORT MATRIX

HP PROPEL CUSTOMIZING THE MARKETPLACE PORTAL

HP PROPEL CATALOG AGGREGATION HELP

HP PROPEL CATALOGS HELP

HP PROPEL MARKETPLACE PORTAL HELP

HP PROPEL ORGANIZATIONS HELP

HP PROPEL OFFERINGS HELP

Version Information

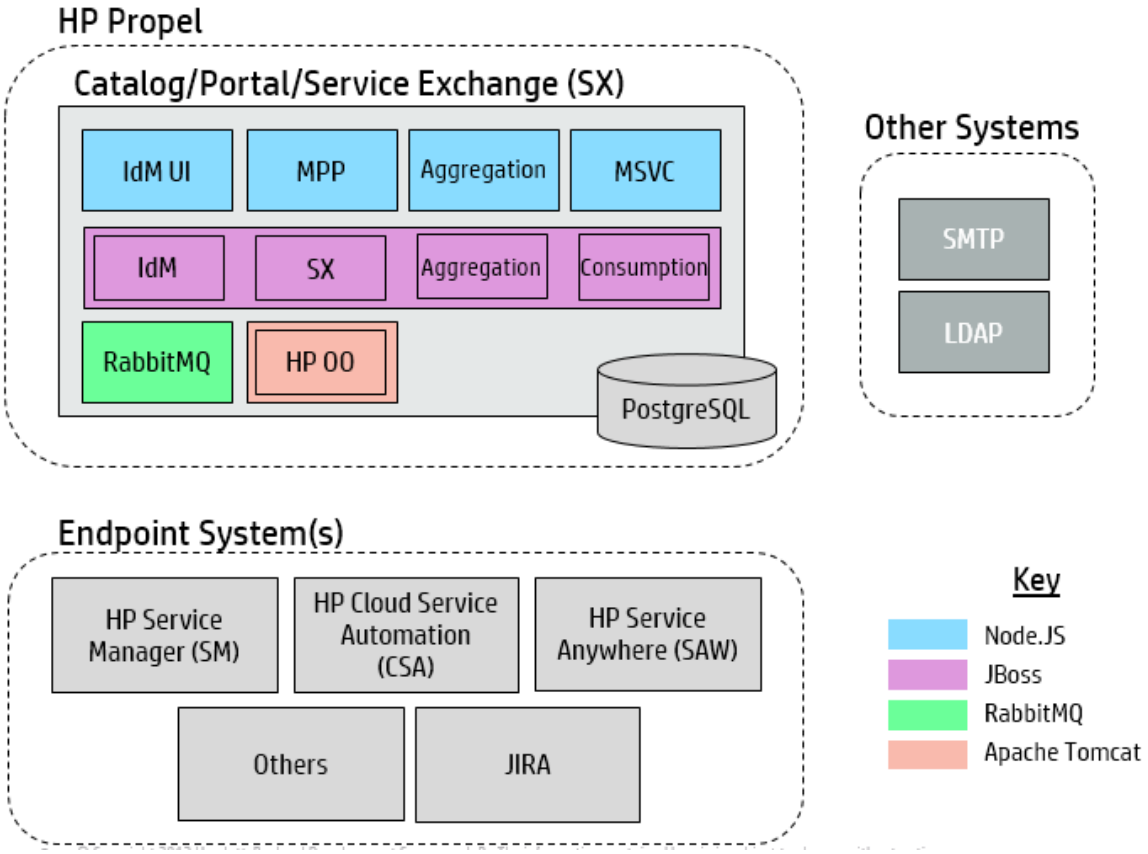
This document relates to version 1.10 of HP Propel.

Secure Deployment

This section provides information on implementing and deploying HP Propel in a secure manner.

HP Propel Topology

HP Propel deployment footprint (or technical system landscape) is described below and includes the recommended security considerations and the components involved.



Note: In the jBoss container, the IdM represents the IdM services and war file.

Many of the HP Propel components have a front-end UI or layer that is served by node.js and a back-end layer that is implemented inside of a web application in Java.

Organizations are configured using the Catalog Administration UI (the grey Organizations tab). This launches a Node.js service where the administrator can create and modify Organizations.

Security bulletins explain how to reconfigure SSL in order to solve issues like shellshock. For example, see the CVE at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271.

Security can be implemented in three different ways:

- Security in minimal implementation topology. HP Propel ships with one virtual server for both types of customers (combined or all-in-one customers who use all of HP Propel components, and Service Exchange customers who only need that component).
- Security in full deployment of HP Propel topology. For details, see "Firewall and Ports" on page 16.
- Security in Service Exchange topology.

JBoss also hosts the following list of services:

- consumption.war
- idm-service.war
- aggregation.war
- sx.war

In HP Propel 1.1, the administrator can control the installation location, but it is usually installed into **/opt/hp/propel**. These WAR files are placed within the **jboss-as/standalone/deployments** subfolder wherever HP Propel has been installed.

Technical System Landscape

HP Propel provides an enterprise-wide, end-user Portal powered by HTML5, JavaScript, Node.js and Java EE. These technologies combine in a seamless, modular micro-services architecture to allow for flexible deployments, customizable to meet geographic distribution, and other enterprise needs.

Additional Information

For additional information about topology, see HP PROPEL CATALOG AGGREGATION HELP.

For additional information about required ports and HTTPS, see the HP PROPEL MARKETPLACE PORTAL HELP.

Default Security Settings

In many cases, it is recommended to modify the default security settings.

- **Authentication** – By default, authentication is not enabled. It is recommended to enable it.
- **TLS Encryption** – By default, HP Propel supports three TLS protocols: 1.0, 1.1, 1.2. It is recommended to reduce this to one or two versions only.
- **TLS Certificate** – By default, a self-signed certificate is provided during the installation of HP Propel. It is recommended to replace this with a custom certificate or one signed by a well-known

certificate authority. For details on how to install a signed certificate into Jboss for the IDM3 User Application, see the HP PROPEL ADMINISTRATION GUIDE.

- **KeyStore, TrustStore, and Server Certificate Passwords** – By default, the default Java passwords are provided for the keyStore, trustStore, and Server Certificate. It is recommended to replace these with encrypted passwords. For details, see "Encryption" on page 24.

OVA is secured out-of-the-box (it has a firewall, security patches, and service users with restricted permissions). It ships with default passwords (the root password for the OVA, the consumer and admin "seeded" users for demos in IdM). It is recommended to change the default passwords. For details, see "Passwords" on page 27.

Physical Security

HP Propel is a virtual appliance. A virtual appliance is a pre-installed, pre-configured operating system and software solution delivered inside a virtual machine. Deploying a software solution as a virtual appliance provides customers with a complete turnkey package that they can download and immediately deploy.

HP Software recommends that the virtual appliance be positioned in the organization data center. The data center should be protected by security controls defined by your organization. Depending on those security controls, you may choose to disable remote access to the appliance, which restricts the administrative capabilities of users with access to the physical data center where the appliance is located.

Common Security Considerations

Thoroughly review the trust boundaries between HP Propel components (web servers, application servers, LDAP servers, identity managers, and other integrating servers) to minimize the number of hops between the components. In addition, it is recommended to use SSL to secure access to servers located across such boundaries.

HP Propel is considered secure as it is structured as a single OVA deployment. This means that most communications are internal between Propel components, and there is no communication of data through the network except for a few communications that occur via ports.

Use SSL to access HP Propel components via the end point systems because the connection is taking place outside the VM machine.

In case of a firewall between HP Propel and the endpoint system; you must ensure the proper configuration according to the vendor recommendation, using the appropriate ports. For details, see "Firewall and Ports" on page 16.

Run periodic trusted root Certificate Authority certificate updates on your clients and servers to ensure that the publisher certificates used in digital code signing are trusted.

Note: Currently, the connection to a database is retained to local host.

Additional Information

For additional information about secure deployment, see the HP PROPEL SERVICE EXCHANGE CONFIGURATION GUIDE to do the following:

- Manually configure HP SX required files.
- Connect to HP CSA, HP SM, HP SAW.
- Connect JIRA to HP SX.

Also see the HP PROPEL SYSTEM AND SOFTWARE SUPPORT MATRIX.

Installation Security Aspects

This section discusses security aspects related to installing HP Propel.

Supported OS Versions

- **Application OS-level security -** The service account should not be root and sensitive files should be protected. Most services are run as specific users (for example, a jboss, postgres, or rabbitmq user). For details about the root user, see "Passwords" on page 27.
- **Virtual appliance -** HP Propel is delivered as a virtual appliance, with hardened (current security patches and configuration).

  Once you deploy HP Propel, you must administer the appliance and you are responsible for keeping its security patches up-to-date by following the security bulletins. Make sure you check the security bulletins (CentOS) for each application and platform.

  You also own the operating system from that moment on, while HP continues to maintain and provide the code.
- **Hardened operating system and dependencies -** The operating system (OS) and dependencies should be hardened. For hardening details, see the table below:

HP Propel Module	Hardening documentation
RabbitMQ	For more information on RabbitMQ and Openstack products, go to the product documentation on the http://www.openstack.org site.
HP Operation Orchestration (OO)	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00996928
CentOS	For more information on CentOS, go to the product documentation on the http://www.centos.org site.

Operating System Security Installation Considerations

- Details about the operating system security are provided at: https://community.cisecurity.org/collab/public/index.php?path_info=categories%2F7%2Fdocuments%2F482.

- It is suggested to disable SSH communication with the machine or to connect it with strong credentials. For details, see "Firewall and Ports" on page 16.
- For the list of supported operating system environments, see the HP PROPEL SYSTEM AND SOFTWARE SUPPORT MATRIX.

Note: The supported environment information provided in the HP Propel Support Matrix is accurate for the HP Propel 1.10 release, but there may be subsequent updates. For the most up-to-date supported environments, see the HP Software Web site using the following URL: http://www.hp.com/go/TDQC_SysReq.

Web Server Security Recommendations

This section includes the web server security recommendations:

- **SSL** - See the HP PROPEL ADMINISTRATION GUIDE for information on enabling SSL for all interactions with the Web server.
- **Node.js** - See "Encryption" on page 24.
- **Consumption** - See the HP PROPEL ADMINISTRATION GUIDE.
- **IdM** - See the HP PROPEL ADMINISTRATION GUIDE.
- **Default passwords** - Make sure to always change the default passwords. For details, see "Default Master Password" on page 27.
- **Encrypt passwords** - To keep sensitive data protected, it is recommended to encrypt passwords. For details, see "Split Master Password" on page 27.
- Always use the minimal possible permissions when installing and running HP Propel.

Application Server Security Recommendations

This section includes the application server security recommendations:

- **JBoss –** For additional information, see the HP PROPEL INSTALLATION GUIDE.
- **Default passwords** - Make sure to always change the default passwords. For details, see "Default Master Password" on page 27.
- **Encrypted passwords** - Create a password vault for JBoss and protect your credentials. For instructions, see https://community.jboss.org/wiki/JBossAS7SecuringPasswords.

For more information on CA products [or insert product name], go to the product documentation on the [insert top level link, e.g., www.hp.com] site.

- Always use the smallest possible number of permissions when installing and running HP Propel.

FAQ

Does HP Propel ensure that configuration files are not stored in the same directory as user data?

The JBoss and Node.js directories are separate from the user data. The user data and attachments are stored in PostgreSQL. The user can reconfigure JBoss and Node.js to log to different directories.

Does HP Propel install with unnecessary functionality disabled by default?

There is no technical licensing in HP Propel, only paper licensing.

Are application resources protected with permission sets that allow only an application to modify application resource configuration files?

Yes.

Does HP Propel execute with no more privileges than necessary for proper operation?

Yes, the permissions model is constantly reviewed and only necessary permissions are required.

Network and Communication Security

This section provides information on network and communication security.

Secure Topology

The HP Propel platform is designed to be part of a secure architecture, and can meet the challenge of dealing with the security threats to which it could potentially be exposed.

Several measures are recommended to securely deploy HP Propel servers:

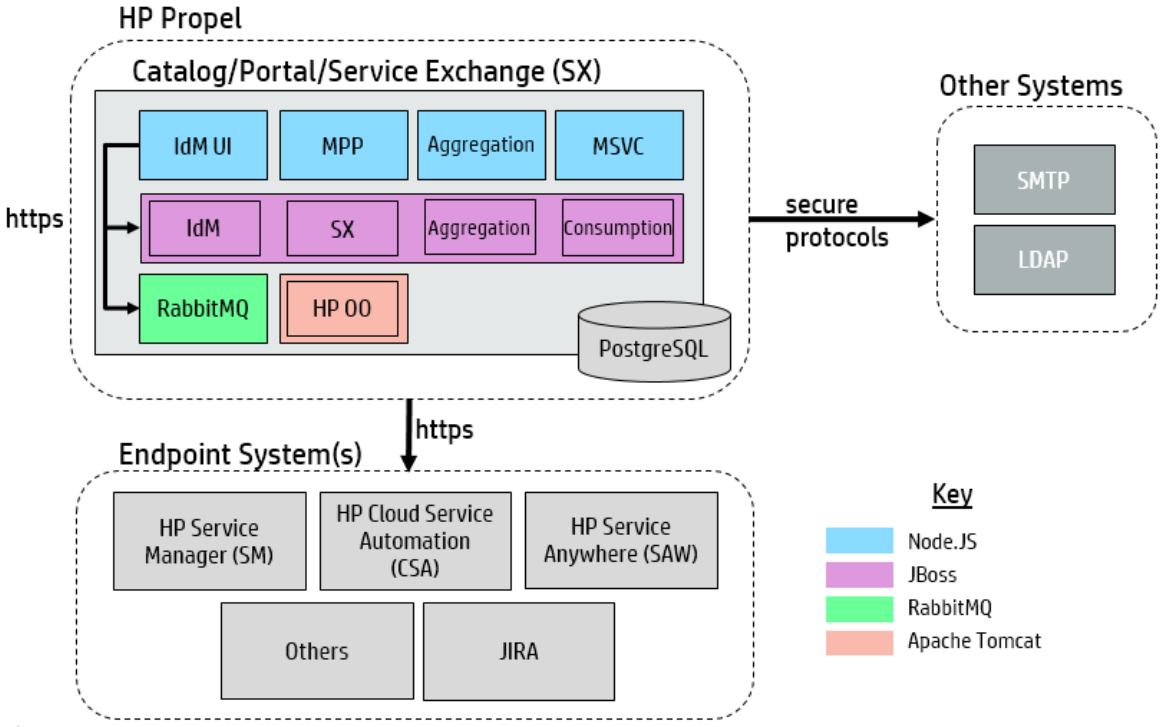
- **SSL communication protocol**

  The SSL protocol secures the connection between the client and the server. URLs that require a secure connection start with HTTPS instead of HTTP.

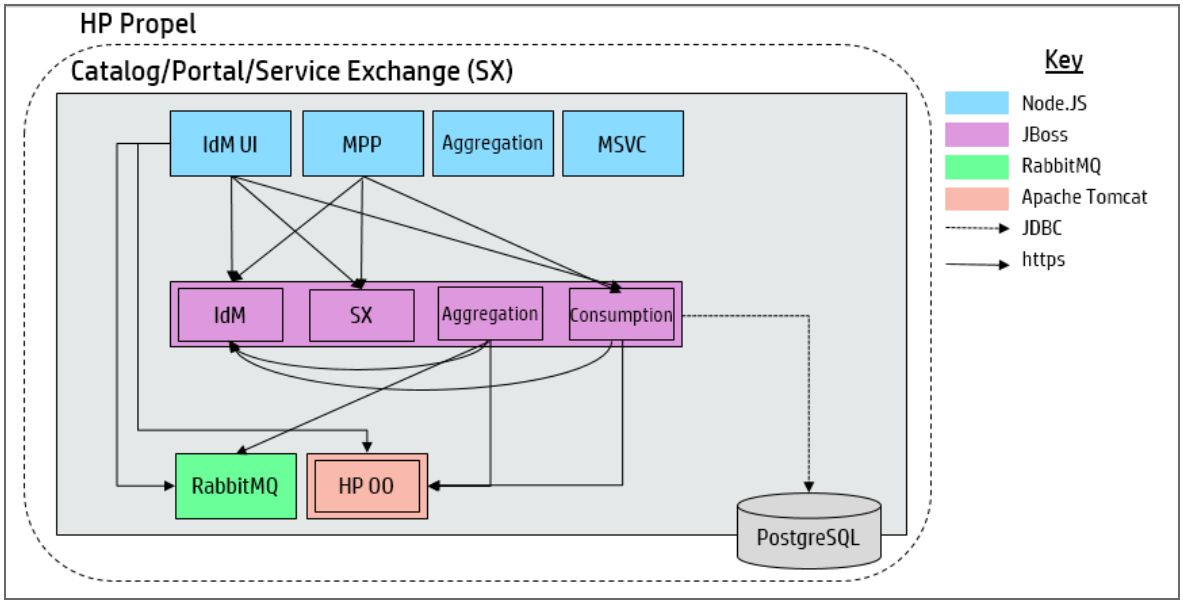
- **Server Cluster Hardware Load Balancer Configuration**

  Approaches such as VM high availability can be used in conjunction with HP Propel. Secure Reverse Proxies or Load Balancers can manage inbound traffic.

The following diagram shows the types of protocols used to communicate with Propel.



Drill down to the internal communications inside the HP Propel machine.



Firewall and Ports

You can configure a firewall on the Propel servers by creating a local firewall/IP tables rule to restrict the access between the servers. However, you must ensure that the Propel servers can still communicate freely.

The HP Propel appliances come pre-configured with the following ports:

Component	Port	Comments	Example	Internal - External
IdM UI	9200	Identity administration UI	https://<propel_server>:9200	External
MPP	8089	Consumer portal	https://<propel_server>:8089/org/<organization>	External
Aggregation	9300	Configuring end point systems in the catalog VM	https://<propel_server>:9300	External
MSVC	9100	Micro services		External
Catalog	8444	Catalog administration	https://<propel_server>:8444/consumption	External
IdM	8444	Identity service	https://<propel_server>:8444/idm_service	Internal

Component	Port	Comments	Example	Internal - External
Service Exchange	8444	Service exchange dashboard	https://<propel_server>:8444/sx	External
HP OO	8443	HP OO administrative interface	https://<propel_server>:8443/oo	Internal
SSH	22	For remote administration, if desired.	ssh <user>@<propel_server>	External
RabbitMQ	5671 15672	Listener Management Listener		Internal

Note: The standard Linux IP configuration can be modified to meet your needs. For example, you can disable remote SSH access.

Communication Channels Security

HP Propel supports the following secure channels:

Secure channel	How to configure
Between the HP Propel VMs (Catalog and SX)	See the HP PROPEL INSTALLATION GUIDE.
Between the Catalog VM and the Endpoint Systems (CSA and SM)	See the HP PROPEL INSTALLATION GUIDE.
Between the identity service on the Catalog VM and the Endpoint Systems (CSA and SM)	See the HP PROPEL INSTALLATION GUIDE.
Between the SX VM and the Endpoint Systems (CSA and SM)	See the HP PROPEL INSTALLATION GUIDE.
Between client (browser) and the HP Propel server	In general, trust is only needed on the client. This is a trust to the authority that issued the server certificate for the HP Propel server.
Between HP Propel and LDAP server	For details, see the HP PROPEL ORGANIZATIONS HELP.
Between HP Propel and the SMTP mail server	Specify a secure port when defining the mail server.

FAQ

Are exceptions required to be added to the firewall policy?

Placing a reverse proxy in front of the HP Propel server is recommended. The list of ports to be open in the firewall for the incoming traffic is documented in "Firewall and Ports" on page 16. The only port that must be opened on the HP Propel server for incoming traffic is the jetty port (8080, or 8443 if you are using a secure connection).

How do I configure the HP Propel server in SSL using the certificate authority?

For details, see https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=KM00756782.

This site requires that you sign in with an HP Passport. Or click **Create an account** to register an HP passport.

User Management, Authentication, and Authorization

This section provides information related to user authentication.

Authentication and Authorization Model

Authentication is the process of identifying an individual, usually based on a user name and password, or certificate.

Authentication Model

HP Propel supports the following authentication methods:

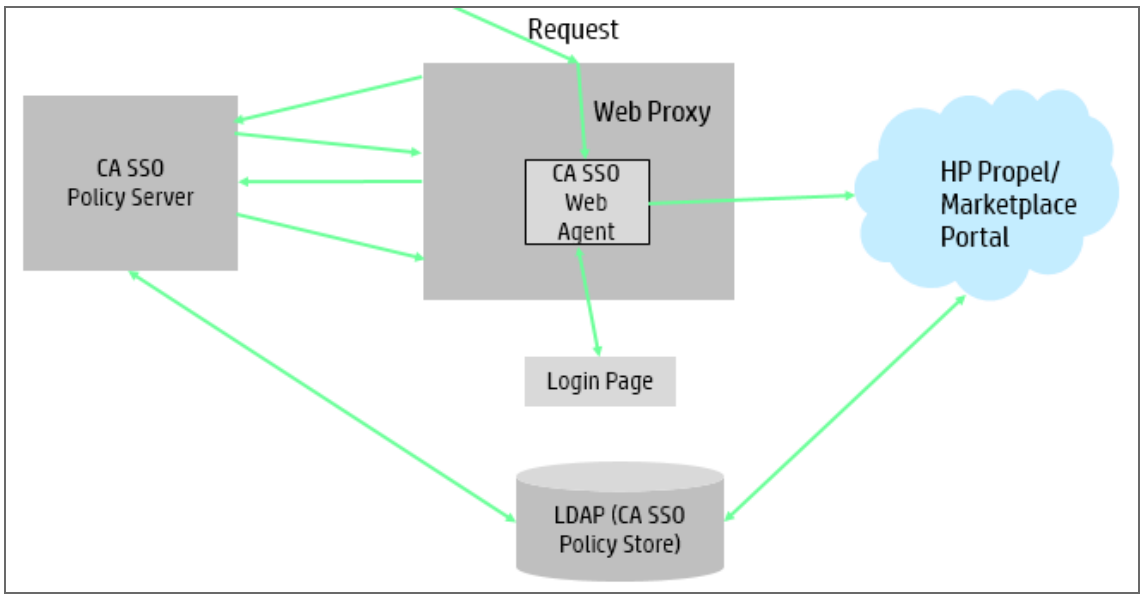
- **Seeded authentication:** HP Propel requires users to enter username and password credentials to gain access to the application. Stored in configuration files, seeded credentials allow the application to be used immediately after installation. Seeded authentication should only be used for initial configuration, evaluation, or other small-scale deployments where integrating with an enterprise LDAP or Active Directory domain is impractical. HP recommends against using seeded authentication in a production environment.
- **LDAP authentication:** You can integrate HP Propel to an LDAP directory service to authenticate using a tenant organization's LDAP domain (external to the HP Propel appliance). The LDAP server supports the LDAP3 protocol. Common servers include OpenLDAP and ApacheDS.

  Note: LDAP is outside the appliance.
- **LDAP federation:** Federate authentication with a tenant organization's LDAP domain.
- **Active Directory:** HP Propel can use a tenant organization’s Active Directory domain to authenticate users.
- **Active Directory federation:** Federate authentication with a tenant organization's Active Directory domain.
- **Certificate-based authentication (smart cards and CAC):** CAC sign-on enables users to log in to the web client directly with a smart card that stores a valid user certificate to authenticate using a configuration specified by the user's tenant organization, possibly validated by LDAP / Active Directory.
- **HP SSO:** An optional but highly recommended for some integrations such as Release Control. Enabling HP SSO for integrations will bypass the login prompts when connecting two HP products.

- **CA SSO:** CA SSO is enabled by editing the configuration files. Enabling it bypasses the logon screen, not the “Service Manager logon screen. For more information on CA SSO and CA products, go to the http://www.ca.com site.

  product documentation on the

  The following diagram shows how a request is processed when HP Propel and CA SSO are integrated:



- The identity service has the following features:
  - REST API for performing authentication, retrieving user information (including authorization information), and token validation.
  - Administrative user interface for managing tenant organization configuration.
- **Keystone federation:** Federate authentication with the Keystone identity service from OpenStack and HP Helion.
- **IdM Authentication Check:** All incoming requests will have an authentication token set on its header ('X-Auth-Token').

  IdM Authentication Check Middleware will connect to the IdM server and send a request to validate the authentication token from the incoming request. If the IdM server returns a valid/success response for the validation, it will forward the requests to the mounted middleware(s). If the IdM server returns a failure/error response for the validation, it returns 403 Forbidden.

  For details, see the HP PROPEL SERVICE EXCHANGE CONFIGURATION GUIDE.

Authorization Model

There are two forms of authorization:

1. Role-based authorization, where a user is assigned to roles based on their LDAP group membership or seeded authentication user definition.

2. Group-based authorization to catalogs, where a user is authorized to access a catalog based on LDAP group membership. The two primary roles used by HP Propel are service consumer for non-privileged users, and consumer organization administrator for a tenant organization's administrators to perform self-service management of their own organization. The provider organization has several additional roles.

For detail, see HP PROPEL ORGANIZATIONS HELP.

Micro Server (msvc-server) - Micro server is an instance of Express.js. This is a very lightweight, stateless web server that will host one or more micro service(s). Following is a high-level overview of the features that micro server will provide:

1. IdM authentication check for all incoming requests.

2. If IdM authentication check fails, returns an authentication error response (such as 401 HTTP Status Code).

3. If IdM authentication check succeeds, forwards the requests to the hosted micro services.

4. Incoming requests will be routed to appropriate micro services by route matching (Route Matching in Express.js).

msvc-server also handles deployment concerns such as http/https, start/stop scripts, and IdM configuration.

Authentication Administration and Configuration

The authentication administration and configuration is done for in the Organization module of HP Propel. For details, see the HP PROPEL ORGANIZATIONS HELP.

Authorization Administration and Configuration

The administration and configuration of the authorizations is handled in the roles and groups sections of the IdM Admin UI. For details, see the HP PROPEL ORGANIZATIONS HELP.

External Authentication

HP Propel supports external authentication with specific configurations. The supported modes include Smart Card authentication, such as CAC, and SSO authentication, such as CA SSO. Contact your HP representative for further details.

Additional Information

For additional information about managing passwords, see the HP PROPEL ADMINISTRATION GUIDE.

For additional information on authenticating and setting up LDAP, see the HP PROPEL ORGANIZATIONS HELP.

For additional information on customizing themes and security classifications throughout an organization, see the HP PROPEL ORGANIZATIONS HELP.

Also see:

- HP PROPEL SERVICE EXCHANGE CONFIGURATION GUIDE
- HP PROPEL ORGANIZATIONS HELP
- HP PROPEL CATALOG AGGREGATION HELP
- HP PROPEL CATALOGS HELP

FAQ

Can HP Propel require account passwords that conform to corporate policy?

LDAP integration is a recommended solution to ensure stronger password policy support.

Can HP Propel limit the number of logon sessions per user and per application?

There is no limit on the number of user logon sessions.

Can HP Propel set up various security classifications?

Yes. HP Propel uses the `securityLevel` KeyPair (common in governmental organizations) to control how the portal advertises its intended use for various security classifications. For additional information about customizing the HP Propel organization's security classifications, see the HP PROPEL ORGANIZATIONS HELP.

Why does my browser "Autocomplete" my credentials?

The three major browsers (Internet Explorer, Google Chrome, and Mozilla Firefox) have decided to ignore `autocomplete=off` in web forms. As a result, when logging in to HP Propel you may, depending on your browser configuration, be prompted to remember your login credentials.

If you are an end user of HP Propel and do not wish to have your login credentials remembered – and they need not be – indicate when prompted by your browser that you do not wish to have your login or password information saved by the browser. Often you can instruct your browser not to prompt you in the future for this site.

It is often possible to configure your browser to disable this ability entirely. This can often be configured either in the browser itself or via corporate IT policy. Refer to your browser documentation or contact your System Administrator for more details.

For additional information, see the following for each browser:

- Internet Explorer: For more information on Internet Explorer and Microsoft products, go to the product documentation on the http://www.microsoft.com site.
- Chrome: For more information on Chrome and the Google products, go to the product documentation on the http://www.google.com site.
- Firefox: For more information on Firefox and the Mozilla products, go to the product documentation on the https://www.mozilla.org site.

Can HP Propel inherit user information and authorization profiles from an external repository, such as LDAP?

No. The information required for proper authentication is imported from LDAP.

Does HP Propel support entity level access restriction?

Yes.

Does HP Propel support limitations associated with user profiles and roles (for example, maximum number of group profiles, predefined profiles, and so on)?

Yes, in HP Propel 1.1, the pre-defined groups are very few, but are used to control access to features like **Shopping** and **Request on Behalf**. Before assigning a group to a role or a catalog, that group must exist in the LDAP directory.

Is Role Management (access to different views and access/edit permission to separate parts) supported?

Yes. In addition to basic **Shopping** / **Request on Behalf** separation, Propel separates consumers (Portal) from administrators (Catalog Admin).

Encryption

This section provides information on data encryption in HP Propel.

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it. For example, the TLS protocol encrypts the communication data.

Note: To ensure FIPS compliance, NO configuration options are allowed!

Encryption Model

HP Propel uses the following encryption models:

Secret splitting.

For details, see "Split Master Password" on page 27.

Secure Sockets Layer (SSL).

This technology secures communication by encrypting data and providing authentication. Without SSL encryption, packets of information travel over networks in full view. For details, see "Encryption" above.

SSL encryption uses two keys:

- Public key. The public key is used to encrypt data.
- Private key. The private key is used to decipher data.

Both keys together are called a certificate. Every SSL certificate is created for a particular server in a specific domain by a Certificate Authority (CA). When an application user accesses a HP Propel server, SSL authenticates the server, and can also be configured to authenticate the client. Additionally, HP Propel establishes an encryption method and a unique key for the communication session.

The HP Propel platform fully supports the TLS 1.2 protocol.

Note: We recommend using the strongest currently available cryptographic algorithms when obtaining server or client certificates, as well as the largest key size (not less than 2048-bit RSA keys). To see the latest NIST approved cryptographic algorithms and key lengths, go to http://csrc.nist.gov/publications/PubsFIPS.html.

Encryption Administration

This section provides information about the encryption administration.

It is recommended to encrypt your passwords. For details, see the HP PROPEL ADMINISTRATION GUIDE.

Digital Signatures

You must validate and verify the digital signature of the signed OVA file. For details, see the HP PROPEL ADMINISTRATION GUIDE.

Password Encryption

- All password attribute values in the mpp.json file must be encrypted with **passwordUtil.js**. The **passwordUtil** tool has been enhanced to generate shares so that the administrator can generate them while configuring the MPP. The **passwordUtil** tool also has the functionality to reconstruct the KEK from the shares read from the configured resources.
- All other encryption for HP Propel is done with **cryptoUtil**. For details, see the HP PROPEL ADMINISTRATION GUIDE.

Best Practices

The HP Propel application server does not have SSL enabled. It is expected and recommended that the front end server, or the reverse proxy will be configured to require SSL.

Additional Information

For additional information about encryption, see the HP PROPEL ADMINISTRATION GUIDE.

For additional information about required ports and HTTPS, see the HP PROPEL MARKETPLACE PORTAL HELP.

FAQ

Does HP Propel transmit account passwords in an approved encrypted format?

It is strongly recommended to enable SSL on HP Propel and LDAP servers to ensure secured account password transmission.

Does HP Propel store account passwords in approved encrypted format?

Admin can choose either stand or hash mode to store user passwords.

User passwords are not stored at all, only the hash; but internal system passwords are stored in AES 256.

Does HP Propel use the Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules and random number generator to implement encryption, key exchange, digital signature, and hash functionality?

Partially. When the administrator enables FIPS, all passwords saved in the configuration file are encrypted with an FIPS compliant AES algorithm, including database password, LDAP password. All user passwords stored in the database are encrypted with an FIPS compliant AES algorithm if the administrator uses the stand password mode.

The cryptography provider used by HP Propel is not FIPS validated.

What are the base product and service authentication methods provided (user name and password)?

User name and password, and LDAP authentication.

HP Propel can be configured to support one of the following authentication methods: user name and password, LDAP authentication, smartcard, and external authentication.

Is SAML v2.0 supported to performing authentication?

No.

Is Single Sign-On (SSO) supported?

Yes. HP Propel 1.1 supports two forms of single sign-on (SSO):

- **CA SSO.** Yes. For information on CA SSO and CA products, go to the http://www.ca.com site.
- **HP SSO.** HP Propel must authenticate users; coming into Propel with an HP SSO cookie generated by an external application is not supported.

Does HP Propel integrate with Identity Management (via API or AD) for system and product users?

HP Propel integrates with CA SSO, where a remotely authenticated user name is passed in the header. This requires a separate configuration. For information on CA SSO and CA products, go to the http://www.ca.com site.

Are there any default vendor-supplied passwords or other security parameters embedded in HP Propel?

Yes, but the defaults can be replaced by configuration.

Passwords

HP Propel uses a master password (or Key Encryption Key – KEK) to encrypt passwords for user accounts that are in the `$PROPEL_HOME/mpp/conf/mpp.json` file, such as the `idmTransportUser` user account. HP recommends that you change the default master password for improved security.

For details, see the HP PROPEL ADMINISTRATION GUIDE.

Password encryption is detailed in "Password Encryption" on page 25.

Default Master Password

As a best practice for security within your organization, HP recommends that you change the default master password (`root` password) during the installation process.To change the default password, see the HP PROPEL ADMINISTRATION GUIDE.

Split Master Password

To avoid hard coding the master password and to improve security, the out-of-the-box master password or Key Encryption Key (KEK) is split into multiple cryptographically-secure shares. Those shares are stored in distributed resources. The KEK can be reconstructed if a specified number of shares (threshold) can be successfully read.

In HP Propel, the implementation is a (3,2) threshold scheme where 3 shares are generated from a KEK and any two are sufficient to reconstruct the KEK.

File-system based resources are the only ones supported at this time.

The distribution of shares to the right resources and configuring the resource permissions is the responsibility of the Administrator.

For details, see the HP PROPEL ADMINISTRATION GUIDE.

Trace and Log Files

This section provides information related to trace and logs.

Log and Trace Model

HP Propel produces several logs for troubleshooting. In addition, the history of changes to existing objects (project, request, and so on) are stored in the database as history. This information remains as long as the object itself is not deleted.

The IdM log file is the **hpcloud-idm-service.log** file in the **<JBoss>/standalone/log** directory.

Trace Security Administration and Features

The trace security administration provides the ability to find a username audit information in logs to reconstruct history about individual user transactions.

Secure Debug Features

HP Propel provides a set of tools for troubleshooting and providing better supportability. These features, which can expose sensitive internal information about the system and about activities performed on the system, are disabled by default and can be switched on by using the site parameters. It is recommend to validate that the parameters are reset to the default values immediately after using the debug features. For details, see the HP PROPEL SERVICE EXCHANGE INSTALLATION AND CONFIGURATION GUIDE.

HP Propel Audit

Recommendations:

- Pay attention to the log level and do not leave the level at DEBUG except for troubleshooting.
- Pay attention to log rotation.
- Restrict access to the log directory.
- If logs archiving is needed, create your own archiving policy.

FAQ

Does HP Propel audit access to need-to-know information and key application events?

No, HP Propel does log key application events such as authentication success and failure.

General questions

How can I report security issues?

Use the following link: https://h41268.www4.hp.com/live/index.aspx?qid=11503

Where can customers obtain the latest information regarding security vulnerabilities in HP Propel?

You can obtain the latest information regarding security vulnerabilities and also register for alerts via this webpage:
https://h20566.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive?ac.admitted=1389784040189.876444892.199480143

Glossary

This section addresses common, industry-wide security concepts.

Access control	Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Appliance	A software environment that includes the operating system and application. It is designed for installation in standard hardware that will be dedicated to running that single application..
Assurance	Based on the fact that the four security goals: integrity, availability, confidentiality, and accountability have been adequately met by a specific implementation. This includes (1) correctly performing functionality, (2) adequate protection against unintentional errors (by users or software), and (3) good enough resistance to intentional penetration or by-pass.
Authentication	The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. It is usually based on a user name and password, or certificate. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Authorization	The granting or denying of access rights to a user, program, or process based on their identity. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Availability	The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Certificate	In cryptography, a public key certificate or digital certificate is an electronic document that uses a digital signature to link a public key with an identity (for example, the name of a person or an organization, their address, and so forth). The digital certificate is used to verify that a public key belongs to an individual and to certify the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.
Certificate Authority (CA)	A trusted organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Countermeasure	A way to mitigate the risk of a threat.

Credential	An object that is verified when presented to the verifier in an authentication transaction. It can be a digital document used in authentication and access control that bind an identity or an attribute to a claimant's token or some other property, such as current network address.
Data integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Defense in Depth	Layers of protection, so that you do not need to rely on a single security measure alone.
Denial of service	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
DMZ architecture	In computer security, a DMZ (or demilitarized zone) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, using the Internet. The purposes of a DMZ is to add an additional layer of security to an organization's local area network (LAN). An external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.
Domain	See "Security domain".
Encryption	The process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not prevent interception, but denies the message content to the interceptor. It can be read only by someone who has the right encryption key to unscramble it. For example, the TLS protocol encrypts the communication data.
Entity	Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Federal Information Processing Standards (FIPS)	The Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements for Cryptographic Modules," was issued by the National Institute of Standards and Technology (NIST) in May, 2001. The FIPS 140-2 standard specifies the security requirements for cryptographic modules utilized within a security system that protects sensitive or valuable data. The benefits of using the FIPS 140-2 compliant crypto module is that the FIPS approved crypto algorithms are deemed appropriate and that they perform the encrypt/decrypt/hash functions correctly and in a FIPS-compliant manner. See also http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
Firewall	A network security system that controls the incoming and outgoing network traffic based on applied rule set. It establishes a barrier between a trusted, secure internal network and another network (the internet) that is not assumed to be secure and trusted. Firewalls exist both as a software solution and as a hardware appliance.

General support	An interconnected information resource under the same direct system management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Hardening	The process of securing a system by reducing its surface of vulnerability. A system has a larger vulnerability surface the more functions it fulfills. Reducing the surface of vulnerability typically includes removing unnecessary software, unnecessary usernames or logins, and unnecessary services; closing network ports; and setting up intrusion-detection systems, firewalls, and intrusion-prevention systems.
HP SSO	HP Single Sign On (SSO) is a mechanism in which a single action of user authentication and authorization can permit a user to access all HP systems that support HP SSO (previously called LWSSO). For example, if users have logged onto another HP product web client that has HP SSO enabled, they can enter the HP Propel application directly, bypassing the HP Propel logon screen.
Identity	Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation). For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
IT security architecture	A description of security principles and an overall approach for architecture complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
IT security goal	See "Security goal".

IT-related risk	The net mission/business impact considering (1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to: 1. Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. 2. Non-malicious errors and omissions. 3. IT disruptions due to natural or man-made disasters. 4. Failure to exercise due care and diligence in the implementation and operation of the IT. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
JBoss Enterprise Application Platform	A Java EE-based application server run time platform used for building, deploying, and hosting highly-transactional Java applications and services.
Keystore	A keystore includes a database containing a private key and an associated certificate, or an associated certificate chain. The certificate chain includes the client certificate and one or more certification authority (CA) certificates.
Least Privilege	The practice of limiting access to the minimal level that will allow normal functioning. This means giving a user account only those privileges that are essential to that user's work.
Lightweight Directory Access Protocol (LDAP)	LDAP is an industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. The directory services share information about users, systems, networks, services, and applications throughout the network.
RabbitMQ	An open source message broker software (sometimes called message-oriented middleware) that implements the Advanced Message Queuing Protocol (AMQP).
Risk	A possible event that could cause damage. For example, financial loss, damage to the company image, and so on. See “IT-related risk”.
Risk analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Risk assessment	See “Risk analysis”.

Risk management	The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Role	A role is a collection of permissions.
Role Permission	A permission is a predefined authorization to perform a task. Usually permissions are assigned to a role.
Secure Sockets Layer (SSL)	A protocol for transmitting private documents via the internet. SSL uses a cryptographic system that uses two keys to encrypt data @ a public key known to everyone and a private or secret key known only to the recipient of the message.
Security	Security is a system property. Security is much more than a set of functions and mechanisms. IT security is a system characteristic as well as a set of mechanisms that span the system both logically and physically. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Security domain	A set of subjects, their information objects, and a common security policy. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Security goals	The security goals are identified by the security policy to guide the procedures, standards and controls used in the IT security architecture design.The security goals are confidentiality, availability, integrity, accountability, and assurance. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Security policy	The statement of required protection of the information objects. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Simple Mail Transfer Protocol (SMTP)	A protocol for sending e-mail messages between servers. It is generally used to send messages from a mail client to a mail server.
Single sign-on (SSO)	See "HP SSO".
System integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
System Security	The processes and mechanisms by which computer-based equipment, information, and services are protected from unintended or unauthorized access, change, or damage.
Threat	Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

Threat analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Threat source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability. Threats arise from human actions and natural events. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Topology	In networking, the logical connections that act between the different gateways, routers, and servers. For details, see ProProfs (http://www.proprofs.com/mwiki/index.php/Security_Topologies).
Transport Layer Security (TLS)	A cryptographic protocol that provides communication security over the internet. Its predecessor is Secure Sockets Layer (SSL). It uses X.509 certificates (asymmetric cryptography) to authenticate the counterpart and to exchange a symmetric key.
Trust model	The generation of trusted authorities or user trust through cryptography. Security is typically based on the authenticated identity of external parties, in centralized systems. In more recent cases, centralized systems have moved to distributed computing that require both authorizing an operating and authenticating the claiming entity.
Truststore	A truststore contains only the certificates trusted by the client (a “trust” store). These certificates are certification authority (CA) root certificates, that is, self-signed certificates. For details, see Oracle (http://docs.oracle.com/cd/E19509-01/820-3503/ggffo/index.html).
User	A user is an object associated with a person (or application entity) representing the person and defining their authorization. Roles are assigned to users to define the actions they are authorized to perform in the application. You can configure different types of users: using LDAP or HP SSO. It is recommended to use LDAP users because LDAP users are secured according to policies implemented by the LDAP provider.
Virtual appliance	A virtual appliance is a preconfigured virtual machine image, ready to run on a hypervisor. Virtual appliances are a subset of the broader class of software appliances. Installation of a software appliance on a virtual machine and packaging that into an image creates a virtual appliance.
Vulnerability	A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system’s security policy. For details, see http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

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 Security Guide (HP Propel 1.10)

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 csa_propel_ie@hp.com.

We appreciate your feedback!


Java™
COMPATIBLE