HP Operations Orchestration

Software Version: 10.2x
Windows and Linux Operating Systems

Security Guide

Document Release Date: May 2015
Software Release Date: November 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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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: **https://softwaresupport.hp.com/**

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**

Contents

Introduction

Welcome to the HP OO Security Guide.

This guide is designed to help IT professionals who deploy and manage HP Operations Orchestration (HP OO) instances in a secure manner. Our objective is to help you make well-informed decisions about the various capabilities and features that HP OO provides to meet modern enterprise security needs.

Security requirements for the enterprise are constantly evolving and this guide 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 guide, please open a support case with the HP support team to document them and we will include them in future editions of this guide.

This document relates to HP OO version 10.2x.

Security Updates Since the Previous Version

Between HP OO 10.10 and 10.20 the following security updates were made:

- It is now possible to grant permissions for system accounts in HP OO. This enables the administrator to control which users can view which system accounts and run flows that use them. This feature is useful for customers with multiple organizations, who may wish to hide some of the system accounts from some users.

  For more information, see "Content Management Enhancements - Apply Permissions to Multiple Roles" in the *HP OO 10.20 Release Notes*.

- When you upgrade an HP OO installation from an earlier 10.x version, the SSL truststore is updated to include the up-to-date trusted root certificates, as published by Oracle. This includes deletion of expired certificates, and import of new ones.

  For more information, see "Installation Enhancements - Updated Trusted Root Certificates" in the *HP OO 10.20 Release Notes*.

- HP OO now offers the option to audit events, so that you can track security breaches. Auditing lets you track actions that took place on Central, such as logins, triggering flows, creating schedules, editing configurations, and so on.

  Currently, you can retrieve the audit trail only via APIs. For more information, see the "Audit" chapter in the *HP OO API Guide*.

- HP OO also supports encryption keys that are sized 2048 bits long (and longer). This is aligns our cryptography keys with the FIPS 186-4 standard.

- A new sslEnabledProtocols property has been added to the **server.xml** file (located at **<installation_folder>/central/tomcat/conf/server.xml**):

```
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
```

This property ensures that only TLS v1, TLS v1.1 and TLS v1.2 are allowed and that SSL 3.0 is not. This prevents vulnerability to the “POODLE” attack (Padding Oracle On Downgraded Legacy Encryption).

Related Documents

For more information about the security hardening of HP OO, see the following documents:

- *HP OO Hardening Guide*
- *HP OO Network Architecture White Paper*

For more information about HP OO, see the following documents:

- *HP OO Concepts Guide*
- *HP OO Administrator Guide*
- *HP OO Installation Guide*
- *HP OO Architecture Guide*
- *HP OO Database Guide*
- *HP OO Central User Guide*
- *HP OO Studio Authoring Guide*
- *HP OO Release Notes*
- *HP OO System Requirements*
- *REST Wizard User Guide*

These and other documents can be found on HPLN (https://hpln.hp.com/node/21/otherfiles#).

Security Concepts

HP OO Glossary

For more information about HP OO concepts, see the *HP OO Concept Guide*.

Role Permission

A permission is a predefined authorization to perform a task. HP OO Central includes a set of permissions that can be assigned to roles.

For example, the **Schedule** permission grants the ability to view and create run schedules.

Role

A role is a collection of permissions.

For example, the **Flow Administrator** role may be assigned the **View Schedules** permission and the **Manage Schedules** permission.

User

A user is an object associated with a person (or application identity) representing the person and defining their authorization.

Roles are assigned to users, to define the actions they are authorized to perform in Central. For example, the user Joe Smith may be assigned the **Flow Administrator** role.

It is possible to configure different kinds of users:

- **LDAP users** log on to Central using their LDAP user name and password. For example, using their Active Directory user name and password.
- **Internal users** log on to Central using the user name and password that was set up locally in Central.
- **LWSSO** - HP Lightweight 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 LWSSO. For example, if users have logged onto another HP product web client that has LWSSO enabled, they can enter the HP OO Central application directly, bypassing the HP OO Central logon screen.

When an internal user and an LDAP user with the same role are logged in, there is no difference between their permissions.

Note: It is recommended to use LDAP users rather than internal users, because LDAP users are secured according to policies implemented by the LDAP provider.

Content Permission

Content permission is permission to view or run individual flows or the flows in a particular folder.

Users who have been assigned a specified role will be able to access the flows according to the content permissions assigned to their role.

For example, users with the **Administrator** role may be entitled to view and run all the flows in the system, while users with the **User** role may be entitled to run certain flows, and have view permission for others.

Common Security Concepts

System Security

The processes and mechanisms by which computer-based equipment, information, and services are protected from unintended or unauthorized access, change, or damage.

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.

Authentication

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

Authorization

Permission to access system objects, based on an individual's identity.

Encryption

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 encode it. For example, the TLS protocol encrypts the communication data.

Countermeasure

A way to mitigate the risk of a threat.

Defense in Depth

Layers of protection, so that you don't have to rely on a single security measure alone.

Risk

A possible event that could cause damage. For example, financial loss, damage to the company image, and so on.

Threat

Triggering a risk event that exploits a vulnerability.

Vulnerability

A weakness in a target that can potentially be exploited by a security threat.

Secure Implementation and Deployment

Default Security Settings

In many cases, it is recommended to modify the default security settings that are provided out-of-the-box.

- **Authentication** – By default, authentication is not enabled in Central. It is recommended to enable it, as soon as users have been set up. For more information, see "Enabling Authentication" in the *HP OO Central User Guide*.
- **Auditing** – By default, auditing is not enabled in Central. It is recommended to enable it. For more information, see "Enabling Auditing" in the *HP OO Central User Guide*.
- **TLS Encryption** – By default, HP OO supports three TLS protocols: 1.0, 1.1, 1.2. It is recommended to work with the latest version. For more information, see "Configuring the TLS Protocol" in the *HP OO Hardening Guide*.
- **TLS Server Certificate** – By default, the user is asked to provide a CA certificate during the installation of the HP OO Server.
- **Client Certificate** – By default, Client Certificate is not enabled. It is recommended to work with Client Certificate to authenticate to Central. For more information, see "Configuring Client Certificate Authentication in Central" in the *HP OO Hardening Guide*.
- **KeyStore, TrustStore, and Server Certificate Passwords** – By default, Java passwords are provided for the keyStore, trustStore, and Server Certificate. It is recommended to replace these with encrypted passwords. For more information, see "Changing and Encrypting/Obfuscating the KeyStore/TrustStore Password" in the *HP OO Hardening Guide*.
- **RC4 Cipher** – By default, the RC4 cipher is enabled. It is recommended to disable the RC4 cipher on the JRE level. For more information, see "Removing the RC4 Cipher from the SSL-supported Ciphers" in the *HP OO Hardening Guide*.
- **Security Banner** – By default, the security banner is not enabled in Central. It is recommended to enable it, with your custom message. For more information, see "Setting Up a Security Banner" in the *HP OO Central User Guide*.
- **Windows Authentication of the Database** – By default, Windows authentication is not enabled in Central. If you are working in the Windows and SQL server environment, it is recommended configure HP OO to work with Windows authentication. See "Configuring HP OO to Work with Windows Authentication" in the *HP OO Database Guide*.
- **Default Algorithms** – The **encryption.properties** file contains the default algorithms. If you want to be compliant with FIPS, see "Configuring HP OO for FIPS 140-2 Level 1 Compliance" in the *HP OO Hardening Guide*. For more information about the FIPS 140-2 Level 1 defaults, see "Encryption Administration" in "Encryption" on page 20.

- **Java Policy** – By default, the **java.policy** file is not hardened. For information about how to modify the **java.policy** file, see "Preventing Flows from Accessing the Central/RAS Local File System" in the *HP OO Hardening Guide*.

HP OO Security Hardening

In addition to this *HP OO Security Guide*, it is recommended to see the *HP OO Hardening Guide*.

The *HP OO Hardening Guide* provides recommendations for safeguarding your HP OO deployment from security risks or threats. Some of the most important reasons to secure an application include protecting the confidentiality, integrity, and availability of an organization's critical information.

To comprehensively protect your HP OO system, it is necessary to secure both HP OO and the computing environment (for example, the infrastructure and the operating system) upon which the application runs.

The *HP OO Hardening Guide* provides recommendations to help secure HP OO at the application level and does not cover how to secure the infrastructure within the customer environment. The customer is solely responsible for understanding his/her infrastructure/environment and applying the respective hardening policies.

Physical Security

HP Software recommends that HP OO is protected by physical security controls defined by your organization. The HP OO server components are installed in a physically secured environment, according to best practice. For example, the server must be in a closed room with access control.

Secure Installation Guidelines

Supported Operating Systems

For the types and versions of supported operating systems, see the *HP OO System Requirements*.

Operating System Hardening Recommendations

Contact your operating system vendor for recommended best practices for hardening your operating system.

For example:

- Patches should be installed
- Unnecessary services/software should be removed or disabled
- Minimal permissions should be assigned to users
- Auditing should be enabled

Tomcat Hardening

When you install HP OO Central, Tomcat is partially hardened by default. If you want extra hardening, see the recommendations in the *HP OO Hardening Guide*.

Installation Permissions

The following permissions required to install and run HP OO:

Installing HP OO	Windows/Linux: Any standard user who is able to run a Java process, and who has permission to create folders and services
Running HP OO	• Windows: The Windows service runs as the system user or a specific user (the user must have access to the HP OO installation directory) • Linux: Any standard user who is able to run a Java process

See also the recommendations in the CIS Apache Tomcat 7.0 document.

Network and Communication Security

The *HP OO Architecture Guide* describes the basic HP OO topology, high availability, and load balancer security.

The *HP OO Network Architecture White Paper* describes the required firewall configuration, and suggests two workarounds that can be applied in cases when, due to policy restrictions, the required firewall configuration cannot be implemented:

- SSH reverse tunneling
- Reverse proxy

Communication Channel Security

Supported Protocols and Configuration

HP OO supports the TLS protocol.

For more information, see "Replacing the Central TLS Server Certificate" in the *HP OO Hardening Guide*.

The Central ports are defined by the administrator during the installation.

Channel Security

HP OO supports the following secure channels:

Channel (Directed)	Supported Secure Protocol
OOSH, browser, Studio Remote Debugger, or RAS → Central	For a secure channel, use the TLS communication for encryption and Client Certificate for authentication.
Central → LDAP Server	To encrypt communication between Central and LDAP, use Secure LDAP, using the TLS protocol.

Administration Interface Security

Accessing the Administration Interface

There are several ways to control access to the administration interface:

- Credentials
- Client certificate
- SAML

Securing the Administration Interface - Recommendations

1. It is recommended to enable authentication in Central.

   See "Enabling Authentication" in the *HP OO Central User Guide*

2. It is recommended to secure the administration interface with the TLS protocol. You should set up TLS between the client and the Central interface for encryption.

   See "Server and Client Certificate Authentication" in the *HP OO Hardening Guide*.

3. It is recommended to work with LDAP users, rather than internal users, because this is more secure.

4. It is recommended to set up authentication to access Central via Client Certificates. This is more secure than user passwords.

   See "Server and Client Certificate Authentication" in the *HP OO Hardening Guide*.

User Management and Authentication

Authentication Model

To enable easy bootstrapping of the authentication mechanism in HP OO, the product starts with authentication disabled.

It is strongly recommended to enable authentication immediately after installation.

For information about how to enable authentication, see "Enabling Authentication" in the *HP OO Central User Guide*.

There are a number of ways to authenticate access to Central.

Choose the method of identifying users:

- User name and password
- Client Certificate
- SAML token
- Single sign on (HP LWSSO)

Choose one of two ways to manage the users:

- LDAP users , saved on an LDAP server as Active Directory (recommended)
- Internal users and passwords, saved locally on the Central server (not recommended)

Types of Users

Different types of users can have different permissions assigned for them. For example, flow author, administrator, system administrator, and so on.

For more examples of different types of users, requiring different permissions, see "Major Personas" in the *HP OO Concepts Guide*.

Authentication Administration and Configuration

Internal or LDAP Users

You can set up internal users with passwords in the Central UI or define the user in the LDAP server and map LDAP groups to Central roles.

Note: Our recommendation is not to use internal users, but to use a more secure alternative such as LDAP users.

For information about configuring internal users, see "Setting Up Security – Internal Users" in the *HP OO Central User Guide*.

For information about mapping LDAP groups to Central roles, see "Setting Up Security – LDAP Authentication" in the *HP OO Central User Guide* and "LDAP Configuration" in the *HP OO API Guide*.

SAML / Client Certificates / LW SSO

For information about configuring Central to work with SAML, see "Setting Up Security – SAML" in the *HP OO Central User Guide*.

For information about configuring Central to work with Client Certificates, see "Client Certificate Authentication" in the *HP OO Hardening Guide*.

For information about configuring Central to work with LW SSO, see "Setting Up Security – LWSSO" in the *HP OO Central User Guide*, "Configuring LWSSO Settings" in the HP OO Administration Guide, and "LW SSO" in the *HP OO API Guide*

Database Authentication

OO supports 4 databases: Oracle, MS SQL, MySQL, and Postgres.

We recommend using a strong database password for database authentication and using a strong password policy. For example, blocking after a number of failed attempts.

When using MS SQL, it is possible to work with either database authentication or with OS authentication. Our recommendation is to work with OS authentication, where this is possible. For example, it is possible to use Windows authentication to access Microsoft SQL Server databases.

- For information about setting up OS authentication, see "Configuring HP OO to Work with Windows Authentication " in the *HP OO Database Guide*.
- See "Changing the Database Password" in the *HP OO Administration Guide*.
- See the best practices recommended by the database vendor (if these exist).

Authorization

Authorization Model

User access to HP OO resources is authorized based on the user's role, and the permissions configured for that role.

See:

- "Setting Up Security – Roles" in the *HP OO Central User Guide*
- "Assigning Permissions to a System Account" in the *HP OO Central User Guide*

Minimal Permissions Guidelines

It is recommended to:

- Select appropriate permissions for the role.
- Use minimal permissions when creating new roles.
- Grant minimal permissions and extend the permissions only as needed to avoid unwanted privilege escalation. For example, start with Viewer permissions and add additional permissions individually as needed.

Authorization Configuration

Central is installed with a number of out-of-the box roles, which you can configure and assign to users. By default, the out-of-the box roles are assigned the following permissions:

Role	Default Permissions
Administrator	All
End_user	None
Everybody	None
Promoter	All the **Content** permissions
System_admin	All the **System** permissions

Default Role

It is possible to configure one of the roles with the **Default Role** attribute. If you do so, make sure that this is the role with the least privileges. Remember that when you give permissions to this role, this affects all LDAP users, in addition to those are explicitly associated with the role.

For more information, see "Assign a role to be the default role" under "Setting Up Security – Roles" in the *HP OO Central User Guide*.

See also:

- "Assigning Permissions to a System Account" in the *HP OO Central User Guide*
- "Setting Permission for Content" in the *HP OO Central User Guide*

Backup

In order to prevent data loss, It is highly recommended to back up your data on the servers onto secure media on a regular basis. This is also helpful for disaster recovery and business continuity.

After installing HP OO, make sure to back up the **central\var\security** folder and the **central\conf\database.properties** file.

Some data on the database schema is encrypted and the keys for decryption are stored locally on the HP OO Central server. If these system files become corrupted or deleted, the schema will be useless, because there will be no way to decrypt the data.

Note: The keys are encrypted, so it is important to include them in the backup. The keys are located in the **security** folder.

See:

- "Backing Up HP OO" in the *HP OO Administration Guide*
- "Setting up Disaster Recovery" in the *HP OO Administration Guide*
- "Backing Up and Recovering the Central Security Files" in the *HP OO Installation Guide*
- "Using a Load Balancer in HP OO Deployment" in the *HP OO Architecture Guide*

Encryption

Encryption Model

HP OO supports encryption and hash algorithms to protect sensitive data. Encryption is designed to prevent the exposure and modification of sensitive data, such as passwords, definitions, and so on, in the HP OO system.

It is important to use well known, standard algorithms without known vulnerabilities, in order to prevent decryption by unauthorized persons.

Note: For example, SSL is not used, because of known vulnerabilities in the SSL protocol.

Static Data

All saved passwords are protected using well known algorithms and none are left in cleartext.

For example:

- The system account passwords are encrypted.
- The internal user passwords are hashed.
- The database passwords are encrypted.

Data in-transit

HP OO uses the Transport Layer Security (TLS) protocol to encrypt the data between components (such as Central and RAS).

Disabling the HTTP port

It is recommended to disable the HTTP port, for security reasons, so that the only communication channel will be on TLS and encrypted. For more information, see "Changing or Disabling the HTTP/HTTPS Ports" in the *HP OO Hardening Guide*.

Encryption Administration

Recommended Encryption Best Practices

In order to reach higher levels of security and cryptography, it is recommended to configure HP OO to be compliant with Federal Information Processing Standards (FIPS) 140-2. HP OO can be set to be compliant with FIPS 140-2 Level 1.

Default Configuration Set

- Symmetric-key algorithm: AES with key size 128
- Hashing algorithm: SHA1

Advanced Settings

After you have configured HP OO for FIPS 140-2 compliance, HP OO uses the following security algorithm:

- Symmetric-key algorithm: AES256
- Hashing algorithm: SHA256

See "Configuring HP OO for FIPS 140-2" in the *HP OO Hardening Guide*.

Digital Certificates

A digital certificate is an electronic "passport" for a person, server, station, and so on.

- To use encryption between a browser and the Central server, you need to install a digital certificate on the server side.
- To use Client Certificate to authenticate the Central server, you need to install a Client Certificate on the client side (for example, on the browser, RAS, OOSH, Studio, and so on).

HP OO uses the Java Keytool utility to manage cryptographic keys and trusted certificates. This utility is included in the HP OO installation folder, in **<installation dir>/java/bin/keytool**.

Certificate Location

Installations of HP OO Central include two files for the management of certificates using Keytool:

- **<installation dir>/central/var/security/client.truststore**: Contains the list of trusted certificates
- **<installation dir>/central/var/security/key.store**: Contains the HP OO private certificate (including the private key)

Access Control to KeyStore and TrustStore

It is recommended that the TrustStore and KeyStore are stored with read permissions only for the user that runs the Central service.

Replacing the HP OO Self-signed Certificate

It is recommended to replace the HP OO self-signed certificate after a new installation of HP OO or if your current certificate has expired.

Part of the process of replacing the certificate is generating a PKCS12 format certificate, using your CA. Contact your CA for specific details about the certificate process or refer to your corporate policy.

For more information, see "Replacing the Central TLS Server Certificate" in the *HP OO Hardening Guide*.

Sensitive Information in a Content Pack

System Account Passwords

Do not include passwords when creating a content pack. The passwords will be obfuscated inside the content pack, which is not a secure option.

The HP OO security best practice is to configure the system account passwords in Central. For more information, see "Setting Up System Accounts for a Content Pack" in the *HP OO Central User Guide*.

Auditing and Log Files

Auditing

Auditing lets you track actions that took place on the Central server, such as logins, triggering flows, creating schedules, editing configurations, and so on. The audit data enables you to track user activity on the Central system, tracking who did what action, when. For example, auditing will show that a user ran a flow, updated a configuration, deleted a schedule, or failed authentication.

The audit data is saved in the database. For more information, see "Auditing" in the *HP OO API Guide*.

Logs

Logs let you trace errors, warnings, information, and debugging messages.

The logs are saved in the file server, in the following locations:

<oo-installation>/central/var/logs

<oo-installation>/studio/logs

<oo-installation>/ras/var/logs.

No Sensitive Data Kept in Audit Records and Log Files

No sensitive data is kept in the audit records or in the log files in the HP OO system.

Getting Audit Records

You can get the audit records via API or via a query to the OO_AUDIT table. For more information, see "Auditing" in the *HP OO API Guide*.

Example of audit data:

```
[
{
“time”:1412312016740, “type”:”AuditConfigurationChange”,
“group”:”AuditManagement”, “subject”:” mydomain\myuser2”,
“outcome”:”Success”, “data”:”{"enabled":false}”
},
{
“time”:1412312016722, “type”:”InternalUserDelete”, “group”:”Authentication-
Authorization”, “subject”:”mydomain\myuser2”, “outcome”:”Success”, “data”:
{"usersNames":["admin"]}"
}
]
```

APIs and Interfaces

API and Interface Model

You can work with the HP Operations Orchestration public Application Programming Interfaces (APIs) instead of via the HP OO Central UI, to perform the same actions. Some actions can only be performed via APIs, such as purging and auditing. The public API is HTTP-based. All APIs are RESTful and use JavaScript Object Notation.

Features and Administration of the API and Interface Security Configuration

It is important to work securely with the APIs. Use the security mechanisms mentioned in this guide (authentication, encryption, and so on) while working with the APIs.

The API interface can work on HTTP or HTTPS.

Note: When you use our APIs to display HTML, it is your responsibility to protect it from XSS attacks.

For more information, see the following chapters in the *HP OO API Guide*:

- "LDAP Configuration"
- "Users"
- "LW SSO Configuration"
- "Authentication"
- "Roles"

Security Questions and Answers

How can I generate a certificate request that can be signed by an external CA?

Export the certificate request and send it to the external CA for signing. For instructions, see "Replacing the Central TLS Server Certificate" in the *HP OO Hardening Guide*.

Which TCP/UDP ports does HP OO use? What is the direction, user, and encryption?

When you install HP OO, you need to configure at least one available port for the Central Server in the HTTP/HTTPS fields. The default provided values are 8080 and 8443, but you can change these. For more information about secure channels between Central and the other components, see "Network and Communication Security" on page 13

Where and how are the credentials stored (admin accounts, integration users)?

See "User Management and Authentication" on page 15.

How do I configure self-signed SSL certificates for Central/RAS /Studio?

During the installation of HP OO, if you do not provide a certificate, a self-signed certificate is created by default. However, it is not recommended to use self-signed certificates, for security reasons. HP recommends working with a certificate from custom-root CA or from a well-known CA.

For more information about configuring certificates for HP OO, see "Encrypting the Communication Using a Server Certificate" in the *HP OO Hardening Guide*.

How do I enable or disable any kind of auditing?

By default, auditing is not enabled. For details on how to enable it, see "Enabling Auditing" in the HP OO Central User Guide. For more information about auditing, see "Auditing and Log Files" on page 23.

How much detail is in the logs, and how do I change the amount of logging?

The logs can be set to different levels of granularity. The default level is INFO, but you can adjust this. For details, see "Adjusting the Logging Levels" in the *HP OO Administration Guide*.

For more information about log files, see "Auditing and Log Files" on page 23.

How is sensitive information encrypted?

See "Encryption" on page 20.

Is the communication between Central and RAS encrypted?

If you use HTTPS, it is encrypted.

Is the communication between HP OO and other integration components (HPNA, CSA, AD, and so on) encrypted?

This depends on the integration that you are using. If you use HTTPS, it is encrypted.

How can I restrict access to the Flow Library, based on the user roles?

See "Setting Up Security – Roles" in the *HP OO Central User Guide*.

What authentication mechanism does HP OO support?

The supported authentication mechanisms are LDAP, SAML and internal users. HP OO also supports Client Certificate and LWSSO. See "User Management and Authentication" on page 15.

Is HP OO FIPS 140-2 compliant?

Yes. For more information, see "Configuring HP OO for FIPS 140-2 Level 1 Compliance" in the *HP OO Hardening Guide*.

What are the authentication methods between Central and RAS?

User password or Client Certificate.

Are all passwords stored encrypted or hashed?

Yes. All saved passwords are protected using well known algorithms and none are left in cleartext.

Can I limit the Central user IP address?

No, this is not supported at the moment.

Is HP OO certified for common criteria?

This is in progress. We are currently "in evaluation". For details, see https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/publication/list/evaluation-product.

When I use OOSH, can I pass sensitive data to Central?

Our recommendation is to use a secure channel when connecting to Central. See "Network and Communication Security" on page 13.


Java™
COMPATIBLE