HP Project and Portfolio Management Center

Software Version: 9.31

Security Guide

Document Release Date: January 2015
Software Release Date: January 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **https://softwaresupport.hp.com**

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.

The following table indicates changes made to this document since the last released edition.

Support

Visit the HP Software Support Online website at: **https://softwaresupport.hp.com**

This website 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 website 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 website. 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 website is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Welcome to This Guide

Welcome to the HP Project and Portfolio Management Center (PPM Center) Security Guide.

This guide provides information for working with PPM Center in a secure environment.

Chapter 1: Secure Implementation and Deployment

This chapter provides information on implementing and deploying PPM Center in a secure manner.

Technical System Landscape

PPM Center is an enterprise-wide application based on Java 2 Enterprise Edition (J2EE) technology. J2EE technology provides a component-based approach to the design, development, assembly, and deployment of enterprise applications. For details, see the *Installation and Administration Guide*.

Security in Basic PPM Center Configuration

For security recommendations for a basic PPM Center configuration, see the *Installation and Administration Guide*.

Security in Clustered PPM Center Configuration

For security recommendations for a clustered PPM Center Configuration, see the *Installation and Administration Guide*.

External SSO Authentication

PPM Center supports external SSO authentication with specific configurations, such as NTLM authentication with Microsoft IIS or SiteMinder. For details, see the *Installation and Administration Guide*.

Common Security Considerations

Thoroughly review the trust boundaries between PPM Center components (PPM Center servers, database servers, LDAP servers, and other integrating servers) to minimize the number of hops. In

addition, it is recommended to use SSL to secure access to servers located across such boundaries.

Note: Currently, PPM Center does not support secure channels to database server. When there is a firewall between any PPM Center deployment components, ensure the proper configuration according to the vendor recommendation.

Best Practice

Although the PPM Center application server supports SSL, it is expected and recommended that the front end server, either the load balancer or the reverse proxy will be configured to require SSL.

Chapter 2: Security Related PPM Server Configuration Parameters

This chapter contains reference to some of the PPM Center server configuration parameters that are relevant to security. Full details can be found in the *Installation and Administration Guide*.

Secure PPM Center Storage

PPM Center allows users to upload files to the server. All files uploaded to the server must be validated, since they can contain viruses, malicious code, or Trojan horses that could infect the entire system. An attacker or a malicious user can upload malicious files from one account and then download them to diverse clients.

It is strongly recommended to implement proper antivirus protection for the file storage allocated for the PPM Center repository.

In addition, the size of the file uploaded as an attachment can be limited by setting the `MAX_WEB_ATTACHMENT_SIZE_IN_MB` server configuration parameter.

Secure Debug Features

PPM Center provides a set of tools for troubleshooting and for 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 following server configuration parameters. It is recommended to validate that the parameters are reset to the default values immediately after using the debugging feature.

The debugging related server configuration parameters are:

- `MULTICAST_DEBUG`
- `SHOW_DEBUGGING_CONSOLE_PER_USER`
- `SQL-Debug`
- `DISABLE_VERBOSE_ERROR_MESSAGES`

JMX Console

JMX console is used to diagnose PPM Center internal services. For details, see the *Installation and Administration Guide*. It is important to limit the JMX console access to only authorized users.

Password Constraints

Admins can set PPM Center user password constraints to secure the PPM Center users.

The following parameters control the user password constraints:

- `USER_PASSWORD_MAX_LENGTH`

  HP recommends that admins set the value of this parameter to `20`.

- `USER_PASSWORD_MIN_DIGITS`

  HP recommends that admins set the value of this parameter to `1`.

- `USER_PASSWORD_MIN_LENGTH`

  HP recommends that admins set the value of this parameter to `8`.

- `USER_PASSWORD_MIN_SPECIAL`

  HP recommends that admins set the value of this parameter to `1`.

HttpOnly

`HttpOnly` is an additional flag included in a Set-Cookie HTTP response header. Using the `HttpOnly` flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie (if the browser supports it).

The HttpOnly parameter is

- `USE_HTTPONLY`

DMS

The followings are the DMS configuration parameters:

- DMS_INSECURE_FILE_EXTENSION_CHECK
- DMS_XSS_CHECK

HP recommends that admins set the values of the above parameters to `true`.

Chapter 3: Installation Security

This chapter provides information on aspects of installation security.

Supported Operating Systems

For the list of supported system environments, see the *Overview of Platform Support*.

Note: The supported environment information in the *Overview of Platform Support* is accurate for the PPM Center version 9.30 release, but there may be subsequent updates. For the most up-to-date supported environments, go to the HP Software manuals site: h20230.www2.hp.com/selfsolve/manuals.

Web Server Security Recommendations

IIS Web Server

See http://www.iis.net/ for information on enabling SSL for all interactions with the Web server.

Note: SSL should be enabled for the entire IIS Web server under which you installed the PPM Center applications.

To disable weak ciphers on IIS, go to http://support.microsoft.com/kb/187498/en- us.

Apache Web Server

See http://httpd.apache.org/docs/current/ssl/ssl_howto.html for information on enabling SSL for all interactions with the Web server and on enforcing strong security.

Application Server Security Recommendations

When configuring SSL on the PPM Center application server, keep your keystore in a private directory with restricted access. The keystore is password protected. Although the Java keystore is password protected, it is vulnerable as long as the password was not changed from its default value of `changeit`.

- Always change default passwords.
- Always encrypted the password in the server configuration. Please see "Configuring Secure Web Logon (Optional)" in the *Installation and Administration Guide*.
- Since the default *admin* user password is documented in PPM Center, it is strongly recommended to change the admin user's password.
- Always change the default password when creating a database schema.
- Always use the minimal possible permissions when installing and running PPM Center.

See the *Creating a System Account* for PPM Center section in the *Installation and Administration Guide* to learn the minimal permission requirement on both Windows and Linux.

See the following sections in the PPM Center *Installation and Administration Guide* to learn the minimal permission requirement on Oracle database:

- Default Permissions for PPM Center Center Schemas

- Other Permissions Needed or Not Needed for PPM Center Center

FAQ

Question

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

Answer

The user can change the location for the PPM Center log files and attachments uploaded to PPM Center according to best practices to avoid mixing user data with configuration files.

Question

Does PPM Center install with unnecessary functionality disabled by default?

Answer

Yes, functionality is license driven.

Question

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

Answer

Yes.

Question

Does PPM Center execute with no more privileges than necessary for proper operation?

Answer

Yes.

Chapter 4: Network and Communication Security

This chapter provides information on network and communication security.

Secure Topology

The PPM Center 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 PPM Center servers:

- Reverse proxy architecture

  One of the more secure recommended solutions is to deploy PPM Center using a reverse proxy. PPM fully supports reverse proxy architecture as well as secure reverse proxy architecture. See the *Installation and Administration Guide* for information on configuring an external Web server as reverse proxy for PPM Center.

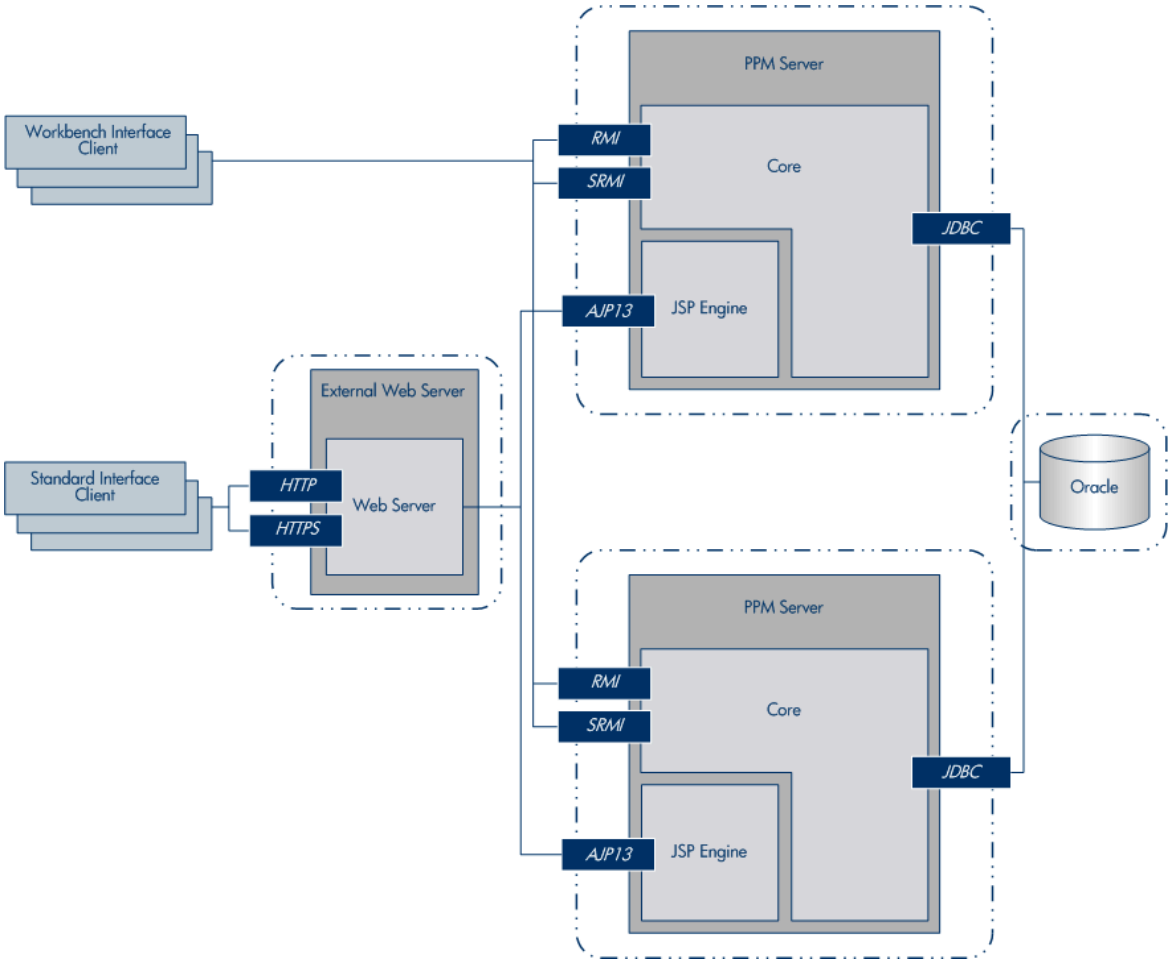
- SSL communication protocol

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

- DMZ architecture using a firewall

  The secure architecture referred to in this document is a typical DMZ architecture using a device as a firewall. The basic concept is to create a complete separation, and to avoid direct access, between the PPM Center clients and the PPM Center servers. This is especially important when opening access to PPM Center to external clients from outside of your organization.

- Server Cluster Hardware Load Balancer Configuration



- Distributed Denial of Service attack protection

  Consider implementing DDoS attack protection on servers hosting PPM Center Web client only in cases where your PPM Center Web client is exposed to the public Internet. In most production environments, deploying PPM Center Web client on the public Internet are rare so carefully consider if this best practice applies to your specific deployment.

  A few DDoS attacks such as Slowloris may be mitigated by implementing third-party protections such as the following:

  - mod_reqtimeout – applicable if using Apache HTTP server
  - mod_qos – applicable if using Apache HTTP server
  - F5 Big IP LTM iRule – applicable if using F5 hardware load balancer in front of the PPM Center Web client

Note: Due to the nature of these types of attacks, it is not possible to implement application-specific fixes or enhancements to prevent these types of attacks.

For more information, refer to the following:

- https://en.wikipedia.org/wiki/Denial-of-service_attack
- http://ha.ckers.org/slowloris/
- http://opensource.adnovum.ch/mod_qos/
- https://httpd.apache.org/docs/trunk/mod/mod_reqtimeout.html
- https://bz.apache.org/bugzilla/show_bug.cgi?id=54263
- https://f5.com/resources/white-papers/mitigating-ddos-attacks-with-f5-technology

Reverse Proxy for Stand Interface Client (Web Client)

A reverse proxy is an intermediate server that is positioned between the client machine and the Web servers. To the client machine, the reverse proxy seems like a standard Web server that serves the client machine's HTTP or HTTPS protocol requests, with no dedicated client configuration required.

The client machine sends ordinary requests for Web content, using the name of the reverse proxy instead of the name of a Web server. The reverse proxy then sends the request to one of the Web servers. Although the response is sent back to the client machine by the Web server through the reverse proxy, it appears to the client machine as if it is being sent by the reverse proxy.

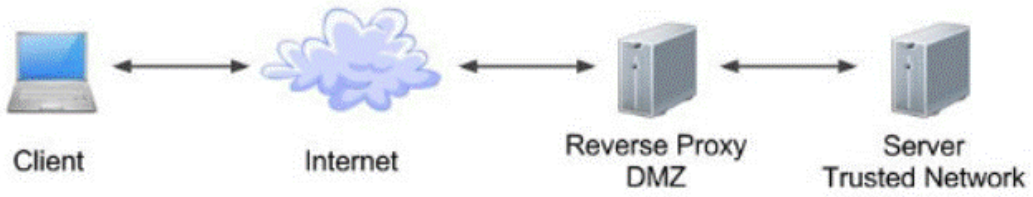
Reverse Proxy Security

A reverse proxy functions as a bastion host. It is configured as the only machine to be addressed directly by external clients, and thus obscures the rest of the internal network. Use of a reverse proxy enables the application server to be placed on a separate machine in the internal network, which is a significant security objective.

DMZ is a network architecture in which an additional network is implemented, enabling you to isolate the internal network from the external one. Although there are a few common implementations of DMZs, this chapter discusses the use of a DMZ and reverse proxy in a back-to-back topology environment.

The following are the main security advantages of using a reverse proxy in such an environment:

- No DMZ protocol translation occurs. The incoming protocol and outgoing protocol are identical (only a header change occurs).
- Only HTTP or HTTPS access to the reverse proxy is allowed, which means that stateful packet inspection firewalls can better protect the communication.
- A static, restricted set of redirect requests can be defined on the reverse proxy.
- Most of the Web server security features are available on the reverse proxy (authentication methods, encryption, and more).
- The reverse proxy screens the IP addresses of the real servers as well as the architecture of the internal network.
- The only accessible client of the Web server is the reverse proxy.
- This configuration supports NAT firewalls.
- The reverse proxy requires a minimal number of open ports in the firewall.
- The reverse proxy provides good performance compared to other bastion solutions.
- Using a secure reverse proxy architecture is easier to maintain. You can add patches to your reverse proxy as needed



Note:

- Although SSL can be enabled on PPM Center application server, it is expected and recommended that the front end server (load balancer or reverse proxy) will be configured to require SSL.
- Follow security guidelines for LDAP servers and Oracle databases.
- Run SNMP server with low permissions.

Communication Channels Security

PPM Center supports the following secure channels:

Secure Channel	How to Configure
Between browser and PPM Center server	In general, trust is only needed on the client. This is a trust to the authority that issued the server certificate for the PPM Center server.
Between PPM Center and LDAP server	PPM Center connects to a LDAP server either in clear text or over SSL. For details, see the *Installation and Administration Guide*.
Between PPM Center and mail server	PPM Center supports SMTP Authentication. PPM Center connects to SMTP Server either in clear text or over SSL. For details, see the *Installation and Administration Guide*.
Between RP/LB and PPM Center server	Configure the PPM Server to accept ajp13 protocol. Setup the reverse proxy or load balance to use Secure HTTP (HTTPs) for outbound communication and forwards the request to PPM Server by ajp13 protocol. For details, see the *Installation and Administration Guide*.

FAQ

Question

Are exceptions required to be added to the firewall policy?

Answer

Placing a reverse proxy in front of the PPM server is recommended. The list of ports to be open in the firewall for the incoming traffic is documented in the *Installation and Administration Guide*.

Chapter 5: Administration Console Interface

This chapter provides information related to PPM Server Configuration by Administration Console (or Admin Console).

Access to Administration Console

To disable access to the Administration Console interface (not including project customization) from the outside, the following URIs can be blocked at the front end (either the load balancer or the reverse proxy):

- `/itg/web/knta/admin/AdminConsole.jsp`

These URIs are subject to change and must be reviewed for each new major version of PPM Center.

Access to project customization can be restricted at the permissions level.

To secure the Administration Console interface:

1. Change the administrator password during the initial setup.
2. Use a strong password for the administrator.

Required Permission to Administration Console

In order to access and use the Administration Console, you must:

- Have the User Administration license
- Have one or more of the following access grants

Access Grant	Permissions
Sys Admin: Server Tools: Execute Admin Tools	Let the user access the Administration Console and the server tools.

Access Grant	Permissions
Sys Admin: Server Tools: Execute SQL Runner	Enables the **SQL Runner** menu in the Administration Console and lets the user run SQL queries from the Administration Console. Without this access grant, the **SQL Runner** menu is invisible.
Sys Admin: Server Tools: Execute File Browser	Enables the File Browser menu Browse PPM Center Server files in the Administration Console and lets the user browse and download PPM Center Server files. Without this access grant, the File Browser is invisible.

Administration Console Actions

For details, see the*Installation and Administration Guide*.

- Viewing PPM Center Server Status from the Administration Console
- Working with Fiscal Periods from the Administration Console
- Viewing and Modifying Server Configuration Parameters from the Administration Console
- Configuring and Migrating the PPM Center Center Document Management system from the Administration Console
- Browsing and Downloading *<PPM_Home>* Directory Files from the Administration Console
- Running SQL Queries from the Administration Console
- Gathering Information for HP Software Support from the Administration Console
- Changing Data Display in Administration Console Tables

Chapter 6: User Management and Authentication

This chapter provides information related to user authentication.

Authentication Model

PPM Center supports the following authentication methods:

- Form login
- External authentication
  - SiteMinder - with special configuration required
  - LDAP server supporting the LDAP3 protocol
  - NTLM (Windows domain account) – integrating with IIS

Authentication Administration and Configurations

For details, see the *Installation and Administration Guide*.

FAQ

Question

Can PPM Center require account passwords that conform to corporate policy?

Answer

PPM Center supports password constraints. For details, check below server configuration parameters.

- USER_PASSWORD_MAX_LENGTH
- USER_PASSWORD_MAX_DIGITS
- USER_PASSWORD_MIN_LENGTH
- USER_PASSWORD_MIN_SPECIAL

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

Question

Describe the PPM Center user session management.

Answer

PPM Center manages user sessions on the application level. Each session has an expiration time that can be configured by the `KINTANA_SESSION_TIMEOUT` parameter.

Question

Can PPM Center limit the number of logon sessions per user and per application?

Answer

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

Chapter 7: Authorization

This chapter provides information related to user authorization in PPM Center.

Authorization Administration

User access to PPM Center resources is authorized based on the user's role and security group membership. See the *Security Model Guide and Reference* for details.

A user must be granted either a System Level License to configure or maintain PPM Center or an Application License to perform daily task.

The single user assigned to multiple groups receives the highest permissions. Check the permissions across all groups.

It is recommended to use minimal permissions when creating new groups. Make sure to select appropriate role for the group. It is always recommended to grant minimal permissions and extend the permissions only as needed to avoid unwanted privilege escalation.

FAQ

Question

Can PPM Center inherit users' information and authorization profiles from an external repository, such as LDAP?

Answer

No.

Question

Does PPM Center supports "role based access control"?

Answer

Yes.

Question

Does PPM Center support entity level access restriction?

Answer

Yes.

Question

Does PPM Center support Field Level access restriction?

Answer

Yes.

Chapter 8: Data Integrity

Data integrity is a critical security requirement. The data backup procedure is an integral part of this requirement.

PPM Center does not provide backup capabilities. Following are some important considerations:

- Backup is especially important before critical actions such as project upgrade. See the *Installation and Administration Guide* for details.
- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Since data backup consumes lots of resources, it is strongly recommended to avoid running backups during peak demand times.

Note: When backing up the database, ensure that the attachments and configuration files are backed up at the same time to reflect the same system state.

Chapter 9: Encryption Model

Full Disk Encryption (FDE)

Full disk encryption (FDE) is supported for all system components, including database, server, repository server, and client machines. Implementation of FDE can have an impact on system performance. For details, contact the vendor providing encryption.

PPM Center Encryption

PPM Center crypto capability is used to encrypt sensitive credentials and store them encrypted in the database or configuration file. Examples of sensitive data include credentials in the database server PPM Center uses, credentials to the LDAP with which PPM Center integrates, and credentials for machines that contain user data.

PPM Center crypto implementation uses the following security configuration:

```
Symmetric block cipher, AES engine, 128 bits key size, JCE provider
Public-key cipher, ElGamal engine, 600 bits key size
```

Password Encryption

User passwords are stored either in its encrypted format or hashed versions by MD5. Please check `kConvertUserPasswords.sh` in the *Installation and Administration Guide*.

By default, PPM Center uses ELGamal to encrypt password. After admin enable FIPs, PPM Center uses AES.

	Stand (Encrypted)	**Hash**
FIPS Enable	AES	MD5
FIPS Disable	ElGamal	MD5

FAQ

Question

Does PPM Center transmit account passwords in an approved encrypted format?

Answer

It is strongly recommended to enable SSL on the PPM Center and LDAP servers to ensure secured account password transmission.

Question

Does PPM Center store account passwords in approved encrypted format?

Answer

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

Question

Does PPM Center 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?

Answer

Partial.

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

Question

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

Answer

User name and password, NTLM, LDAP authentication.

Question

Is SAML v2.0 supported for performing authentication?

Answer

No.

Question

Is Single Sign On (SSO) supported?

Answer

Yes, for SiteMinder, NTLM, and HP LWSSO.

Question

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

Answer

PPM Center integrates with SiteMinder, where a remotely authenticated user name is passed in the header. This requires a separate configuration. For details, see the *Installation and Administration Guide*.

Chapter 10: Logs

This chapter provides information related to logs.

Log and Trace Model

PPM Center produces several logs for troubleshooting and audit. 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.

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.

Log and Trace Security Administration and Features

Sensitive data is kept on log files. PPM Center provides applicative logs that can report all system events according to log level. It is the user's responsibility not to insert unprotected sensitive data to regular PPM Center entity fields.

The data provided in log files depends on the log level. For details, see the *Installation and Administration Guide*.

FAQ

Question

Does PPM Center audit access to need-to-know information and key application events?

Answer

Yes, through the application log files.

Question

Does PPM Center display the user's time and date of the last change in data content?

Answer

Yes, for entity fields marked as history enabled.

Question

Does PPM Center support the creation of transaction logs for access and changes to the data?

Answer

The information can be found in the application logs based on the log level. For details, see the *Installation and Administration Guide*.

Chapter 11: General Questions

Question

How can I report security issues?

Answer

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

Question

Where can customers obtain the latest information regarding security vulnerabilities in PPM Center?

Answer

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

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 (Project and Portfolio Management Center 9.31)

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 HPSW-BTO-PPM-SHIE@hp.com.

We appreciate your feedback!