Project and Portfolio Management Center

Software version: All versions

Security Guide

Go to Help Center online

https://admhelp.microfocus.com/ppm/

Document release date: July 2024

Send Us Feedback

Let us know how we can improve your experience with the Security Guide.

Send your email to: admdocteam@opentext.com

Legal Notices

Disclaimer
Certain versions of software accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. This software was acquired on September 1, 2017 by Micro Focus and is now offered by OpenText, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Contents

Welcome to this guide

This guide provides security guidelines for use when working with OpenText ™ PPM.

Secure Implementation and Deployment

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

Technical System Landscape

PPM 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 Configuration

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

Security in Clustered PPM Configuration

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

Security in Configuration Files

It is recommended that you protect configuration files with proper permission configuration. By not implementing the proper permissions for configuration file you may expose the system to increased security risks. You understand and agree to assume all associated risks and hold OpenText harmless for the same. It remains at all times your sole responsibility to assess your own regulatory and business requirements. OpenText does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to customers in conducting customer's business.

It is recommended that you restrict the read and write permission to the configuration files only to the owner by running the command: `chmod 600` *<Configuration_File_Name>*.

External SSO Authentication

PPM 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 components (PPM servers, database servers, LDAP servers, and other integrating servers) to minimize the number of hops. In addition, it is recommended to use TLS to secure access to servers located across such boundaries.

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

Best Practice

It is recommended to use TLS to secure communications between applications.

Use the following parameters to configure the use of TLS:

- HTTPS_PROTOCOL
- HTTPS_ENABLED_PROTOCOLS
- SMTP_SSL_ENABLED_PROTOCOL

- SSL_CLIENT_SOCKET_ENABLED_PROTOCOL
- HTTPS_CIPHERS

For details, see the *Server parameters*.

> **Note:** Ensure to use the proper cipher suites for TLS.

Security Related PPM Server Configuration Parameters

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

Secure PPM Storage

PPM 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 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 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 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 user password constraints to secure the PPM users.

The following parameters control the user password constraints:

- `USER_PASSWORD_MAX_LENGTH`

  PPM recommends that admins set the value of this parameter to `16`.

- `USER_PASSWORD_MIN_DIGITS`

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

- `USER_PASSWORD_MIN_LENGTH`

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

- `USER_PASSWORD_MIN_SPECIAL`

  PPM recommends that admins set the value of this parameter to `0`.

- `PASSWORD_EXPIRATION_DAYS`

  PPM recommends that admins set the value of this parameter to `90`.

- `PASSWORD_REUSE_RESTRICTION_DAYS`

  PPM recommends that admins set the value of this parameter to `366`.

- `USER_PASSWORD_MIN_UPPERCASE_LETTERS`

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

- `USER_PASSWORD_MIN_LOWERCASE_LETTERS`

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

Restrict access to cookies

You can ensure that cookies are sent securely and are not accessed by unintended parties or scripts in one of the following ways: with the `HttpOnly` attribute or with the `Secure` attribute.

HttpOnly attribute

`HttpOnly` is an additional attribute included in a Set-Cookie HTTP response header. Using the `HttpOnly` attribute 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`

Secure attribute

A cookie with the `Secure` attribute is only sent to the server with an encrypted request over the HTTPS protocol. Using the `Secure` attribute prevents the transmission of the cookie in clear text, thus prevents cookies being observed by unauthorized parties.

To set the `Secure` attribute:

1. Open the **server.conf** file and set the **BASE_URL** parameter to start with **https**.
2. In the **server.conf** file, set the **SET_SESSION_COOKIE_SECURE_FLAG_IN_HTTPS** parameter to **true**.
3. Run the **kUpdateHtml.sh** script. For details, see the *System Administration Guide*.
4. Restart PPM.

DMS

The followings are the DMS configuration parameters:

- DMS_INSECURE_FILE_EXTENSION_CHECK
- DMS_XSS_CHECK

We recommend that admins set the values of the above parameters to `true`.

Installation Security

This chapter provides information on aspects of installation security.

Supported Operating Systems

For the list of supported system environments, see the System Requirements and Compatibility Matrix PDF.

Web Server Security Recommendations

IIS Web Server

See https://docs.microsoft.com/en-us/documentation/ 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 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.

Recommendations to protect against slow HTTP attacks

Slow HTTP attacks are denial-of-service (DoS) attacks in which the attacker sends HTTP requests in pieces slowly, one at a time to a web server. Here are the recommendations for the Apache web server to protect it against slow HTTP attacks.

- Use the <Limit> and <LimitExcept> directives to drop requests with methods not supported by the URL alone won't help, because Apache waits for the entire request to complete before applying these directives. Therefore, use these parameters in conjunction with the LimitRequestFields, LimitRequestFieldSize, LimitRequestBody, LimitRequestLine, LimitXMLRequestBody directives as appropriate. For example, it is unlikely that your web app requires an 8190 byte header, or an unlimited body size, or 100 headers per request, as most default configurations have.
- Set reasonable TimeOut and KeepAliveTimeOut directive values. The default value of 300 seconds for TimeOut is overkill for most situations.
- Increase the default value of ListenBackLog, which is helpful when the server can't accept connections fast enough.
- Increase the MaxRequestWorkers directive to allow the server to handle the maximum number of simultaneous connections.
- Adjust the AcceptFilter directive, which is supported on FreeBSD and Linux, and enables operating system specific optimizations for a listening socket by protocol type. For example, the httpready Accept Filter buffers entire HTTP requests at the kernel level.

NGINX web server

If your PPM sever is integrated with the NGINX web server, configure the following in NGINX to enable NGINX to accept headers with underscores:

1. In the server block of the NGINX configuration, add the following parameter:

   ```
   underscores_in_headers on
   ```

2. Validate and reload the configuration by running the following command:

   ```
   nginx -t

   service nginx reload
   ```

Enable CORS filter

Cross-Origin Resource Sharing (CROS) filter is an implementation of W3C's CORS specification, which is a mechanism that enables cross-origin requests.

The filter works by adding required Access-Control-* headers to HttpServletResponse object. The filter also protects against HTTP response splitting. If request is invalid, or is not permitted, then request is rejected with HTTP status code 403 (Forbidden). A flowchart that demonstrates request processing by this filter is available.

Use the following parameters to enable CORS filter:

- **ENABLE_CORS_FILTER**: enable CORS filter.
- **ACCESS_CONTROL_ALLOW_ORIGIN:** specify the permitted domains for making requests from the webpage. Separate multiple values with commas.Do not use * due to Tomcat's parameter restrictions.

Application Server Security Recommendations

When configuring SSL on the PPM 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. See "Configure secure PPM pages" in the *Installation and Administration Guide*.
- Since the default *admin* user password is documented in PPM, 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.

See the *Creating a System Account* for PPM 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 *Installation and Administration Guide* to learn the minimal permission requirement on Oracle database:

- *Default Permissions for PPM Center Schemas*

- *Other Permissions Needed or Not Needed for PPM Center*

PPM Purge Tool

The PPM Purge Tool is used to permanently delete (purge) stale database data by specifying purging criteria. Pay attention to the following for the use of this tool:

- To use this tool, you must have both the SYS DBA and PPM application administrator access grants.
- It is highly recommended that this tool should be installed on a dedicated server that only the tool users with both the SYS DBA and administrator access grants can have access to, rather than on an end-user's machine.
- When using this tool, the following database permissions are required:
  - create session
  - create database link
  - create procedure
  - create sequence
  - create synonym
  - create table
  - create view
  - create trigger
  - create job

    - select on v_$session
    - execute on dbms_session
    - execute on DBMS_MONITOR
    - select on v_$parameter
    - select on v_$mystat
    - select on v_$process
    - select on v_$session
    - execute on dbms_stats
- Remote access to this tool is allowed. We recommend that you do not enable it for security best practice. If you still require remote access to this tool, make sure the IP addresses are allowed.
- Follow the instructions in the *Installation and Administration Guide* about how to use this tool

PPM AntiSamy

AntiSamy is an HTML, CSS, and JavaScript filter that sanitizes use input based on a policy file. PPM AntiSamy gains wisdom from the OWASP AntiSamy project. For more information about OWASP AntiSamy project, see https://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project.

PPM AntiSamy makes sure user's HTML, CSS and JavaScript input strictly follows rules defined by the policy file `antisamy-ppm.xml`. For example, if you enable the AntiSamy feature, you cannot open hyperlinks on request details page or project details page. This is because the hyperlink-kind input by default does not meet the rules defined by `antisamy-ppm.xml`. To make hyperlinks accessible in PPM, you can configure the policy file as you demand.

For more information about using PPM AntiSamy, see the *Installation and Administration Guide*.

FAQ

Question

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

Answer

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

Question

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

Answer

Yes.

Network and Communication Security

This chapter provides information on network and communication security.

Secure Topology

The PPM 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 servers:

- Reverse proxy architecture

  One of the more secure recommended solutions is to deploy PPM 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.

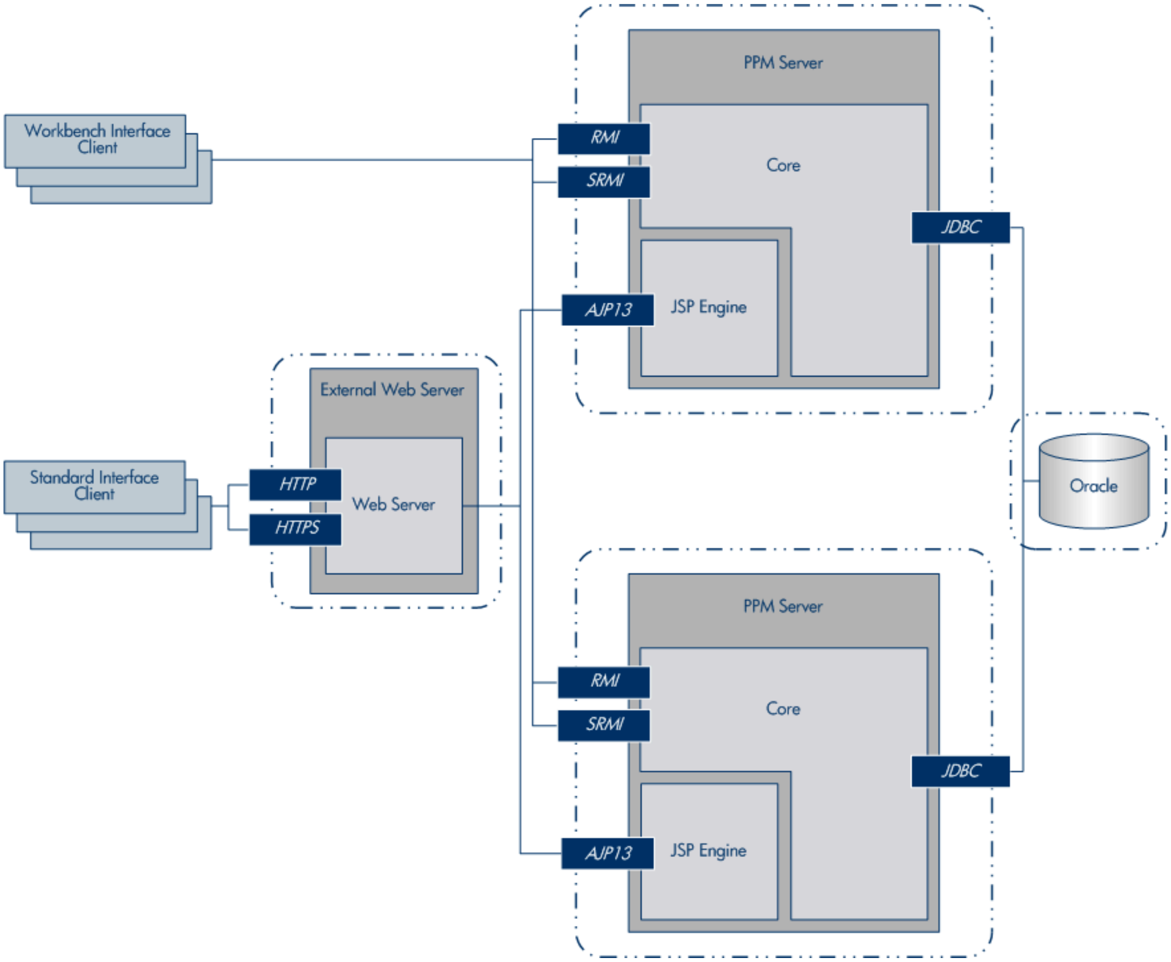
- SSL communication protocol

  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 clients and the PPM servers. This is especially important when opening access to PPM 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 Web client only in cases where your PPM Web client is exposed to the public Internet. In most production environments, deploying PPM 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 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
- 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

- Denial-of-service (DoS) attack protection

  Consider implementing DoS attack protection in on-premises deployments. You can use Apache Tomcat RateLimitFilter to mitigate DoS attack.

  > **Note:** In SaaS deployments, AWS WAF is a better choice.

  To mitigate DoS attack, set the following parameters in the Admin Console or the **server.conf** file to limit request to web server:

Parameter	Description
DOS_ENFORCE	Set true to enable rate limiter DoS filter
DOS_BUCKET_DURATION_IN_SECONDS	Duration in seconds
DOS_BUCKET_REQUESTS	Number of requests per duration
DOS_STATUS_CODE	Status code to return when the number of requests per duration exceeds the maximum number allowed
DOS_STATUS_MESSAGE	Status message to return when the number of requests per duration exceeds the maximum number allowed

- Host header positing attack protection

Set the **HOST_HEADER_PROTECTION_ENABLED** parameter to **true** to mitigate host header positing attack. When this parameter is set to **true**, only requests with host header in the trusted URLs (must be the same domain specified in either the TRUESTED_URL or BASE_URL parameter) are allowed.

Optionally, use the **HOST_HEADER_PROTECTION_MESSAGE** parameter to configure the message returned when the request is rejected due to host header protection.

- Enforce HTTPS

  When your base URL starts with HTTPS, you can set the **ENABLE_SECURITY_RESPONSE_HEADERS** parameter to **true** to apply HTTP Strict-Transport-Security (HSTS). The HSTS response header informs browsers to access the site only using HTTPS and convert any future HTTP attempts to HTTPS.

  This approach is more secure than configuring a simple HTTP-to-HTTPS (301) redirect on your server, as the initial HTTP connection in a redirect can be vulnerable to man-in-the-middle attacks.

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

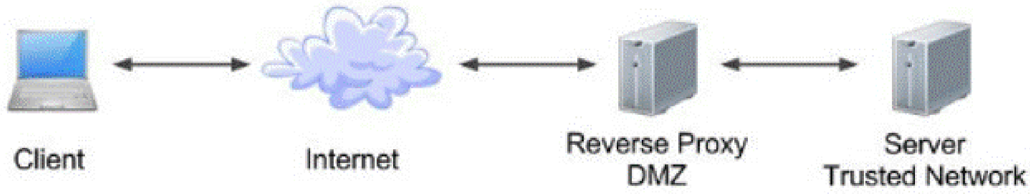
A reverse proxy functions as a bastion host. It is configured as the only machine to be addressed directly by external clients, and thus obscures the rest of the internal network. Use of a reverse proxy enables the application server to be placed on a separate machine in the internal network, which is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

Secure Channel	How to Configure
Between browser and PPM 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 server.
Between PPM and LDAP server	PPM connects to a LDAP server either in clear text or over SSL. For details, see the *Installation and Administration Guide*.
Between PPM and mail server	PPM supports SMTP Authentication. PPM connects to SMTP Server either in clear text or over SSL. For details, see the *Installation and Administration Guide*.
Between RP/LB and PPM 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*.

CSRF Mitigation Recommendations

Cross-Site Request Forgery (CSRF) attacks are attacks that force a user's web browser to perform unwanted actions on a trusted web application where the user is authenticated.

PPM implements CSRF mitigation by using a new CSRF token for every new session. To enable the mitigation, set the **FORCE_NEW_CSRF_TOKEN_ON_NEW_SESSION** parameter to `true`. When this parameter is set to `true`, each time when a user successfully logs in to PPM, a new CSRF token is generated. When a user closes the web browser, the CSRF token changes.

SSRF Mitigation Recommendations

Server-Side Request Forgery (SSRF) attacks allow an attacker to manipulate the server-side application to make requests to an unintended location.

PPM implements the SSRF mitigation by validating the host header of each request to which PPM is redirected. To enable the mitigation, set the following parameters to **true**:

- **CHECK_HOST_HEADER_WHEN_REDIRECT**. When this parameter is set to **true**, when a request needs to be redirected, PPM checks the host header's domain of the request. If the host header is not the same as the base URL, the request is rejected.
- **dashboard.CHECK_HOST_HEADER_WHEN_REDIRECT**. When this parameter is set to **true**, when a request received by PPM dashboard pages needs to be redirected, PPM checks the host header's domain of the request. If the host header is not the same as the base URL, the request is rejected.

  > **Note:** You can enable this parameter only in the **server.conf** file.

  For details on how to modify the server parameters, see the *System 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*.

Web application security with OWASP Stinger

This chapter provides information on implementing web application security with OWASP Stinger.

Overview of OWASP Stinger

Developers consistently implement sporadic, ad-hoc input validation mechanisms for web applications. However, lack of a centralized and well-defined input validation mechanism exposes the application to a variety of attacks, including SQL Injection, Cross Site Scripting (XSS), and Command Injection. To improve security and protect the information assets, many organizations implement OWASP Stinger into their software development life cycle.

OWASP Stinger aims to develop a centralized input validation component which can be easily applied to existing or developmental applications. Using a declarative security model, OWASP Stinger has the ability to validate all HTTP requests coming into an application.

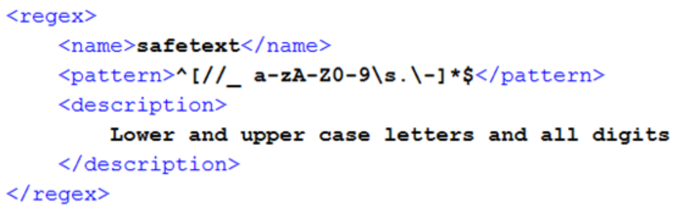
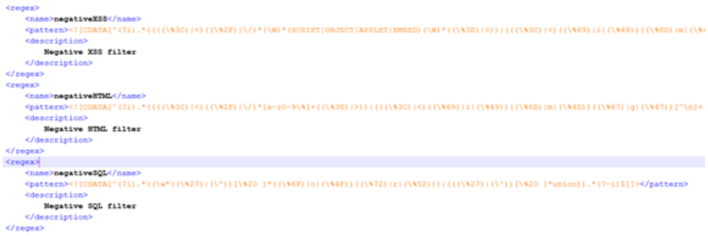
The basic idea of OWASP Stinger is to define validation rules for the cookies and parameters of an HTTP request. These rules are specified in simple XML files using the Security Validation Definition Language. Furthermore, Stinger 2 is implemented as a J2EE filter so that all HTTP traffic is validated before it is ever processed by the web application.

OWASP Stinger is integrated with PPM as a filter (ValidationFilter). It is highly configurable and easy to plug and unplug.

Define validation rules

OWASP Stinger uses regular expressions for parameter validations.

It uses an allow list and a deny list to define validation rules.

<table>
<tr>
<td><b>Allow list</b></td>
<td>Identifies the cookies and parameters that can be passed to the web application.
Usually, the allow list defines the predefined parameters. For example:

<pre>
<regex>
    <name>safetext</name>
    <pattern>^[//_ a-zA-Z0-9\s.\-]*$</pattern>
    <description>
        Lower and upper case letters and all digits
    </description>
</regex>
</pre></td>
</tr>
<tr>
<td><b>Deny list</b></td>
<td>Blocks general JS/HTML/SQL injection. It is used for custom fields, especially in multibyte language.
For example:

<pre>
<regex>
    <name>negativeXSS</name>
    <pattern><![CDATA[^(?i).*((((\%3C)|<)((\%2F)|\/)*(\W)*(SCRIPT|OBJECT|APPLET|EMBED)(\W)*((\%3E)|>))|(((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%
    <description>
        Negative XSS filter
    </description>
</regex>
<regex>
    <name>negativeHTML</name>
    <pattern><![CDATA[^(?i).*((((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>))|(((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+
    <description>
        Negative HTML filter
    </description>
</regex>
<regex>
    <name>negativeSQL</name>
    <pattern><![CDATA[^(?i).*((\w*((\%27)|(\'))[\%20]*((\%6F)|o|(\%4F))((\%72)|r|(\%52)))|(((\%27)|(\'))[\%20]*union)).*(?-i)$]]></pattern>
    <description>
        Negative SQL filter
    </description>
</regex>
</pre></td>
</tr>
</table>

To define the validations rules, open the **Stinger.xml** file in the **<PPM HOME>/conf/** directory to edit the allow and deny lists.

Reconfigure validation rules

Ideally, all true positive Cross Site Scripting (XSS) can be captured and blocked by this means, because every payload should have either `<script` … (or its alternative, such as `%3cSCRIPT`…) or some inbuilt function such as “alert” in it, which can be identified by the Stinger deny list.

Sometimes, however, false positive XSS may also be captured and blocked. To bypass false positive XSS, check the rule for a specific URL or parameter and reconfigure the validation rules. Moreover, you should continuously update the deny list as the XSS attacking technology evolves.

Troubleshooting

Problem: When updating a request page, the page gets blocked and the following error message is displayed on the page and recorded in the server log:

```
parameter P_43HV with value 116.116.<div id="igriddiv" width="298"
height="38"><iframe src="/demo/demo.html"
height="38"></iframe></div>.<div id="i griddiv" width="298"
height="38"><iframe src="/demo/demo.html" height="38"></iframe></div>
from 10.123.211.74 has been encoded
```

```
The P_43HV parameter is malformed
```

Resolution:

1. Check the **Stinger.xml** file to find the rule for the request URL. The rule is as follows:

   ```
   <name>RequestUpdate.jsp</name>
   <path>/.*/web/knta/crt/RequestUpdate.jsp.*</path>
   ```

2. Check if the predefined regex pattern accepts the input:

   ```
   <regex><![CDATA[(?s)(?i)((?!<script)(?![^a-z]+alert[ ]*\()
   (?!onerror).)*]]></regex>
   ```

   In this case, the regex pattern accepts the input.

3. Check the general rule that applies to all URLs. The rule is as follows:

   ```
   <name>general rule for anti-XSS</name>
   ```

   ```
   <path>/.*</path>
   ```

4. You find that `iframe` is blocked by the following rule:

   ```
   regex><![CDATA[(?s)(?i)((?!%3Cscript)(?!<script)(?!
   (alert|prompt|confirm)[\s]*\()(?!onerror)(?!onchange[^a-z]{1})(?!on
   (db|aux){0,1}click)(?!onload)(?!onmouse)(?!javascript[\s]*:)
   (?!<iframe)(?!cmd\|).)*]]></regex>
   ```

5. To allow `iframe`, remove `iframe` from the rule:

```
regex><![CDATA[(?s)(?i)((?!%3Cscript)(?!<script)(?!
(alert|prompt|confirm)[\s]*\()(?!onerror)(?!onchange[^a-z]{1})(?!on
(db|aux){0,1}click)(?!onload)(?!onmouse)(?!javascript[\s]*:)
(?!cmd\|).)*]]></regex>
```

Content Security Policy

PPM uses the Content-Security-Policy HTTP response header to restrict the resources, such as images and JavaScript that are allowed to load.

The default Content-Security-Policy header value is:

```
'default-src blob: 'self' 'unsafe-inline' 'unsafe-eval' %TRUSTED_
EXTERNAL_URLS%;img-src 'self' data: %TRUSTED_EXTERNAL_URLS%;font-src
'self' data:
```

Where `%TRUSTED_EXTERNAL_URLS%` is a placeholder that is replaced by the value of the **TRUSTED_EXTERNAL_URLS** server parameter.

You can modify the content security policy by editing either of the following parameters:

Parameter	Description
TRUSTED_EXTERNAL_URLS (Recommended)	Use this parameter to add the URLs of the sites from which you want to embed content, either using iframes or reading scripts, images, or other resources from the sites. The default value of this parameter is: `https://app.powerbi.com admhelp.microfocus.com`, enabling the embedding of the PPM online help and PowerBI on dashboards. If you want to embed other web sites as iframes on PPM with a URL portlet, Web Frame portlet, or HTML+ portlet, add the external web site domains to the **TRUSTED_EXTERNAL_URLS** parameter.
CONTENT_SECURITY_POLICY	Use this parameter to edit the value of the Content-Security-Policy HTTP response header. See content-security-policy.com for a reference on this header and its possible values.

> **Note:** It is strongly recommended to modify the **TRUSTED_EXTERNAL_URLS** parameter instead of the **CONTENT_SECURITY_POLICY** parameter.

For details on how to modify the server parameters, see the *System Administration Guide*.

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.

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 Server files in the Administration Console and lets the user browse and download PPM Server files. Without this access grant, the File Browser is invisible.

Administration Console Actions

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

- Viewing PPM 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 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 Software Support from the Administration Console
- Changing Data Display in Administration Console Tables

User Management and Authentication

This chapter provides information related to user authentication.

Authentication Model

PPM 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 require account passwords that conform to corporate policy?

Answer

PPM 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 user session management.

Answer

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

Answer

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

Authorization

This chapter provides information related to user authorization in PPM.

Authorization Administration

User access to PPM 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 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 inherit users’ information and authorization profiles from an external repository, such as LDAP?

Answer

No.

Question

Does PPM supports “role based access control”?

Answer

Yes.

Question

Does PPM support entity level access restriction?

Answer

Yes.

Question

Does PPM support Field Level access restriction?

Answer

Yes.

Data Integrity

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

PPM 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.

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 Encryption

PPM 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 uses, credentials to the LDAP with which PPM integrates, and credentials for machines that contain user data.

PPM 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
```

It is recommended that you use strong encryption to encrypt sensitive credentials. Check the `kEncrypt.sh` command in the *Installation and Administration Guide*.

Password Encryption

User passwords are stored either in its encrypted format or hashed versions by SHA256.

By default, user passwords are encrypted. To hash user passwords, do the following:

1. Run the **kConvertUserPasswords.sh** script to convert existing user passwords to the hashing algorithm.

For details, check the **kConvertUserPasswords.sh** script in the *Installation and Administration Guide*.

2. Set the **USER_PASSWORD_ENCRYPTION** parameter to **SHA256**

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

FIPS Option	Standard (Encrypted)	Hash
FIPS Enable	AES	SHA256
FIPS Disable	ElGamal	SHA256

FAQ

Question

Does PPM transmit account passwords in an approved encrypted format?

Answer

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

Question

Does PPM store account passwords in approved encrypted format?

Answer

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

Question

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

Answer

PPM 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*.

Logs

This chapter provides information related to logs.

Log and Trace Model

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

Answer

Yes, through the application log files.

Question

Does PPM 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 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*.

Cookies

PPM uses the following cookies:

Cookie	Description	Retention duration
JSESSIONID	Mandatory cookie. This is the session cookie. Keeps a session active.	Session lifecycle
CSRF_X_ TOKEN	Mandatory cookie. Protects against CSRF.	Session lifecycle
Logon cookie	Optional cookie. Disabled by default. Enables the server to retain a password when a user logs in to PPM.	Persistent cookie