



# Security Tools in Payara® Platform

The Payara® Platform - Production-Ready,  
Cloud Native and Aggressively Compatible.

Payara Platform is a supported open source software for enterprises that enables reliable and secure deployments of Jakarta EE and MicroProfile applications on premises, in the cloud, or hybrid environments. Payara Platform is built and supported by a team of DevOps engineers committed to ensuring it's the best option for Java EE and Jakarta EE applications in production. Making the platform secure and providing useful built-in security tools for application developers and production administrators is an essential part of the platform in order to make the production systems secure and reliable.

Payara Platform engineers follow vulnerability registries and pre-emptively analyse if they affect Payara Server, Payara Micro or other products in the platform. Then they make sure that all the vulnerabilities that may impact Payara Platform are fixed as soon as possible.

Using Payara Platform Enterprise gives you additional reassurance that your production systems are secured and safe, with:

- Monthly releases including security fixes
- Critical security patches and alerts to their availability
- Support portal and customer knowledgebase to contact Payara engineers and access information about vulnerabilities and security fixes
- 10-year software life cycle to maintain the security and stability of your applications
- Exclusive access to extensively tested, fully supported binary builds of Payara Platform
- Access to fully supported builds of OpenJDK with recent security fixes

Payara Platform also provides tools to secure and restrict access to a production system, encrypt communication, and audit security events and configuration changes.



### Server Requirements

Derived from GlassFish Server Open Source Edition, Payara Server uses the same basic system requirements:

- JDK8u163 or above
- 512MB RAM

### Support for Any Operating System Running One of the Following Java Virtual Machines

- Oracle JDK8 (u162+)
- Azul Zulu JDK8 (u162+)
- OpenJDK JDK8 (u162+)
- Oracle JDK 11 (11.0.4+)
- Azul Zulu JDK11 (11.0.4+)
- OpenJDK JDK11 (11.0.4+)

## Secure Production Installation

Most important in a production environment is to properly secure all services exposed by the application and the administration interface, and to make sure that all sensitive data is encrypted and protected. Payara Platform is designed to encrypt sensitive information and secure access to it. So, in most cases, you don't need to think about it. In other cases, it's simple to enable additional security measures even for less sensitive features and data, such as metrics and health status.

Payara Platform provides a self-signed certificate that can be directly used to secure the communication with SSL/TLS encryption. It's also easy to install and use custom certificates. Payara Server supports SSL/TLS encryption for HTTP listeners, including the admin interface, as well as for remote method invocation (IIOP) calls. It provides a preconfigured HTTP listener and Admin interface with HTTPS enabled using the self-signed certificate by default. Payara Micro also provides a preconfigured HTTPS listener with a self-signed certificate which can be replaced by a custom certificate.

The administration and JMX monitoring interfaces of Payara Server require encrypted and password protected access when accessed remotely. This is to lead to the best practices in production systems to ensure that no unauthorized access to administration and sensitive information is allowed. Other interfaces that provide sensitive data like metrics and health status offer an option to force encrypted and restricted access.

All of the certificates and passwords stored in Payara Server configuration are encrypted using a master password. This password is not stored in the configuration and needs to be supplied when the server is started. (This is true unless you are using the default master password, which isn't recommended for production.)

### Related Products & Services

- [Payara Enterprise](#)
- [Migration & Project Support](#)
- [Payara Accelerator Consultancy](#)
- [Payara Micro](#) - microservices and cloud environments
- [Payara Scales](#) - high-density memory store and WAN replication

### Payara Enterprise Production Support

Options include:

- 24x7 – for mission critical environments
- 10x5 – business hours support

Ensures service level agreement (SLA) operation of your application server with:

- Unlimited tickets
- Customer Knowledge Base
- On-boarding support
- 10-year software lifecycle
- Fully supported production binaries
- Fully supported ecosystem components
- Access to Zulu Enterprise-fully-supported builds of OpenJDK



The bundled domain (a configuration template) called **production** provides sensible defaults for setting up a new, secure and production ready Payara Server installation. Among other configuration settings, it disables all development features, which could pose a security risk in production.

## Restricting Access to Privileged Users

Besides securing the communication links, it's also very important to define which users are permitted to access applications, and administration and monitoring interfaces, and which permissions are granted to them. Payara Platform has a solid foundation around providing security tools and several authentication and authorisation mechanisms to set permission levels.

Administration access can be restricted to admin users authenticated with a file-based realm stored and encrypted in Payara Server configuration.

For restricting access to applications and their features, multiple types of security modules are provided out of the box:

- LDAP
- Database
- Client Certificates
- Encrypted file-based database

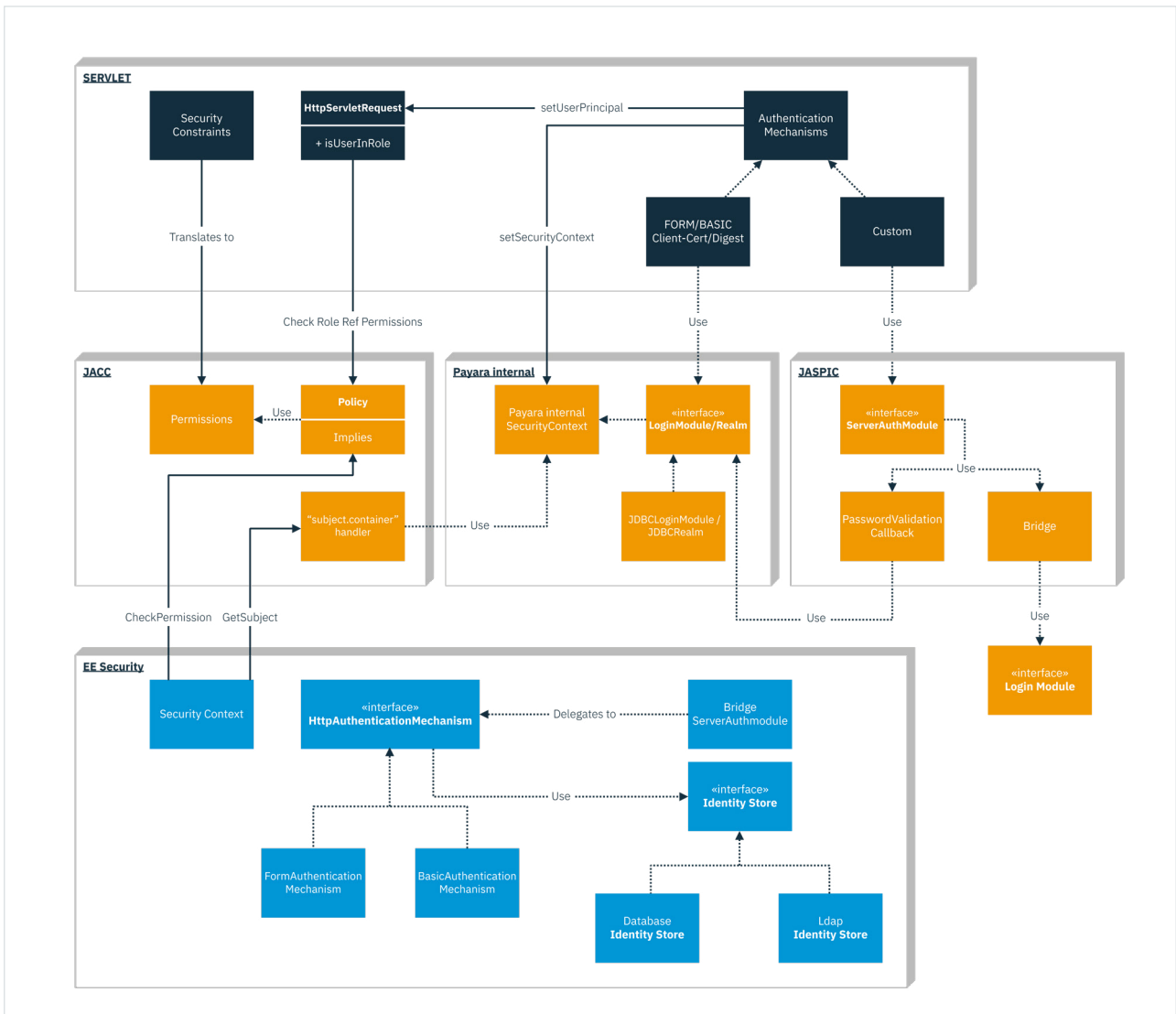
More security modules can be plugged into Payara Server or Payara Micro using the standard JACC interface to enable a custom authentication and authorisation mechanism.

Further, applications using Payara Platform can rely on more authentication mechanisms supported by the Security API and Payara API:

- OpenID
- OAuth2
- Yubikey
- JSON Web Token

Additional custom mechanisms can be provided by the application. Payara Platform even allows mixing multiple built-in or custom authentication mechanisms in the applications to allow for greater flexibility.

The following picture shows individual security components in Payara Platform:



## Single Sign-on

When Single Sign On is enabled in Payara Server, all web applications in the same SSO group will share authentication state. So, if a user logs in to a web application he will be implicitly logged in into all other applications in the same SSO group. Web applications form the same SSO group if:

- Applications use the same security realm
- Applications deploy on the same virtual server in a single-instance deployment
- Single Sign-on failover is enabled in a high-availability deployment

## Integrations with Third-Party Security Tools

Payara Platform integrates with several widely used security tools. These integrations are very well documented and Payara Enterprise customers can get additional guidance if they encounter any problems.

Identity and Access Management tools:

- ForgeRock Open AM (recommended)
- Keycloak

Standard security integrations supported:

- Authentication and authorisation using any LDAP server (e.g. OpenDJ)
- Authentication using pluggable JCE security providers (e.g. BouncyCastle, IAIK-JCE)

## Auditing and Monitoring

Identifying who can access sensitive data in your application at specific times, and how, is a crucial task that can be eased with the audit capabilities that are included in Payara Platform.

**Security Audit Modules** allow creating audit trails of all authentication and authorization decisions. Audit modules are simple Java classes that can be plugged into Payara Platform. They can be used to programmatically take special actions when authentication or authorization events are triggered by the JACC container.

**Admin Console Auditing Service** allows ability to log all actions and operations executed via the administration console for auditing purposes. The service can alert administrators of suspicious activity as soon as possible or archive the events for future analysis.

## Java Support with Security Fixes

Payara Platform is supported and tested on a variety of operating systems and Java virtual machines.

On top of that, Payara Enterprise Support customers have access to fully supported builds of Zulu Enterprise OpenJDK with security fixes to run Payara Platform. This allows customers to receive security fixes for both Payara Platform and the underlying Java runtime.

## Payara Platform is Ideal for Reliable and Secure Deployments

Whether you plan to develop and deploy applications on premises, in the cloud, or hybrid environments, Payara Platform is the perfect platform to make your deployments reliable and secure. Both Payara Server and Payara Micro have a strong toolset of security components for most use cases in the industry, so you won't have to worry about implementing your own security measures from scratch. Payara Platform also provides powerful auditing, alerting and monitoring to give you enough information about any suspicious activity.

If you're a Payara Enterprise customer in need of further assistance, the Payara Accelerator team can provide customized consultancy services to advise on applying strict security measures or apply them for you. Your Payara Enterprise subscription provides support for issues with securing Payara Platform or integrating it with third-party services, allows you to raise questions and request enhancements, and gives you access to private builds of Payara Server, Payara Micro and Zulu Enterprise OpenJDK with security fixes.

## Payara Server Resources

**Try Payara Server.** Experience the benefits of developing Java EE applications in our Java application server.

Download: <https://www.payara.fish/downloads>

Security Fixes Summary: <https://docs.payara.fish/security/security-fix-list.html>

**Just getting started with Payara?** Watch a video tutorial, read technical overviews and resources to get the most out of Payara Server.

Learn more: <http://info.payara.fish/getting-started-with-payara-server-useful-resources>

**Secure Payara Server.** Learn more and try the security features of Payara Server:

- [Configuring Security in Payara Server with LDAP](#) (User Guide)
- [ForgeRock Integration with Payara Server](#) (Blog)
- [Security Auditing in Payara Server](#) (Blog)
- [Admin Console Auditing Service](#) (Payara Server Documentation)

**Get Involved.** Join the Payara Community and help feed the fish! Payara Server is, and always will be, open source and we want your ideas, feedback and collaboration for ensuring Payara Server is the best option for production Java EE applications.

Learn more: <https://www.payara.fish/community>

## About Payara Services, Ltd

Payara Services is a global open source company and a recognized leader in the creation of innovative infrastructure software for today and tomorrow. We are proud to nurture and grow an open and collaborative community that builds on the needs of all to advance our software and services while providing support, stability, and security.

Our engaged team operates with the freedom and support to develop industry-leading products and services that enable our users to create world-class solutions across a diverse range of industries.

We help shape the future of the industry through our direct contributions to Jakarta EE and Eclipse MicroProfile® as Eclipse Foundation Solutions Members and members of the Project Management Committee.



*Jakarta EE® and MicroProfile® are registered trademarks of the Eclipse Foundation.*



**sales@payara.fish**



**+44 207 754 0481**



**www.payara.fish**

Payara Services Ltd 2016 All Rights Reserved. Registered in England and Wales; Registration Number 09998946  
Registered Office: Malvern Hills Science Park, Geraldine Road, Malvern, United Kingdom, WR14 3SZ