Oracle® Hospitality Self-Hosted Token Proxy Service

Security Guide

Release 19.2
F20918-01
July 2020

ORACLE

Oracle Hospitality Self-Hosted Token Proxy Service Security Guide, Release 19.2

F20918-01

Contents

Preface

The Token Proxy Service (TPS) is a proxy interface for the hosted OPERA application. This proxy service only processes the token or PAN exchange.

This document provides security reference and guidance for the Oracle Hospitality Self-Hosted Token Proxy Service.

Audience

This document is intended for end users and for system administrators installing the Token Proxy Service.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/.

Revision History

Table 1 Revision History

Date	Description of Change
July 2019	Initial Publication
July 2020	Revised content across the entire document

1

Token Proxy Service Security Overview

This chapter provides an overview of the Oracle Hospitality Token Proxy Service security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date**. This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible**. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity**. Establish who should access which system components, and how often, and monitor those components.
- **Install software securely**. For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. Performing a Secure Token Proxy Service Installation has more information on installing the software securely.
- **Learn about and use the Token Proxy Service security features**. Implementing Token Proxy Service SecurityImplementing Token Proxy Service Security has more information on the Token Proxy Service security features.
- **Use secure development practices**. For example, take advantage of existing database security functionality instead of creating your own application security.
- **Keep up to date on security information**. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. Oracle's Critical Patch Updates and Security Alerts website has more information on security-related patch updates and security alerts: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

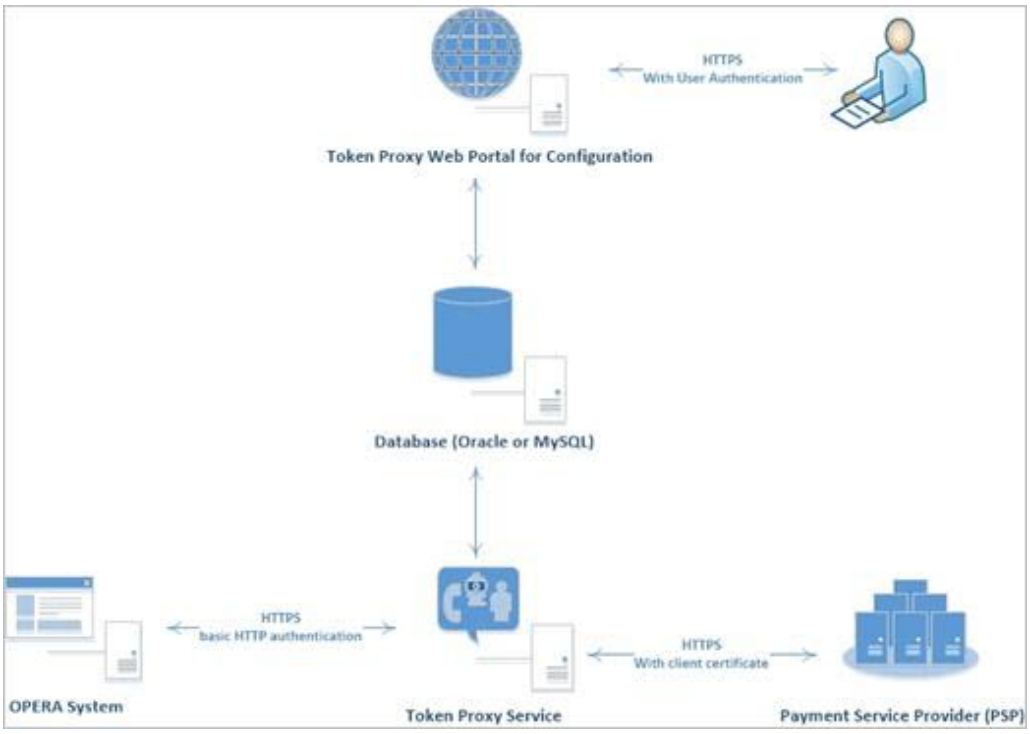
Token Proxy Exchange Service

The Token Proxy Exchange Service is a proxy interface for the hosted OPERA application. This proxy service only processes the token or PAN exchange. The partner payment service providers contain the actual token functionality. As a result,

no financial transactions are exchanged and no PCI data saves in the Token Proxy Exchange Service system.

The Token Proxy Exchange system has three main components:

- The Database is used to store the configuration from the web portal, and the service will read from it.
- The Token Proxy Exchange Web Portal is used to configure the settings used by the service. It is a web application suitable for hosting in WebLogic or Tomcat.
- The Token Proxy Exchange Service is a standalone application that can be run as a Windows service. This application creates a listener to listen on a TCP port (configured in the database but default to 443) to listen for XML messages posted over HTTPS. This listener must be exposed to the client (for example, OPERA systems).



OPERA system communicates with Token Proxy Service using a HTTPS TLS 1.2 connection. TPS uses basic HTTP authentication to validate the request that comes from a trusted client.

The Token Proxy Service communicates securely with third-party payment service providers by using HTTPS TLS 1.2 with client certificates.

Authorized datacenter administrators can use the Token Proxy Exchange Service web portal to configure the service, such as the merchant account and payment provider information.

Recommended Deployment Configurations

The Token Proxy Exchange Service web portal deploys either on Oracle WebLogic server or Tomcat. The Token Proxy Exchange Service is a standalone application that can be run as a Windows service. The database server runs on Oracle 12c database or My SQL 8.0 or above.

The Token Proxy Exchange Service listener manages its own use of the certificates provided by the datacenter using TLS1.2, so a firewall or load balancer (if present) must not offer any form of HTTPS to HTTP bridging functionality, and instead the connection must be passed directly to the Token Proxy Exchange Service.

The certificates provided must be installed on all servers running the Token Proxy Exchange Service in the event the service is installed on multiple machines for load balance or fail over. In case if the certificate has to be deployed at load balancer, then a certificate should also be deployed at TPS app server to establish HTTPS connection from load balancer to TPS server. It is highly recommended to use CA signed certificates.

The service will also make outgoing connections to the Payment Service Provider. This outgoing connection will be to a URL specified by the payment service provider and the host or port will be specified by the PSP. Port 443 is the requested and recommended standard.

This outgoing connection can be over the internet or over VPN, but must be using HTTPS with TLS1.2 or greater. HTTPS over a VPN connection is recommended for security reason.

Component Security

Oracle Database Security

The Oracle Database Security Guide contains more information about the security best practices.

MySQL Database Security

https://dev.mysql.com/doc/refman/8.0/en/security.html contains more information about the security best practices for MySQL database.

Oracle WebLogic Server Security

The Securing a Production Environment for Oracle WebLogic Server Guide from Oracle Fusion Middleware contains more information.

By default, WebLogic Server is configured with two keystores, which are located in the DOMAIN_HOME\security and WL_HOME\server\lib directories, respectively:

- DemoIdentity.jks - Contains a demonstration private key for WebLogic Server. This keystore contains the identity for WebLogic Server.
- DemoTrust.jks - Contains the trusted certificate authorities from the WL_HOME \server\lib\DemoTrust.jks and the JDK cacerts keystores. This keystore establishes trust for WebLogic Server.

> **Note:**
>
> You should never use these demonstration keystores in a production environment. In production, we recommend to use CA signed certificate.

For information about how to configure keystores for use in a production environment, see Obtaining and Storing Certificates for Production Environments; Steps to create a self-signed certificate and configure Custom Identity and Custom Trust with Weblogic Server using Keytool.

Personal Data Security

Personally identifiable information identifies or can be used to identify, contact, or locate the person to whom the information pertains.

Token Proxy Service collects only minimal data (first name, last name and email) and is limited to the users who are assigned to manage the configuration. Token Proxy Service Configuration Web Portal provides a user profile page which shows the user's information in the system and allow the user to update or delete them.

The user account profile data can be deactivated but cannot be immediately deleted to maintain the integrity of the audit trail. The deactivated user can be permanently removed from the database after a configurable retention period. The data once purged, cannot be re-created, accessed or read.

Based on the secure connection from TPS to PSP, Personal data is encrypted during the process of communication. The Personal data is encrypted and saved in database.

2

Performing a Secure Token Proxy Service Installation

This chapter describes how to plan for installing the Token Proxy Service. Refer to the **Oracle® Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide** on the Oracle Help Center for information.

Configuring the Installation

Before you install the Token Proxy Exchange Service, you must complete the following tasks:

- Have Java JDK 1.8 installed and apply latest Java update.
- Have Oracle Database or MySQL 8.0 or above installed.
- Have WebLogic 12c installed if you have decided to use WebLogic as the web server.
- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.

For details, please refer to the **Oracle® Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide**.

Installing the Token Proxy Service

You can perform a custom installation or a complete installation. You can use the custom installation option to avoid installing options and products not required for your environment. The Oracle Hospitality Token Proxy Service Installation Guide contains more information.

Installing the Token Proxy Service consists of three parts:

- Database
- Token Proxy Web Portal
- Token Proxy Service

During the database install, a database user will be created for Token Proxy Service. The password must follow the below guidelines and contain:

- At least 8 characters
- At least one upper case letter and one lower case letter
- At least one number
- At least one special character !@#$%^&*

If Tomcat is selected as web server to host TPS web portal, the installer will create a Tomcat user account. The password must follow the below guidelines and contain:

- At least 8 characters
- At least one upper case letter and one lower case letter
- At least one number
- At least one special character !@#$%^&*

Granting permissions on WebLogic user account

When Weblogic is used and the WebLogic OS user is not an administrator then write permission needs to be granted in **\ProgramData\TokenProxy**directory.

Tomcat User Account Password Expiration Policy

The Tomcat User Account Password by default is set to expire after 42 days. Please update password/default expiration date range as required. Please refer to **Oracle® Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide - Auto Deployment on Tomcat - Change the Password Expiration Policy for Windows User Account**.

Post-Installation Configuration

This section describes additional security configuration steps to complete post installation of Token Proxy Service.

Applying Software Patches

Apply the below software patches:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Apply the latest Token Proxy Service patches available on My Oracle Support.

Follow the installation instructions included with the patch.

Configuring the Token Proxy Exchange Service

To configure the Token Proxy Exchange Service follow these guidelines:

- To manage the Token Proxy Exchange Service use the web portal and create a system administrator account. Enter the user name as the employee's email, then an email is sent to the system administrator account that contains a link with a

unique password reset token. Choose a new password by meeting the password requirements.

- After you create the system administrator account, you can create the other users and clients. Use the client user accounts to configure the third-party payment service provider connections. Define the user name and password for basic HTTP authentication in OPERA.
- You must change the password frequently following the guidelines for:
  - database user
  - web portal user
  - HTTP authentication
- The PSP Client Side Certificates expiration date depends on what the PSP is set during creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated prior to the expiration date to avoid downtime to the interface.

Replace the default self-signed certificates with CA signed

When Tomcat is selected as web server to host TPS web portal, the installer will create a self-signed certificate for Tomcat as server's certificate. In production, CA signed certificate is highly recommended. Please refer to the **Oracle® Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide about "Tomcat – Certificate Configuration Wizard" and "Tomcat HTTPS Listener"** for steps to replace self-signed certificate with the CA signed certificate.

Data Purging

Audit data save to database. Purge data according to the merchant's contract policy.

3

Implementing Token Proxy Service Security

Token Proxy Service Exchange Security

Managing Users

Access to Token Proxy Configuration Web Portal is secured through Form-Based Authentication. The user is required to have a valid username and password in order to have access to the Portal.

Users are not allowed to create accounts by themselves; instead, the Web Portal administrator is responsible for creating the accounts and assigning the appropriate permissions to the accounts. By default, user accounts get created without a predefined password, instead, users are asked to create a password when logging in for the first time.

Token Proxy Configuration Portal uses Role-based Authorization in order to control the access to the different areas in the web portal, a Role is basically a named collection of privileges which can be assigned to users.

The system administrator role has the below privileges:

- Create or maintain users
- Create or modify any client
- Maintain the card type translation
- View or maintain the audit logs

A client user can only log in and manage existing clients that they are specifically assigned to by a system administrator user. The client user role cannot create or view the details of other clients.

The Security mechanism in Token Proxy Configuration portal implements the following features:

- You must use an email as the user ID for the Token Proxy Exchange Service web portal.
- Create passwords using a reset password link containing a unique random token sent by email.

- The database stores passwords using a salt hash format. The hash algorithm is SHA256.
- All password values are validated to ensure they meet the required minimum complexity.
- The system administrator and the client user roles are created during the installation.
- Configurable password expiration (default value: 90 days).
- Configurable account locking mechanism based on failed logging attempts (default: 3 failed attempts, default lock time: 240 minutes).
- Configurable Password History validation (users will not be able to repeat passwords used in the past, default: last 4 passwords).
- One-time-token-based reset password mechanism with configurable token expiration time.

Authenticating the Service

For details about the certificate requirements for OPI Communication to PSP, please refer to the **Oracle® Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide**.

> **Note:**
>
> The PSP Client Side Certificates expiration date depends on what the PSP is set during creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated prior to the expiration date to avoid downtime to the interface.

Using the Audit Trail

Token Proxy Configuration Portal also features an Auditing mechanism that allows to keep record of actions performed by users, actions such as:

- Successful user login
- Failed user login attempts
- Configuration updates
- Authorization or Authentication updates

Using the Token Proxy Exchange Service web portal, you can view the audit records and export the audit records to a spreadsheet.

The audit records are saved in the database for a minimum of 90 days. The Auditing mechanism allows exporting the data from Database into .xls files for long term storage. You can manually purge the audit records from the application. Purge data according to the merchant’s contract policy.

4

Appendix Secure Deployment Checklist

This appendix lists actions that need to be performed to create a secure system. The following is an example:

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Practice the principle of least privilege.
  - Grant necessary privileges only.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Restrict network access.
- Apply all security patches and workarounds.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Protect the Oracle listener.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Check network IP addresses.