

Oracle® Payment Interface

Oracle Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide



Release 6.1
E91140-05
September 2019



Oracle Payment Interface Oracle Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide, Release 6.1

E91140-05

Copyright © 2017, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	5
<hr/>	
1 Overview of Token Proxy Service	1-1
Components Parts	1-1
Installation Prerequisites	1-1
The Database	1-1
The Web Portal	1-2
Token Proxy Service	1-2
Recommended System Requirements	1-3
<hr/>	
2 Installing Token Proxy Service	2-1
Pre-Installation Checklist	2-1
Installing Token Proxy Service	2-1
Manually Deploying the .WAR file in WebLogic	2-5
Token Proxy Configuration Web Portal	2-6
Token Proxy Exchange Setup	2-7
<hr/>	
3 Configuration Web Portal	3-1
Signing In	3-1
Listeners	3-1
Creating and configuring PSPs	3-1
Deleting PSPs	3-2
Configuring Clients	3-2
Card Type	3-4
Creating Additional Users	3-6
Roles	3-7
Audit	3-8
<hr/>	
4 Certificates	4-1
Certificates for Communication between TPS and PSP	4-1
Certificates for Communication between Opera and TPS	4-2
Creating CSR Using Java Keytool Utility	4-3
<hr/>	
5 OPIConfigX.exe	5-1
<hr/>	
6 Opera Configuration	6-1
Configuring the CC Vault	6-1
<hr/>	
7 Token Proxy Service Maintenance & FAQ	7-1

Services	7-1
Modify, Repair, or Remove Token Proxy Service	7-1
Token Proxy Service Log Files	7-2
Token Proxy Service Password Maintenance	7-3
OPI Client Certificate Creator	7-4
TPS Configuration Backup	7-5

Preface

Purpose

This document describes how to install the Oracle Payment Interface (OPI) Self-Hosted Token Proxy Service.

This document does not cover installation of any prerequisites, for which a separate documentation is already available.

Audience

This document is intended for installers of OPI Self-Hosted 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 and any associated log files
- Screenshots 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/>

Oracle WebLogic product documentation is available on the Oracle Help Center at
<http://docs.oracle.com/en/middleware/>

Oracle Database product documentation is available on the Oracle Help Center at
<http://docs.oracle.com/en/database/>

Revision History

Date	Description of Change
November 2017	Initial publication.
December 2018	Added schema expiration information
March 2019	Updated PSP Configuration
April 2019	<ul style="list-style-type: none">• Added sections in Chapter 4 Certificates• Updated content in Chapter 5 OPIConfigX.exe• Updated formatting and cover page with new template.

Date	Description of Change
May 2019	Updated the snapshots in Chapter 3 Token Proxy Web Portal
July 2019	Updated security bugs in few chapters.

Overview of Token Proxy Service

Components Parts

Token Proxy Service has the following three main components:

- Database
- Token Proxy Service Web Portal
- Token Proxy Service

Installation Prerequisites

Before installing Token Proxy Service, verify your environment meets the following requirements:

- 64-bit host.
- Windows Server 2008 R2, 2012 R2, 2016
- Oracle 12c database server installed and running, and the user understands how to use and configure Oracle DB.
- WebLogic running to host the Web Portal, and the user understands how to use and configure Oracle WebLogic 12c.
- An SMTP server exists for sending emails to users.
- JRE (Java Runtime Environment) 1.8. If Token Proxy Service is installed on the same host as WebLogic (which includes JDK), a separate JRE for Token Proxy Service is not required.

The Database

- The database stores the configuration and audit log from the Web Portal.
- The Token Proxy Service requires read-only access to the database. If required, you can configure a different Token Proxy Service database user with a lower-level of privileges.
- The Web Portal requires a database user with privileges to make changes within the database.

 **NOTE:**

During installation, the Token Proxy Service creates a database schema. OPI does not override the period of time this schema remains valid because the

schema expiration date may already be defined by existing policies of the environment in which it is being installed.

By default, Oracle Database defines an expiration date of six months after creation. Be aware that if the schema's password expires, and the Token Proxy Service is subsequently unable to read from or write to the database, then service interruptions should be expected.

The Web Portal

- The Web Portal is used to configure the settings used by the Token Proxy Service.
- The Web Portal is a web application supplied in a WAR file suitable for hosting in WebLogic. It relies on WebLogic to store some of its configuration, such as the database connection string (datasource), and to provide a trusted SSL certificate for connections from users accessing the configuration web portal.

Token Proxy Service

The Token Proxy standalone application runs automatically as a service.

Connections from Listeners

- The application creates a Listener to monitor a TCP port for XML messages posted over HTTPS. The default Listener port is 443, but it can be set to a custom port number in the database. This Listener must be exposed to the client (Opera systems, for example).
- The Listener manages its own use of the certificates (TLS1.2) provided by the data center team, so a firewall or load balancer (if present) must not offer any form of HTTPS-to-HTTP bridging functionality. Instead, the connection must be passed directly to the Token Proxy Service.
- The certificates provided must be installed on all servers running the Token Proxy Service in the event the service is installed on multiple machines for load balance or failover

Connections to PSPs (Payment Service Providers)

- The service also makes outgoing connections to PSPs.
- The outgoing connection is to a URL specified by the PSP and the host/port (and optionally a path) is specified by the PSP.
- The outgoing connection can be over the internet or over VPN, but it must use HTTPS with TLS1.2 or greater.

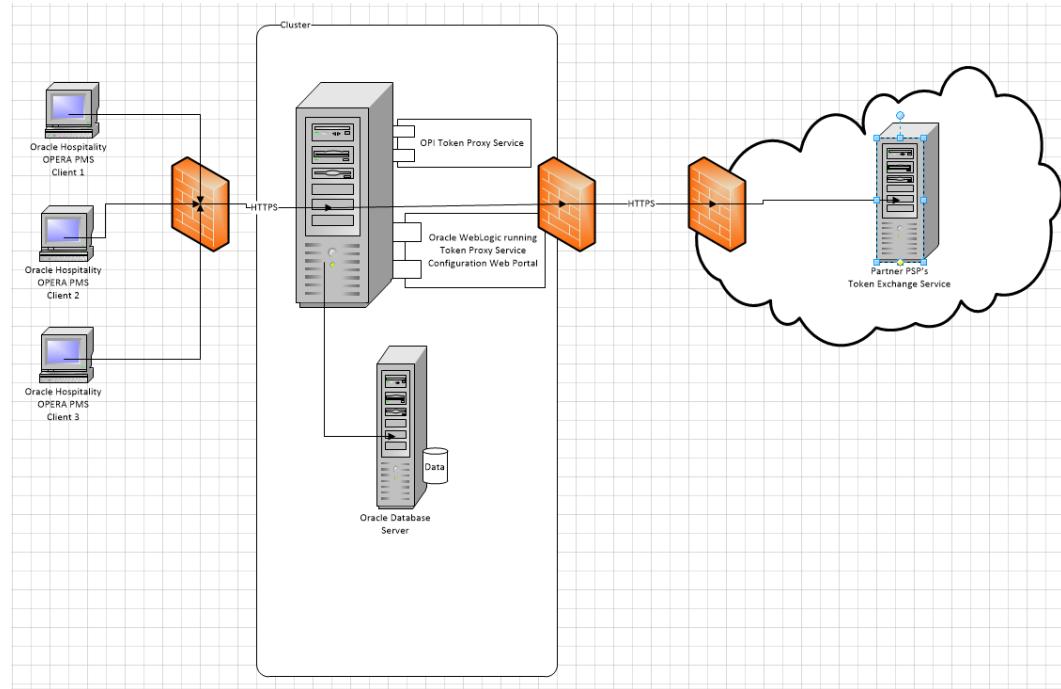
Recommended System Requirements

Table 1-1 – Recommended System Requirements

Dedicated	On Web Portal/WebLogic Host*
4 x vCPU	8 x vCPU
16 GB RAM	32 GB RAM
100 GB OS	100 GB OS
100 GB Data	100 GB Data

* The recommended requirements are increased due to the heavy footprint of WebLogic.

Figure 1-1 - Example Installation/Configuration



Installing Token Proxy Service

The Token Proxy Service installer verifies the existence of any required components, creates a database user, deploys a database schema, deploys the Web Portal used for configuration, and deploys the Token Exchange Service.

Installation and configuration of WebLogic & Oracle 12c is not the focus of this document.

Pre-Installation Checklist

Before installing Token Proxy Service, ensure you have the following information available:

- Oracle Database Information
 - Host, port, & service ID
 - DBA user credentials
 - User credentials that are approved for creation and meet any partner requirements.
- WebLogic host & authentication credentials
- SMTP host, port, & authentication credentials
- PSP details (including certificates)
- Client details (including Card Type setup from client's Opera configuration)
- Some installations may include additional network configuration and whitelisting in the data center, which requires network-specific information/IP addresses.

Installing Token Proxy Service

To install the Token Proxy Service, navigate to the TokenProxyInstaller_6.1.0.x.exe file, and then double-click it to begin.

- The installer creates installation logs in C:\TokenProxy\v6.1\LOGS.
- The installer verifies system compatibility and looks for the MW_HOME environment variable to use when deploying the Web Logic configuration.
- The installer allows you to proceed without the MW_HOME variable, but doing so limits the Web Logic deployment tasks the installer can complete. The MW_HOME variable is not mandatory because it is possible to run the Token Proxy Installer to deploy only the Token Proxy Service component.

Creating the MW_HOME Variable

If you do not have an MW_HOME variable and want to use the Token Proxy Installer to deploy the WebLogic .WAR file and to create the datasource on the machine you are running the installer on, cancel the installation and create an environment variable to reflect your WebLogic environment.

- Open Windows System Properties, click the **Advanced** tab, and then click **Environment Variables**.
- Click **New** in the **System Variable** section, and then enter **MW_HOME** in the **Variable name** field and the path of the WebLogic installation in the **Variable value** field.
- This will vary depending on your WebLogic installation path, but an example value might be :\\Oracle\\Middleware\\Oracle_Home
- Click **OK** to confirm, and then exit System Properties.
- Re-run the installer after creating the MW_HOME Environment Variable.

1. Select the **Complete** or **Custom** setup type.
- **Complete**: Install all components.
- **Custom**: Install selected components.
2. Enter the Token Proxy installation path, and then click **Next**.
3. Click **Install**.
4. On the **Database Server** dialog box, enter the credentials (Name/IP, Port #, Service) to allow the Token Proxy Service installer to connect to your Oracle 12c Database. The installer supports pluggable and legacy non-pluggable database formats.
5. Click **Next**.
6. Enter the **DBA Login ID** and **Password**. The installer requires DBA access to create a Token Proxy Service database user and to configure a Token Proxy Service database schema. The installer checks password complexity.
7. Enter the **User Name** and **Password** for the new database user. The installer checks password complexity.
8. Click **Next**.

The installer attempts to connect to the database using the supplied DBA credentials. If the connection fails, logs are written to your installation path. If required, resolve any connectivity or user/password issues and retry the database connection.

The installer attempts to create the user details specified in Step 7. If there are issues creating the DB User, make sure the database specified is open for updating. For example, using SQL Developer, connect to the database and execute the following command: ALTER DATABASE OPEN

The new database user has the **RESOURCE** role granted and has the following privileges:

- Create Materialized View
- Create Sequence

- Create Session
- Create Table
- Create Trigger
- Create View

9. Enter the **Host** address and the **Port** number.

- **Host:** The FQDN (Fully Qualified Domain Name) that you allocate in DNS to the Token Proxy Web Portal.
- **Port:** The HTTPS port number the Web Portal deployment is configured to listen on in Web Logic.

These details must be set correctly so that links in system generated emails (such as password resets) contain the correct URL.

To update Web Portal URL Configuration settings post-installation, edit **\ProgramData\TokenProxy\application.properties** using a text editor. You must restart the Web Logic logical server running the Token Proxy Service Web Portal for any configuration change to take effect.

10. Click **Next**.

11. Enter the SMTP server details. The Token Proxy Service requires access to SMTP server in order to send password reset emails.

- **smtp.host:** Your SMTP mail server address
- **smtp.port:** Your SMTP mail server port
- **Use TLS:** Select this option if the SMTP server supports TLS secured connections for sending login credentials. Enable this option in a production environment, if supported.
- **Authentication Required:** Select this option if the SMTP server requires username and password credentials to send email. If not required, uncheck this option and ignore the **smtp.username** and **smtp.password** fields.
 - **smtp.username:** If 'Authentication Required' is selected, set to the username of the SMTP credentials.
 - **smtp.password:** If 'Authentication Required' is selected, set to the password of the SMTP credentials.

12. Click **Next**.

The configuration file is created in the following path:
\ProgramData\TokenProxy\application.properties

To update SMTP settings post-installation, edit **\ProgramData\TokenProxy\application.properties** using a text editor. You must restart the Web Logic logical server running the Token Proxy Service Web Portal for any configuration change to take effect.

13. Select a Deployment Option.

- **Auto Deployment:** Select this option for a guided deployment of the WebLogic WAR file and datasource.

- **Manual Deployment:** Select this option if the Web Portal will be deployed in a clustered WebLogic environment. Deployments in clustered WebLogic environments must be performed manually.

14. Click **Next**.

15. Enter the WebLogic Connection Settings. This dialog does not appear when performing a manual deployment.

The connection is used to push the Token Proxy Service Web Portal .WAR file into WebLogic, and to create the Token Proxy Service Web Portal datasource configuration.

- **Host:** WebLogic IP address
- **Port:** WebLogic port number
- **Username:** WebLogic user name
- **Password:** WebLogic password
- **Protocol:**
 - **T3** is the default WebLogic Protocol.
 - **T3S** is the T3 Protocol with SSL.
 - **HTTP** is T3 wrapped in HTTP to allow routing through firewalls, if required.
 - **HTTPS** is T3S wrapped in HTTP to allow routing through firewalls, if required.

16. Click **Test Connection** to verify connectivity. If necessary, adjust the settings until the test succeeds, and then click **Next**.

By default, the WebLogic logical server Listen Address is localhost. In order for the Token Proxy Service installer to connect to WebLogic, the WebLogic logical server Listen Address may need to be set to an **IP**, **Hostname**, or **0.0.0.0**, depending on your Web Logic Environment.

17. Enter the WebLogic logical server name that the Token Proxy Service Web Portal will be deployed to.

- **Admin Server:** Deploy the Web Portal to the Admin server. Not recommended.
- **Deploy to one or more named servers:** Enter the name(s) of the WebLogic target server(s) where you want to deploy the WebPortal. Multiple servers can be specified as a comma-delimited list.

Prior to deploying the Web Portal configuration, verify the following:

- WebLogic Node Manager is running.
- WebLogic is running.
- The server you select for Web Portal deployment is running in WebLogic.

18. Click **Next**.

19. Select a datasource creation option.

- **Create a default datasource for the database connection:** Select this option for the installer to configure the WebLogic datasource that the Token Proxy Service Web Portal uses to communicate with the database.
- **I will create and manage the datasource myself:** Select this option to configure the datasource manually.

20. Click **Next**. If you previously selected **Create a default datasource for the database connection**, then the Token Proxy Service installer will attempt to add the datasource configuration.

If any part of the WebLogic deployment fails, then you are returned to the WebLogic Connection Settings dialog box. Resolve the issue and try to deploy again.

The installer will deploy the WebLogic configuration for the WebLogic Deployment and WebLogic Datasource components if WebLogic and Database are available.

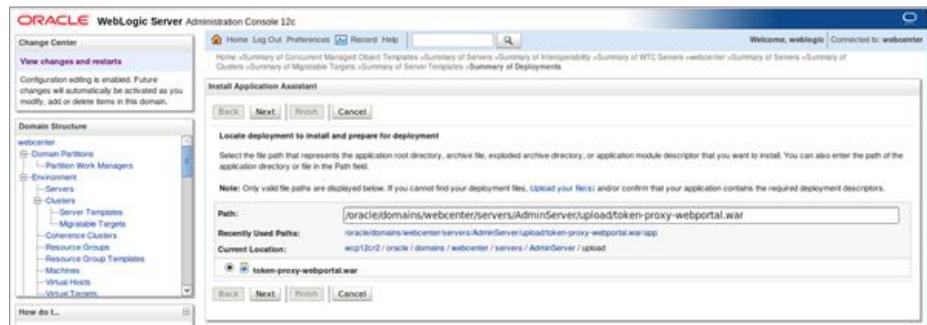
21. The **OPI Token Service** Windows service installation completes. The service remains in a stopped state until the Web Portal configuration is complete.

22. Click **Finish** to complete the Token Proxy Service installation.

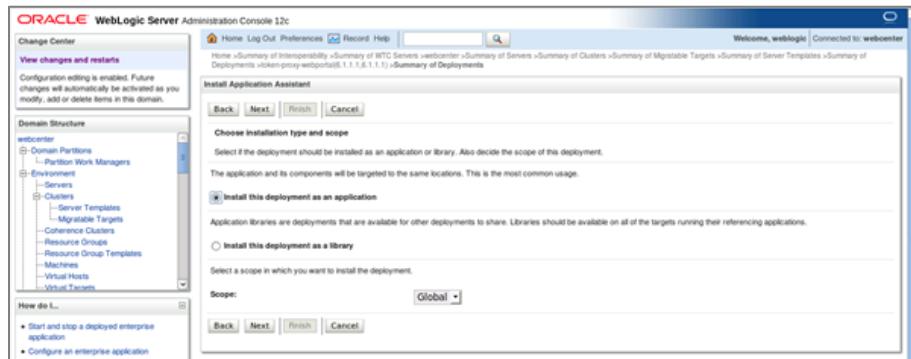
Manually Deploying the .WAR file in WebLogic

The Token Proxy Installer uploads the .WAR file to WebLogic as an Application deployment, unless you select the option to manually complete the WebLogic deployment.

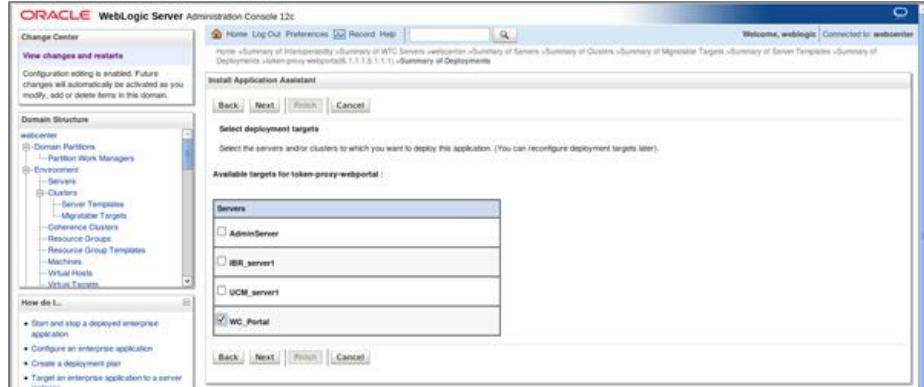
1. In the **WebLogic Server Administration Console**, locate the Token Proxy Service .WAR files location.



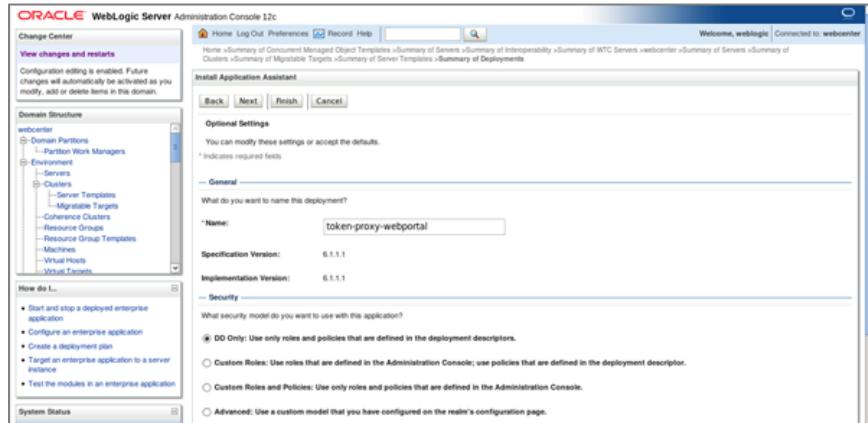
2. Select **Install this deployment as an application**.



3. Select the **WC_Portal** option.



4. Select **DD Only**, and then select other options required for your WebLogic environment.



5. Click **Finish**.

Token Proxy Configuration Web Portal

After deploying the Token Proxy Service .WAR file, your configuration portal should be accessible.

If the web portal starts up correctly, then you can browse to it using HTTPS and the configured FQDN (Fully Qualified Domain Name), port and application context, as shown in the following examples:

<https://example.com/token-proxy-webportal> if using standard HTTPS port 443.

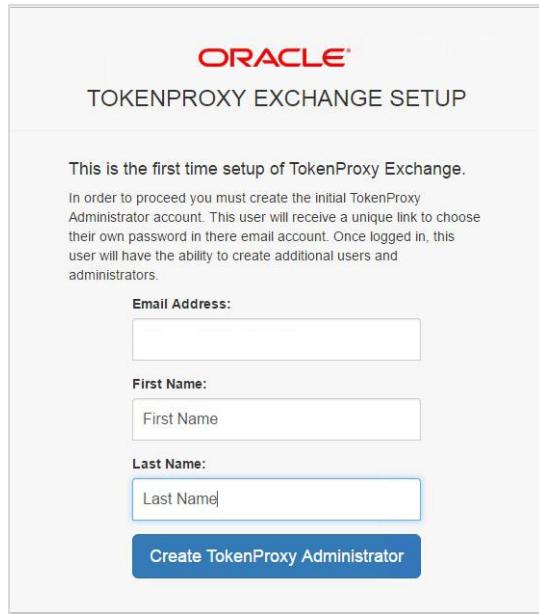
<https://example.com:8788/token-proxy-webportal> if using a non-standard port.

The portal detects that the initial configuration was not performed and redirects you to the Token Proxy Service Administrator Setup page.

The SMTP settings specified during installation must be correct. Incorrect settings prevent the admin from receiving initial login details and prohibits further configuration.

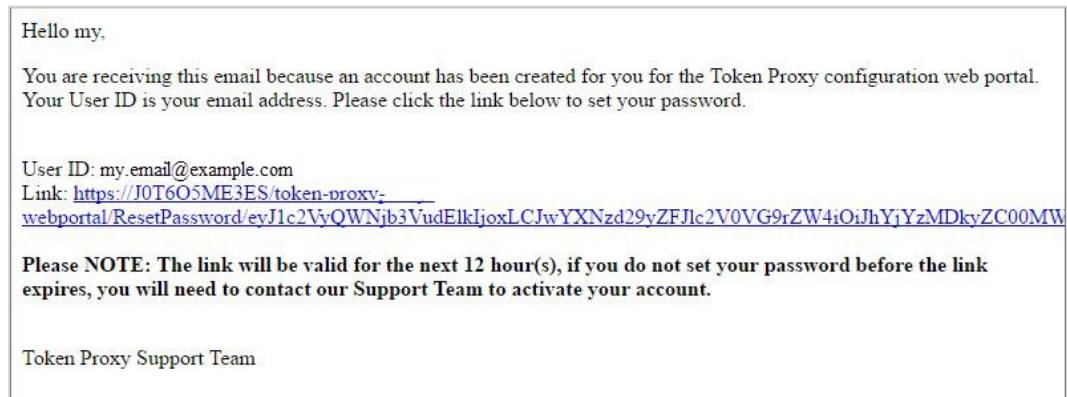
The default context root for the Token Proxy Service WebPortal is **/token-proxy-webportal**. This can be changed manually within WebLogic's configuration, although doing so will have adverse effect on the installer functionality for future modifications, repairs, or upgrades.

Token Proxy Exchange Setup



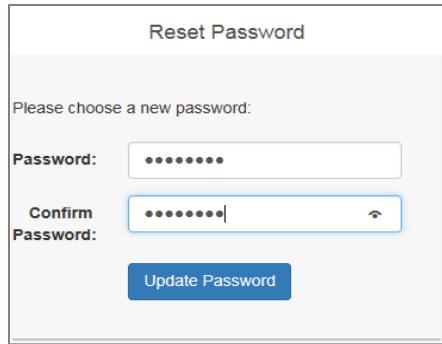
The Token Proxy Exchange Setup page should be completed by the person who will be managing the Token Proxy Service.

After completing the form, the Token Proxy Exchange Setup sends an email to the admin user that contains a link with a unique password reset token.



By default, the link is valid for 12 hours/720 minutes. To change the time limit, edit the **userTokenLifeSpan=720** setting in **C:\ProgramData\TokenProxy\application.properties** using a text editor.

The link in the email opens the password reset page, as shown below:



A screenshot of a 'Reset Password' dialog box. The title bar says 'Reset Password'. The main area contains the text 'Please choose a new password:'. Below this are two input fields: 'Password:' and 'Confirm Password:'. Both fields contain the placeholder text '*****'. A blue 'Update Password' button is at the bottom.

Passwords must meet the following criteria:

- Must be between 8 and 20 characters in length.
- Must contain characters from each of the following categories:
 - Capital or lowercase letters: A/a through Z/z
 - Digits: 0 through 9
 - Symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` | ~

3

Configuration Web Portal

You may experience formatting and performance issues if you view the Web Portal using a browser that does not support HTML5.

Signing In

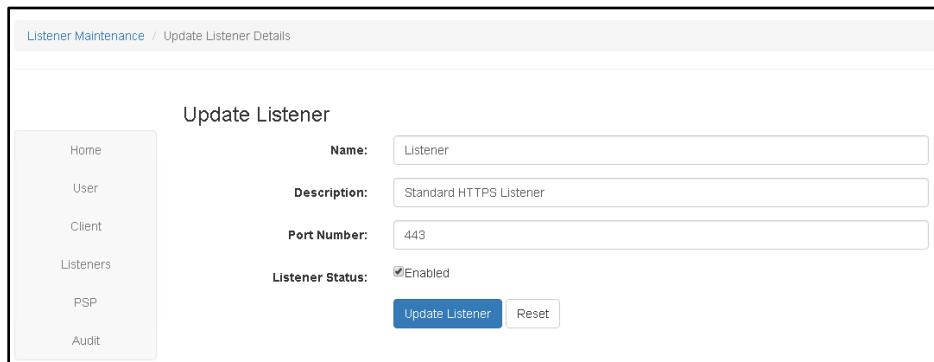
To sign in, browse to the application root and enter your credentials. The Token Proxy Service Web Portal home page opens.

Listeners

The initial setup procedure creates a standard HTTPS Listener. This is the port the Token Proxy Service listens on for connections from Oracle Hospitality Opera PMS clients.

Updating the Listener

On the main menu, click **Listeners**, and then select **Update** for the appropriate Listener record. All Listeners records are hardcoded to use a certificate named OPI_Listener.pfx.



The screenshot shows the 'Update Listener' page within the Listener Maintenance interface. The left sidebar has tabs for Home, User, Client, Listeners (which is selected), PSP, and Audit. The main form has fields for Name (Listener), Description (Standard HTTPS Listener), Port Number (443), and Listener Status (Enabled with a checked checkbox). There are 'Update Listener' and 'Reset' buttons at the bottom.

Creating and configuring PSPs

1. On the main menu, click **PSP**.
2. On the **Actions** menu, click **Create PSP**.
3. Enter the **Name** and **Description**.
4. **Host:** Enter the IP address of the PSP or server name. For example if the URL provided by the partner is <https://upitest.shinhwaworld.com:443/token.do>, then enter only upitest.shinhwaworld.com in the host field and do not append https://.
5. **Port:** Enter the port number to connect to the partner. For example: 443.

6. **Context Path:** Enter the context path provided by the partner if any. For example: token.do
7. Enter the PSP's **Failover Host** and **Failover Port** if the PSP has failover services available.
8. Select the **Active** option to allow the PSP to be chosen when creating a client.
9. Enter the **Proxy Host** and **Proxy Port** details if the outbound access to the PSP should go via a proxy.
10. Restart the OPI Token Service for the configuration to take immediate effect. Always restart the OPI Token Service after creating or changing a PSP.
 - Deselect the **Active** option to set a PSP to inactive status.
 - Use the **Filters** to show only Active or Inactive PSPs.

Deleting PSPs

1. On the main menu, click **PSP**.
2. Click the **Update** drop-down list for the record you want to remove, and then click **Delete**.

Configuring Clients

1. On the main menu, click **Client**, and then click **Create Client** on the **Actions** menu.
2. Enter the client **Name** and **Description**.
The **Account ID** should be set as the Oracle Hospitality Opera PMS **CHAINCODE & PROPERTYCODE**.
3. Enter the **Username** and **Password** the Oracle Hospitality Opera PMS client system should use to authenticate with the Token Proxy Service. The Username must be unique.
These values should match the values set in Opera on the **Config | Setup | Property Interfaces | Interface Configuration | <OPI Interface Record> | Edit | Custom Data tab**.
4. Select a **Listener**. The client accepts incoming tokenization requests from the Listener.
5. Select a **PSP**. The client forwards tokenization requests to the PSP.

The PSP uses the **PSP Account Identifier** to uniquely identify client tokenization requests. It is recommended the **PSP Account Identifier** be set the same as the **Account ID** value, for continuity where client chains have some properties communicating with a PSP's tokenization solution via OnPremise Token Exchange, and other properties communicating via Token Proxy. Although, this will ultimately depend on how the PSP have configured the client on their side.

Max Items Per Request is the number of records included in each tokenization request to the PSP. The Token Proxy Service processes the records received into batches of the number specified. The default **Max Items Per Request** is 50.

6. Select the **Card Type Table** as either 'Default Card Type Table' or 'Copy from Client' option. If 'Copy from Client' option is selected, then you can copy the card type configuration from the client system.
7. Select the **Active** option to activate the client account.
8. Click **Create Client**.

Client Maintenance / Create Client

Client Account Details

Home **User** **Client** **Listeners** **PSP** **Audit**

Name: Hotel1

Description: Hotel1

Account ID: CHAINCODE|PROPERTYCODE

Username: user

Password:

Verify Password:

Listener: Standard HTTPS Listener

Payment Service Provider: TestPSP

PSP Account Identifier: HotelIdentifier

Max Items Per Request: 50

Card Type Table: Default Card Type Table
 Copy from Client

Client Status: Active

Create Client **Reset**

Troubleshooting:

- If you cannot find the required Listener or PSP in a drop-down list, verify the **Active** option is selected on the Listener or PSP page.
- Always restart the OPI Token Service after creating or changing a client.

Updating Clients

The process of updating the client is similar to creating it, except that the credentials section is different.

- The **Username** field appears as read-only.
- **Change Credentials** allows you to update the username, or the username and password.

- Always restart the OPI Token Service after creating or changing a client.
- Deselect the **Active** option to set a client to inactive status.
- Use the **Filters** to show only active or inactive clients.

Deleting Clients

1. On the main menu, click **Client**.
2. Click the **Update** drop-down list for the record you want to remove, and then click **Delete**.

Card Type

The Card Type page allows you to manage the IssuerId/Card Type mappings for each Client. It is a subsection of the Client page. On the Client's page, select Update for the relevant record and then click **Manage Card Types**.

The Token Proxy web portal will create any new Client records with a set of predefined Card Type to IssuerId mappings. These need tailored to complement the Clients actual configuration.

Card Type Mapping

- **Issuer ID:** Select the value from Table 2 – Predefined Credit Card Mappings. Partners expect one of the listed numeric values. These numeric values come from the OraclePaymentInterface spec.
- **Client Card Type:** The Client Card Type value comes from the Oracle Hospitality PMS Client configuration.
- **Description:** Provides information about the mapping.

All tokenization requests that have a **Card Type** value with an unrecognized mapping will be returned to the Oracle Hospitality PMS client as **CA 98 Cash**.

Updating a Card Type

1. On the Client's page, select **Update** for the relevant record and then click **Manage Card Types**.
2. From the **Action** column, select **Update** for the relevant Card Type record.
3. Amend the details as required, click **Save Changes**.

Adding a New Card Type

If there are any additional local tenders configured, they will also need to be added to the clients Token Proxy configuration.

1. On the Client's page, select **Update** for the relevant record and then click **Manage Card Types**.
2. On the **Actions** menu, click **Create Card Type**.
3. Enter the details as required, and then click **Save Changes**.

 **NOTE:**

It is not possible to have duplicate IssuerId records. For example, it is not possible to configure the following example because TokenProxy would not know whether to forward IssuerId 01 responses to VA or VS.

VA	01	VISA
VS	01	VISA

However, it is possible to map multiple IssuerId's to the same client card type if consolidation is required by the client.

For example, if site only has *Mastercard* configured in their PMS system, they may wish to map both *Mastercard* & *Mastercard Debit* to the same MC card type.

MC	02	MasterCard
MC	24	MasterCard Debit

Deleting a Card Type

1. On the Client's page, select Update for the relevant record and then click **Manage Card Types**.
2. From the **Action** column, click the **Update** drop-down list for the record you want to remove, and then click **Delete**.

Default Card Type Configuration

The following tables lists the Client Credit Card Type, the Token Proxy Service Issue ID, and a description of the card

Table 3-1 – Predefined Credit Card Mappings

Card Type	Issuer ID	Description
ZZ	00	Local/Debit
VA	01	VISA
MC	02	MasterCard
AX	03	American Express
DC	04	Diners Club
JC	05	JCB
CU	06	China Union Pay

Card Type	Issuer ID	Description
GC	07	SVC/Gift card
ZZ	08	Others
CD	09	CUP Debit
ZY	10	Debit SMS
ZZ	11	Bank Card
DS	12	Discover
PC	13	PayPal
SD	16	UKDM/Switch
VE	17	VISA Electron
VD	18	VISA Debit
MA	19	Maestro
VP	20	VPay
AL	21	Alliance
EC	22	EC Chip
BC	23	GiroCard
MD	24	MasterCard Debit

Creating Additional Users

1. On the main menu, click **User**, and then click **Create User** on the **Actions** menu.
 - **Login Name:** Email address of the new User. The password reset email is sent to this email address.
 - **First name:** First name of the new User
 - **Last name:** Last name of the new User
 - **Account Status:**
 - **Active:** Activates the account.
 - **Locked:** System administrator may need to uncheck this option if a user cannot log in to the system.
2. Drag the required **Role** for the new User from the **Available** box to the **Assigned** box, and then click **Create User**.

User Maintenance / Create User

Create User

Home
User
Client
Listeners
PSP
Audit

User Email: client1.user@example.com

First Name: Client

Last Name: user

Account Status: Active Locked

Client Systems(s):

Available Clients	Assigned Clients
Hotel1	

Role(s):

Available Roles	Assigned Roles
SystemAdmin	ClientUser

Create User **Reset**

Deactivating Users

It is not possible to delete users; they can only be deactivated.

1. Deselect the **Active** option on the user profile to remove web portal access rights.
2. Use the Filters to show only active or inactive users.

Roles

The Token Proxy Configuration Portal includes the following two predefined Roles:

- **System Administrator:** Can view all pages within the Web Portal.
- **Client User:** Can only view the Home Page and the Client System Configuration Pages.

After you create a Client System, you can further restrict Client User access by dragging a **Client System** from **Available Clients** to **Assigned Clients** on the Update User page.

User Maintenance / Update User

Update User Details

Home User Client Listeners PSP Audit

Login Name: client1.user@example.com

First name: Client1

Last name: user

Account Status: Active Locked

Client Systems(s):

Available Clients	Assigned Clients
	Hotel1

Role(s):

Available Roles	Assigned Roles
SystemAdmin	ClientUser

Save Changes **Reset**

Audit

The Audit page displays audit log information detailing configuration completed via the Web Portal.

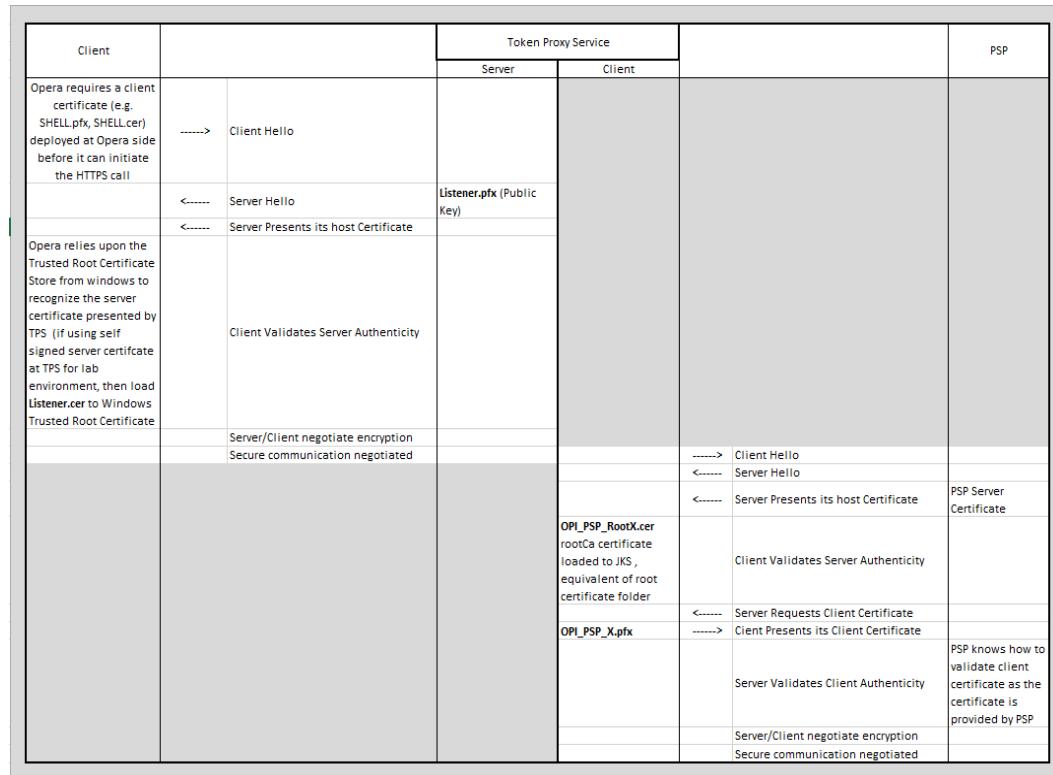
- Use the **Filters** menu to filter the displayed records.
- Click **Export XLS** to export records in Excel format.
- Click the **Purge** button to purge any Audit Trail events that are older than 90 days.

4

Certificates

HTTPS is mandatory for the communication between Opera and TPS and between TPS and PSP, therefore certificates are required to set up for each of the communication path.

The below diagram depicts the certificates used for each of the communication path during a transaction.



Certificates for Communication between TPS and PSP

In order for TPS to properly trust the PSP server, it requires a copy of the public root (in the format of the .cer or .crt file) of the server certificate deployed at PSP.

The public root of the PSP server certificate will need to be imported into a Java key store file with name **OPI_PSP_XRoot** (where X is replaced with the unique id of the PSP record from the Token Proxy Service configuration web portal). You can use the TPS certificate manager tool to set up the public root of the PSP server certificate in the required key store. For more details, please refer to Self-hosted Token Proxy Service Cert Manager User Guide published at https://docs.oracle.com/cd/E79534_01/index.html.

In order for TPS to properly identify itself to the PSP, so that PSP can authenticate to ensure TPS's identity, TPS also requires PSP to provide a client certificate file which is to be deployed at TPS side. The client certificate file is in the .pfx file format and is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. Because this client certificate file is provided by the PSP, the PSP should have no issue authenticating TPS when TPS presents this client certificate during HTTPS handshake.

In order for TPS software to pick up the client certificate file, the file is expected to be named OPI_PSP_X.pfx (where X is replaced with the unique id of the PSP record from the Token Proxy Service configuration web portal). The client certificate file should also be placed at the TPS key folder. You can use the TPS certificate manager tool to set up the client certificate file so that the file will be automatically named properly and placed at the right location.

The certificate manager tool will also automatically take care of the configuring the certificate passwords for TPS.

NOTE:

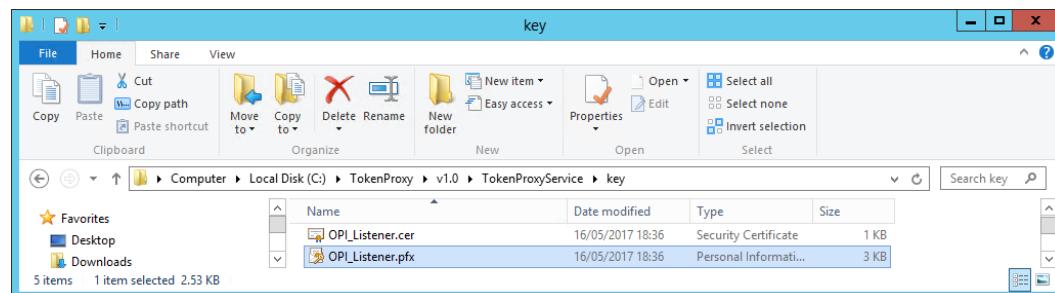
The Certificates expiration date will vary depending on what was set during initial configuration. You can check the expiration date using tools like: certutil –dump <pfx file>. The certutil tool is a command line tool that comes with Windows OS. **You must update the certificates prior to the expiration date to avoid downtime to the Token Proxy Service.**

Certificates for Communication between Opera and TPS

For HTTPS communication between Opera and Token Proxy Service, a server certificate is required to be deployed on the listener at the Token Proxy Service side.

The server certificate deployed with Token Proxy Service should be a CA signed certificate provided by the third party. Refer to section "[Creating CSR Using Java Keytool Utility](#)" if you have questions about how to create a certificate signing request.

Token Proxy Service expects the server certificate to be named OPI_Listener.pfx. The file should be located in the TPS key folder (see image below).



Similar to the certificates used between TPS and PSP, you can also use the certificate manager tool to set up the server certificate deployed at TPS side for HTTPS communication between Opera and TPS.

Opera also requires a client certificate file to be deployed at Opera side for its HTTPS communication to TPS.

- The client certificate file required by Opera can be created with the [Client Certificate Creator](#) tool, and should have a common name that reflects the Chain Code and Property Code of the Opera system on which they will be used.
- Copy the .pfx and .cer files to a temporary location on any Opera registered terminal from where you will run the Token Exchange transactions. Import the certificates using mmc.exe.
 - The .pfx import to Personal. You will need the password assigned to the certificate in order to import it.
 - The .crt import to Trusted Root Certification Authorities.

Certificates created with the Certificate Creator tool have a default expiration date of five years from the date of creation. **You must update the Token Proxy Service Server Side Certificates prior to the expiration date to avoid downtime to the Token Proxy Service.**

Any client that connects to the Token Proxy Service will also require the public key of the Token Proxy Service listener importing to the Trusted Root Certificate Folder in order to validate the authenticity of the Token Proxy Service.

Creating CSR Using Java Keytool Utility

It would be customer's responsibility to obtain the CA signed certificate. The process of using Java keytool utility is to generate a Certificate Signing Request as follows:

Step 1: Generate a Keystore and Private Key

Create a certificate keystore and private key by executing the following keytool command:

NOTE:

The keytool utility is located in your JDK's "\bin" directory [your JDK folder path, for example: C:\Program Files\Java\jdk1.8.0_162]\bin\keytool -genkey -alias <your_alias_name (pick whatever name you deem proper)> -keyalg RSA -keystore <your_keystore_filename (pick whatever name you deem proper for your keystore)>

Specify a password (and remember your password)

Step 2: Generate a CSR

The CSR is then created using the following command:

[your JDK folder path, for example: C:\Program Files\Java\jdk1.8.0_162]\bin\keytool -certreq -alias <your_alias_name (the alias

name you created above)> -keyalg RSA -keystore <your_keystore_filename (the keystore name you created above)> -file certreq.csr -

 **NOTE:**

When generating a CSR, enter the domain of your website (i.e. www.example.com) in the "first- and lastname" field.

After the CSR file is created, you can order your SSL/TLS certificate through your certificate vendor by following their corresponding procedure using the CSR file.

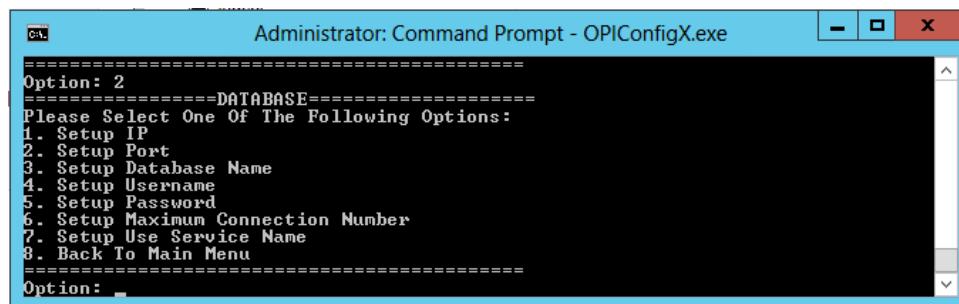
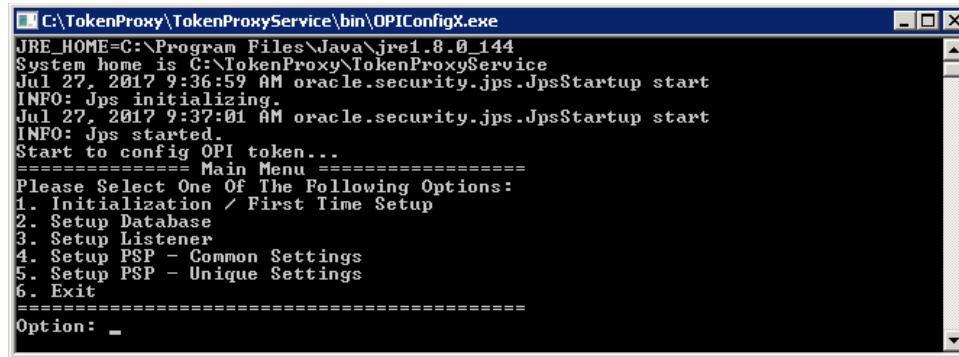
5

OPIConfigX.exe

The **OPIConfigX.exe** utility allows you to set passwords for the Database, Listener, and PSPs in the Token Proxy Service configuration.

\TokenProxyService\bin\OPIConfigX.exe

- 1. Initialization/First Time Setup:** Runs all options consecutively (If you plan to use certificate manager to set up certificates, then you can skip this option because you will only need to use OPIConfigX to set up the database).
- 2. Setup Database:** Configures the Token Proxy Service configuration for the Oracle Database. This option does not change the User or Password at the database side, it only updates the Token Proxy Service configuration. The Database configuration change should be made by the database administrator.



- Setup IP:** The IP address of the Oracle Database.
- Setup Port:** The port number of the Oracle Database.
- Setup Database Name:** The Token Proxy Service database name created during installation.
- Setup Username:** The username for the Token Proxy Service database created during installation.
- Setup Password:** The password for the Token Proxy Service database created during installation.
- Setup Maximum Connection Number:** The default is 40.

- **Setup Use Service Name:** If connecting to an Oracle Pluggable Database, the service name should be used.

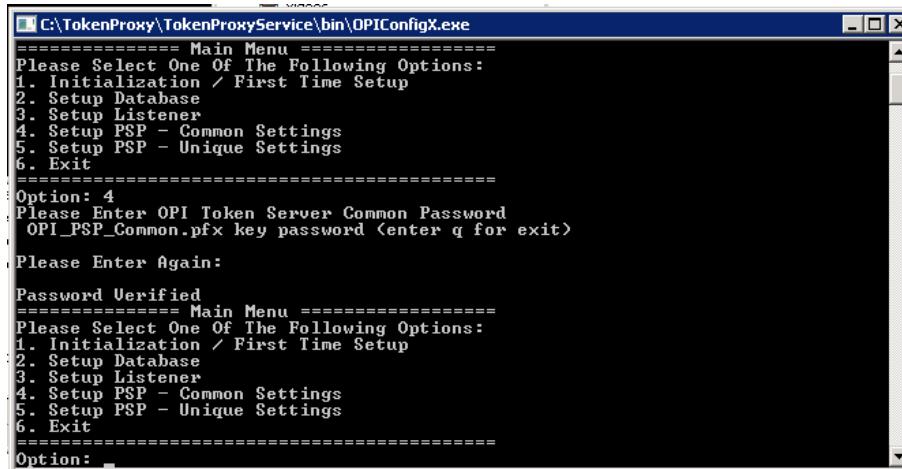
3. **Setup Listener:** Sets the password of the Listener certificates (If you plan to use certificate manager to set up certificates, then you can skip this option because you will only need to use OPIConfigX to set up the database).



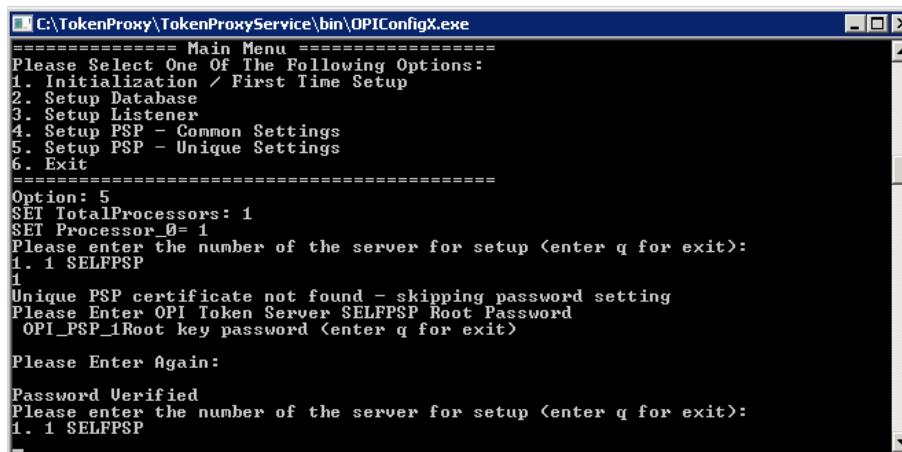
This option sets the password for the following Listener certificate:

\TokenProxyService\key\OPI_Listener.pfx

4. **Setup PSP – Common Settings:** Sets the password of the common PSP certificates (If you plan to use certificate manager to set up certificates, then you can skip this option because you will only need to use OPIConfigX to set up the database).



5. **Setup PSP – Unique Settings:** Sets the password of the **PSP certificates** (If you plan to use certificate manager to set up certificates, then you can skip this option because you will only need to use OPIConfigX to set up the database).



- If the database and PSPs have been configured correctly in the Web Portal, then select the number for the PSP certificate password you want to set.
- Enter and confirm the password for both the .pfx and the root certificates.

6. **Exit:** Exits the OPIConfigX utility.

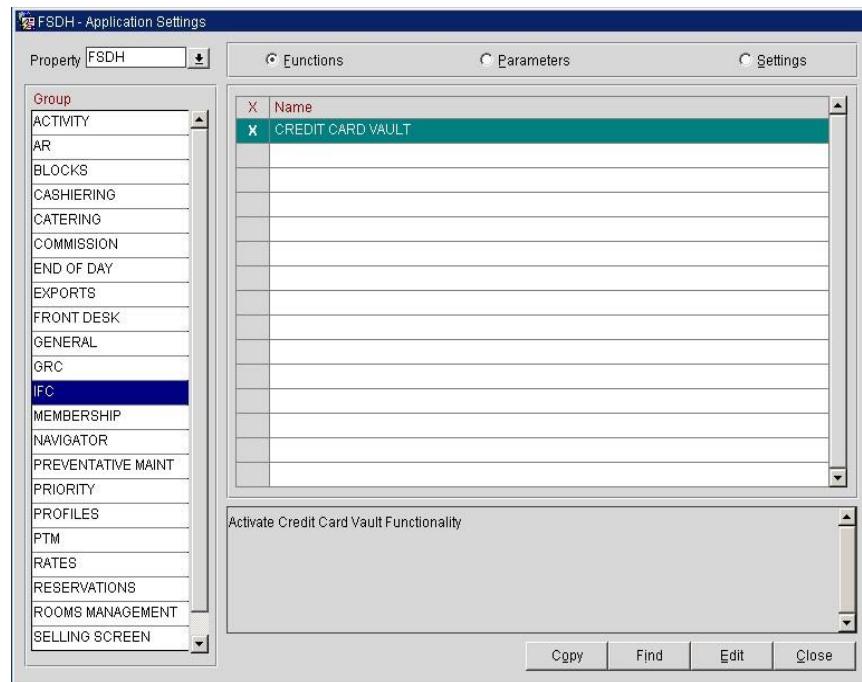
6

Opera Configuration

Configuring Opera for real-time transactions via OPI/IFC8 is not the focus of this document. For information about configuring Opera and OPI/IFC8, refer to the *OPI and OPERA Installation Guide* found at: http://docs.oracle.com/cd/E79534_01/index.html

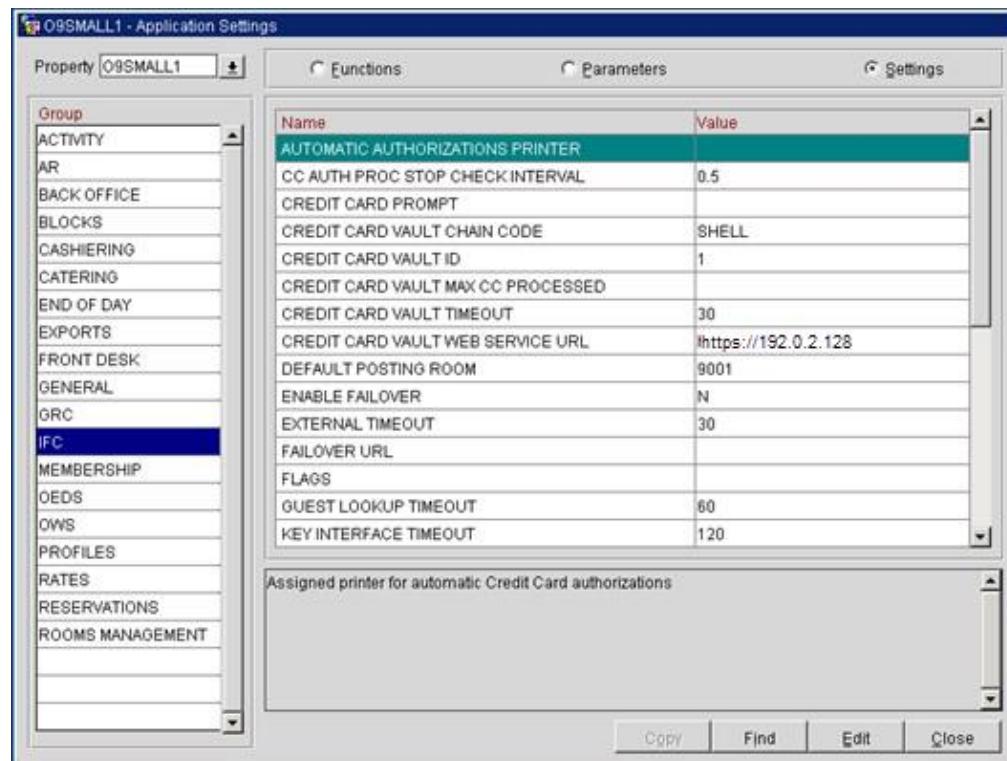
Configuring the CC Vault

Navigate to **Setup | Application Settings | IFC Group | Functions**, and then enable **CREDIT CARD VAULT**.



Configuration | Setup | Application Settings | IFC | Settings

- OPERA uses the **CREDIT CARD VAULT CHAIN CODE** for the certificate lookup.
- **CREDIT CARD VAULT WEB SERVICE URL** value should be in the format:
`https://<ipaddress_ksi_host>:<port>`
- **CREDIT CARD VAULT ID** is currently not used.
- **CREDIT CARD MAX CC PROCESSED** is set to what the PSP can support for the number of records sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. If this field is blank, then the default value is 50.
- **CREDIT CARD VAULT TIMEOUT** is set to the timeframe to wait for a response from the Token Proxy Service. At least 45 is recommended.

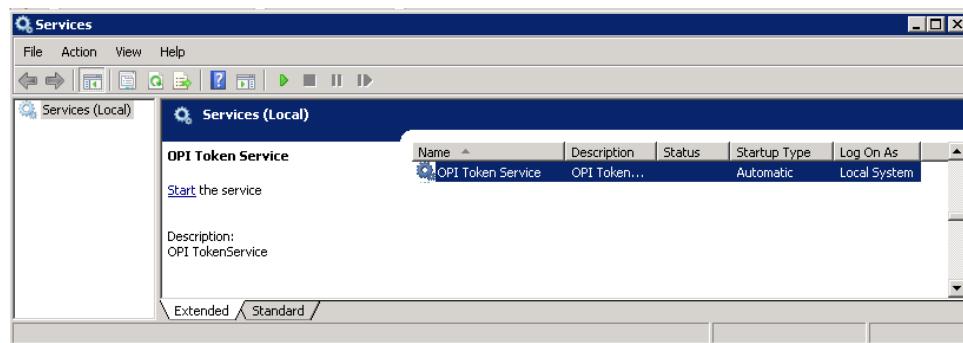


Token Proxy Service Maintenance & FAQ

Services

When Token Proxy Service installation is complete, an OPI Token Service is present. The OPI Token Service should start when your configuration is complete or after a reboot.

- Always restart the OPI Token Service after creating or changing a client.



Modify, Repair, or Remove Token Proxy Service

To Modify, Repair, or Remove the Token Proxy service:

- Run the Token Proxy Service installer on a system with an existing installation of Token Proxy Service.
- Select the **Custom** installation option, and then choose to **Modify, Repair, or Remove**.

Modify

Allows you to add new features or remove already installed components.

If you select the Modify option, then the installer attempts to install each component selected and removes any components that are not selected, regardless of what components are already installed.

For example, if the host machine already has the service component installed and Modify is run:

- If Datasource, Web Portal and Service are selected, then the installer will attempt to install all three components.
- If Datasource, Web Portal are selected and Service is not selected, then the installer will install Datasource & Web Portal components, and removes the service component.

- If Datasource, Web Portal and Service are selected, and they are already installed the installer will do nothing.

Repair

Reinstalls the currently installed features. All credentials entered during installation must be entered again during repair.

Remove

The Token Proxy Service installer removes the components in the reverse order of deployment.

- All credentials entered during installation must be entered again during removal to allow the installer to access and remove various components.
- WebLogic must be running for the Token Proxy Service installer remove the portal and datasource configuration.
- The Token Proxy Service database is not deleted during the removal process.

Token Proxy Service Log Files

Installation

The Token Proxy Service general installation log is written to:

\TokenProxy\6.1\LOGS\TokenProxy_Installation.log

As each of the Token Proxy Service components are installed, there are more specific logs relating to each part, that are written to;

\TokenProxy\LOGS

- i. Schema
- ii. TokenProxyService
- iii. TokenProxyWebPortal

Token Proxy Service Configuration Logs

Configuration Audit data is stored in the Token Proxy Service database. Log in to the Token Proxy Web Portal as a System Administrator to view the data.

Token Proxy Service – Service Logs

Token Proxy Service – service logs are found at the path

\TokenProxy\TokenProxyService\log

These logs are only created and populated once the **OPI Token Service** is up and running.

Debug.log

General detailed logging.

- Rotated by file size, the maximum size is 20MB.
- Current debug log filename is **debug.log**.
- The previous debug log filename is **debug.log.1**
- **debug.log.X**, sort by date.

Gateway.log

- Rotated by file size. The maximum size is 20MB.

System.log

- Check the Token Proxy Service build number.
- Rotated by file size. The maximum size is 20MB.

Transaction.log

- Lists details of each transaction handled by the Token Proxy Service.
- Rotated daily.
- The current transaction log filename is **transaction.log**
- The previous day's transaction log filename is **transaction.log.YYYY-MM-DD**

Token Proxy Service Password Maintenance

The passwords for the Token Proxy Service database and various certificates are set during installation.

You can use the [OPICConfigX.exe](#) utility to update passwords post-installation within the Token Proxy Service configuration.

\TokenProxy\TokenProxyService\bin\OPICConfigX.exe

```
===== Main Menu =====
Please Select One Of The Following Options:
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP
5. Exit
=====
Option: 
```

Select the required function, and then enter the updated credentials you want to set in the OPI configuration.

NOTE:

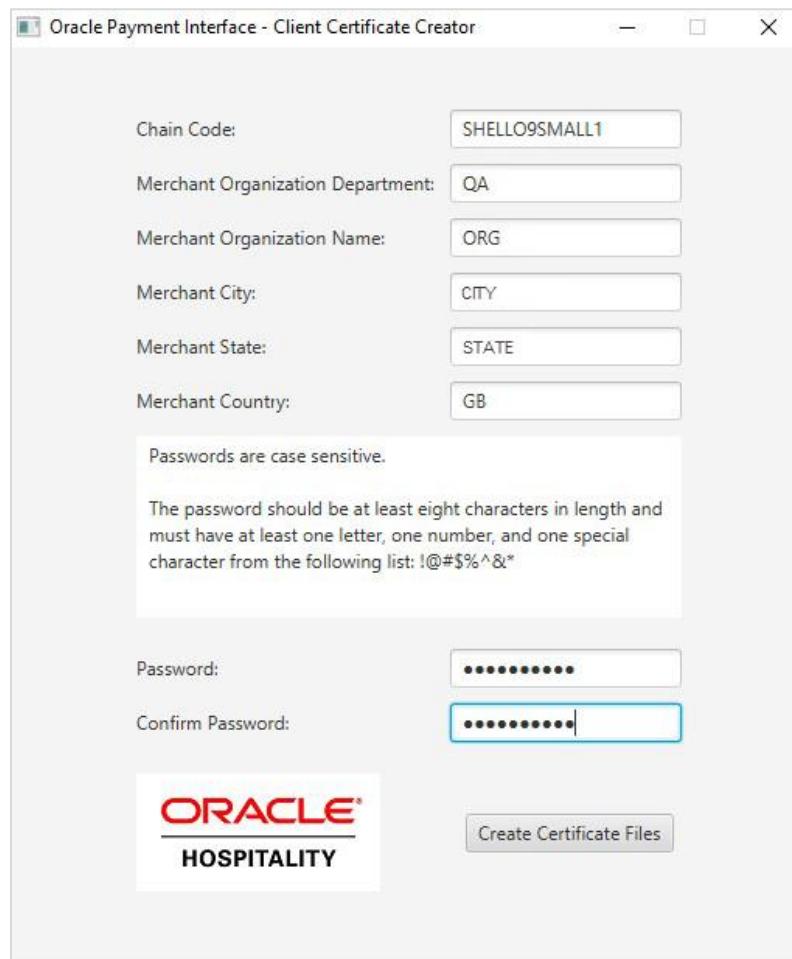
The OPIConfigX.exe utility does not change the Oracle database password itself. The Database Administrator should change the password via the preferred method.

OPI Client Certificate Creator

The OPI Client Certificate Creator utility can be used to create self-signed certificates.

The OPI Client Certificate Creator is included in the subfolders of the Token Proxy Service installation.

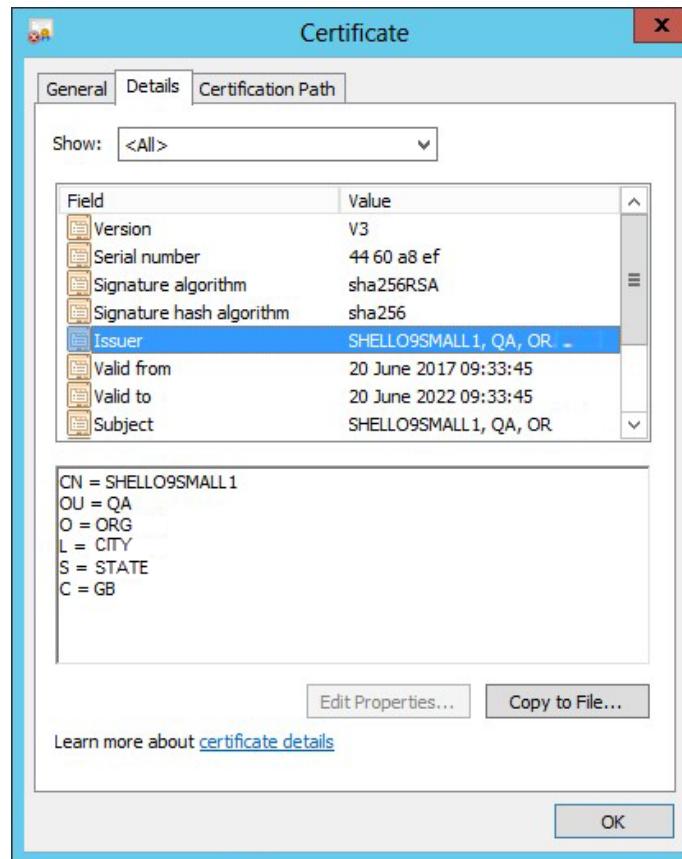
1. Run **CertCreator.jar**, and then add the required information.
2. Click **Create Certificate Files** when complete.



3. Specify the location to save the certificates, enter the filename, and then click **Save**.
 - Both a .pfx and .cer are created in the specified location.
 - The certificate expires five years from the date of creation.

The OPI Client Certificate Creator fields translate to standard certificate attributes as follows:

Chain Code	>	CN	(CommonName)
Merchant Organization Department	>	OU	(OrganizationalUnit)
Merchant Organization Name	>	O	(Organization)
Merchant City	>	L	(Locality)
Merchant State	>	S	(StateOrProvinceName)
Merchant Country	>	C	(CountryName)



TPS Configuration Backup

The Token Proxy configuration is held within the database created by the installer.

Listener and PSP Certificates are held within
\TokenProxy\v1.0\TokenProxyService\key

Encrypted Passwords for the database connection and certificates are held with the wallet files in **\TokenProxy\v1.0\TokenProxyService\properties**.