Oracle® Hospitality Payment Interface

PSP Certificate Management User Configuration Guide

Release 20.3
F35727-02
May 2023

ORACLE

Oracle Hospitality Payment Interface PSP Certificate Management User Configuration Guide Release 20.3

F35727-02

Contents

Preface

Purpose

This document describes how Payment Service Provider (PSP) Certificate Management User can manage and resolve certificate expiry issues in the OPI Configurator tool.

Audience

This document is intended for PSP Certificate Management User.

Customer Support

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

https://iccp.custhelp.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/

Table 1 Revision History

Date	Description
July 2020	• Initial Publication
November 2020	• Updated for release 20.3
March 2022	• Updated content in PSP Certificate Management chapter
May 2023	• Updated the Customer Support section with the new support portal name and URL

1

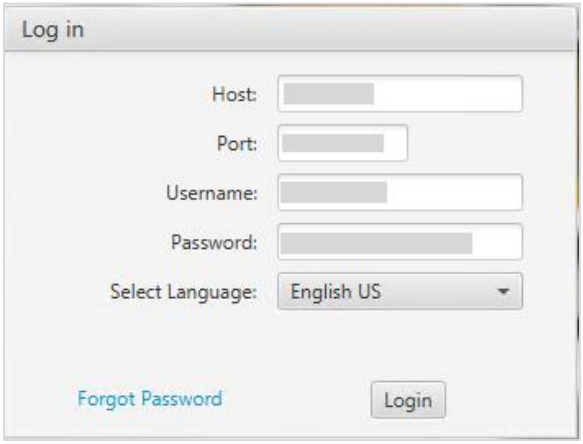
PSP Certificate Management

PSP Certificate Management user allows PSP support personnel to update the certificates on behalf of the customer. They have access only to Certificate Management in the OPI Configuration tool and can update only PSP certificates that are provided by PSP.

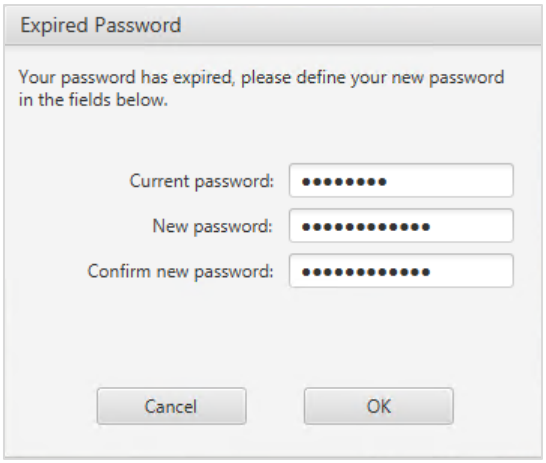
> **NOTE:**
>
> PSP Certificate Management user can only access OPI Configuration tool in 'Standard' mode and cannot access the Wizard mode.

PSP Certificate Management Users First Login

1. Double click **OraclePaymentInterface\v20.3\Config\LaunchConfigurator.bat.**
2. Log in to the OPI Configuration tool by providing the PSP Certificate Management user account **Username** and **Password.**



3. The first time you log in to the OPI configuration tool as a new user, you must enter a **Username** and a **One-time Password**.
4. Enter the **One-time Password** again, and then enter and confirm the **New Password**.

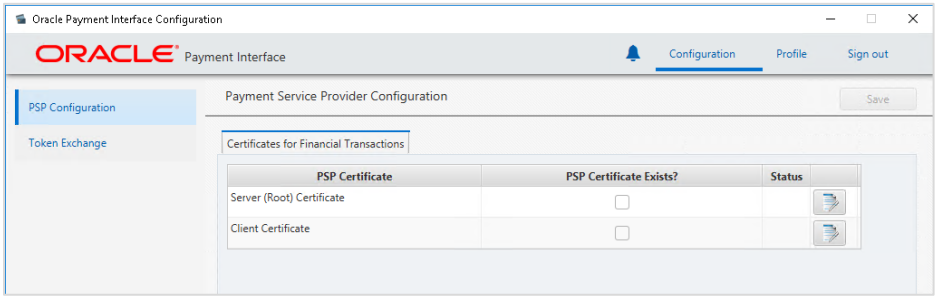


5. Click **OK**.

   The system appears with a message saying “Your password was changed successfully, please sign in with your new password”.

6. Click **OK**.

   You can now log in with your username and new password. The PSP Configuration home page appears.



   You can perform the following operations in the OPI Configuration tool:

   – Import PSP Certificates for Financial Transactions and Token Exchange.

   – Update passwords for certificates and keystores.

   – View Notification icon and resolve certificate expiry issues by updating the certificates.

   – Editing your User Profile.

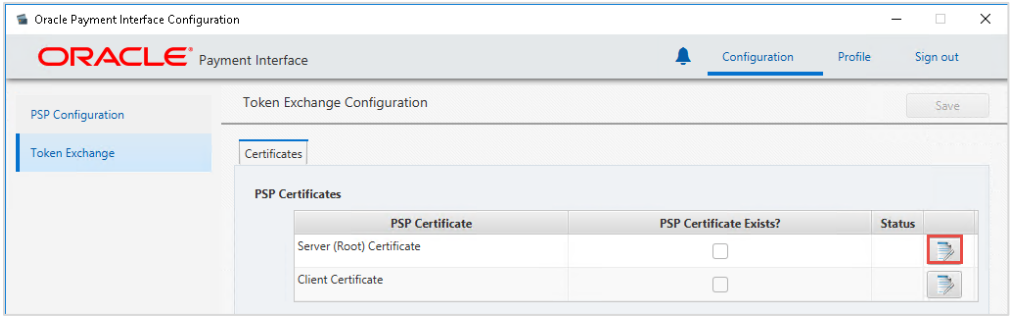
For more information on how to create a new user or change a forgotten password, see OPI Installation and Reference Guide.

Import Certificates for Token Exchange

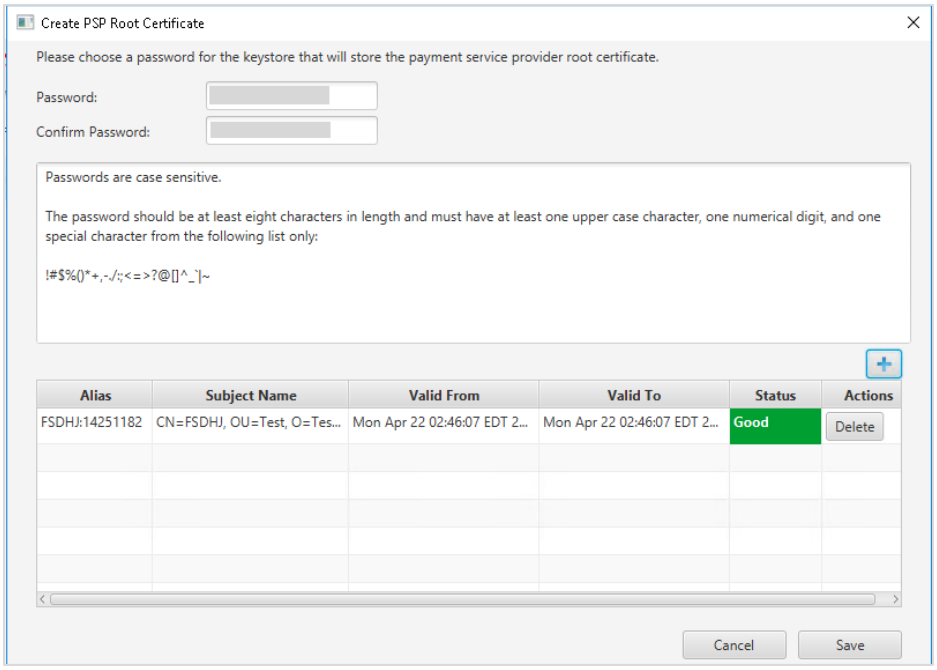
You can import certificates for token exchange on behalf of the customer that are provided by PSPs.

To import PSP Server (Root) certificates for token exchange:

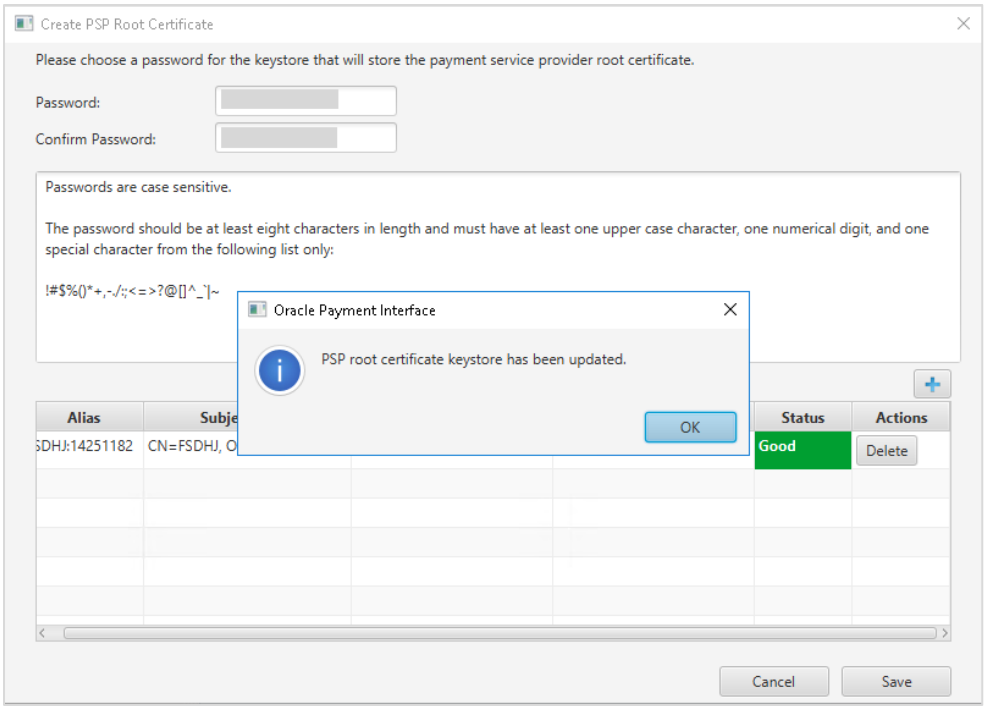
1. Log in to the OPI Configuration tool.
2. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Server (Root) Certificate**.



3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** ( ) icon or you can also drag and drop the .cer or.crt.



4. Click **Save**.

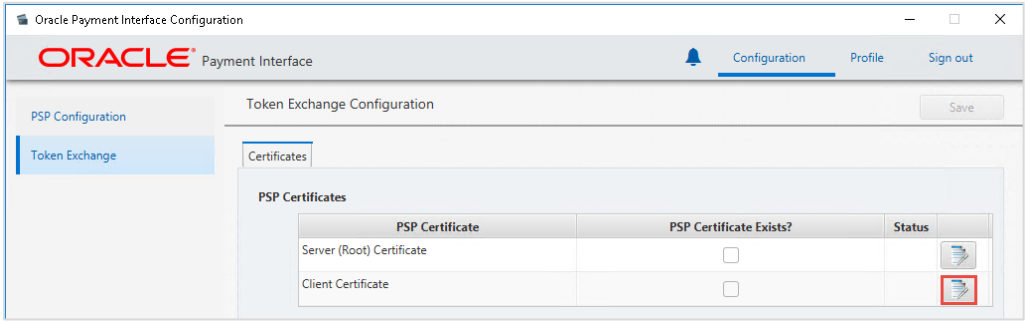


5. Click **OK**.

To import PSP Client certificates for token exchange:

You can import client certificates for Token exchange on behalf of the customer that are provided by PSPs.

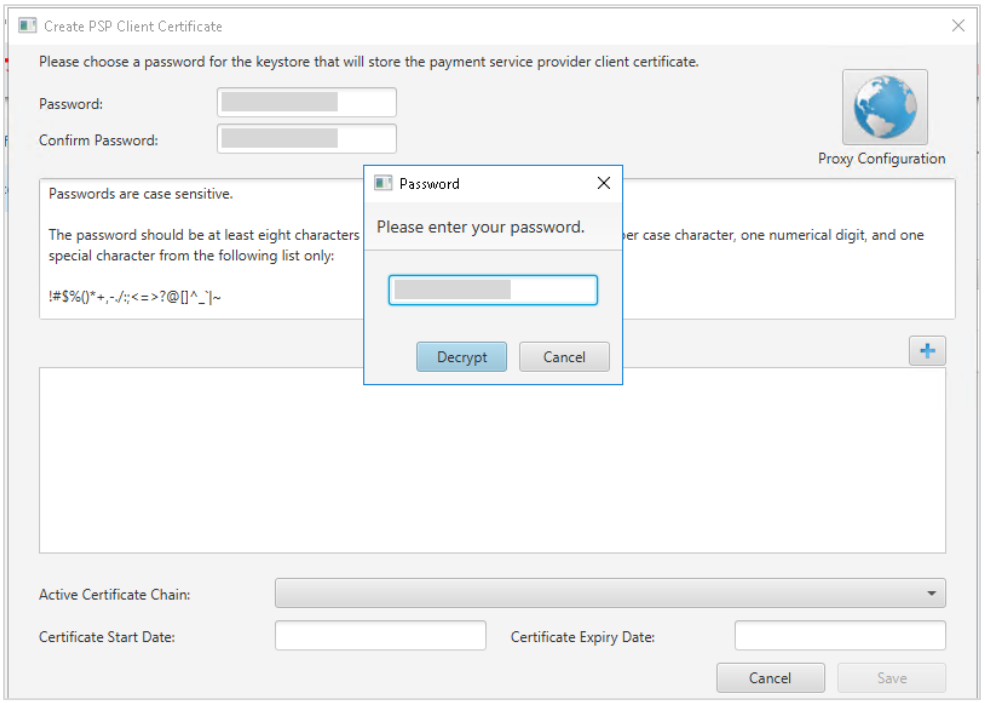
1. Log in to the OPI Configuration tool.
2. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Client Certificate**.



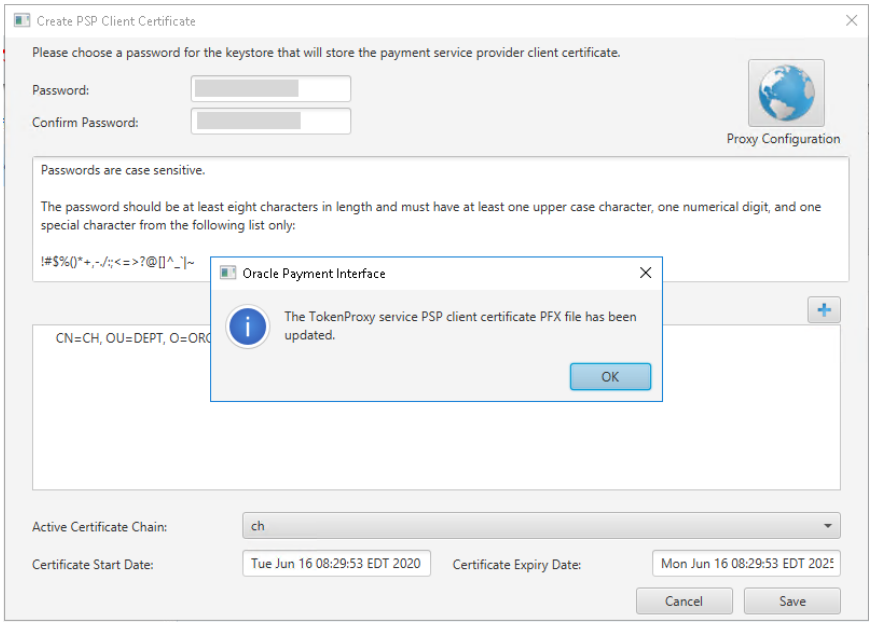
3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** ( ) icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration.

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.



4. Click **Save.**



5. Click **OK**.

> **NOTE:**
>
> PSP support personnel should run testing with the customer to validate whether the functionality is still working after the certificates are updated.

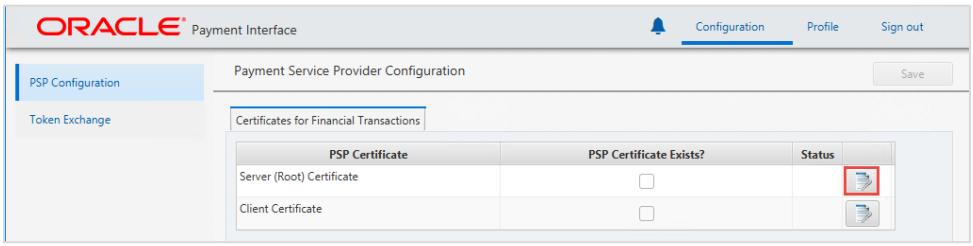
Import Certificates for Financial Transactions

PSP Certificates for Financial Transaction

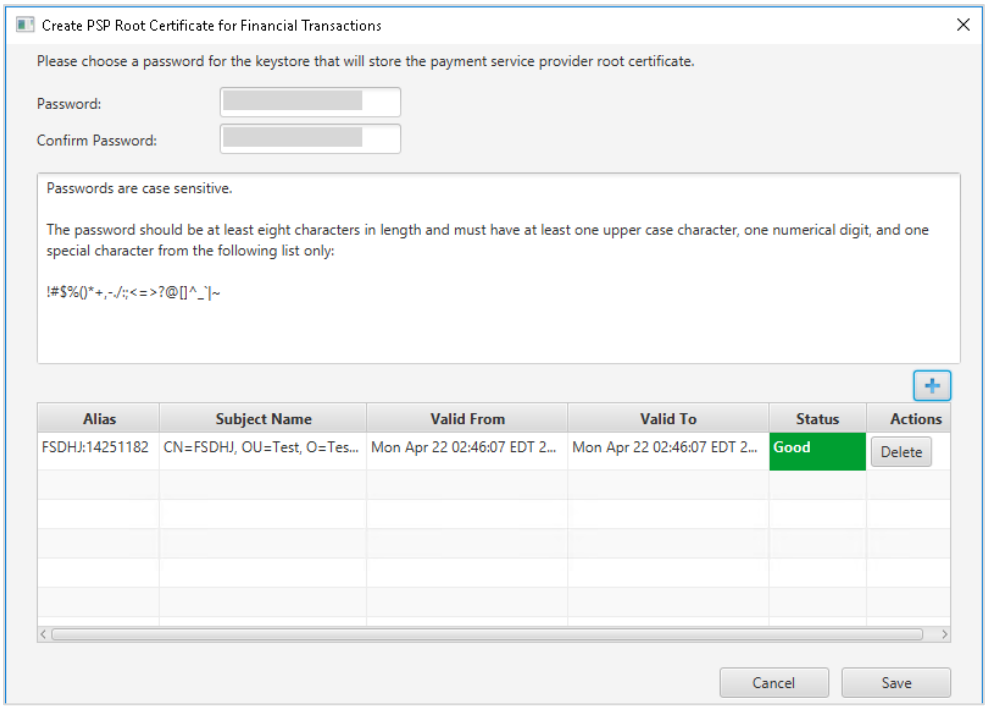
You can import server (root) certificates for financial transactions on behalf of the customer that are provided by PSPs. These certificates are required only if the PSP is requesting two way certificate authentication for financial transactions, which is not common.

To import PSP Server (Root) certificates for financial transactions:

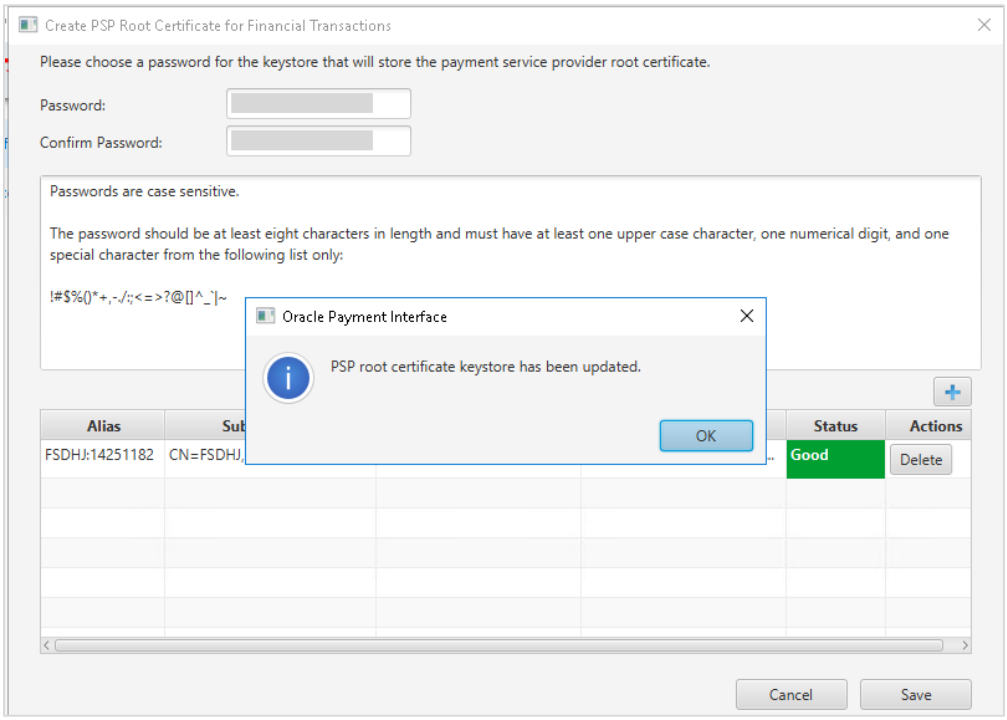
1. Log in to the OPI Configuration tool.
2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Server (Root) Certificate**.



3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** ( ) icon or you can also drag and drop the .cer or.crt.



4. Click **Save**.



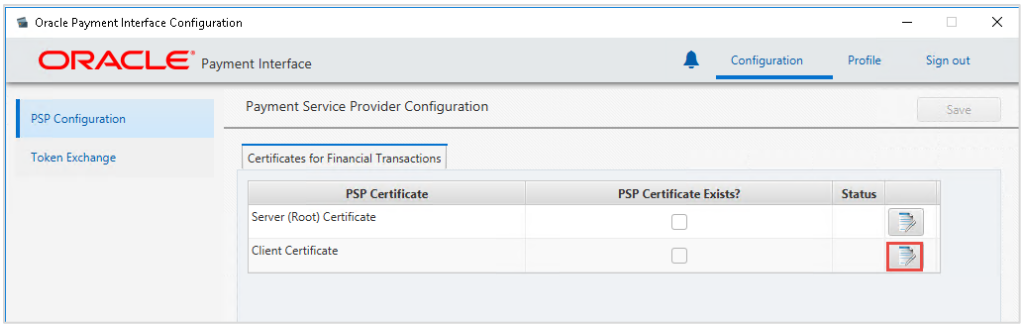
5. Click **OK**.

To import PSP Client certificates for financial transactions:

You can import client certificates for financial transactions.

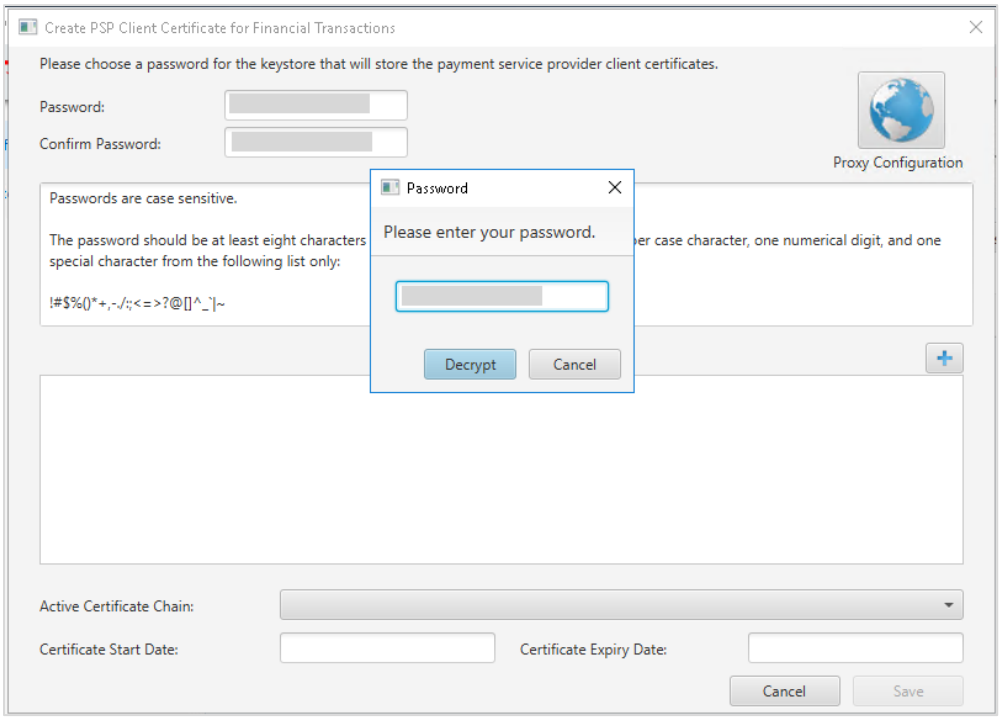
1. Log in to the OPI Configuration tool.

2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Client Certificate**.

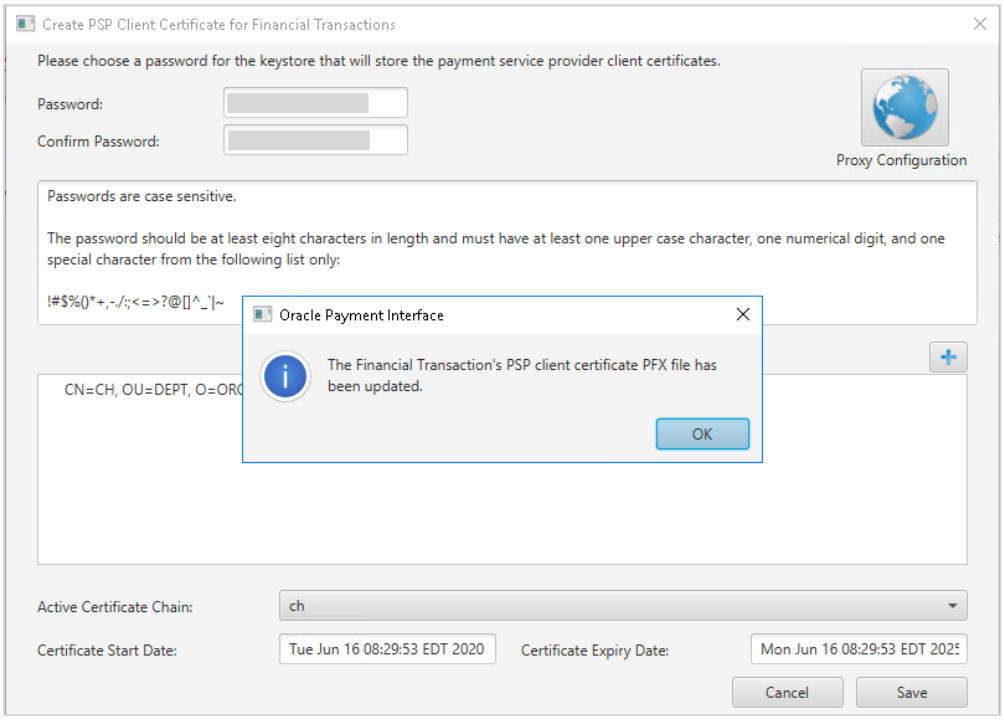


3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** ( ) icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration.

> **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.



4. Click **Save.**



5. Click **OK**.

> **NOTE:**
>
> PSP support personnel should run testing with the customer to validate whether the functionality is still working after the certificates are updated.

Update Passwords for Certificates and Keystores

To update passwords for certificates and keystores:

1. Log in to the OPI Configuration tool.
2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Server (Root) Certificate/Client Certificate**.

Or

3. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Server (Root) Certificate/Client Certificate**.
4. Update the password for the keystore of your choice meeting the requirements, and browse to the location of the certificate you want to import from **add** ( ) icon or you can also drag and drop the .cer or.crt.
5. Click **Save** to update the password.

> **NOTE:**
>
> PSP support personnel should run testing with the customer to validate whether the functionality is still working after the certificates are updated.

View Notification icon and resolve Certificate expiry issues

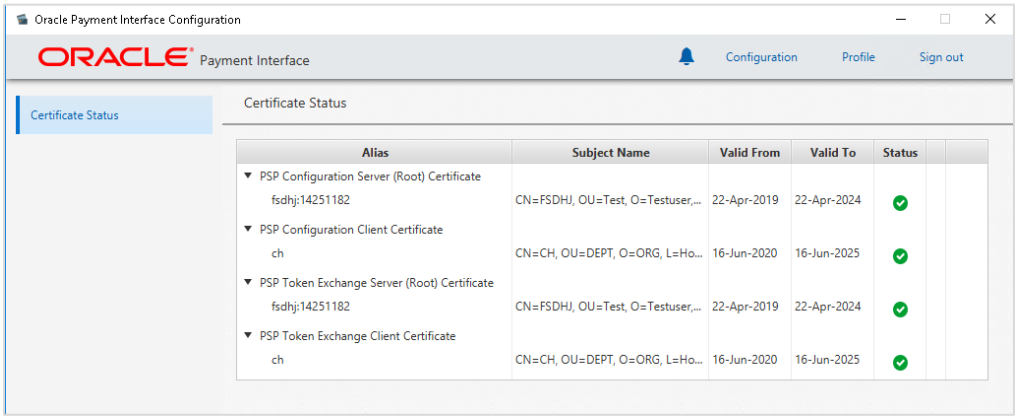
You can view Certificate Expiry related notifications that are available in the OPI Configuration tool using a notification icon. Click this icon to view all the certificate expiry related notifications and this icon will turn to red color if there are any expired certificates or about to expire certificates and the user attention is required to update these certificates.

Following is the expiration status of all the certificates:

- - Certificates that are in ‘Good’ status.
- - Certificates that are in ‘About to expire’ status and needs to updated before they expire.
- - Certificates that are in ‘Expired’ status and needs to updated with new certificates.

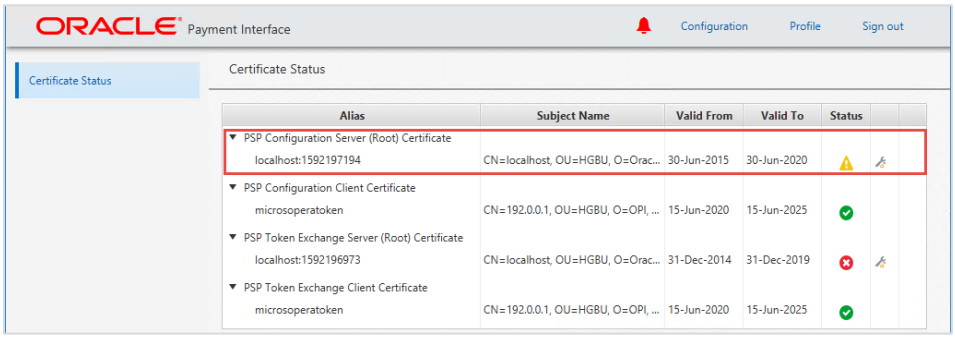
To view certificates in ‘Good’ status:

- Log in to the OPI Configuration tool.
- On the home page, click notification icon to view the ‘Good’ certificate status:

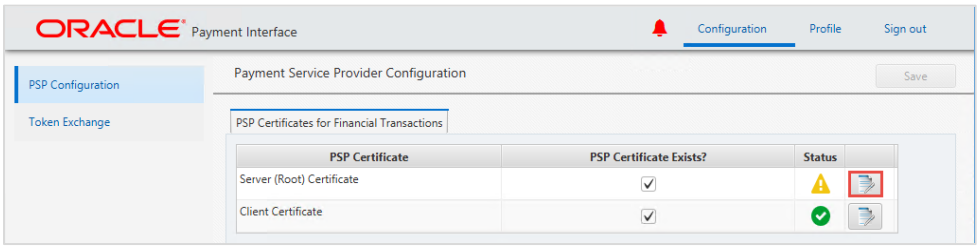


To view and update certificates in 'About to expire' status:

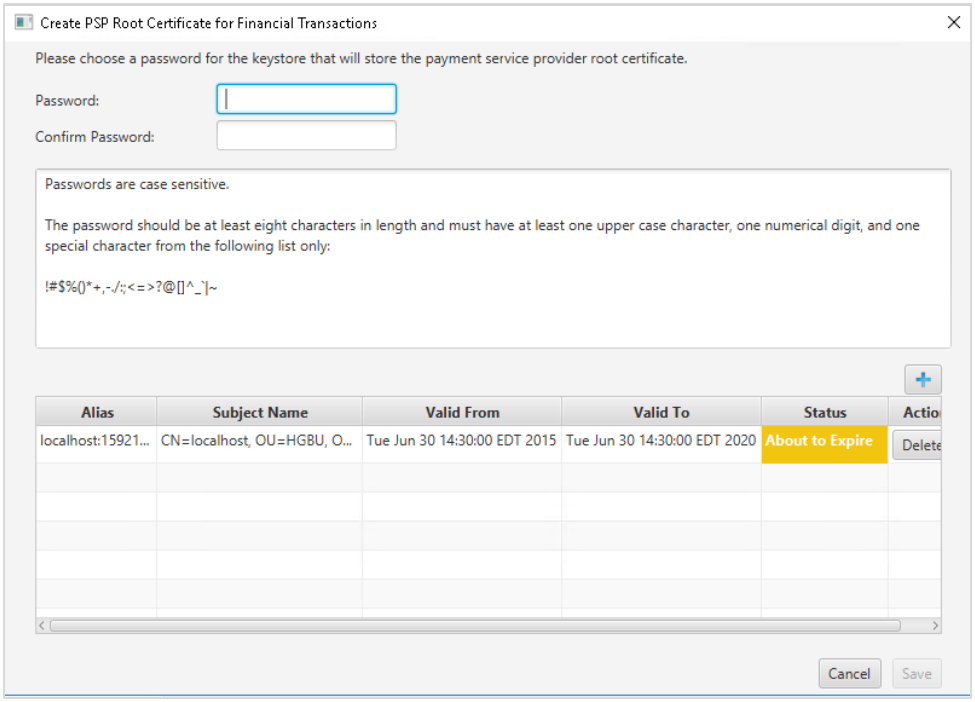
1. Log in to the OPI Configuration tool.
2. On the home page, click notification icon to view the 'About to expire' certificate status:



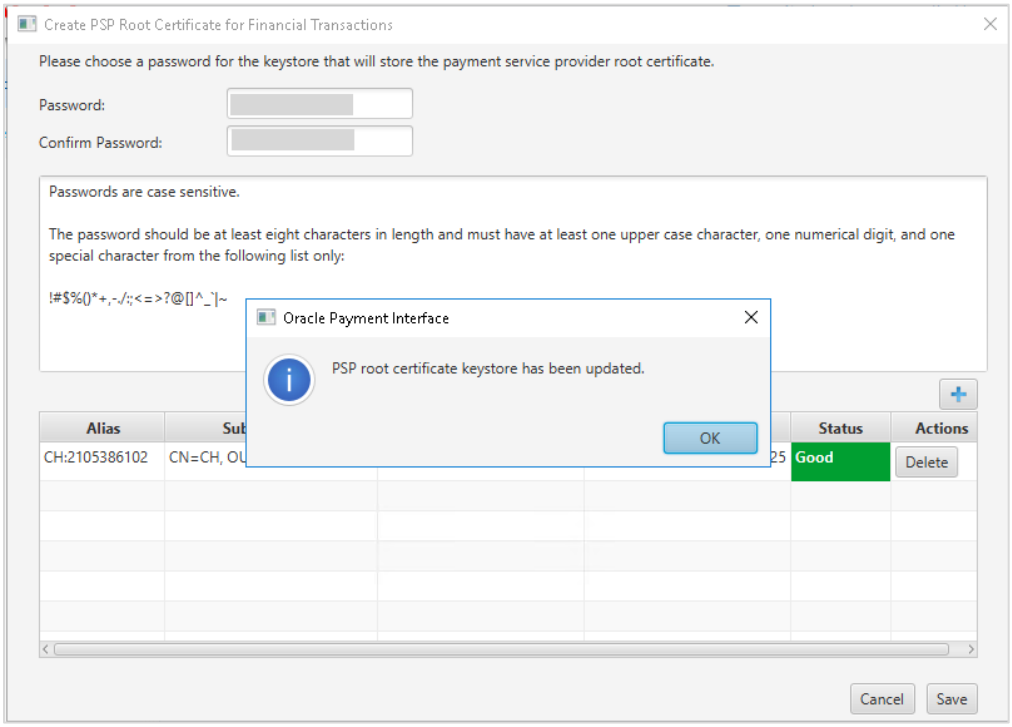
3. Click to delete and update the certificate details.



4. Edit the Certificate details.



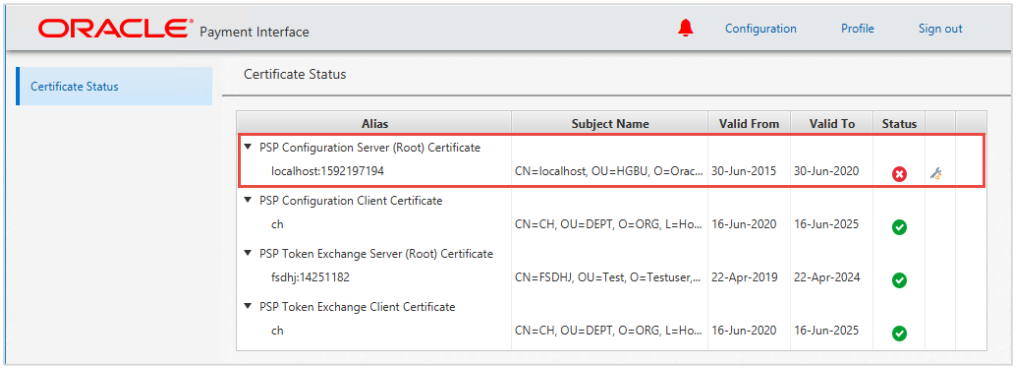
5. Click **Delete** to delete the 'About to Expire' certificate.
6. Enter the password for the keystore and browse to the location of the certificate want to import from **add** ( ) icon or you can also drag and drop the .cer or.crt.
7. Click **Save**.



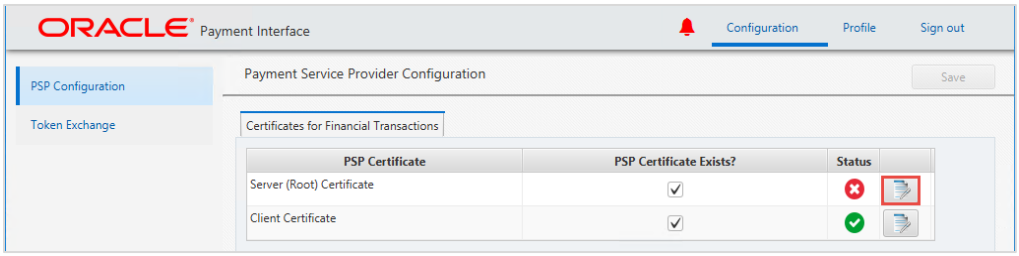
8. Click **OK**.

To view and update certificates in 'Expired' status:

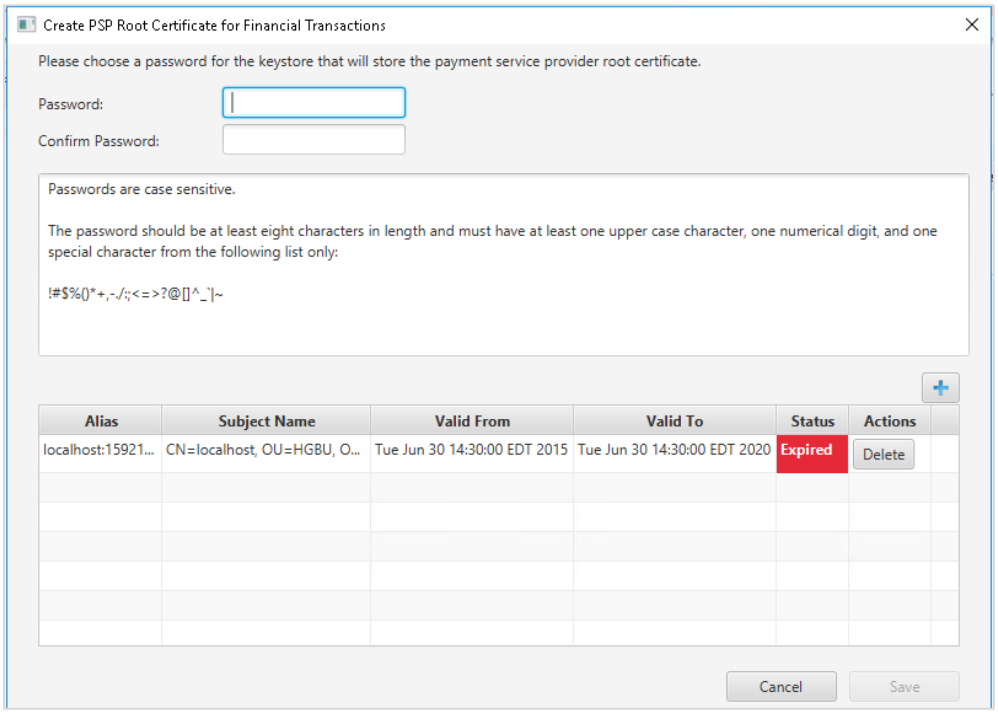
1. Log in to the OPI Configuration tool.
2. On the home page, click notification icon to view the 'Expired' certificate status:



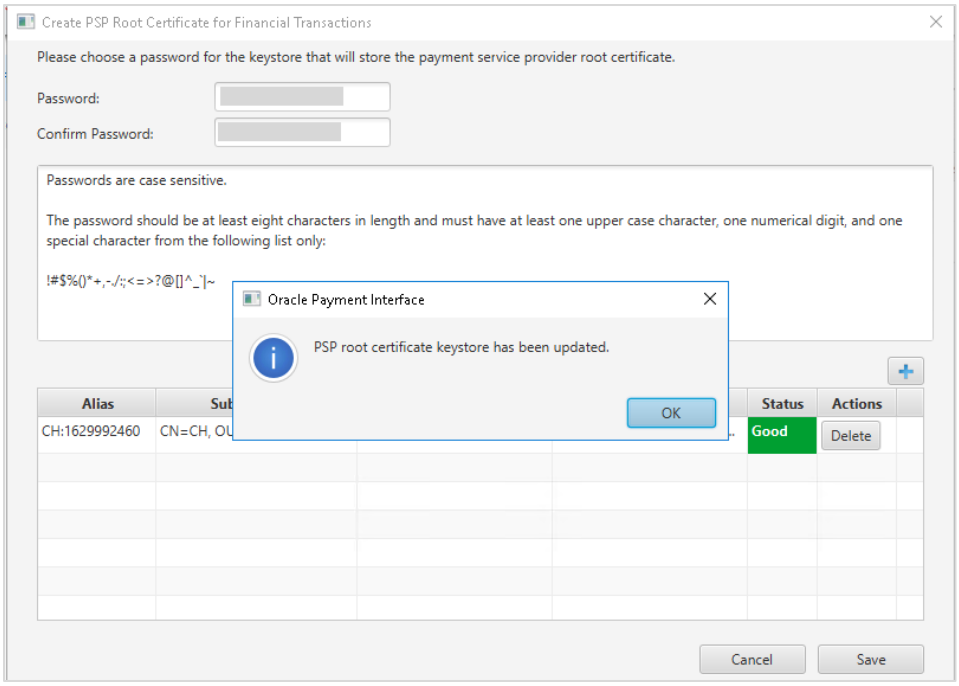
3. Click to delete and update the certificate details.



4. Edit the Certificate details.



5. Click **Delete** to delete the 'Expired' certificate.
6. Enter the password for the keystore and browse to the location of the certificate want to import from **add** ( ) icon or you can also drag and drop the .cer or.crt.
7. Click **Save**.



8. Click **OK**.

> **NOTE:**
>
> PSP support personnel should run testing with the customer to validate whether the functionality is still working after the certificates are updated.

Editing Your User Profile

You can change your **First name**, **Last name**, and **Password**, if required. The Username cannot be edited once it has been created.

First Name and Last Name

You can edit your First Name and Last Name after logging in.

1. Select the **Profile** tab.
2. On the **User Information** page, update the values as required, and then click **Save**.

Changing Your Password

1. On the **Profile** tab, select **Change Password**, enter the **Current password**, and then enter and confirm the **New Password**.
2. Click **Change** when finished.

NOTE:

After changing the password, you should immediately sign out of the configurator and then logon again using the new password. Failure to sign out after changing the password could cause the account to be locked out.