

Oracle Hospitality Payment Interface PSP Certificate Management User Configuration Guide



Release 20.4
F95680-01
June 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2010, 2024, 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

Contents	iii
<hr/>	
Preface	iv
<hr/>	
1 PSP Certificate Management	1-1
<hr/>	
PSP Certificate Management Users First Login	1-1
Import Certificates for Token Exchange	1-3
Import Certificates for Financial Transactions	1-6
Update Passwords for Certificates and Keystores	1-9
View Notification icon and resolve Certificate expiry issues	1-10
Editing Your User Profile	1-14

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
June 2024	<ul style="list-style-type: none">• Initial Publication

1

PSP Certificate Management

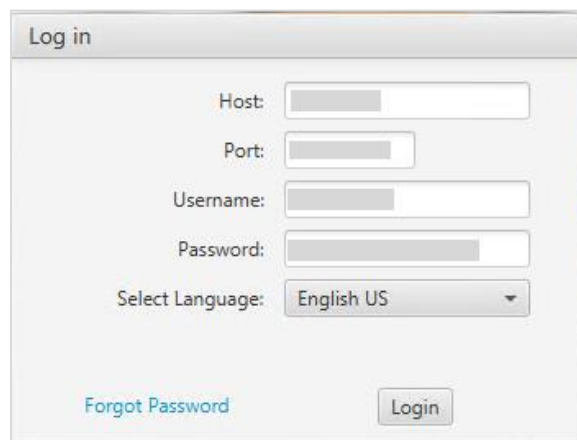
PSP Certificate Management user allows PSP support personnel to update the certificates on behalf of the customer. They have access only to Certificate Management in the OPI Configuration tool and can update only PSP certificates that are provided by PSP.

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

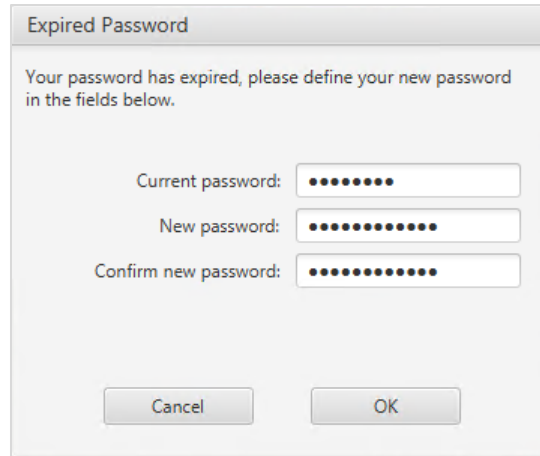
1. Double click **OraclePaymentInterface\v20.4\Config\LaunchConfigurator.bat**.
2. Log in to the OPI Configuration tool by providing the PSP Certificate Management user account **Username** and **Password**.



The screenshot shows a 'Log in' dialog box with the following fields and controls:

- Host:
- Port:
- Username:
- Password:
- Select Language:
- Forgot Password (link)
- Login (button)

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**.



Expired Password

Your password has expired, please define your new password in the fields below.

Current password: [password field]

New password: [password field]

Confirm new password: [password field]

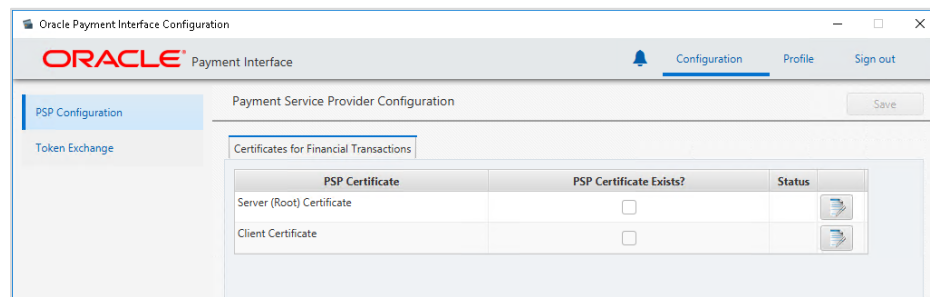
Cancel OK

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.

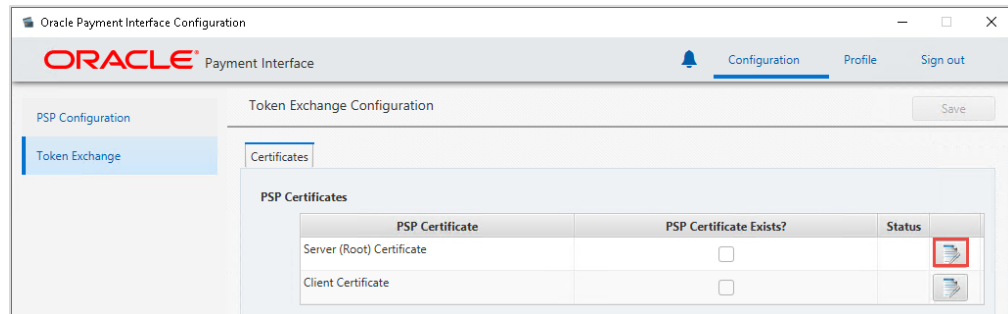
For more information on how to create a new user or change a forgotten password, see [OPI Installation and Reference Guide](#).

Import Certificates for Token Exchange

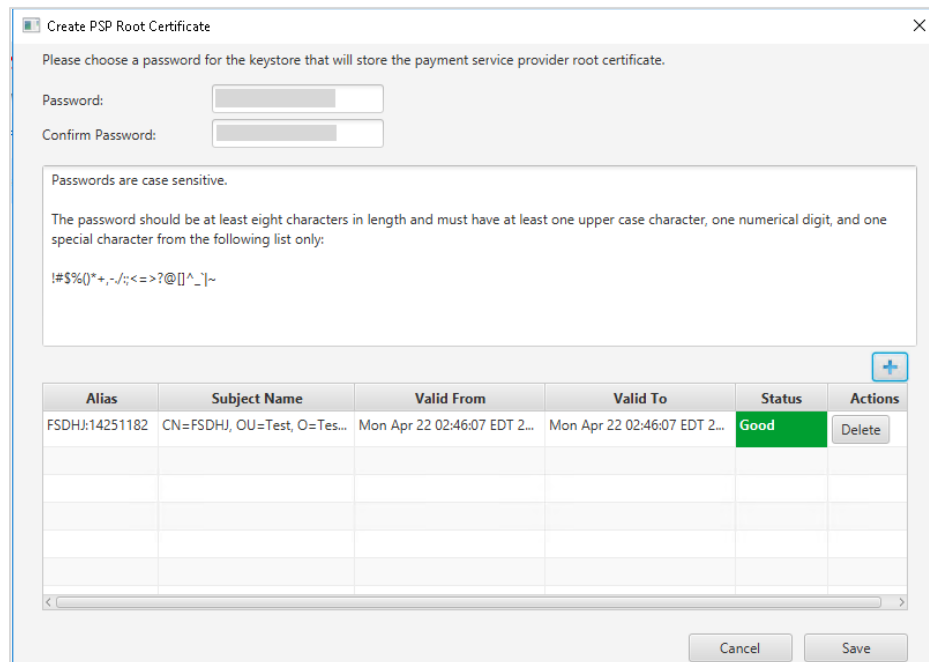
You can import certificates for token exchange on behalf of the customer that are provided by PSPs.

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

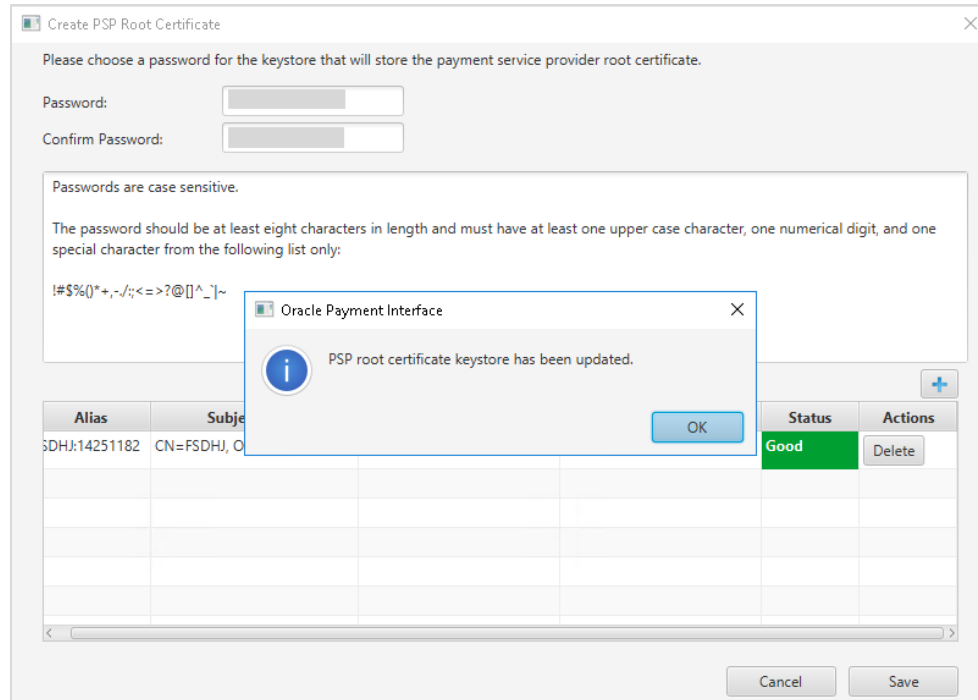
1. Log in to the OPI Configuration tool.
2. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Server (Root) Certificate**.



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**.

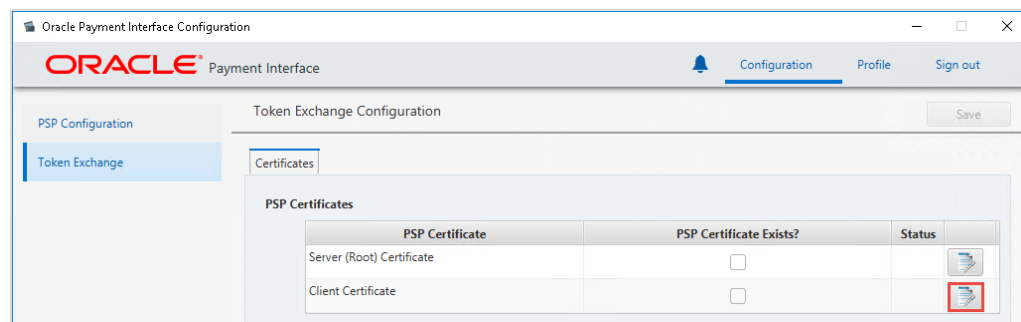


5. Click **OK**.

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.

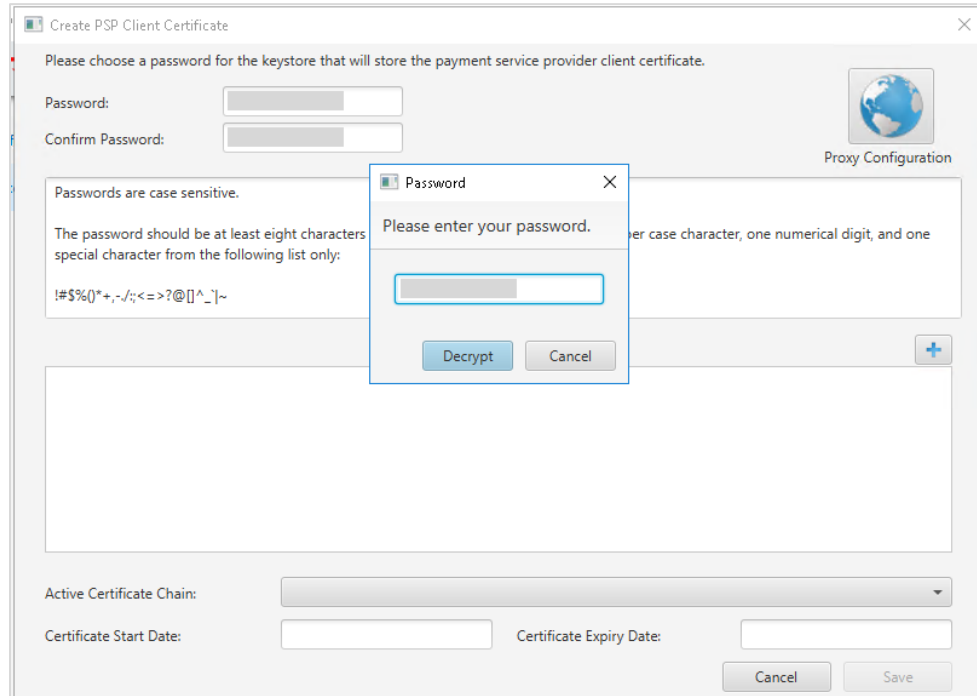
1. Log in to the OPI Configuration tool.
2. Select **Token Exchange** tab, click **Certificates** subtab and then edit the **Client Certificate**.



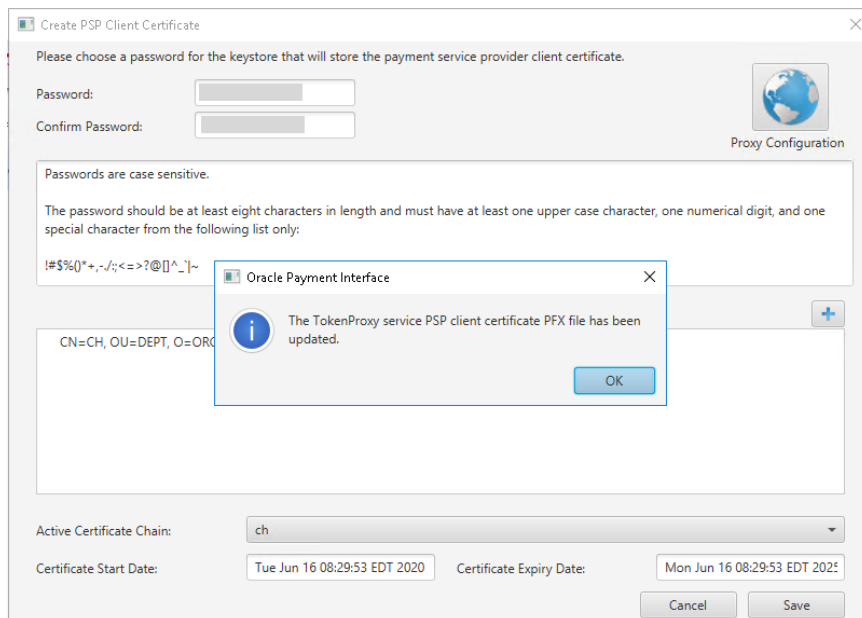
3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add (+)** icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below 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.

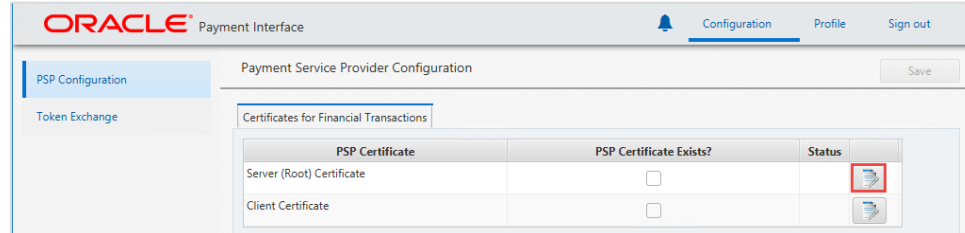
Import Certificates for Financial Transactions


PSP Certificates for Financial Transaction

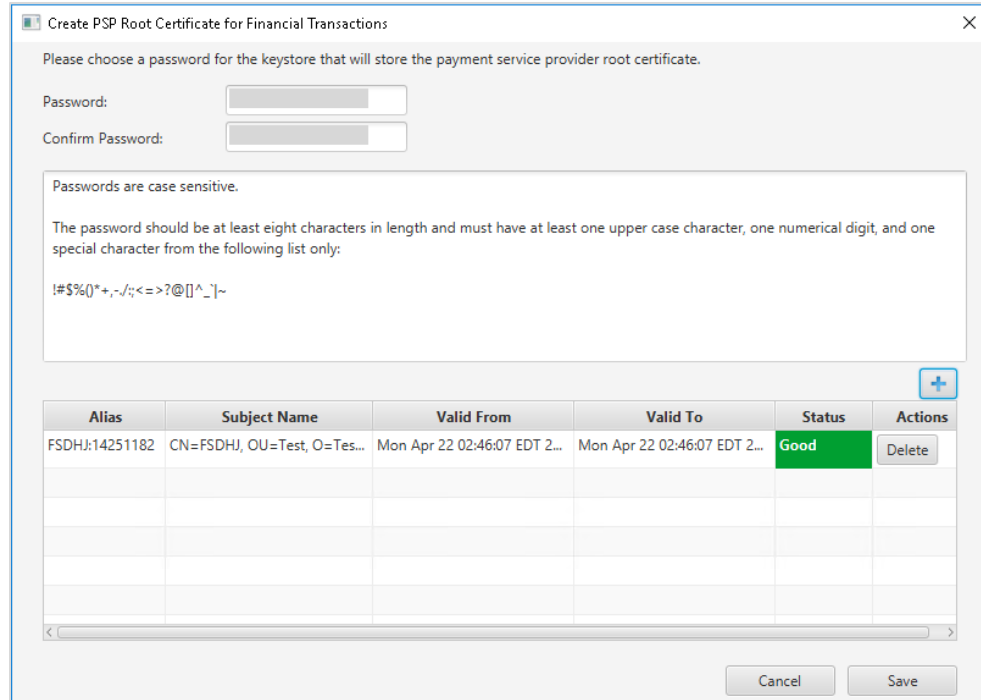
You can import server (root) certificates for financial transactions on behalf of the customer that are provided by PSPs. These certificates are required only if the PSP is requesting two way certificate authentication for financial transactions, which is not common.

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

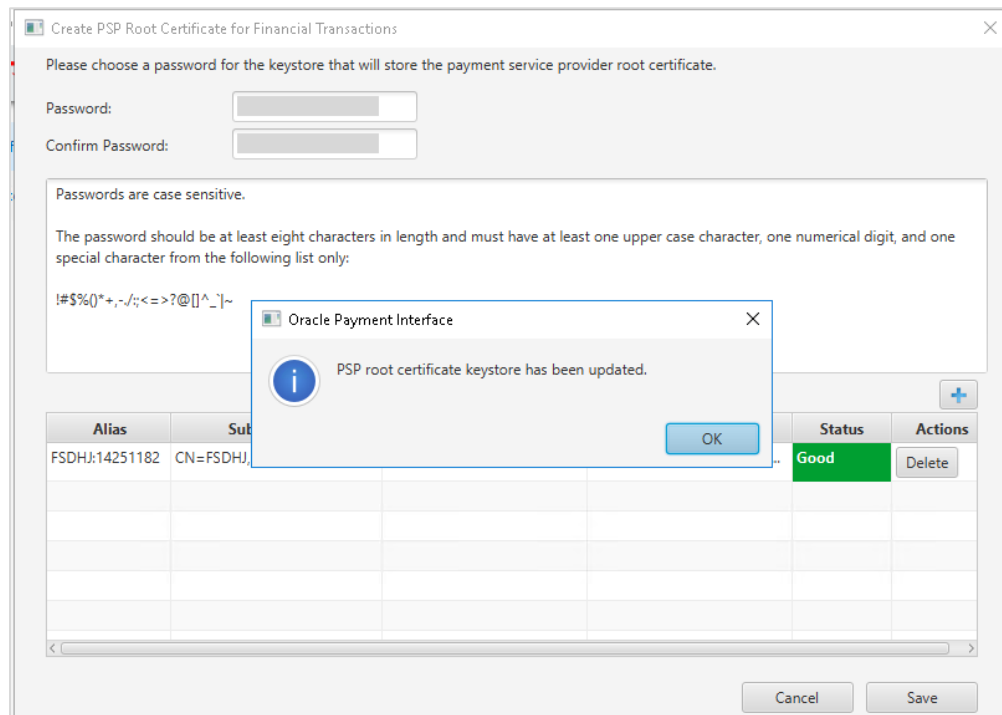
1. Log in to the OPI Configuration tool.
2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Server (Root) Certificate**.



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**.



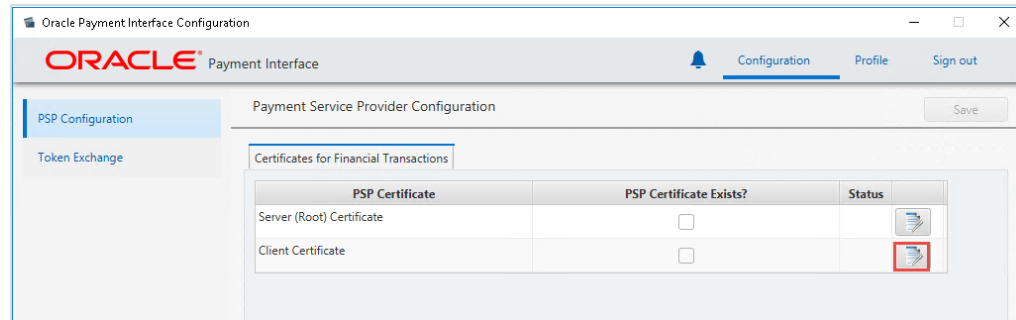
5. Click **OK**.

To import PSP Client certificates for financial transactions:

You can import client certificates for financial transactions.

1. Log in to the OPI Configuration tool.

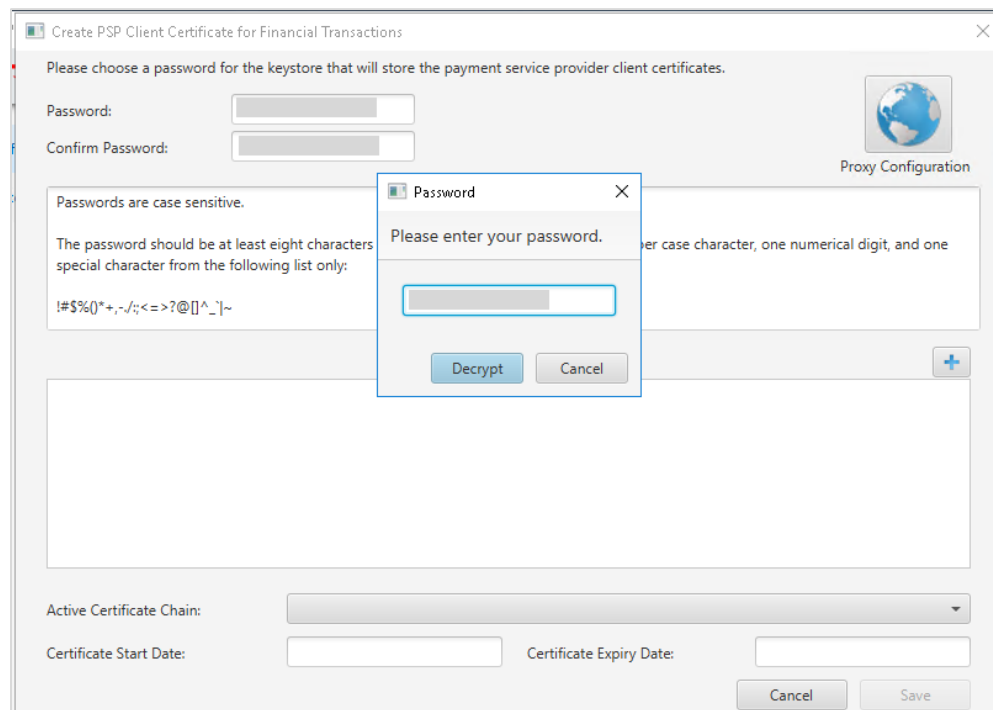
2. Select **PSP Configuration** tab, click **Certificates for Financial Transactions** subtab and then edit the **Client Certificate**.



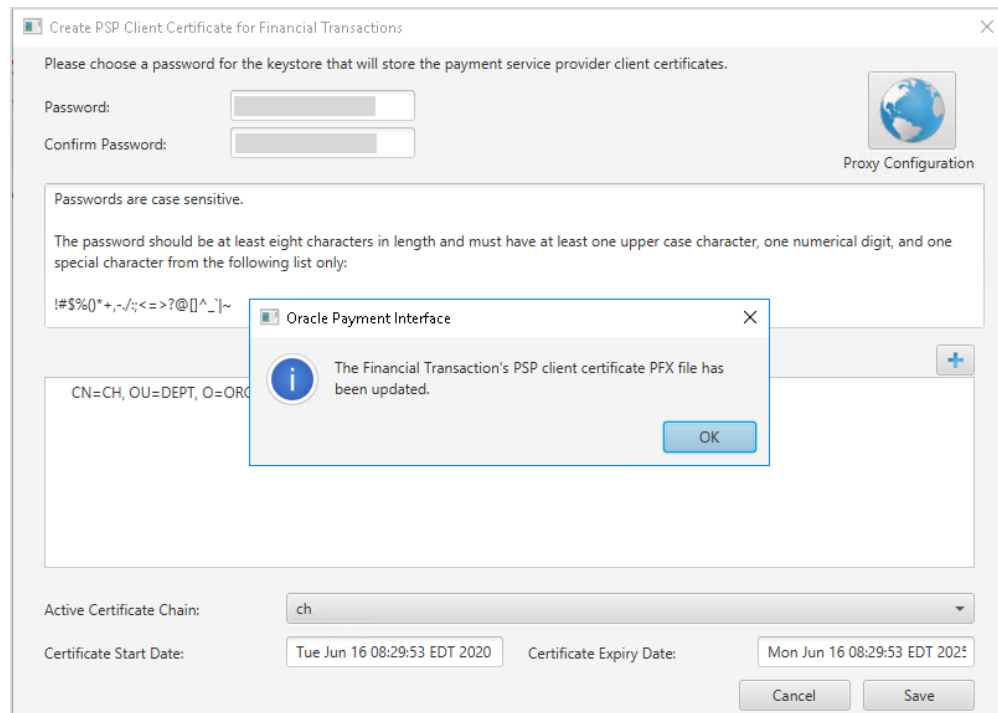
3. Enter the password for the keystore and browse to the location of the certificate you want to import from **add** () icon or you can also drag and drop the .pfx. You will need the password for this .pfx file to decrypt it. The passwords must meet the minimum complexity requirements discussed below 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

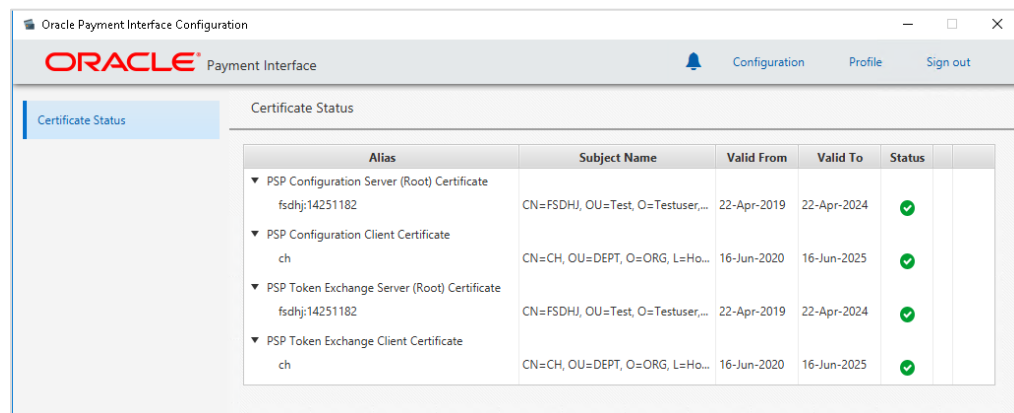
You can view Certificate Expiry related notifications that are available in the OPI Configuration tool using a notification icon . Click this icon to view all the certificate expiry related notifications and this icon will turn to red color  if there are any expired certificates or about to expire certificates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

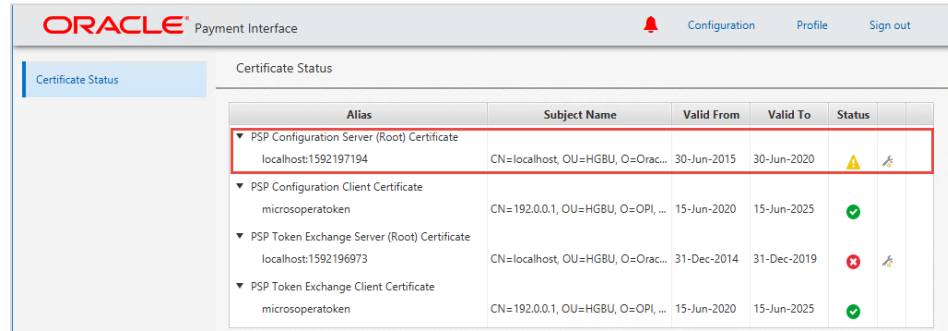
- Log in to the OPI Configuration tool.
- On the home page, click notification icon  to view the 'Good'  certificate status:



Alias	Subject Name	Valid From	Valid To	Status
▼ PSP Configuration Server (Root) Certificate fsdhj:14251182	CN=FSDHJ, OU=Test, O=Testuser,...	22-Apr-2019	22-Apr-2024	
▼ PSP Configuration Client Certificate ch	CN=CH, OU=DEPT, O=ORG, L=Ho...	16-Jun-2020	16-Jun-2025	
▼ PSP Token Exchange Server (Root) Certificate fsdhj:14251182	CN=FSDHJ, OU=Test, O=Testuser,...	22-Apr-2019	22-Apr-2024	
▼ PSP Token Exchange Client Certificate ch	CN=CH, OU=DEPT, O=ORG, L=Ho...	16-Jun-2020	16-Jun-2025	


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

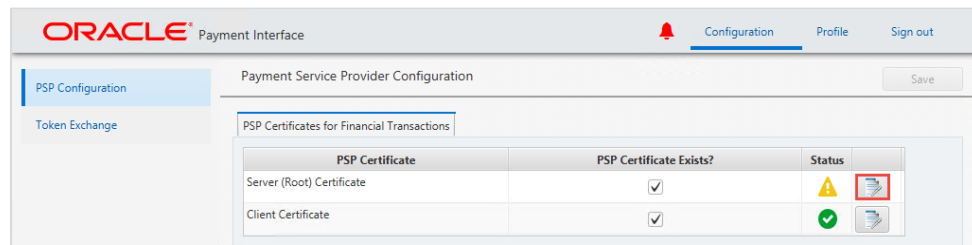
1. Log in to the OPI Configuration tool.
2. On the home page, click notification icon  to view the 'About to expire' certificate status: 



The screenshot shows the 'Certificate Status' page in the Oracle Payment Interface. A table lists certificates with columns for Alias, Subject Name, Valid From, Valid To, Status, and an action icon. The first row, 'PSP Configuration Server (Root) Certificate', is highlighted with a red border and has a yellow warning triangle in the Status column.

Alias	Subject Name	Valid From	Valid To	Status	
localhost:1592197194	CN=localhost, OU=HGBU, O=Orac...	30-Jun-2015	30-Jun-2020		
microoperatoken	CN=192.0.0.1, OU=HGBU, O=OPI, ...	15-Jun-2020	15-Jun-2025		
localhost:1592196973	CN=localhost, OU=HGBU, O=Orac...	31-Dec-2014	31-Dec-2019		
microoperatoken	CN=192.0.0.1, OU=HGBU, O=OPI, ...	15-Jun-2020	15-Jun-2025		

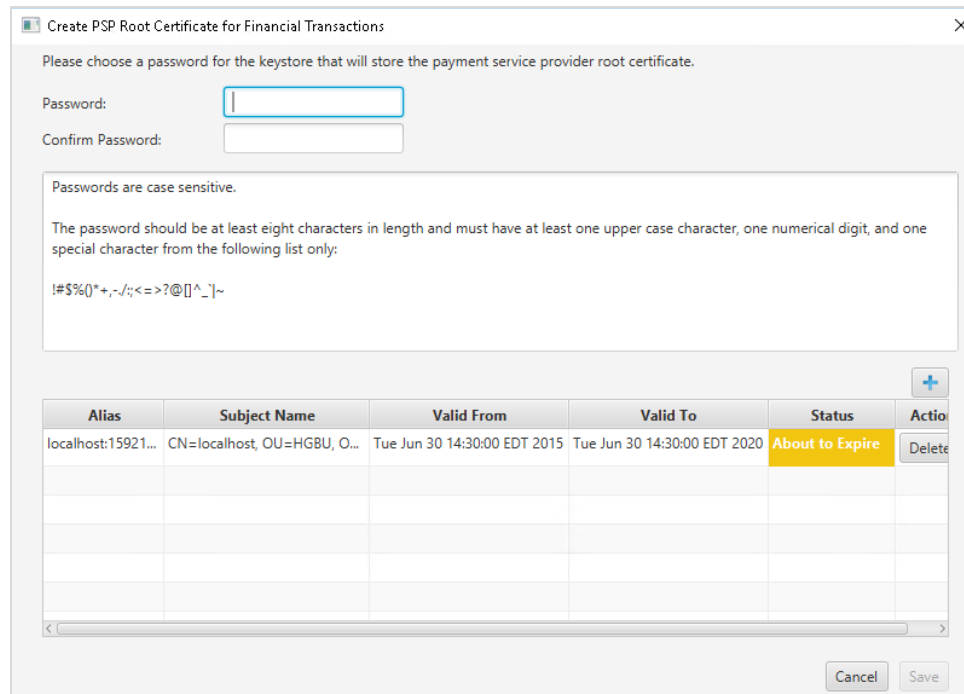
3. Click  to delete and update the certificate details.



The screenshot shows the 'Payment Service Provider Configuration' page. A table titled 'PSP Certificates for Financial Transactions' has columns for PSP Certificate, PSP Certificate Exists?, and Status. The 'Server (Root) Certificate' row has a yellow warning triangle and a pencil icon in the Status column.

PSP Certificate	PSP Certificate Exists?	Status
Server (Root) Certificate	<input checked="" type="checkbox"/>	
Client Certificate	<input checked="" type="checkbox"/>	

4. Edit the Certificate details.



The dialog box prompts for a password for the keystore. It includes a password field, a confirm password field, and a list of allowed characters. Below the text is a table showing the certificate details.

Please choose a password for the keystore that will store the payment service provider root certificate.

Password:

Confirm Password:

Passwords are case sensitive.

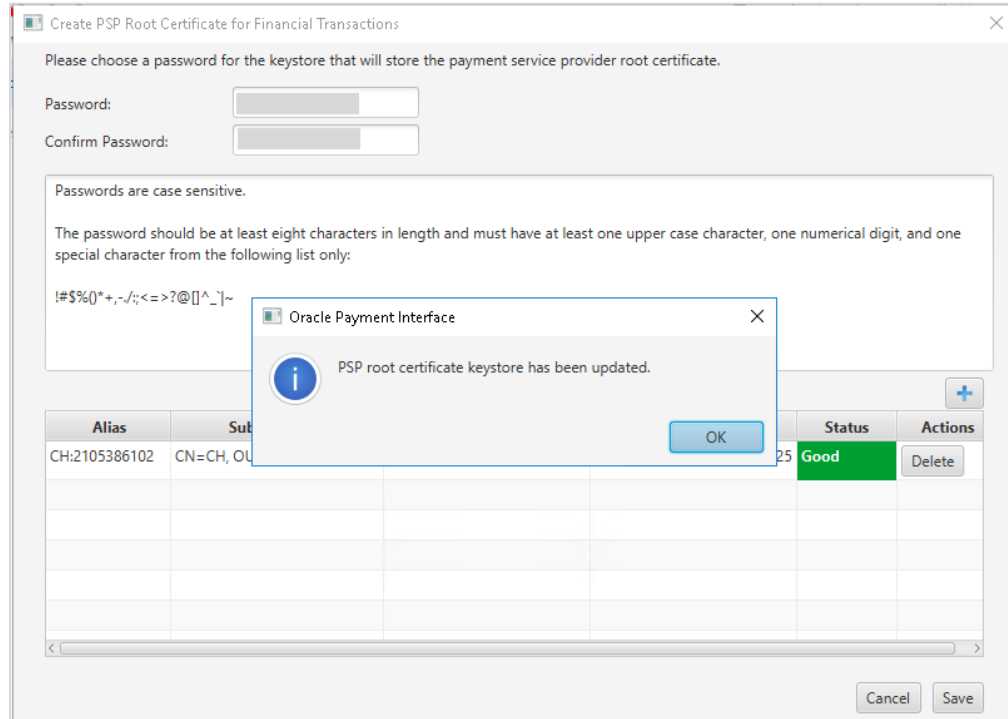
The password should be at least eight characters in length and must have at least one upper case character, one numerical digit, and one special character from the following list only:

!#\$%()*+,-./:;<=>?@[]^_`~

Alias	Subject Name	Valid From	Valid To	Status	Action
localhost:15921...	CN=localhost, OU=HGBU, O...	Tue Jun 30 14:30:00 EDT 2015	Tue Jun 30 14:30:00 EDT 2020	About to Expire	Delete

Buttons: Cancel, Save

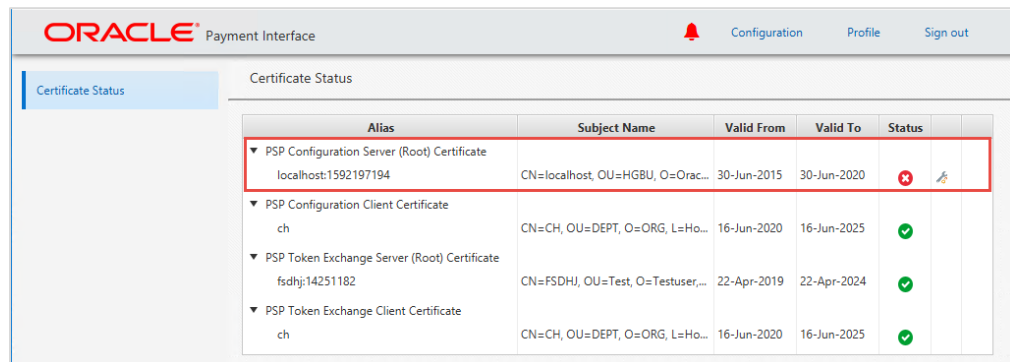
5. Click **Delete** to delete the 'About to Expire' certificate.
6. Enter the password for the keystore and browse to the location of the certificate want to import from **add** (+) icon or you can also drag and drop the .cer or.crt.
7. Click **Save**.




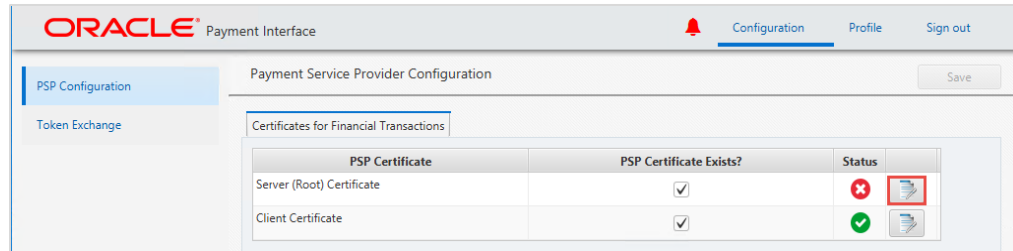
8. Click **OK**.

To view and update certificates in 'Expired' status:

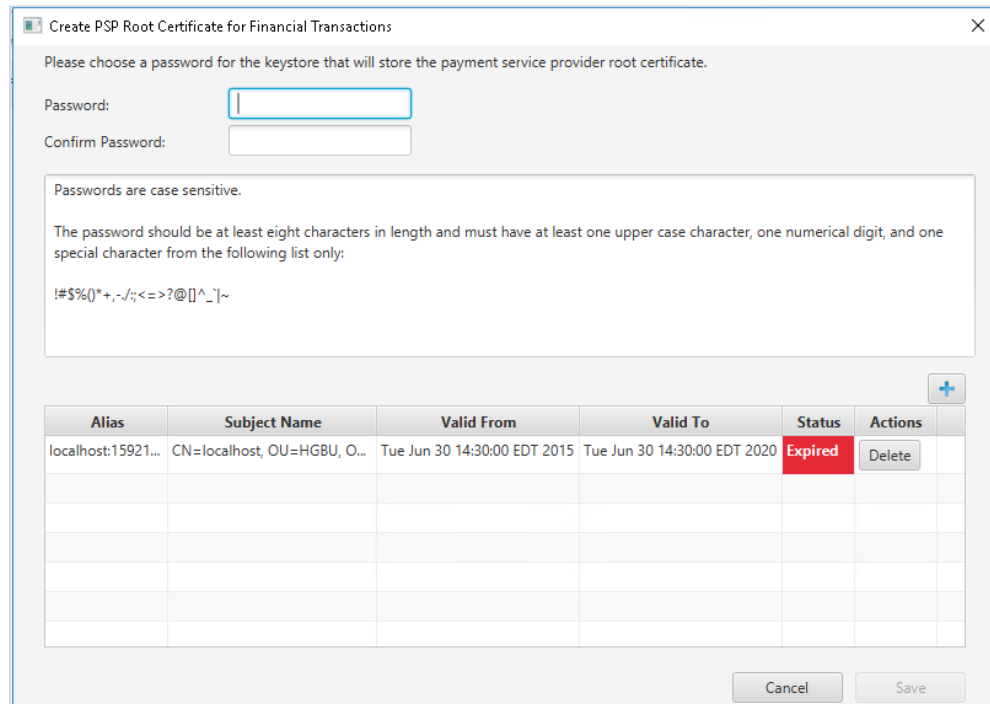
1. Log in to the OPI Configuration tool.
2. On the home page, click notification icon  to view the 'Expired'  certificate status:



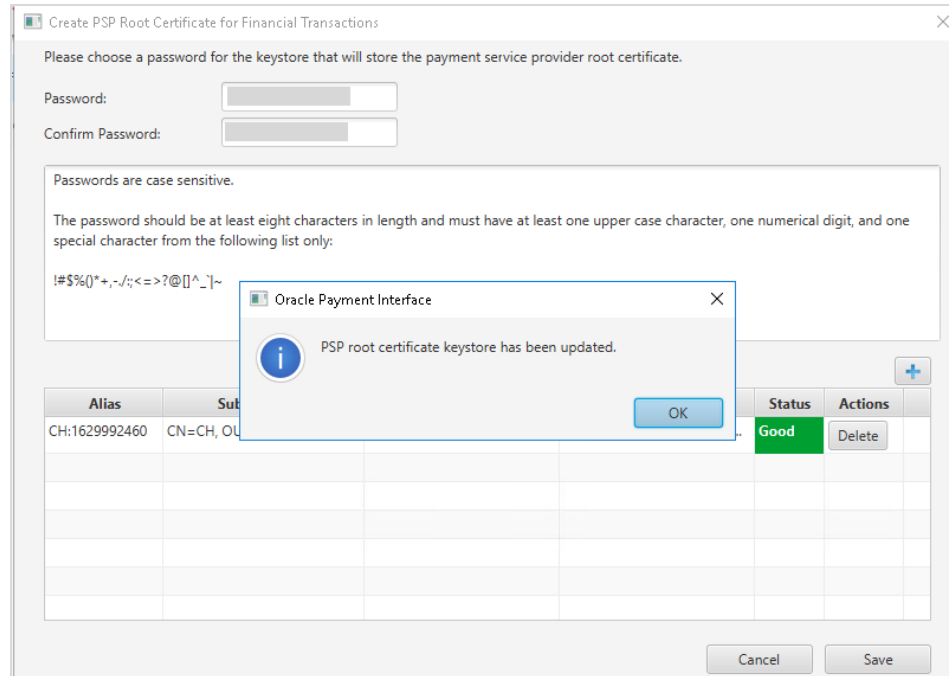
3. Click  to delete and update the certificate details.



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.