Oracle Hospitality Self-Hosted Token Proxy Service

Installation and Configuration Guide

Release 19.2
F21088–05
January 2024

Oracle Hospitality Self-Hosted Token Proxy Service Installation and Configuration Guide, Release 19.2

F21088–05

Contents

5 Configuration Web Portal

6 Upgrading the TPS

7 Certificates

8 OPIConfigX.exe

9 Certificates Request using Cert Manager

10 OPERA Configuration

11 Token Proxy Service Maintenance

Preface

The Token Proxy Service is designed to provide a token exchange proxy service for hosted applications. This document describes how to install the Oracle Hospitality 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 the Self-Hosted Token Proxy Service.

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/.

Oracle WebLogic product documentation is available on the Oracle Help Center at https://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

Table 1   Revision History

Date	Description of Change
July 2019	Initial Publication
March 2020	Updated TPS DemoIdentity Upgrade details in the Chapter 6.
July 2020	Revised content across the entire document

Table 1 (Cont.) Revision History

Date	Description of Change
March 2021	- Updated content in Tomcat HTTPS Listener section in the Chapter 9. - Added screens in WebLogic and Tomcat - Certificate Configuration Wizard sections in the Chapter 9.
March 2023	Updated content to confirm support of Oracle 19c Database.
June 2023	Updated the Customer Support section with the new support portal name and URL
January 2024	Updated content in the Certificates Chapter 7.

1 Overview of Token Proxy Service

The Token Proxy Service is designed to provide a token exchange proxy service for hosted applications. It is a proxy interface that works with your application to communicate with payment service providers (PSP), on whom it relies to provide the actual token functionality. It connects to PSPs via the internet or virtual private network (VPN).

Components

Token Proxy Service has three components:

- Database
- Token Proxy Web Portal
- Token Proxy Service

Installation Prerequisites

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

- 64-bit host
- Windows Server 2008 R2, 2012 R2, 2016, 2019 and Windows 10
- You can install either Oracle or MySQL database:
  - Oracle 12c/19c database server installed and running, and the user understands how to use and configure Oracle DB.
  - MySQL 8.0 database is installed and running.
- WebLogic running to host the Web Portal and the user understands how to use and configure WebLogic 12c. This is not required if you want to deploy TPS using Tomcat.
- 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.

Note:

Token Proxy Service 19.2 has the following options for database and deployment:

- Supports Oracle12c/19c database and allows deployment of Token Proxy WebPortal on WebLogic.
- Supports Oracle12c/19c database and allows deployment of Token Proxy WebPortal on Tomcat.
- Supports MySQL database and allows deployment of Token Proxy WebPortal on Tomcat.

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 less 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. TPS does not override the period of time. This database schema remains valid because the schema expiration date is already defined by existing policies of the environment where the database is installed. By default, Oracle Database defines an expiration date of six months after creation. Be aware that if the schema password expires, and the Token Proxy Service is subsequently unable to read from or write to the database, 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 or Tomcat. It relies on the selected web server 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 via the Token Proxy Web Portal. This Listener must be exposed to the client (for example, OPERA systems).
- The 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. 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 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.

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 or 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.

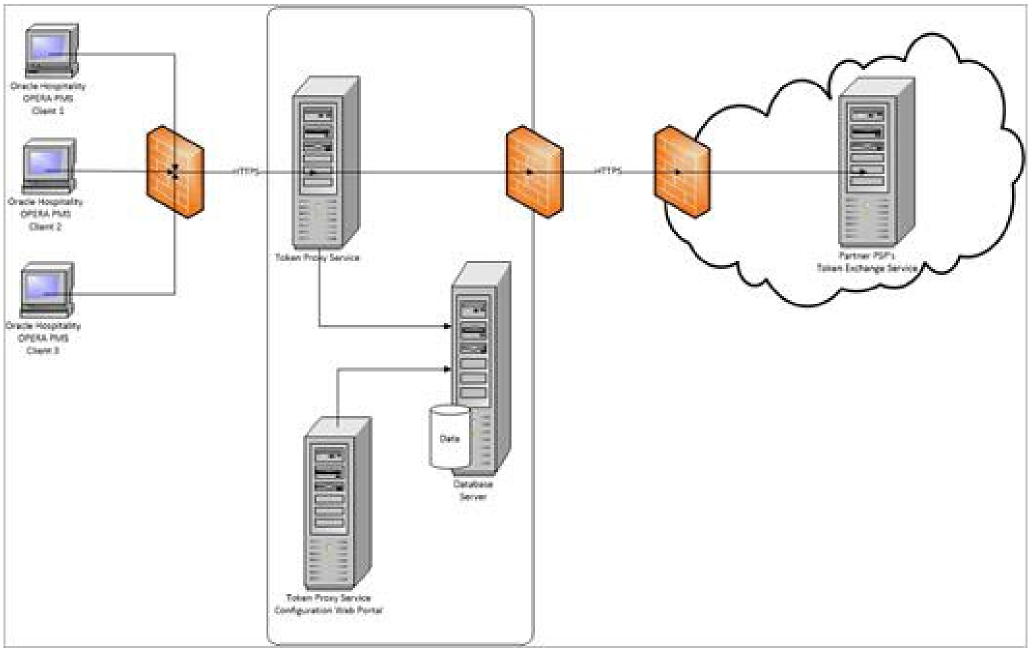
Recommended System Requirements

Table 1-1 Recommended System Requirements

Dedicated or when using Tomcat	When installed on Web Portal/WebLogic Host*
4 x vCPU	4 x vCPU
16 GB RAM	16 GB RAM
100 GB OS	100 GB OS
100 GB Data	100 GB Data

Note:

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


Oracle Hospitality
OPERA PMS
Client 1
Oracle Hospitality
OPERA PMS
Client 2
Oracle Hospitality
OPERA PMS
Client 3
HTTPS
Token Proxy Service
HTTPS
Partner PSP's
Token Exchange Service
Data
Database
Server
Token Proxy Service
Configuration Web Portal

2

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.

The Installation and configuration of WebLogic, MySQL and Oracle 12c/19c is not the focus of this document.

Pre-Installation Checklist

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

You have installed and configured either Oracle or MySQL database before installing Token Proxy Service.

- Oracle Database Information
  - Host, port#, and service name
  - DBA user credentials
- MySQL Database Information
  - Host, port# and database name
  - DBA user credentials

Note:

By default MySQL is installed with configuration that allows the root user to connect only via the localhost address. In the scenario where your MySQL database is not installed on the same host as the other elements of your Token Proxy system, you would need to configure MySQL with an additional users, so the database server will accept the connection via an address other than localhost.

- Connect to the MYSQL Database as the “root” user.
- Run the following queries: USE mysql; SELECT user, host FROM user

  You will see that the "root" user is only related to the "localhost" host
- Once it is verified that the root user only has permission to connect in localhost, run the following query:

  Create user 'root'@'<hostname_or_lan_ip_address>’ identified by “<root password>”;

  Grant all privileges on *.* to 'root'@'<hostname_or_lan_ip_address>’with grant option;

  Where <hostname_or_lan_ip_address> is the hostname or ip address you want to be able to connect to the database via, and "<root_password> is the user the root password.

  For more information refer to the MySQL documentation; https://dev.mysql.com/doc/mysql-installation-excerpt/8.0/en/mysql-installer-workflow-server.html
- If you want to, run the first query again to verify that the root user has the connect permission with server IP.

- WebLogic host and authentication credentials. This is required only when Tomcat is not selected as the web server.
- SMTP host, port, and 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 or IP addresses.

Installing Token Proxy Service

To install the Token Proxy Service, navigate to the TokenProxyInstaller_19.2.0.x.exe file, and then double-click it to begin.

- The installer creates installation logs in C:\TokenProxy\LOGS.
- The installer verifies system compatibility and looks for the MW_HOME environment variable to use when deploying the WebLogic configuration.
- The installer allows you to proceed without the MW_HOME variable, but doing so limits the WebLogic 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. MW_HOME is not needed if you want to deploy Token Proxy Service using Tomcat.

Creating the MW_HOME Variable

> **Note:**
>
> This section is not applicable if you want to deploy Token Proxy Service using Tomcat.

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 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.

3
Token Proxy Service Complete Installation

1. Right-click **TokenProxyInstaller_19.2.0.0.exe** file and select Run as Administrator to perform an installation.

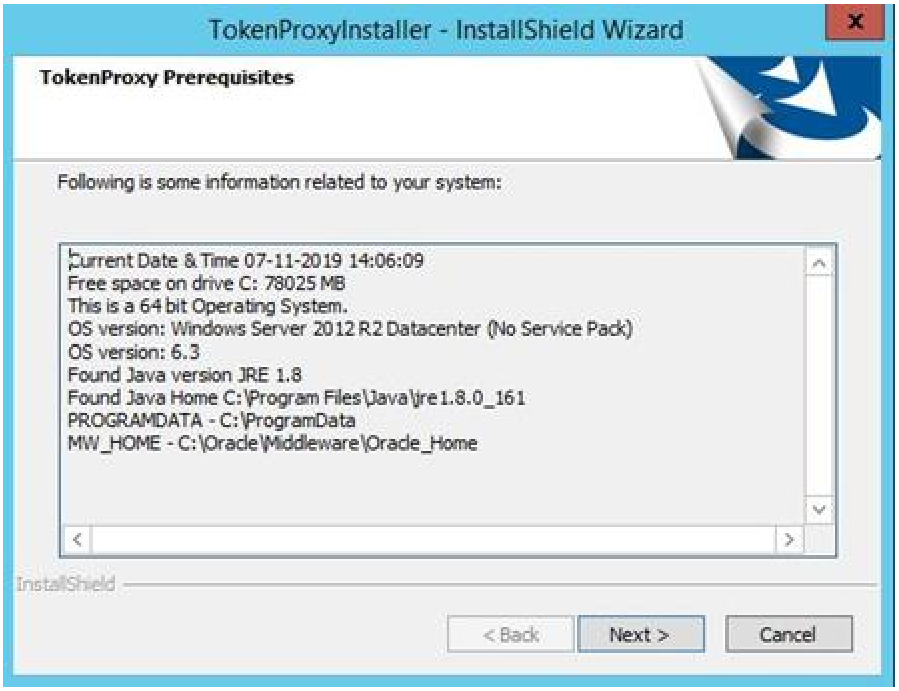
   The installer creates installation logs in C:\TokenProxy\LOGS.

   The installer verifies system compatibility and looks for the MW_HOME environment variable to use when deploying the WebLogic configuration. The installer allows you to proceed without the MW_HOME variable, but doing so limits the WebLogic deployment tasks the installer can complete. The MW_HOME variable is not mandatory because you can install the Token Proxy Service by using Tomcat which allows deployment of Token Proxy WebPortal on Tomcat.

   > **Note:**
   >
   > If the MW_HOME is not found, then the installer will prevent the Token Proxy Portal Auto Deployment on WebLogic server.

2. Click **Next** to proceed with the installation.

   Ensure all the prerequisites for the Token Proxy installation are met.



TokenProxy Prerequisites

Following is some information related to your system:

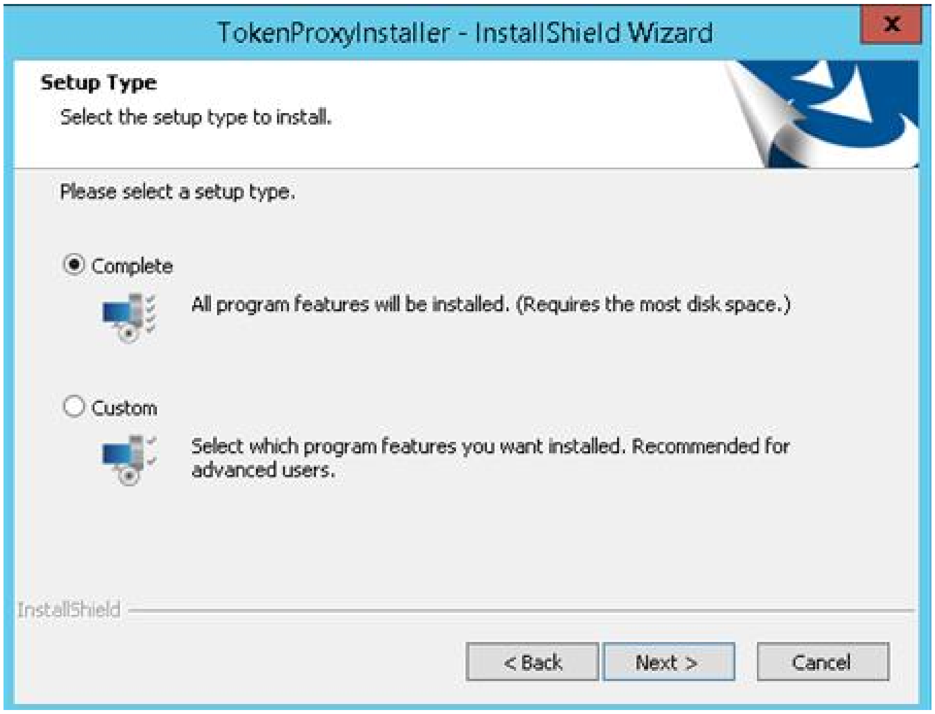
```
Current Date & Time 07-11-2019 14:06:09
Free space on drive C: 78025 MB
This is a 64 bit Operating System.
OS version: Windows Server 2012 R2 Datacenter (No Service Pack)
OS version: 6.3
Found Java version JRE 1.8
Found Java Home C:\Program Files\Java\jre1.8.0_161
PROGRAMDATA - C:\ProgramData
MW_HOME - C:\Oracle\Middleware\Oracle_Home
```

3. Select either the **Complete** or **Custom** installation option:

   - **Complete**: Installs the Database, Token Proxy Web Portal and Token Proxy Service during the installation process.

- **Custom**: Allows installation of only the modules selected. You can also use this mode to install Token Proxy Service only on multiple servers if they want to deploy multiple TPS servers behind a load balancer for high availability. For example, if you want to install the Database on one host and the WebPortal on a different host, you can run the installer on both the machines, with only the relevant components selected for each machine.
  - Database
  - Token Proxy Web Portal
  - Token Proxy Service

  The steps below cover a Complete Installation. If you are installing the Token Proxy Service components to different hosts, see the Token Proxy Service Custom Installation section.



TokenProxyInstaller - InstallShield Wizard

Setup Type

Select the setup type to install.

Please select a setup type.

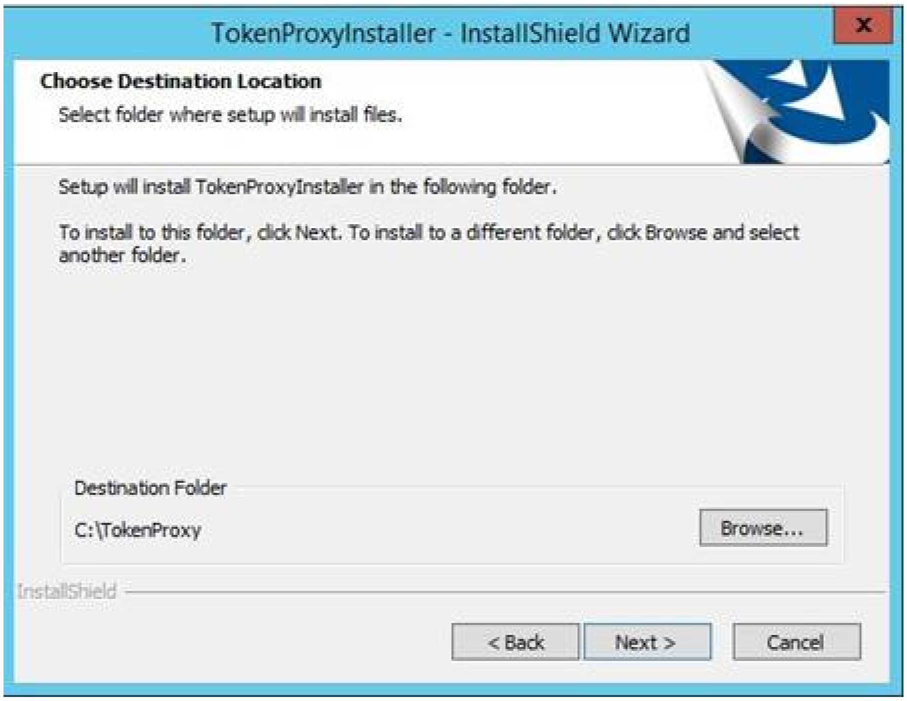
● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Select which program features you want installed. Recommended for advanced users.

4. Click **Browse** to amend the installation drive or Token Proxy installation path, if required and then click **Next**.



TokenProxyInstaller - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

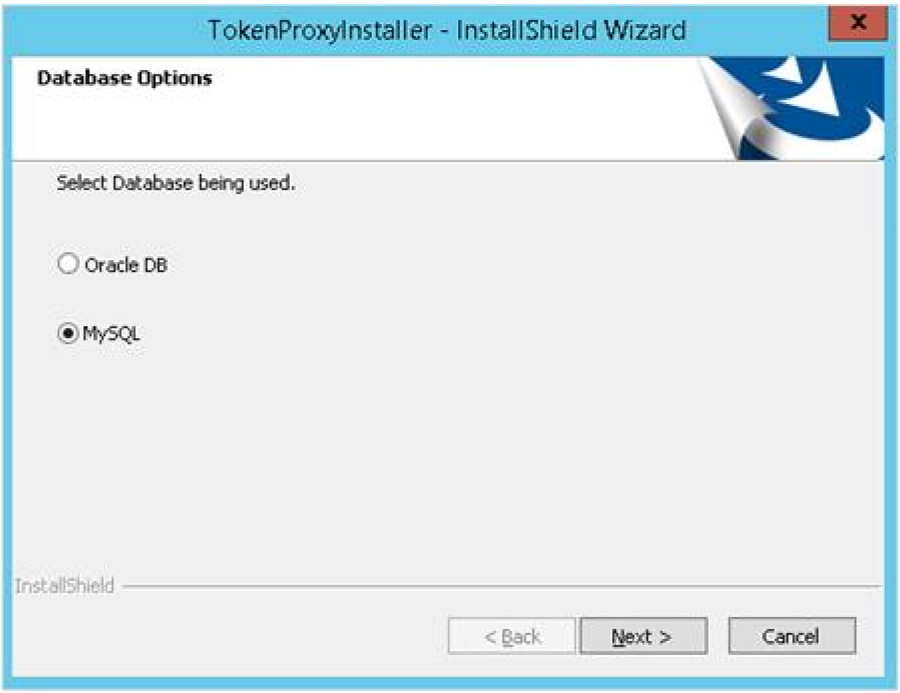
Setup will install TokenProxyInstaller in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\TokenProxy

5. Click **Install** to begin the installation.
6. Select your Database type:
   a. MySQL
   b. Oracle DB



TokenProxyInstaller - InstallShield Wizard

Database Options

Select Database being used.

○ Oracle DB

● MySQL

7. Click **Next**.
8. Enter the relevant connection details for your database type. Details can be provided by the individual who installed or configured the database software.

9. On the **Database Server** screen, enter the following credentials to allow the Token Proxy Service installer to connect to your Oracle 12c/19c or MySQL Database. The installer supports pluggable and legacy non-pluggable database formats.

   MySQL

   a. **Name/IP**: The Hostname or IP Address used for communication to the database. If the TPS and its database are installed on the same host machine, then you can enter the value as ‘localhost’ here.

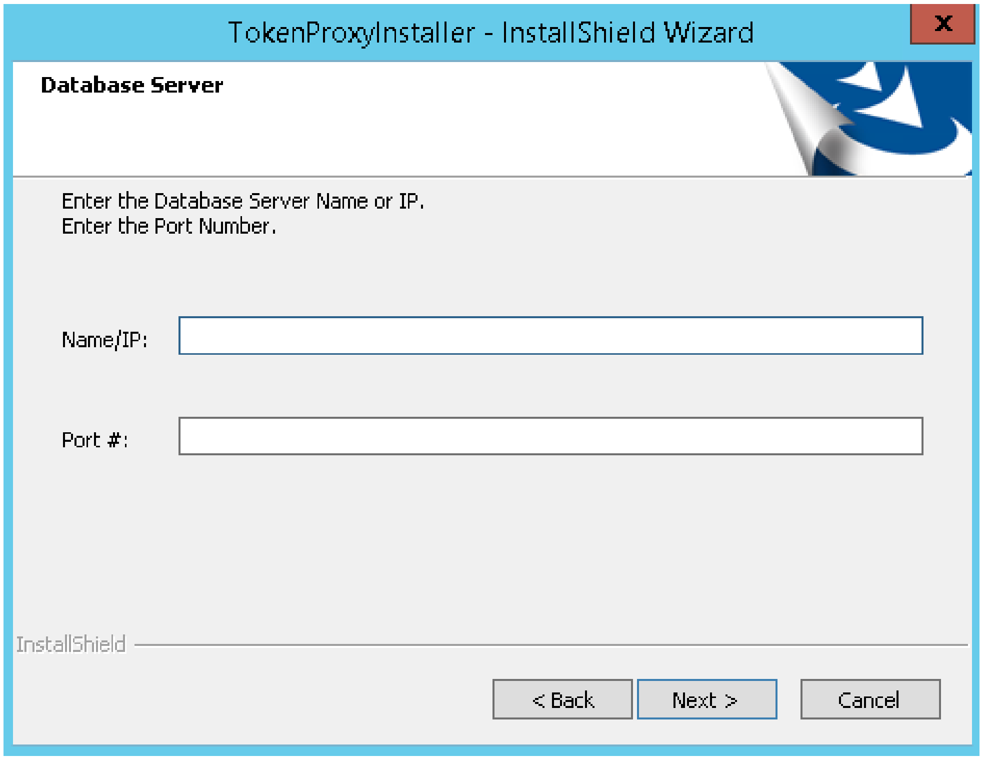
   b. **Port #**: The Port number used for communication to the database.

   Oracle DB

   a. **Name/IP**: The Hostname or IP Address used for communication to the database. If the TPS and its database are installed on the same host machine, you can enter the value as ‘localhost’ here.

   b. **Port #**: The Port number used for communication to the database.

   c. **Service Name**: The service name used to connect to the Oracle database.



TokenProxyInstaller - InstallShield Wizard

Database Server

Enter the Database Server Name or IP.
Enter the Port Number.

Name/IP:

Port #:

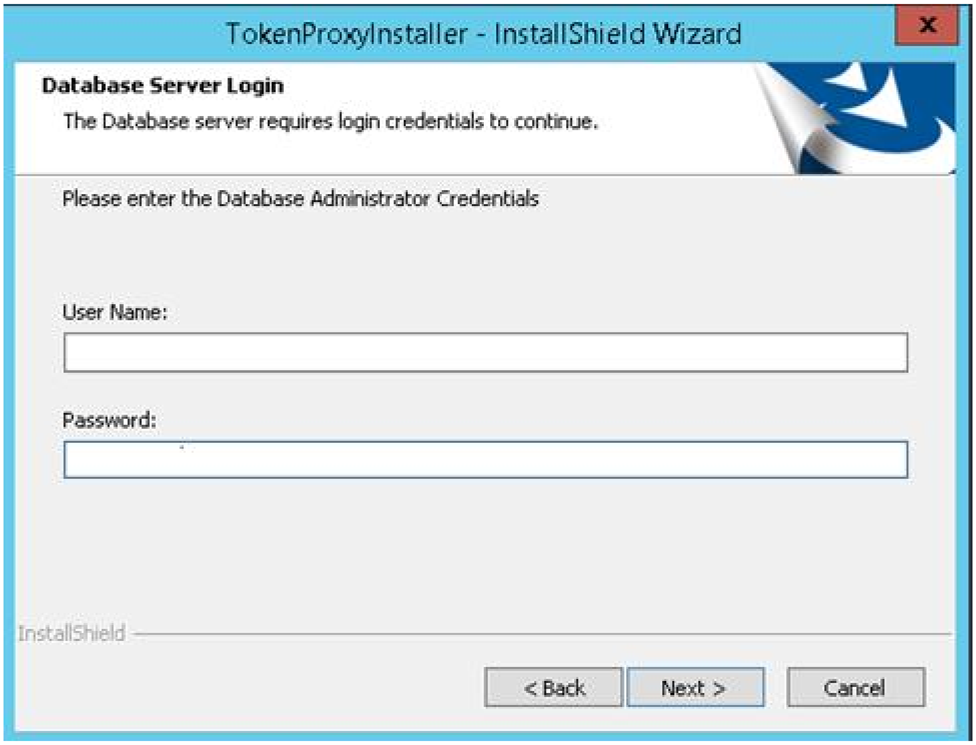
10. Click **Next**

11. Enter the database credentials. The installer requires DBA access to create a Token Proxy Service database user and configure a Token Proxy Service database schema.

    a. For MySQL the Login ID: = root

    b. For Oracle database, enter the DBA user name or Login ID.

    c. Enter the correct password for the DBA user.



TokenProxyInstaller - InstallShield Wizard
Database Server Login
The Database server requires login credentials to continue.
Please enter the Database Administrator Credentials
User Name:
Password:
InstallShield
< Back
Next >
Cancel

12. Click **Next**.

13. Enter the following details.

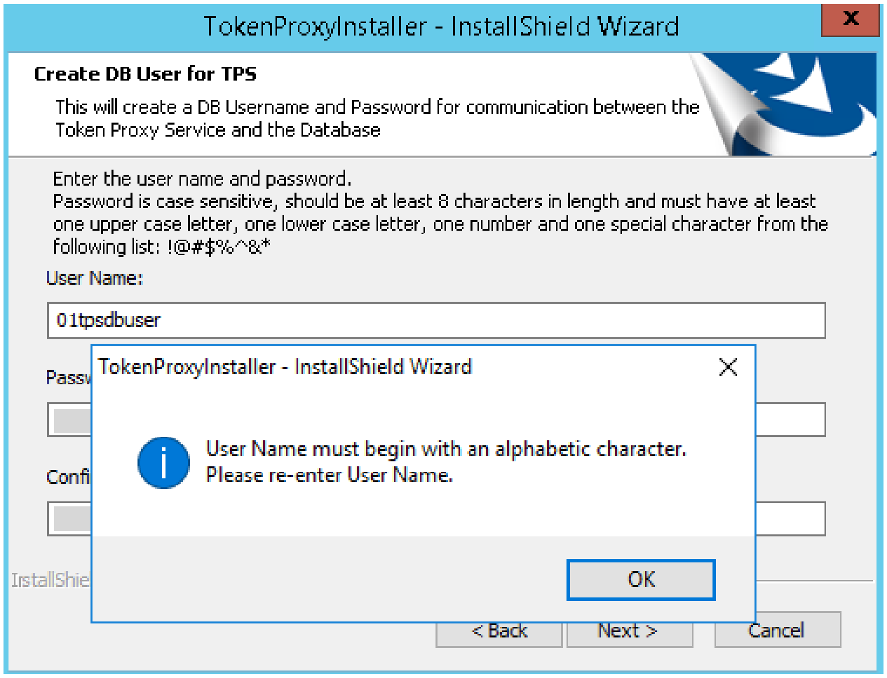
    a. **User Name**: Create a new user. When creating the username for the database, the installer allows only alphanumeric characters and should start only with an alphabetic character.

    b. **Password**: Create a password. The Password is case sensitive, and should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list:!@#$%^&*

    c. Confirm the password, and then click **Next**.

       - The installer attempts to connect to the database using the DBA credentials provided. 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 13. If there are any issues in creating the DB User, make sure the database specified is open for updating.



TokenProxyInstaller - InstallShield Wizard

Create DB User for TPS

This will create a DB Username and Password for communication between the Token Proxy Service and the Database

Enter the user name and password.
Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

User Name: 01tpsdbuser

TokenProxyInstaller - InstallShield Wizard

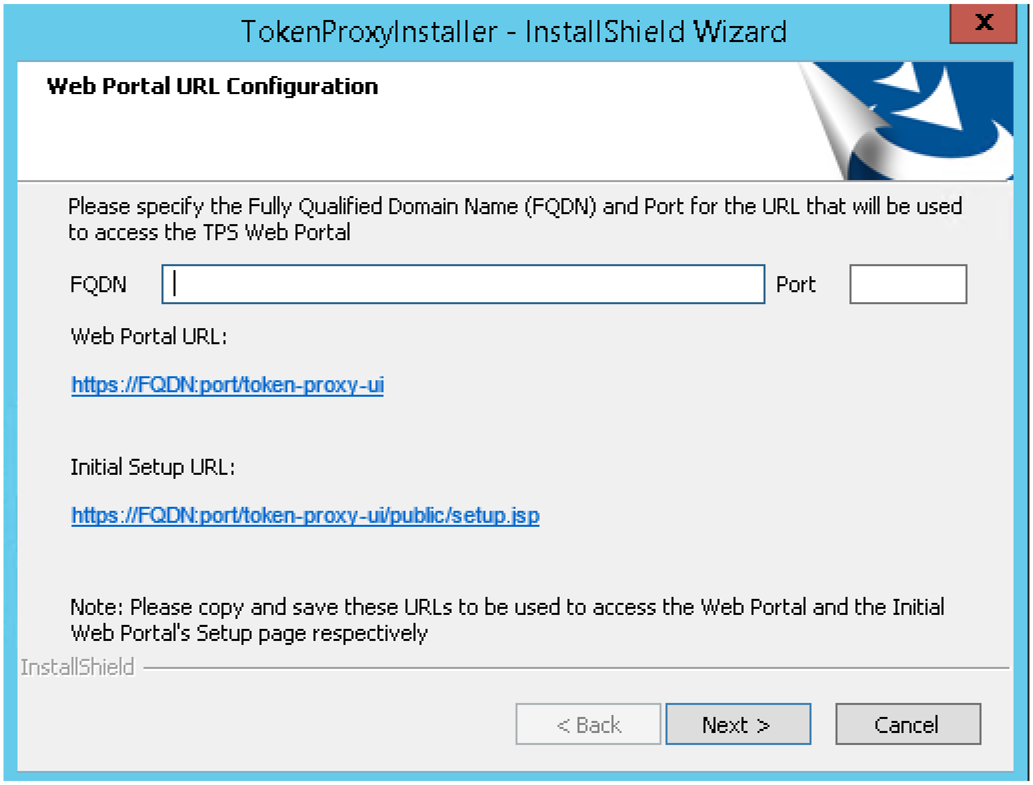
User Name must begin with an alphabetic character.
Please re-enter User Name.

14. Enter the URL where the web portal need to be installed and Port#.

    a. **FQDN** – The Fully Qualified Domain Name (FQDN) that is used to access the Token Proxy Service Web Portal.

    b. **Port** – The HTTPS port number the Web Portal deployment is configured to listen on WebLogic or Tomcat.

       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.



TokenProxyInstaller - InstallShield Wizard

Web Portal URL Configuration

Please specify the Fully Qualified Domain Name (FQDN) and Port for the URL that will be used to access the TPS Web Portal

FQDN

Port

Web Portal URL:

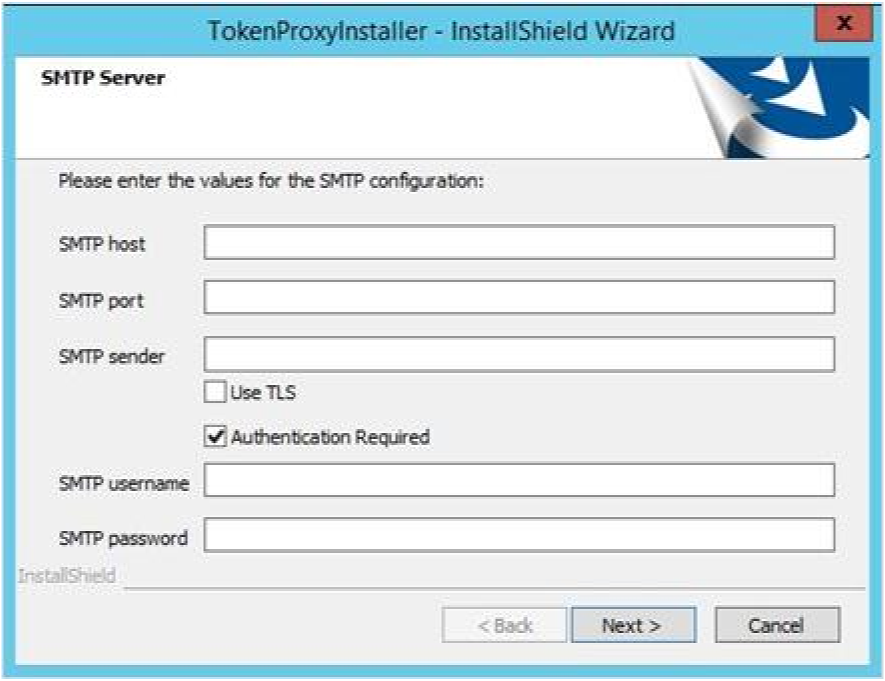
https://FQDN:port/token-proxy-ui

Initial Setup URL:

https://FQDN:port/token-proxy-ui/public/setup.jsp

Note: Please copy and save these URLs to be used to access the Web Portal and the Initial Web Portal's Setup page respectively

15. Click **Next**.
16. Enter the SMTP server details. The Token Proxy Service requires access to SMTP server in order to send password reset emails.
    a. **SMTP host**: Your SMTP mail server address.
    b. **SMTP port**: Your SMTP mail server port.
    c. **SMTP sender**: The email address that any password reset emails will show as sent from.
    d. **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.
    e. **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.
        i. **SMTP username**: If 'Authentication Required' is selected, set the username of the SMTP credentials.
        ii. **SMTP password**: If 'Authentication Required' is selected, set the password of the SMTP credentials.



TokenProxyInstaller - InstallShield Wizard

SMTP Server

Please enter the values for the SMTP configuration:

☐ Use TLS

☑ Authentication Required

17. Click **Next**.

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

    Utilities are deleted from the following path: **\TokenProxy\Utilities**

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

18. Select a Deployment Option.

    a. **Auto Deployment on WebLogic**: Select this option for a guided deployment of the Token Proxy Service Web Portal .WAR file and datasource into WebLogic. Refer to Auto deployment on WebLogic section for more details.

    b. **Auto Deployment on Tomcat**: Select this option for a guided deployment of the Token Proxy Service Web Portal .WAR file into Tomcat. Refer to Auto Deployment on Tomcat section for more details.

    c. **Manual Deployment on WebLogic**: Select this option if the Web Portal will be deployed in a clustered WebLogic environment. Deployments in clustered WebLogic environments must be performed manually. Refer to Manual deployment on WebLogic section for more details.

4
Token Proxy Service Custom Installation

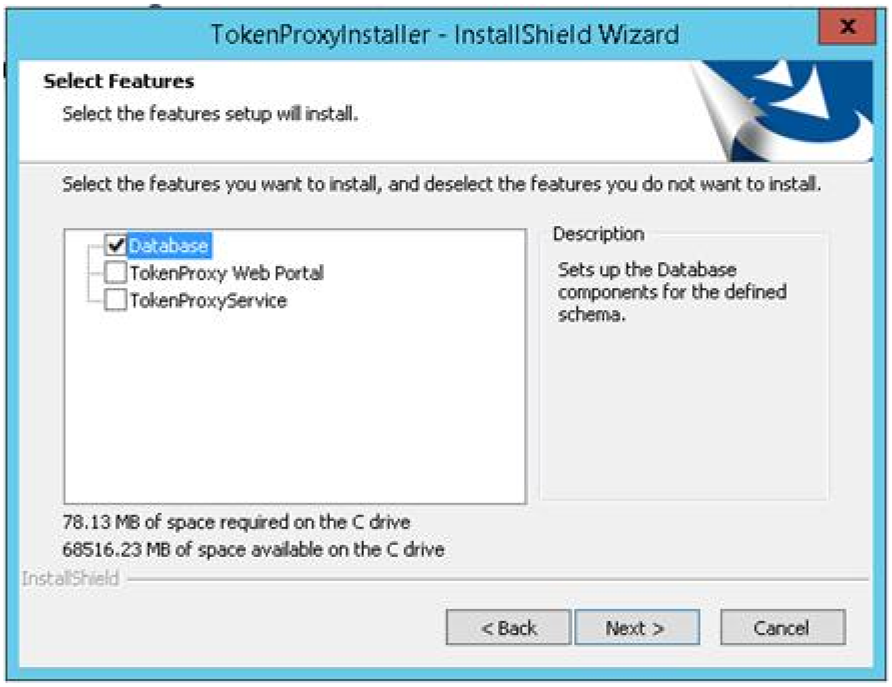
Token Proxy Service has three components. These components can be installed all on one host, or on separate hosts.

The correct order (required) for a custom install is:

- Database
- Token Proxy Web Portal
- Token Proxy Service

Part 1: Database

1. Right-click **TokenProxyInstaller_19.2.0.0.exe** file and select **Run as Administrator** to perform an installation.
2. Click **Next** to proceed with the installation.
3. On the **Setup Type** screen, select the **Custom** installation option and then click **Next**.
4. Click **Browse** to amend the installation drive or Token Proxy installation path, if required and then click **Next**.
5. On the **Select Features** screen, select the **Database** component and then click **Next**.



TokenProxyInstaller - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Database
☐ TokenProxy Web Portal
☐ TokenProxyService

Description

Sets up the Database components for the defined schema.

78.13 MB of space required on the C drive
68516.23 MB of space available on the C drive

6. Click **Install** to begin the installation.

7. Select your Database type:
   a. MySQL
   b. Oracle DB
8. Click **Next**.
9. Enter the relevant connection details for your database type. Details can be provided by the individual who installed or configured the database software.
10. On the **Database Server** screen, enter the following credentials to allow the Token Proxy Service installer to connect to your Oracle 12c/19c or MySQL Database. The installer supports pluggable and legacy non-pluggable database formats.

    MySQL

    a. **Name/IP**: The Hostname or IP Address used for communication to the database. If the TPS and its database are installed on the same host machine, then you can enter the value as ‘localhost’ here.
    b. **Port #**: The Port number used for communication to the database.

    Oracle DB

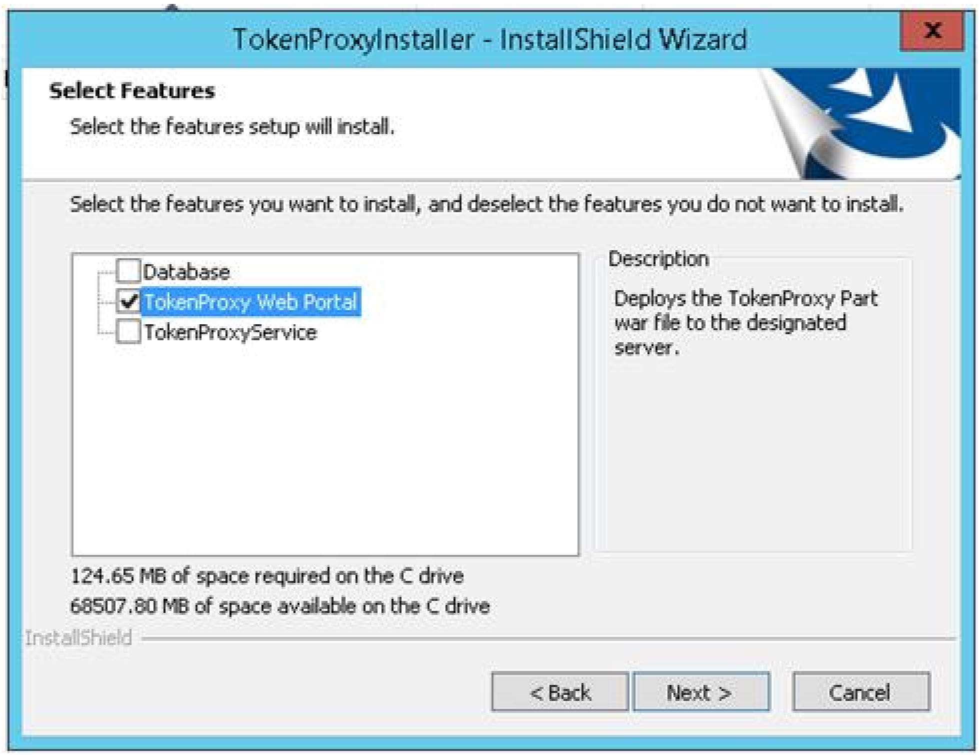
    a. **Name/IP**: The Hostname or IP Address used for communication to the database. If the TPS and its database are installed on the same host machine, you can enter the value as ‘localhost’ here.
    b. **Port #**: The Port number used for communication to the database.
    c. **Service Name**: The service name used to connect to the Oracle database.
11. Click **Next**.
12. Enter the database credentials. The installer requires DBA access to create a Token Proxy Service database user and configure a Token Proxy Service database schema.
    a. For MySQL the Login ID: = root
    b. For Oracle database, enter the DBA user name or Login ID.
    c. Enter the correct password for the DBA user.
13. Click **Next**.
14. Enter the following details.
    a. **User Name**: Create a new user. When creating the username for the database, the installer allows only alphanumeric characters and should start only with an alphabetic character.
    b. **Password**: Create a password. The Password is case sensitive, and should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list:!@#$%^&*
    c. Confirm the password, and then click **Next**.
       - The installer attempts to connect to the database using the DBA credentials provided. 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 14. If there are any issues in creating the DB User, make sure the database specified is open for updating.

15. Click **Finish**.

Part 2: Token Proxy Web Portal

1. Right-click **TokenProxyInstaller_19.2.0.0.exe** file and select **Run as Administrator** to perform an installation.
2. Click **Next** to proceed with the installation.
3. On the **Setup Type** screen, select the **Custom** installation option and then click **Next**.
4. Click **Browse** to amend the installation drive or Token Proxy installation path, if required and then click **Next**.
5. On the **Select Features** screen, select the **Token Proxy Web Portal** component and then click **Next**.



Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- □ Database
- ☑ TokenProxy Web Portal
- □ TokenProxyService

Description

Deploys the TokenProxy Part war file to the designated server.

124.65 MB of space required on the C drive

68507.80 MB of space available on the C drive

Note:

If you want to install Token Proxy Web Portal and want to create datasource using the installer, then the prerequisite is database. The installer will prompt for the database details for datasource creation.

6. Click **Install**to begin the installation.

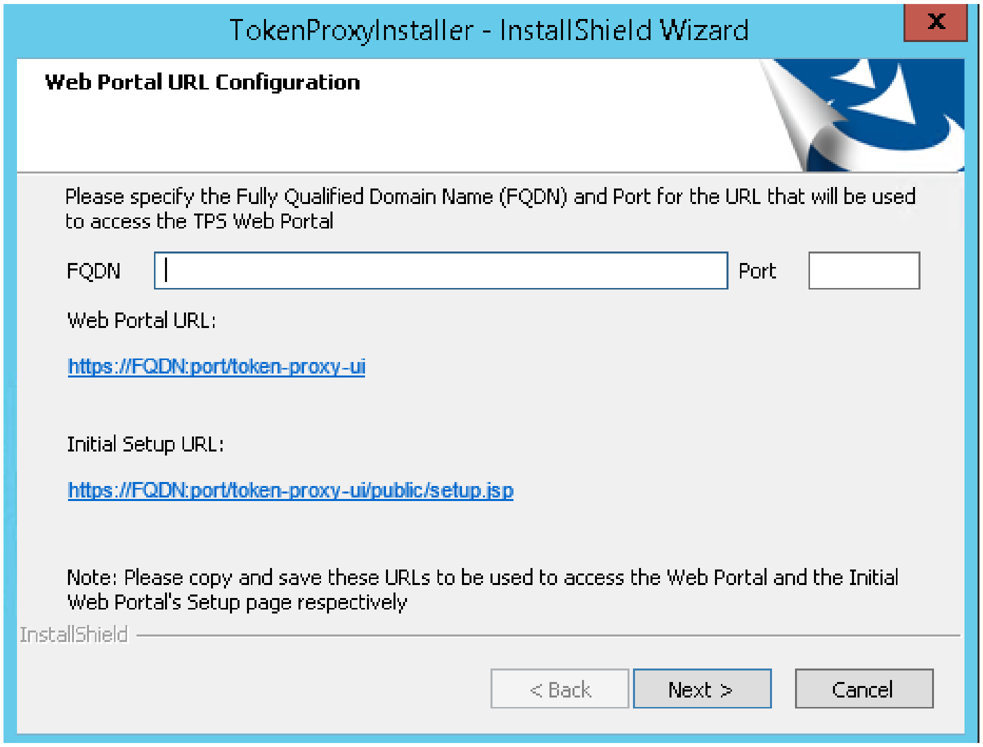
7. Enter the URL where the web portal need to be installed and Port#.

   a. **FQDN**: The Fully Qualified Domain Name (FQDN) that is used to access the Token Proxy Service Web Portal.

   b. **Port**: The HTTPS port number the Web Portal deployment is configured to listen on in WebLogic or Tomcat.

      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.



TokenProxyInstaller - InstallShield Wizard

Web Portal URL Configuration

Please specify the Fully Qualified Domain Name (FQDN) and Port for the URL that will be used to access the TPS Web Portal

FQDN: | Port:

Web Portal URL:

https://FQDN:port/token-proxy-ui

Initial Setup URL:

https://FQDN:port/token-proxy-ui/public/setup.jsp

Note: Please copy and save these URLs to be used to access the Web Portal and the Initial Web Portal's Setup page respectively

8. Click **Next**.

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

   a. **SMTP host**: Your SMTP mail server address.

   b. **SMTP port**: Your SMTP mail server port.

   c. **SMTP sender**: The email address that any password reset emails will show as sent from.

   d. **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.

   e. **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.

      i. **SMTP username**: If ‘Authentication Required’ is selected, set the username of the SMTP credentials.

   ii. **SMTP password**: If ‘Authentication Required’ is selected, set the password of the SMTP credentials.

10. Click **Next**.

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

    Utilities are deleted from the following path: **\TokenProxy\Utilities**

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

11. Select a Deployment Option.

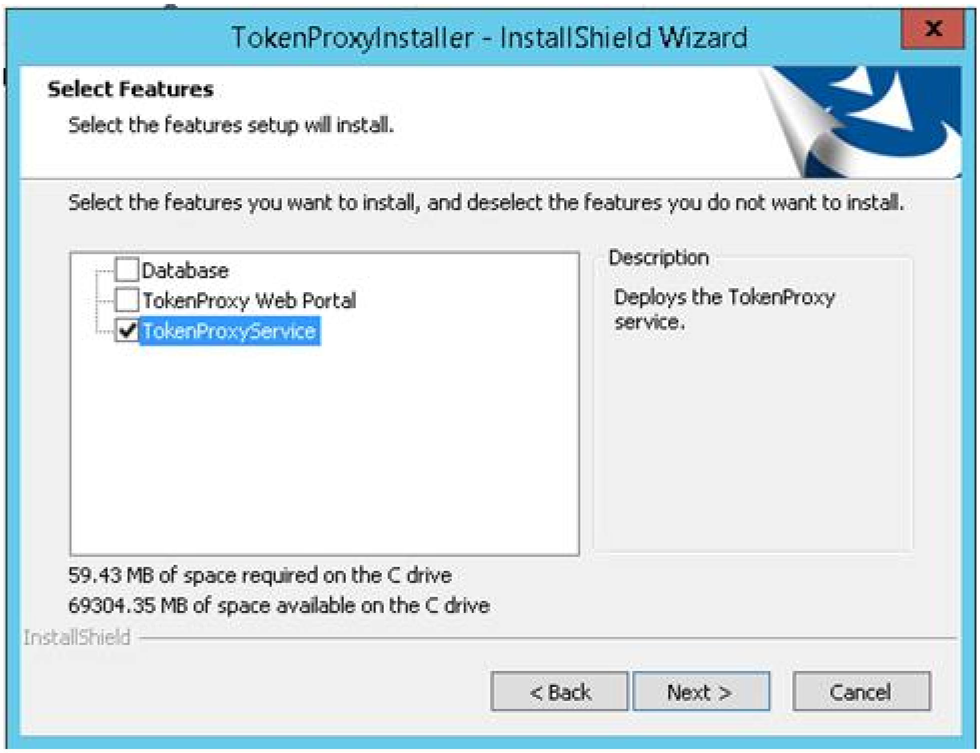
    a. **Auto Deployment on WebLogic**: Select this option for a guided deployment of the Token Proxy Service Web Portal .WAR file and datasource into WebLogic. Refer to Auto deployment on WebLogic section for more details.

    b. **Auto Deployment on Tomcat**: Select this option for a guided deployment of the Token Proxy Service Web Portal .WAR file into Tomcat. Refer to Auto Deployment on Tomcat section for more details.

    c. **Manual Deployment on WebLogic**: Select this option if the Web Portal will be deployed in a clustered WebLogic environment. Deployments in clustered WebLogic environments must be performed manually. Refer to Manual deployment on WebLogic section for more details.

Part 3: Token Proxy Service

1. Right-click **TokenProxyInstaller_19.2.0.0.exe** file and select **Run as Administrator** to perform an installation.
2. Click **Next** to proceed with the installation.
3. On the **Setup Type** screen, select the **Custom** installation option and then click **Next**.
4. Click **Browse** to amend the installation drive or Token Proxy installation path, if required and then click **Next**.
5. On the **Select Features** screen, select the **Token Proxy Service** component and then click **Next**.



TokenProxyInstaller - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- □ Database
- □ TokenProxy Web Portal
- ☑ TokenProxyService

Description

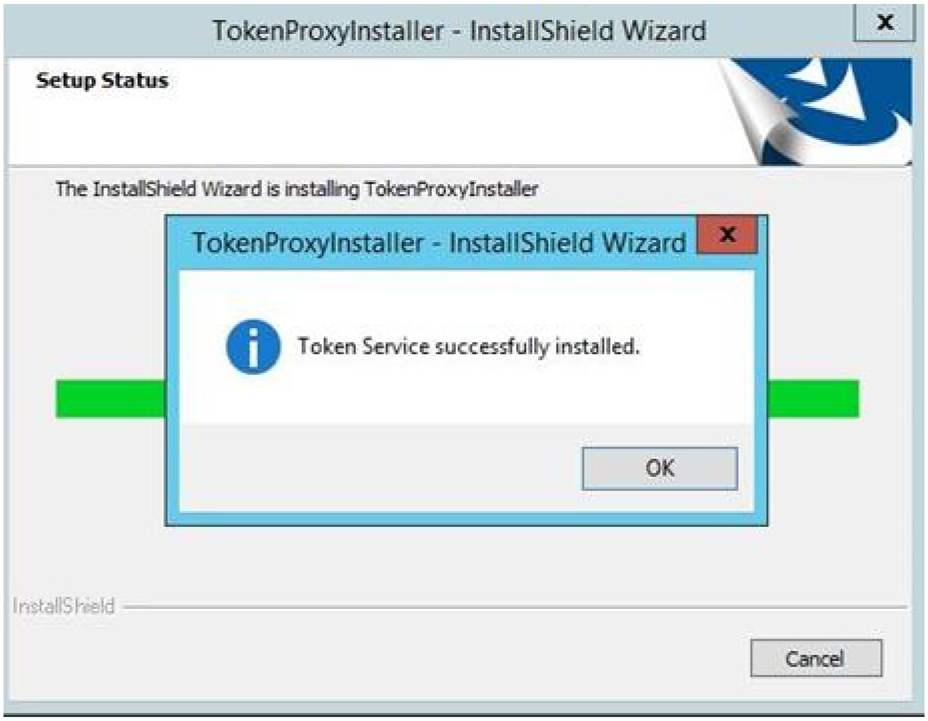
Deploys the TokenProxy service.

59.43 MB of space required on the C drive
69304.35 MB of space available on the C drive

> **Note:**
>
> If you want to install the Token Proxy Service and want to connect the service to database, then the prerequisite is database.

6. Click **Install** to begin the installation.

   The installer installs the Token Proxy Service.



TokenProxyInstaller - InstallShield Wizard

Setup Status

The InstallShield Wizard is installing TokenProxyInstaller

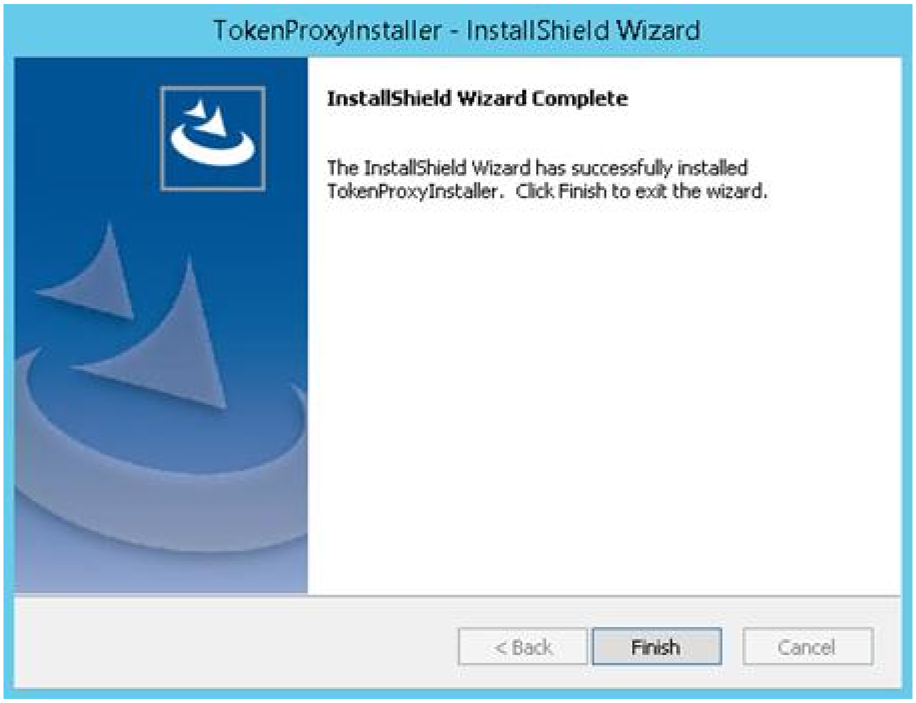
TokenProxyInstaller - InstallShield Wizard

Token Service successfully installed.

Note:

The **OPI Token Service** Windows service installation completes. The service remains in stopped state until the Web Portal configuration is complete. The **Apache Tomcat for TPS** Windows service installation completes. The service remains in stopped state until the Web Portal configuration is complete. This service is applicable only if you choose to deploy TPS using Tomcat.

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



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed TokenProxyInstaller. Click Finish to exit the wizard.

Auto Deployment on WebLogic

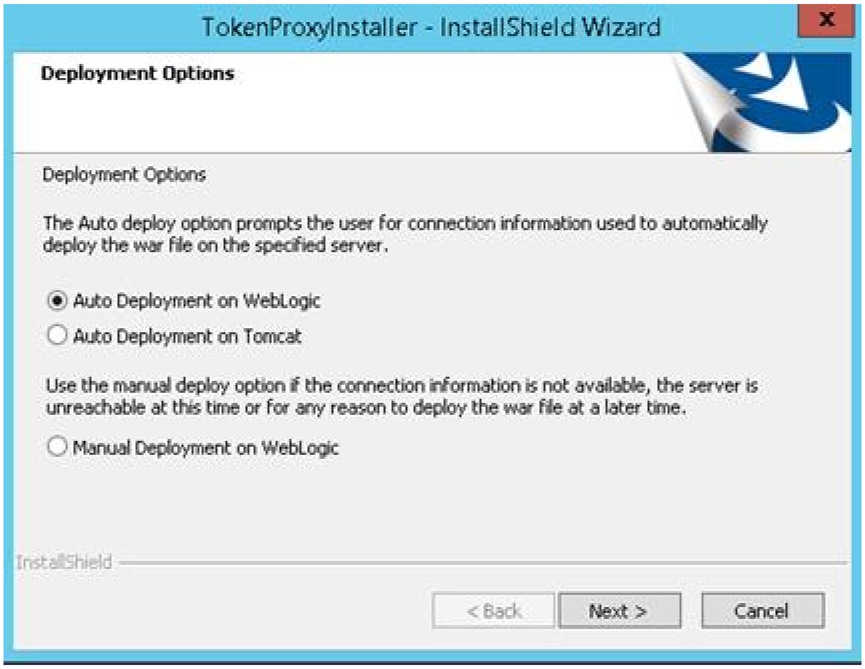
You can auto deploy the Token Proxy Service Web Portal .WAR file and datasource into WebLogic only if **Oracle** database is selected.

> **Note:**
>
> If the Token Proxy Portal is installed on WebLogic, then the Manage Server(s) that are hosting the Token Proxy Portal will need to be restarted once the installation has been completed in order for the configuration changes to take effect.

Granting permissions on WebLogic user account

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

1. On the **Deployment Options** screen, select **Auto deployment on WebLogic** option for a guided deployment of the Token Proxy Service Web Portal.



TokenProxyInstaller - InstallShield Wizard

Deployment Options

Deployment Options

The Auto deploy option prompts the user for connection information used to automatically deploy the war file on the specified server.

● Auto Deployment on WebLogic

○ Auto Deployment on Tomcat

Use the manual deploy option if the connection information is not available, the server is unreachable at this time or for any reason to deploy the war file at a later time.

○ Manual Deployment on WebLogic

2. Click **Next**.

3. On the **WebLogic Connection Settings** screen, enter the following details. This screen 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.

   a. **Host**: WebLogic IP address.

   b. **Port**: WebLogic port number.

   c. **Username**: WebLogic user name.

   d. **Password**: WebLogic password.

   e. **Protocol**:

      i. **T3** is the default WebLogic Protocol.

      ii. **T3S** is the T3 Protocol with SSL.

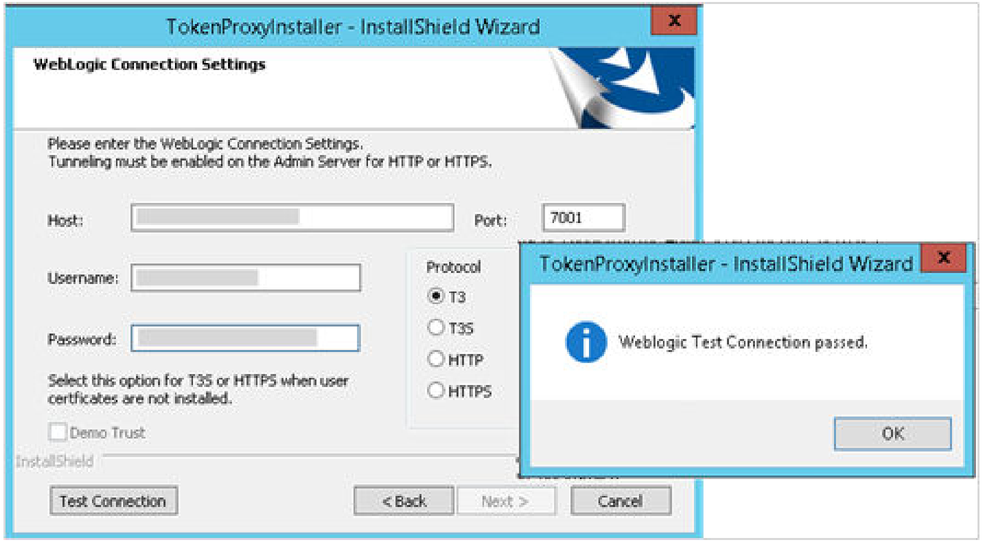
      iii. **HTTP** is T3 wrapped in HTTP to allow routing through firewalls, if required.

      iv. **HTTPS** is T3S wrapped in HTTP to allow routing through firewalls, if required.

   f. **Demo Trust**: Select this option for **T3S** or **HTTPS** when user certificates are not installed while installing the WebLogic.

4. 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 WebLogic Environment.


TokenProxyInstaller - InstallShield Wizard
WebLogic Connection Settings
Host:
Port:
Username:
Password:
Protocol
InstallShield
Test Connection
< Back
Next >
Cancel
TokenProxyInstaller - InstallShield Wizard
OK

Please enter the WebLogic Connection Settings.
Tunneling must be enabled on the Admin Server for HTTP or HTTPS.

Port: 7001

Protocol: ● T3 ○ T3S ○ HTTP ○ HTTPS

Select this option for T3S or HTTPS when user certficates are not installed.

□ Demo Trust

Weblogic Test Connection passed.

5. Enter the name of the WebLogic **Server** you want to deploy or undeploy the Token Proxy Service Web Portal.

   - **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.

6. Click **Next**.

7. 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.

8. Click **Next**. If you have previously selected **Create a default datasource for the database connection**, the Token Proxy Service installer attempts 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.

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

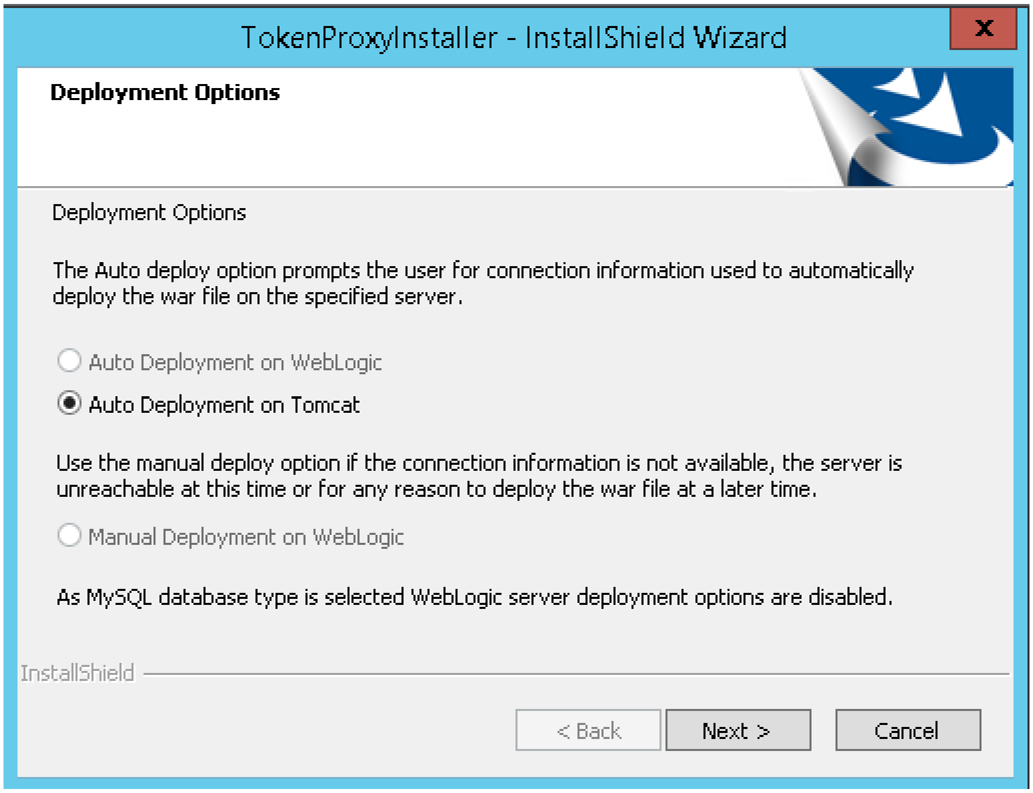
10. Click **Finish** to complete the Token Proxy Service installation.

Auto Deployment on Tomcat

You can auto deploy the Token Proxy Service Web Portal .WAR file on Tomcat if **MySQL** database is selected.

1. On the **Deployment Options** screen, **Auto deployment on Tomcat** option is selected by default.

> **Note:**
>
> **Auto Deployment on WebLogic** and **Manual Deployment on WebLogic** options are disabled for MySQL.



TokenProxyInstaller - InstallShield Wizard

Deployment Options

Deployment Options

The Auto deploy option prompts the user for connection information used to automatically deploy the war file on the specified server.

○ Auto Deployment on WebLogic

● Auto Deployment on Tomcat

Use the manual deploy option if the connection information is not available, the server is unreachable at this time or for any reason to deploy the war file at a later time.

○ Manual Deployment on WebLogic

As MySQL database type is selected WebLogic server deployment options are disabled.

2. Click **Next**.
3. On the **Create Tomcat User Account** screen, enter the following details.
   a. **User Name**: Create a new user.
   b. **Password**: Create a password. The Password is case sensitive, and should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list:!@#$%^*.
   c. Confirm the password, and then click **Next**.

   This user will have access to the files in the Tomcat installation.

> **Note:**
>
> The Tomcat User Account Password by default is set to expire after 42 days (Windows default domain policy). Please update password/default expiration date range as required. Refer to Change the password expiration policy for windows user account in the **Auto Deployment on Tomcat** section of **Token Proxy Service Custom Installation**.

4. On the **Tomcat HTTPS Certificate** screen, create the Password and confirm it.

   The Password is case sensitive, and should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list:!@#$%^&*.

5. Click **Next**.

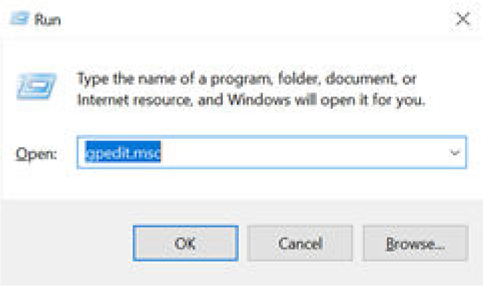
   When Tomcat is selected as web server to host the TPS web portal, the installer creates a self-signed certificate for Tomcat as server's certificate. In production, CA signed certificate is highly recommended. Refer to "Tomcat – Certificate Configuration Wizard" and "Tomcat HTTPS Listener" section for steps to replace self-signed certificate with the CA signed certificate.

> **Note:**
>
> If you are performing Custom installation, then the installer will prompt for database details for datasource creation.

6. The **Apache Tomcat for TPS** Windows service installation completes. The service remains in stopped state until the Web Portal configuration is complete.
7. Click **Finish** to complete the Token Proxy Service installation.

Change the Password Expiration Policy for Windows User Account

1. Open Run Application (Win + R).

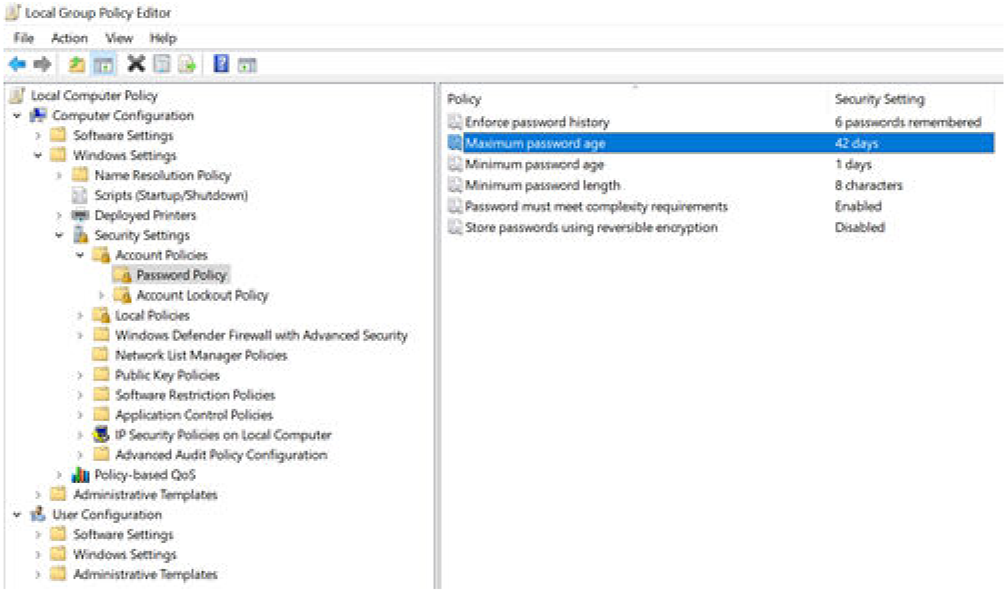


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

2. Enter **gpedit.msc** and click **OK**. Local Group Policy Editor will be displayed.

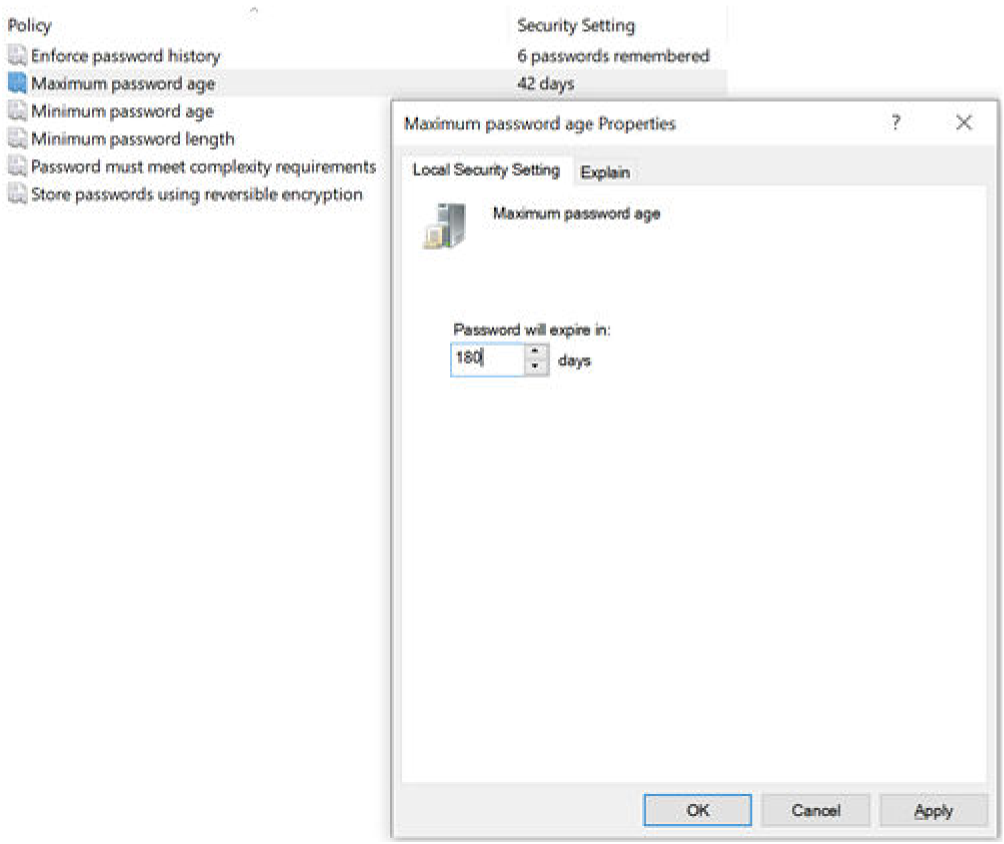


- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
        - Local Policies
        - Windows Defender Firewall with Advanced Security
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Policy	Security Setting
Enforce password history	6 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

3. Go to **Computer Configuration -> Windows Settings -> Security settings -> Account Policies -> Password Policy**.

4. Double click on **Maximum password age** on the right panel.



Policy	Security Setting
Enforce password history	6 passwords remembered
Maximum password age	42 days
Minimum password age	
Minimum password length	
Password must meet complexity requirements	
Store passwords using reversible encryption	

Maximum password age

Password will expire in:
180 days

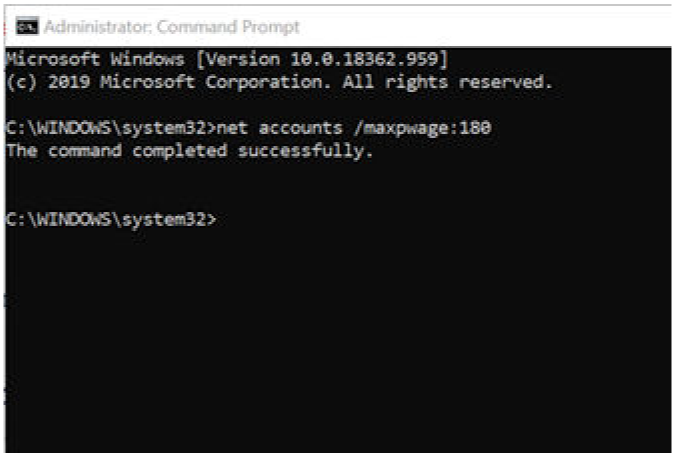
5. Set the expiration days as per your organization's password policy. Click on **Apply** and then **OK**.

> **Note:**
>
> This change is applicable to all the user accounts in the system.

Alternate Way

The password expiry policy can also be set using command line.

1. Open **Command Prompt** as Administrator.
2. Set the password expiration days as per your organization's password policy. Execute the command **net accounts /maxpwage:180**



```
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net accounts /maxpwage:180
The command completed successfully.


C:\WINDOWS\system32>
```

> **Note:**
>
> Here **180**, is the password age. Change this as per your organization's password policy.

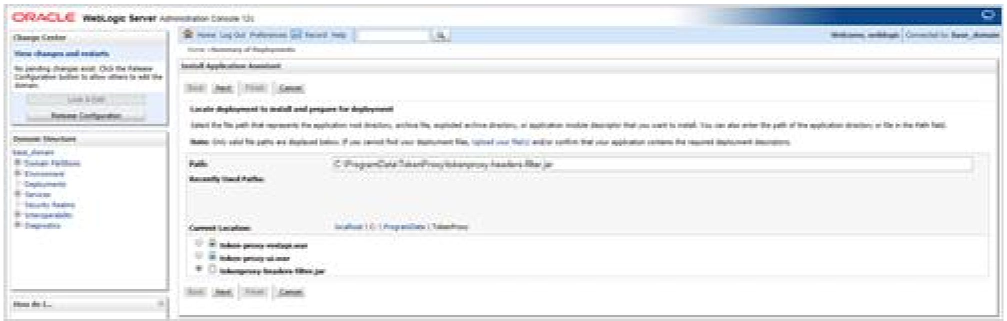
Manual Deployment on WebLogic

The Token Proxy Installer deploys two .WAR files (token-proxy-restapi.war, token-proxy-ui.war) and a .JAR file (tokenproxy-headers-filter.jar) on WebLogic as an Application deployment, unless you select the option to manually complete the WebLogic deployment.

The headers jar (tokenproxy-headers-filter.jar) should be deployed before either of the WAR files. Successful deployment of the .WAR files is possible only if the .JAR file has already been deployed. Once the installation is complete, you can find the required files for manual deployment at C:\ProgramData\TokenProxy.

> **Note:**
>
> If the Token Proxy Portal is installed on WebLogic, the Manage Server(s) that are hosting the Token Proxy Portal will need to be restarted once the installation has been completed in order for the configuration changes to take effect.

1. In the **WebLogic Server Administration Console**, select **Deployments** menu.
2. Select the **Lock & Edit** option and then click **Install**.
3. Browse to the C:\ProgramData\TokenProxy directory and select the **tokenproxy-headers-filter.jar** file.



Install Application Assistant

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or file in the Path field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the required deployment descriptors.

Path: C:\ProgramData\TokenProxy\tokenproxy-headers-filter.jar

Recently Used Paths:

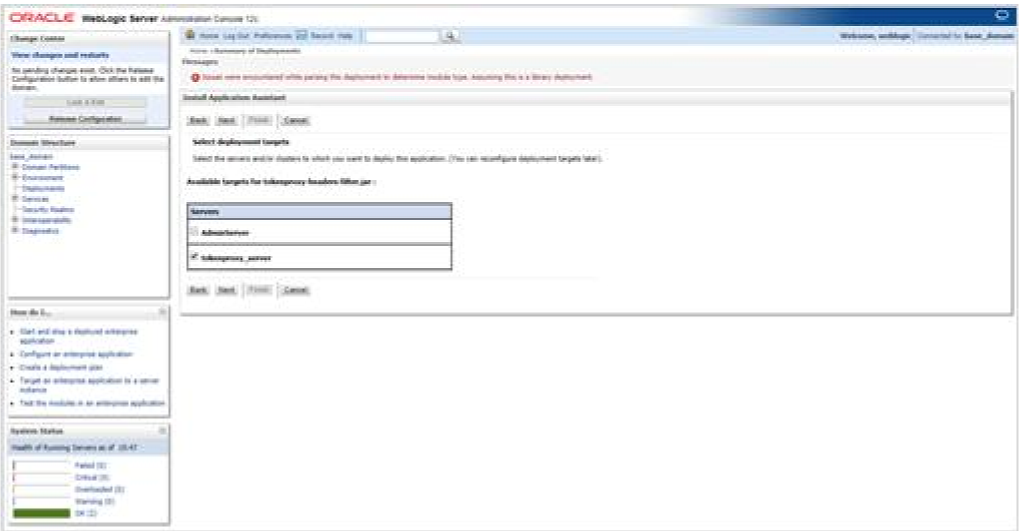
Current Location: localhost \ C: \ ProgramData \ TokenProxy

○ token-proxy-restapi.war
○ token-proxy-ui.war
● tokenproxy-headers-filter.jar

ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Lock & Edit
Release Configuration
Domain Structure
Home Log Out Preferences Record Help
Back Next Finish Cancel
How do I...

4. Click **Next**.
5. Select the target **Server** to which you want to deploy the application and then click **Next**.

   The message reporting that Weblogic has assumed this as a library deployment, is only a warning and is correct, the tokenproxy-headers-filter.jar is a library not an application.



Messages

Issues were encountered while parsing this deployment to determine module type. Assuming this is a library deployment.

Install Application Assistant

Select deployment targets

Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later).

Available targets for tokenproxy-headers-filter.jar :

Servers
☐ AdminServer
☑ tokenproxy_server

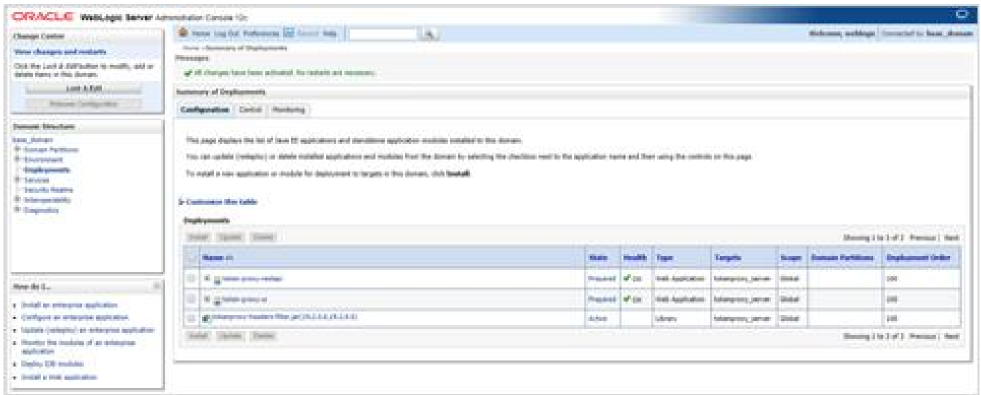
ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Lock & Edit
Release Configuration
Domain Structure
Home Log Out Preferences Record Help
Back Next Finish Cancel
How do I...
System Status

6. Select **DD Only**, and then select the other options required for your WebLogic environment.
7. Click **Finish** to complete the deployment, you are redirected to the Deployments screen.
8. To deploy the **token-proxy-restapi.war** file:

   a. Select **Install**.
   b. The C:\ProgramData\TokenProxy directory should be retained from the previous deployment, if not browse and select the **token-proxy-restapi.war.**
   c. Click **Next**.
   d. Select **Install this deployment as an application**.
   e. Click **Next**.
   f. Select the target **Server** to which you want to deploy the application, and click **Next**.
   g. Select **DD Only**, and then select the other options required for your WebLogic environment.
   h. Click **Finish** to complete the deployment, you are redirected to the Deployments screen.

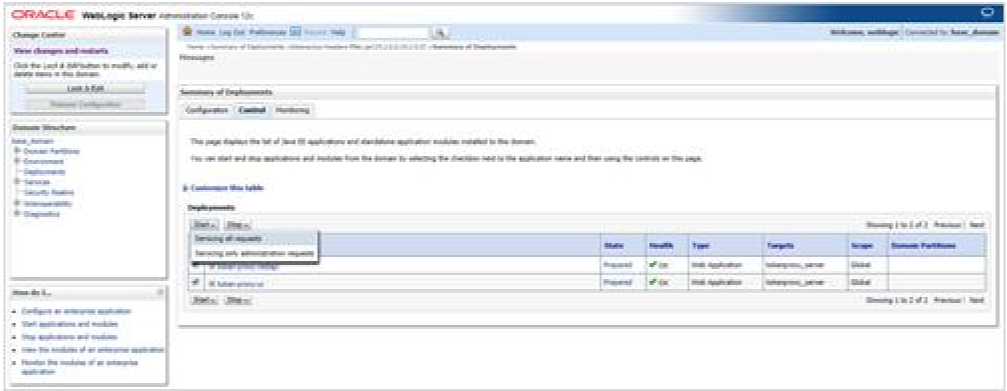
9. To deploy the **token-proxy-ui.war** file:
   a. Select **Install**.
   b. The C:\ProgramData\TokenProxy directory should be retained from the previous deployment, if not browse and select the **token-proxy-ui.war**.
   c. Click **Next**.
   d. Select **Install this deployment as an application**.
   e. Click **Next**.
   f. Select the target **Server** to which you want to deploy the application, and click **Next**.
   g. Select **DD Only**, and then select the other options required for your WebLogic environment.
   h. Click **Finish** to complete the deployment, you are redirected to the Deployments screen.

10. Once all the files are deployed, click **Activate Changes**.



Name	State	Health	Type	Targets	Scope	Domain Partitions	Deployment Order
token-proxy-restapi	Prepared	✓ OK	Web Application	tokenproxy_server	Global		100
token-proxy-ui	Prepared	✓ OK	Web Application	tokenproxy_server	Global		100
[illegible]	Active		Library	tokenproxy_server	Global		100

11. Click the **Control** tab and then select the **token-proxy-ui.war** and **token-proxy-restapi.war** web applications.
12. Click **Start** and then select **Servicing all requests** to start the web applications.
13. Click **Yes** to start the selected deployments and **No** to discard the process.


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
base_domain
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure an enterprise application
Start applications and modules
Stop applications and modules
View the modules of an enterprise application
Monitor the modules of an enterprise application
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Messages
Summary of Deployments
Configuration Control Monitoring
Customize this table
Start Stop
Servicing all requests
Servicing only administration requests
Showing 1 to 2 of 2 Previous | Next

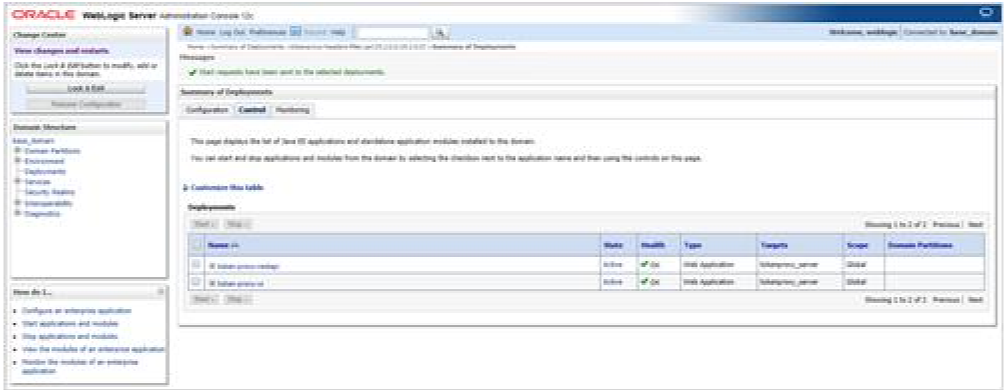
This page displays the list of Java EE applications and standalone application modules installed to this domain.

You can start and stop applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on this page.

Deployments

Name	State	Health	Type	Targets	Scope	Domain Partitions
token-proxy-restapi	Prepared	✓ OK	Web Application	tokenproxy_server	Global	
token-proxy-ui	Prepared	✓ OK	Web Application	tokenproxy_server	Global	

14. Once the deployed web applications show **Active** state, then you can access the Web Portal using your browser.


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
base_domain
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure an enterprise application
Start applications and modules
Stop applications and modules
View the modules of an enterprise application
Monitor the modules of an enterprise application
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Messages
Summary of Deployments
Configuration Control Monitoring
Customize this table
Start Stop
Showing 1 to 2 of 2 Previous | Next

✓ Start requests have been sent to the selected deployments.

This page displays the list of Java EE applications and standalone application modules installed to this domain.

You can start and stop applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on this page.

Deployments

Name	State	Health	Type	Targets	Scope	Domain Partitions
token-proxy-restapi	Active	✓ OK	Web Application	tokenproxy_server	Global	
token-proxy-ui	Active	✓ OK	Web Application	tokenproxy_server	Global	

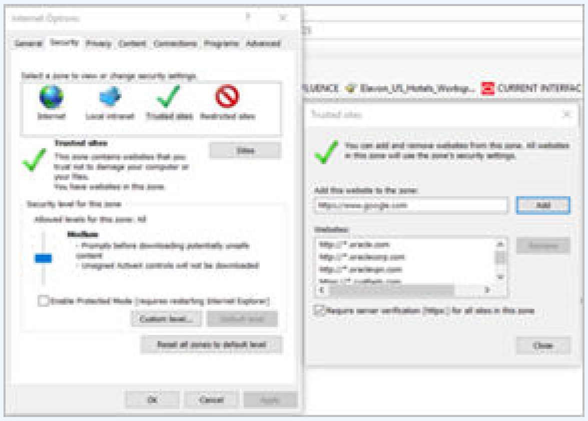
Token Proxy Configuration Web Portal

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

Note:

To access Token Proxy Service web portal using Internet Explorer (IE), you need to edit the IE settings as given below:

- Add URL to IE Trusted Sites list.
- Deselect “Display intranet sites in Compatibility view” check box in IE compatibility view settings.



Internet Options

Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Allowed levels for this zone: All

Medium
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

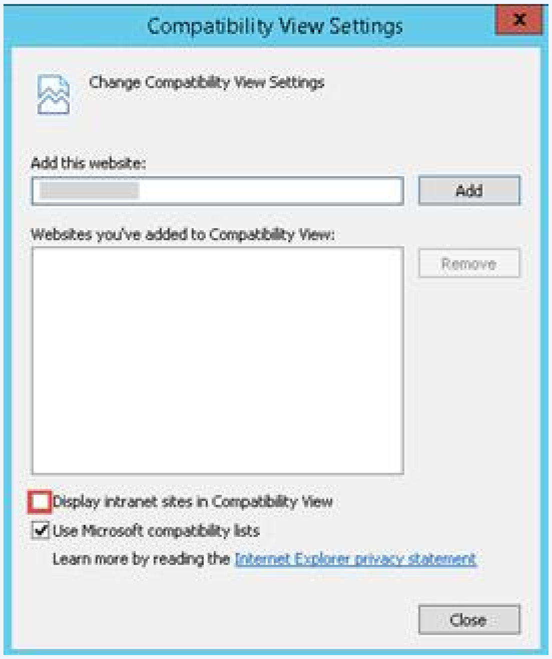
Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:
https://www.google.com

Websites:
http://*.oracle.com
http://*.oraclecorp.com
http://*.oraclegtn.com

☑ Require server verification (https:) for all sites in this zone



Compatibility View Settings

Change Compatibility View Settings

Add this website:

Websites you've added to Compatibility View:

□ Display intranet sites in Compatibility View
☑ Use Microsoft compatibility lists
Learn more by reading the Internet Explorer privacy statement

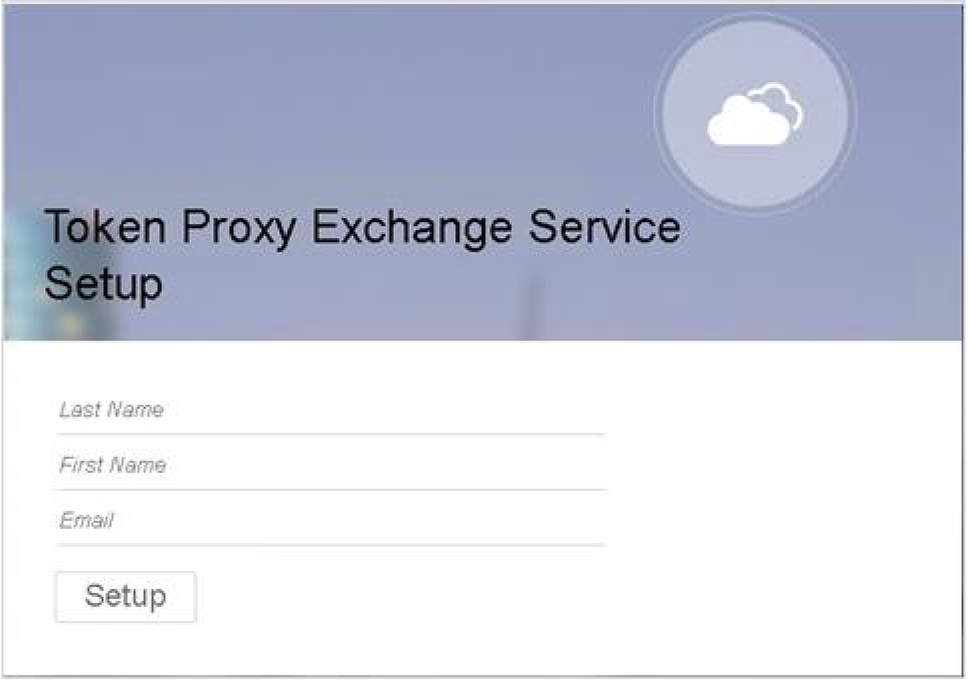
If the web portal starts correctly, then you can browse to it using HTTPS and the configured FQDN (Fully Qualified Domain Name), port and application context, as shown in the following example: https://<FQDN>:<port>/token-proxy-ui/public/setup.jsp for both standard and non-standard ports.

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

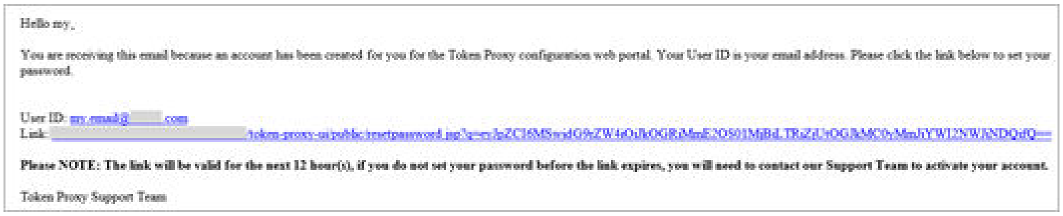
Token Proxy Exchange Setup

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

1. On the **Token Proxy Exchange Setup** page, enter the following details.
   a. **Last Name**: Enter your last name.
   b. **First Name**: Enter your first name.
   c. **Email**: Enter your email address.



2. Click **Setup**. The Token Proxy Exchange Setup sends an email to the admin user that contains a link with a unique password reset token.



Hello my,

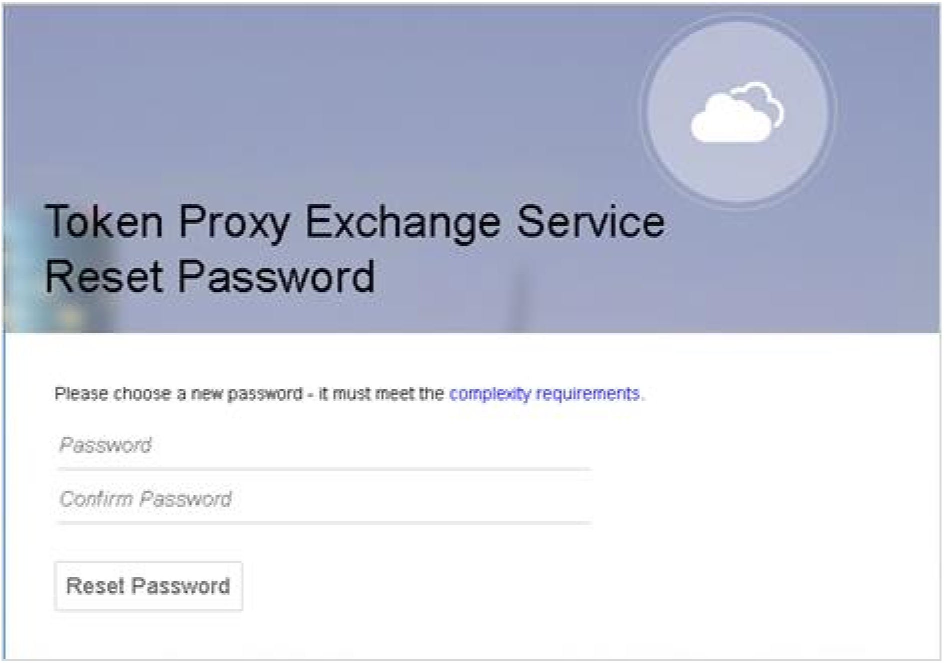
You are receiving this email because an account has been created for you for the Token Proxy configuration web portal. Your User ID is your email address. Please click the link below to set your password.

User ID: my.email@[redacted].com
Link: [redacted]/token-proxy-ui/public/resetpassword.jsp?q=eyJpZCI6MSwidG9rZW4iOiJkOGRiMmE2OS01MjBiLTRiZjUtOGJkMC0yMmJiYWI2NWJiNDQifQ==

Please NOTE: The link will be valid for the next 12 hour(s), if you do not set your password before the link expires, you will need to contact our Support Team to activate your account.

Token Proxy Support Team

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:



Token Proxy Exchange Service
Reset Password

Please choose a new password - it must meet the complexity requirements.

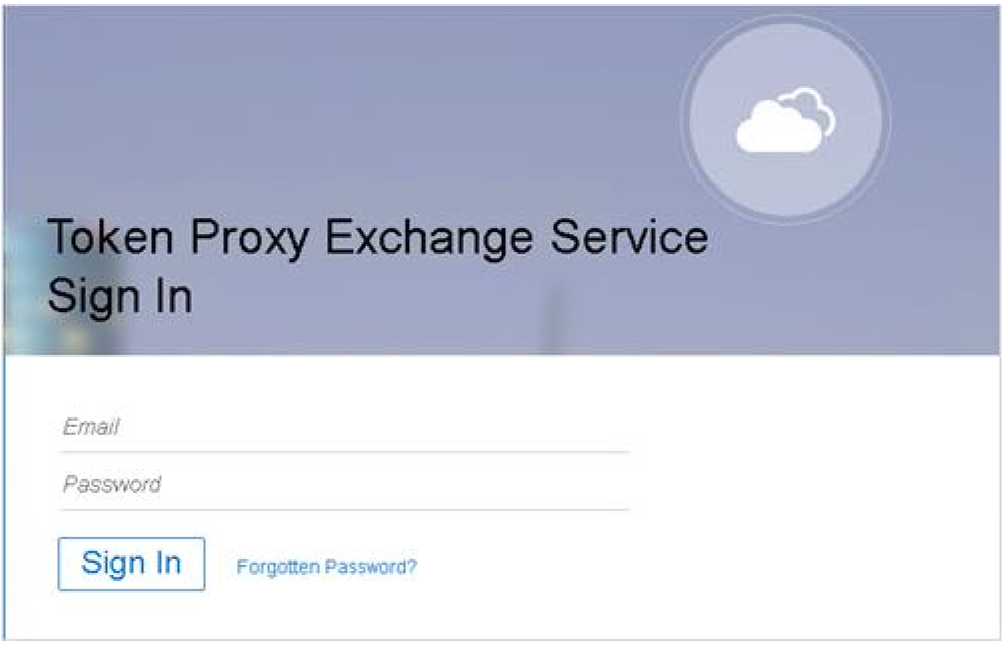
3. Enter the **Password** and confirm it.
4. Click **Reset Password** to reset the password.

   The passwords must be at least 8 characters in length and contain:

   - One upper case letter
   - One lower case letter
   - One number
   - One special character from the list: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` | ~

   > **Note:**
   >
   > The default password expiry date is 180 days and all passwords need to be reset before they expire.

5. Once the Admin user chooses the new password, then you are navigated to the **Token Proxy Exchange Service Sign In** page.



Token Proxy Exchange Service Sign In

6. Enter your **Email** address and **Password** to login into the Token Proxy Exchange Service home page.

   Forgotten Password allows you to choose a new password. Click **Forgotten Password**, this navigates to **Token Proxy Exchange Service Sign In** page where you need to enter your email address used to login to your Token Proxy service account. Click **Reset Password**. An email is sent that contains a link to change your password. Repeat steps 2 through 4 to choose the new password.

5

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.

Update User Profile

You can update your user profile once you login to the Token Proxy Service Web Portal home page.

1. On the top right corner of the **TPS** home page, click **User Name**, and then select Update Profile to update the user information.
2. Make necessary changes to **First Name** or **Last Name** and click **Update** to update the User Information.

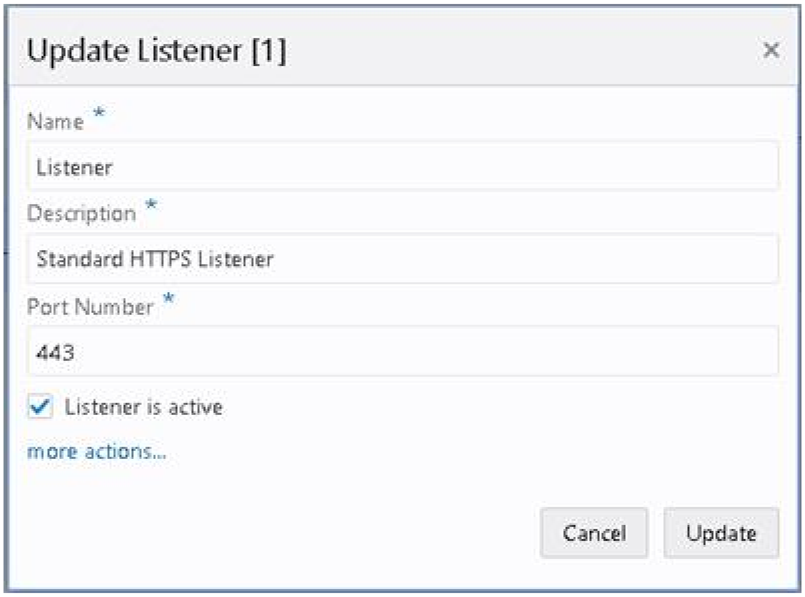
   You cannot update the email address as it is read only.
3. You can update your password by providing the **Old Password**, **New Password** and **Confirm Password**. Click **Update Password** to update the password details.

Listeners

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

Updating the Listener

On the **TPS** home page, click **Listeners** tab, and then select the appropriate Listener record to update. Make necessary changes and click **Update** to update the Listener details. All Listeners records are hardcoded to use a certificate named OPI_Listener.pfx.



Update Listener [1]

Name *

Listener

Description *

Standard HTTPS Listener

Port Number *

443

☑ Listener is active

- Click more actions and then click Delete to delete a Listener configuration. A confirmation pop-up window appears, click Yes to proceed with the deletion and No to discard the process.

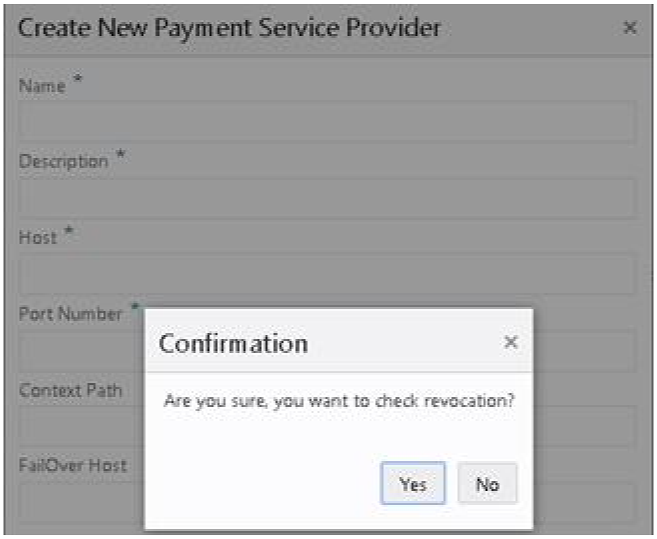
The following are the actions that can be performed for Listeners:

- **Create New Listener**: This action helps you to create new listener details by providing the **Name**, **Description** and **Port Number**. Select **Listener is active** option to make the Listener active.
- **Search Listeners**: This action helps you to search listeners by providing either **Name** or **Port Number**.
- **Show active listeners**: Select this option to lists all active listeners.
- **Show Inactive listeners**: Select this option to lists all inactive listeners.
- **Show all listeners**: Select this option to lists all active and inactive listeners.

Creating and configuring PSPs

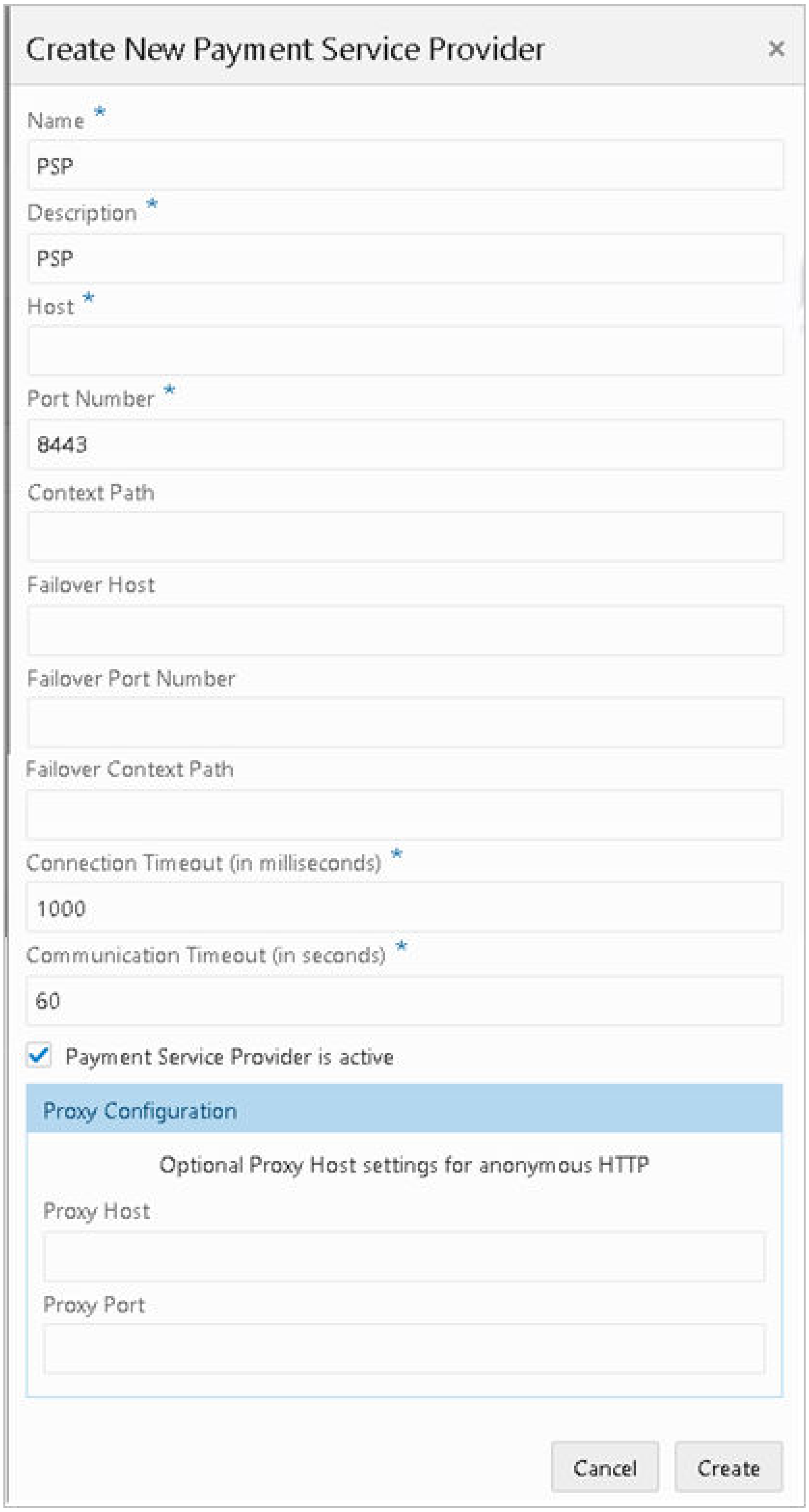
Revocation Check

Certificate Revocation check is an important security feature that should be enabled at all times wherever possible in a production environment. By default, new PSP records are created with a Revocation check enabled for the certificates that PSP provides for TPS to communicate with them. On the confirmation pop-up window, click **Yes** to enable Revocation check. The **Revocation Check** option is only visible while updating a PSP, not when creating a new PSP.



Are you sure, you want to check revocation?

1. On the **TPS** home page, click **Payment Service Providers** tab.
2. On the **Payment Service Providers** home page, click **Create New Payment Service Provider**.
3. Enter the **Name** and **Description**.
4. **Host**: Enter the URL provided by the partner. For example if the URL provided by the partner is https:// myhost.us.example.com:port/token.do, then enter only myhost.us.example.com in the host field and do not append https://.
5. **Port Number**: Enter the port number to connect to the partner. For example: 8788.
6. **Context Path**: Enter the context path provided by the partner if any.
7. Enter the PSP’s **Failover Host**, **Failover Port Number** and **Failover Context Path** if the PSP has failover services available.
8. **Connection Timeout (in milliseconds)**: The number of milliseconds TPS will wait when initiating a connection to the PSP Host before timing out.
9. **Communication Timeout (in seconds)**: The number of seconds TPS will wait for a response from the PSP Host before timing out.
10. Select the **Payment Service Provider is active** option to allow the PSP to be chosen when creating a client.
11. Enter the **Proxy Host** and **Proxy Port** details if the outbound access to the PSP should go via a proxy. These details are optional proxy host settings for anonymous HTTP.
12. Click **Create**.
13. 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 **Payment Service Provider is active** option to set a PSP to inactive status.



Create New Payment Service Provider ×

Name *
PSP

Description *
PSP

Host *

Port Number *
8443

Context Path

Failover Host

Failover Port Number

Failover Context Path

Connection Timeout (in milliseconds) *
1000

Communication Timeout (in seconds) *
60

☑ Payment Service Provider is active

Proxy Configuration

Optional Proxy Host settings for anonymous HTTP

Proxy Host

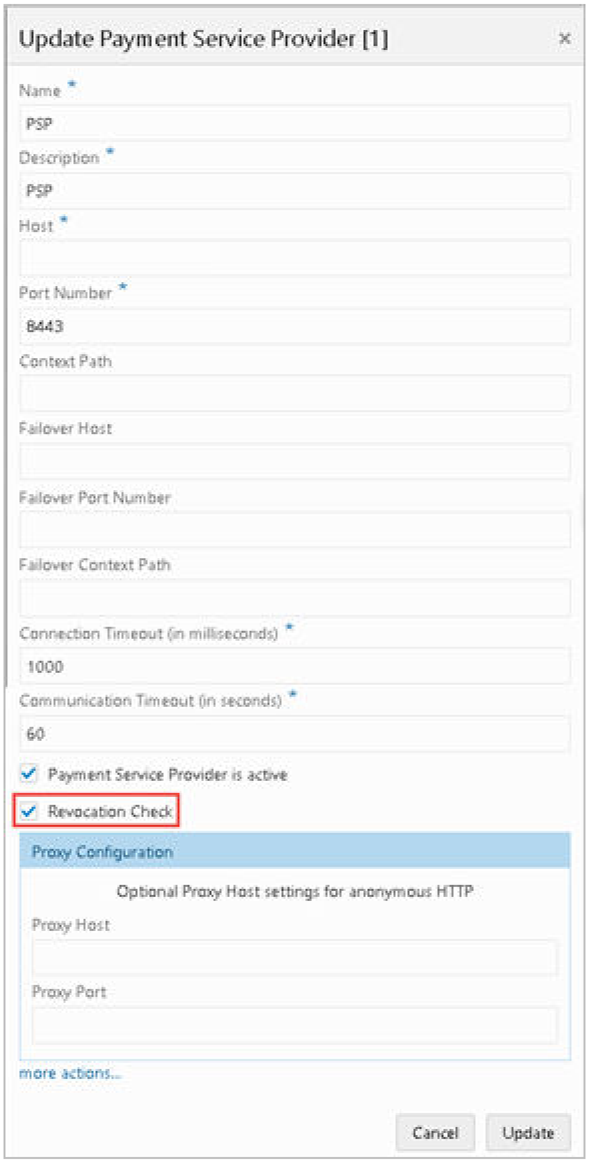
Proxy Port

Updating PSPs

The **Revocation Check** option is only visible while updating a PSP, not when creating a new PSP, as 'Revocation Check' should always be enabled by default. However some of the PSP's are unable to support certificate revocation due to their infrastructure. In these limited cases, the certificate 'Revocation Check' option can be disabled via the PSP configuration page in the TPS webportal.

The **Revocation Check** option should only be disabled where implicitly instructed to do so by the PSP.

1. On the **Payment Service Providers** home page, select the appropriate PSP record you want to update.
2. Make necessary changes and click **Update** to update the PSP details.



Update Payment Service Provider [1]

Name *
PSP

Description *
PSP

Host *

Port Number *
8443

Context Path

Failover Host

Failover Port Number

Failover Context Path

Connection Timeout (in milliseconds) *
1000

Communication Timeout (in seconds) *
60

☑ Payment Service Provider is active

☑ Revocation Check

Proxy Configuration

Optional Proxy Host settings for anonymous HTTP

Proxy Host

Proxy Port

more actions...

Deleting PSPs configuration

1. On the **Payment Service Providers** home page, select the appropriate PSP record you want to delete.

2. Click **more actions** and then click **Delete** to delete a PSP configuration. A confirmation pop-up window appears, click **Yes** to proceed with the deletion and **No** to discard the process.

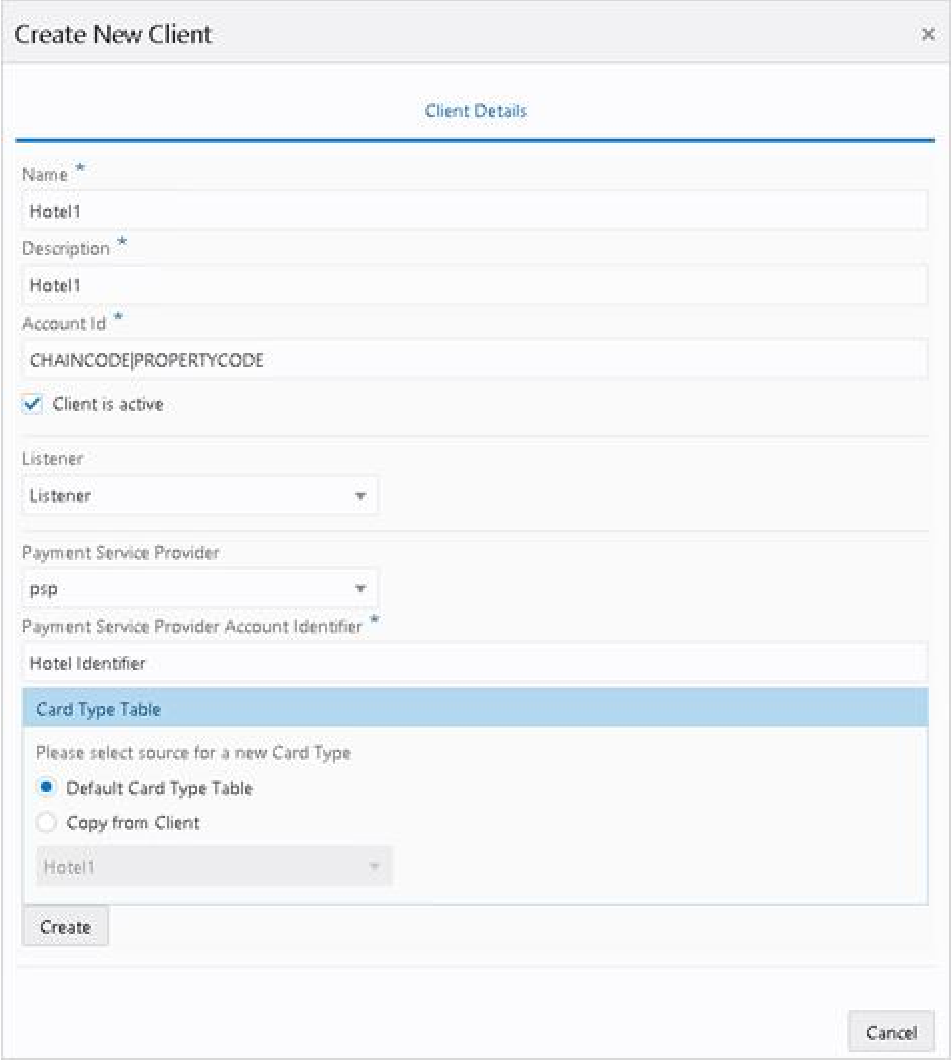
Additional feature of PSPs

The following are the actions that can be performed for Payment Service Providers:

- **Search PSPs**: This action helps you to search PSPs by providing either **Name** or **Port Number**.
- **Show active PSPs**: Select this option to lists all active PSPs.
- **Show Inactive PSPs**: Select this option to lists all inactive PSPs.
- **Show all PSPs**: Select this option to lists all active and inactive PSPs.

Configuring Clients

1. On the **TPS** home page, click **Clients** tab.
2. On the **Clients** home page, click **Create New Client**.
3. Enter the client **Name** and **Description**.
4. The **Account ID** should be set as the Oracle Hospitality OPERA PMS **CHAINCODE and PROPERTYCODE**.
5. Select a **Listener**. The client accepts incoming tokenization requests from the Listener.
6. Select a **Payment Service Provider**. The client forwards tokenization requests to the PSP.
7. The PSP uses the **Payment Service Provider Account Identifier** to uniquely identify client tokenization requests. It is recommended the **PSP Account Identifier** should be set same as the **Account ID** value, for continuity where client chains have some properties communicating with a PSP's tokenization solution via On Premise 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.
8. 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.
9. Select the **Active** option to activate the client account.
10. Click **Create**



Create New Client

Client Details

Name *

Hotel1

Description *

Hotel1

Account Id *

CHAINCODE|PROPERTYCODE

☑ Client is active

Listener

Listener

Payment Service Provider

psp

Payment Service Provider Account Identifier *

Hotel Identifier

Card Type Table

Please select source for a new Card Type

● Default Card Type Table

○ Copy from Client

Hotel1

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

1. On the **Clients** home page, select the appropriate Client record you want to update.
2. Click **Client Details** subtab.
3. Make necessary changes and click **Update** to update the client details.
   - Always restart the OPI Token Service after creating or changing a client.
   - Deselect the **Active** option to set a client to inactive status.

Deleting Clients

1. On the **Clients** home page, select the appropriate Client record you want to delete.
2. Click **Client Details** subtab
3. Click more actions and then click **Delete** to delete a client. A confirmation pop-up window appears, click **Yes** to proceed with the deletion and **No** to discard the process.

Client Credentials

You can create the client credentials once the client details are created.

1. On the **Clients** home page, select the appropriate Client record you want to create client credentials.
2. Click **Client Credentials** subtab.
3. Enter the **Username** and **Password**, the client system should use to authenticate with the Token Proxy Service. The Username must be unique.

   The passwords must be at least 8 characters in length and contain:

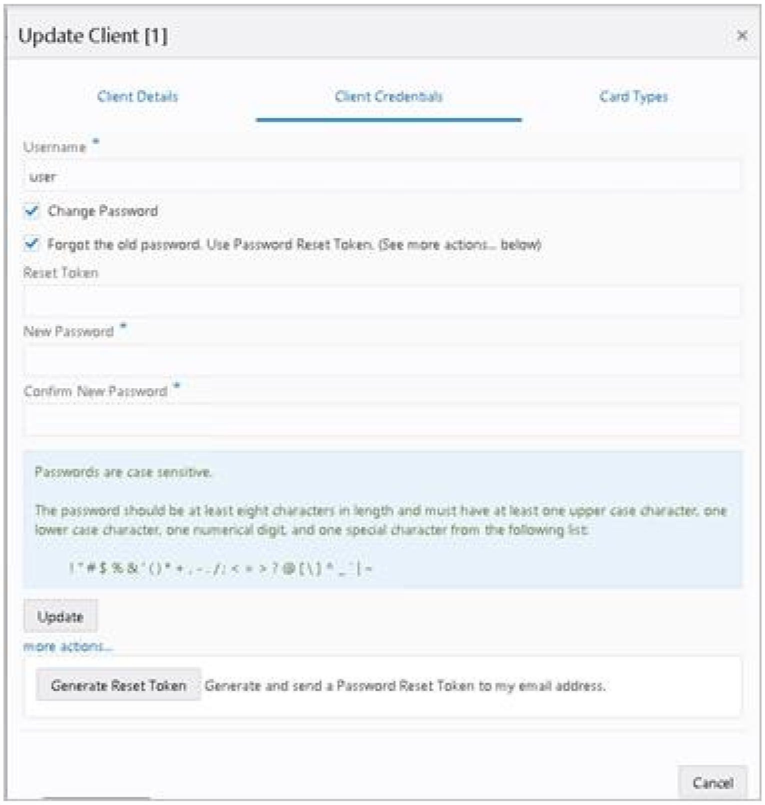
   - One upper case letter
   - One lower case letter
   - One number
   - One special character from the list: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` | ~

   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. Click **Create**.

Update Client Credentials

1. On the **Clients** home page, select the appropriate Client record you want to update client credentials.
2. Click **Client Credentials** subtab.
3. Update the **Username**, **Old Password** , **New Password** and **Confirm New Password**.

   If you have forgotten the old password, then you can reset your password by selecting the **Forgot the old password**. **Use Password Reset Token** option. Click more actions and then click **Generate Reset Token**. A token is sent to your email address. You can use this code provided in the email to reset the basic authorization credentials password. Copy the reset code and paste it in the **Reset Token** field.



Username *

user

☑ Change Password

☑ Forgot the old password. Use Password Reset Token. (See more actions... below)

Reset Token

New Password *

Confirm New 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 lower case character, one numerical digit, and one special character from the following list:

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

Generate and send a Password Reset Token to my email address.

4. Click **Update** to update the username, or the username and password.

Card Type

The Card Type page allows you to manage the IssuerId or Card Type mappings for each Client. It is a tab on the **Client details** page.

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

Card Type Mapping

- **Issuer ID**: Select the value from Table 5-1 – 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 **Clients** home page, select the appropriate Client record you want to update a card type.
2. Click **Card Types** subtab.
3. Select the relevant Card Type record you want to update.
4. Amend the details as required, click **Update**.

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 **Clients** home page, select the appropriate Client record you want to create a new card type.
2. Click **Card Types** subtab.
3. Enter the **Issuer Id**, **Client Card Type** and **Description** as required.
4. Click **Create New Card**.

> **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.

Table 5-1 Card Types

VA	01	VISA
VS	01	VISA

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

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

Table 5-2 Master Card Type

MC	02	MasterCard
MC	24	MasterCard Debit

Deleting a Card Type

1. On the **Clients** home page, select the appropriate Client record you want to remove a card type.

2. Click **Card Types** subtab.
3. Select the relevant Card Type record you want to delete and then click **more actions** and then click **Delete** to delete a card type. A confirmation pop-up window appears, click **Yes** to proceed with the deletion and **No** to discard the process.

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 5-3 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
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
ZZ	25	WeChatPay
ZZ	26	AliPay

The OPI specification also defines ‘IssuerID’s 31 to 45 for local use, these are not included in the ‘Default Card Type Table’ but are valid ID’s that can be configured manually where clients have configured local card types.

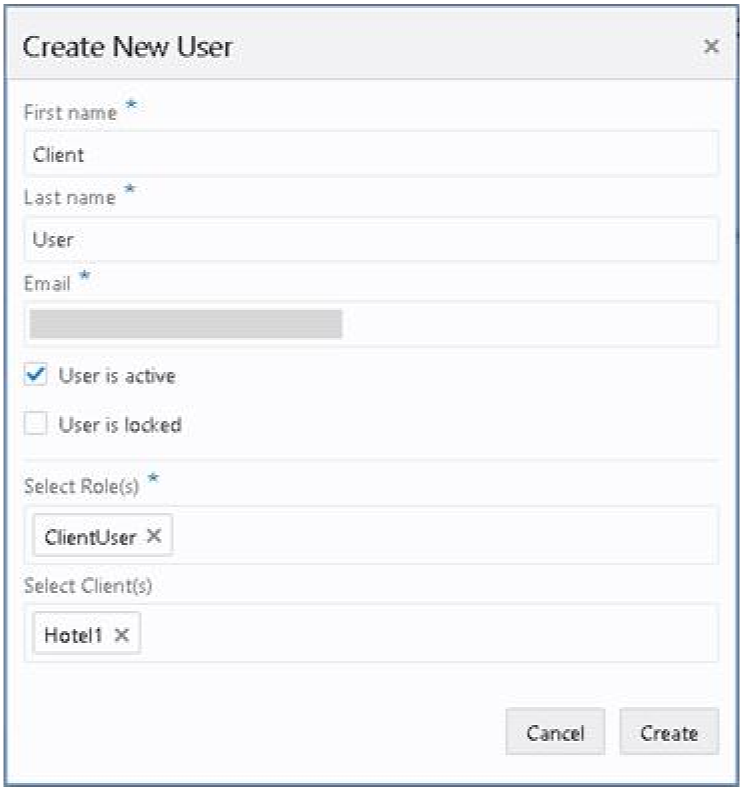
Additional features for Clients

The following are the actions that can be performed for Clients:

- **Search Clients**: This action helps you to search client information by providing the client **Name**.
- **Show active clients**: Select this option to lists all active clients.
- **Show Inactive clients**: Select this option to lists all inactive clients.
- **Show all clients**: Select this option to lists all active and inactive clients.

Creating Additional Users

1. On the **TPS** home page, click **Users** tab.
2. On the **Users** home page, click **Create New User**.
3. **First name**: First name of the new User.
4. **Last name**: Last name of the new User.
5. **Email**: Email address of the new User. The password reset email is sent to this email address.
6. **User is active**: Select this option to activate the user account.
7. **User is locked**: System administrator may need to uncheck this option if a user cannot log in to the system.
8. Select the required **Role** for the new User. The Token Proxy Configuration Portal includes the following two predefined Roles:
   a. **System Administrator**: Can view all pages within the Web Portal.
   b. **Client User**: Can only view the Home Page and the Client System Configuration pages to which the user has been assigned.
9. Select the **Clients** from the available list.
10. Click **Create User**.



Create New User ×

First name *

Client

Last name *

User

Email *

[redacted]

☑ User is active

□ User is locked

Select Role(s) *

ClientUser ×

Select Client(s)

Hotel1 ×

Updating Users

1. On the **Users** home page, select the appropriate User record you want to update.
2. Make necessary changes and click **Update** to update the user details.

Deleting Users

1. On the **Users** home page, select the appropriate User record you want to delete.
2. Click **more actions** and then click **Delete** to delete a user. A confirmation pop-up window appears, click **Yes** to proceed with the deletion and **No** to discard the process.

Additional features for Users

The following are the actions that can be performed for Users:

- **Search Users**: This action helps you to search user information by providing the **First Name**, **Last Name** or **Email**.
- **Show active users**: Select this option to lists all active users.
- **Show Inactive users**: Select this option to lists all inactive users.
- **Show all users**: Select this option to lists all active and inactive users.

Audit

The Token Proxy Service includes an Audit function to keep track of any configuration updates. Only System Administrators can view the Audit information. The System Administrator should login to the Token Proxy Service Configuration Web Portal and click **Audits** tab.

Audit Search

Use the available filters to narrow the search criteria as required.

- **Start Date** – Enter the date to search from in the format dd-mm-yyyy, or click the calendar icon

  📅

  and select the required date.
- **End Date** – Enter the date to search up to in the format dd-mm-yyyy, or click the calendar icon

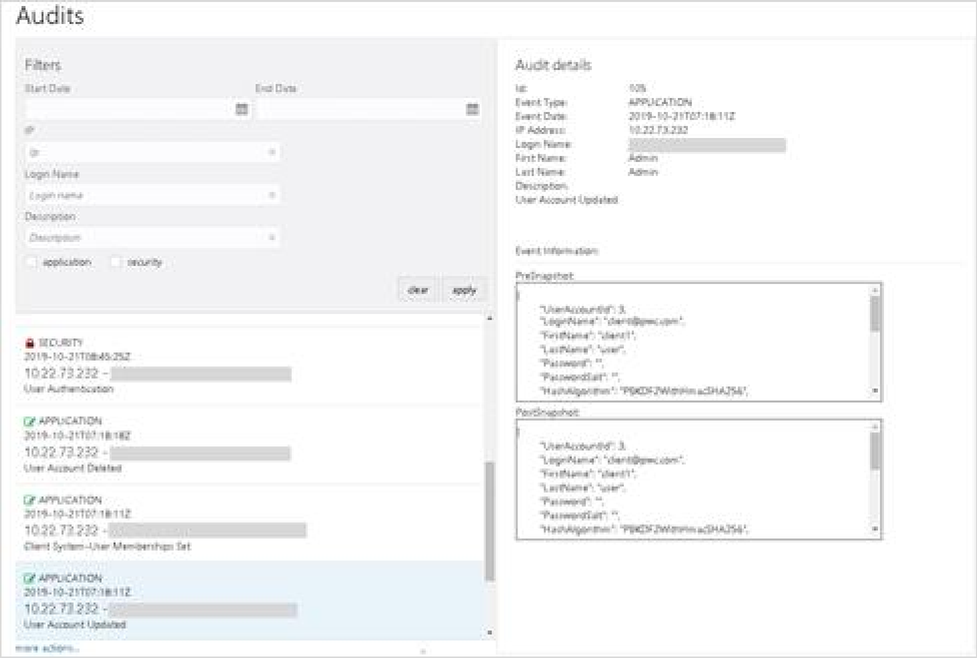
  📅

  and select the required date.
- **IP** – Events containing the IP Address value entered.
- **Login Name** – Events containing the login name value entered.
- **Description** – Events containing the Description value entered.
- **Event type**;
  - Application – Configuration related events
  - Security – User account related events

Click **Apply** to display the relevant Audit details.

By default, the search results are displayed in descending **Event Time** order. To view details of a particular event, click the **Event Type** on the relevant row.

Depending on the event type, you may see additional information in the **Pre-snapshot** and **Post-snapshot** fields, showing the before and after values, if the event was a configuration update.



SECURITY
2019-10-21T08:45:25Z
10.22.73.232 - [redacted]
User Authentication

APPLICATION
2019-10-21T07:18:18Z
10.22.73.232 - [redacted]
User Account Deleted

APPLICATION
2019-10-21T07:18:11Z
10.22.73.232 - [redacted]
Client System–User Memberships Set

APPLICATION
2019-10-21T07:18:11Z
10.22.73.232 - [redacted]
User Account Updated

Id:	105
Event Type:	APPLICATION
Event Date:	2019-10-21T07:18:11Z
IP Address:	10.22.73.232
Login Name:	[redacted]
First Name:	Admin
Last Name:	Admin

Description:
User Account Updated

PreSnapshot:

```
{
    "UserAccountId": 3,
    "LoginName": "client@pwc.com",
    "FirstName": "client1",
    "LastName": "user",
    "Password": "",
    "PasswordSalt": "",
    "HashAlgorithm": "PBKDF2WithHmacSHA256",
```

PostSnapshot:

```
{
    "UserAccountId": 3,
    "LoginName": "client@pwc.com",
    "FirstName": "client1",
    "LastName": "user",
    "Password": "",
    "PasswordSalt": "",
    "HashAlgorithm": "PBKDF2WithHmacSHA256",
```

Manage Audits

System Administrator can export records in Excel format and also purge any Audit events that are older than 90 days.

- On the **Audits** page, click **more actions** at the bottom of the page to export and purge Audit records.
- **Export**
  - Select **Export all records** option and then click **Export** to export all records in Excel format.
  - Select **Export filtered records** option and then click **Export** to export only the filtered records in Excel format.
- **Purge**
  - Enter the date in the format dd-mm-yyyy, or click the calendar icon

    📅

    and select the required date and then click **Purge** to purge any Audit events that are older than 90 days.

6

Upgrading the TPS

VERY IMPORTANT: Read and follow the upgrade directions.

> **Note:**
>
> - TPS 6.1 can be upgraded to TPS 19.2.
> - Make sure that the Admin and the target web server are in running state.

TPS DemoIdentity Upgrade

The demo identity certificates that are deployed by default with the installation of WebLogic should have been replaced during installation to enhance the security of your environment. The demo identity certificates that are deployed by default with the installation of WebLogic should have been replaced during installation to enhance the security of your environment. If self-signed certificates were deployed to your WebLogic instance during installation, you will have to rollback your WebLogic to trust the DemoIdentity in order for the upgrade installer to use WLST to connect to the WebLogic admin server in order that it can apply any required updates.

If you deployed CA signed certificates to your WebLogic instance during installation, depending on how your CA signed certificates were signed, your connection may be trusted by the JavaStandardTrust keystore, and therefore WLST should be able to connect to the WebLogic admin server. If your CA signed certificates are not trusted by the JavaStandardTrust keystore, then you would also have to rollback your weblogic to trust the DemoIdentity certificates in order for the installer to use WLST to connect to the WebLogic admin server in order that it can apply any required updates.

Alternatively, you may want to update the deployments in WebLogic manually.

Restoring Weblogic DemoIdentity Certificates

- Make sure you have the details of your certificates, as these will need to be reinstated again after the update process has been completed.
- Login to your WebLogic's admin console.
- Navigate to the **Environment | Servers** tab.
- Select the AdminServer.
- Navigate to the **Keystores** tab.
- Select **'Lock and Edit'** the configuration.

- Select the **'Change'** option and select the **'Demo Identity and Demo Trust'** option from the list.
- **'Save'** your changes, and **'Release Configuration'**.
- Restart the wls admin server.
- Once the update has completed successfully restore your certificates using the Cert Manager in the normal way.

Manual Deployment/UnDeployment on Weblogic

If you want to manually update the Weblogic deployments, you must first manually undeploy the existing deployments.

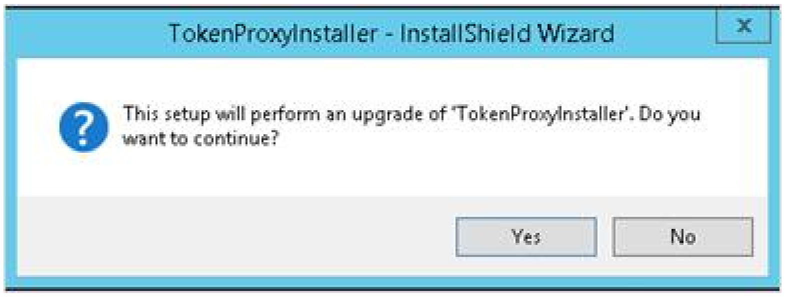
If you are upgrading from TPS 6.1 there was only one deployment in this version.

- Login to your WebLogic's admin console.
- Navigate to the **Environment | Deployments** tab.
- Select **'Lock and Edit'** the configuration.
- Select the tickbox next to the 'token-proxy-webportal' deployment.
- Select **'Delete'** to remove the deployment.
- Select **'Yes'** to confirm the deletion of the deployment.
- Select **'Activate Changes'**.

Installation of the new Deployments will be as per the steps listed in the section 'Manual Deployment on WebLogic'.

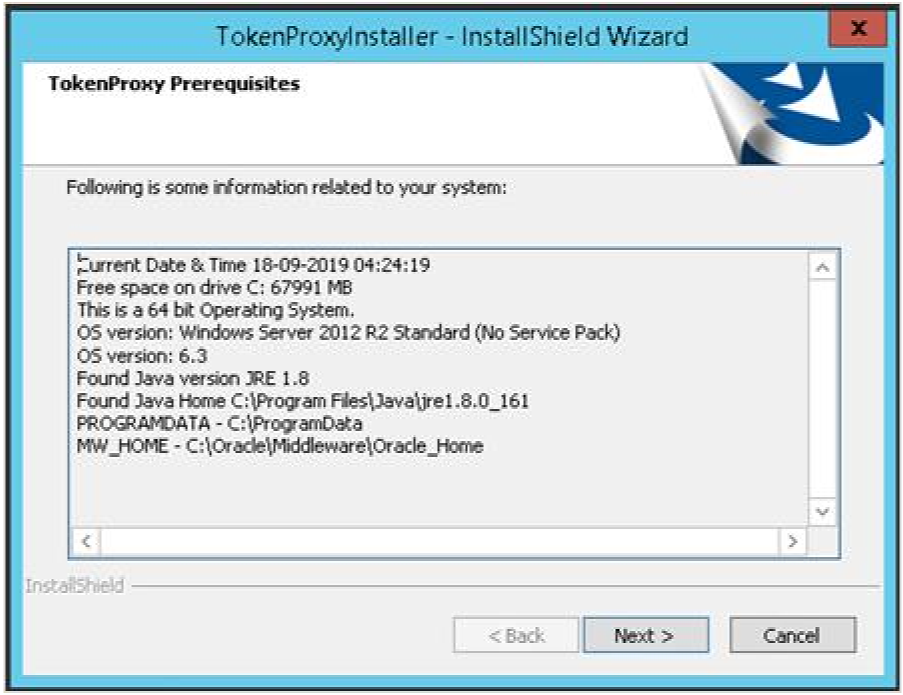
Upgrading TPS 6.1 to 19.2

1. Right-click **TokenProxyInstaller_19.2.0.0.exe** file and select **Run as Administrator** to perform an upgrade.
2. Click **Yes** to perform an upgrade of Token Proxy Installer installation.


TokenProxyInstaller - InstallShield Wizard

This setup will perform an upgrade of 'TokenProxyInstaller'. Do you want to continue?

3. Click **Next** to proceed with the installation.
4. Ensure all the prerequisites for the Token Proxy installation are met.



Following is some information related to your system:

```
Current Date & Time 18-09-2019 04:24:19
Free space on drive C: 67991 MB
This is a 64 bit Operating System.
OS version: Windows Server 2012 R2 Standard (No Service Pack)
OS version: 6.3
Found Java version JRE 1.8
Found Java Home C:\Program Files\Java\jre1.8.0_161
PROGRAMDATA - C:\ProgramData
MW_HOME - C:\Oracle\Middleware\Oracle_Home
```

5. Click **Next**.

   The installer updates the Token Proxy Service from 6.1 to 19.2.

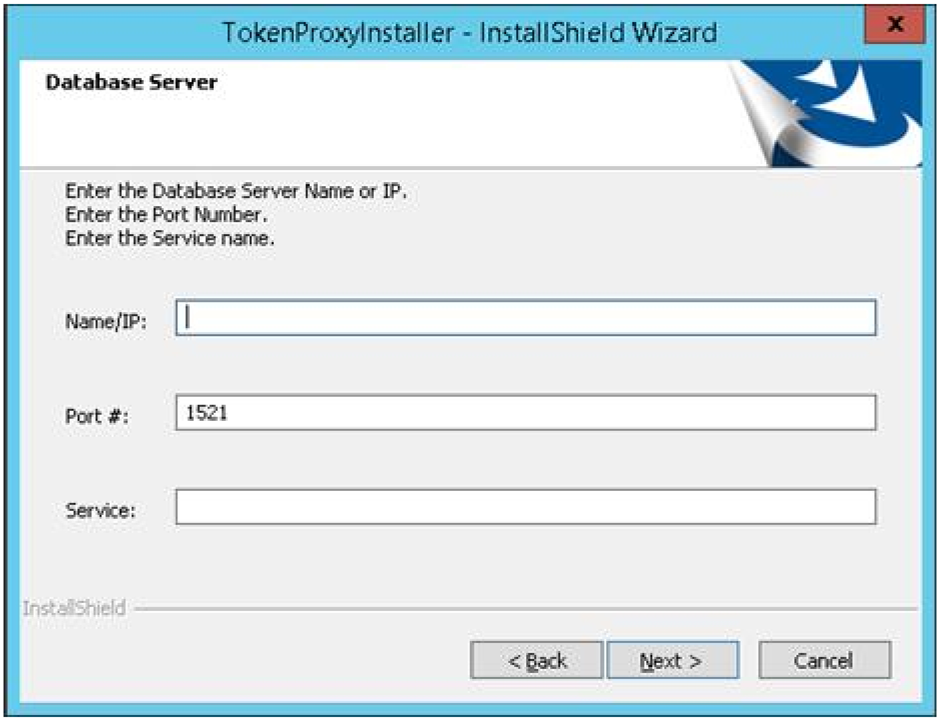
   > **Note:**
   >
   > By default the installer checks which components are installed for TPS 6.1 then the installer upgrades it accordingly.
   >
   > - If you have performed **'Complete'** installation for TPS 6.1, then it upgrades all the three components.
   >   - Database
   >   - Token Proxy Web Portal
   >   - Token Proxy Service.
   > - If you have performed **'Custom'** installation for TPS 6.1, then it upgrades only the selected components.
   > - As the TPS 6.1 installer supports only Oracle database, so the upgradation for TPS 19.2 is allowed only with Oracle database.

6. Enter the following credentials to allow the Token Proxy Service installer to connect to your Oracle 12c/19c database.

   a. **Name/IP**: The Hostname or IP Address used for communication to the database.

   b. **Port #**: The Port number used for communication to the database.

   c. **Service Name**: The service name used to connect to the Oracle database.



TokenProxyInstaller - InstallShield Wizard

Database Server

Enter the Database Server Name or IP.
Enter the Port Number.
Enter the Service name.

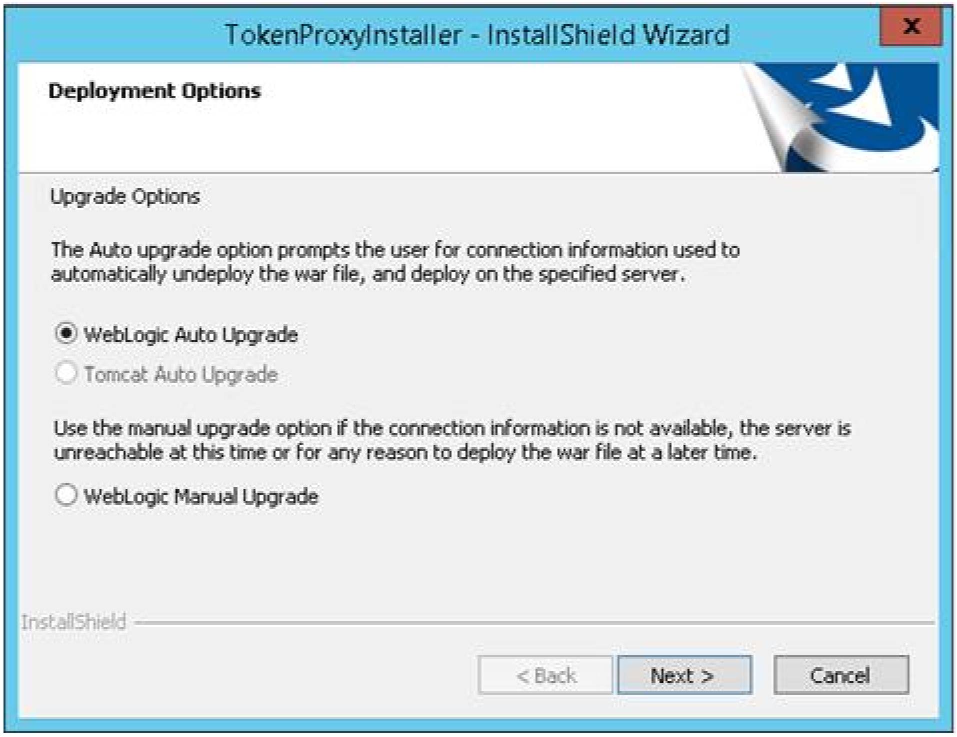
Name/IP:

Port #: 1521

Service:

7. Click **Next**.
8. Enter the existing TPS **Database User Name** and **Password**.
9. Click **Next**.
   - The installer attempts to connect to the database using the DBA credentials provided. 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 starts the PatchDB update and upgrades the database component.
   - On the **Data Upgrade Tools Results** screen, click **Next**.
10. On the **Deployment Options** screen, select any of the upgrade option to undeploy the existing war file and deploy the new war and jar files on the server.
    - **WebLogic Auto Upgrade**: Select this option to automatically undeploy the existing war file and deploy the new war and jar files on WebLogic. Please follow the below steps 11 through 19 for an auto upgrade.
    - **WebLogic Manual Upgrade**: Select this option only if the connection is not available. In this case you have to undeploy the existing war files manually and deploy the new war and jar files by selecting form your machine.
      - If manual upgrade is selected, then installer retrieves the deployment files in C:\ProgramData\TokenProxy.
      - The installer successfully updates the configuration file.
      - The installer successfully upgrades the Token Proxy Service.
      - The installer attempts to delete the Utilities from the Token Proxy Service.
      - The installer completes the update of the Token Proxy Service installer to 19.2.

- You can deploy two .WAR files (token-proxy-restapi.war, token-proxy-ui.war) and a .JAR file (tokenproxy-headers-filter.jar) on WebLogic manually. The war and jar files are available at C:\ProgramData\TokenProxy directory. Refer to Manual Deployment on WebLogic section for more details.



TokenProxyInstaller - InstallShield Wizard

Deployment Options

Upgrade Options

The Auto upgrade option prompts the user for connection information used to automatically undeploy the war file, and deploy on the specified server.

● WebLogic Auto Upgrade

○ Tomcat Auto Upgrade

Use the manual upgrade option if the connection information is not available, the server is unreachable at this time or for any reason to deploy the war file at a later time.

○ WebLogic Manual Upgrade

11. Click **Next**.
12. On the **WebLogic Connection Settings** screen, enter the following WebLogic Connection Settings. This dialog box does not appear when performing a manual deployment.

    The connection is used to undeploy the Token Proxy Service Web Portal .WAR file from WebLogic and deploy two .WAR files (token-proxy-restapi.war, token-proxy-ui.war) and a .JAR file (tokenproxy-headers-filter.jar) on WebLogic.

    a. **Host**: WebLogic IP address.

    b. **Port**: WebLogic port number.

    c. **Username**: WebLogic user name.

    d. **Password**: WebLogic password.

    e. **Protocol**:

       i. **T3** is the default WebLogic Protocol.

       ii. **T3S** is the T3 Protocol with SSL.

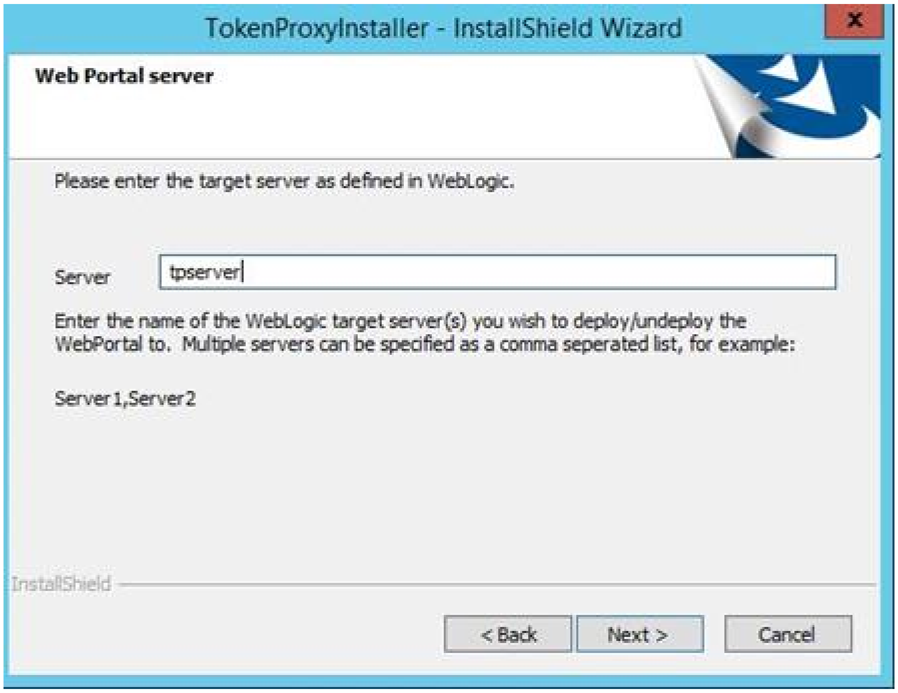
       iii. **HTTP** is T3 wrapped in HTTP to allow routing through firewalls, if required.

       iv. **HTTPS** is T3S wrapped in HTTP to allow routing through firewalls, if required.

    f. **Demo Trust**: Select this option for **T3S** or **HTTPS** when user certificates are not installed while installing the WebLogic.
13. 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 WebLogic Environment.

14. On the **Web Portal server** screen, enter the name of the WebLogic **Server** where you want to undeploy and deploy the new Token Proxy Service Web Portal.
    - 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.



Web Portal server

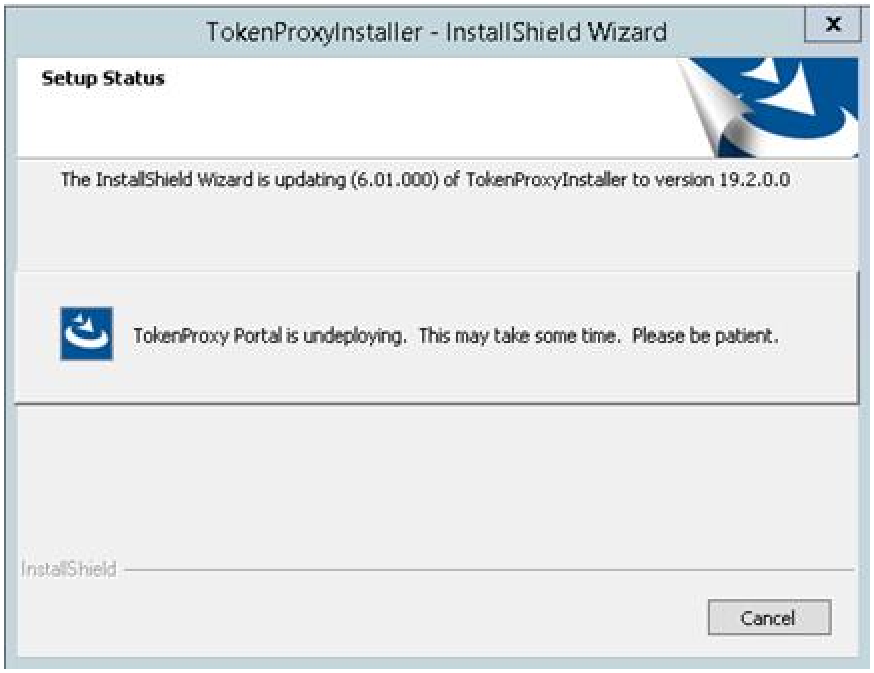
Please enter the target server as defined in WebLogic.

Server: tpserver

Enter the name of the WebLogic target server(s) you wish to deploy/undeploy the WebPortal to. Multiple servers can be specified as a comma seperated list, for example:

Server1,Server2

15. Click **Next**.
    - The Installer successfully updates the configuration file.
    - The Installer attempts to undeploy the Web Portal.



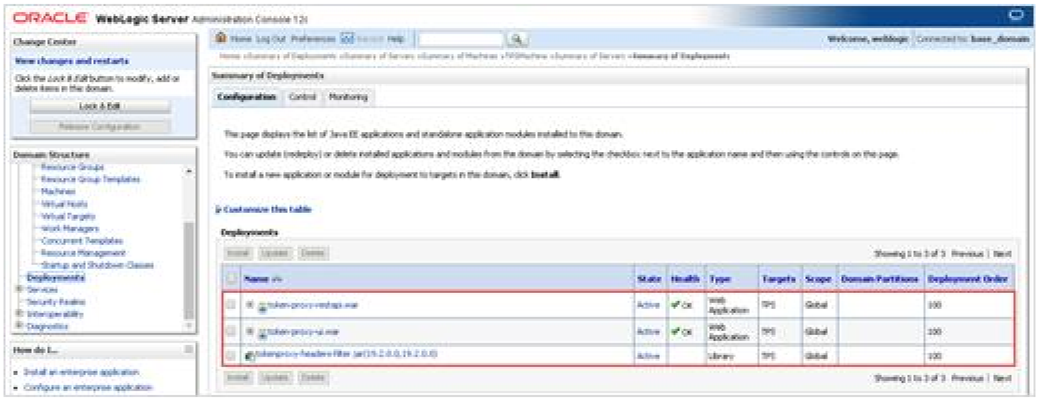
TokenProxyInstaller - InstallShield Wizard

Setup Status

The InstallShield Wizard is updating (6.01.000) of TokenProxyInstaller to version 19.2.0.0

TokenProxy Portal is undeploying. This may take some time. Please be patient.

16. On the **Token Proxy Portal Results** screen, click **Next**.
17. Click **OK**.
    - The Installer initiates the Token Proxy Portal deployment process.
    - The Installer attempts to deploy two .WAR files, and a .JAR file on WebLogic.



Summary of Deployments

Click the Lock & Edit button to modify, add or delete items in this domain.

The page displays the list of Java EE applications and standalone application modules installed to this domain.

You can update (redeploy) or delete installed applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on the page.

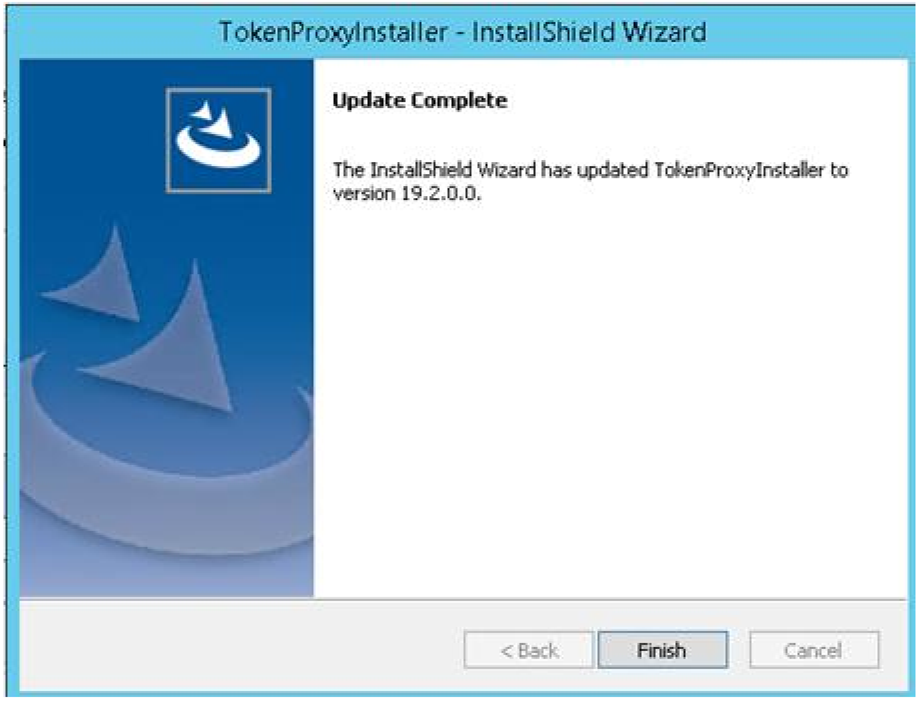
To install a new application or module for deployment to targets in this domain, click **Install**.

Deployments

□	Name	State	Health	Type	Targets	Scope	Domain Partitions	Deployment Order
□	token-proxy-restapi.war	Active	✓ OK	Web Application	TPS	Global		100
□	token-proxy-ui.war	Active	✓ OK	Web Application	TPS	Global		100
□	tokenproxy-headers-filter.jar(19.2.0.0,19.2.0.0)	Active		Library	TPS	Global		100

18. On the **Setup Status** screen, click **OK**.

    The Installer attempts to delete the Utilities from the Token Proxy Service.
19. Click **Finish** to complete the update of the Token Proxy Service installer to 19.2.



Update Complete

The InstallShield Wizard has updated TokenProxyInstaller to version 19.2.0.0.

Note:

The token proxy webportal url is changed from TPS 6.1 to TPS 19.2.

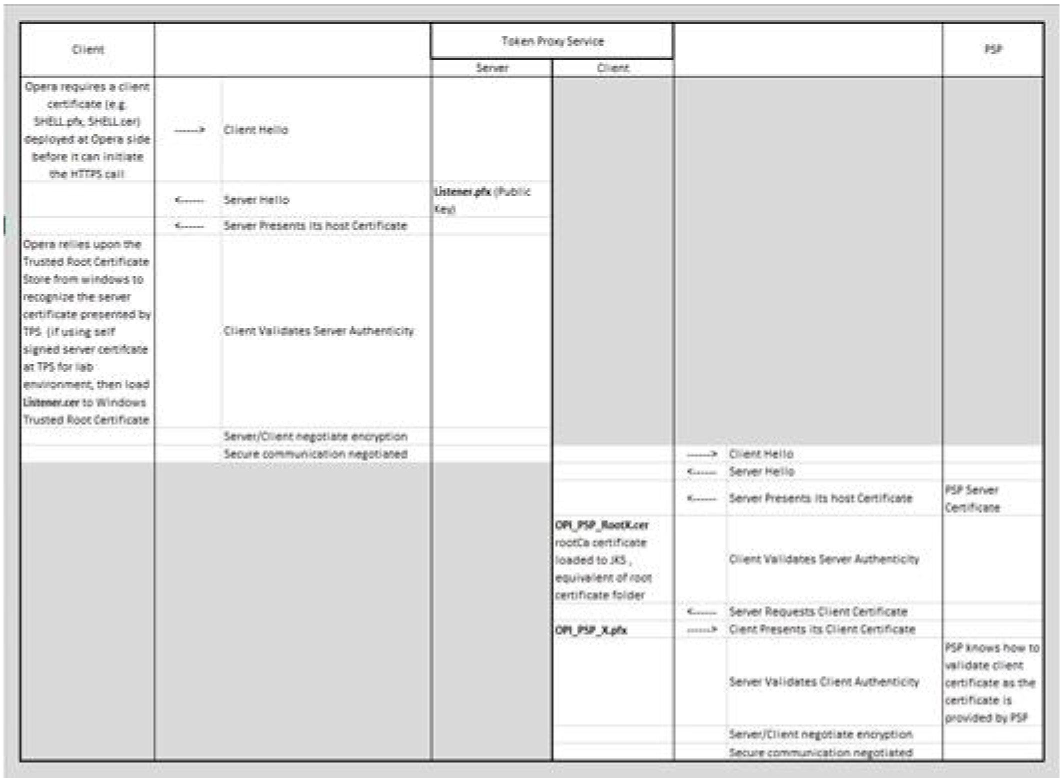
- The users have previously accessed **TPS 6.1** web portal as given below: https://<fqdn>:<port>/token-proxy-webportal
- The **TPS 19.2** upgraded web portal need to be accessed as given below: https://<fqdn>:<port>/token-proxy-ui

7 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.

Important: Please note that a Public SSL certificate is required. If you attempt to install OPI TPS with a self-signed certificate then you will receive a warning.



Client			Token Proxy Service				PSP
			Server	Client			
Opera requires a client certificate (e.g. SHELL.pfx, SHELL.cer) deployed at Opera side before it can initiate the HTTPS call	------->	Client Hello					
	<-------	Server Hello	**Listener.pfx** (Public Key)				
	<-------	Server Presents its host Certificate					
Opera relies upon the Trusted Root Certificate Store from windows to recognize the server certificate presented by TPS. (if using self signed server certificate at TPS for lab environment, then load **Listener.cer** to Windows Trusted Root Certificate		Client Validates Server Authenticity					
		Server/Client negotiate encryption					
		Secure communication negotiated					
					------->	Client Hello	
					<-------	Server Hello	
					<-------	Server Presents its host Certificate	PSP Server Certificate
				OPI_PSP_RootX.cer rootCa certificate loaded to JKS , equivalent of root certificate folder		Client Validates Server Authenticity	
					<-------	Server Requests Client Certificate	
				OPI_PSP_X.pfx	------->	Client Presents its Client Certificate	
						Server Validates Client Authenticity	PSP knows how to validate client certificate as the certificate is provided by PSP
						Server/Client negotiate encryption	
						Secure communication negotiated	

Certificates for Communication between TPS and PSP

In order for TPS to properly trust the PSP Application, it requires two files which will be provided by the PSP.

- The **Public Root certificate** (in the format of the *.cer or *.crt file) of the server certificate deployed on the PSP end.
- The **Client Certificate** file which is to be deployed on the TPS.

- 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).
- The **TPS Certificate Manager tool** can be used to set up the public root of the PSP server certificate into the required key store. Refer to Certificate Requests using Cert Manager section for more details.
- 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. It will be protected by a password.
- The Token Proxy Service Payment Service Provider Certificates are available for both Tomcat and WebLogic.
- The TPS Certificate Manager can also be used to import required certificates into the root certificate files for each PSP configured on a Token Proxy Service.
- It is possible to retrieve the PSP record number from the Token Proxy Service configuration database, and import the selected certificates public key to a keystore it creates with the required file name, and set the password in the TPS wallet, which means this step does not need to be completed with the existing OPIConfigX utility.
- The options will be disabled until database setup has been completed with the OPIConfigX utility.

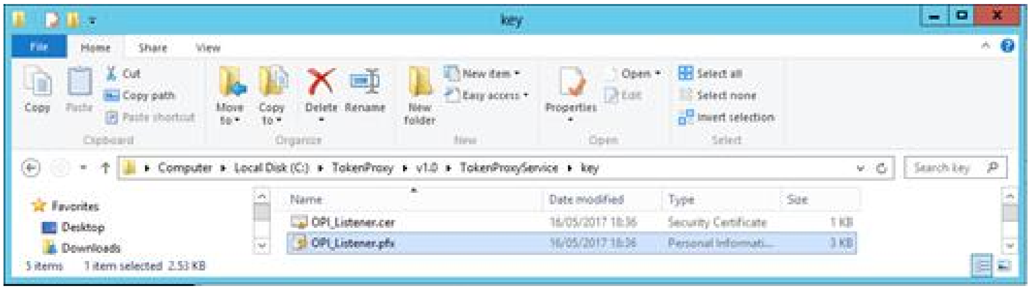
> **Note:**
>
> The Certificates expiration date depends on what is set during initial configuration. You can check the expiration date using tools like: certutil –dump <pfx file>. The certutil tool is a command line tool that comes with Windows OS. You must update the certificates prior to the expiration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

Certificates for Communication between OPERA and TPS

For HTTPS communication between OPERA and the 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 the Token Proxy Service should be a CA signed certificate provided by the third party.

The 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).



Computer ▸ Local Disk (C:) ▸ TokenProxy ▸ v1.0 ▸ TokenProxyService ▸ key

Name	Date modified	Type	Size
OPI_Listener.cer	16/05/2017 18:36	Security Certificate	1 KB
OPI_Listener.pfx	16/05/2017 18:36	Personal Informati...	3 KB

5 items   1 item selected 2.53 KB

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.

Note:

For OPERA software whose version meets the minimum version requirement, the client certificates are not required to be deployed on OPERA side for token exchange functionality. You only need to load the public key for the root of the server certificate (.cer file) on OPERA side if it is not already trusted at OPERA side.

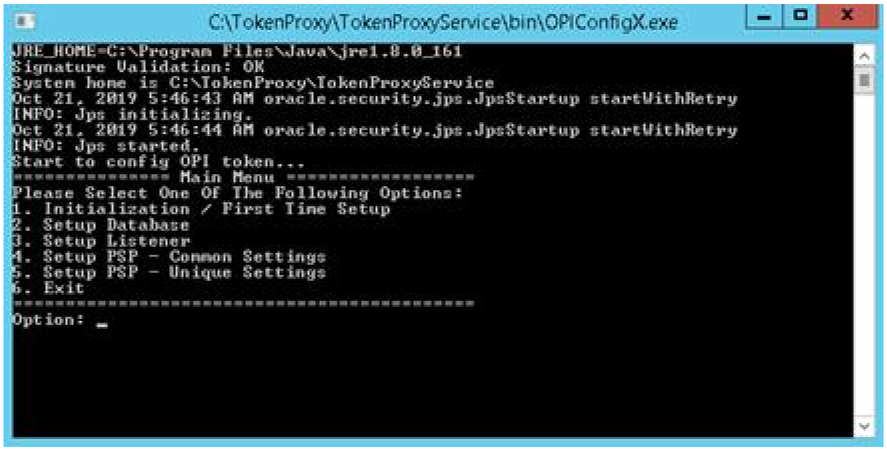
Certificates created with the Certificate Creator tool have a default expiration date of five years from the date of creation. You must update the Token Proxy Service Server Side Certificates prior to the expiration date to avoid downtime to the Token Proxy Service.

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.

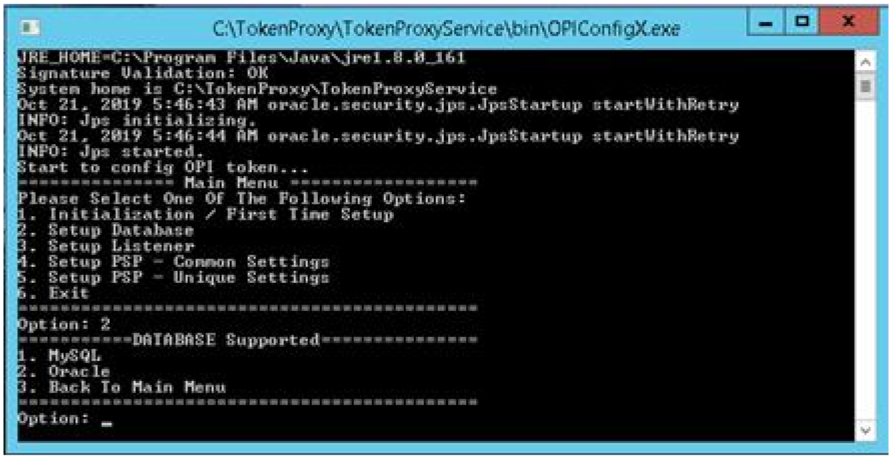
8 OPIConfigX.exe

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 MySQL or 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.

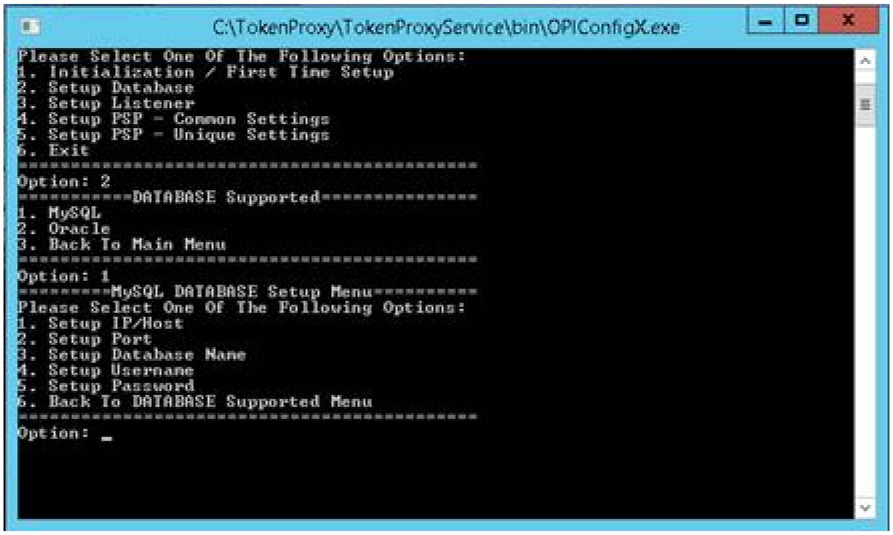


```
JRE_HOME=C:\Program Files\Java\jre1.8.0_161
Signature Validation: OK
System home is C:\TokenProxy\TokenProxyService
Oct 21, 2019 5:46:43 AM oracle.security.jps.JpsStartup startWithRetry
INFO: Jps initializing.
Oct 21, 2019 5:46:44 AM oracle.security.jps.JpsStartup startWithRetry
INFO: Jps started.
Start to config OPI token...
=============== Main Menu ==================
Please Select One Of The Following Options:
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: _
```

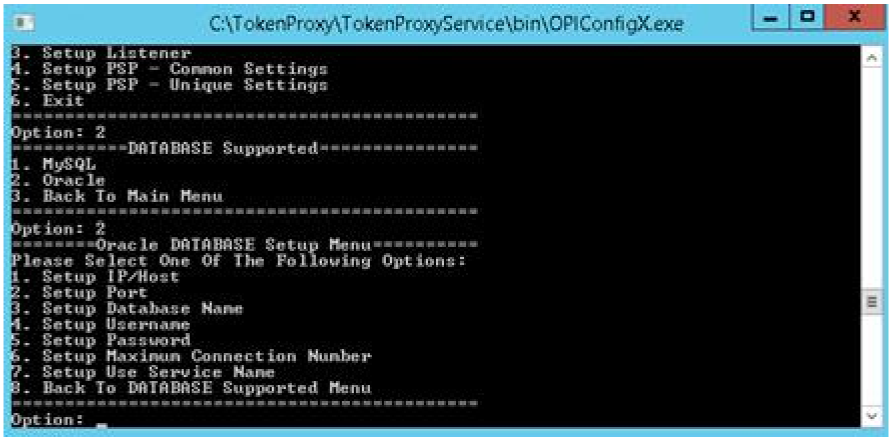


```
JRE_HOME=C:\Program Files\Java\jre1.8.0_161
Signature Validation: OK
System home is C:\TokenProxy\TokenProxyService
Oct 21, 2019 5:46:43 AM oracle.security.jps.JpsStartup startWithRetry
INFO: Jps initializing.
Oct 21, 2019 5:46:44 AM oracle.security.jps.JpsStartup startWithRetry
INFO: Jps started.
Start to config OPI token...
=============== Main Menu ==================
Please Select One Of The Following Options:
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: 2
===========DATABASE Supported===============
1. MySQL
2. Oracle
3. Back To Main Menu
============================================
Option: _
```

- Select either **MySQL** or **Oracle** Database option.



```
Please Select One Of The Following Options:
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: 2
===========DATABASE Supported===============
1. MySQL
2. Oracle
3. Back To Main Menu
============================================
Option: 1
=========MySQL DATABASE Setup Menu==========
Please Select One Of The Following Options:
1. Setup IP/Host
2. Setup Port
3. Setup Database Name
4. Setup Username
5. Setup Password
6. Back To DATABASE Supported Menu
============================================
Option: _
```



```
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: 2
===========DATABASE Supported===============
1. MySQL
2. Oracle
3. Back To Main Menu
============================================
Option: 2
========Oracle DATABASE Setup Menu==========
Please Select One Of The Following Options:
1. Setup IP/Host
2. Setup Port
3. Setup Database Name
4. Setup Username
5. Setup Password
6. Setup Maximum Connection Number
7. Setup Use Service Name
8. Back To DATABASE Supported Menu
============================================
Option: _
```

The below options are available for both MySQL and Oracle Databases:

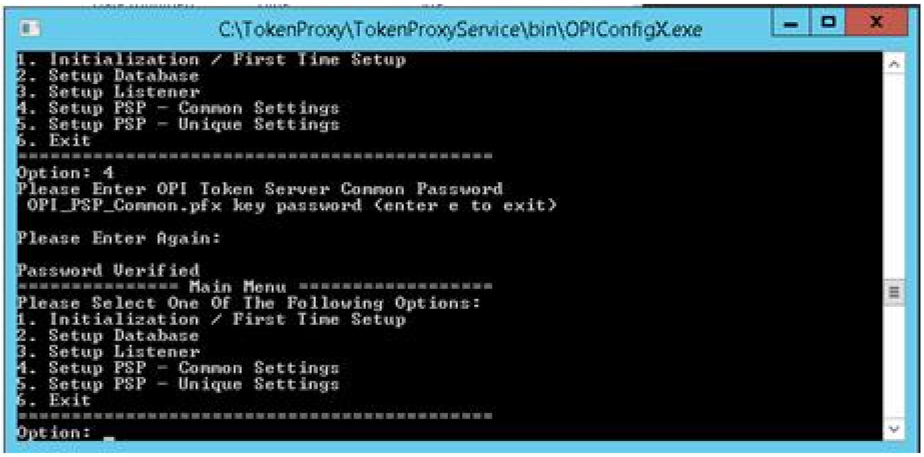
- **Setup IP/Host**: The IP address of the MySQL or Oracle Database.
- **Setup Port**: The port number of the MySQL or Oracle Database.
- **Setup Database Name**: The Token Proxy Service database name created during installation.
- **Setup Username**: The username for the Token Proxy Service database created during installation.
- **Setup Password**: The password for the Token Proxy Service database created during installation.

These two options are available only if you select Oracle Database.

- **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**, **Setup PSP – Common Settings** and **Setup PSP – Unique Settings**: Use certificate manager to set up certificates of the Listener and the

password of the common and unique PSP certificates. Refer to the Certificate Requests using Cert Manager section for more details.



```
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: 4
Please Enter OPI Token Server Common Password
 OPI_PSP_Common.pfx key password (enter e to exit)

Please Enter Again:

Password Verified
================ Main Menu ==================
Please Select One Of The Following Options:
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: _
```

- If the database and PSPs have been configured properly in the Web Portal, then select the number for the PSP certificate password you want to set.

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

9 Certificates Request using Cert Manager

The Listener certificates are to be purchased from a third party certificate authority. The certificate's Common or Alternate name values should match the Hostnames whenever they will be accessed.

Keep in mind that while requesting certificates, you may need separate certificates for backup/failover nodes, or you can be able to request a cert with the common name as the primary host, and the backup/failover nodes in the certificates with alternative name values.

In order to use all of Cert Managers functionality, Cert Manager will need to be deployed on all machines which host WebLogic or Tomcat and the Token Proxy Service. It is not designed to deploy certificates on remote machines. **Cert Manager Tool needs to be run as an administrator**.

In some environments Database, Tomcat or WebLogic and the Token Proxy may reside on the same host, however if your environment has the Database, Tomcat or WebLogic and the Token Proxy on different machines, the Cert Manager will need to be deployed on each host separately.

Cert Manager will check the presence of WebLogic and the Token Proxy on the host, and will restrict certain functionality if it does not find WebLogic or the Token Proxy Service installations.

Cert Manager requires Java to be installed, but since both WebLogic and the Token Proxy Service also requires Java, there should be no additional Java prerequisite to run Cert Manager.

Before Running

To use Cert Manager to deploy your Token Proxy Service certificates, Cert Manager should be able to connect to the Token Proxy Service database, in order to read configuration.

Therefore in a new installation scenario the Token Proxy Service database connection details must be defined before using Cert Manager using the OPIConfigX utility.

Cert Manager performs the similar certificate functions to the OPIConfigX utility, which can also be used if required.

Self-Hosted Token Proxy

Cert Manager is packaged with Self-Hosted Token Proxy, it resides in the TokenProxy folder.

:\TokenProxy\TokenProxyCertManager\certmanager-frontend.jar

Standalone

Cert Manager is also a standalone tool that can be used on existing installations of the Token Proxy. This is available from https://support.oracle.com.

Deploying Cert Manager from an Installed Token Proxy Service to a WebLogic host

In case of separate WebLogic and the Token Proxy Service hosts, where you have the Cert Manager on your Token Proxy Server host as part of the Token Proxy Service installation, but need to transfer it to your WebLogic host(s), you will need to copy the whole TokenProxyCertManager folder to your WebLogic machine.

Logs

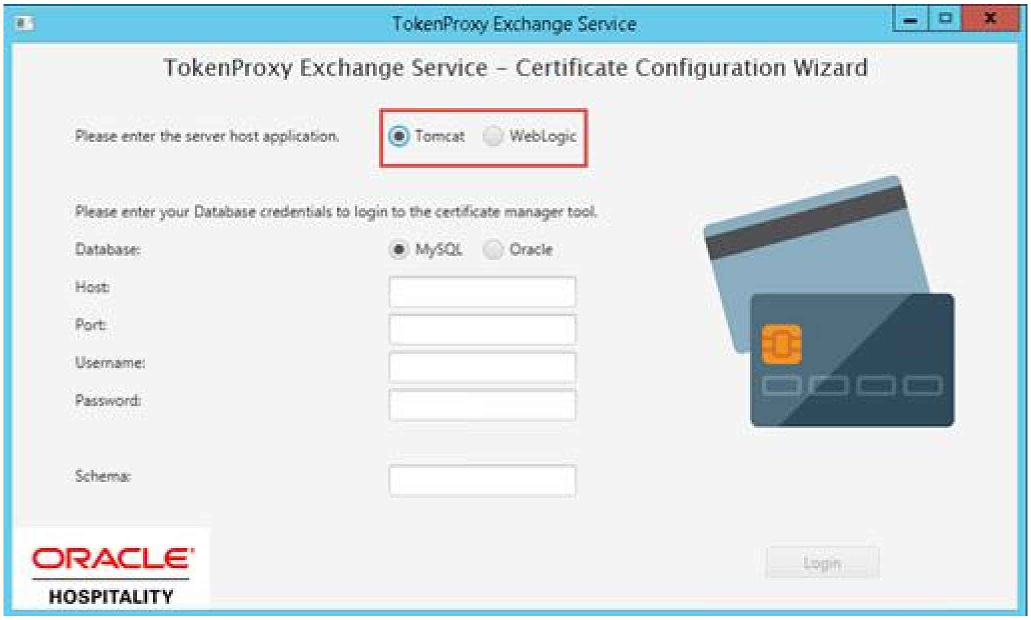
If something is not working as expected, you should be able to see more information on why by consulting the Cert Manager logs;

: \TokenProxy\TokenProxyCertManager\log

Logs will also need to be supplied in the event of any support request.

Wizard Mode - Login

The Login screen has two options such as **Tomcat** and **WebLogic**. You need to select either Tomcat or WebLogic option and specify valid connection details and credentials to configure the certificates.



TokenProxy Exchange Service

TokenProxy Exchange Service – Certificate Configuration Wizard

Please enter the server host application. ● Tomcat ○ WebLogic

Please enter your Database credentials to login to the certificate manager tool.

Database: ● MySQL ○ Oracle

Host:

Port:

Username:

Password:

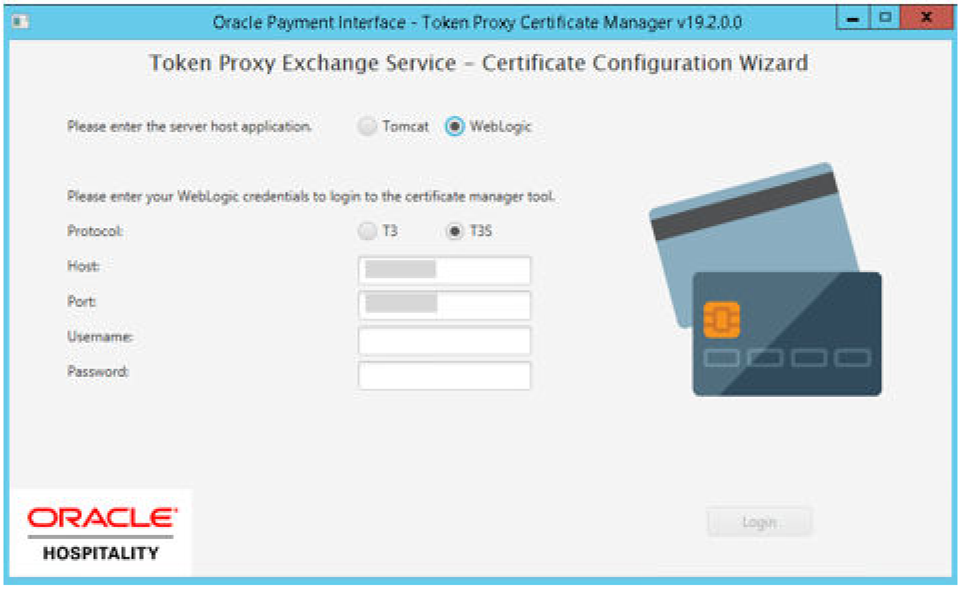
Schema:

WebLogic - Certificate Configuration Wizard

On the **Login** screen if **WebLogic** option is selected, then you need to enter your WebLogic credentials to login to the Cert Manager tool.

1. **Protocol**
   - T3 / T3S the default option selected is T3S, as it is presumed that T3 access to your WebLogic Admin server is disabled.
2. **Host**
   - The default value is localhost. If WebLogic is not installed on the local machine, then enter the host details.
   - The value provided can be the hostname or IP address of your WebLogic server. No http/https prefix should be provided, the Cert Manager will amend this as required based on the Protocol specified.
3. **Port**
   - The default port value is 7002, this is the default WebLogic port that WebLogic uses when it is installed. If your Admin managed server port is not 7002, then update this with the correct port number.
4. **Username**
   - Your user name for the WebLogic Admin Server, for example, the same Username you use to login to the WebLogic console page.
5. **Password**
   - Your password for the WebLogic Admin Server, for example, the same Password you use to login to the WebLogic console page.

Once you have provided the valid credentials, click **Login** to proceed.



Oracle Payment Interface - Token Proxy Certificate Manager v19.2.0.0

Token Proxy Exchange Service - Certificate Configuration Wizard

Please enter the server host application. ○ Tomcat ● WebLogic

Please enter your WebLogic credentials to login to the certificate manager tool.

Protocol: ○ T3 ● T3S

Host: [redacted]

Port: [redacted]

Username:

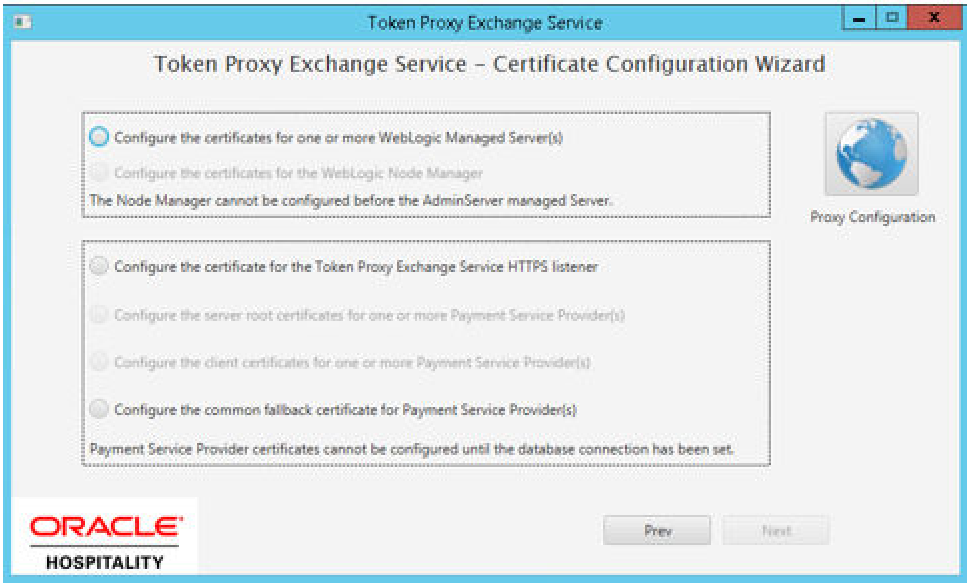
Password:

If your login is successful, then you should be navigated to a page where you can select any of the following six options:

- Configure the certificates for one or more WebLogic Managed Server(s).
- Configure the certificates for the WebLogic Node Manager.

> **Note:**
>
> The Node Manager cannot be configured before the AdminServer managed server.

- Configure the certificates for the TokenProxy Exchange Service HTTPS Listener.
- Configure the server root certificates for one or more Payment Service Provider(s).
- Configure the client certificates for one or more Payment Service Provider(s).
- Configure the common fallback certificate for Payment Service Provider(s).



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

○ Configure the certificates for one or more WebLogic Managed Server(s)
○ Configure the certificates for the WebLogic Node Manager
The Node Manager cannot be configured before the AdminServer managed Server.

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener
○ Configure the server root certificates for one or more Payment Service Provider(s)
○ Configure the client certificates for one or more Payment Service Provider(s)
○ Configure the common fallback certificate for Payment Service Provider(s)
Payment Service Provider certificates cannot be configured until the database connection has been set.

Proxy Configuration

Proxy configuration may be required in an environment that requires a proxy to access the internet.

Cert Manager will access the internet for the purpose of certificate revocation checks, and to check and download any missing intermediaries in your certificates chain of trust.

1. To configure a Proxy, go to the Proxy configuration in the main screen or use globe icon

   when options are selected.

2. Check the Proxy Enabled option, enter the valid information as required and select apply.

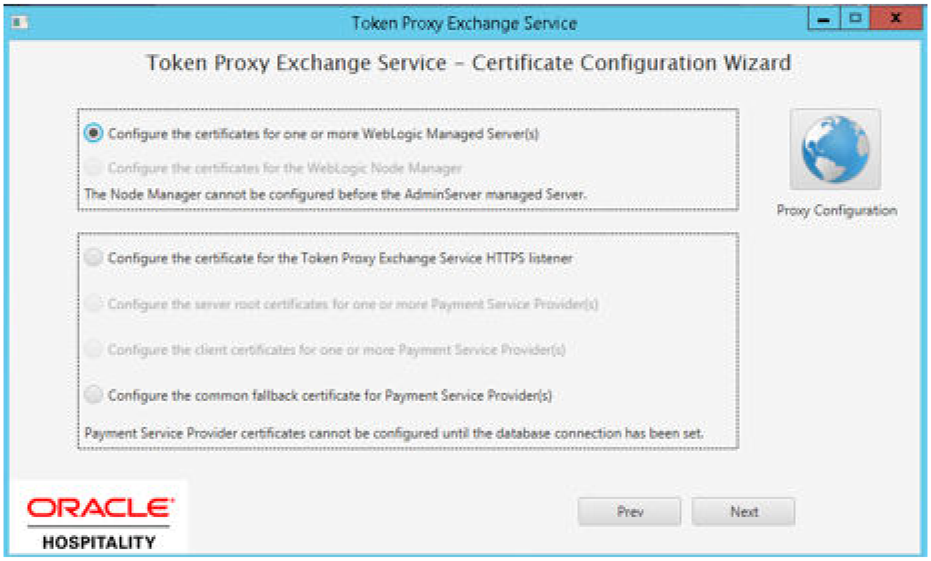
WebLogic Managed Server

Cert Manager allows the user to connect to the WebLogic Admin Server, and update the certificate associated with any of the managed servers.

This allows users to update the certificate that is seen in the browser when accessing the Token Proxy Webportal pages.

The Common Name of the certificate that is applied to the Managed Server should reflect the hostname of the URL by which it will be accessed, otherwise regardless of serving the certificate up, a user’s browser will still show the URL as insecure as hostname validation will fail.

1. After Login, select the option **Configure the certificates for one or more WebLogic Managed Server(s)**.



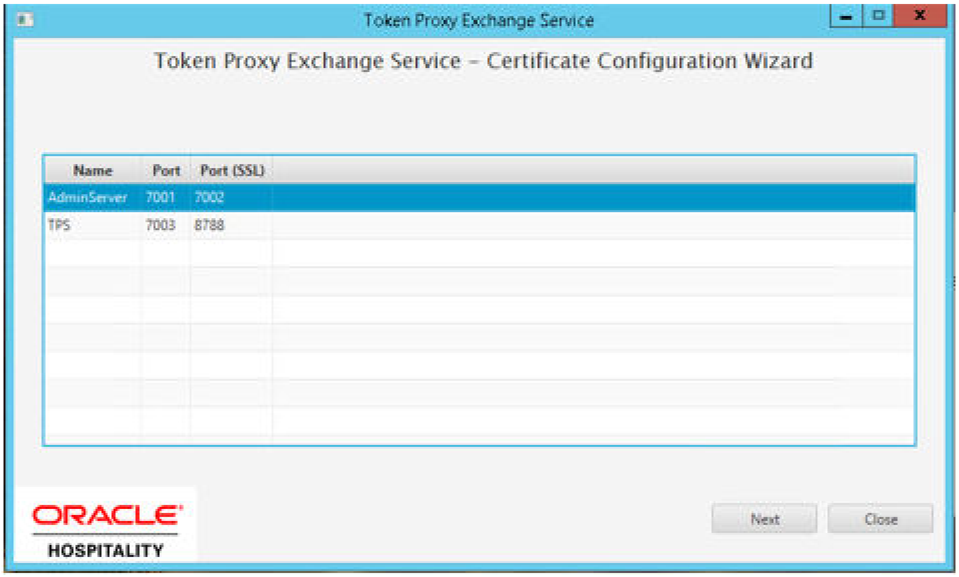
Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

● Configure the certificates for one or more WebLogic Managed Server(s)
○ Configure the certificates for the WebLogic Node Manager
The Node Manager cannot be configured before the AdminServer managed Server.

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener
○ Configure the server root certificates for one or more Payment Service Provider(s)
○ Configure the client certificates for one or more Payment Service Provider(s)
○ Configure the common fallback certificate for Payment Service Provider(s)
Payment Service Provider certificates cannot be configured until the database connection has been set.

2. You will be provided with a list of the managed servers that are present on your WebLogic instance.

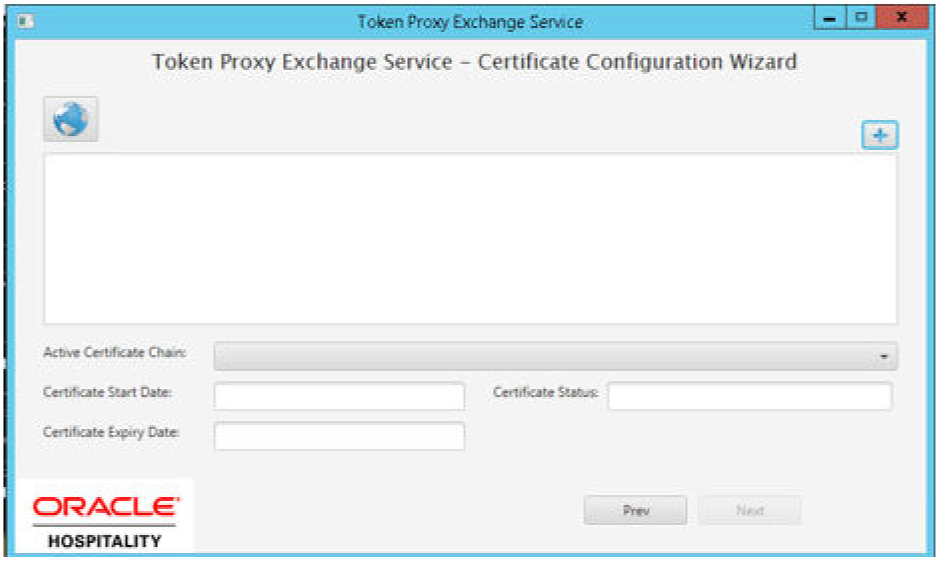


Token Proxy Exchange Service - Certificate Configuration Wizard

Name	Port	Port (SSL)
AdminServer	7001	7002
TPS	7003	8788

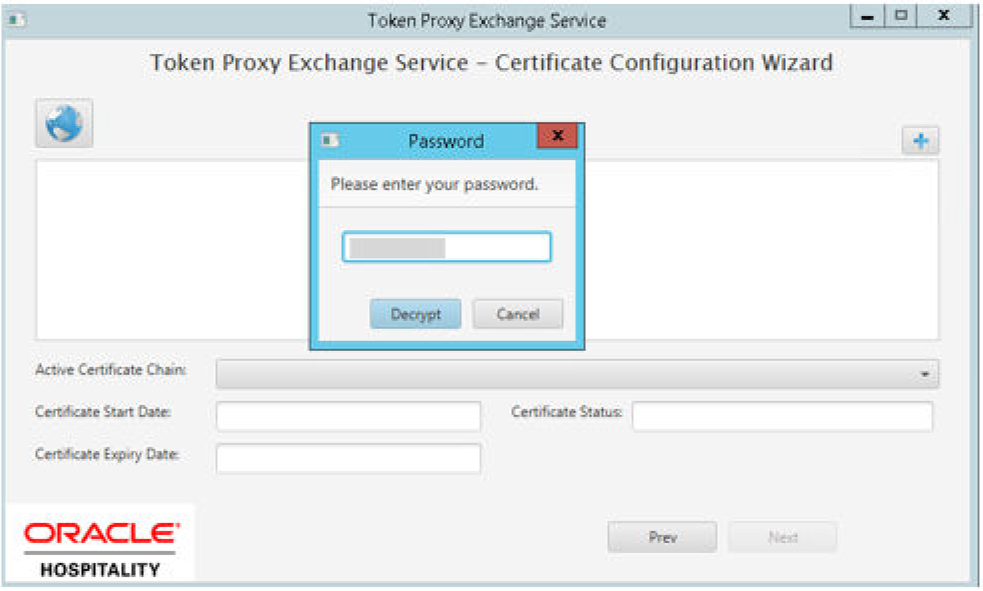
3. Select the Managed Server that you want to assign a certificate to. If you need to add certificates to the **AdminServer** and the **tokenproxy_server**, repeat the process for both.

4. The Cert Manager allows the supported certificate to be imported by browsing or using drag and drop. Browse to the location of the certificate you want to import from add icon (+) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).



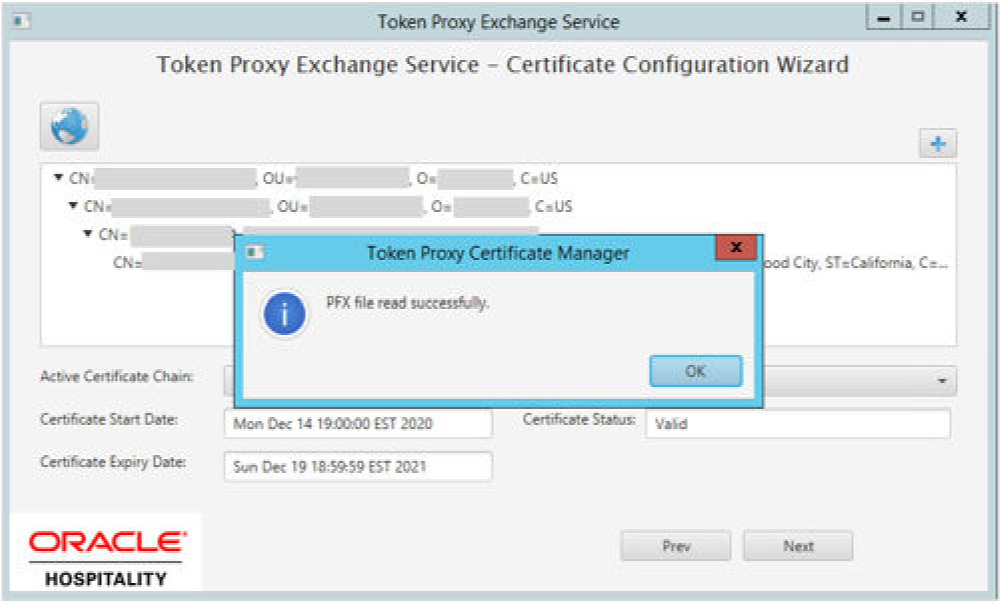
Token Proxy Exchange Service - Certificate Configuration Wizard

5. You will be prompted to provide the password for the certificate you have selected. Enter the password and select **Decrypt**.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password
Decrypt
Cancel
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

Please enter your password.

6. If the entered password is correct, then you should see a **file read successfully** message.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Token Proxy Certificate Manager
OK
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

▾ CN=[redacted], OU=[redacted], O=[redacted], C=US
▾ CN=[redacted], OU=[redacted], O=[redacted], C=US
▾ CN=[redacted]
CN=[redacted] ood City, ST=California, C=...

PFX file read successfully.

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

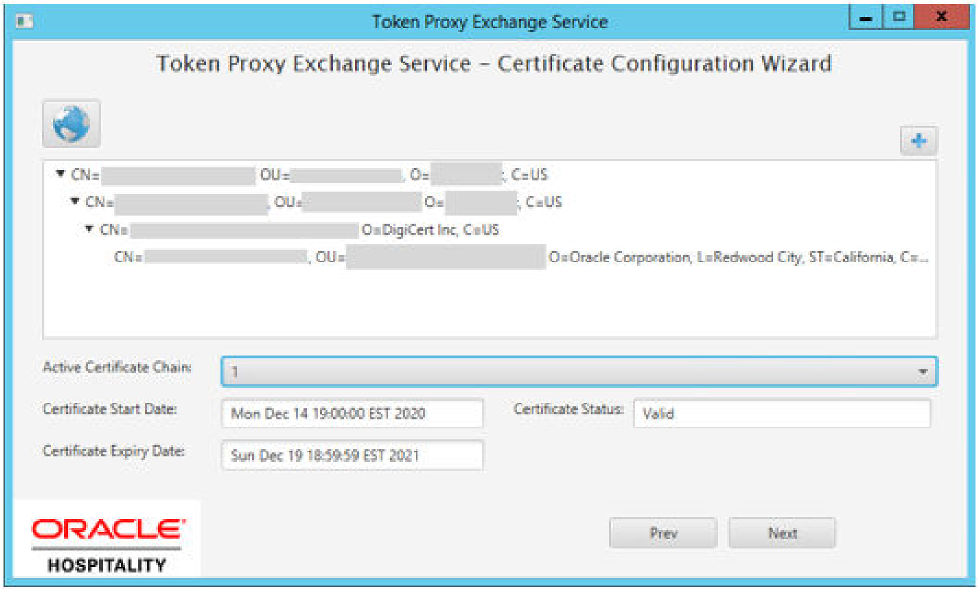
Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

7. The **Cert Manager** will display the certificate chains from the certificate provided.

8. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.

9. This will display the associated **Certificate Expiry Date** and **Status**.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

- CN=[redacted], OU=[redacted], O=[redacted], C=US
  - CN=[redacted], OU=[redacted], O=[redacted], C=US
    - CN=[redacted], O=DigiCert Inc, C=US
      - CN=[redacted], OU=[redacted], O=Oracle Corporation, L=Redwood City, ST=California, C=...

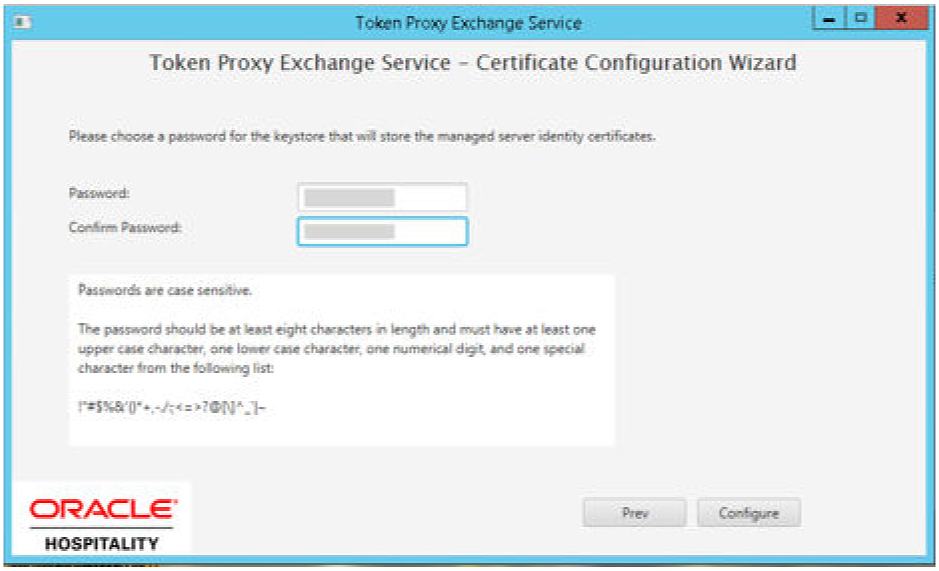
Active Certificate Chain: 1

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

10. Click **Next** to choose a password for the keystore.
11. Provide and confirm the password that meets the minimum requirements, for the keystore that will store identity certificate.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the managed server identity certificates.

Password: [redacted]

Confirm Password: [redacted]

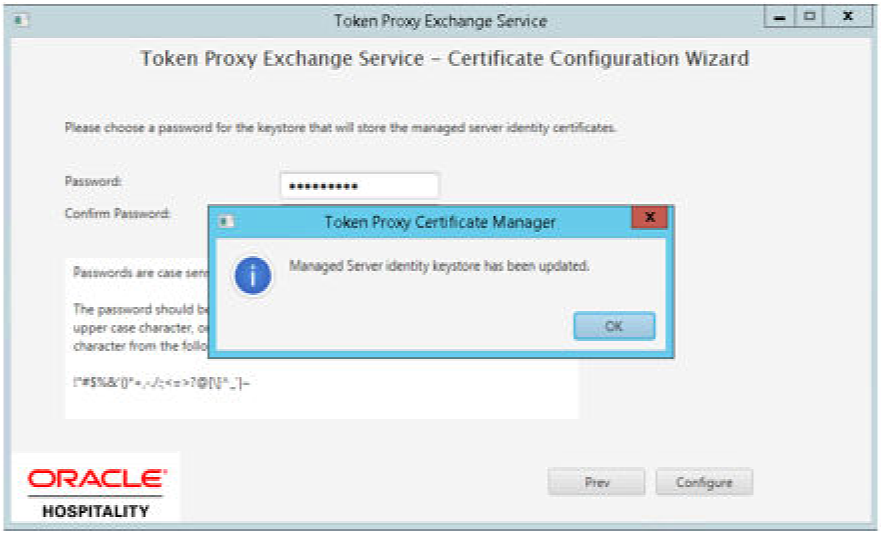
Passwords are case sensitive.

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

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

12. Click **Configure** to configure the Managed server certificates.

Managed Server identity keystore has been updated, will be displayed once the process is complete. You will be returned to the list of Managed Servers so that you can update your other Managed Servers. Click **OK** to return to the option selection screen.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the managed server identity certificates.

Password: ••••••••••

Confirm Password:

Passwords are case sen

The password should b
upper case character, o
character from the follo

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

Token Proxy Certificate Manager

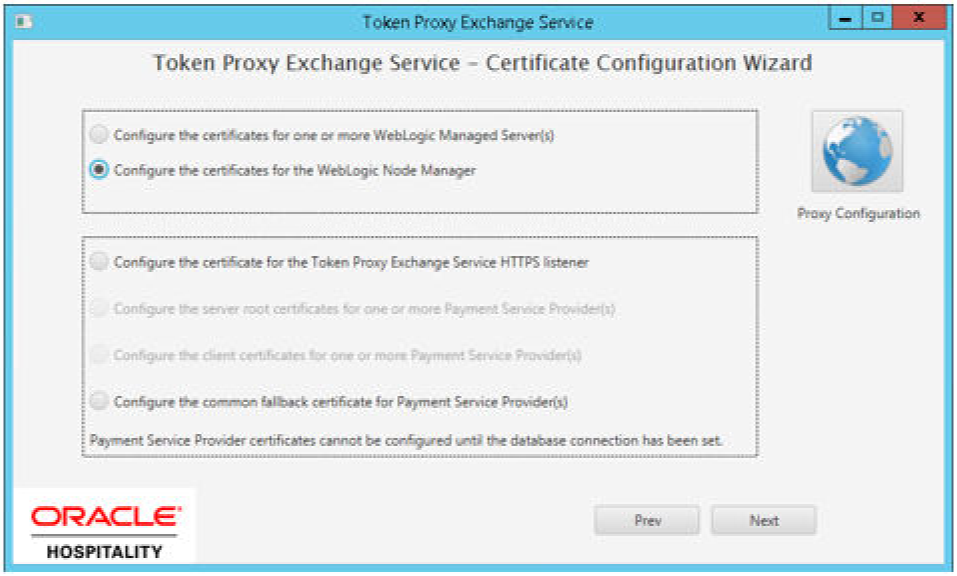
Managed Server identity keystore has been updated.

WebLogic Node Manager

Cert Manager also allows the user to connect to the WebLogic Admin Server, and update the certificate associated with the Node Manager.

This option will be disabled until you have the WebLogic managed server certificates configured.

1. After WebLogic server certificates are configured, select **Configure the certificates for the WebLogic Node Manager**.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

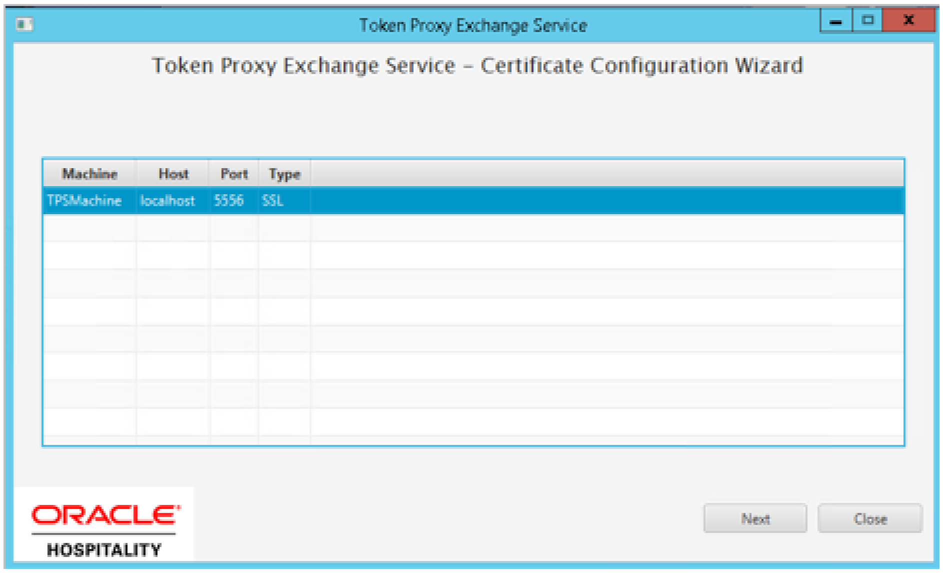
○ Configure the certificates for one or more WebLogic Managed Server(s)
● Configure the certificates for the WebLogic Node Manager

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener
○ Configure the server root certificates for one or more Payment Service Provider(s)
○ Configure the client certificates for one or more Payment Service Provider(s)
○ Configure the common fallback certificate for Payment Service Provider(s)

Payment Service Provider certificates cannot be configured until the database connection has been set.

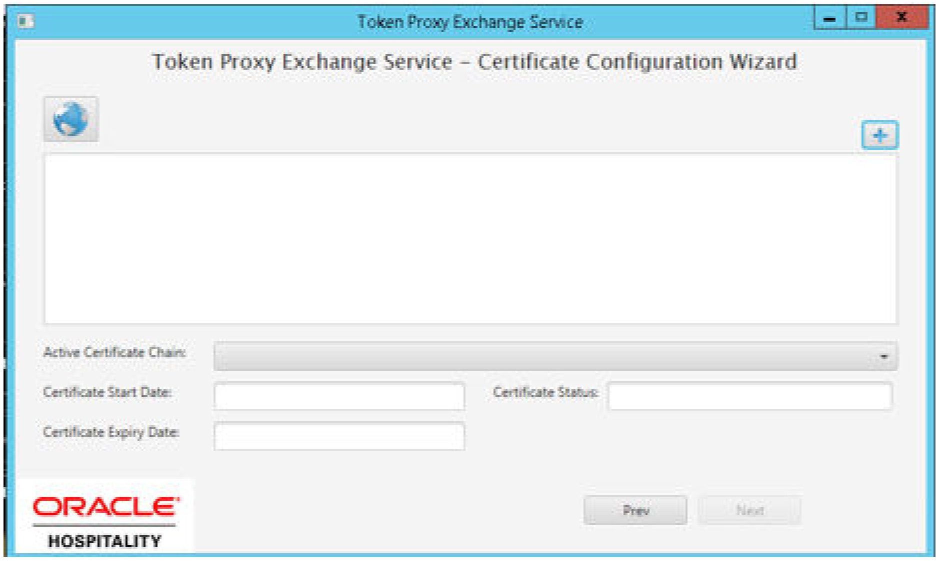
2. You will be provided with a list of the machines that are present on your WebLogic instance.

3. Select the Machine that you want to assign a certificate to. If you need to add certificates to the **Machine 1** and **Machine 2**, repeat the process for both.

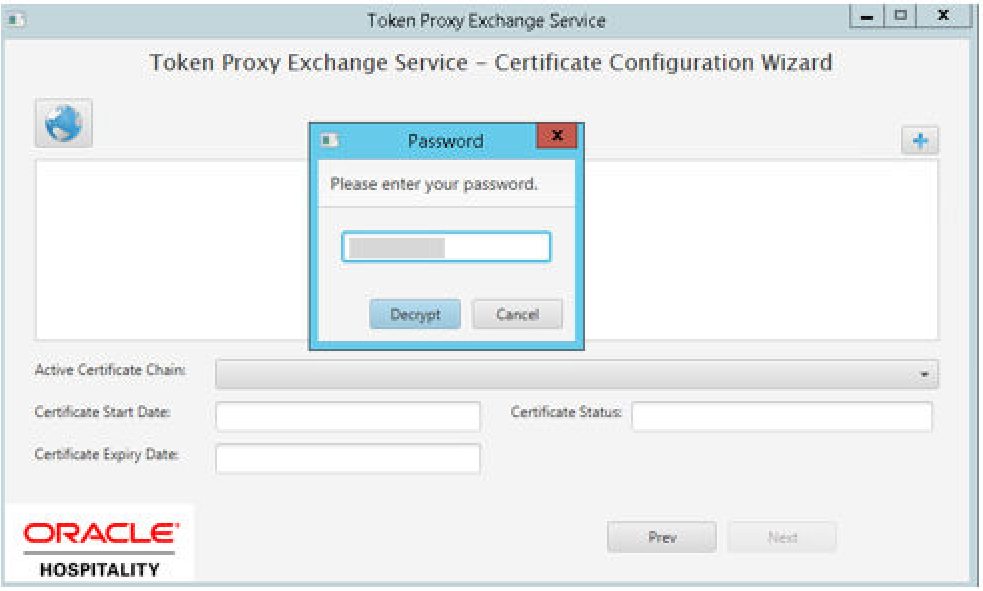

Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
ORACLE
HOSPITALITY
Next
Close

Machine	Host	Port	Type
TPSMachine	localhost	5556	SSL

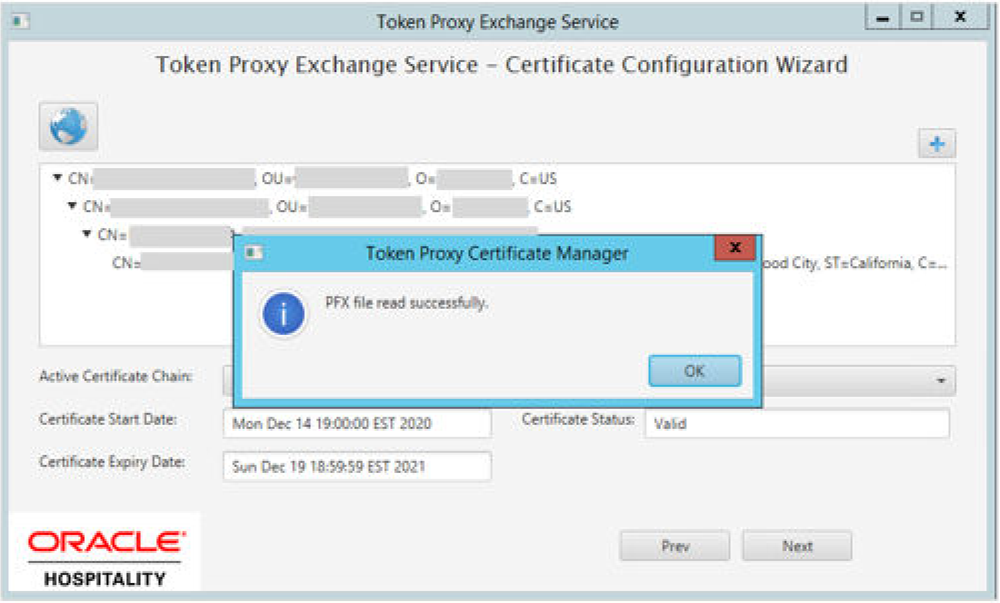
4. The Cert Manager allows the supported certificate to be imported by browsing or using drag and drop. Browse to the location of the certificate you want to import from add icon
(
+
) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

5. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt**.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password
Please enter your password.
Decrypt
Cancel
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

6. If the entered password is correct, then you should see a **file read successfully** message.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Token Proxy Certificate Manager
OK
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

▾ CN=[redacted], OU=[redacted], O=[redacted], C=US
▾ CN=[redacted], OU=[redacted], O=[redacted], C=US
▾ CN=[redacted]
CN=[redacted] ...ood City, ST=California, C=...

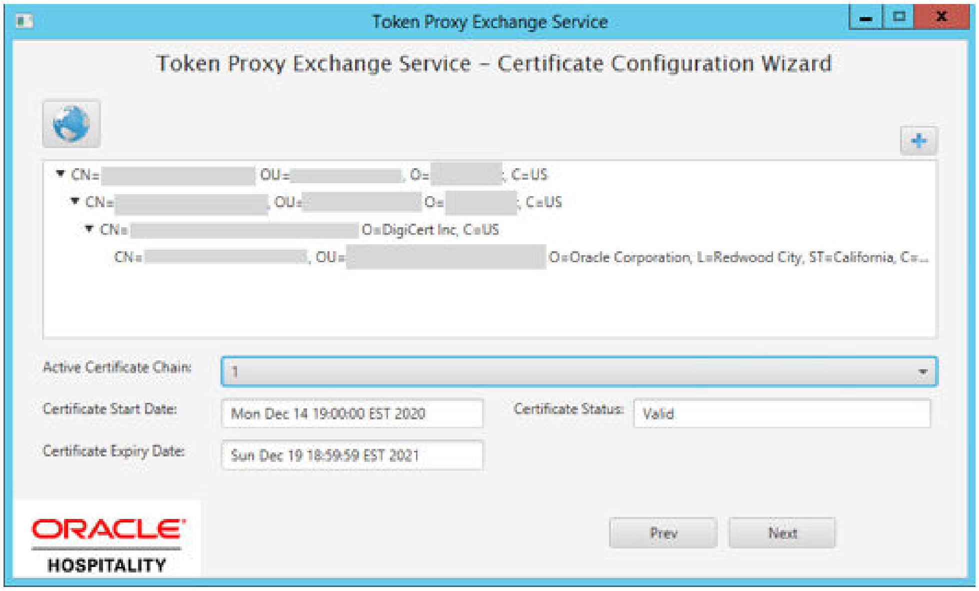
PFX file read successfully.

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

7. The **Cert Manager** will display the certificate chains from the certificate provided.
8. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
9. This will display the associated **Certificate Expiry Date** and **Status**.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

- CN=[redacted] OU=[redacted], O=[redacted], C=US
  - CN=[redacted], OU=[redacted] O=[redacted], C=US
    - CN=[redacted] O=DigiCert Inc, C=US
      - CN=[redacted], OU=[redacted] O=Oracle Corporation, L=Redwood City, ST=California, C=...

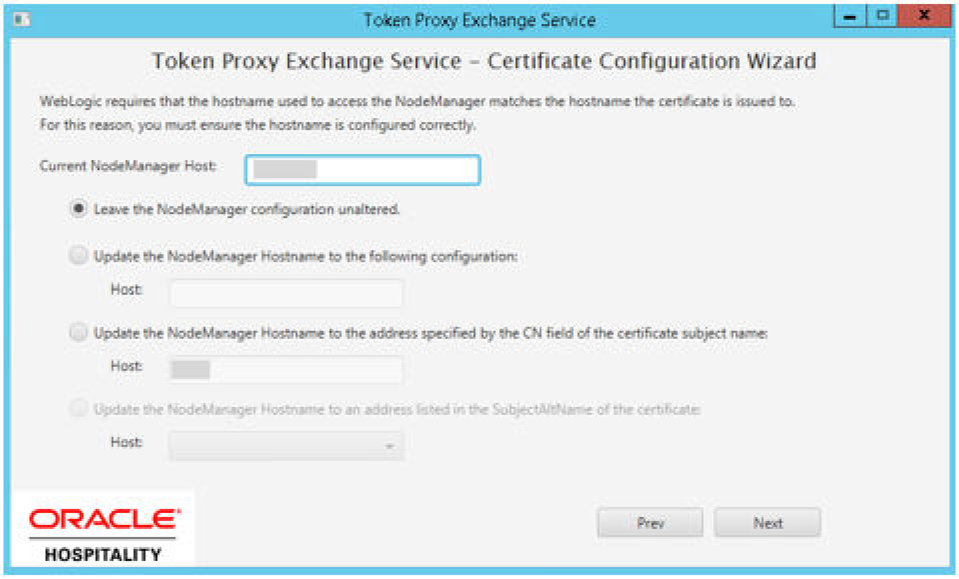
Active Certificate Chain: 1

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

10. On the next page you will have four options to configure the hostname, so the node manager matches the hostname the certificate is issued to.
    - Leave the Node Manager configuration unaltered:
      – Allows a user to make these changes in WebLogic manually if they required or it can be that the value is already correct so needs no update.
    - Update the NodeManager Hostname to the following configuration:
      – Allows user to update the NodeManager Hostname to a value defined by the user.
    - Update the NodeManager Hostname to the address specified by the CN (CommonName) field of the certificate subject name.
      – Allows users to set the Hostname to a value same as the CN value.
    - Update the NodeManager hostname to the address listed in the SubjectAltName of the certificate:
      – Allows user to update the NodeManager hostname to the address specified by the Alternative Name of the certificate set the NodeManager value as the AltName value selected from the drop-down menu.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

WebLogic requires that the hostname used to access the NodeManager matches the hostname the certificate is issued to. For this reason, you must ensure the hostname is configured correctly.

Current NodeManager Host: [redacted]

● Leave the NodeManager configuration unaltered.

○ Update the NodeManager Hostname to the following configuration:

Host:

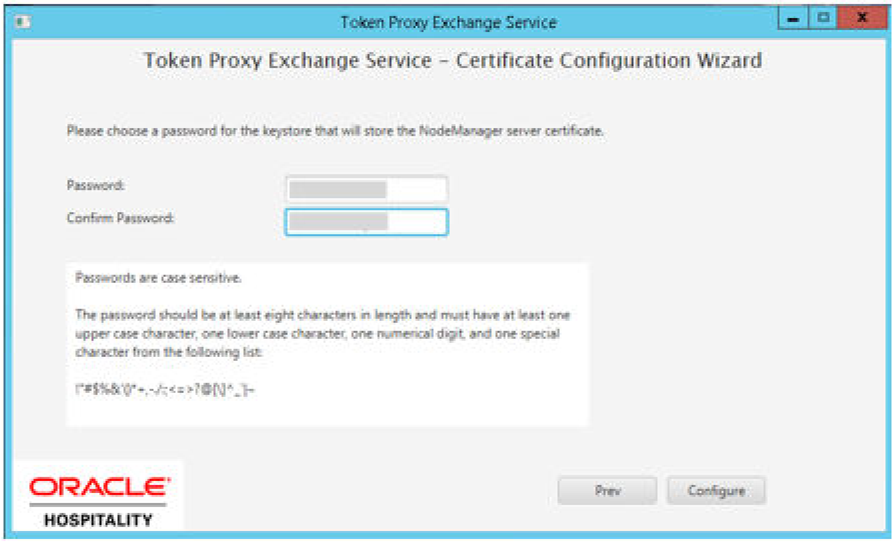
○ Update the NodeManager Hostname to the address specified by the CN field of the certificate subject name:

Host: [redacted]

○ Update the NodeManager Hostname to an address listed in the SubjectAltName of the certificate:

Host:

11. Click **Next** to choose a password for the keystore.
12. Provide and confirm the password that meets the minimum requirements, for the keystore that will store the Node manager certificate.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the NodeManager server certificate.

Password: [redacted]

Confirm Password: [redacted]

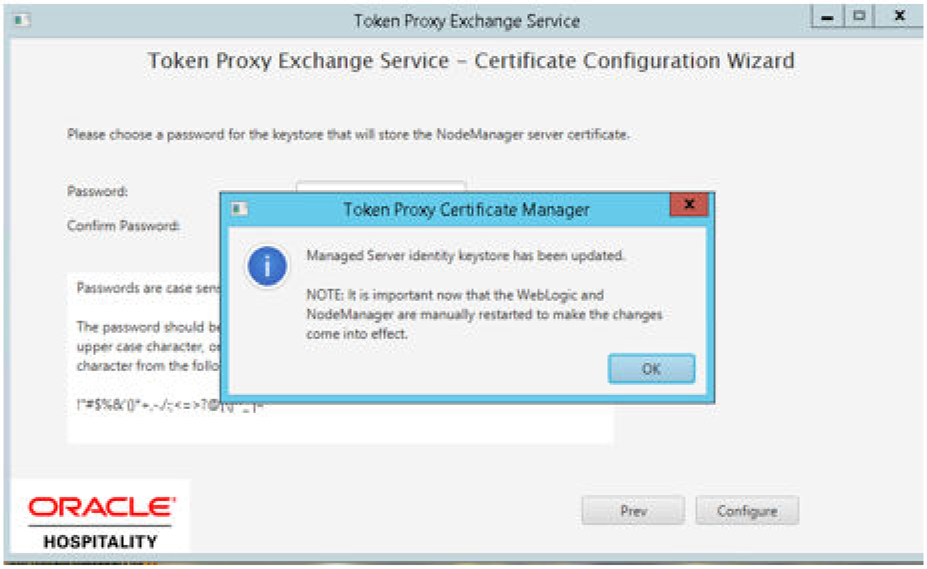
Passwords are case sensitive.

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

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

13. Click **Configure** to configure the Node manager certificates.

    Managed Server identity keystore has been updated, it is important that the WebLogic and Node manager are manually restarted to make the changes come into effect. Click **OK** to return to the option selection screen.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password:
Confirm Password:
Token Proxy Certificate Manager
OK
ORACLE
HOSPITALITY
Prev
Configure

Please choose a password for the keystore that will store the NodeManager server certificate.

Passwords are case sens

The password should be
upper case character, o
character from the follo

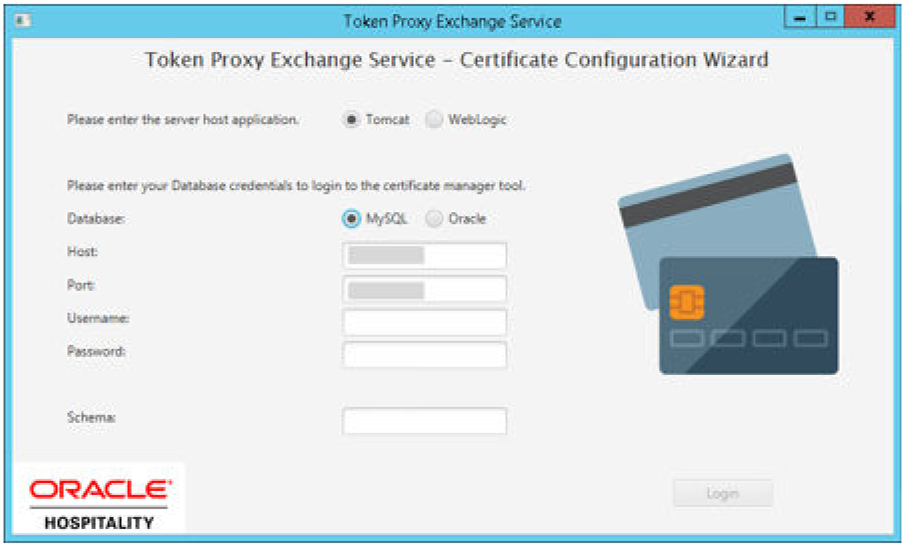
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Managed Server identity keystore has been updated.

NOTE: It is important now that the WebLogic and NodeManager are manually restarted to make the changes come into effect.

Tomcat - Certificate Configuration Wizard

1. On the **Login** screen if **Tomcat** option is selected, then you can either select Oracle or MySQL database. You need to enter your database credentials to login to the Cert Manager tool.
2. Select your Database type:
   a. MySQL
   b. Oracle DB
   - **MySQL**


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
ORACLE
HOSPITALITY
Login

Please enter the server host application. ● Tomcat ○ WebLogic

Please enter your Database credentials to login to the certificate manager tool.

Database: ● MySQL ○ Oracle

Host:

Port:

Username:

Password:

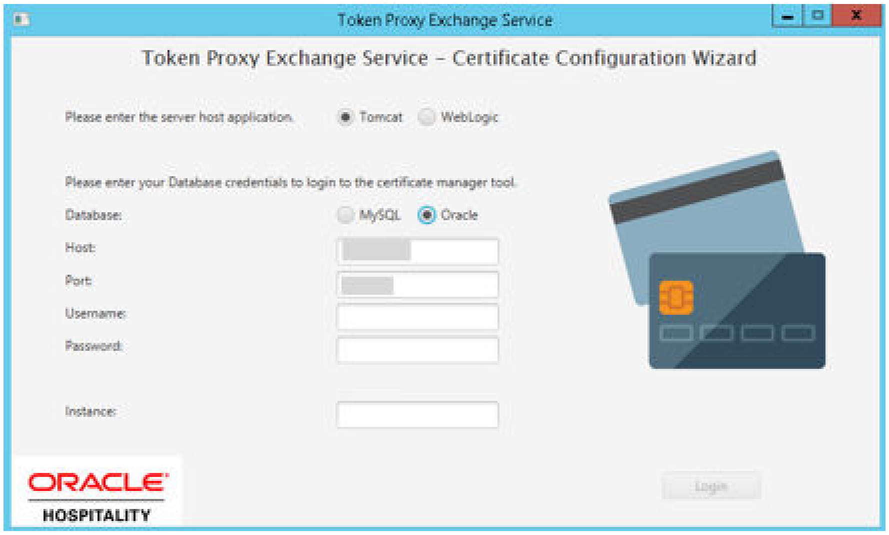
Schema:

– **Host** – The default value is localhost, if MySQL database is not installed on the local machine, then enter the host details.

The value provided can be the hostname or IP address of your server where MySQL database is installed. No http/https prefix should be provided, the Cert Manager will amend this as required based on the Protocol specified.

- **Port** – The default port value is 3306, this is the default MySQL database port that MySQL DB uses when installed. If your MySQL database port is not 3306, then update this with the correct port number.
- **Username** – Your TPS database username for example, the same username you use to connect to MySQL database.
- **Password** – Your TPS database password for example, the same password you use to connect to MySQL database.
- **Schema** – Your database schema configured details should be provided here.

- **Oracle DB**



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Please enter the server host application. ● Tomcat ○ WebLogic

Please enter your Database credentials to login to the certificate manager tool.

Database: ○ MySQL ● Oracle

Host: [redacted]

Port: [redacted]

Username:

Password:

Instance:

- **Host** – The default value is localhost, if Oracle database is not installed on the local machine, then enter the host details.

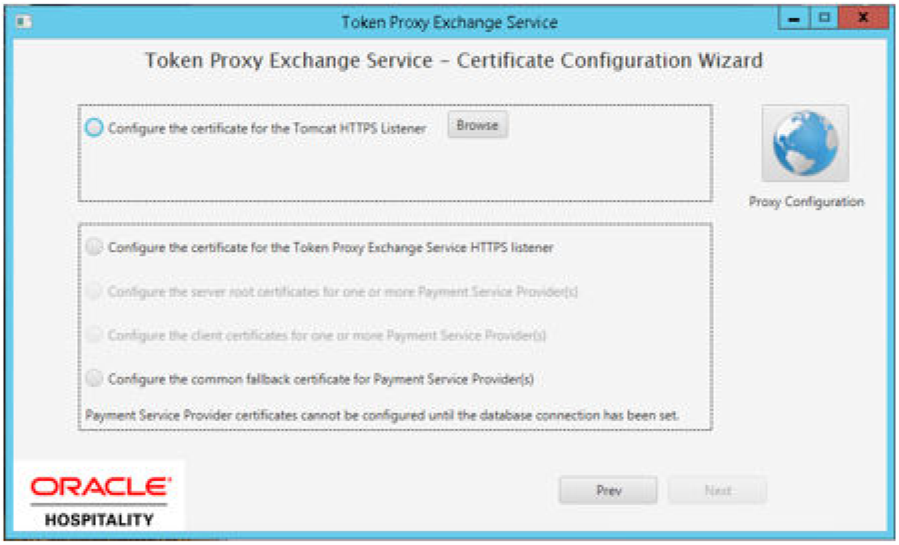
The value you provide can be the hostname or IP address of your server where Oracle database is installed. No http/https prefix should be provided, the Cert Manager will amend this as required based on the Protocol specified.

- **Port** – The default port value is 1521, this is the default Oracle database port that Oracle DB uses when installed. If your Oracle database port is not 1521, then update this with the correct port number.
- **Username** – Your database Admin user name for example, the same username you use to connect to Oracle database.
- **Password** – Your database Admin password for example, the same Password you use to connect to Oracle database.
- **Instance** – The service name used to connect to the Oracle database.

3. Once you have provided the valid credentials, click **Login** to proceed.

If your login is successful, then you should be navigated to a page where you can select any of the following five options:

- Configure the certificates for the Tomcat HTTPS Listener.
- Configure the certificates for the TokenProxy Exchange Service HTTPS Listener.
- Configure the server root certificates for one or more Payment Service Provider(s).
- Configure the client certificates for one or more Payment Service Provider(s).
- Configure the common fallback certificate for Payment Service Provider(s).



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

○ Configure the certificate for the Tomcat HTTPS Listener [Browse]

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener

○ Configure the server root certificates for one or more Payment Service Provider(s)

○ Configure the client certificates for one or more Payment Service Provider(s)

○ Configure the common fallback certificate for Payment Service Provider(s)

Payment Service Provider certificates cannot be configured until the database connection has been set.

Proxy Configuration

Proxy configuration may be required in an environment that requires a proxy to access the internet.

Cert Manager will access the internet for the purpose of certificate revocation checks, and to check and download any missing intermediaries in your certificates chain of trust.

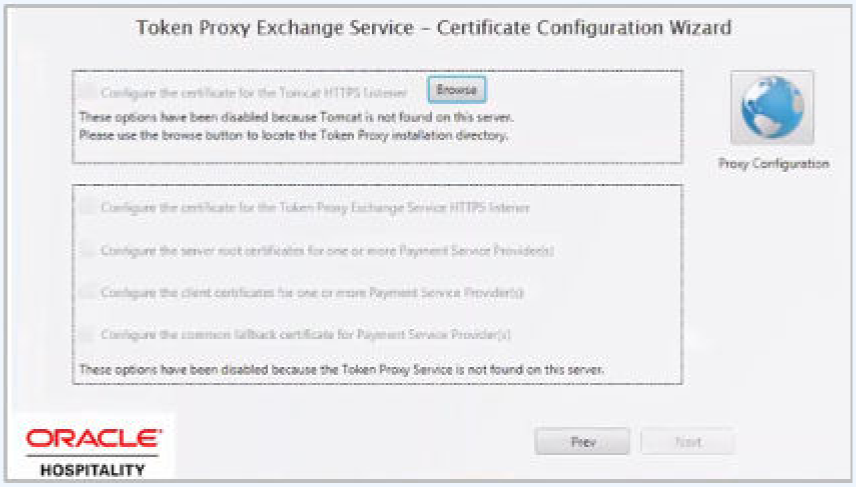
1. To configure a Proxy, go to the Proxy configuration in the main screen or use globe icon

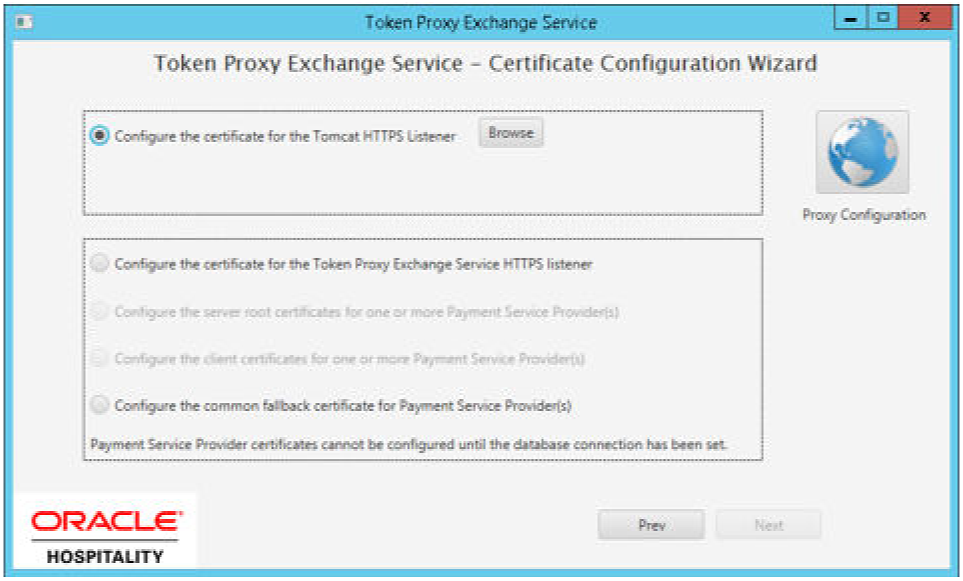
   when options are selected.
2. Check the Proxy Enabled option, enter the valid information as required and select apply.

Tomcat HTTPS Listener

Cert Manager allows the user to import required certificates into root certificate files for the Listener record configured on a Tomcat.

1. After Login, select the option **Configure the certificates for the Tomcat HTTPS Listener**.

> **Note:**
>
> If you have installed Token Proxy in any path/directory other than C:\TokenProxy you will see this message "These options have been disabled because Tomcat is not found on this server. Please use the browse button to locate the Token Proxy installation directory". In this case use **Browse** to point to the correct location of the Token Proxy.
>
> 
>
> Token Proxy Exchange Service – Certificate Configuration Wizard
>
> □ Configure the certificate for the Tomcat HTTPS Listener
>
> These options have been disabled because Tomcat is not found on this server.
> Please use the browse button to locate the Token Proxy installation directory.
>
> □ Configure the certificate for the Token Proxy Exchange Service HTTPS listener
>
> □ Configure the server root certificates for one or more Payment Service Provider(s)
>
> □ Configure the client certificates for one or more Payment Service Provider(s)
>
> □ Configure the common fallback certificate for Payment Service Provider(s)
>
> These options have been disabled because the Token Proxy Service is not found on this server.
>
>



Token Proxy Exchange Service – Certificate Configuration Wizard

● Configure the certificate for the Tomcat HTTPS Listener

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener

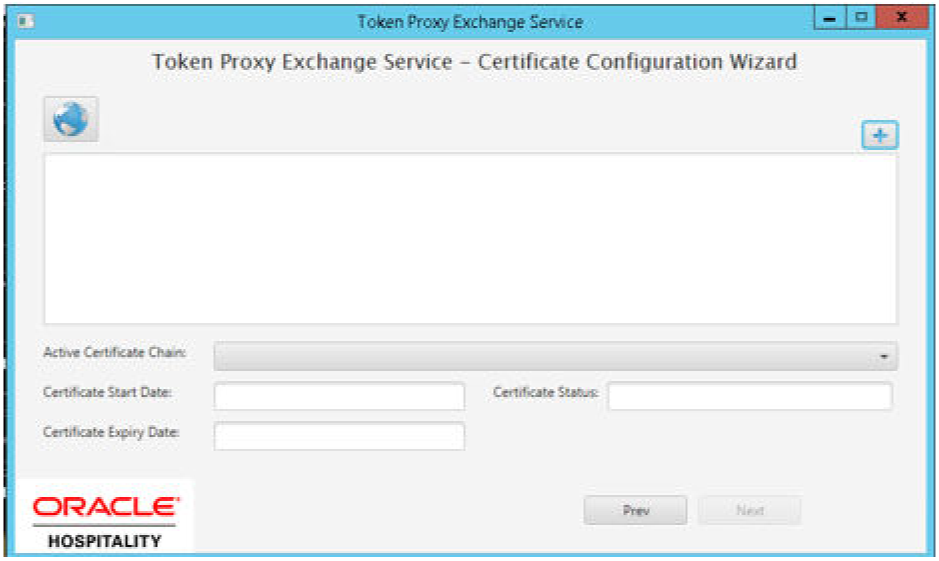
○ Configure the server root certificates for one or more Payment Service Provider(s)

○ Configure the client certificates for one or more Payment Service Provider(s)

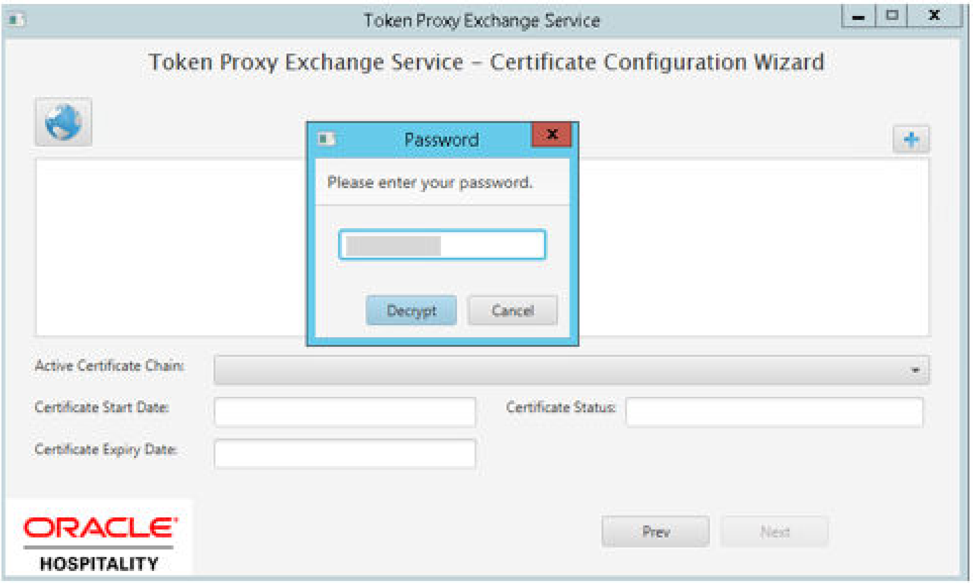
○ Configure the common fallback certificate for Payment Service Provider(s)

Payment Service Provider certificates cannot be configured until the database connection has been set.

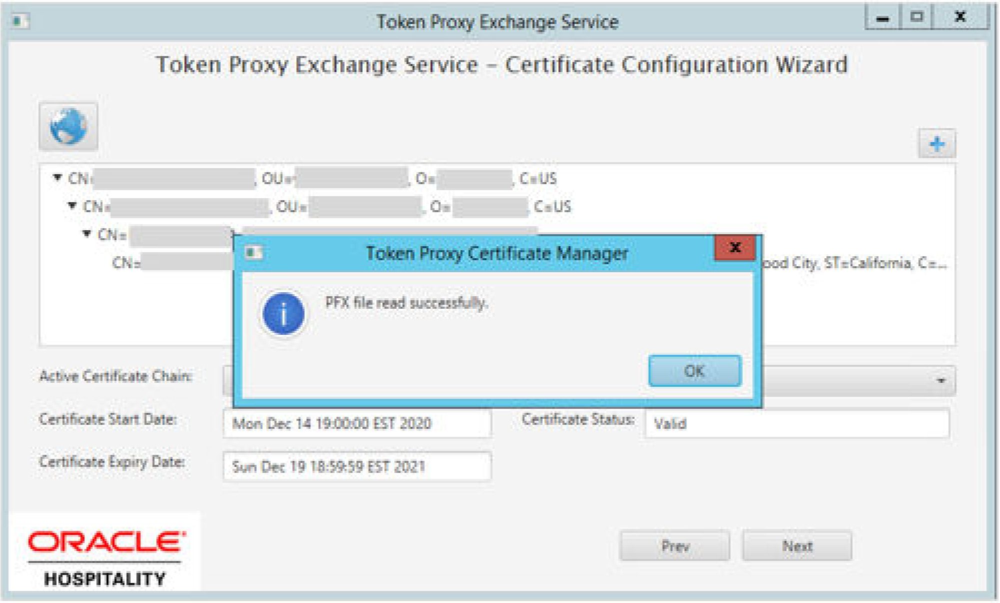
2. The Cert Manager allows the supported certificate to be imported by browsing or using drag and drop. Browse to the location of the certificate you want to import from **add** icon (+) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

3. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt**.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password
Please enter your password.
Decrypt
Cancel
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

4. If the entered password is correct, then you should see a **file read successfully** message.



Token Proxy Exchange Service – Certificate Configuration Wizard

▼ CN=[redacted], OU=[redacted], O=[redacted], C=US
▼ CN=[redacted], OU=[redacted], O=[redacted], C=US
▼ CN=[redacted]
CN=[redacted] ood City, ST=California, C=...

Token Proxy Certificate Manager

PFX file read successfully.

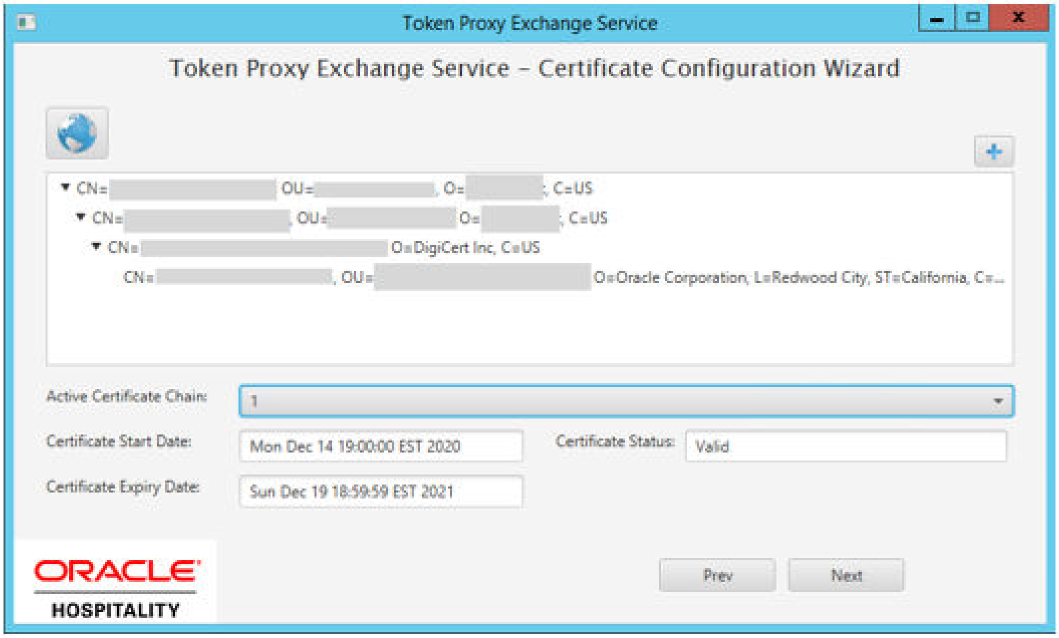
Active Certificate Chain:

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

5. The **Cert Manager** will display the certificate chains from the certificate provided.
6. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
7. This will display the associated **Certificate Expiry Date** and **Status**.



Token Proxy Exchange Service – Certificate Configuration Wizard

▼ CN=[redacted] OU=[redacted], O=[redacted], C=US
▼ CN=[redacted], OU=[redacted] O=[redacted], C=US
▼ CN=[redacted] O=DigiCert Inc, C=US
CN=[redacted], OU=[redacted] O=Oracle Corporation, L=Redwood City, ST=California, C=...

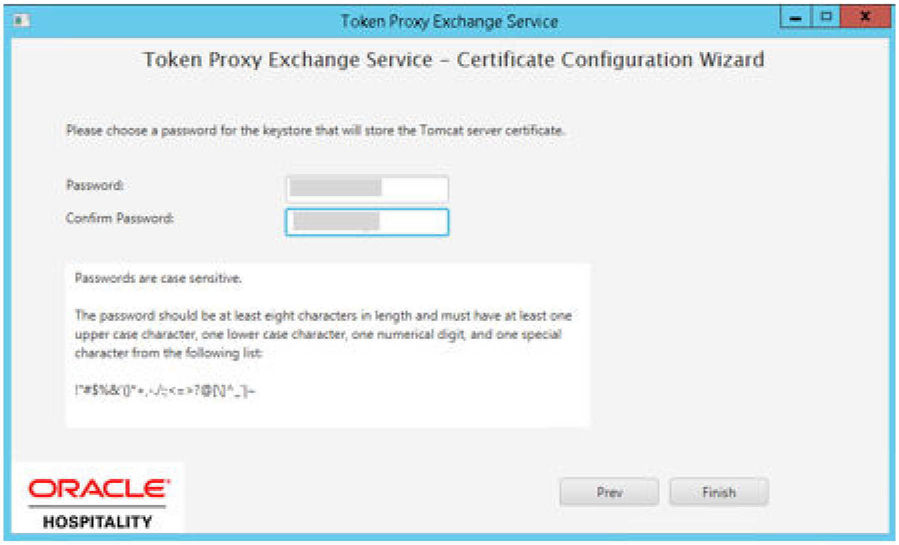
Active Certificate Chain: 1

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

8. Click **Next** to choose a password for the keystore.
9. Provide and confirm the password that meets the minimum requirements, for the keystore that will store Tomcat server certificate.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the Tomcat server certificate.

Password:

Confirm Password:

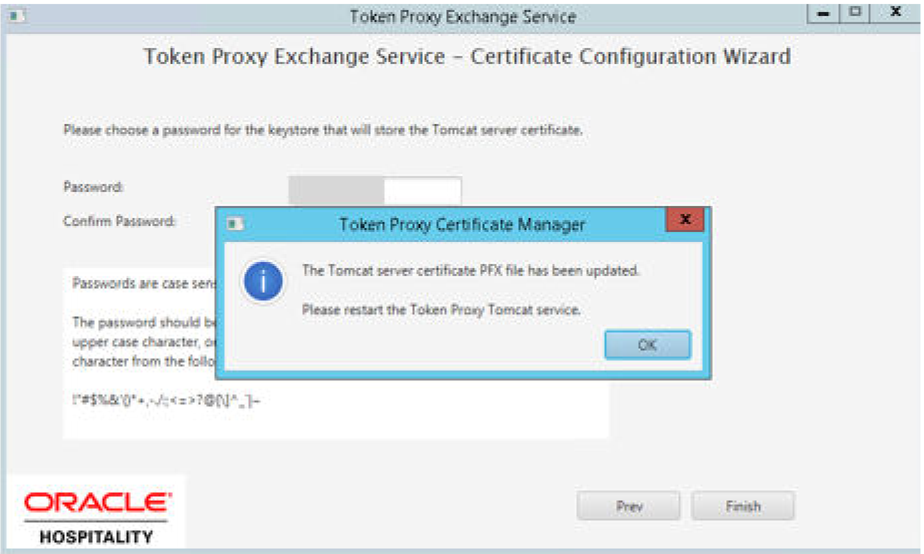
Passwords are case sensitive.

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

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

10. Click **Finish** to configure the Tomcat server certificate.

    The Token Proxy service listener PFX file has been updated with OPI_Listener.pfx in directory: \TokenProxy\TokenProxyService\key\.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the Tomcat server certificate.

Password:

Confirm Password:

Passwords are case sen

The password should b
upper case character, o
character from the follo

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

Token Proxy Certificate Manager

The Tomcat server certificate PFX file has been updated.

Please restart the Token Proxy Tomcat service.

11. Click **OK** to return to the option selection screen.

Token Proxy Service Listener Certificate

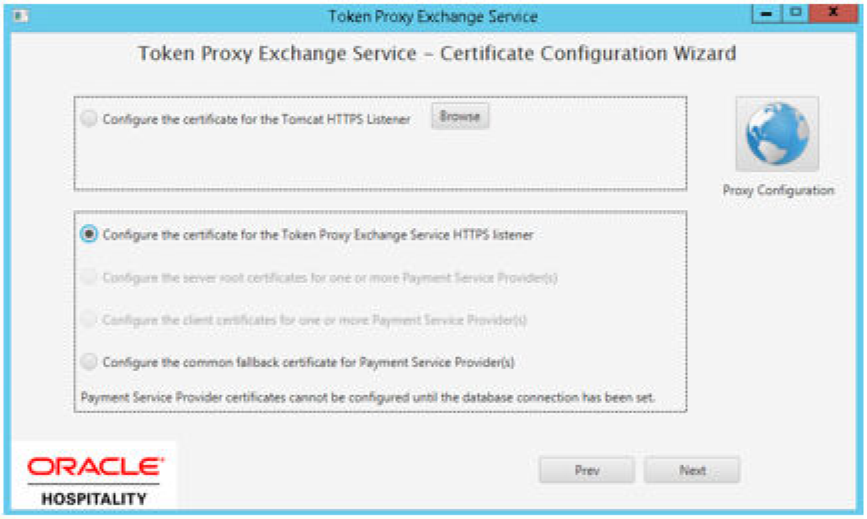
Note:

The Token Proxy Service Listener Certificate is available for both Tomcat and WebLogic.

The Cert Manager can also assist importing required certificates into root certificate files for the Listener record configured on a Token Proxy system.

It is possible to import the selected certificates public key to a keystore it creates with the required file name, and set the password in the TPS wallet, which means this step does not need to be completed with the existing OPIConfigX utility.

1. After login, select the option **Configure the certificates for the TokenProxy Exchange Service HTTPS Listener**.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

○ Configure the certificate for the Tomcat HTTPS Listener [Browse]

● Configure the certificate for the Token Proxy Exchange Service HTTPS listener

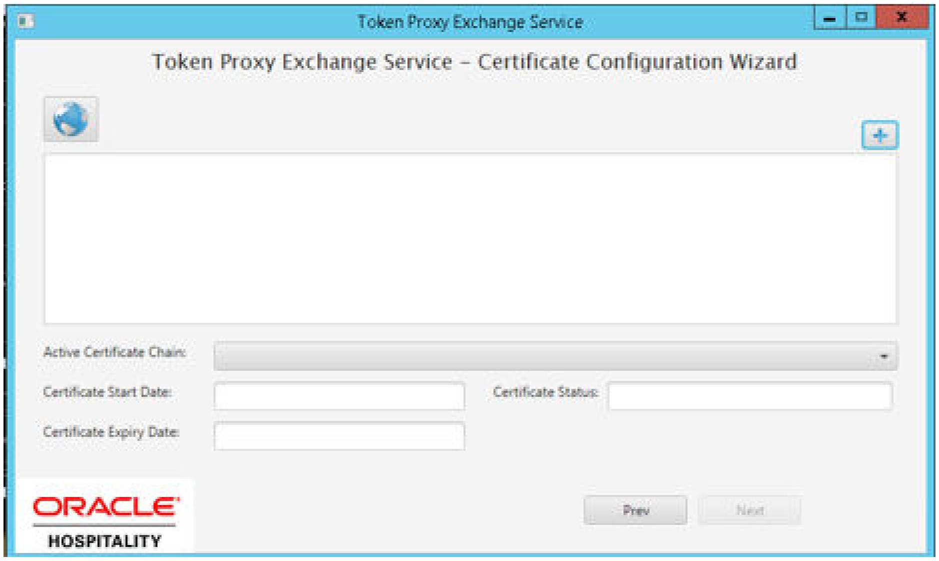
○ Configure the server root certificates for one or more Payment Service Provider(s)

○ Configure the client certificates for one or more Payment Service Provider(s)

○ Configure the common fallback certificate for Payment Service Provider(s)

Payment Service Provider certificates cannot be configured until the database connection has been set.

2. The Cert Manager allows the supported certificate to be imported by browsing or using drag and drop. Browse to the location of the certificate you want to import from **add** icon (+) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

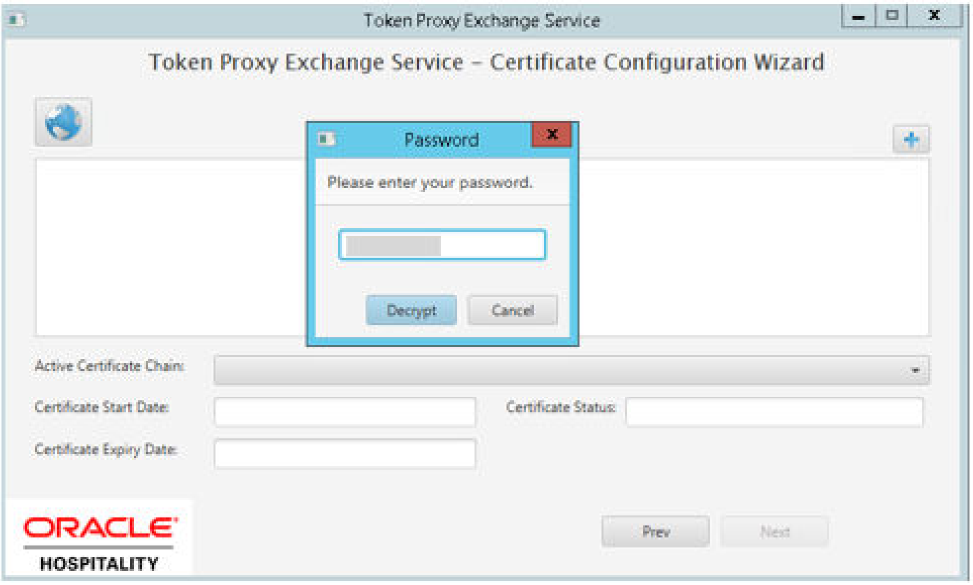
Active Certificate Chain:

Certificate Start Date:

Certificate Status:

Certificate Expiry Date:

3. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt**.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Password

Please enter your password.

[redacted]

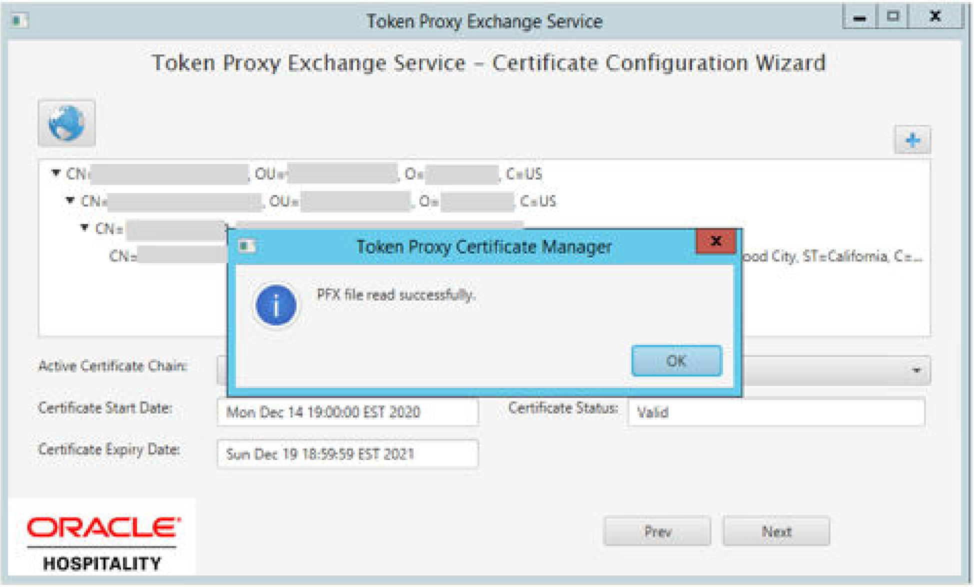
Active Certificate Chain:

Certificate Start Date:

Certificate Status:

Certificate Expiry Date:

4. If the entered password is correct, then you should see a **file read successfully** message.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

```
▾ CN=[redacted], OU=[redacted], O=[redacted], C=US
  ▾ CN=[redacted], OU=[redacted], O=[redacted], C=US
    ▾ CN=[redacted]
        CN=[redacted]                                     ood City, ST=California, C=...
```

Token Proxy Certificate Manager

PFX file read successfully.

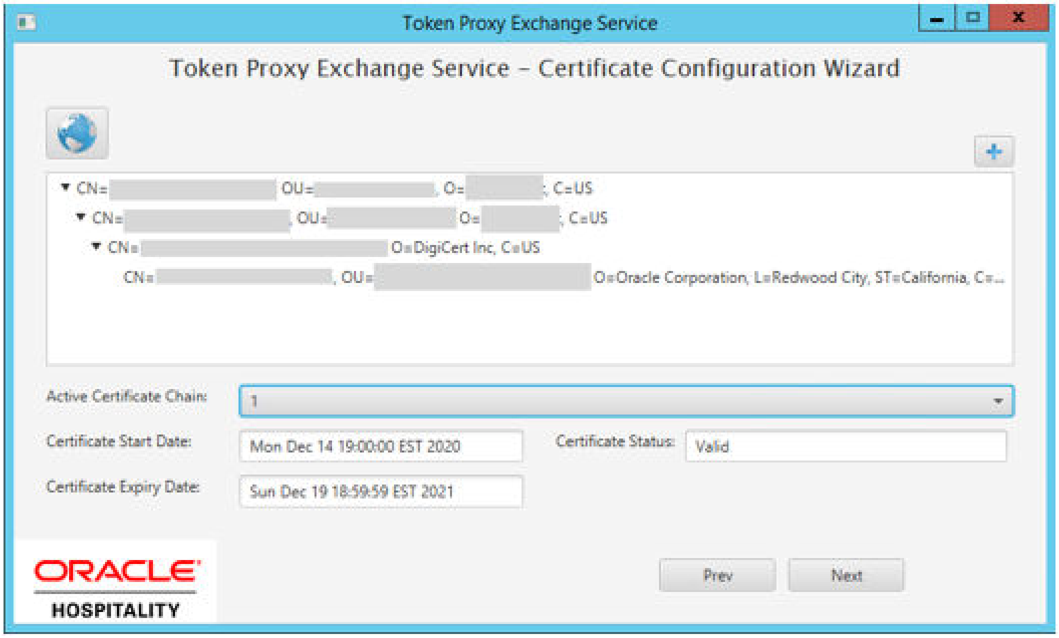
Active Certificate Chain:

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

5. The **Cert Manager** will display the certificate chains from the certificate provided.
6. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
7. This will display the associated **Certificate Expiry Date** and **Status**.



Token Proxy Exchange Service – Certificate Configuration Wizard

- CN=[redacted] OU=[redacted], O=[redacted], C=US
  - CN=[redacted], OU=[redacted] O=[redacted], C=US
    - CN=[redacted] O=DigiCert Inc, C=US
      - CN=[redacted], OU=[redacted] O=Oracle Corporation, L=Redwood City, ST=California, C=...

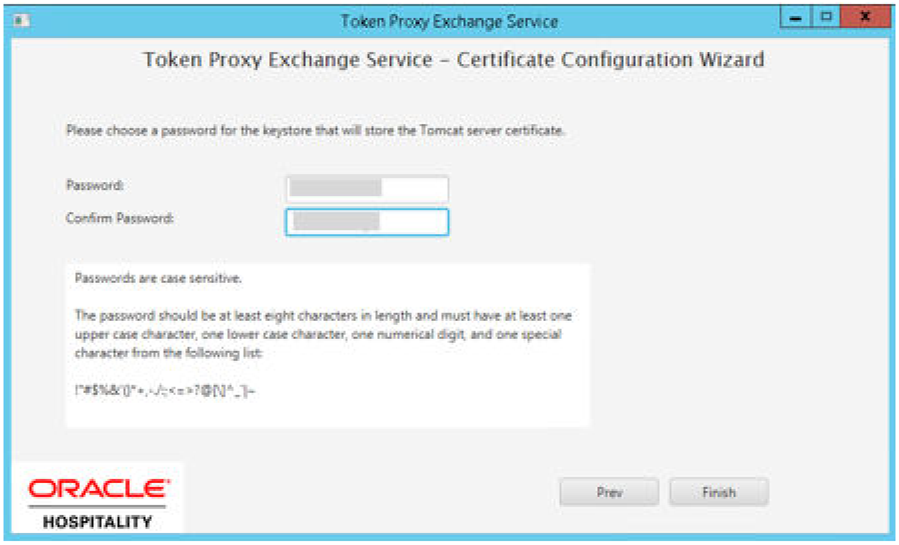
Active Certificate Chain: 1

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

8. Click **Next** to choose a password for the keystore.
9. Provide and confirm the password that meets the minimum requirements, for the keystore that will store listener certificate.



Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the Tomcat server certificate.

Password: [redacted]

Confirm Password: [redacted]

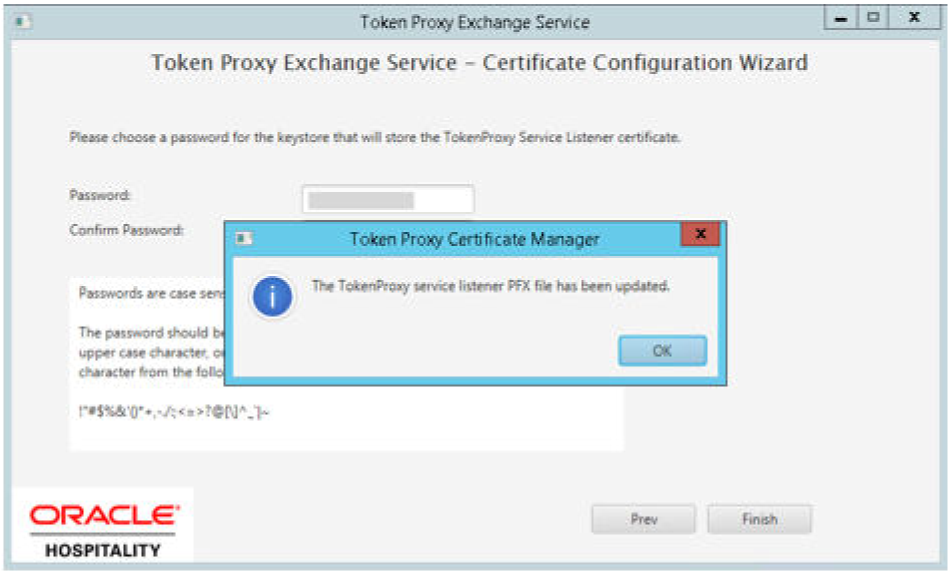
Passwords are case sensitive.

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

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

10. Click **Finish** to configure the listener certificate.

    The Token Proxy service listener PFX file has been updated with OPI_Listener.pfx in directory: \TokenProxy\TokenProxyService\key\.



Token Proxy Exchange Service – Certificate Configuration Wizard

Please choose a password for the keystore that will store the TokenProxy Service Listener certificate.

Password:

Confirm Password:

Passwords are case sens

The password should be
upper case character, o
character from the follo

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

The TokenProxy service listener PFX file has been updated.

11. Click **OK** to return to the option selection screen.

Token Proxy Service Payment Service Providers

> **Note:**
>
> The Token Proxy Service Payment Service Provider Certificates are available for both Tomcat and WebLogic.

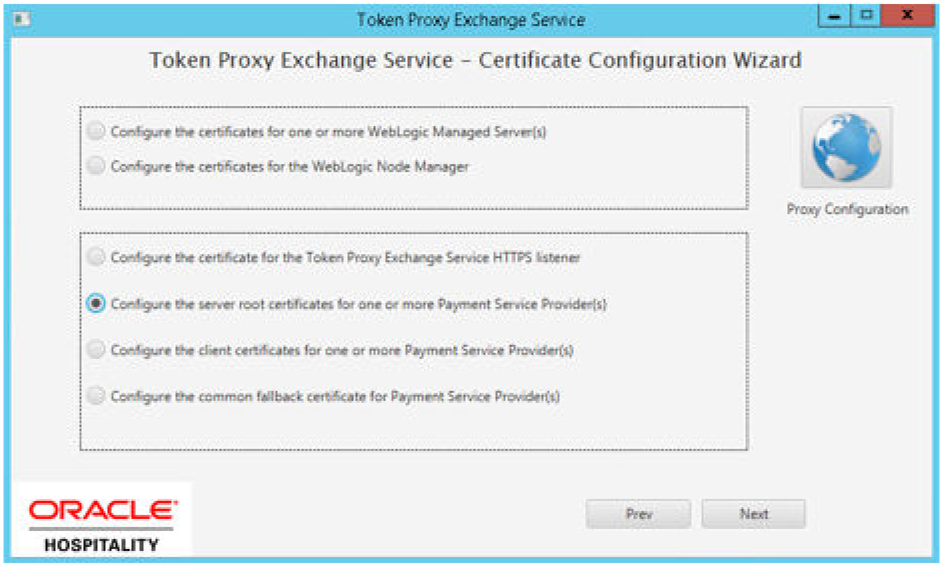
The Cert Manager can also assist importing required certificates into root certificate files for each PSP configured on a Token Proxy system.

It is possible to retrieve the PSP record number from the Token Proxy Service configuration database, and import the selected certificates public key to a keystore it creates with the required file name, and set the password in the TPS wallet, which means this step does not need to be completed with the existing OPIConfigX utility.

The options below will be disabled until database setup has been completed with the OPIConfigX utility.

PSP Server root certificates

1. For the PSP server root certificates, after login select the option **Configure the server root certificates for one or more Payment Service Provider(s)**.

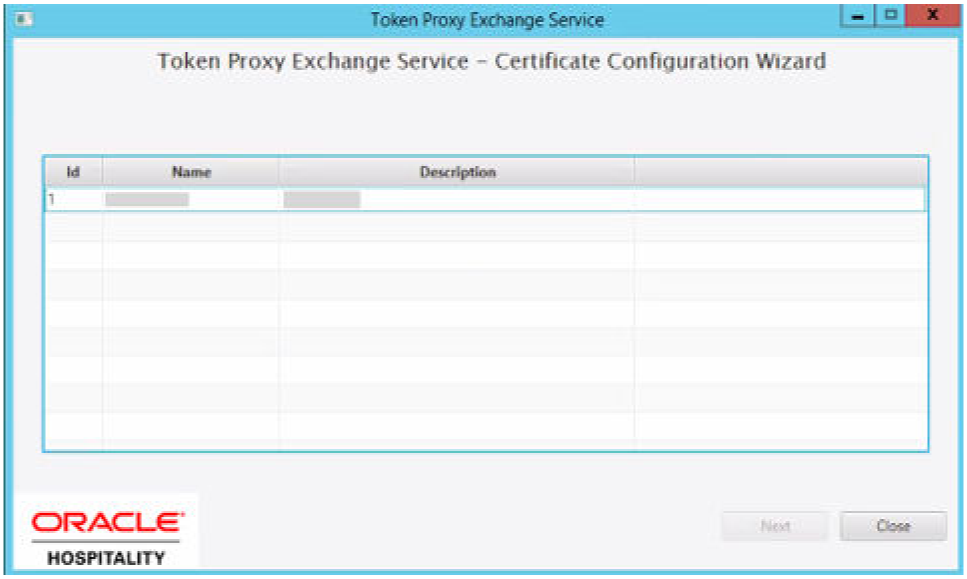


Token Proxy Exchange Service – Certificate Configuration Wizard

○ Configure the certificates for one or more WebLogic Managed Server(s)
○ Configure the certificates for the WebLogic Node Manager

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener
● Configure the server root certificates for one or more Payment Service Provider(s)
○ Configure the client certificates for one or more Payment Service Provider(s)
○ Configure the common fallback certificate for Payment Service Provider(s)

2. You will be provided with a list of the **Payment Service Providers** that are configured in your TokenProxy Webportal.

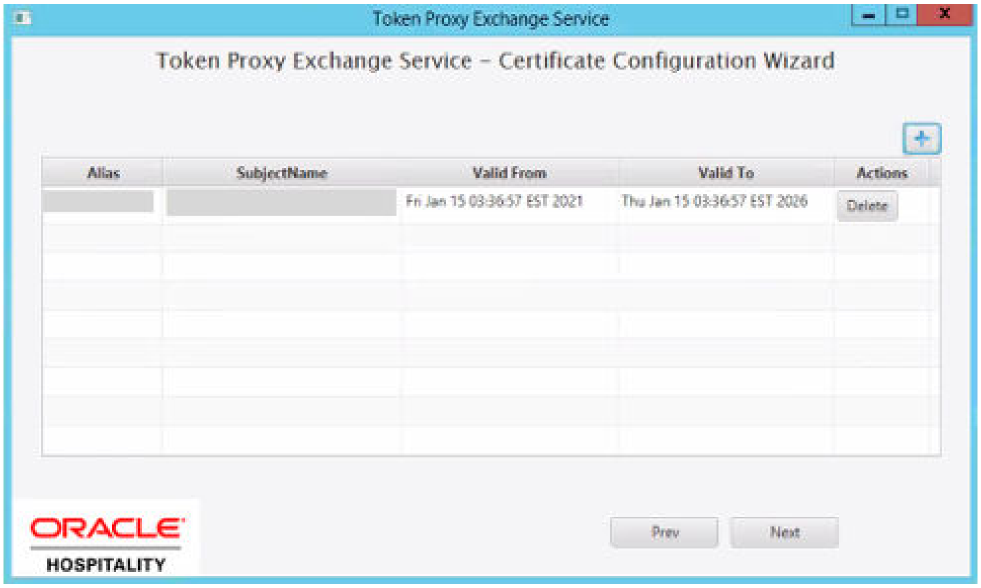


Token Proxy Exchange Service – Certificate Configuration Wizard

Id	Name	Description
1	[redacted]	[redacted]

3. Select the Payment Service Provider that you want to assign a certificate to. If you need to add certificates to multiple Payment Service Providers, repeat the process for each as required.

4. The Cert Manager allows the supported certificate to be imported by browsing or using drag and drop. Browse to the location of the certificate you want to import from **add** icon (+) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).



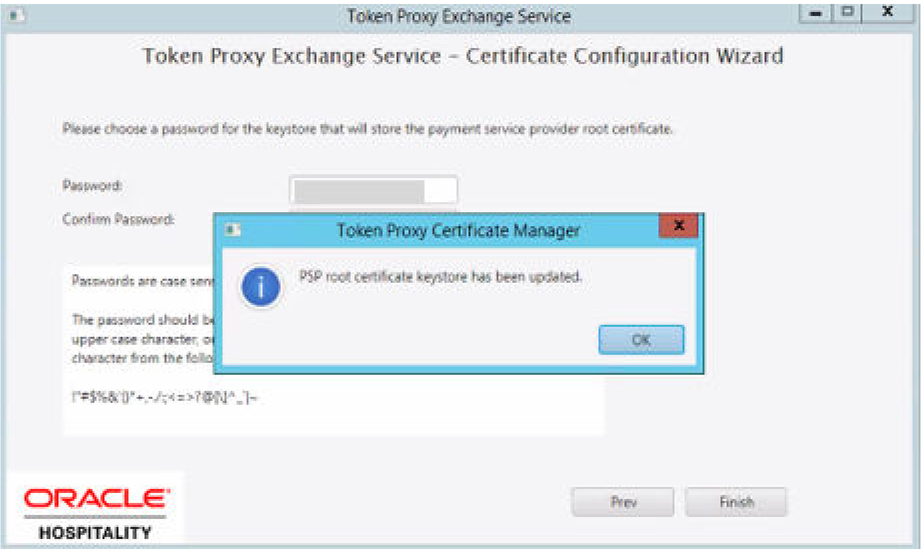
Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

Alias	SubjectName	Valid From	Valid To	Actions
[redacted]	[redacted]	Fri Jan 15 03:36:57 EST 2021	Thu Jan 15 03:36:57 EST 2026	Delete

5. If the password is correct, then you should see a **file read successfully** message.

   The window will display the certificate information from the certificate provided.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password: [redacted]

Confirm Password:

Passwords are case sens

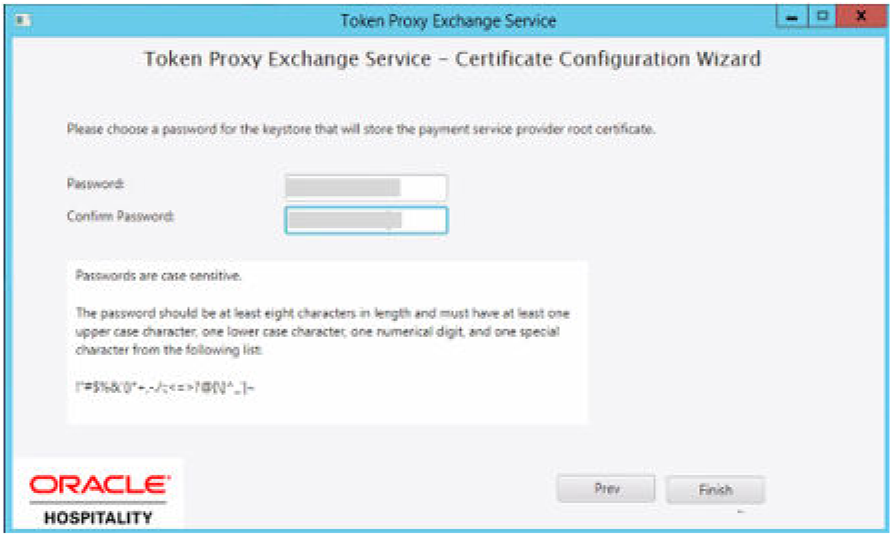
The password should be
upper case character, o
character from the follo

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

Token Proxy Certificate Manager

PSP root certificate keystore has been updated.

6. Click **Next** to choose a password for the keystore.
7. Provide and confirm the password that meets the minimum requirements, for the keystore that will store payment service provider root certificate.



Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

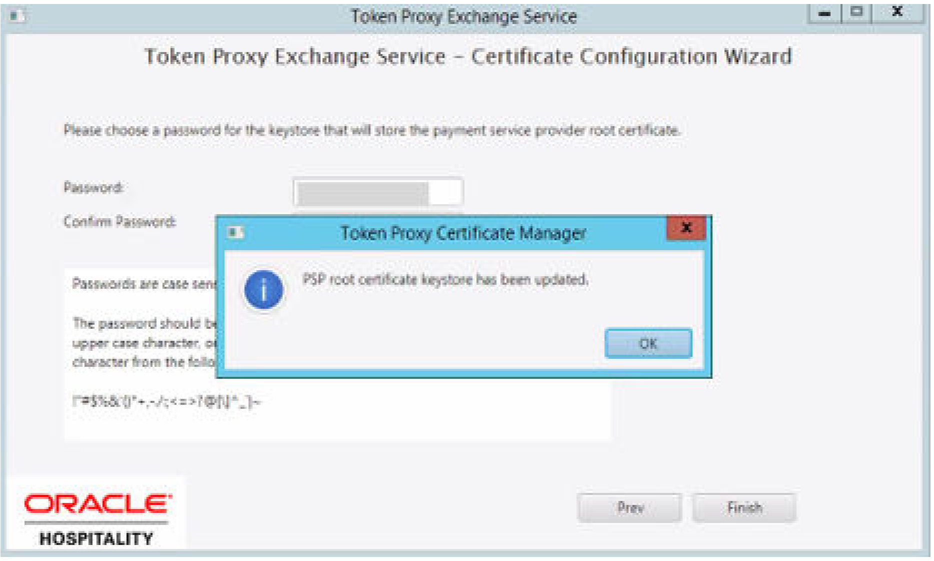
Confirm Password:

Passwords are case sensitive.

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

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

8. Click **Finish** to configure the payment service provider root certificate Select to create the root certificate.
9. **PSP root certificate keystore has been updated** with OPI_PSP_1Root in directory :\TokenProxy\TokenProxyService\key.



Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

Confirm Password:

Passwords are case sens

The password should be
upper case character, o
character from the follo

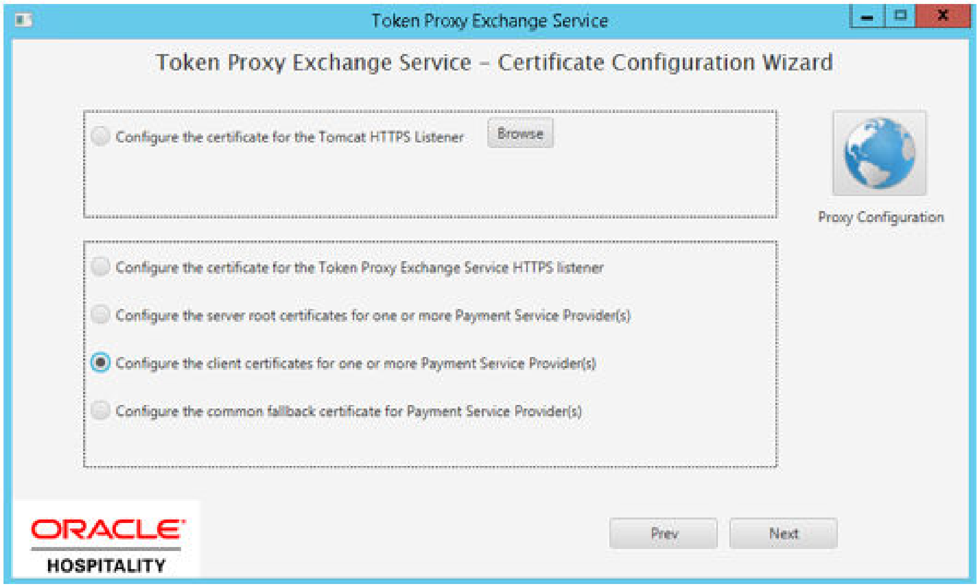
!"#$%&'()*+,-./:;<=>?@[\]^_]~

PSP root certificate keystore has been updated.

10. If all PSPs requiring an update have been updated, click**OK** to return to the option select screen.

PSP Client certificates

1. For PSP Client certificates, after login select the option **Configure the client certificates for one or more Payment Service Provider(s)**.



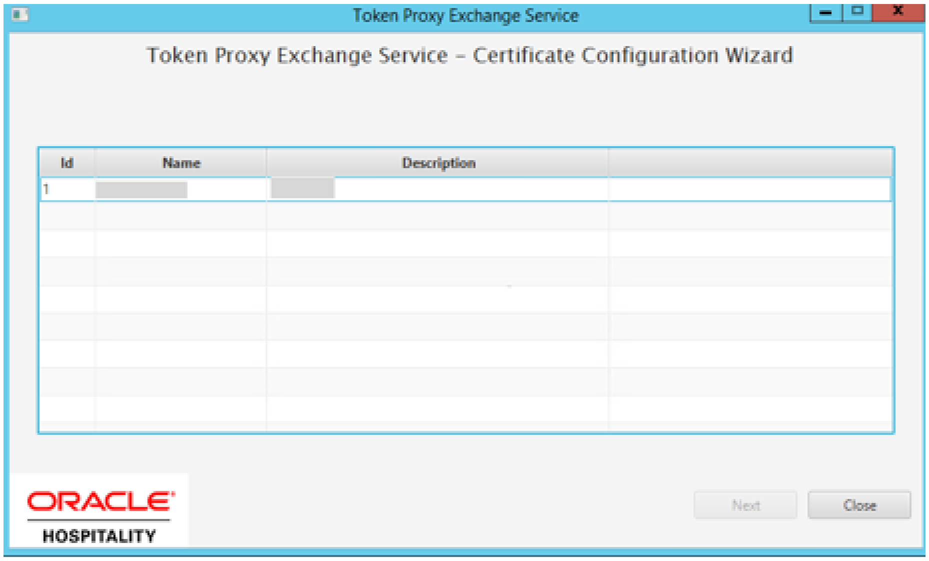
Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

- ○ Configure the certificate for the Tomcat HTTPS Listener

- ○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener
- ○ Configure the server root certificates for one or more Payment Service Provider(s)
- ● Configure the client certificates for one or more Payment Service Provider(s)
- ○ Configure the common fallback certificate for Payment Service Provider(s)

2. You will be provided with a list of the **Payment Service Providers** that are configured in your TokenProxy Webportal.



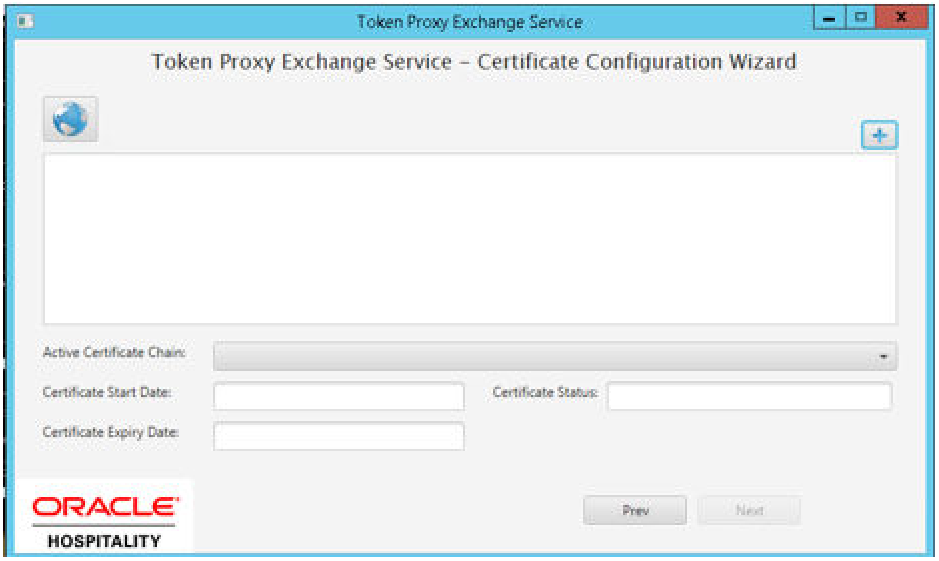
Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

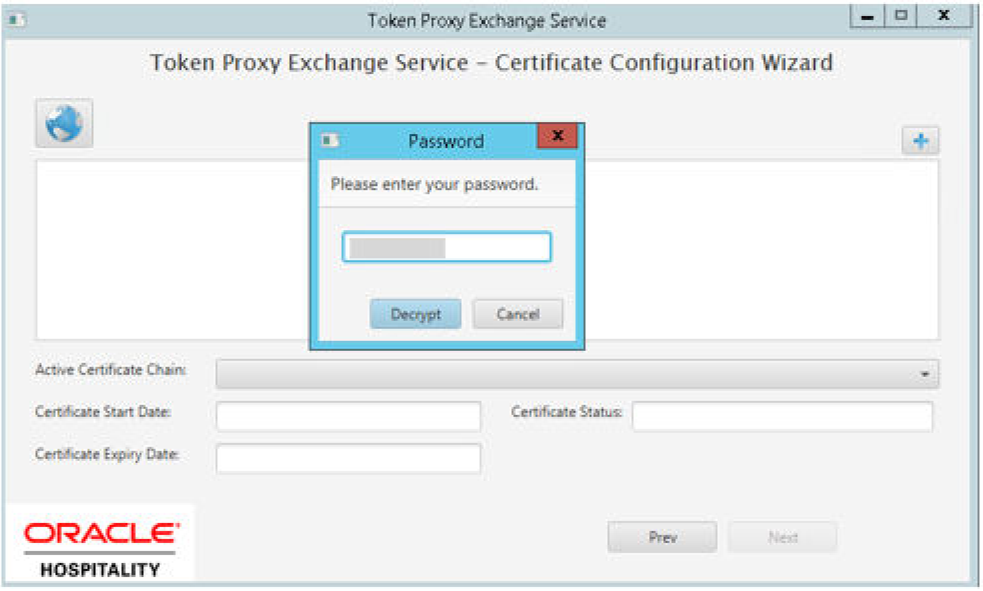
Id	Name	Description	
1	[redacted]	[redacted]	

3. Select the Payment Service Provider that you want to assign a certificate to. If you need to add certificates to multiple Payment Service Providers, repeat the process for each as required.

4. The Cert Manager allows the supported certificate to be imported by browsing or using drag and drop. Browse to the location of the certificate you want to import from **add** icon
   (
   +
) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).

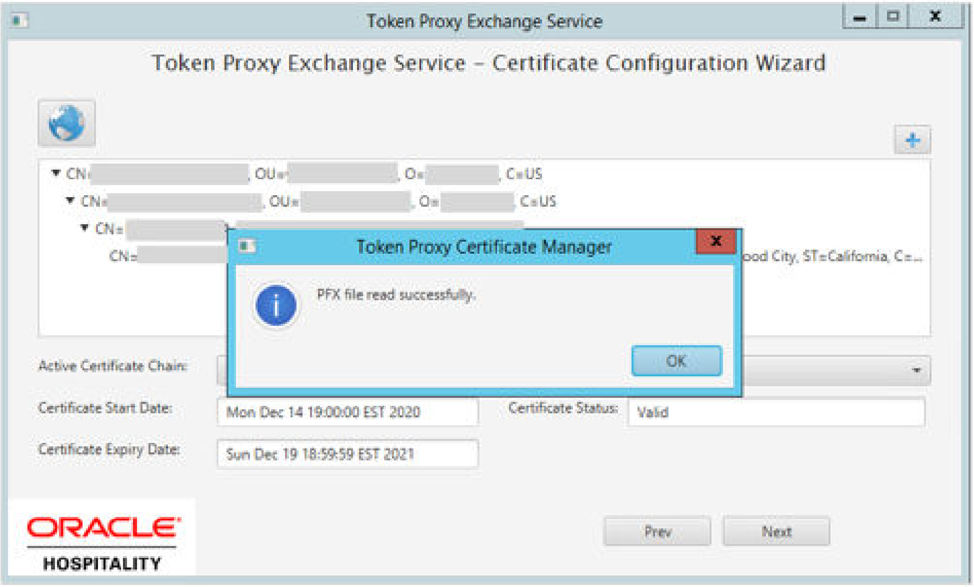

Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

5. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt**.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password
Decrypt
Cancel
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

Please enter your password.

6. If the password is correct, then you should see a **file read successfully** message.



Token Proxy Exchange Service – Certificate Configuration Wizard

- CN=[redacted], OU=[redacted], O=[redacted], C=US
  - CN=[redacted], OU=[redacted], O=[redacted], C=US
    - CN=[redacted]
      - CN=[redacted] ...ood City, ST=California, C=...

Token Proxy Certificate Manager

PFX file read successfully.

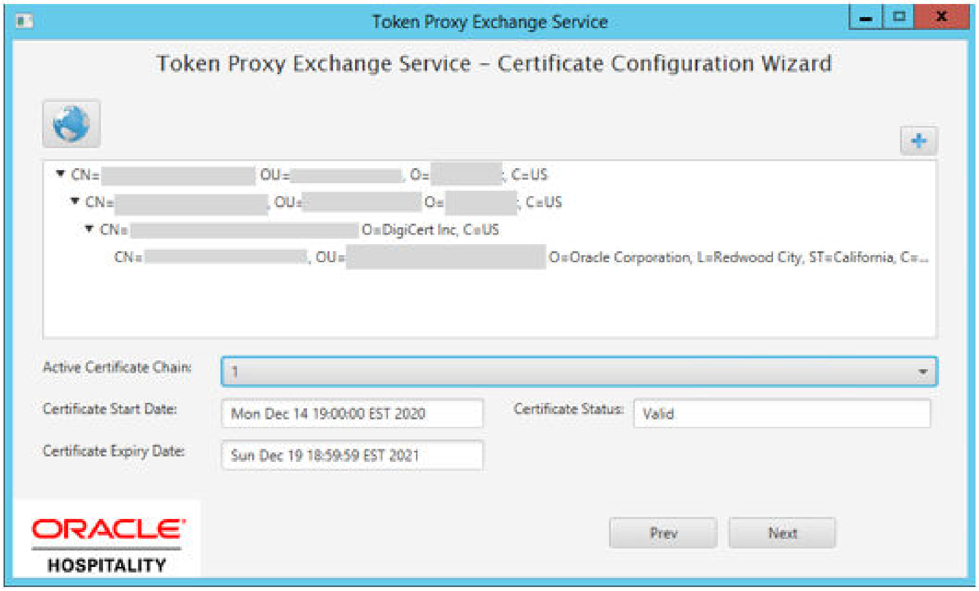
Active Certificate Chain:

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

7. The **Cert Manager** will display the certificate chains from the certificate provided.
8. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
9. This will display the associated **Certificate Expiry Date** and **Status**.



Token Proxy Exchange Service – Certificate Configuration Wizard

- CN=[redacted] OU=[redacted], O=[redacted], C=US
  - CN=[redacted], OU=[redacted] O=[redacted], C=US
    - CN=[redacted] O=DigiCert Inc, C=US
      - CN=[redacted], OU=[redacted] O=Oracle Corporation, L=Redwood City, ST=California, C=...

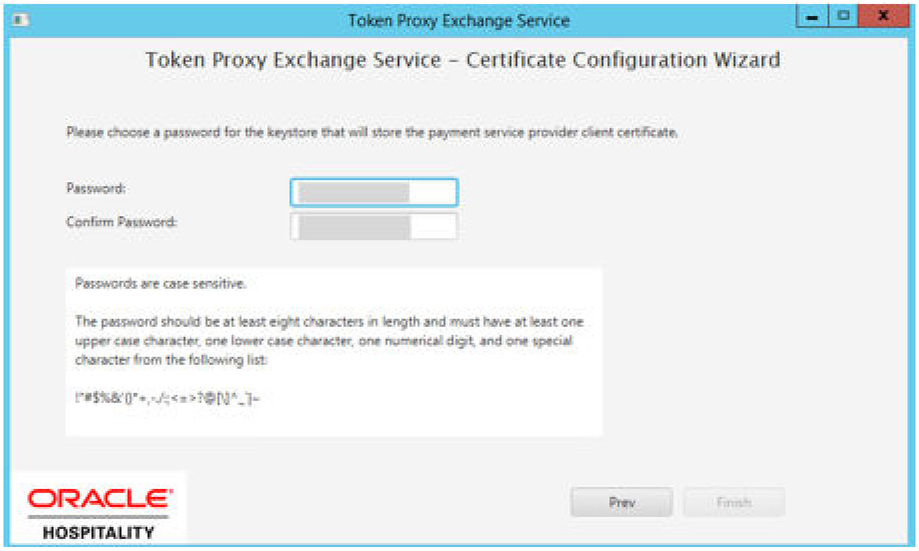
Active Certificate Chain: 1

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

10. Click **Next** to choose a password for the keystore.
11. Provide and confirm the password that meets the minimum requirements, for the keystore that will store payment service provider client certificate.



Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

Confirm Password:

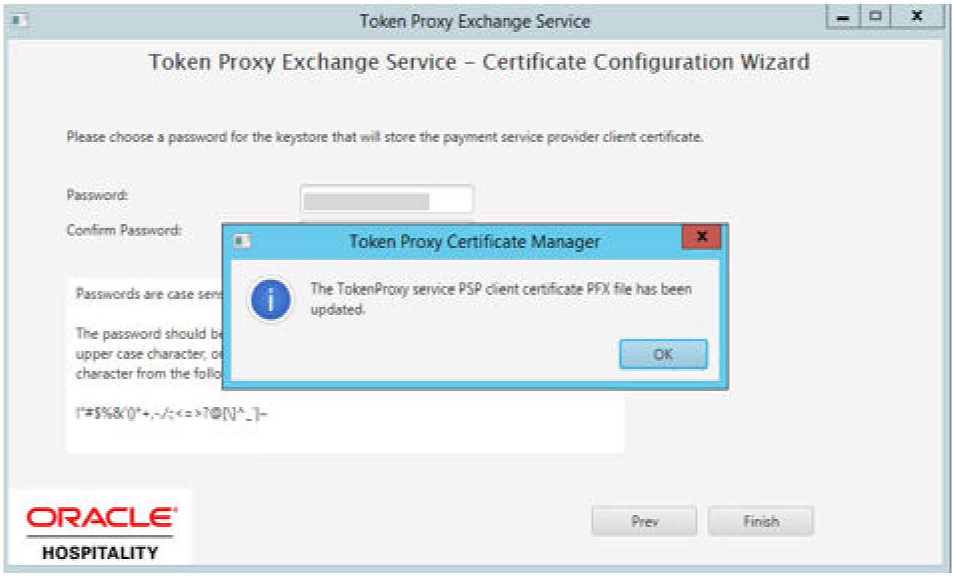
Passwords are case sensitive.

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

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

12. Click **Finish** to configure payment service provider client certificate.

    The TokenProxy service PSP client certificate PFX file has been updated with OPI_PSP_1.pfx in directory: \TokenProxy\TokenProxyService\key.



Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

Confirm Password:

Passwords are case sens

The password should b
upper case character, o
character from the follo

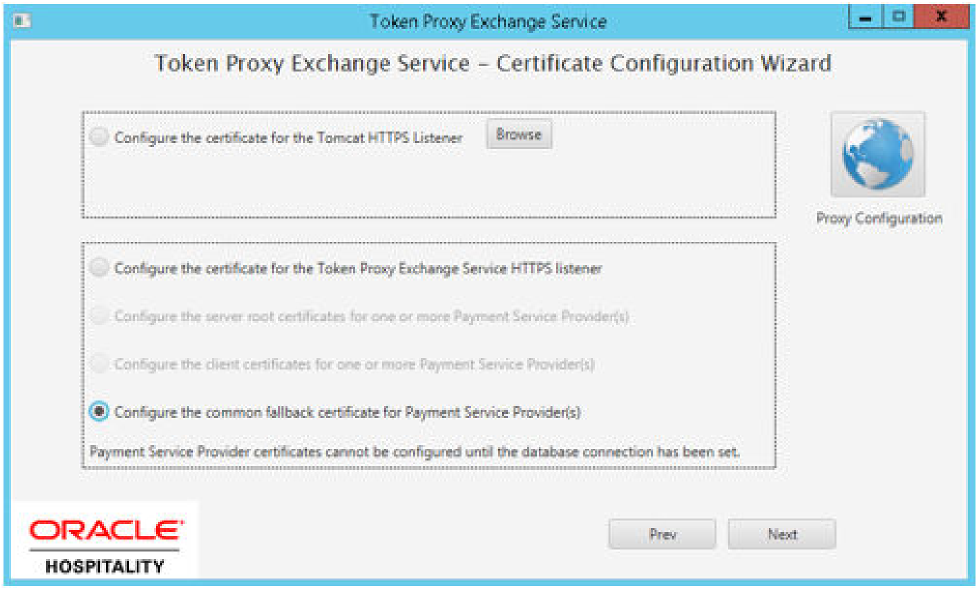
!"#$%&'()*+,-./:;<=>?@[\]^_]~

The TokenProxy service PSP client certificate PFX file has been updated.

13. If all PSPs require an update have been updated, click **OK** to return to the option selection screen.

PSP Common certificates

1. For the PSP Common certificates, after login select the option **Configure the common fallback certificate Payment Service Provider(s)**.



Token Proxy Exchange Service – Certificate Configuration Wizard

○ Configure the certificate for the Tomcat HTTPS Listener

○ Configure the certificate for the Token Proxy Exchange Service HTTPS listener

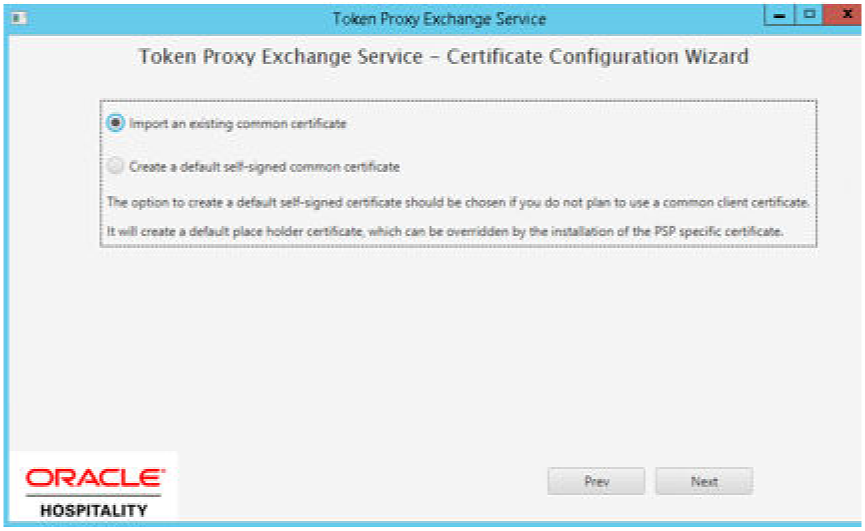
○ Configure the server root certificates for one or more Payment Service Provider(s)

○ Configure the client certificates for one or more Payment Service Provider(s)

● Configure the common fallback certificate for Payment Service Provider(s)

Payment Service Provider certificates cannot be configured until the database connection has been set.

2. You will have two options. If you select the first option **Import an existing common certificate**, then the Cert Manager allows you to import an existing certificate by browsing or using drag and drop. Click **Next**



Token Proxy Exchange Service – Certificate Configuration Wizard

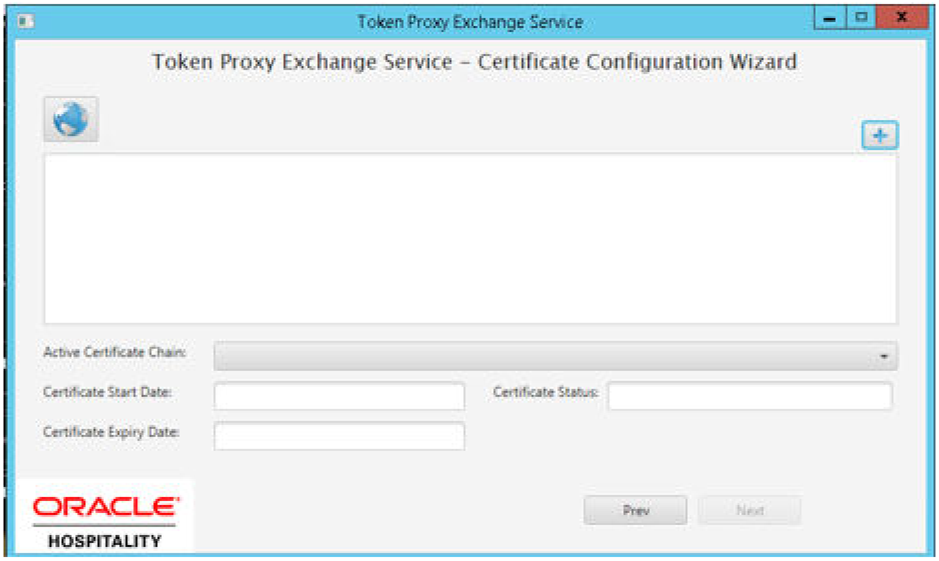
● Import an existing common certificate

○ Create a default self-signed common certificate

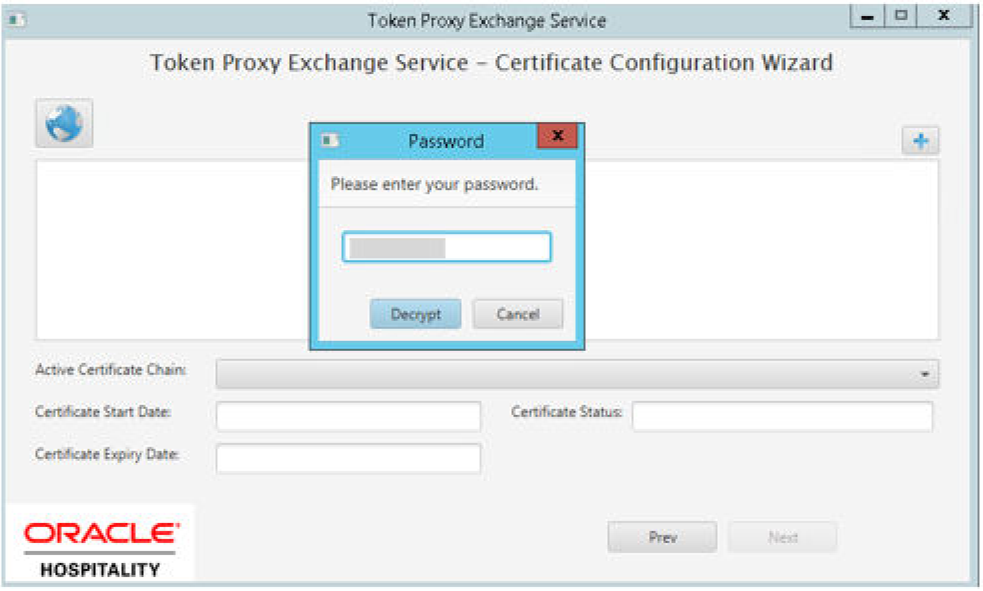
The option to create a default self-signed certificate should be chosen if you do not plan to use a common client certificate. It will create a default place holder certificate, which can be overridden by the installation of the PSP specific certificate.

.

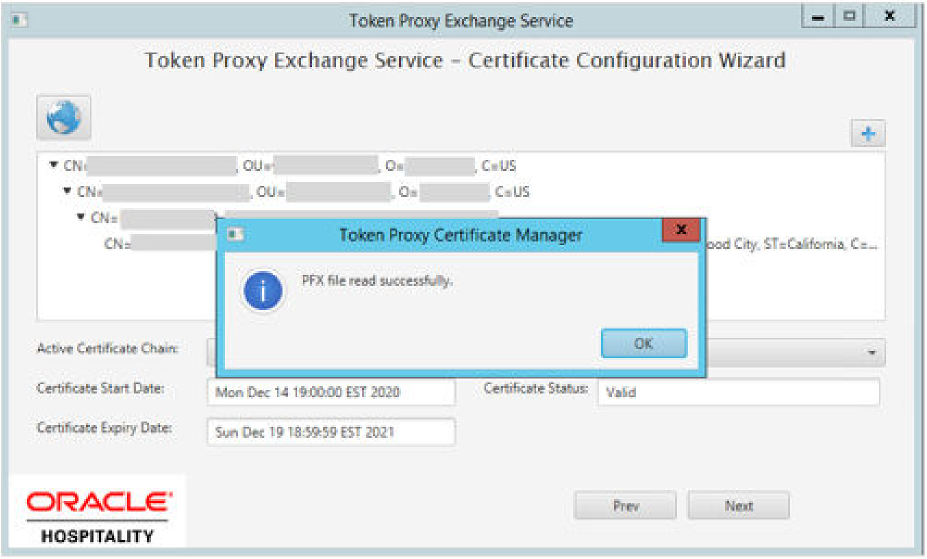
- Browse to the location of the certificate you want to import from **add** icon (+) available on the top right of the page or you can also drag the certificate to the Cert Manager page (be attentive of the File Extension filter in the file browser window).


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

- You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt**.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password
Please enter your password.
Decrypt
Cancel
Active Certificate Chain:
Certificate Start Date:
Certificate Status:
Certificate Expiry Date:
ORACLE
HOSPITALITY
Prev
Next

- If the password is correct, then you should see a **file read successfully** message.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Token Proxy Certificate Manager
OK
Prev
Next
ORACLE
HOSPITALITY

CN=[redacted], OU=[redacted], O=[redacted], C=US
CN=[redacted], OU=[redacted], O=[redacted], C=US
CN=[redacted]
CN=[redacted] ood City, ST=California, C=...

PFX file read successfully.

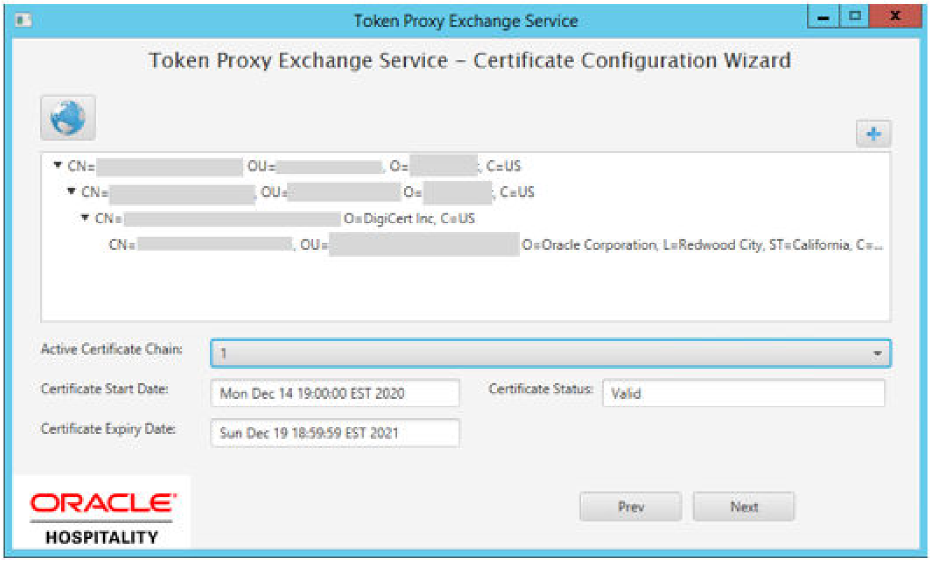
Active Certificate Chain:

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

- The **Cert Manager** will display the certificate chains from the certificate provided.
- Select from the **Active Certificate Chain** drop-down list that requires an alias if more than one is available.
- This will display the associated **Certificate Expiry Date** and **Status**.


Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Prev
Next
ORACLE
HOSPITALITY

CN=[redacted], OU=[redacted], O=[redacted], C=US
CN=[redacted], OU=[redacted], O=[redacted], C=US
CN=[redacted] O=DigiCert Inc, C=US
CN=[redacted], OU=[redacted] O=Oracle Corporation, L=Redwood City, ST=California, C=...

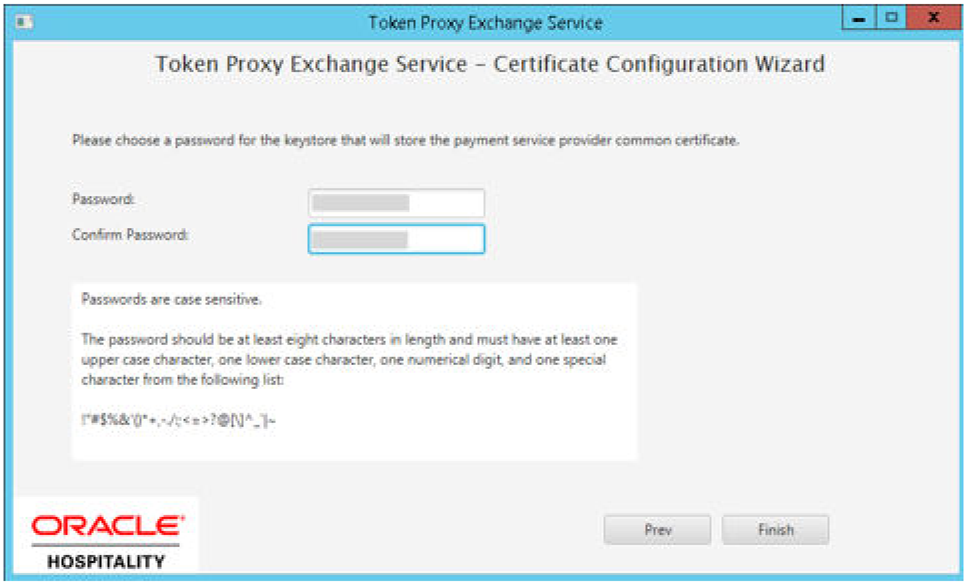
Active Certificate Chain: 1

Certificate Start Date: Mon Dec 14 19:00:00 EST 2020

Certificate Status: Valid

Certificate Expiry Date: Sun Dec 19 18:59:59 EST 2021

- Click **Next** to proceed to choose a password.
- Provide and confirm the password that meets the minimum requirements, for the payment service provider common certificate that will be created.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

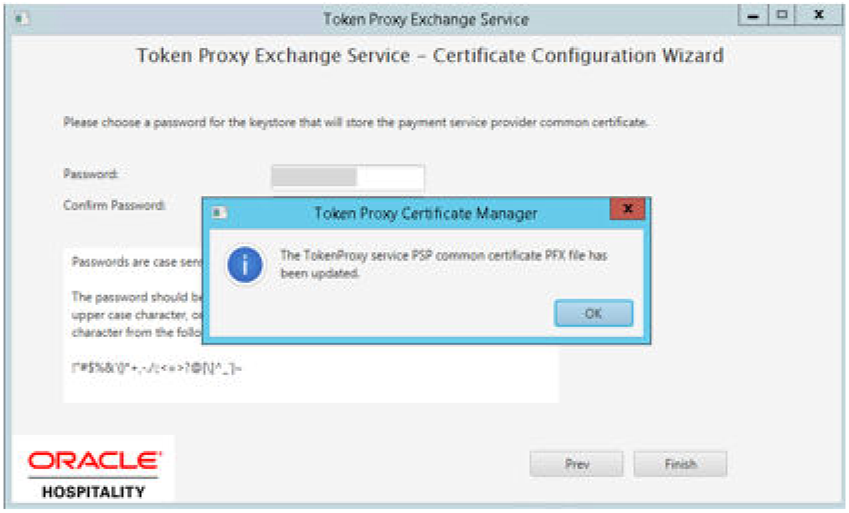
Confirm Password:

Passwords are case sensitive.

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

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

- Click **Finish** to create the payment service provider common certificate.
- The TokenProxy service PSP common certificate PFX file has been updated with OPI_PSP_1Root in directory: \TokenProxy\TokenProxyService\key.



Token Proxy Exchange Service

Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

Confirm Password:

Passwords are case sens

The password should be
upper case character, o
character from the follo

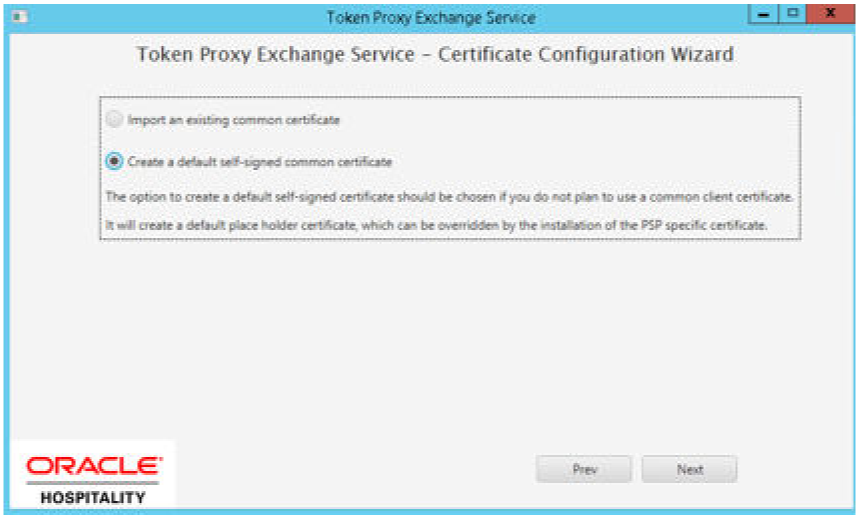
!"#$%&'()*+,-./:;<=>?@[\]^_]~

Token Proxy Certificate Manager

The TokenProxy service PSP common certificate PFX file has been updated.

- Click **OK** to return to the option selection screen.

3. Select the second option **Create a default self-signed common certificate**.



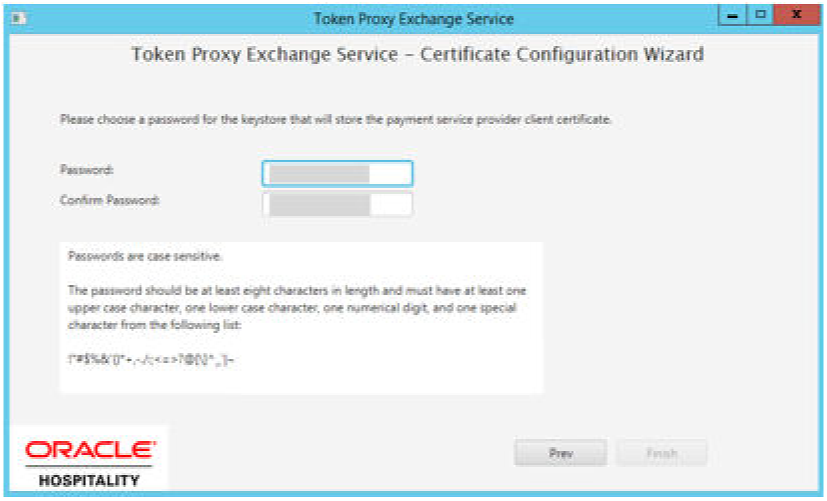
Token Proxy Exchange Service – Certificate Configuration Wizard

○ Import an existing common certificate

● Create a default self-signed common certificate

The option to create a default self-signed certificate should be chosen if you do not plan to use a common client certificate.
It will create a default place holder certificate, which can be overridden by the installation of the PSP specific certificate.

- Click **Next** to choose a password for the keystore.
- Provide and confirm the password that meets the minimum requirements, for the root certificate that will be created.



Token Proxy Exchange Service – Certificate Configuration Wizard

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

Password:

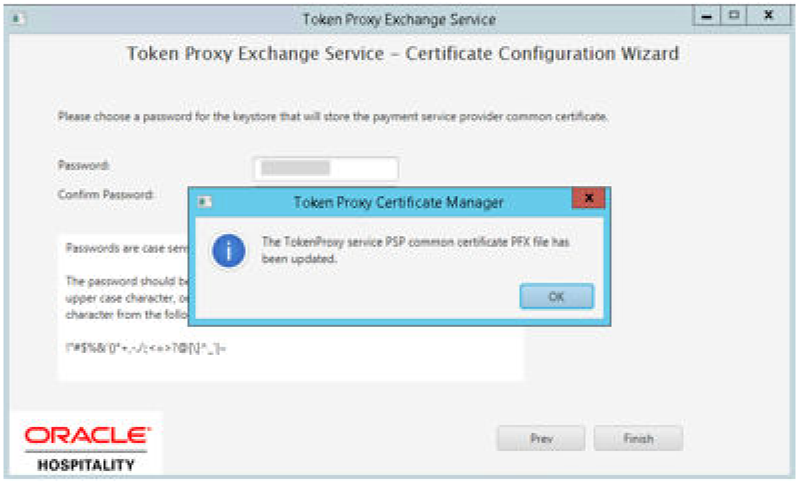
Confirm Password:

Passwords are case sensitive.

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

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

- Click **Finish** to create a default self-signed common certificate.



Token Proxy Exchange Service
Token Proxy Exchange Service – Certificate Configuration Wizard
Password:
Confirm Password:
Token Proxy Certificate Manager
OK
ORACLE
HOSPITALITY
Prev
Finish

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

Passwords are case sen

The password should be
upper case character, o
character from the follo

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

The TokenProxy service PSP common certificate PFX file has been updated.

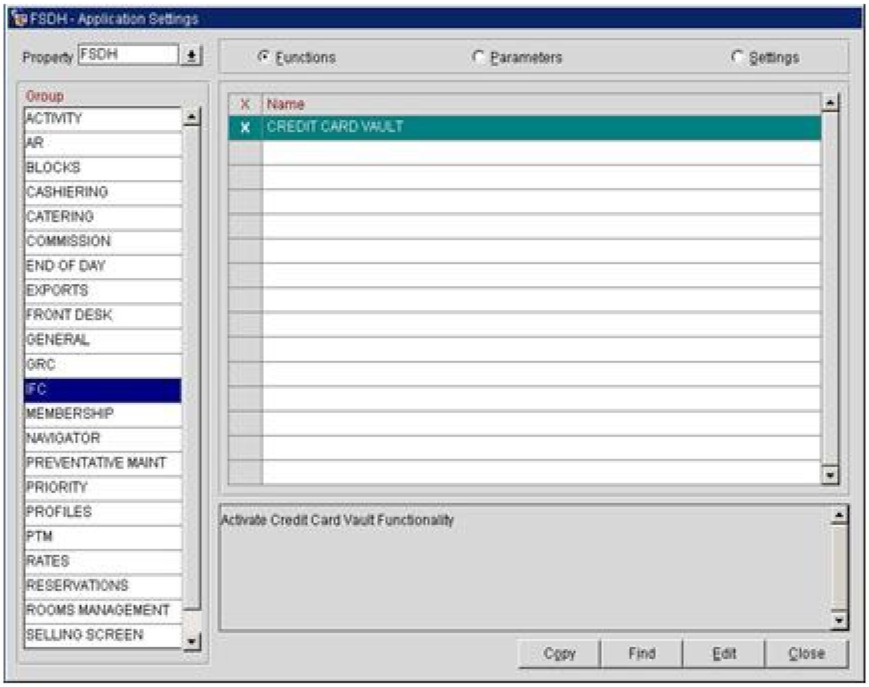
- The TokenProxy service PSP common certificate PFX file has been updated with OPI_PSP_1Root in directory: \TokenProxy\TokenProxyService\key.
- Click **OK** to return to the option selection screen.

10
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 **Oracle Hospitality OPERA Property Management System Installation Guide** on the Oracle Help Center.

Configuring the CC Vault

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


FSDH - Application Settings

Property FSDH

● Functions ○ Parameters ○ Settings

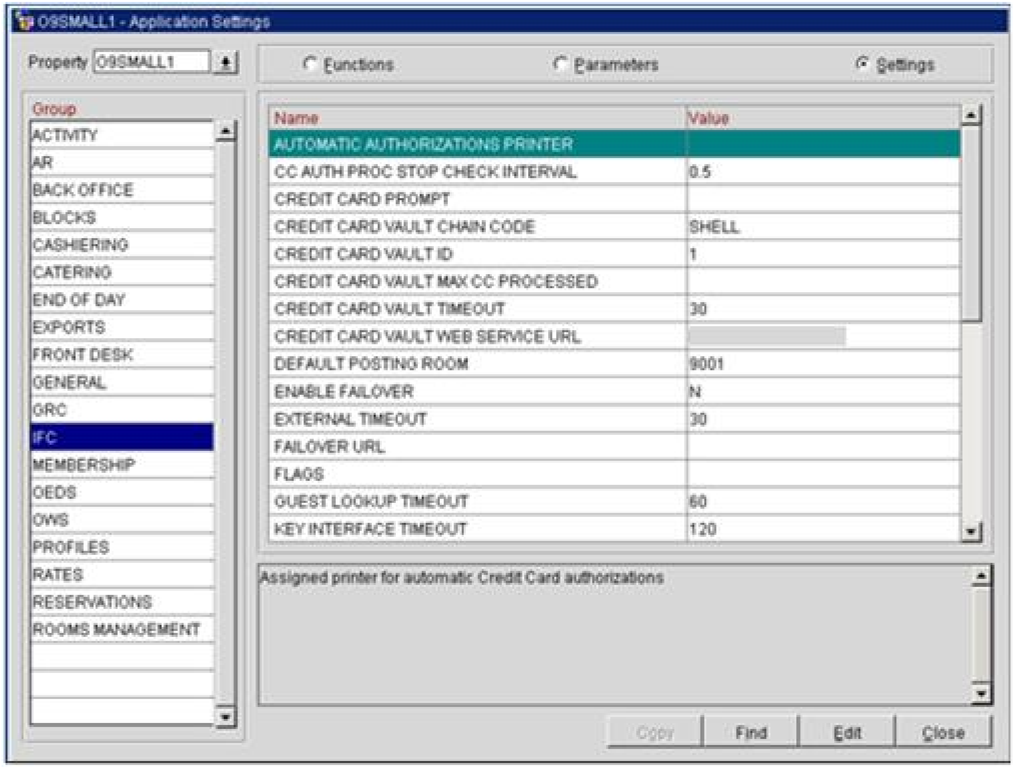
X	Name
X	CREDIT CARD VAULT

Activate Credit Card Vault Functionality

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_opi_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.



Property O9SMALL1

Name	Value
AUTOMATIC AUTHORIZATIONS PRINTER	
CC AUTH PROC STOP CHECK INTERVAL	0.5
CREDIT CARD PROMPT	
CREDIT CARD VAULT CHAIN CODE	SHELL
CREDIT CARD VAULT ID	1
CREDIT CARD VAULT MAX CC PROCESSED	
CREDIT CARD VAULT TIMEOUT	30
CREDIT CARD VAULT WEB SERVICE URL	
DEFAULT POSTING ROOM	9001
ENABLE FAILOVER	N
EXTERNAL TIMEOUT	30
FAILOVER URL	
FLAGS	
GUEST LOOKUP TIMEOUT	60
KEY INTERFACE TIMEOUT	120

Assigned printer for automatic Credit Card authorizations

Application settings are changed based on the OPERA Version 5.5.0.18.1, 5.5.0.19 and 5.6.1.0 above.

These settings can be set per property and are moved to the **Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | Custom Data** tab.

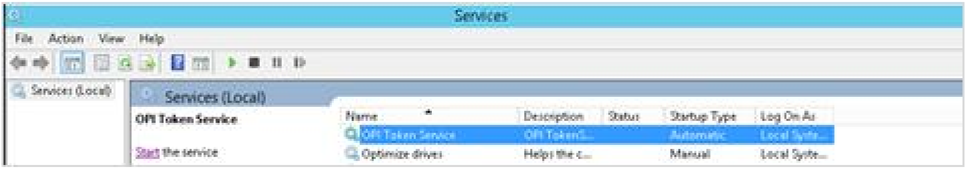
The Token URL is moved to the **Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | General**.

11 Token Proxy Service Maintenance

Services

When the 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.



OPI Token Service

Start the service

Name	Description	Status	Startup Type	Log On As
OPI Token Service	OPI TokenS...		Automatic	Local Syste...
Optimize drives	Helps the c...		Manual	Local Syste...

Modify, Repair, or Remove Token Proxy Service

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

1. Run the Token Proxy Service installer on a system with an existing installation of Token Proxy Service.
2. 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 has been run:

- If the Datasource, Web Portal and Service are selected, then the installer will attempt to install all three components.
- If the Datasource, Web Portal are selected and Service is not selected, then the installer will install Datasource and Web Portal components, and removes the service component.
- If the 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. This is required only when Tomcat is not selected as the web server.
- 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\v19.2\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\

- Schema
- TokenProxyService
- TokenProxyWebPortal
- Utilities

Token Proxy Service Configuration Logs

Configuration Audit data is stored in the Token Proxy Service database. Login 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

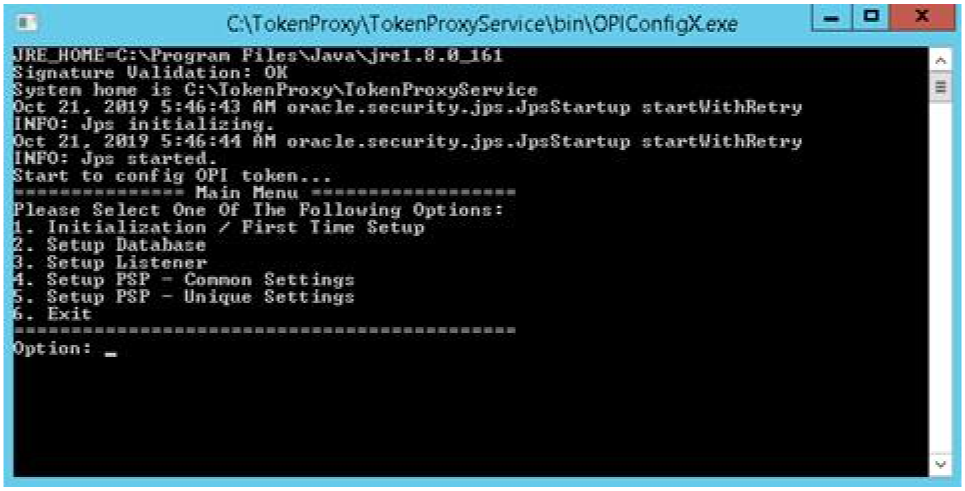
- Lists details of each transaction handled by the Token Proxy Service.
- Rotated daily.
- The current transaction log filename is **transaction.log**.
- The previous day’s transaction log filename is **transaction.log.YYYY-MM-DD** .

Token Proxy Service Password Maintenance

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

You can use the OPIConfigX.exe utility to update passwords post-installation within the Token Proxy Service configuration.

\TokenProxy\TokenProxyService\bin\OPIConfigX.exe



```
JRE_HOME=C:\Program Files\Java\jre1.8.0_161
Signature Validation: OK
System home is C:\TokenProxy\TokenProxyService
Oct 21, 2019 5:46:43 AM oracle.security.jps.JpsStartup startWithRetry
INFO: Jps initializing.
Oct 21, 2019 5:46:44 AM oracle.security.jps.JpsStartup startWithRetry
INFO: Jps started.
Start to config OPI token...
=============== Main Menu ==================
Please Select One Of The Following Options:
1. Initialization / First Time Setup
2. Setup Database
3. Setup Listener
4. Setup PSP - Common Settings
5. Setup PSP - Unique Settings
6. Exit
============================================
Option: _
```

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

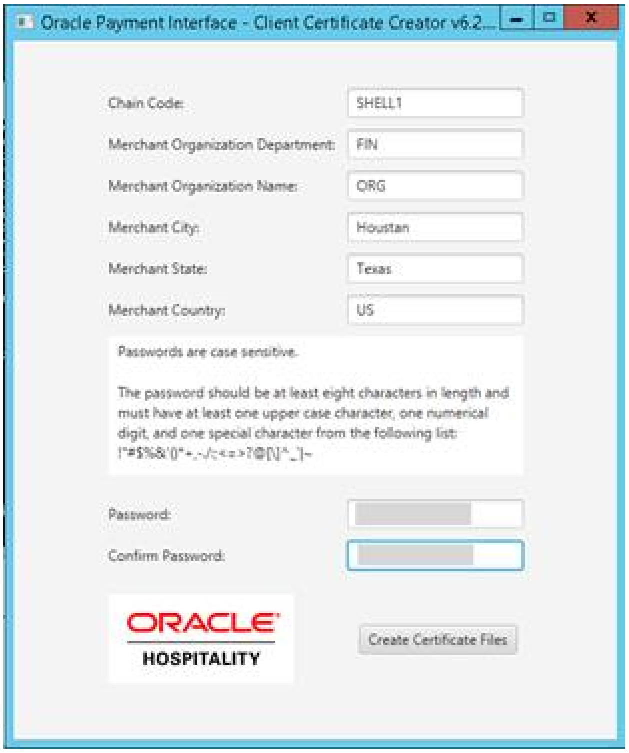
> **Note:**
>
> The OPIConfigX.exe utility does not change the Oracle or MySQL database password itself. The Database Administrator should change the password via the preferred method.

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.



Oracle Payment Interface - Client Certificate Creator v6.2...

Chain Code: SHELL1

Merchant Organization Department: FIN

Merchant Organization Name: ORG

Merchant City: Houstan

Merchant State: Texas

Merchant Country: US

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

Password: [redacted]

Confirm Password: [redacted]

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)

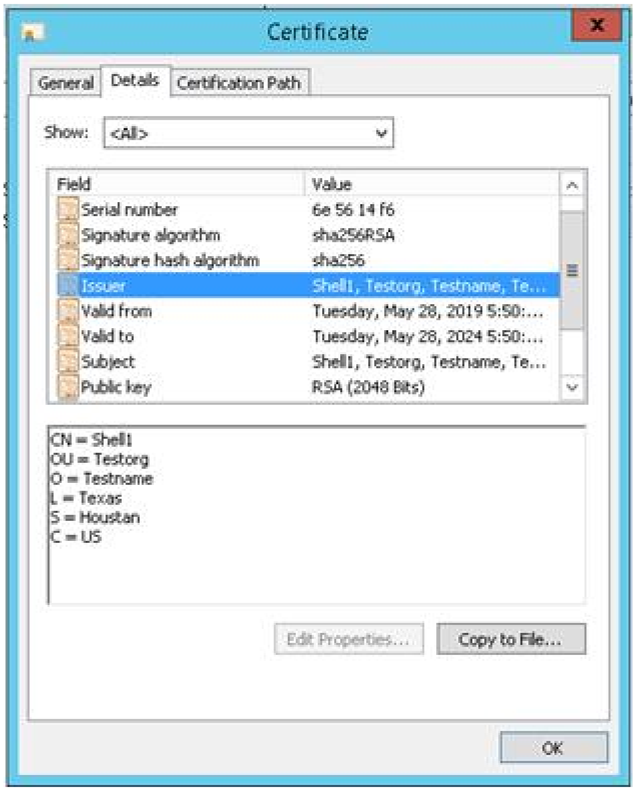
Merchant Organization Department > OU (OrganizationalUnit)

Merchant Organization Name > O (Organization)

Merchant City > L (Locality)

Merchant State > S (StateOrProvinceName)

Merchant Country > C (CountryName)



Field	Value
Serial number	6e 56 14 f6
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Shell1, Testorg, Testname, Te...
Valid from	Tuesday, May 28, 2019 5:50:...
Valid to	Tuesday, May 28, 2024 5:50:...
Subject	Shell1, Testorg, Testname, Te...
Public key	RSA (2048 Bits)

```
CN = Shell1
OU = Testorg
O = Testname
L = Texas
S = Houstan
C = US
```

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**.

If anyone wants to backup their configuration in order to restore it in the event of a disaster recovery, then you need to backup the following files;

- :\TokenProxy\TokenProxyService\properties\cwallet.sso
- :\ProgramData\TokenProxy\tpskeystore
- :\ProgramData\TPSKeystore\TPSKeystore.properties