Oracle® Hospitality Self-Hosted Token Proxy Service

Cert Manager User Guide

Release 6.1

F17704-01

March 2019

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

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

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

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

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

Contents

Preface

This document describes how Cert Manager will improve the usability, and help minimize the user errors during the process of setting up certificates for WebLogic and Token Proxy Service.

The Cert Manager will be used for both Cloud Token Proxy Service and Self Hosted Token Proxy Service, with different GUI/TUI modes plugging into the same framework. Please note that the initial release only includes the GUI mode for use on Windows hosts.

The Cert Manager will be included in new releases of Token Proxy Service from 19.2.0.0, but will also available separately, so that it can be applied and used for maintenance with existing Token Proxy Service installations.

Audience

This document is intended for users concerned with the installation and maintenance of the Token Proxy System.

Customer Support

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

https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Documentation

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

Revision History

Date	Description of Change
January 2019	• Initial publication

1 Certificate Requests

The 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.

Bear 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.

2 Using Cert Manager

In order to use all of Cert Managers functionality, Cert Manager will need to be deployed on all the machines which host WebLogic and Token Proxy Service. It is not designed to deploy certificates on remote machines.

In some environments WebLogic and Token Proxy may reside on the same host, however if your environment has the WebLogic and 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 Token Proxy on the host, and will restrict certain functionality if it does not find WebLogic or Token Proxy Service installations.

Cert Manager requires Java to be installed, but since both WebLogic and 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
```

Oracle 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 Token Proxy. This is available from https://support.oracle.com.

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

In the scenario of separate WebLogic and 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.

3 Wizard Mode

Login

The Login screen has the following options, and you will need to specify valid connection details and credentials for your WebLogic Admin managed server.

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, you will need to change this.
    - The value you provide 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, change this to match the correct port number.
4. **Username**
    - Your user name for the WebLogic Admin Server, i.e. the same Username you use to login to the WebLogic console page.
5. **Password**
    - Your password for the WebLogic Admin Server, i.e. the same Password you use to login to the WebLogic console page.

Once you have supplied valid credentials, select **Login** to proceed.

If your login is successful, you should be navigated to a page where you can select from the following six options;

- Configure the certificates for one or more WebLogic Managed Server(s)
- Configure the certificates for the WebLogic Node Manager
- Configure the certificates for the TokenProxy Exchange Service HTTPS Listener
- Configure the 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)

Proxy Configuration

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

Cert Manager accesses 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).**
2. You will be provided with a list of the managed servers that are present on your WebLogic instance.
3. Select the Managed Server that you wish to assign a certificate to. If you need to add certificates to the **AdminServer** and the **tokenproxy_server**, repeat the process for both.
4. Cert Manager allows supported certificate import by browsing or drag and drop.
5. Browse to the location of the certificate you wish to import from add icon available on the top right of the page or drag the certificate to the Cert Manager page (be mindful of the File Extension filter in the file browser window).
6. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt.**
7. If the password entered is correct, you should see a **file read successfully** message.
8. In the **Java Standard Trust Store,** display will be the certificate chains from the certificate provided.
9. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
10. This will display the associated **Certificate Expiry Date** and **Status.**
11. Select **Next** to proceed to the root certificate creation page.

12. Provide and confirm a password, meeting the minimum requirements, for the root certificate that will be created.
13. Select **Configure** to create the root certificate.
14. **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, if all the Managed Servers requires an update have been updated, select **Close** to return to the option select screen.

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.**
2. You will be provided with a list of the machines that are present on your WebLogic instance.
3. Select the Machine that you wish to assign a certificate to. If you need to add certificates to the **Machine 1** and the **Machine 2**, repeat the process for both.
4. Cert Manager allows supported certificate import by browsing or drag and drop.
5. Browse to the location of the certificate you wish to import from add icon available on the top right of the page or drag the certificate to the Cert Manager page (be mindful of the File Extension filter in the file browser window).
6. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt.**
7. If the entered password is correct, you should see a **file read successfully** message.
8. In the **Java Standard Trust Store**, display will be the certificate chains from the certificate provided.
9. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
10. This will display the associated **Certificate Expiry Date** and **Status.**
11. 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 could 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 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 NodeManger 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.

12. Select **Next** to proceed to the root certificate creation page.
13. Provide and confirm a password, meeting the minimum requirements, for the root certificate that will be created.
14. Select **Configure** to create the root certificate.
15. **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. You will be returned to the option select screen.

TPS Listener Certificate

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.**
2. Cert Manager allows supported certificate import by browsing or drag and drop.
3. Browse to the location of the certificate you wish to import from add icon available on the top right of the page or drag the certificate to the Cert Manager page (be mindful of the File Extension filter in the file browser window).
4. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt.**
5. If the entered password was correct you should see a **file read successfully** message.
6. In the **Java Standard Trust Store,** display will be the certificate chains from the certificate provided.
7. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
8. This will display the associated **Certificate Expiry Date** and **Status.**
9. Select **Next** to proceed to the root certificate creation page.
10. Provide and confirm a password, meeting the minimum requirements, for the root certificate that will be created.
11. Select **Finish** to create the root certificate.

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

TPS Payment Service Providers

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 PSP server root certificates, after login select the option **Configure the server root certificates for one or more Payment Service Providers.**
2. You will be provided with a list of the **Payment Service Providers** that are configured in your TokenProxy Webportal.
3. Select the Payment Service Provider that you wish to assign a certificate to. If you need to add certificates to multiple Payment Service Providers, repeat the process for each as required.
4. Cert Manager allows supported certificate import by browsing or drag and drop.
5. Browse to the location of the certificate you wish to import from add icon available on the top right of the page or drag the certificate to the Cert Manager page (be mindful of the File Extension filter in the file browser window).
6. You should see a **file read successfully** message.
7. The window will display the certificate information from the certificate provided.
8. Select **Next** to proceed to the root certificate creation page.
9. Provide and confirm a password, meeting the minimum requirements, for the root certificate that will be created.
10. Select **Finish** to create the root certificate.
11. **PSP root certificate keystore has been updated** with OPI_PSP_1Root in directory :\TokenProxy\TokenProxyService\key
12. If all PSP requiring an update have been updated, select **Close** 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 Providers.**
2. You will be provided with a list of the **Payment Service Providers** that are configured in your TokenProxy Webportal.

3. Select the Payment Service Provider that you wish to assign a certificate to. If you need to add certificates to multiple Payment Service Providers, repeat the process for each as required.
4. Cert Manager allows supported certificate import by browsing or drag and drop.
5. Browse to the location of the certificate you wish to import from add icon available on the top right of the page or drag the certificate to the Cert Manager page (be mindful of the File Extension filter in the file browser window).
6. You will be prompted to supply the password for the certificate you have selected. Enter the password and select **Decrypt.**
7. If the password was correct you should see a **file read successfully** message
8. In the **Java Standard Trust Store**, display will be the certificate chains from the certificate provided.
9. Select from the **Active Certificate Chain** drop-down list, the required alias if more than one is available.
10. This will display the associated **Certificate Expiry Date** and **Status.**
11. Select **Next** to proceed to the root certificate creation page.
12. Provide and confirm a password, meeting the minimum requirements, for the root certificate that will be created.
13. Select **Finish** to create the root certificate.
14. **The TokenProxy service PSP client certificate PFX file has been updated** with OPI_PSP_1.pfx in directory :\TokenProxy\TokenProxyService\key
15. If all the PSP requires an update have been updated, select **Close** to return to the option select screen.

PSP Common certificates

1. For PSP Common certificates, after login select the option **Configure the common fallback certificate Payment Service Providers.**
2. You will have two options available first option **Import an existing common certificate will allow you to** import an existing certificate.
3. If you select second option **Create a default self-signed common certificate.**
4. Select **Next** to proceed to the root certificate creation page.
5. Provide and confirm a password, meeting the minimum requirements, for the root certificate that will be created.
6. Select **Finish** to create the root certificate.
7. **The TokenProxy service PSP common certificate PFX file has been updated** with OPI_PSP_1Root in directory :\TokenProxy\TokenProxyService\key