Oracle® Healthcare Precision Medicine

Administrator's Guide

Release 1.0

E76044-01

June 2016

ORACLE®

Oracle Healthcare Precision Medicine Administrator's Guide, Release 1.0

E76044-01

Contents

Preface v

Audience v
Disclaimer v
Documentation Accessibility v
Finding Information and Patches on My Oracle Support v
Finding Documentation on Oracle Technology Network vii
Related Documents vii
Conventions viii

1 EMR Configuration

1.1 Overview 1-1
1.2 Configuration 1-1
1.3 Configuring the OPSS Keystore 1-3
1.3.1 Using the Enterprise Manager 1-3
1.3.2 Using the WebLogic Scripting Tool 1-6
1.3.3 Granting Permission to Use the Keystore 1-6

2 External System Configurations

2.1 Dalliance 2-1
2.1.1 Dalliance Configuration 2-1
2.1.1.1 Retrieving a List of Genome Configurations 2-1
2.1.1.2 Adding a Genome Configuration 2-2
2.1.2 Dalliance Configuration by Genome Version 2-3
2.1.2.1 Retrieving Configuration for a Genome Version 2-3
2.1.2.2 Updating an Existing Genome Configuration 2-3
2.1.2.3 Deleting a Genome Version Configuration 2-4
2.2 Thomson Reuters 2-4
2.2.1 Thomson Reuters Credential Configuration 2-5
2.2.1.1 Retrieving a List of User Credentials Configured for Thomson Reuters 2-5
2.2.1.2 Adding a User Credential for Invoking Thomson Reuters 2-5
2.2.1.3 Updating Organization Level User Credentials for Invoking Thomson Reuters 2-6
2.2.1.4 Deleting Organization Level User Credential U. sed for Invoking Thomson Reuters 2-6
2.2.2 User-Specific Thomson Reuters Credential Configuration 2-7

2.2.2.1 Getting Credential Details for a User Configured for Thomson Reuters 2-7
2.2.2.2 Updating User Credentials for Invoking Thomson Reuters 2-7
2.2.2.3 Deleting User Credentials Used for Invoking Thomson Reuters 2-8
2.3 N-Of-One 2-8
2.3.1 N-of-One Credential Configuration 2-8
2.3.1.1 Getting Credentials Configured for N-of-One 2-9
2.3.1.2 Adding a Credential for Invoking N-of-One 2-9
2.3.1.3 Updating Credentials for Invoking N-of-One 2-10
2.3.1.4 Deleting Credential Used for Invoking N-of-One 2-10
2.4 Enabling or Disabling Features Related to External Systems 2-10
2.4.1 Returning State of Current Features 2-11
2.4.2 Enabling or Disabling Features in Oracle Healthcare Precision Medicine 2-11

3 Published Report Template Configuration

3.1 Configuring the Logo in the Report Header and Footer 3-1
3.2 Configuring the Text in the Report Header and Footer 3-1

4 Annotation Pane Configuration

4.1 GET Annotation Pane Configuration 4-1
4.2 UPDATE Annotation Pane Configuration 4-2

5 Loader API

5.1 Fetch Job Status and Log 5-1
5.1.1 Job Status 5-1
5.1.2 Job Log 5-1
5.2 Data Ingestion with Loaders 5-2
5.2.1 Preferred Transcript Loader 5-2

Index

Preface

This document describes how to perform various configurations for Oracle Healthcare Precision Medicine. The user installing Oracle Healthcare Foundation should have some knowledge of WebLogic and Linux.

Audience

This document is intended for:

- The implementation team that wants to install OHPM
- System Administrators

Disclaimer

The Oracle Healthcare Precision Medicine software is only a search tool and is not intended to, and must not replace the clinician's judgment or experience. Furthermore, the healthcare professional using this search tool should employ their professional judgment concerning the reliability and accuracy of the information in the various knowledge databases that are employed or selected as content for reports generated using Oracle Healthcare Precision Medicine.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Finding Information and Patches on My Oracle Support

Your source for the latest information about Oracle Healthcare Analytics Data Integration is Oracle Support's self-service Web site, My Oracle Support (formerly MetaLink).

Before you install and use an Oracle software release, always visit the My Oracle Support Web site for the latest information, including alerts, release notes, documentation, and patches.

Creating a My Oracle Support Account

You must register at My Oracle Support to obtain a user name and password account before you can enter the Web site.

To register for My Oracle Support:

1. Open a Web browser to http://support.oracle.com.
2. Click the **Register here** link to create a My Oracle Support account. The registration page opens.
3. Follow the instructions on the registration page.

Signing In to My Oracle Support

To sign in to My Oracle Support:

1. Open a Web browser to http://support.oracle.com.
2. Click **Sign In**.
3. Enter your user name and password.
4. Click **Go** to open the My Oracle Support home page.

Searching for Knowledge Articles by ID Number or Text String

The fastest way to search for product documentation, release notes, and white papers is by the article ID number.

To search by the article ID number:

1. Sign in to My Oracle Support at http://support.oracle.com.
2. Locate the Search box in the upper right corner of the My Oracle Support page.
3. Click the sources icon to the left of the search box, and then select Article ID from the list.
4. Enter the article ID number in the text box.
5. Click the magnifying glass icon to the right of the search box (or press the Enter key) to execute your search.

   The Knowledge page displays the results of your search. If the article is found, click the link to view the abstract, text, attachments, and related products.

In addition to searching by article ID, you can use the following My Oracle Support tools to browse and search the knowledge base:

- Product Focus — On the Knowledge page, you can drill into a product area through the Browse Knowledge menu on the left side of the page. In the Browse any Product, By Name field, type in part of the product name, and then select the product from the list. Alternatively, you can click the arrow icon to view the complete list of Oracle products and then select your product. This option lets you focus your browsing and searching on a specific product or set of products.
- Refine Search — Once you have results from a search, use the Refine Search options on the right side of the Knowledge page to narrow your search and make the results more relevant.

- Advanced Search — You can specify one or more search criteria, such as source, exact phrase, and related product, to find knowledge articles and documentation.

Finding Patches on My Oracle Support

Be sure to check My Oracle Support for the latest patches, if any, for your product. You can search for patches by patch ID or number, or by product or family.

To locate and download a patch:

1. Sign in to My Oracle Support at http://support.oracle.com.
2. Click the **Patches & Updates** tab.

   The Patches & Updates page opens and displays the Patch Search region. You have the following options:

   - In the Patch ID or Number is field, enter the primary bug number of the patch you want. This option is useful if you already know the patch number.
   - To find a patch by product name, release, and platform, click the Product or Family link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.
4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download**. Follow the instructions on the screen to download, save, and install the patch files.

Finding Documentation on Oracle Technology Network

The Oracle Technology Network Web site contains links to all the latest Oracle user and reference documentation. To find user documentation for Oracle products:

1. Go to the Oracle Technology Network at

   http://www.oracle.com/technetwork/index.html and log in.
2. Mouse over the Support tab, then click the **Documentation** hyperlink.

   Alternatively, go to Oracle Documentation page at

   http://www.oracle.com/technology/documentation/index.html
3. Navigate to the product you need and click the link.

   For example, scroll down to the Applications section and click Oracle Health Sciences Applications.
4. Click the link for the documentation you need.

Related Documents

For more information, see the following documents:

- Oracle Healthcare Precision Medicine Installation Guide
- *Oracle Healthcare Precision Medicine Administrator's Guide*
- *Oracle Healthcare Precision Medicine User's Guide*
- *Oracle Healthcare Precision Medicine Security Guide*
- *Oracle Healthcare Precision Medicine Release Notes*

- *Oracle Healthcare Precision Medicine Release Content Document*
- *Oracle Healthcare Precision Medicine Electronic Technical Reference Manual*
- *Oracle Healthcare Precision Medicine Third Party Licenses and Notices*

Conventions

The following text conventions are used in this document:

boldface - Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

italic - Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

`monospace` - Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 EMR Configuration

This section describes EMR configuration. It contains the following topics:

- Section 1.1, "Overview"
- Section 1.2, "Configuration"
- Section 1.3, "Configuring the OPSS Keystore"

1.1 Overview

You must configure OHPM to successfully integrate with EPIC EMR so that genomic reports can be published to EMR from OHPM. This section describes how to configure EMR.

Multiple EMR integration configurations can be created and maintained in OHPM. However, at any given point in time, only one configuration will remain in the active status. If not, the genomic report will not be published to EMR from OHPM.

1.2 Configuration

Perform the following steps to configure OHPM for EPIC EMR:

> **Note:** Steps 1 to 4 in the following list should be performed only if EMR configuration was *not* done during installation.

1. Note down the host name and the TCP/IP or TLS port number where EPIC EMR listens for incoming lab result message.

   This TCP/IP or TLS port typically is the EPIC Interconnect HL7 V2 interface that can handle base64 encoded attachments. Although both TCP/IP and TLS are supported in this integration, Oracle strongly recommends that you use TLS since it is more secure.

2. Get the Certificate Authority (CA) Certificate of the CA that signed the digital certificates used by EPIC TLS.

   CA certificates are generally from standard public CAs like Verisign. If EPIC was configured to use a self-signed certificate, then use the local CA certificate employed to sign the certificate request.

3. Load the CA Certificate into OHPM WebLogic Server's Oracle Platform Security Services (OPSS) keystore. You can do this either:

   - Using the Enterprise Manager

- Using the WebLogic Scripting Tool

4. Grant permission to read the keystore.
5. Use the EMR Integration Configuration REST service available as part of the OHPM application to configure details required to publish a report to the EMR using the TLS keystore created in the previous step.

   The service end point of the EMR Integration Configuration REST service and definition of its payload are as follows:

Table 1–1 Service End Point

HTTP Method	URL	Description
GET/DELETE	http://<host>:<port>/trc/opmemrintegration/resources/opm/api/v1.0/emrconfigservice/emrconfig/{emrId}	Retrieve or Delete EMR integration configuration for a given EMR ID
GET	http://<host>:<port>/trc/opmemrintegration/resources/opm/api/v1.0/emrconfigservice/emrconfig/status/{status}	Retrieve EMR integration configuration for a given status. Status is active *A* or Inactive *I*.
POST/PUT	http://<host>:<port>/trc/opmemrintegration/resources/opm/api/v1.0/emrconfigservice/emrconfig	Create or Update using the EMRIntegrationConfig payload

Table 1–2 Definition of Payload

Field (XML/JSON)	Description	Valid Value Set	Example
emrIntegrationConfig	Root Element	-	-
createdById	Created by user ID (automatically populated)	-	-
createdOnDt	Date when record was created (automatically populated)	-	-
description	Description of the EMR	User defined	EPIC EMR
emrId	A unique ID for the configuration. Used to update.	User defined	Epic_1
emrType	Type of the EMR	EPIC	EPIC
integrationHost	Host name or IP of the remote EMR system for TCP/TLS communication, otherwise NULL	Remote host name/IP	remotehost.com
integrationPort	Port number for TCP/TLS communication, otherwise NULL	Valid remote host port number	8088
integrationUrl	SOAP/REST URL for SOAP/REST end point, otherwise NULL	Valid URL	https://host:7002/epic/fhir/svc
integrationAuthMethod	Authentication method for calling remote service	HTTP-BASIC, WS-SECURITY	HTTP-BASIC
integrationAuthUsername	Username for HTTB-BASIC and WS-SECURITY. Credentials must be available in OPSS/JPS configuration	User defined	testuser
integrationSslKeystore	OPSS/JPS keystore name in stripe *OPMApp*. Mandatory when the integration URL starts with https.	User defined	castore
messageFormat	The format of the EMR message to be generated	HL7V2	HL7V2
messageTemplateLoc	Location of the template. The default location for EPIC is templates/EPIC_HL7V2.template	Valid file location	templates/EPIC_HL7V2.template
receivingApplication	The name of the application receiving the HL7V2 message.	User defined	EPIC
receivingFacility	The name of the facility receiving the HL7V2 message.	User defined	EPIC-LAB

Table 1–2 (Cont.) Definition of Payload

Field (XML/JSON)	Description	Valid Value Set	Example
reportTestName	Test name (code) to represent genomic test result, based on what EMR accepts	User defined	GENE^GENOMIC EXAM
rowWid	Internally generated surrogate primary key	-	-
sendingApplication	The name of the application sending the HL7V2 message.	User defined	ORACLE-MI
sendingFacility	The name of the facility sending the HL7V2 message.	User defined	GENETIC-LAB
status	Status of the configuration record	A (active), I (inactive)	A
transportProtocol	Transport protocol supported by this EMR	TCP, TLS, SOAP1, SOAP2, REST	TLS

Following is a sample XML payload for the REST service to create a TLS connection configuration to EPIC:

```
<?xml version="1.0" encoding="UTF-8"?>
<emrIntegrationConfig>
   <description>EPIC EMR Configuration</description>
   <emrId>Epic_Id1</emrId>
   <emrType>EPIC</emrType>
   <integrationHost>localhost</integrationHost>
   <integrationPort>8081</integrationPort>
   <integrationSslKeystore>emrtruststore</integrationSslKeystore>
   <messageFormat>HL7V2</messageFormat>
   <messageTemplateLoc>templates/EPIC_HL7V2.template</messageTemplateLoc>
   <receivingApplication>EPIC</receivingApplication>
   <receivingFacility>EPC</receivingFacility>
   <reportTestName>GENOMIC^REPORT</reportTestName>
   <sendingApplication>ORACLE-PM</sendingApplication>
   <sendingFacility>ORACLE-PM</sendingFacility>
   <status>A</status>
   <transportProtocol>TLS</transportProtocol>
</emrIntegrationConfig>
```

6. Enable publishing the report to EMR. For details, see Section 2.4, "Enabling or Disabling Features Related to External Systems".

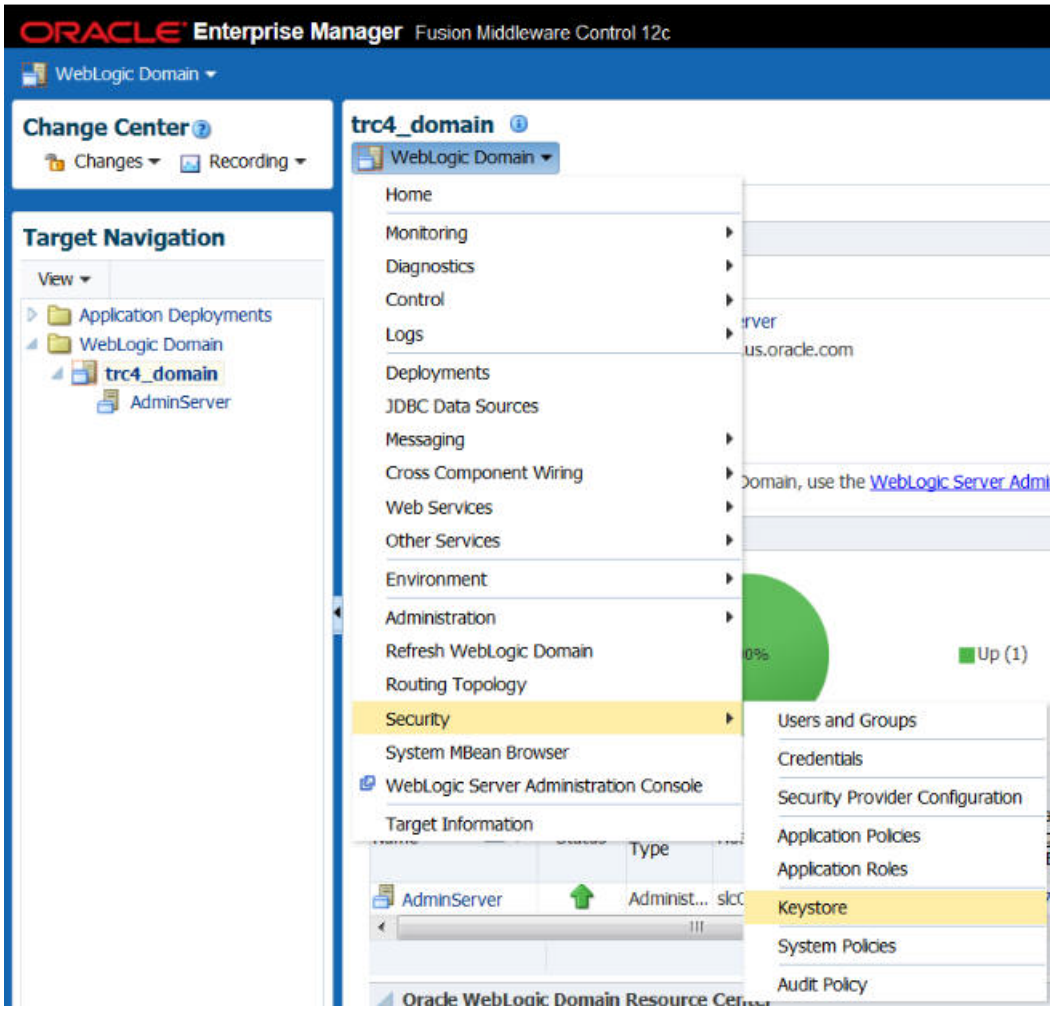
1.3 Configuring the OPSS Keystore

You can configure the OPSS keystore using either of the following methods.

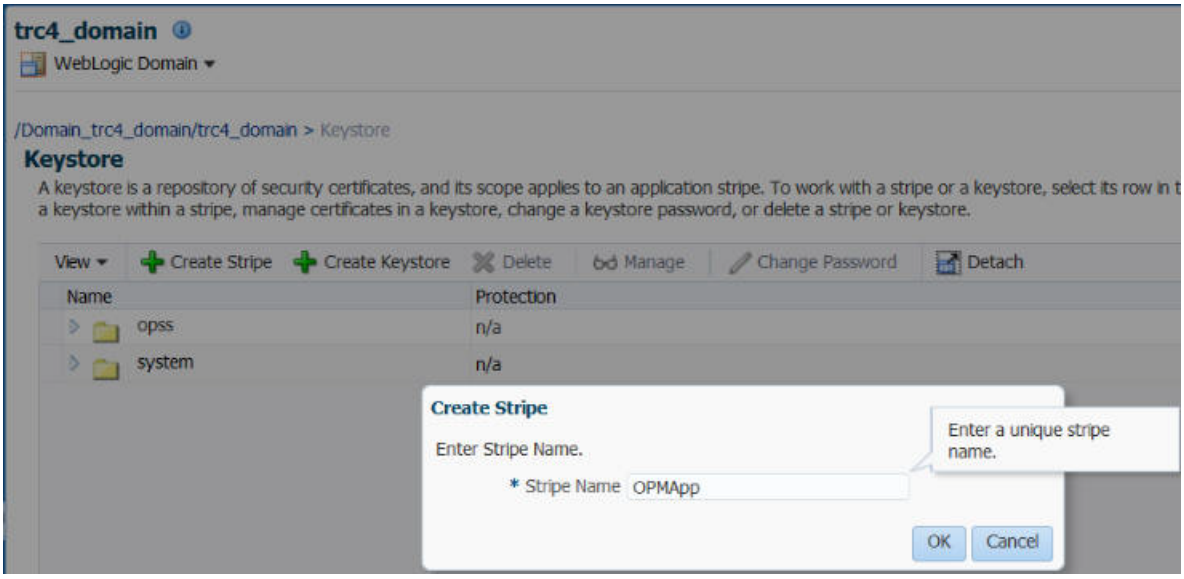
1.3.1 Using the Enterprise Manager

This involves the following steps:

1. Log into WebLogic Enterprise Manager Fusion Middleware Control.
2. Navigate to **WebLogic Domain** > **Security** > **Keystore**.

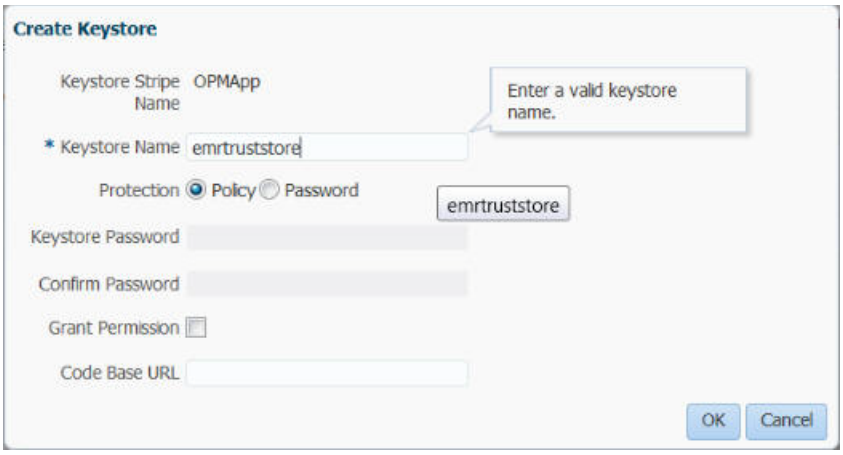


3. Click **Create Stripe** to create a new stripe named OPMApp.



4. Click **OK**.

5. Click **Create Keystore**.
6. Create a new keystore that will be used in the EMR integration configuration. For example, emrtruststore.

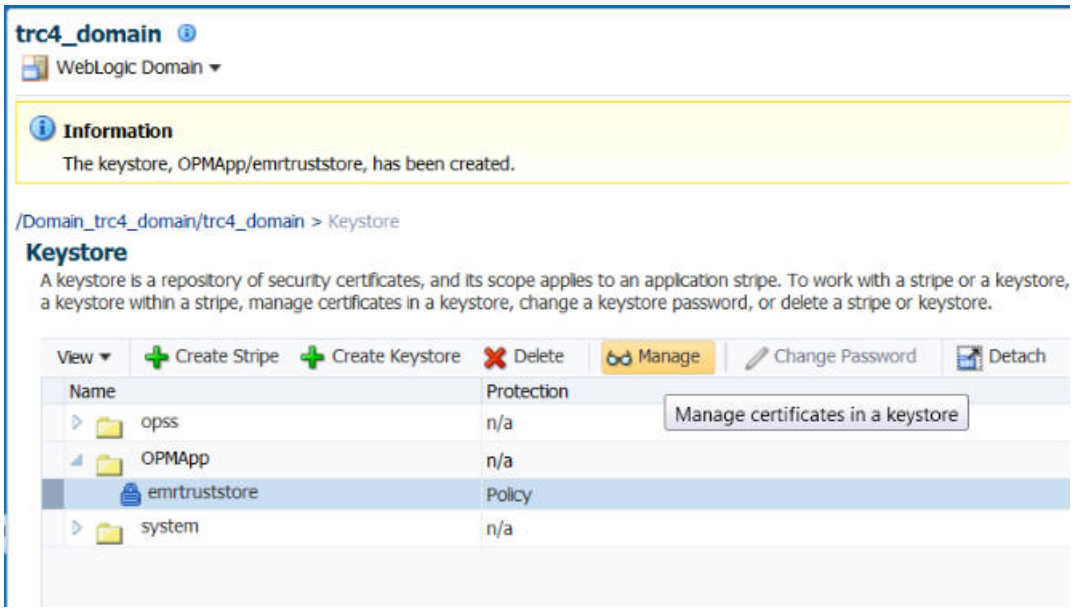


7. Ensure that Policy is selected for **Protection**.
8. Deselect **Grant Permission**.
9. Click **OK**.

   For details on creating a keystore, see the section on Creating a Keystore with Fusion Middleware Control in the *Oracle® Fusion Middleware Securing Applications with Oracle Platform Security Services* available at the following location

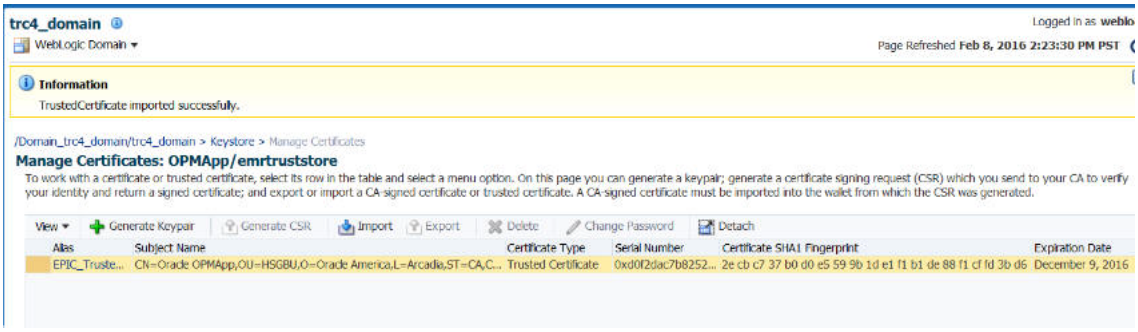
   https://docs.oracle.com/middleware/1213/idm/app-security/kssadm.htm#CACHHHCH

10. Select the keystore created in the previous step and click **Manage**.



11. Click **Import**.
12. Select the **Certificate Type** as Trusted Certificate.
13. Enter an **Alias**.

14. You can either browse and select the CA certificate file or copy the certificate content into the text field provided.
15. Click **OK**. The CA trusted certificate is successfully added to the keystore.



For details on creating a keystore, see the section on Importing a Certificate or Trusted Certificate with Fusion Middleware Control in the *Oracle® Fusion Middleware Securing Applications with Oracle Platform Security Services* available at the following location

https://docs.oracle.com/middleware/1213/idm/app-security/kssadm.htm#CACDEAJH

1.3.2 Using the WebLogic Scripting Tool

Perform the following steps to configure the OPSS keystore using WLST.

1. Load the CA Certificate into Oracle Platform Security Services (OPSS) using the WebLogic Scripting Tool (WLST). Use the following commands:

```
$ cd $MIDDLEWARE_HOME/wlserver/common/bin
$ ./wlst.sh
wls:/offline> connect()
Please enter your username: '<weblogic admin user>'
Please enter your password:'<weblogic admin user password>'
Please enter your server URL [t3://localhost:7001]: '<weblogic admin url>')
wls:/ohpm_domain/serverConfig> svc = getOpssService(name='KeyStoreService')
wls:/ohpm_domain/serverConfig> svc.createKeyStore(appStripe='OPMApp',
name='emrtruststore', password='', permission=true)
wls:/ohpm_domain/serverConfig>
svc.importKeyStoreCertificate(appStripe='OPMApp', name='emrtruststore',
password='', alias='EPIC_Trusted_Cert', keypassword='',
type='TrustedCertificate', filepath='<full path to the CA certificate file>')
```

1.3.3 Granting Permission to Use the Keystore

Perform the following steps to grant permission to use the keystore created in OPSS using WLST.

1. Connect to weblogic admin server using wlst. Refer above steps for example.
2. Execute the following wlst command:

```
grantPermission(appStripe="OPMApp",
codeBaseURL='file:${oracle.deployed.app.dir}/OHF-Opm-App${oracle.deployed.app.ext}',
permClass="oracle.security.jps.service.keystore.KeyStoreAccessPermission",
permTarget="stripeName=OPMApp,keystoreName=emrtruststore,alias=*",
permActions="read")
```

2

External System Configurations

This chapter details configuration APIs for external systems used in OHPM. These are REST based services and are authenticated using BASIC authentication. Admin user (having pm_admin_group role) can use these services for configuration.

It includes the following topics:

- Section 2.1, "Dalliance"
- Section 2.2, "Thomson Reuters"
- Section 2.3, "N-Of-One"
- Section 2.4, "Enabling or Disabling Features Related to External Systems"

Common Request Header

All API invocations with base path as /trc/opmconfigapi/ should have header value **X-Requested-By** set with the value OPM.

2.1 Dalliance

REST API's to manage genome version details required by the Dalliance genome browser. DAS server details are required for configuring Dalliance.

2.1.1 Dalliance Configuration

PATH	<server url>//trc/opmconfigapi/v1.0/config/dalliance
ACCEPTS	application/json
RETURNS	application/json

2.1.1.1 Retrieving a List of Genome Configurations

Method

GET - Genome configurations

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

Response

HTTP Status: 200 (success)

Body: Example

```
{
    "name":"HG19",
    "authority":"GRCh",
    "version":"38",
    "sequenceTrackUrl":"<URL>",
    "genesTrackUrl":"<URL>",
    "dnaVersion": "V68"
},
{
    "name":"HG18",
    "authority":"NCBI",
    "version":"37",
    "sequenceTrackUrl":"<URL>",
    "genesTrackUrl":"<URL>",
    "dnaVersion": "V68"
}
```

2.1.1.2 Adding a Genome Configuration

Method

POST - Add a genome configuration. You will have to provide DAS server URLs that are used in Dalliance to plot variant details.

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

body		body	{
			"name":"<UCSC_NAME>",
			"authority":"<authority_name>",
			"version":"<version_number>",
			"sequenceTrackUrl":"<DAS server sequence track URL>",
			"genesTrackUrl":"<DAS server sequence track URL>"
			"dnaVersion": "<DNA Reference Build Version>"
			}

Response

Code	Reason	Representation
200	success	{ "success": "true" }

2.1.2 Dalliance Configuration by Genome Version

PATH	<server url>/trc/opmconfigapi/v1.0/config/dalliance/{genomeVersion}
ACCEPTS	application/json
RETURNS	application/json

2.1.2.1 Retrieving Configuration for a Genome Version

Method
GET - Configuration for a genome version

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
genomeVersion	Genome version	path	String

Response

Code	Reason	Representation (Example)
200	success	{ "name":"HG19", "authority":"GRCh", "version":"38", "sequenceTrackUrl":"<URL>", "genesTrackUrl":"<URL>" "dnaVersion": "V68" }

2.1.2.2 Updating an Existing Genome Configuration

Method
PUT - Update an existing genome configuration

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
genomeVersion	Genome version	path	string

body		body	<pre>{
			"name":"<UCSC_NAME>",
			"authority":"<authority_name>",
			"version":"<version_number>",
			"sequenceTrackUrl":"<URL>",
			"genesTrackUrl":"<URL>"
			"dnaVersion": "<DNA Reference Build Version>"
			}</pre>

Response

Code	Reason	Representation

200	success	<pre>{
		"success": "true"
		}</pre>

2.1.2.3 Deleting a Genome Version Configuration

Method

DELETE - Configuration for a genome version

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
genomeVersion	Genome version	path	string

Response

Code	Reason	Representation (Example)
200	success	

2.2 Thomson Reuters

REST APIs to manage credentials for invoking Thomson Reuters genomic APIs. Valid subscription for Thomson Reuters APIs is required for consuming them. You must enable the Thomson Reuters related feature after configuring the credential. For details, see Section 2.4, "Enabling or Disabling Features Related to External Systems".

Admin user can configure the organization level and own (if available) credentials to access Thomson Reuters APIs. Molecular pathologists can add their own credentials to access Thomson Reuters by using this API.

2.2.1 Thomson Reuters Credential Configuration

PATH	<server url>/trc/opmconfigapi/v1.0/config/credential/thomsonReuters
ACCEPTS	application/json
RETURNS	application/json

2.2.1.1 Retrieving a List of User Credentials Configured for Thomson Reuters

Method

GET - Users configured for Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

Response

Code	Reason	Representation (Example)
200	success	

```
{
    "id":"1001",
    "credentialType":"USER",
    "username":"testuser",
    "password":"" -- Is not loaded in GET
},
{
    "id":"1002",
    "credentialType":"ORG",
    "username":"testorg",
    "password":"" -- Is not loaded in GET
}
```

2.2.1.2 Adding a User Credential for Invoking Thomson Reuters

Method

POST - Add a user credential for invoking Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
body		body	

```
{
    "credentialType":"USER|ORG",
    "username":"<USER_ID>",
    "password":"<PASSWORD>"
}
```

Response

Code	Reason	Representation (Example)

200	success	<pre>{
		"id":"1231",
		"credentialType":"USER",
		"username":"testuser",
		"password":"" -- Is not loaded
		}</pre>

2.2.1.3 Updating Organization Level User Credentials for Invoking Thomson Reuters

Method

PUT - Update user credential for invoking Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

body		body	<pre>{
			"id":"1002",
			"credentialType":"ORG",
			"username":"testOrg",
			"password":"<PASSWORD>"
			}</pre>

Response

Code	Reason	Representation (Example)

200	success	<pre>{
		"success": "true"
		}</pre>

2.2.1.4 Deleting Organization Level User Credential Used for Invoking Thomson Reuters

Method

DELETE - Delete a user credential used for invoking Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

Response

Code	Reason	Representation (Example)
200	success	{ "success": "true" }

2.2.2 User-Specific Thomson Reuters Credential Configuration

PATH	<server url>/trc/opmconfigapi/v1.0/config/credential/thomsonReuters/{credentialID}
ACCEPTS	application/json
RETURNS	application/json

2.2.2.1 Getting Credential Details for a User Configured for Thomson Reuters

Method
GET - User details for a user configured for Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
credentialID		path	integer

Response

Code	Reason	Representation (Example)
200	success	{ "id":"1002", "credentialType":"USER", "username":"testorg", "password":"" -- Is not loaded in GET }

2.2.2.2 Updating User Credentials for Invoking Thomson Reuters

Method
PUT - Update user credential for invoking Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
credentialID		path	integer

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

body		body	<pre>{
			"id":"1002",
			"credentialType":"USER",
			"username":"testUser",
			"password":"<PASSWORD>"
			}</pre>

Response

Code	Reason	Representation

200	success	<pre>{
		"success": "true"
		}</pre>

2.2.2.3 Deleting User Credentials Used for Invoking Thomson Reuters

Method

DELETE - Delete a user credential used for invoking Thomson Reuters

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
credentialID		path	integer

Response

Code	Reason	Representation

200	success	<pre>{
		"success": "true"
		}</pre>

2.3 N-Of-One

The following REST APIs have been provided to manage configurations for invoking N-of-One genomic interpretation APIs. Enable N-of-One related features after configuring N-of-One details. For details, see Section 2.4, "Enabling or Disabling Features Related to External Systems".

2.3.1 N-of-One Credential Configuration

PATH	<server url>/trc/opmconfigapi/v1.0/config/credential/nof1
ACCEPTS	application/json
RETURNS	application/json

2.3.1.1 Getting Credentials Configured for N-of-One

Method

GET - User credential for N-of-One

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

Response

Code	Reason	Representation
200	success	{ "id":"1002", "credentialType":"ORG", "authorizationToken": null "productKey":"<productKey>", "customerId":"<customerId>" }

authorizationToken is not loaded in GET.

2.3.1.2 Adding a Credential for Invoking N-of-One

Method

POST - Add credential details for invoking N-of-One

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
body		body	{ "authorizationToken": "<AUTH TOKEN>", "productKey":"<productKey>", "customerId":"<customerId>" }

Response

Code	Reason	Representation
200	success	{ "id":"1231", "credentialType":"ORG", "authorizationToken": "<AUTH TOKEN>" "productKey":"<productKey>", "customerId":"<customerId>" }

2.3.1.3 Updating Credentials for Invoking N-of-One

Method

PUT - Update credential details for N-of-One

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

body		body	<pre>{
			"authorizationToken": "<AUTH TOKEN>",
			"productKey":"<productKey>",
			"customerId":"<customerId>"
			}</pre>

Response

Code	Reason	Representation

200	success	<pre>{
		"authorizationToken": "<AUTH TOKEN>"
		"productKey":"<productKey>",
		"customerId":"<customerId>"
		}</pre>

2.3.1.4 Deleting Credential Used for Invoking N-of-One

Method

DELETE - Delete credential used for invoking N-of-One

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

Response

Code	Reason	Representation

200	success	<pre>{
		"success": "true"
		}</pre>

2.4 Enabling or Disabling Features Related to External Systems

PATH	<server url>/trc/opmconfigapi/v1.0/config/externalFeaturesState
ACCEPTS	application/json
RETURNS	application/json

2.4.1 Returning State of Current Features

Method

GET - Returns current features state

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

Response

Code	Reason	Representation

200	success	<pre>{
		"dalliance":false,
		"thomsonReuters":false,
		"clinvar":true,
		"nof1":false,
		"emr":false
		}</pre>

2.4.2 Enabling or Disabling Features in Oracle Healthcare Precision Medicine

Method

PUT - Enable or disable features in OHPM

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

body		body	<pre>{
			"dalliance":false,
			"thomsonReuters":false,
			"clinvar":true,
			"nof1":false,
			"emr":true
			}</pre>

Response

Code	Reason	Representation

200	success	<pre>{
		"success": "true"
		}</pre>

3

Published Report Template Configuration

This section describes how an admin user can configure the text and logo that appear in header and footer of the published PDF report. It includes the following sections:

- Section 3.1, "Configuring the Logo in the Report Header and Footer"
- Section 3.2, "Configuring the Text in the Report Header and Footer"

3.1 Configuring the Logo in the Report Header and Footer

The report logo should be stored on domain_home on the server and the paths (including the logo name) should be configured using admin APIs.

Images for the logo should be of 0.75″ × 0.75" dimension (height*width) so that the logo is not stretched or squeezed.

Use the following API to configure the report logo:

Method	PUT
API Path	<server url>/trc/opmconfigapi/v1.0/config/{configurationName}

JSON Body	:{
	"Key":"value "
	}

Example	host:port/trc/opmconfigapi/v1.0/config/PUBLISH_REPORT_HEADER_LOGO1
	{
	"PUBLISH_REPORT_HEADER_LOGO1":"./DynImages/Footer.jpg "
	}

Configuration Key Names for header and footer logo images are:

- Header Logo
  - PUBLISH_REPORT_HEADER_LOGO1
  - PUBLISH_REPORT_HEADER_LOGO2
- Footer Logo
  - PUBLISH_REPORT_FOOTER_LOGO

3.2 Configuring the Text in the Report Header and Footer

Admin user can configure the text in the report header and footer using the same API that is used to configure the logo.

Configuration Names for header and footer text are:

- Report Header: Text at top of report header, 3 lines
  - PUBLISH_REPORT_HEADER_LINE1
  - PUBLISH_REPORT_HEADER_LINE2
  - PUBLISH_REPORT_HEADER_LINE3
- Report Footer: Text at bottom of report, 2 lines
  - PUBLISH_REPORT_FOOTER_LINE1
  - PUBLISH_REPORT_FOOTER_LINE2

4

Annotation Pane Configuration

This section describes how to configure the annotation pane using REST APIs. It contains the following sections:

- Section 4.1, "GET Annotation Pane Configuration"
- Section 4.2, "UPDATE Annotation Pane Configuration"

4.1 GET Annotation Pane Configuration

Gets all the annotation pane UI details as JSON.

PATH	<server url>/trc/opmconfigapi/v1.0/config/annotationPane
ACCEPTS	application/json
RETURNS	application/json
METHOD	GET

Response

Code	Reason	Representation (Example)
200	success	

Example

```
{
    "eltWid": 1,
    "type": "PANE",
    "level": 0,
    "displayOrder": 0,
    "label": "Annotation",
    "items": [{
        "eltWid": 2,
        "type": "INPUT",
        "level": 1,
        "displayOrder": 0,
        "label": "Significance",
        "data_type": "ENUM",
        "attr_wid": 57,
        "data_key": "significance",
        "options": {
            "multiple": false,
            "read_only": false,
            "display": true,
            "allow_custom": false
```

```
            },
            "values": [{
                "wid": 2,
                "label": "Likely Benign",
                "value": 2,
                "displayOrder": 3
            }, {
                "wid": 1,
                "label": "Unknown Significance",
                "value": 1,
                "displayOrder": 4
            }]
        }, {
            "eltWid": 3,
            "type": "INPUT",
            "level": 1,
            "displayOrder": 1,
            "label": "Associated Diagnosis",
            "data_type": "LOOKUP",
            "attr_wid": 71,
            "data_key": "var_associated_diseases",
            "data_url": "diagnoses",
            "options": {
                "multiple": true,
                "read_only": false,
                "display": true,
                "allow_custom": true
            }
        }]
}
```

4.2 UPDATE Annotation Pane Configuration

This updates the label, display (True or False) and Display Order on the Annotation pane. The user has to be admin role of pm_admin_group.

> **Note:** While updating, make sure the display order is correct. This value cannot be duplicated for all siblings.

PATH	<server url>/trc/opmconfigapi/v1.0/config/annotationPane/changed
ACCEPTS	application/json
RETURNS	application/json
METHOD	PUT

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION
body		body	`[{ "etlWid":Number, "label":String, "display" : String, "displayOrder" : String }]`

Example

```
[{
    "eltWid": 2,
    "label": "Significance",
    "display": true,
    "displayOrder": 0
}, {
    "eltWid": 3,
    "label": "Associated Diagnosis",
    "display": true,
    "displayOrder": 1
}]
```

Response

Code	Reason	Representation (Example)
200	success	

5

Loader API

This section describes the APIs for OHPM loaders. It contains the following topics:

- Section 5.1, "Fetch Job Status and Log"
- Section 5.2, "Data Ingestion with Loaders"

5.1 Fetch Job Status and Log

You can view the latest job status (running or completed), progress and the completion status (success or failure). If the job failed, you can see more information on the error by referring the job logs.

For Authorization, provide a user that is in the allowed role (pm_admin_group)

5.1.1 Job Status

This provides the current status for the Loader Job.

PATH	<server url>/trc/opmconfigapi/v1.0/config/loader/jobstatus/{jobId}
ACCEPTS	application/json
RETURNS	application/json
METHOD	GET

Response

Code	Reason	Representation (Example)

200	success	<pre>{
		  "status": "COMPLETE",
		  "links": [
		  {
		  "rel": "logs",
		  "href":
		"/trc/opmconfigapi/v1.0/config/loader/jobstatus/{jobId}/logs"
		  }
		  ]
		}</pre>

500	error	error message object

5.1.2 Job Log

This provides detailed log information for the job.

PATH	<server url>/trc/opmconfigapi/v1.0/config/loader/jobstatus/{jobId}/logs
ACCEPTS	application/json
RETURNS	application/json
METHOD	GET

Response

Code	Reason		Representation (Example)

200	success		[
			{
			"insertDate": string,
			"logDetail": string,
			"errorCode": string,
			"errorInfo": string
			}
			]

500	error	error message object	

5.2 Data Ingestion with Loaders

5.2.1 Preferred Transcript Loader

Loads the preferred transcript data files into the OHPM environment.

Allowed Roles for API: pm_admin_group

Loader Procedure: load_pref_transcr_stg

PATH	<server url>/trc/opmconfigapi/v1.0/config/loader/preferred-transcript
ACCEPTS	application/json
RETURNS	application/json
METHOD	POST

Request

PARAMETER	DESCRIPTION	PARAMETER TYPE	DATA TYPE/ REPRESENTATION

body		body	{
			"file": "{bucketName}/{objectName}",
			"readSize":Number,
			"fullRefresh" : boolean
			}

- *readSize* is optional in the request
- *fullRefresh* is optional and if not specified, the default value is false.

> **Note:** For the *file* input parameter, specify the *bucketName* and *objectName* that was used in the File Upload Service when uploading the file. If you have manually uploaded the file, then directly specify the file name.

Example

```
{
    "file":"mypreferred/preferred_transcript_2020"
    "readSize" : 8
}
```

Response

Code	Reason	Representation (Example)

200	success	`HTTP/1.1 202 Accepted`
		`Location: /trc/opmconfigapi/v1.0/config/loader/jobstatus/{jobId}`
		Note: The `Location` points to the URI for the JobId. Use this to fetch the job status.

500	error	error message object

Index

C

configuration
dalliance, 2-1
emr, 1-1
n-of-one, 2-8
thomson reuters, 2-4
configure annotation pane
GET, 4-1
UPDATE, 4-2
configure published report
logo, 3-1
text, 3-1

D

data ingestion with loaders, 5-2

E

external system features
disabling, 2-10
enabling, 2-10

J

job log, 5-1
job status, 5-1

L

loader design, 5-1

P

patches, vii
preferred transcript loader, 5-2