

ORACLE

Oracle Forms

Integration with Identity and Access Management (IAM)

February, 2024, Version [1.0]

Copyright © 2024, Oracle and/or its affiliates

Public

Purpose statement

This document provides the instructions necessary to enable integration Oracle Forms 12.2.1.19 or newer with Identity and Access Management Cloud Service (IAM). Refer to the [IAM documentation](#) for additional details.

Table of contents

Overview	4
Requirements	5
IAM Server Configuration	6
Creating an IAM Application	6
Creating the App Gateway	9
App Gateway Client	11
Prerequisites	11
Setting up App Gateway Client on Middle Tier	11
Running the Oracle App Gateway Docker Container	13
Installing and Starting Docker	13
Importing the App Gateway Docker Image	14
Running the Docker Image	14
Stopping the Docker Container	15
Enabling IAM Integration in Forms	15
Optional Steps	16
Usage Notes	17
Troubleshooting	18
References	20

Overview

Oracle Identity and Access Management (IAM) provides identity management, single sign-on (SSO), and identity governance for applications on-premise, in the cloud, or for mobile devices. Employees and business partners can access applications at any time, from anywhere, and on any device in a secure manner. In the case of Oracle Forms, the ability to expose single sign-on functionality was previously limited to using Oracle Access Manager. With this introduction to integration with IAM, Oracle Forms can now use either OAM or IAM (Cloud) for Single Sign-on requirements.

The following instructions are based on information provided in the Identity and Access Management documentation. These instructions will illustrate how to incorporate the use of Single Sign-on with Oracle Forms using IAM.

For more details about any of the following instructions, refer to the IAM documentation.

<https://docs.oracle.com/en-us/iaas/Content/Identity/home.htm>

These instructions assume that the IAM App Gateway will be configured on a Linux operating system.

There are several major steps required to configure Oracle Forms with IAM. Those steps include the following:

1. Create IAM application
2. Create App Gateway
3. Setting up the App Gateway Client (via docker)
4. Enabling SSO in an Oracle Forms application.

Images in this document may differ from your environment, based on the current version at the time these instructions are reviewed. Regardless of the images seen, the instructions and concepts should remain the same or similar.

Requirements

This document will assume the following. If you do not meet these requirements, be sure to address those gaps before continuing.

The following instructions assume the use of “Identity and Access Management” (IAM) and not its predecessor, “Identity Cloud Service” (IDCS) although the terms IAM and IDCS may be used interchangeably throughout.

1. You must be running Oracle Forms 12.2.1.19 or newer, installed on-premise or in Cloud.
2. The Oracle Forms applications must be launched using Java Web Start or Forms Standalone Launcher. Launching applications using the embedded applet configuration in Microsoft Internet Explorer or Edge (with IE-mode) is not supported.
3. The IAM Service environment must be accessible from the server where the [IAM App Gateway \(Client\)](#) is running.
4. The administrator performing the task of implementing this integration configuration must have administration privileges in the IAM Service environment.
5. The administrator performing the task of implementing this integration configuration must have privileges to download and configure the [IAM App Gateway](#) on the middle tier or the desired alternative server where App Gateway will be configured.
6. The administrator performing the task of implementing this integration configuration must have privileges to access and make administrative changes to the middle tier software (i.e., Oracle Forms).
7. Because the required App Gateway client is only available as a Docker Image or full Virtual Machine (VM), familiarity with using either Docker or running a Virtual Machine will be helpful. This document will only cover the use of the Docker Image. A similar configuration approach can be used for using the full VM. Refer to the IAM documentation for assistance with configuring and using the full VM.
8. A current SSL/TLS certificate (from a trusted CA) associated with the host that will be running the App Gateway client and/or the Forms middle tier. *(Recommended but not required)*

IAM Server Configuration

Creating an IAM Application

The following steps will be used to create the IAM Application, as well as create the needed resource settings and authentication policies.

1. Log into your Oracle Cloud tenancy from where you plan to setup this IAM environment.
2. Click on Identity and Security from the left side menu (hamburger button) of your OCI environment.
3. Click on Domains under Identity.
4. If you have not already created a Domain for IAM, create one now by clicking on the Create Domain button. If you already have one and plan to use it for the Oracle Forms integration, continue to the next step. Any Domain Type can be used, however carefully consider the limitations associated with each when selecting.



Figure 1 - IAM Domain listings

5. Click on the desired Domain in order to display its details screen.
6. Click on Integrated Applications, on the left.
7. Click on Add Application found above the displayed table.
8. In the presented dialog, select Enterprise Application and click Launch Workflow.

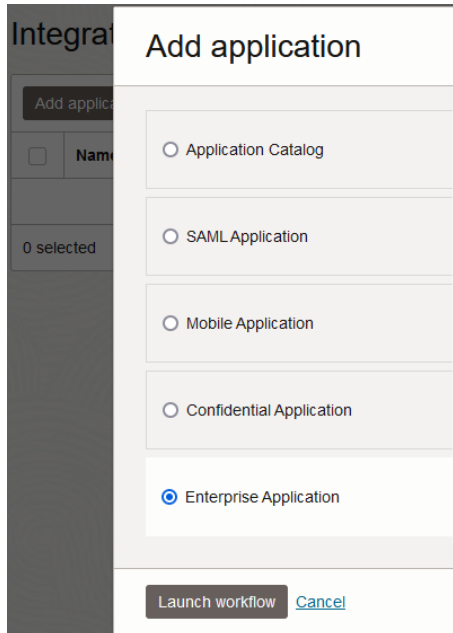


Figure 2 - Add application dialog

9. In the presented dialog, enter the following:

Name: Provide a desired name to reference this IAM Application.

Description: Optionally, provide a desired description for this IAM application.

Application Icon: Optionally, provide an icon that will appear in the Applications table.

In the section titled *URLs*:

Application URL: Enter the fully qualified URL that points to the IAM App Gateway environment, but include the Forms context root and app name (e.g. `/forms/frmservlet`). Do not include application arguments. An IP address can be used in place of the *host.domain*.

Syntax example:

`https://<APP_GATEWAY_HOST.DOMAIN>:<IAM_SSL_PORT>/forms/frmservlet`

Refer to the descriptions below each field for information explaining their purpose.

Display in My Apps: checked

10. Click Next on the bottom to continue.

11. Skip the OAuth configuration. Click Next to continue.

12. Add the following Resources by clicking the Add Resource button for each numbered row in the table below. Adding a description is optional, but recommended.

	Resource Name	Resource URL	URL Query String	Use Regex Expressions	Description
1	Protected resource	<code>/forms/frmservlet.*</code>	<code>oamMode=true</code>	Yes	Forms application protected resource
2	Anonymous access resource	<code>/forms/frmservlet.*</code>		Yes	Forms application anonymous access
3	Anonymous access resource 2	<code>/forms/frmservlet</code>	<code>ifcmd=startsession</code>		Forms application anonymous resource 2
4	Protected RAD resource	<code>/forms/radservlet.*</code>		Yes	Forms application protected RAD resource
5	Public resource	<code>/*</code>		Yes	Forms application public resource

13. Check the Audience Validation *and* Require Secure Cookies boxes, if not already checked.

14. Check the Add Managed Resources box, if not already checked.

15. Add the following Managed Resources by clicking the Add Managed Resource button for each in the table below. Be sure the Priority order matches the table shown.

Priority	Resource	Authentication Method	Enable Audience Validation
1	Protected resource	Form or Access Token	Yes
2	Anonymous access resource	Anonymous	
3	Anonymous access resource 2	Anonymous	
4	Protected RAD resource	Form or Access Token	Yes
5	Public resource	Public	

The Managed Resources table should resemble the following. Be sure the Priority of each is as listed in the above table and as shown in Figure 3 below. Make corrections to the priorities as needed to match the list shown.

Managed resources

<input type="checkbox"/>	Priority	Name	Resource URL	
<input type="checkbox"/>	1	Protected resource .*	/forms/frmservlet.*	⋮
<input type="checkbox"/>	2	Anonymous access resource .*	/forms/frmservlet.*	⋮
<input type="checkbox"/>	3	Anonymous access resource 2	/forms/frmservlet	⋮
<input type="checkbox"/>	4	Protected RAD resource	/forms/radservlet.*	⋮
<input type="checkbox"/>	5	Public resource	/*	⋮

0 selected Showing 5 items

Figure 3 - Managed resources table list

16. Click the Finish button. This will return you to this Integrated Application’s Details screen.
17. Click the Active button found above the Application Information tab.

Creating the App Gateway

The following steps will be used to create the App Gateway configuration settings.

More information about setting up an App Gateway can be found in the [References](#) section of this document.

1. Navigate to this Domain’s Overview screen by using the breadcrumb at the top left of the page.
2. Using the vertical menu on the left, click Security then App Gateways.
3. Click on Create App Gateway.
4. Enter an easily identifiable Name and Description.
5. Click the Add Host link found on the left side then click the Add Host button to enter the following two entries from the table below. Note that the first row is for requests received as non-SSL and the second is for handling SSL requests. Non-SSL requests will be redirected to SSL to ensure the highest degree of security.

Replace the Host Identifier, Host, and Port with those that match your system. Also, carefully review the Additional Properties values and ensure they are appropriate for your environment. References to host, IP address, or port should reflect those which are user accessible. Refer to the “Setting Up App Gateway” section of the IAM documentation for more details.

Host identifier	Host	App Gateway Port	SSL enabled	Additional Properties
appgateway-nonssl	<App Gateway client hostname>	7777 (non-SSL port)	NO	return 301 https://\$host:4443\$request_uri;
appgateway-ssl	<App Gateway client hostname>	4443 (SSL port)	YES	ssl_certificate /home/oracle/keys/ssl.cert; ssl_certificate_key /home/oracle/keys/ssl.key; ssl_protocols TLSv1 TLSv1.1 TLSv1.2; ssl_ciphers HIGH:!aNULL:!MD5;

The certificate and key paths presented in the Additional Properties column must be as shown regardless of whether you are using a certificate provided from a trusted CA or a self-generated certificate.

6. Click Add Host to accept the changes.
7. Click on Next.
8. Click on Add App.
9. In the Application field, select the app created earlier in the instructions above.
10. In the Select a Host field, select the SSL entry created earlier in the instructions above.
11. In the Resource Prefix field, enter a forward slash “/”.

12. In the Origin Server field, enter the fully qualified non-SSL URL (use the SSL URL if not using non-SSL) that points to the middle tier (Forms) host.domain:port
13. In the Additional Properties field, enter the string in the example below. Replace “9001” in the example with the port used by your Forms managed server.

If the App Gateway client is running on a different machine than the Forms middle tier, replace “\$host” below with the user accessible host.domain (or IP address) of the Forms middle tier.

```
proxy_set_header Host $host:9001;
```

Application
OracleFormsExampleAMApplication

Select the enterprise application.

Select a host
OracleFormsPMAAppGateway_ssl

Select the host for this app from the list of hosts added to this app gateway.

Resource prefix
/

Origin server
http://YourMiddleTierServer:9001

Additional properties *Optional*
proxy_set_header Host \$host:9001;

Enter additional NGINX directives to the location block.

Figure 4 - App Gateway example app where App Gateway and mid-tier are on the same machine

14. Click on Add App at the bottom.
15. Click Close.
16. Make note of the Client ID and Client Secret now seen in the App Gateway Information panel. Do not share this information with others. This information will be needed in the following steps.
17. Click on Activate App Gateway.

App Gateway Client

The following steps will be used to create the App Gateway client and start the server. More information about the App Gateway client can be found in the [References](#) section of this document.

Prerequisites

1. Administrative access to the machine where the App Gateway will be running is required.
2. Because the App Gateway client will be using ports 7777 and 4443 in this example, stop all processes currently running on those ports. For example, Oracle HTTP Server typically uses these ports by default. Be sure to stop that server or any others that might use those ports before continuing.
3. Ensure you have the Client ID and Client Secret previously obtained in an earlier step above.
4. Ensure that Docker is properly installed and running on this machine. If not, do so now. Installation will require “root” access.

Setting up App Gateway Client on Middle Tier

1. Navigate to the Identity Domain Overview screen for the domain created in an earlier step above.
2. Click on Settings from the left side menu.
3. Click on Downloads.
4. Download the latest version of these titles onto the machine where the App Gateway client will be configured (e.g. the middle tier machine).
 - **App Gateway Docker Image for Identity Cloud Service**
 - **App Gateway Wallet Tool**

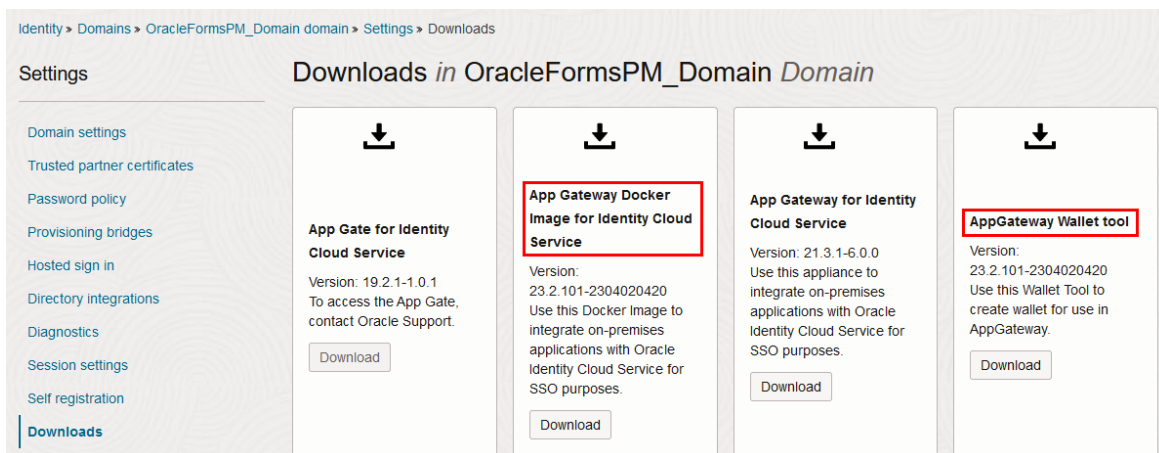


Figure 5 - List of downloads

5. Create directories for the Docker image and Wallet Tool. Also create a directory to store the key and certificate files that will be created below. For example:

```
mkdir /u01/oracle/appgateway/docker
mkdir /u01/oracle/appgateway/wallettool
mkdir /u01/oracle/appgateway/keys
```

6. Extract the contents of the Docker Image downloaded earlier into the 'docker' directory and the contents of the Wallet Tool into the 'wallettool' directory. The docker extraction will include a .gz file. Do not extract it. Leave it in the gz format.
7. Change the current directory to enter the 'keys' directory created above.

```
cd /u01/oracle/appgateway/keys
```

8. Create a self-generated certificate with the following command. Make changes in the example to accommodate your needs.

Note that using a self-generated certificate is not recommended for production use. Further, such a configuration may not work correctly when attempting to run an Oracle Forms application using Forms 12c Standalone Launcher. Using a certificate provided by a known and trusted certificate authority is always recommended.

```
openssl req -new -newkey rsa:2048 -days 730 -nodes -x509 -subj
/C=US/ST=CA/L=RedwoodShores/O=OracleUSAInc/OU=Forms/CN=yourserver.com/emailAddress=youradmini
strator@example.com -keyout ssl.key -out ssl.cert
```

9. Change directory to the location of the Wallet Tool:

```
cd /u01/oracle/appgateway/wallettool
```

10. Execute each of the following one line at a time in the shell:

```
export CLIENT_ID=<ENTER YOUR CLIENT ID FROM THE EARLIER STEP ABOVE>
export CLIENT_SECRET=<ENTER YOUR CLIENT SECRET FROM THE EARLIER STEP ABOVE>
echo $CLIENT_SECRET | env LD_LIBRARY_PATH=./lib ./cgwallettool --create -i $CLIENT_ID
```

11. Move the created wallet to the 'keys' directory.

```
mv cwallet.sso ../keys/cwallet.sso
```

12. Change directories to the 'appgateway' directory. For example:

```
cd /u01/oracle/appgateway
```

13. In the 'appgateway' directory, create a text file and name it appgateway-env (do not include an extension). Add the following contents to the file and save it. Replace <> entries with those that are appropriate for your system.

```
CG_APP_TENANT=<tenant name>
IDCS_INSTANCE_URL=<idcs instance url>
NGINX_DNS_RESOLVER=<resolver ip>
```

CG_APP_TENANT

The tenant name identifier of the Identity Domains instance. This is not your Cloud account/tenancy name. The IAM tenant name is the first portion of the IDCS Instance URL (up to the first dot, but not including the protocol) you will use below. On the Domain Overview page, the "Domain URL" can be found in the Domain Information panel (See Figure 6 below). Copy the first portion of the URL. For example: idcs-1234567890abcdefghijkl

IDCS_INSTANCE_URL

The URL required to access the IAM instance. Enter the entire URL. This can be found on the Identity Domain Overview screen in the Domain Information tab.

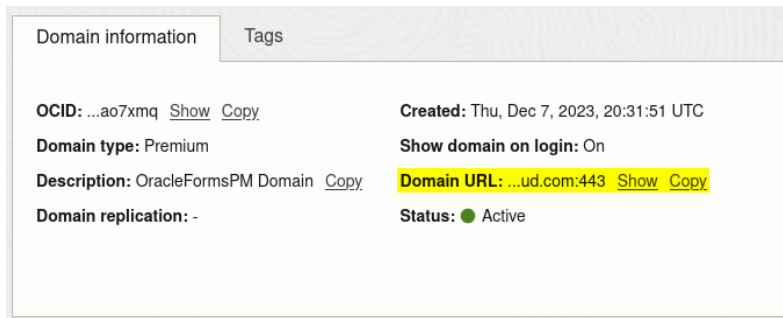


Figure 6 - Identity Domain Overview

NGINX_DNS_RESOLVER

Enter the nameserver found in the file `/etc/resolv.conf`. The default value is 127.0.0.1

Running the Oracle App Gateway Docker Container

The following steps will be used to install and run [Docker](#) and the App Gateway Docker Image that was previously downloaded.

More information about running Docker can be found in the [References](#) section of this document.

Installing and Starting Docker

To install Docker, do the following:

1. If Docker is not already installed on the machine, as the “root” user install Docker with this command:

```
yum install docker-engine
```

2. As the “root” user add the current user to the Docker group. Skip the first command if a “docker” group already exists.

```
groupadd docker
usermod -aG docker oracle
```

Replace “oracle” above with the user that will own the AppGateway Docker environment.

3. As the “root” user, start Docker with the following command then return to your user:

```
systemctl start docker
```

4. Verify that the file `/var/run/docker.sock` has 766 permissions. If not, as the root user change the permissions on the file using the `chmod` command. If this permission is not set properly, the user (e.g., ‘oracle’) will not be able to connect to the Docker image or start it.
5. Exit from the ‘root’ user and verify that Docker is running and can be accessed by the current user (e.g., oracle). The following command should return the contents of the local repository, which will be empty if this is a new installation. Otherwise, it will list the images previously created. No errors should be presented. It may be necessary to reboot the machine if Docker does not start without error and you just installed it. If any permissions errors are presented, refer to the previous step.

```
docker images
```

Importing the App Gateway Docker Image

1. Open a shell and change directory (i.e., “cd”) to the directory where you extracted the App Gateway Docker file (.tar.gz) in step 6 of “[Setting up App Gateway Client on Middle Tier](#)” above (e.g., /u01/oracle/appgateway/docker).
2. Execute the following in order to load the image:

```
docker load --input appgateway-<VERSION NUMER>.tar.gz
```

Running the Docker Image

To run the Docker Image for the *first time*, do the following:

1. List the available images by executing this command. Some of this information will be needed in order to start the image:

```
docker images
```

This will output something similar to the following:

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
idcs/idcs-appgateway	23.2.101-2304020420	ba1249c25dc3	9 months ago	498MB

2. To run the docker image execute the following command. The exact values may need to be adjusted to match your system and desired settings. Refer to the IAM Setup documentation for more information. Links can be found in the [References](#) section of this guide.

```
docker run -it -p 4443:4443 -p 7777:7777 --name appgateway --env-file
/u01/oracle/appgateway/appgateway-env --env HOST_MACHINE=`hostname -f` --volume
/u01/oracle/appgateway/keys/cwallet.sso:/usr/local/nginx/conf/cwallet.sso --volume
/u01/oracle/appgateway/keys:/home/oracle/keys --net=host idcs/idcs-appgateway:23.2.101-
2304020420
```

In the above example, replace the “idcs-appgateway” version with the version you downloaded. The version number is part of the downloaded file name.

Given the above example settings, the App Gateway client listener in the container can be accessed using the hostname:4443 or hostname:7777. For example:

```
https://<hostname>:4443
```

To verify IAM and the App Gateway are responding, run the following from a browser:

```
https://<app gateway host>:<port>/cloudgate/v1/about
```

This will return a JSON page indicating a “RUNNING” status. If you see any other result, likely the App Gateway is not configured correctly and/or is not accessible from the client browser.

If the above is not accessible, verify that the value of “HOST_MACHINE” provided above is an accessible hostname by users. If you do not have a registered domain name you can alternatively use the machine’s public facing IP address.

The above command can only be used the first time the contain image is started. Refer to Step 3 in the “Stopping the Docker Container” for information on restarting after having stopped previously.

Stopping the Docker Container

To stop the running Docker container, do the following:

1. Determine the Container ID by running this command:

```
docker ps
```

The output will resemble the following, although only two columns are shown below:

CONTAINER ID	IMAGE
ebe97115c307	idcs/idcs-appgateway:22.2.61-2203221920

2. Using the Container ID from above, execute the “stop” command.

```
docker stop <container ID>
```

You can alternatively use the container name.

```
docker stop <container name>
```

3. After the container has been stopped, it can be restarted using the same settings previously used, with the following Docker command:

```
docker start <contain name>
```

Enabling IAM Integration in Forms

Now that IAM App Gateway has been configured, it will be necessary to let Forms know it is expected to use it.

1. Using Fusion Middleware Control, access the Forms Web Configuration settings page. Click on the menu Navigation button (aka hamburger) found near the upper left side. Expand the “Forms” node. Then click on the “forms” instance to be modified (e.g. forms1).
2. Click on “Web Configuration” to access its administration screen.
3. On the upper right side, click on the padlock icon then select “Lock & Edit”.
4. In the upper table, select the desired Section Name to be used with IAM. If enabling for all, select “default”.
5. Scroll down to the lower table and expand the pop-list labeled “Show” and select “sso” from the list.
6. Set the value of “ssoMode” to “TRUE”.
7. If you plan to use Java Web Start to launch the applications, click the Add button found at the top of the parameters table. Add the parameter “webstart_codebase”. The value will be the URL pointing to the Forms codebase, but use the IAM host and port.
8. Click on “Apply” (just above the current table).
9. On the upper right side, click on the padlock icon then select “Activate Changes”.
10. To run your Forms app, use this format:

```
https://<IAM AppGateway host>:<port>/forms/frmservlet?config=<Forms config name>
```

Optional Steps

Although these steps are optional, they are recommended. Since the Java Web Start jnlp file cannot be reused, there is no reason to retain it after it has been used. The following step will enable a JWS setting that will automatically remove (delete) the downloaded jnlp file after it has been launched. This will help to improve the user's experience by not creating duplicate files, as well as improve security.

1. In Fusion Middleware Control, navigate to the “Forms” instance (e.g. forms1) associated with this IAM configuration.
2. From the “Forms” drop-down list, select Advanced Configuration.
3. Using the “Activate Edit Session” switch (padlock upper right side), select “Lock & Edit”.
4. In the “Select Category” field, select “Client Templates”.
5. From the “Select File” field, select “base.jnlp” or “webutil.jnlp” (if using a WebUtil enabled app) or your own custom jnlp template if one was created and being used.
6. Add the following to the <resources> section of the template exactly as it appears below:

```
<property name="jnlp.delete.jnlp.file" value="true"/>
```

Select Category: Client Templates
Miscellaneous

Select File: base.htm
base.jnlp
basejpl.htm
basejpl_jnlp.htm

Warning: File contents intended for languages not supported by this browser may not appear correctly.

base.jnlp Apply Revert

```
<?xml version="1.0" encoding="UTF-8"?>
<jnlp spec="1.0"
  xmlns:jfx="http://javafx.com"
  %jnlp_param%="%"jnlp_param_value%">
<information>
  <title>Oracle Forms Services</title>
  <vendor>Oracle Corporation</vendor>
  <homepage href="http://www.oracle.com"/>
  <description>Oracle Forms Services applet launcher.</description>
  <description kind="short">Oracle Forms Applet</description>
</information>
<security>
  <all-permissions/>
</security>
<update check="always" policy="prompt-run"/>
<resources>
  <property name="jnlp.delete.jnlp.file" value="true"/>
  <!-- Application Resources -->
  <j2se version="%java_version%" href="http://java.sun.com/products/autodl/j2se"/>
  <jfx:javafx-runtime version="2.2+"/>
  <jar href="%contextRoot%/java/frmall.jar" download="eager" main="true" />
  <extension name="Extensions" href="%contextRoot%/java/extensions.jnlp"/>
</resources>
```

Figure 7 - Advanced edit screen for Forms Client Templates

7. Click on Apply to save the change.
8. Using the “Activate Edit Session” switch (padlock upper right side), select “Activate Changes”.

Usage Notes

- Oracle Forms must be version 12.2.1.19 or newer.
- The use of Microsoft Internet Explorer or Microsoft Edge with IE-mode are not supported with this configuration.
- The Oracle Cloud tenancy used for this configuration must offer *Identity and Access Management (IAM)* and not its predecessor *Identity Cloud Service (IDCS)*. If your tenancy requires the creation of an Identity Domain, you are using IAM.
- The use of a self-generated SSL/TLS certificate, as instructed in this document will result in various warnings during application startup. It is therefore recommended that a certificate obtained from a known and trusted authority be used.
- The use of the Fusion Middleware SSL/TLS “Demo” certificate is not supported for use with this configuration.
- It may not be possible to use a self-generated SSL/TLS certificate if launching applications using the Forms Standalone Launcher (FSAL). A certificate provided by a known and trusted CA, as described above should be used.

Troubleshooting

Additional troubleshooting information can be found in the IAM documentation here:

https://docs.oracle.com/en-us/iaas/Content/Identity/troubleshooting/troubleshooting_root.htm

When Did Issue Occur	Issue/Error	Possible Cause	Corrective Action
Setup	The PATCH payload is invalid. The "op" or "Operations" attribute can't be null or empty.	<ul style="list-style-type: none"> The Edit panel Save button was pressed, but no changes were made. You attempted to add a Resource or Policy without first saving previous changes. 	<ul style="list-style-type: none"> Use the Cancel link rather than Save if no changes were entered. Cancel current changes and save previous changes. Reattempt to add new changes.
Runtime	HTTP-502 (Bad Gateway)	<ul style="list-style-type: none"> Forms Managed Server is not running. WLS Managed Server is not accessible by the App Gateway client. 	<ul style="list-style-type: none"> Verify the Managed Server is running. Verify firewall (OS and/or external) is allowing communication between the App Gateway client and middle tier server and IAM Cloud Service and App Gateway client. (e.g. ports). Verify the setting for Origin server is correct.
Runtime	HTTP-504 (Gateway Time-out)	<ul style="list-style-type: none"> Origin server (Forms middle tier) not accessible. 	<ul style="list-style-type: none"> Verify the setting for Origin server is correct. Verify the managed server is running. Verify the managed server port is accessible through the firewall.
Runtime	<p>"No subject alternative names present."</p> <p>or</p> <p>"FRM-92575: SSL/TLS hostname verification failed."</p>	<ul style="list-style-type: none"> You are using a self-generated SSL certificate or a certificate that is not properly formatted. The server name (App Gateway client machine) and the server name used in the SSL certificate do not match. 	<ul style="list-style-type: none"> Obtain a certificate from a trusted Certificate Authority (CA). Ensure the server name used with the certificate request matches the server name (in the URL) on which the IAM App Gateway is running.
Runtime	FRM-93261: JNLP file launched from unexpected IP address	<ul style="list-style-type: none"> You have attempted to copy the downloaded jnlp file (if configured to use Java Webstart) and moved the file to another machine. The administrator has enabled the jnlpMatchIP setting (set to TRUE). 	<ul style="list-style-type: none"> Be sure to not copy/move the downloaded jnlp file to another machine, as this is not supported. Disable (set to FALSE) the Forms Web Configuration parameter jnlpMatchIP.

<p>Runtime</p>	<p>Java error indicating that extensions.jnlp cannot be downloaded when trying to run with Java Web Start.</p>	<ul style="list-style-type: none"> • App Gateway client not running on same host with middle tier. 	<ul style="list-style-type: none"> • Verify that extensions.jnlp exists on the server and its file permissions are appropriate for accessing. • Verify the file can be downloaded from a web browser. Use the same protocol, IAM server hostname, and port used by the App Gateway client. • Set Forms Web Configuration parameter webstart_codebase . The value should reflect the same protocol, IAM server, and port used by the App Gateway client.
----------------	--	---	--

References

<https://www.youtube.com/embed/Op5TLTBBABI>

<https://docs.oracle.com/en-us/iaas/Content/Identity>

https://docs.oracle.com/en-us/iaas/Content/Identity/appgateways/faq_using-app-gateways-faq.htm

<https://docs.oracle.com/en-us/iaas/Content/Identity/appgateways/understand-app-gateway.htm>

<https://docs.oracle.com/en-us/iaas/Content/Identity/appgateways/set-app-gateway.htm>

<https://docs.oracle.com/en-us/iaas/Content/Identity/appgateways/register-app-gateway.htm>

<https://docs.oracle.com/en-us/iaas/Content/Identity/appgateways/deploy-oracle-app-gateway-docker-container.htm>

<https://www.docker.com>

<https://docs.docker.com/engine/reference/commandline/docker>

<https://www.openssl.org/docs/manpages.html>

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2023, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.