Oracle® Fusion Middleware

Oracle WebCenter Forms Recognition API Installation Guide

12c (12.2.1.4.0)

F16563-02

April 2021

Documentation for the WebCenter Forms Recognition RESTful API, that describes methods to upload and manage external documents.

ORACLE®

Oracle Fusion Middleware Oracle WebCenter Forms Recognition API Installation Guide, 12c (12.2.1.4.0)

F16563-02

Contents

1   About the WebCenter Forms Recognition RESTful API

The WebCenter Forms Recognition RESTful API provides methods for uploading and managing external documents. Runtime Server further processes the uploaded documents.

1.1   About the User Role

The WebCenter Forms Recognition API user must be a valid WebCenter Forms Recognition user with AEB or ADM role. See *Users, groups, and roles* in the *WebCenter Forms Recognition Designer Guide* for more information.

1.2   Prerequisites

1.2.1   Internet Information Services

WebCenter Forms Recognition API requires that you have installed on your server or workstation Internet Information Services (IIS) and .NET Framework 4.6 or later.

Before you install the WebCenter Forms Recognition API, make sure that the following features are enabled:

- .NET Extensibility
- ASP.NET 4.5
- Windows Authentication
- .NET Framework

2 Getting Started with WebCenter Forms Recognition API Installation

The WebCenter Forms Recognition (WFR) API installation files are included in the WebCenter Forms Recognition setup package.

2.1 Install WebCenter Forms Recognition API

To install the WebCenter Forms Recognition API, complete the following steps:

> **Note:** You need to run the installation from a local directory.

1. Navigate to the `[WebCenter Forms Recognition setup]` directory.

2. Optional. Copy the `[WebCenter Forms Recognition setup]\`**`OracleWFRAPI`** directory to the workstation or server on which you want to install WebCenter Forms Recognition API.

3. Open `OracleWFRApi_Installer.bat` with a text editor.

4. Search for the `InstallDir, AppPoolName, OracleWFRApiAppName,` and `ServerApiPath` attributes and verify that the values correspond to your needs.

   > **Note:** *InstallDir* should be something like *<Installation Path>\WebCenter Forms Recognition\OracleWFRAPI*. Replace *<Installation Path>* path with actual path.

5. Save and close the file.

6. Execute `OracleWFRApi_Installer.bat` as an administrator user.

7. Review the command prompt window for success or error messages.

   > **Note:** In case of errors, you can rerun `OracleWFRApi_Installer.bat` as often as required.

8. Modify the database connection string as described in the next section.

2.2 Modify the Database Connection String

To modify the database connection string, complete the following steps:

1. Open IIS Manager.
2. Right-click **OracleWFRAPI** and then select **Explore**.
3. Open `Web.config` in a text editor.
4. Search for the `<connectionStrings>` element.
5. For an ORACLE database, modify the following values:
   a. Set **Data Source**.
   b. Set **User ID** to the service account user ID.
   c. Set **Password** to the service account password.

   ```
   <connectionStrings> <add name="Entities"
   connectionString="metadata=res://*/Entity.ORAEntities.csdl|res:
   ```

```
//*/Entity.ORAEntities. ssdl|res://*/Entity.ORAEntities.msl;
provider=EFOracleProvider; Provider Connection String='Data
Source=<OracleServerName\InstanceName>;User
ID=<UserID>;Password=<UserPassword>'"
providerName="System.Data.EntityClient" /> </connectionStrings>
```

6. For a **SQL Server** database, modify the following values:
   a. Set **Data Source**.
   b. Set **Initial Catalog** to the SQL Server database catalog.
   c. Set **User ID** to the service account user ID.
   d. Set **Password** to the service account password.

```
<connectionStrings> <add name="Entities"
connectionString="metadata=res://*/Entity.Entities.csdl|res://*
/Entity
.Entities.ssdl|res://*/Entity.Entities.msl;
provider=System.Data.SqlClient;provider connection string="Data
Source=<DataSource>;Initial
Catalog=<SQLServerDatabaseCatalog>;Integrated
Security=false;User
ID=<UserId>;Password=<UserPassword>;MultipleActiveResultSets=Tr
ue&quot;" providerName="System.Data.EntityClient" />
</connectionStrings>
```

7. Optional. Encrypt the Password for a Database Connection String.
8. Save and close the file.

2.3 Encrypt the Password for a Database Connection String

Password encryption in configuration files is optional, but highly recommended. To provide an encrypted password for the database connection in a configuration file, complete the following steps:

1. To create an encrypted password, complete the following substeps:
   a. In the `[Installation path]\WebCenter Forms Recognition\Bin\bin` directory, create a new batch file and give it a meaningful name, such as `CreateEncryptedPassword.bat`.
   b. Copy the following line to the batch file, replacing `MyPassword` with the password you want to encrypt.

   ```
   DstCrypt.exe /text MyPassword > EncryptedPassword.txt
   ```

   Note: The maximum password length is 30 characters.

   c. Save and close the file.
   d. In Windows Explorer, double-click the batch file.
   e. From `[Installation path]\WebCenter Forms Recognition\Bin\bin`, open `EncryptedPassword.txt` in a text editor and copy the encrypted password to the clipboard.
2. Open the required configuration file in a text editor.
3. Search for the `<connectionStrings>` element.
4. In the `<add name>` element, set password as an asterisk.

   ```
   <add name="Entities" Password=*>
   ```

5. In the `<appSettings>` element, add a line with your encrypted password according to the following example.

```
<appSettings> <add key="EncrPwd" value="The_encrypted_Password"/>
</appSettings>
```
6. Save and close the file.

2.4 Specify the Maximum Document File Size

The maximum file size allowed is 256MB. To specify a smaller maximum file size complete the following steps:

1. Open IIS Manager.
2. Right-click **OracleWFRAPI** and then select **Explore**.
3. Open `Web.config` in a text editor.
4. Search for the following line:

```
<add key="MaxFileUploadLimit" value="262144" />
```
5. Set the value parameter to the required value in KB.

2.5 Enable Method Logging

To enable method logging, complete the following steps:

Note: Enable method logging for debugging purposes only as this may affect performance.

---

1. Open IIS Manager.
2. Right-click **OracleWFRAPI** and then select **Explore**.
3. Open `Web.config` in a text editor.
4. Search for the following line.

```
<add key="EnableMethodLog" value="false" />
```
5. Set the value parameter to `true`.
6. In the `[Installation path]\WebCenter Forms Recognition\WebCenter Forms Recognition Web Server` directory, review the `trace.log` file.

2.6 Specify the Token Expiry Time

To specify the token expiry time, complete the following steps:

1. Open IIS Manager.
2. Right-click **OracleWFRAPI** and then select **Explore**.
3. Open `Web.config` in a text editor.
4. Search for the following line:

```
<add key="TokenExpireTime" value="60" />
```
5. Set the value parameter to the required value in minutes.

2.7 Specify the Batch List Limit

To specify the maximum number of batches returned by the `GET ExternalBatch` method, complete the following steps:

> **Note**: The `GET ExternalBatch` method uses the `BatchListLimit` value as default if the optional limit parameter is not specified before executing the method.

1. Open IIS Manager.
2. Right-click **OracleWFRAPI** and then select **Explore**.
3. Open `Web.config` in a text editor.
4. Search for the following line:

   ```
   <add key="BatchListLimit" value="1000" />
   ```
5. Set the value parameter to the required number.

2.8 Configure IIS

The Oracle WFR API installer performs the initial IIS configuration. To verify or modify this configuration, complete the following steps:

1. In IIS, under **Default Web Site**, select **OracleWFRAPI**.
2. In the left pane, right-click **OracleWFRAPI** and then click **Edit Permissions**.
3. In the **Properties** dialog box, on the **Security** tab, review the permissions and then click **OK.**
4. In the middle pane, double-click **Authentication**.
5. In the **Authentication** pane, verify that Windows Authentication is enabled.
6. Right-click **Windows Authentication** and then click **Providers**.
7. In the **Providers** dialog box, verify or add the required providers.
8. In the left pane, click **Application Pools**.
9. In the middle pane, right-click **OracleWFRAPIAppPool** and then select **Advanced Settings**.
10. In the **Advanced Settings** dialog box, verify the following settings and then click **OK**.
    - `Identity = NetworkService`

      > **Note:** The chosen identity needs permissions to access and read files from the `[Installation path]\OracleWFRApiServer` directory and its subdirectories.

    - `Enable 32-bit Applications = True`

2.9 Configure Component Logging

To configure the location of the component log files, complete one of the following steps:

- To save component log files to the default location, in the `C:\Windows\SysWOW64\inetsrv` directory, create a directory named `Log`.

> **Note:** If WebCenter Forms Recognition is installed on the same server, this registry key directs all WebCenter Forms Recognition component log files to this custom location.

2.10 About API Command Line

OracleWFR.CommandLine.Client is an example application, which uses WebCenter Forms Recognition API to upload sets of documents as external batches. Both the source code and compiled application are provided.

See `Readme.txt` in the `[InstallationPath]\OracleWFRAPI\OracleWFR.CommandLine.Client` directory for more information.

2.11 Update Oracle WFR API

The Oracle WFR API installer does not provide an update procedure. If you need to update to a newer version, complete the following steps to retain your unique customizations and back up your settings:

1. Copy the `[Installation path]\OracleWFRAPI` directory to a backup directory.
2. If you modified the settings for the OracleWFRAPI application in IIS, note your settings.
3. Complete the steps in Install WebCenter Forms Recognition API.
4. Compare all customized settings in the backed up `CONFIG` files with the `CONFIG` files in `[Installation path]\OracleWFRAPI` and modify the values if required.
5. In IIS, compare the settings for the OracleWFRAPI application with your previous settings and modify the settings if required.

3 Troubleshooting

If the WFR RESTful API is not working, then verify the problem using the following steps:

1. Open IIS Manager.
2. Right-click **OracleWFRAPI** and then select **Explore**.
3. Open `trace.log` in a text editor. It includes the below error:

```
FATAL System.UnauthorizedAccessException: Filename: redirection.config
Error: Cannot read configuration file due to insufficient permissions
```

To fix the above error, follow these steps:

1. Change the **App Pool** (associated with site OracleWFRAPI) -> **Advanced Settings** -> **Identity** to the user who has modify permissions on C:\Windows\System32\inetsrv\. To check the permissions, browse to C:\Windows\System32\inetsrv\ then folder **Properties** -> **Advanced** -> **Effective access**.
2. Restart the IIS Server.

3.1 Server Error in '/OracleWFRAPI' Application

If there is an HTML response for the failed API request, then take the following actions prescribed in the HTML response. This usually happens due to malformed request or some invalid characters.

3.1.1 Runtime Error

Description: An application error occurred on the server. The current custom error settings on this application prevent the details of the application error from being viewed remotely (for security reasons). The error details, however, can be viewed in browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->
<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

Note: The current error page that you see can be replaced by a custom error page by modifying the `defaultRedirect` attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->
<configuration>
    <system.web>
        <customErrorsmode="RemoteOnly"
defaultRedirect="mycustompage.htm"/>
    </system.web>
</configuration>
```