Oracle® Fusion Middleware

Oracle WebCenter Forms Recognition API Installation Guide

14c (14.1.1.0.0)

F73586-01

August 2023

Provides steps to install the WebCenter Forms Recognition API

ORACLE®

Oracle Fusion Middleware Oracle WebCenter Forms Recognition API Installation Guide, 14c (14.1.1.0.0)

F73586-01

Table of Contents

About the WebCenter Forms Recognition RESTful API

The WebCenter Forms Recognition RESTful API provides methods to upload and manage external documents. The uploaded documents are further processed by Runtime Server.

About the User Role

The WebCenter Forms Recognition API user must be a valid WebCenter Forms Recognition user and have AEB or ADM role. For more information, see "Users, groups, and roles" in the *Oracle WebCenter Forms Recognition Designer User's Guide*.

Prerequisites

Internet Information Services

WebCenter Forms Recognition API requires that you have installed Internet Information Services (IIS) on your server or workstation. Before you install the WebCenter Forms Recognition API, verify that the following features are enabled in IIS.

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

.NET Framework

WebCenter Forms Recognition API requires that you have installed .NET Framework 4.6 or later on your server or workstation.

Load Balancer

When using a load balancer, ensure to enable sticky sessions.

About WebCenter Forms Recognition API Installation

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

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. Run **OracleWFRAPI_Installer.bat** as an administrator.
7. Review the **Command Prompt** window for success or error messages.

   Note: If an error occurred, you can rerun **OracleWFRAPI_Installer.bat** as often as required.

8. Modify the database connection string.

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.
   - Set `Data Source` to the data source.
   - Set `User ID` to the service account user ID.
   - Set `Password` to the service account password.
6. For a SQL Server database, to connect using Windows integrated security, modify the following values.
   - Set `Data Source` to the required data source.
   - Set `Initial Catalog` to the SQL Server database catalog.
   - Remove `User ID=<UserID>;Password=<UserPassword>;`.
   - Set `Integrated Security` to `SSPI`.
7. For a SQL Server database, to connect using SQL Server authentication, modify the following values.
   - Set `Data Source` to the data source.
   - Set `Initial Catalog` to the SQL Server database catalog.
   - Set `User ID` to the service account user ID.
   - Set `Password` to the service account password.
8. Optional. Encrypt the password for a database connection string.
9. Save and close the file.

Encrypt a Password for a Database Connection String

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

1. 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**.
2. Copy one of the following options to the batch file, replacing `MyPassword` with the password you want to encrypt.

Note:

- The maximum character length for a password to encrypt using **RSA-1024** is 30.
- The maximum character length for a password to encrypt using **RSA-3072** is 280.

3.
   - To encrypt the password using the internal RSA-3072 key, use the following option.

     ```
     DstCrypt.exe /text "MyPassword" >> EncryptedPW_
     InternalKeys3072.txt
     ```

   - To encrypt the password using the internal RSA-1024 key, use the following option.

     ```
     DstCrypt.exe /text "MyPassword" /keysize "1024" >>
     EncryptedPW_ InternalKeys1024.txt
     ```

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

   Example

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

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

    Example

    ```
    <appSettings>
    <add key="EncrPwd" value="The_encrypted_Password"/>
    </appSettings>
    ```

11. Save and close the file.

Specify the Maximum Document File Size

The maximum file size which can be uploaded 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.

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.

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.

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 ExternalBatchmethod uses the BatchListLimitvalue 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.

Configure IIS

The WebCenter Forms Recognition 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 click **Advanced Settings**.
10. In the **Advanced Settings** dialog box, verify the following settings and then click **OK**.
    - **Identity = ApplicationPoolIdentity.**
    - **Enable 32-bit Applications = True.**

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

11. Navigate to the **%WINDIR%/System32/inetsrv** directory and then complete the following substeps.
    1. Right-click the **config** directory and then click **Properties**.
    2. In the **config Properties** dialog box, on the **Security** tab, click **Edit**.
    3. In the **Permissions for config** dialog box, to add a new user, click **Add**.
    4. In the **Select Users or Groups** dialog box, click **Locations**.
    5. In the **Locations** dialog box, select the computer where Web Verifier is installed, and then click **OK**.
    6. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** field, type `IIS_IUSRS` and then click **OK**.
    7. In the **Permissions for config** dialog box, verify that the user has the following permissions and then click **Apply**.
        - Read & execute
        - List folder contents
        - Read
    8. If an error message is displayed, click **Continue**.

Configure Server Security for WebCenter Forms Recognition API

To configure the server security, complete the following tasks.

1. Add the User Context in SQL Server
2. Verify the IIS Identity
3. Set Permissions for BAPI Installation Directory

Add the User Context in SQL Server

To use the WebCenter Forms Recognition API (WFRAPI), your users need access rights

for the SQL Server database with the WFRAPI user context. The default user context is Network Service. You can change the default user context to a service account.

Note: If you log on to SQL Server using Windows authentication, you need to add the domain username to the SQL Server database in addition to the NT Authority/Network Service.

To add the user context to SQL Server, complete the following steps.

1. In **Microsoft SQL Server Management Studio**, in the left pane, click **Security > Logins**.
2. Right-click **Logins** and then click **New Login**.
3. In the **Login** dialog box, click **Search**.
4. In the **Select User or Group** dialog box, in the **Enter the object name to select** field, type either `IIS AppPool\OracleWFRAPIAppPool` or the name of the user context, click **Check Names** and then click **OK**.
5. In the **Login Properties** dialog box, in the left pane, click **User Mapping**.
6. In the upper right pane, in the **Map** column, select the check box for the required database.
7. In the lower right pane, select the following database roles and then click **OK**.
   - db_datareader
   - db_datawriter
   - db_runner

Verify the IIS Identity

To verify that IIS run under the appropriate identity, complete the following steps.

1. In **Internet Information Services (IIS) Manager**, in the **Connections** pane, open the server node and then click **Application Pools**.
2. In the **Application Pools** pane, right-click **OracleWFRAPIAppPool** and then click **Advanced Settings**.
3. In the **Advanced Settings** dialog box, under **Process Model**, verify that the **Identity** property has the value `ApplicationPoolIdentity` or the name of the service account.

Set Permissions for WFRAPI Installation Directory

The WebCenter Forms Recognition API application pool or the service account, if used, needs access to its installation directory.

1. In **Windows Explorer**, right-click the [Installation path]\OracleWFRAPI directory and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Edit**.
3. In the **Permissions** dialog box, click **Add**.
4. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** field, type either `IIS AppPool\OracleWFRAPIAppPool` or the name of the user context, click **Check Names** and then click **OK**.

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*.
- To save component log files to a custom location, see "Create the registry key ErrorTraceDir " in the *Oracle WebCenter Forms Recognition Installation Guide*.

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

About API Command Line

OracleWFRApi.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.

For more information, see "Readme.txt" in the [Installation path]\OracleWFRAPI\WebCenter Forms Recognition.CommandLine.Client directory.

Update the Oracle WebCenter Forms Recognition API

The WebCenter Forms Recognition 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.

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: ilename: 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.

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.

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>
```

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>
        <customErrors mode="RemoteOnly"
defaultRedirect="mycustompage.htm"/>
    </system.web>
</configuration>
```