# Oracle Functional Services

# Post OIC upgrade Apex Dashboard not rendering info

**Version Management:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Change Description** | **Section/Page** | **Changed by** | **Status**  **(Draft/Final)** | **Version** |
| 21 Oct 2025 | Post OIC upgrade Apex Dashboard not rendering info | 1 | Sagnik | Draft | 1 |

## Specification for Oracle Development / Configuration

:

|  |  |
| --- | --- |
| **Incident Number/ Jira** | CEN-13228 / 3-40183087978 |
| **RFC Title**  One sentence description of the required change | Post OIC upgrade Apex Dashboard not rendering info |
| **Purpose of Change**  What is the functionality to be used for (more detail) | To provide users with a user-friendly and centralized approach to efficiently plan and manage day to day activities |
| **Responsible User** | **Rowan/Christo** |
| **Functional Consultant** | **Mumtaz Mohamed** |
| **Developer** | Smitha Aldrin |
| **Date of request** | 9 Oct 2025 |
| Business Requirements | |

*Scenario:*

After the Oracle Integration Cloud (OIC) upgrade (Gen3), the APEX dashboard is no longer able to render data because it was using basic authentication (username/password). The new OIC version requires OAuth2 authentication, and the integration between APEX and OIC is broken across DEV, TEST, and PROD environments.

|  |
| --- |
| **Impact Analysis** |

*List the impact on the following:*

* *Business Area / Processes affected.*
* *DB details*

* *Storage requirements:* N/A
* *Performance – Online and Batch windows:* N/A
* *Security and Authorisation access: Oracle APEX* Role Based Access
* *User training:* N/A
* *Implementation timing constraint/s:* N/A
* *Cross-dependencies on other projects or RFC implementations:* N/A
* *Data Impacts:* N/A
* *List the different solution options and motivating factors for the recommended solution.* 
  + Restore the APEX dashboard’s ability to render and display OIC data after the OIC authentication upgrade.
  + Ensure secure, maintainable authentication by moving from basic authentication to OAuth2, in line with Oracle’s requirements.
  + Abstract sensitive configuration (client/secret) so it is not exposed in code.

|  |
| --- |
| **Functional Requirements** |

* NA

|  |
| --- |
| **Technical Requirements** |

* Amend APEX code to use OAuth2 authentication via APEX\_WEB\_SERVICE.OAUTH\_AUTHENTICATE\_CREDENTIAL.
* Store wallet path and password in APEX workspace parameters (not hardcoded).
* Create and configure wallets with only ROOT & INTERMEDIATE certificates, stored at defined paths per environment.
* Use static credential IDs for web credentials stored in APEX.
* Ensure all endpoints and callback URLs are added to the “Valid for URL” section in APEX.
* Address and resolve ORA-29024 (certificate validation failure) by ensuring correct certificates are loaded and referenced.
* Provide PL/SQL code samples for token retrieval and REST calls.
* Coordinate with DBAs for OAuth security configuration and with ACS team for implementation

|  |
| --- |
| **Performance Analysis** |

*Is a Performance Analysis required for this development?* NO

|  |
| --- |
| **Testing Requirements** |

### ****Test Strategy & Scenarios****

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Test Scenario | Steps | Expected Result | Notes/References |
| 1 | OAuth2 Token Retrieval | Execute PL/SQL/APEX code to retrieve OAuth2 token using credentials from APEX workspace config | Token is successfully retrieved; credentials are not exposed in code or logs | [CEN-13228: Post OIC upgrade | Apex Dashboard not rendering info**WIP**](https://oldmutual.atlassian.net/browse/CEN-13228?focusedCommentId=787771) |
| 2 | REST API Call to OIC Endpoint | Use retrieved token to call OIC REST endpoint from APEX | API call succeeds and returns expected data | https://omlaoicdev.opc.oracleoutsourcing.com/ic/ws/integration/v1/flows/soap/OML\_INT\_GL\_BUDGE\_CENTR\_DETAI/1.0/ |
| 3 | Wallet Path and Password Retrieval | Retrieve wallet path and password from APEX workspace parameters | Correct wallet is used; no hardcoded values in code | Wallets should only have ROOT & INTERMEDIATE certificates |
| 4 | Certificate Validation | Make REST call with valid and invalid certificates | Valid: call succeeds; Invalid: ORA-29024 error is raised and handled gracefully | [CEN-13228: Post OIC upgrade | Apex Dashboard not rendering info**WIP**](https://oldmutual.atlassian.net/browse/CEN-13228?focusedCommentId=735832) |
| 5 | URL Whitelisting | Attempt REST calls to both whitelisted and non-whitelisted URLs | Whitelisted: call succeeds; Others: ORA-20987 error | [CEN-13228: Post OIC upgrade | Apex Dashboard not rendering info**WIP**](https://oldmutual.atlassian.net/browse/CEN-13228?focusedCommentId=710186) |
| 6 | Environment-Specific Configuration | Deploy and test in DEV, TEST, PROD with their own credentials, wallet, and URLs | All environments function independently and securely | Wallet paths: /interface/j\_omla/{instanceID}/Wallet/ (DEV/TEST), /interface/i\_omla/{instanceID}/Wallet/ (PROD) |
| 7 | Security and Access Control | Attempt to access credentials/configuration from unauthorized users | Access denied; only authorized users (e.g., APEX\_ADMINISTRATOR\_ROLE) can manage credentials | XXCUS user requires APEX ADMIN access |
| 8 | Error Handling | Simulate token expiry, invalid credentials, and network failures | Errors are logged and handled; no sensitive info leaked |  |
| 9 | Negative Testing | Use invalid credentials, expired tokens, incorrect URLs | Appropriate error messages; no data leakage |  |
| 10 | Regression Testing | Test dashboard functionality after authentication change | Dashboard renders OIC data as before, with new authentication |  |