

Oracle Financial Services Behavior Detection

API Services Guide

Release 8.1.2.1.0

June 2022



Oracle Financial Services Behavior Detection API Services Guide

Copyright © 2024 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information on third party licenses, click [here](#).

Document Control

Table 1: Revision History

| Date | Edition | Description |
|-----------|-----------|--|
| June 2022 | 8.1.2.1.0 | Created first version of OFS BD 8.1.2.1.0 API Service Guide. |

Table of Contents

| | | |
|----------|--|-----------|
| 1 | Preface | 5 |
| 1.1 | Purpose of this Document | 5 |
| 1.2 | Intended Audience..... | 5 |
| 1.3 | Related Documents..... | 5 |
| 2 | Overview | 6 |
| 2.1 | Types of Services..... | 6 |
| 2.2 | Prerequisites..... | 6 |
| 3 | Configuring Tables | 7 |
| 3.1 | Trusted Pair | 7 |
| 3.2 | Alert Suppression..... | 8 |
| 4 | Services | 9 |
| 4.1 | Trusted Pairs | 9 |
| 4.1.1 | <i>Run Trusted Pair API</i> | 9 |
| 4.1.2 | <i>Response Parameters</i> | 10 |
| 4.1.3 | <i>Response JSON Sample</i> | 12 |
| 4.2 | Alert Suppression..... | 13 |
| 4.2.1 | <i>Run Alert Suppression API</i> | 13 |
| 4.2.2 | <i>Response Parameters</i> | 15 |
| 4.2.3 | <i>Response JSON Sample</i> | 17 |
| 5 | OFSAA Support Contact Details | 19 |
| 6 | Send Us Your Comments | 20 |

1 Preface

This preface provides supporting information for the Oracle Financial Services Behavior Detection Application Pack (OFS BD) API Services.

Topics:

- [Purpose of this Document](#)
- [Intended Audience](#)
- [Related Documents](#)

1.1 Purpose of this Document

This document contains the API services information for Oracle Financial Services Behavior Detection Application Pack. The objective of this API Services Guide is to provide information about the REST APIs for OFSBD.

This guide assumes that the audience has technical and functional expertise in using and working with REST APIs. This document does not teach REST concepts.

1.2 Intended Audience

This document is intended for users of OFS BD. You must be able to utilize the API service to allow full or filtered Trusted Pair and Alert Suppression data to be loaded to OFS BD based on inputs provided.

1.3 Related Documents

This section identifies additional documents related to OFS BD. You can access from the [Documentation Library \(OHC\)](#).

- Oracle Financial Services Behavior Detection Installation Guide
- Oracle Financial Services Behavior Detection User Guide

To find more information about Oracle Financial Services and our complete product line, visit our Web site www.oracle.com/financialservices.

2 Overview

OFS BD API offers services to allow the OFS BD to consume trusted pair and Alert Suppression information present in AML Case Management System.

Trusted Pair is the concept of reducing the number of false positives events by identifying transactions between parties viewed as having a trusted relationship. The Trusted Pair API will allow full or filtered Trusted Pair data to be loaded to OFS BD based on inputs provided.

Alert Suppression enables the automatic suppression of a particular entity's newly-generated alerts based on criteria such as highlight, scenario, and suppression rule begin and end date. The Alert Suppression API will allow full or filtered Trusted Pair data to be loaded to OFS BD based on inputs provided.

Topics:

- [Types of Services](#)
- [Prerequisites](#)

2.1 Types of Services

The following service is supported:

- **Trusted Pairs** - This service allows OFS BD to consume trusted pair information present within AML Case Management System.
- **Alert Suppression** - This service allows OFS BD to consume Alert Suppression information present within AML Case Management System.

2.2 Prerequisites

The following are the list of prerequisites to use the API service:

1. Behavior Detection 8121 setup should be installed.
2. The user should have knowledge about Behavior Detection Trusted Pair and Alert suppression Functionality. For information about these functionalities, see the [Oracle Financial Services Behavior Detection User Guide](#).
3. Invoke the Trusted Pair API prior to ingestion. Invoke the Alert Suppression API after ingestion and prior to post processing jobs.
4. The user should have the REST Service URL as received from AML Case Management System.
5. The user must have Access Credentials to the REST Web service (Trusted Pair, Alert Suppression) as received from AML Case Management System.

3 Configuring Tables

Topics:

- [Trusted Pair](#)
- [Alert Suppression](#)

3.1 Trusted Pair

For the Trusted Pair API, status code and direction code are configured using `kdd_trusted_pair_map` table.

Table 1: Columns in `kdd_trusted_pair_map`

| Column Name | Description |
|--------------|--|
| MAP_COLUMN | Column Name of Behavior Detection Trusted Pair Table |
| LOOKUP_CODE | Field value received from AML Case Management System |
| LOOKUP_VALUE | Configured field value in Behavior Detection |

- Status code and Direction code can be configured by updating LOOKUP_CODE in `kdd_trusted_pair_map` table
- LOOKUP_CODE can be updated as per the value we get from the AML Case Management System

NOTE User should not update MAP_COLUMN, LOOKUP_VALUE field.

The default data values in the `kdd_trusted_pair_map` table are mentioned below:

Table 2: Default Values for `kdd_trusted_pair_map`

| MAP_COLUMN | LOOKUP_CODE | LOOKUP_VALUE |
|------------|-------------|--------------|
| TP_DIRN_CD | SEND | SEND |
| TP_DIRN_CD | RECEIVE | RECEIVE |
| TP_DIRN_CD | BOTH | BOTH |
| STATUS_CD | TPAPP | AC |
| STATUS_CD | TPEXP | IAC |

3.2 Alert Suppression

For the Alert Suppression API, status code and direction code are configured using `kdd_service_map` table.

Table 3: Columns in `kdd_service_map`

| Column Name | Description |
|--------------|---|
| SERVICE_NAME | Name of the Rest service provider |
| MAP_COLUMN | Column Name of Behavior Detection Alert Suppression Table |
| LOOKUP_CODE | Field value received from AML Case Management System |
| LOOKUP_VALUE | Configured field value in Behavior Detection |

LOOKUP_CODE can be updated as per the value we get from the AML Case Management System.

NOTE User should not update SERVICE_NAME, MAP_COLUMN, LOOKUP_VALUE field.

The default data values in the `kdd_service_map` table are mentioned below

Table 4: Default Values for `kdd_service_map`

| MAP_COLUMN | LOOKUP_CODE | LOOKUP_VALUE |
|-----------------------------|-------------|--------------|
| LAST_SUPPR_RESULT_STATUS_CD | SUPAPP | AC |
| LAST_SUPPR_RESULT_STATUS_CD | SUPEXP | IAC |

4 Services

The following services are available:

- [Trusted Pairs](#)
- [Alert Suppression](#)

4.1 Trusted Pairs

This service allows Oracle Financial Services Behavior Detection (OFS BD) to consume trusted pair information present within AML Case Management System. The following topics explain how to configure and use the Trusted Pair information:

- [Run Trusted Pair API](#)
- [Response Parameters](#)
- [Response JSON Sample](#)
- [Alert Suppression](#)

4.1.1 Run Trusted Pair API

Follow these steps to run the trusted pair API service.

1. To configure the Trusted pair API using the Trusted Pair configurator:
 - a. Login to APP Server and navigate to `$FIC_HOME/database/db_tools/`
 - b. Open `log4j2.xml` file with a notepad and update the String from `@ORION_DB_DBTOOLS_PATH@` to `{FIC Home Path}/database/db_tools`

NOTE {FIC Home Path} should be replaced with the exact FIC Home path
(For example: `/scratch/ofsaapp/BDECM812/BDECM812`)

- c. Login to APP Server and navigate to `$FIC_HOME/database/db_tools/bin` (For example, `cd $FIC_HOME/database/db_tools/bin`)
- d. Execute `tp_configurator.sh` (Step: `./tp_configurator.sh`)
- e. Provide the URL, Username and Password of the Trusted Pair REST Service as received from AML Case Management System. This will update the trusted pair configuration file, `tpconfig.xml` (Located at `$FIC_HOME/database/db_tools/mantas_cfg/` in APP Server)
- f. The Trusted Pair API provides the option to filter by Business domain(s). The `tpconfig.xml` can be configured by updating the tag `<Domain>` with Business domain(s). When configured only filtered data as per specified Business Domain(s) will flow into Behavior Detection Trusted pair Tables (`kdd_trusted_pair`, `kdd_trusted_pair_mbr`) from AML Case Management System.
 - `<Domain>d</Domain>` for single domain,
 - `<Domain>d,a</Domain>` for multiple domains

NOTE Multiple domain(s) should be comma delimited

- g. The Trusted Pair API provides the option to filter according to Jurisdiction. The `tpconfig.xml` can be configured by updating the tag `<Jurisdiction>` with Jurisdiction(s). When configured

only filtered data as per specified Jurisdiction(s) will flow into Behavior Detection Trusted pair Tables (kdd_trusted_pair, kdd_trusted_pair_mbr) from the AML Case Management System.

- <Jurisdiction>AMEA</Jurisdiction> for single Jurisdiction,
- <Jurisdiction>AMEA,IN</Jurisdiction> for multiple Jurisdictions

NOTE Multiple Jurisdictions should be comma delimited.

2. After configuring the Trusted Pair API, navigate to \$FIC_HOME/database/db_tools/bin directory of APP Server and Execute tp_dataload.sh. For example,
 - a. cd \$FIC_HOME/database/db_tools/bin
 - b. ./tp_dataload.sh

On successful execution, the console will display the message "Job Completed Successfully..." and return code will be 0 in \$FIC_HOME/database/db_tools/logs/trustedpair.log file. The Trusted Pair information will flow from AML Case Management System to Behavior Detection data base tables (kdd_trusted_pair, kdd_trusted_pair_mbr).

If any error occurs during execution of tp_dataload.sh, the status code will be -1 in the \$FIC_HOME/database/db_tools/logs/trustedpair.log file.

Each trusted pair record received from REST Service, with status codes such as Approved and Expired (Example, TPAPP, TPEXP) will get stored as AC, IAC respectively in the Behavior Detection Trusted pair table.

4.1.2 Response Parameters

The following table describes the details of response parameters.

NOTE The API response is in a String format.

Table 1: Trusted Pairs Response Parameter Details

| Business Name | API Response Data Element | Description | Data Type and Length |
|---------------------------|---------------------------|--|----------------------|
| Trusted pair Code | tpCode | For ECM created Trusted pairs this is the same as Trusted pair Seq (running seq). This column is added to support Third party Trusted pairs in future. | String (100) |
| Trusted pair Sequence ID | tpSeqId | Displays Running Sequence | Number (10) |
| Trusted Pair Created ID | tpCreatId | Displays ID of the user who requested the Trust. It is a number. | Number (10) |
| Trusted Pair Created Date | tpCreateDate | Displays Date on which Trust request happened | Date |
| Expiration Date | tpExprnDate | Displays Expiration date of the Trust record | Date |

Table 1: Trusted Pairs Response Parameter Details

| Business Name | API Response Data Element | Description | Data Type and Length |
|---------------------------------|---------------------------|---|----------------------|
| Status Code | tpStatusCode | <p>Displays out of box statuses present in FCC_TP_STATUS table in ECM. Clients can configure their own statuses. F_ACTIVE_FL denotes the Statuses in which a Trust record is Active. F_SHARED_FL denotes the statuses of Trust Records which will be moved to BD.</p> <p>For example:</p> <ul style="list-style-type: none"> • V_STATUS_CD <ul style="list-style-type: none"> ■ TPPND ■ TPAPP ■ TPREJ ■ TPEXP • V_STATUS_NM <ul style="list-style-type: none"> ■ Pending Approval ■ Approved ■ Rejected ■ Expired • F_ACTIVE_FL <ul style="list-style-type: none"> ■ Y ■ N • F_SHARED_FL <ul style="list-style-type: none"> ■ Y ■ N | String (20) |
| Event Code | tpEventCode | Displays the Event Code for which they identified the parties from transactions | Number (22) |
| Case ID | tpCaseld | Displays the case ID which was used to create the trusted pair | String (15) |
| Trusted pair Member Sequence ID | tpMbrSeqId | Displays Running Sequence | Number (10) |
| Party1 Sequence | tpMbrParty1Seq | For External Entity, External Entity Sequence will be passed. Else "" will be passed. | String (30) |
| Party1 ID | tpMbrParty1Id | Displays External Entity ID/Account ID | String (50) |
| Party1 ID type | tpMbrParty1TypeCd | Displays Internal Account (one of IA, GL) and External Entity (one of XA, CC, CO, DL, GM, GP, LE, MC, ND, NR, PP, SS, TX, AR, OT, IBAN) | String (20) |
| Party1 Name | tpMbrParty1Nm | Displays External Entity/Account Name | String (350) |
| Party1 Risk | tpMbrParty1RiskNb | Displays External Entity/Account Risk | Number (3) |
| Party1 Jurisdiction | tpMbrParty1JurisdictionCd | Displays Jurisdiction of External Entity /Account | String (5) |

Table 1: Trusted Pairs Response Parameter Details

| Business Name | API Response Data Element | Description | Data Type and Length |
|------------------------|---------------------------|--|----------------------|
| Party1 Business domain | tpMbrParty1BusDmn | Displays Business domain of External Entity / Account | String (65) |
| Party2 Sequence | tpMbrParty2Seq | For External Entity External Entity Sequence will be passed. Else "" will be passed. | String (30) |
| Party2 ID | tpMbrParty2Id | Displays External Entity ID/Account ID | String (50) |
| Party2 ID type | tpMbrParty2TypeCd | Displays Internal Account (one of IA, GL) and External Entity (one of XA,CC,CO,DL,GM,GP,LE,MC,ND,NR,PP,SS,TX,AR,OT,IBAN) | String (20) |
| Party2 Name | tpMbrParty2Nm | Displays External Entity/Account Name | String (350) |
| Party2 Risk | tpMbrParty2RiskNb | Displays External Entity /Account Risk | Number (3) |
| Party2 Jurisdiction | tpMbrParty2JurisdictionCd | Displays Jurisdiction of External Entity /Account | String (5) |
| Party2 Business domain | tpMbrParty2BusDmn | Displays Business domain of External Entity / Account | String (65) |
| Direction | tpDirnCd | Out of box displays values SEND, RECEIVE, BOTH | String (7) |
| Last Modified by | tpReviewerId | Displays Reviewer ID. It is a number. | Number (10) |
| Last Modified date | tpReviewDate | Displays Review Date | Date |
| Last Comment | tpReviewComment | Displays Review Reason | String (2500) |

4.1.3 Response JSON Sample

This section contains a response JSON sample to get Trusted Pair information. The entries in this sample are only for reference purposes.

```
{
  "tpCode": "",
  "tpSeqId": "",
  "tpCreateId": "",
  "tpCreateDate": "",
  "tpExprnDate": "",
  "tpStatusCode": "",
  "tpEventCode": "",
  "tpCaseId": "",
  "tpMbrSeqId": "",
```

```

"tpMbrParty1Seq": " ",
"tpMbrParty1Id": "",
"tpMbrParty1Nm": "",
"tpMbrParty1TypeCd": "",
"tpMbrParty1RiskNb": "",
"tpMbrParty1JrsdcnCd": "",
"tpMbrParty1BusDmn": "",
"tpMbrParty2Seq": "",
"tpMbrParty2Id": "",
"tpMbrParty2Nm": "",
"tpMbrParty2TypeCd": "",
"tpMbrParty2RiskNb": "",
"tpMbrParty2JrsdcnCd": "",
"tpMbrParty2BusDmn": "",
"tpDirnCd": "",
"tpReviewerId": "",
"tpReviewDate": "",
"tpReviewComment": ""
}

```

4.2 Alert Suppression

This service allows Oracle Financial Services Behavior Detection (OFS BD) to consume Alert Suppression information present within AML Case Management. The following topics explain how to configure and use the Alert Suppression information:

- [Run Alert Suppression API](#)
- [Response Parameters](#)
- [Response JSON Sample](#)

4.2.1 Run Alert Suppression API

Follow these steps to run the Alert Suppression API service.

1. Follow these steps to configure the Alert Suppression API using the Alert Suppression configurator.
 - a. Login to APP Server and navigate to \$FIC_HOME/database/db_tools/
 - b. Open log4j2.xml file with a notepad and update the String from @ORION_DB_DBTOOLS_PATH@ to {FIC Home Path}/database/db_tools

NOTE {FIC Home Path} should be replaced with the exact FIC Home path (For example: /scratch/ofsaapp/BDECM812/BDECM812)

- c. Login to APP Server and navigate to `$FIC_HOME/database/db_tools/bin` (For example, `cd $FIC_HOME/database/db_tools/bin`).
- d. Execute `alsup_configurator.sh` (Step: `./alsup_configurator.sh`)

NOTE Run the script only once to configure API URL, username, password, and other parameters.

- e. Provide the URL, Username, Password, `BICTypeLength` of the Alert Suppression REST Service as received from AML Case Management System. It will update alert suppression configuration file i.e. `serviceconfig.xml` (File is located at path `$FIC_HOME/database/db_tools/mantas_cfg/` in APP Server).

NOTE `BICTypeLength` in `serviceconfig.xml` should be same as in `BDF.xml`(File is located at path `$FIC_HOME/bdf/config/BDF.xml` in APP Server)

- The Behavior Detection Alert Suppression API provides the option to filter according to Business domain(s). User can configure the `serviceconfig.xml` by updating the tag `<Domain>` with Business domain(s). When configured only filtered data as per specified Business Domain(s) will flow into Behavior Detection Alert Suppression Tables (`kdd_auto_suppr_alert`) from AML Case Management System. For example,
 - `<Domain>d</Domain>` for single domain,
 - `<Domain>d,a</Domain>` for multiple domains

NOTE Multiple domain(s) should be comma delimited

- The Behavior Detection Alert Suppression API provides the option to filter according to Jurisdiction. User can configure the `serviceconfig.xml` by updating the tag `<Jurisdiction>` with Jurisdiction(s). When configured only filtered data as per specified Jurisdiction(s) will flow into Behavior Detection Alert Suppression Tables (`kdd_auto_suppr_alert`) from the AML Case Management System. For example,
 - `<Jurisdiction>AMEA</Jurisdiction>` for single Jurisdiction
 - `<Jurisdiction>AMEA,IN</Jurisdiction>` for multiple Jurisdictions

NOTE Multiple Jurisdiction should be comma delimited.

2. After configuring Alert Suppression, Navigate to `$FIC_HOME/database/db_tools/bin` directory of APP Server and Execute `alsup_dataload.sh`. For example,
 - a. `cd $FIC_HOME/database/db_tools/bin`

b. `./alsup_dataload.sh`

NOTE

- Before running the 507 post processing jobs, run the `alsup_dataload.sh` script everyday which populates alert suppression data and it is full load.
- The template 507 (for alert suppression) must be run every day for suppressing alerts based on the active suppression rules created during the previous script execution (`alsup_dataload.sh`).

On successful execution, the console will display the message "Job Completed Successfully..." and return code will be 0 in `$FIC_HOME/database/db_tools/logs/alertsuppression.log` file. The Alert Suppression information will flow from the AML Case Management System to Behavior Detection data base tables (`kdd_auto_suppr_alert`).

If any error occurs during execution of `alsup_dataload.sh`, the status code will be -1 in the `$FIC_HOME/database/db_tools/logs/alertsuppression.log` file.

NOTE

After execution the rejected records will be archived at each execution in a separate log file whose complete details with path will be given in `$FIC_HOME/database/db_tools/logs/alertsuppression.log` file.

Each alert suppression record received from REST Service with status codes Approved and Expired (SUPAPP and SUPEXP) will get stored as AC, IAC respectively in Behavior Detection Alert suppression table.

4.2.2 Response Parameters

The following table describes the details of response parameters.

NOTE

The API response is in a String format.

Table 2: Alert Suppression Response Parameter Details

| Business Name | API Response Data Element | Description | Data Type and Length |
|----------------------------|---------------------------|---|----------------------|
| Suppression Code | supCode | For ECM created Suppression rules this would be similar to Suppression rule Seq (running seq). But this column has been added in case we have Third party Suppression rules in the future | String (100) |
| Suppression Sequence ID | supSeqId | Running Sequence | Number (10) |
| Suppression Created ID | supCreatId | ID of the user who requested the Suppression rule. | Number (10) |
| Suppression Created Date | supCreateDate | Date on which Suppression rule request happened | Date |
| Suppression Effective Date | supEffectiveDate | Effective date of the Suppression rule record | Date |

Table 2: Alert Suppression Response Parameter Details

| Business Name | API Response Data Element | Description | Data Type and Length |
|-----------------------------|---------------------------|--|----------------------|
| Suppression Expiration Date | supExprnDate | Expiration date of the Suppression rule record | Date |
| Suppression Status Code | supStatusCode | <p>The following OOB statuses are present in the FCC_SUP_STATUS table in ECM. Clients can configure their own statuses. F_ACTIVE_FL denotes the Statuses in which we say a Suppression rule is Active. F_SHARED_FL denotes the statuses of Suppression rule which will be moved to BD.</p> <p>For example:</p> <ul style="list-style-type: none"> • V_STATUS_CD <ul style="list-style-type: none"> ▪ SUPPND ▪ SUPAPP ▪ SUPREJ ▪ SUPEXP • V_STATUS_NM <ul style="list-style-type: none"> ▪ Pending Approval ▪ Approved ▪ Rejected ▪ Expired • F_ACTIVE_FL <ul style="list-style-type: none"> ▪ Y ▪ N • F_SHARED_FL <ul style="list-style-type: none"> ▪ Y ▪ N | String (20) |
| Event Code | supEventCode | The Event Code of the event which was selected and the Suppression request was made. | Number (22) |
| Case ID | supCaseId | The case ID which was used to create the Suppression request | String (15) |
| Scenario Key | supScenarioSkey | The Scenario Skey of the Event selected | Number (10) |
| Scenario Original Skey | upScenarioOrigSkey | The Scenario Original Skey fetched from FCC_SCENARIO_MASTER table using The Scenario Skey of the Event | Number (22) |
| Entity Type | supEntityType | Focus Type of the Event selected | Varchar2(50) |
| Centricity Code | supCentricityCd | Centricity ID from kdd_centricity table using the Focus Type of Event | Number (10) |

Table 2: Alert Suppression Response Parameter Details

| Business Name | API Response Data Element | Description | Data Type and Length |
|--------------------|---------------------------|--|----------------------|
| Entity Sequence ID | supEntitySeq | For External Entity/Address focus type, pass External Entity Sequence/Address Sequence respectively else it will be "" | Varchar2(30) |
| Entity ID | supEntityId | For Client bank, pass instn_id_type_cd '/' institution_cd else it is the Focus Entity ID | Varchar2(50) |
| Jurisdiction | supJrsdcnCd | Jurisdiction of Event selected | String (5) |
| Business domain | supBusDmn | Business domain of Event selected | String (65) |
| Last Modified by | supReviewerId | This can be considered as Reviewer ID. It is a number | Number (10) |
| Last Modified date | supReviewDate | This can be considered as Review Date | Date |
| Last Comment | supReviewComment | This can be considered as Review Reason- | String (2500) |

4.2.3 Response JSON Sample

This section contains a response JSON sample to get Alert Suppression information. The entries in this sample are only for reference purposes.

```
{
  "supCode": "",
  "supSeqId": "",
  "supCreateId": "",
  "supCreateDate": "",
  "supEffectiveDate": "",
  "supExprnDate": "",
  "supStatusCode": "",
  "supEventCode": "",
  "supCaseId": "",
  "supScenarioSkey": " ",
  "supScenarioOrigSkey": "",
  "supEntityType": "",
  "supCentricityCd": "",
  "supEntitySeq": "",
  "supEntityId": "",
  "supJrsdcnCd": "",
  "supBusDmn": "",
```

```
"supReviewerId": "",  
"supReviewDate": "",  
"supReviewComment": ""  
}
```

OFSAA Support Contact Details

Raise a Service Request (SR) in [My Oracle Support \(MOS\)](#) for queries related to OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.

