

# Oracle® Banking Corporate Lending Process Management API Security Guide



Release 14.7.5.0.0  
G14986-01  
September 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2018, 2024, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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. No other rights are granted to the U.S. Government.

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, MySQL, and NetSuite 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.

# Contents

## Preface

---

Purpose	iv
Audience	iv
Documentation Accessibility	iv
Critical Patches	v
Diversity and Inclusion	v
Related Resources	v
Conventions	v
Screenshot Disclaimer	v
Acronyms and Abbreviations	vi
Basic Actions	vi
Symbols and Icons	vii
Scope	x

## 1 Securing API Services

---

1.1 API Layer	1-1
1.2 List of Services	1-5

## Index

---

# Preface

This topic contains following sub-topics:

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Critical Patches](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)
- [Basic Actions](#)
- [Symbols and Icons](#)
- [Scope](#)

## Purpose

This document provides security-related usage and configuration recommendations for Oracle Banking Corporate Lending Process Management. This guide may outline procedures required to implement or secure certain features, but it is also not a general-purpose configuration manual.

## Audience

This guide is primarily intended for Developers for Oracle Banking Corporate Lending Process Management and third party or vendor software's. Some information may be relevant to IT decision makers and users of the application are also included.

**Note:**

Readers are assumed to possess basic operating system, network, and system administration skills with awareness of vendor/third-party software's and knowledge of Oracle Banking Corporate Lending Process Management application.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

## Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at [Critical Patches](#), [Security Alerts and Bulletins](#). All critical patches should be applied in a timely manner to make sure effective security, as strongly recommended by [Oracle Software Security Assurance](#).

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## Related Resources

For more information on any related features, refer to the following documents:

- *Routing Hub Configuration User Guide*

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

## Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

## Acronyms and Abbreviations

The list of the acronyms and abbreviations that are used in this guide are as follows:

**Table 1 Acronyms and Abbreviations**


Acronyms	Abbreviations
API	Application Programming Interface
JSON	JavaScript Object Notation
JWT	JSON Web Tokens
OAM	Oracle Access Manager
OAuth	Open Authorization
SAML	Security Assertion Markup Language
SSO	Single Sign-On

## Basic Actions

**Table 2 List of Basic Actions**

Action	Description
<b>Approve</b>	Click <b>Approve</b> to approve the initiated report. This button is displayed, once the user click <b>Authorize</b> .
<b>Audit</b>	Click <b>Audit</b> to view the maker details, checker details of the particular record, and record status. This button is displayed only for the records that are already created.
<b>Authorize</b>	Click <b>Authorize</b> to authorize the record created. A maker of the screen is not allowed to authorize the report. Only a checker can authorize a record. This button is displayed only for the already created records.
<b>Close</b>	Click <b>Close</b> to close a record. This action is available only when a record is created.
<b>Confirm</b>	Click <b>Confirm</b> to confirm the performed action.
<b>Cancel</b>	Click <b>Cancel</b> to cancel the performed action.
<b>Compare</b>	Click <b>Compare</b> to view the comparison through the field values of old record and the current record. This button is displayed in the widget, once the user click <b>Authorize</b> .
<b>Collapse All</b>	Click <b>Collapse All</b> to hide the details in the sections. This button is displayed, once the user click <b>Compare</b> .
<b>Expand All</b>	Click <b>Expand All</b> to expand and view all the details in the sections. This button is displayed, once the user click <b>Compare</b> .

Table 2 (Cont.) List of Basic Actions

Action	Description
<b>New</b>	Click <b>New</b> to add a new record. The system displays a new record to specify the required data.  <div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; background-color: #E6F2FF; margin-top: 10px;"> <p> <b>Note:</b> The fields which are marked with Required are mandatory.</p> </div>
<b>OK</b>	Click <b>OK</b> to confirm the details in the screen.
<b>Save</b>	Click <b>Save</b> to save the details entered or selected in the screen.
<b>View</b>	Click <b>View</b> to view the report details in a particular modification stage. This button is displayed in the widget, once the user click <b>Authorize</b> .
<b>View Difference only</b>	Click <b>View Difference only</b> to view a comparison through the field element values of old record and the current record, which has undergone changes. This button is displayed, once the user click <b>Compare</b> .

## Symbols and Icons

The following symbols and icons are used in the screens.

Table 3 Symbols and Icons - Common





Symbol/Icon	Function
	Minimize
	Maximize
	Close
	Perform Search

Table 3 (Cont.) Symbols and Icons - Common










Symbol/Icon	Function
	Open a list
	Add a new record
	Navigate to the first record
	Navigate to the last record
	Navigate to the previous record
	Navigate to the next record
	Grid view
	List view
	Refresh



Table 3 (Cont.) Symbols and Icons - Common








Symbol/Icon	Function
	Calendar
	Filter
	Copy a record
	Click this icon to add a new row.
	Click this icon to delete an existing row.
	Click to view the created record.
	Click to unlock, delete, authorize or view the created record.

Table 4 Symbols and Icons - Audit Details



Symbol/Icon	Function
	A user
	Date and time

Table 4 (Cont.) Symbols and Icons - Audit Details







Symbol/Icon	Function
	Unauthorized or Closed status
	Authorized or Open status

Table 5 Symbols and Icons - Widget

Symbol/Icon	Function
	Open status
	Unauthorized status
	Closed status
	Authorized status

## Scope

### Read Sections Completely

Each section should be read and understood completely. Instructions should never be blindly applied. Relevant discussion may occur immediately after instructions for an action, so be sure to read whole sections before beginning implementation.

### Understand the Purpose of this Guidance

The purpose of the guidance is to provide security-relevant code and configuration recommendations.

**Limitations**

This guide is limited in its scope to security-related guideline for developers.

# 1

## Securing API Services

This topic describes about securing API services.

Different applications deployed on disparate platforms and using different infrastructure need to be able to communicate and integrate seamlessly with Oracle Banking Corporate Lending Process Management in order to exchange data. The Oracle Banking Corporate Lending Process Management Service API Gateway will cater to these integration needs.

The integration needs supported by the Gateway can be broadly categorized from the perspective of the Gateway as follows:

- Inbound application integration – used when any external system needs to add, modify or query information within Oracle Banking Corporate Lending Process Management.
- Outbound application integration – used when any external system needs to be accessed for processing transactions within Oracle Banking Corporate Lending Process Management.
- [API Layer](#)  
This topic describes about the API Security.
- [List of Services](#)  
This topic contains information about the list of API services.

### 1.1 API Layer

This topic describes about the API Security.

Oracle Banking Corporate Lending Process Management application provides the API Layer (also known as the Service API Layer), which is used by the external users to access the Oracle Banking Corporate Lending Process Management functionalities.

Access to the API Layer is granted only through the following methods,

- OAuth with OAM (Oracle Access Manager)
- OAuth without OAM
- Oracle Banking Routing Hub

As stated before, in case the customer does not have OAM, an enterprise API Management layer should be implemented to protect the service API(s)

#### Register OAuth Clients with API Gateway

New Oath users can be registered with Oracle Banking Microservices Architecture using the below endpoint.

```
http://<hostname>:<port>/api-gateway/createOauthUsers
```

#### Sample Headers:

Header: **appid**: SECSR001

Header: **Content-Type:** application/json

Header: **userId:** <USERID>

Header: **Authorization:** Bearer <<JWT Access Token>>

**Sample Request Body:**

```
{
  "UserList": [
    {
      "clientId": "<< clientId >>",
      "clientSecret": "<< clientSecret >>",
      "validity": "<< Validity in seconds >>"
    },
    {
      "clientId": "<< clientId >>",
      "clientSecret": "<< clientSecret >>",
      "validity": "<< Validity in seconds >>"
    }
  ]
}
```

**Modify Token Expiry of Registered OAuth Client**

Token expiry time can be updated using the below endpoint:

<http://<hostname>:<port>/api-gateway/modifyvalidity>

**Sample headers:**

Header: **appld:** SECSR001

Header: **Content-Type:** application/json

Header: **userId:** <USERID>

Header: **Authorization: Bearer** <<JWT Access Token>>

**Sample Request Body:**

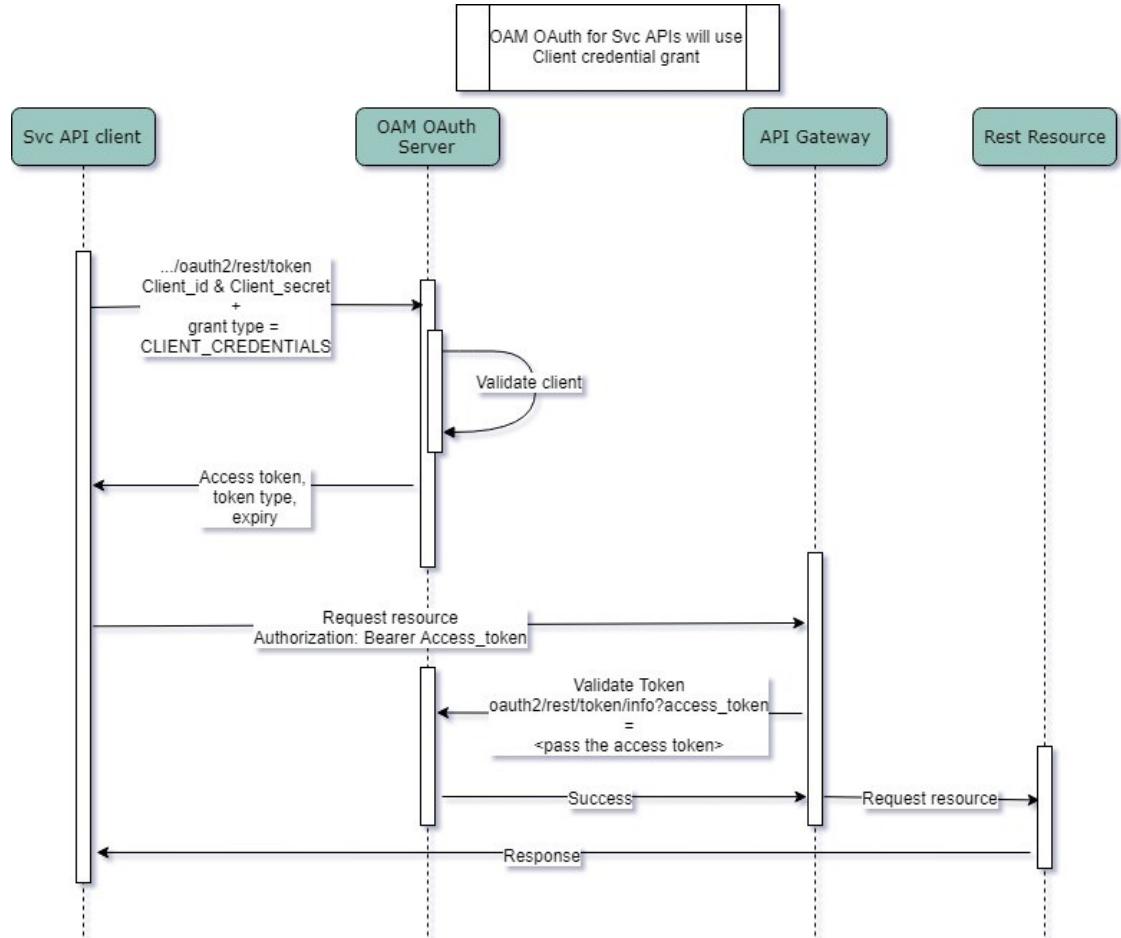
```
{"client_id":"<< clientId >>","validity":"<< Validity in seconds >>"}
```

**API Security with OAuth**

**OAuth with OAM**

The flow is depicted below

Figure 1-1 OAuth with OAM

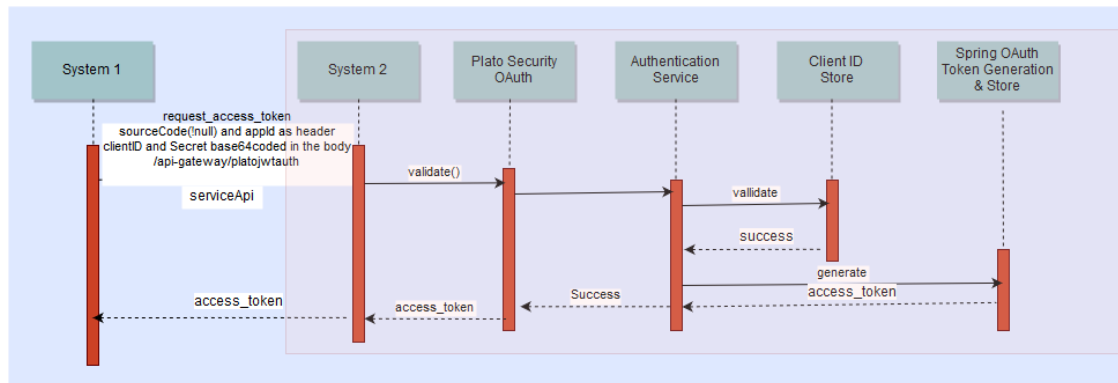


- API clients pass the client id & client secret and grant type as CLIENT CREDENTIALS. To get the access token, use the endpoint /oauth2/rest/token.
- API clients pass the access token in the authorization header as bearer token in their subsequent calls to access the Service API's.
- API Gateway validates the client access token on OAM Authorization server.
- If valid, it passes the request onto the Svc API's and gets the response.
- The client can refresh to get a new token before the current token expires. If the token expires, they can pass the client ID and client secret to get a new token.

**OAuth without OAM**

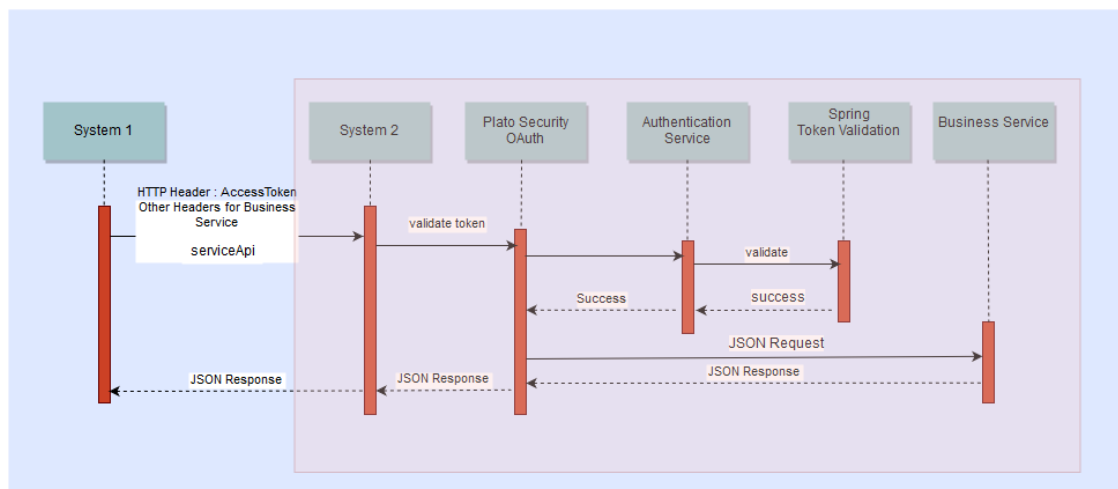
The flow for token generation is depicted below:

**Figure 1-2 OAuth without OAM - Token Generation flow**



The flow for accessing svc is depicted below:

**Figure 1-3 OAuth without OAM - Accessing svc flow**



- API clients pass the client ID & client secret in the body and other required headers. To get the access token, use the below endpoint.

`http://<<hostname>>:<<port>>/api-gateway/platojwtauth/.`

- API clients pass the access token in the authorization header as bearer token in their subsequent calls to access the Service API's.
- API Gateway validates the client access token on the Authorization server.
- If valid, it passes the request on to the Svc API's and gets the response.
- The client can refresh to get a new token before the current token expires. If the token expires, they can pass the client ID and client secret to get a new token. Additional facilities of increasing the tokens are also provided.

**Access APIs through Oracle Banking Routing Hub**

If the external services (services in bank or consulting) need to access APIs in Oracle Banking Microservices Architecture modules, the services will first have to generate an access token

using Oracle Banking Routing Hub endpoints and then use the token to authorize themselves to access the endpoints.

Refer to **Authentication** section in **Routing Hub Configuration User Guide** for the further details.

## 1.2 List of Services

This topic contains information about the list of API services.

Refer to the Rest API Documentation for the list of API services.



# Index

## A

---

API Layer, [1-1](#)

## L

---

List of Services, [1-5](#)

## S

---

Securing API Services, [1-1](#)