

Oracle® Banking Branch

API Security Guide



14.7.0.0.0
F75182-01
November 2022



Copyright © 2021, 2022, 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, 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.

Contents

1 Securing API Services

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

Preface

This guide provides security-related usage and configuration recommendations for Oracle Banking Branch. It may outline procedures required to implement or secure certain features. This guide is not for general-purpose configuration.

- [Audience](#)
- [Conventions](#)
- [Scope](#)
- [Acronyms and Abbreviations](#)
- [List of Topics](#)

Audience

This guide is primarily intended for Developers of Oracle Banking Branch and the third-party or vendor software. Some information that may be relevant to IT decision-makers and users of the application are also included.



Note:

Readers are assumed to possess the basic operating system, network, and system administration skills with an awareness of vendor/third-party software and knowledge of Oracle Banking Branch application.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	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.

Scope

The scope of this guide is as follows:

Table Scope

Scope	Description
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 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 guidelines for developers.

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this guide:

Table Acronyms and Abbreviations

Acronym/Abbreviation	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CSRF	Cross-Site Request Forgery
ECC	Elliptic Curve Cryptography
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
JPQL	Jakarta Persistence Query Language
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
OJET	Oracle JavaScript Extension Toolkit
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
SHA-1	Secure Hash Algorithm 1
SMS	Security Management System
SMTD	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Algorithm
XSS	Cross Site Scripting

List of Topics

This guide is organized into the following topics:

Table List of Topics

Topics	Description
Securing API Services	This topic provides information about securing API services.

1

Securing API Services

Different applications deployed on disparate platforms and using different infrastructure should be able to communicate and integrate seamlessly with the Oracle Banking Branch in order to exchange data.

The Oracle Banking Branch Service API Gateway will cater to these integration needs.

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

Table 1-1 Integrations

Integration	Description
Inbound Application Integration	This integration is used when any external system needs to add, modify or query information within Oracle Banking Branch.
Outbound Application Integration	This integration is used when any external system needs to be accessed for processing transactions within Oracle Banking Branch.

- [API Security](#)
The Oracle Banking Branch provides an API Layer (Service API Layer) for external users to access Oracle Banking Branch functionality.
- [List of Services](#)
This topic provides information about the List of API Services.

1.1 API Security

The Oracle Banking Branch provides an API Layer (Service API Layer) for external users to access Oracle Banking Branch functionality.

Access to this API layer is granted only via the following methods:

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



Note:

If 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**: SECSRV001
- 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: **appId**: SECSRV001
- Header: **Content-Type**: application/json
- Header: **userId**: <USERID>
- Header: **Authorization**: Bearer <<JWT Access Token>>

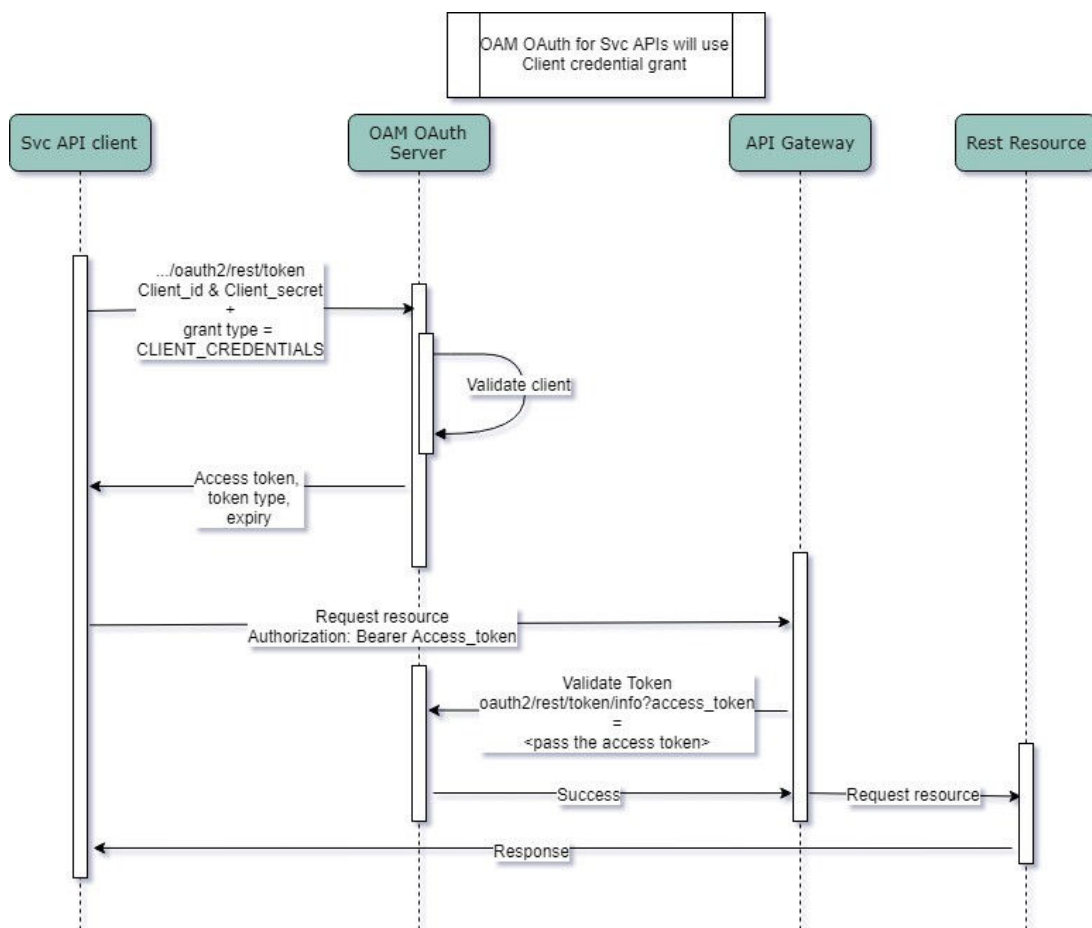
Sample Request Body

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

API Security with OAuth**OAuth with OAM (Oracle Access Manager)**

The flow is explained below.

Figure 1-1 OAuth with OAM (Oracle Access Manager)



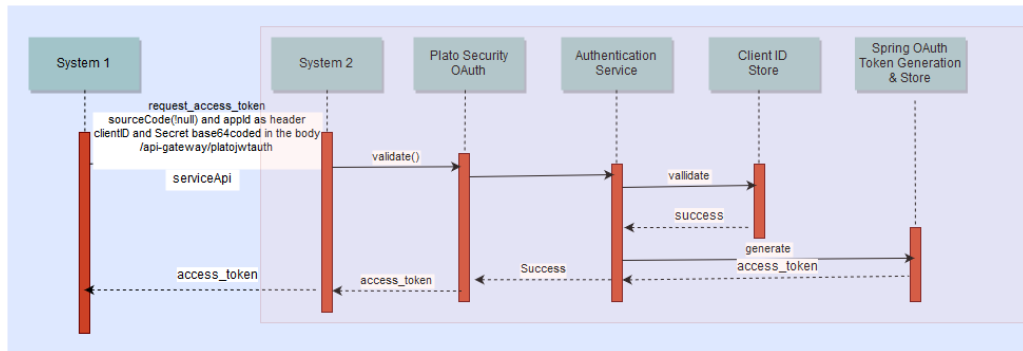
The process flow is as follows:

- API clients pass the client ID and client secret and grant type as CLIENT CREDENTIALS, to get the access token, using the below endpoint: /oauth2/rest/token.
- API Clients will pass the access token in the Authorization Header as a Bearer token in their subsequent calls to access the Service APIs.
- API Gateway validates the client access token on the OAM Authorization server.
- If valid, it passes the request on to the SVC APIs and gets the response.
- The client can choose to get a new token (refresh) before the expiry of the current token. In case the token expires, they will pass the client Id and client secret to get a new token.

OAuth without OAM

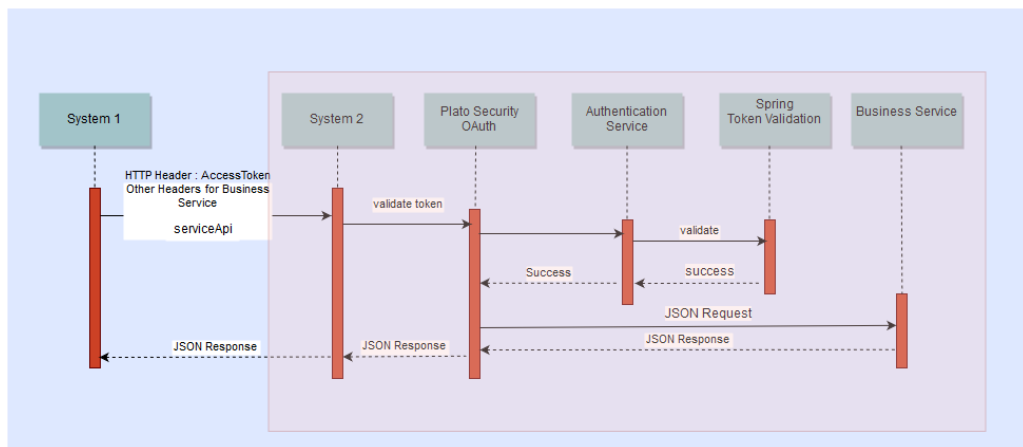
The flow for token generation is depicted below:

Figure 1-2 OAuth without OAM - Token Generation



The flow for accessing SVC is depicted below:

Figure 1-3 OAuth without OAM - Accessing SVC



The process flow is as follows:

- API clients pass the client ID and client secret in the body and other required headers, to get the access token, using the below endpoint: `http://<<hostname>>:<<port>>/api-gateway/platojwtauth/`.
- API Clients will pass the access token in the Authorization Header as a Bearer token in their subsequent calls to access the Service APIs.
- API Gateway validates the client access token on the Authorization server.
- If valid, it passes the request on to the SVC APIs and gets the response.
- The client can choose to get a new token (refresh) before the expiry of the current token. In case the token expires, they will pass the client Id and client secret to get a new token.
- Also, an additional facility for increasing the token is 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 under **Implementation** topic in Routing Hub Configuration User Guide for the further details.

1.2 List of Services

This topic provides information about the List of API Services.

Refer to the REST API Documentation for the detailed inbound APIs.