

# Oracle® Communications Billing and Revenue Management

## Security Guide



Release 15.0

F86222-01

February 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

---

Audience	viii
Documentation Accessibility	viii
Diversity and Inclusion	viii

## 1 BRM Security Overview

---

Basic Security Considerations	1-1
About Protecting Data	1-2
Recommended Deployment Configurations	1-2
Operating System Security	1-3
Oracle Database Security	1-3

## 2 Performing a Secure BRM Installation

---

Preinstallation Tasks	2-1
Installing BRM Securely	2-2
Postinstallation Tasks	2-2
Lock and Expire Default User Accounts	2-2
Change Default User Passwords	2-3
Use Strong Passwords for BRM User Schema	2-3
Enable SSL/TLS for SQL*NET	2-3
Use Secure TLS Connections	2-3
Enforce Password Management	2-4
Tighten File Permissions	2-4
Configure Maximum Number of Invalid Login Attempts	2-4
Log Customer Service Representative Activities	2-4
Integrate Paymentech	2-5

## 3 Performing a Secure Pricing Design Center Installation

---

Recommended Installation Mode	3-1
Operating System Security	3-1

Preinstallation Tasks	3-2
Installation Tasks	3-2
Postinstallation Configuration	3-2
Managing Cookies	3-3
Using Secure Cookies	3-3
Configuring the Session Timeout	3-4
Managing File Permissions	3-5
Uninstalling Pricing Design Center	3-5
About Changing Passwords in the Wallets	3-5
Implementing Pricing Design Center Security	3-6
About Authentication	3-6
About Authorization	3-6
Configuring Authentication and Authorization by Using OIM	3-6
Configuring OAM in WebLogic Server	3-7
Adding Users and Assigning Roles in OIM	3-8
Verifying OIM Configuration in WebLogic Server	3-8

## 4 Performing a Secure ECE Installation

---

About Deploying ECE into a Secure Environment	4-1
Installing ECE	4-1
About ECE Security	4-2
About Oracle Coherence Security	4-2
About Oracle Database Security	4-2
About Oracle NoSQL Database Security	4-2
About Cluster Security	4-3
About the KeyStore Files and SSL Considerations	4-3
About Trusted Host Information	4-4
About JMX Security	4-4
Postinstallation Security Tasks	4-5

## 5 Managing BRM Security

---

The Security Model	5-1
Configuring and Using Authentication	5-2
Authentication of Applications	5-2
Authentication of Accounts	5-2
Configuring and Using Access Control	5-2
Permissions	5-2
Roles	5-3
Managing CSR Passwords	5-3

Account Lockout	5-4
Automatic Logout	5-4
Access Control in BRM Web Services Manager	5-4
Configuring and Using Security Audit	5-4
Monitoring Login Attempts	5-5
Encryption	5-5
Using Oracle ZT Encryption Scheme	5-5
Securing Sensitive Customer Data	5-5
Using Credit Card Tokenization	5-5
Masking Sensitive Data in Log Files	5-6
Securing BRM Network Ports	5-6
About Managing ECE Security	5-6

## 6 Security Considerations for Developers

---

Using the BRM SDK	6-1
Security Considerations for ECE Developers	6-1

## 7 Billing Care Security

---

About Installing Billing Care Securely	7-1
Encrypting OAP Entries in Infranet.properties	7-1
Securing Web Cookies	7-1
Implementing Billing Care Security	7-2
About Identity Management Suite	7-2
About Authentication	7-3
About Authorization	7-3
About Billing Care Authorization Resources	7-4
Policies on Transaction Limits	7-17
About Auditing	7-17
Developing Secure Applications for Billing Care	7-19
Creating a Resource Type with OPSS	7-19
About REST API Authorization	7-19
About UI Authorization	7-19
Adding New Resource Types	7-19
Storing Billing Care Passwords in Oracle Wallet	7-20
Storing Configuration Entries in the Billing Care Wallet	7-20

## 8 Billing Care REST API Security

---

About Authentication and Authorization	8-1
Setting Up OAuth with Oracle Identity Cloud Service	8-1

Creating a Confidential OAuth Application for the Resource Server	8-2
Creating a Confidential OAuth Application for Your Client Application	8-3
Encoding the Client's Credentials in Base64 Format	8-3
Configuring OAuth Settings Using IDCS	8-4
Storing the Resource Server's Credentials in the Wallet	8-4
Requesting an OAuth Access Token	8-5
Setting Up OAuth with Oracle Access Management	8-5
Configuring OAuth Services	8-6
Configuring WebLogic Server to Access LDAP Server	8-8
Configuring OAuth Settings Using Oracle Access Management	8-9
Requesting an OAuth Access Token	8-9

## 9 BRM REST Services Manager Security

---

About Authentication and Authorization	9-1
Setting Up OAuth with Oracle Identity Cloud Service	9-1
Creating Confidential OAuth Applications	9-2
Assigning Users to Groups (3-Legged OAuth Only)	9-4
Generating an Authorization Code (3-Legged OAuth Only)	9-4
Encoding the Client ID and Client Secret in Base64 Format	9-5
Requesting an OAuth Access Token	9-5
Refreshing OAuth Access Tokens (3-Legged OAuth Only)	9-6
Setting Up OAuth using Oracle Access Management	9-6
Enabling OAuth Services	9-7
Creating an OAuth Identity Domain	9-7
Creating a Resource Server	9-9
Creating an OAuth Client	9-10
Using Two-Legged OAuth to Create an Access Token	9-11
Using Three-Legged OAuth to Create an Access Token	9-12
Creating Resources in the Oracle Access Management Server	9-12
Configuring the Oracle HTTP Server	9-13
Generating the OAuth Access Token	9-14
Scopes and Roles for Accessing REST Services Manager	9-14

## 10 PDC REST Services Manager Security

---

About PDC REST Services Manager Security	10-1
Setting Up OAuth for PDC REST Services Manager with Oracle Identity Cloud Service	10-2
Creating Confidential OAuth Applications for PDC REST Services Manager	10-2
Setting Up Security with Oracle Identity Cloud Service in the PDC REST Services Manager Configuration File	10-2
Requesting an OAuth Access Token from Oracle Identity Cloud Service	10-4

Setting Up OAuth for PDC REST Services Manager with Oracle Access Management	10-4
Enabling OAuth Services for PDC REST Services Manager	10-5
Creating an OAuth Identity Domain for PDC REST Services Manager	10-5
Creating a Resource Server for PDC REST Services Manager	10-6
Creating an OAuth Client for PDC REST Services Manager	10-7
Setting Up Security with Oracle Access Management in the PDC REST Services Manager Configuration File	10-8
Requesting an OAuth Access Token from Oracle Access Management	10-10
Securing Inbound Communications	10-11
Securing Outbound Requests to PDC	10-12
Encrypting Sensitive Data	10-13
PDC REST Services Manager Security Configuration Reference Information	10-13
OAuth Configuration Properties for Outbound Requests	10-13
Basic Authentication Configuration Properties for Outbound Requests	10-14
Example application.yaml Security Configuration with Oracle Identity Cloud Service	10-15
Example application.yaml Security Configuration with Oracle Access Management	10-17

## 11 Business Operations Center Security

---

About Installing Business Operations Center	11-1
About Implementing Business Operations Center Security	11-1
About Identity and Access Management	11-1
About Authentication	11-2
About Authorization	11-2
Creating Authorization Policies for Business Operations Center	11-4
Storing Business Operations Center Passwords in Oracle Wallet	11-5
Storing Configuration Entries in the Business Operations Center Wallet	11-6

## A Secure Deployment Checklist

---

BRM Checklist	A-1
PDC Checklist	A-1

# Preface

This guide provides guidelines and recommendations for managing security in Oracle Communications Billing and Revenue Management (BRM), Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE), Oracle Communications Pricing Design Center (PDC), Oracle Communications Billing Care, and Business Operations Center.

## Audience

This guide is intended for business analysts, developers, and system administrators.

## 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 customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## 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.



# 1

## BRM Security Overview

Learn about security in Oracle Communications Billing and Revenue Management (BRM).

Topics in this document:

- [Basic Security Considerations](#)
- [About Protecting Data](#)
- [Recommended Deployment Configurations](#)
- [Operating System Security](#)
- [Oracle Database Security](#)

### Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.

The system administrator is responsible for ensuring that all the installed software dependencies are kept up to date wherever possible. Oracle supports software versions where the software vendor declares backward compatibility to the version certified with BRM, and the upgrade is a minor version increment (i.e., A.B.C to A.B.D).

System administrators need to adopt this policy for software dependencies for which upgrades are generally related to security rather than focusing on functionality.

Review the latest product release documentation for any new guidelines to follow.

- **Restrict network access to critical services.** Keep the BRM Business Process, Data Management, and Data tiers behind a firewall. The firewall provides assurance that access to these systems is restricted to a known network route, which can be monitored and restricted if necessary. As an alternative, a firewall router substitutes for multiple independent firewalls.

Oracle does not recommend placing a firewall between the Data Management and Data tiers because the connection between these two tiers is persistent. As such, it is vital that a firewall not terminate the connection after a period of time.

Configure the TNS Listener Valid Node Checking feature, which restricts access based on IP address. Restricting database access by IP address can cause application client/server programs to fail for DHCP clients. To resolve this, consider using static IP addresses, a software/hardware VPN, or Windows Terminal Services or equivalent.

- **Limit privileges as much as possible.** Give users only as much access as necessary to perform their work. Review user privileges regularly to determine relevance to current work requirements.
- **Monitor system activity.** Ensuring system security requires good security protocols, proper system configuration, and system monitoring. Establish who should access which system components, and how often, and monitor those components.

See "[Configuring and Using Security Audit](#)" for more information.

- **Install software securely.** For example, use firewalls, secure protocols such as secure sockets layer (SSL), transport layer security (TLS), and secure passwords.

See "[Performing a Secure BRM Installation](#)" for more information.

- **Learn and use the BRM security features.** See "[Managing BRM Security](#)".
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible.

See *Critical Patch Updates, Security Alerts and Bulletins* on the Oracle website.

## About Protecting Data

When planning your BRM implementation, consider the following:

- **Which resources need to be protected?**

Many resources in the production environment can be protected, including information in databases accessed by BRM and the availability, performance, applications, and the integrity of the BRM architecture. Consider the resources you want to protect when deciding the level of security you must provide.

- You need to protect customer data, such as credit card numbers.
- You need to protect internal data, such as proprietary source code.
- You need to protect system components from being disabled by external attacks or intentional system overloads.

- **Who are you protecting data from?**

For all BRM implementations, resources must be protected from everyone on the Internet. But what data should also be protected from the employees on the intranet in your enterprise? What data should be accessible to a system administrator?

For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflow to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

- **What will happen if protections on strategic resources fail?**

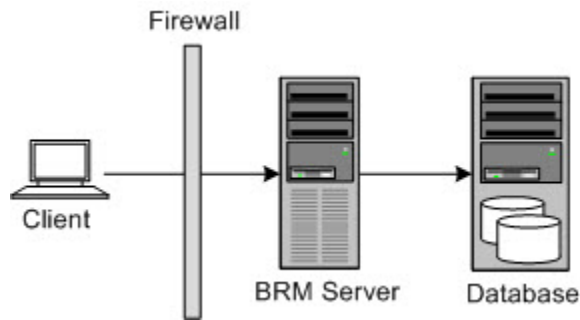
In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource helps you protect it properly.

## Recommended Deployment Configurations

This section describes recommended deployment configurations for BRM.

[Figure 1-1](#) shows the general architectural recommendation using the well-known and generally accepted trusted network.

**Figure 1-1 Traditional Trusted Network View**



Firewalls separating the protecting trusted networks provide two essential functions:

- Blocking any traffic types that are known to be illegal
- Providing intrusion containment, should successful intrusions take over processes or processors.



**Note:**

Oracle recommends not having a second firewall between the BRM server and the database server.

## Operating System Security

To secure your operating system, see the following documents:

- [Guide to the Secure Configuration of Red Hat Enterprise Linux 8](#)
- [Security Hardening Red Hat Enterprise Linux 8](#)

## Oracle Database Security

To secure your database, see [Oracle Database Security Guide](#).

# 2

## Performing a Secure BRM Installation

Learn how to install Oracle Communications Billing and Revenue Management (BRM) securely.

Topics in this document:

- [Preinstallation Tasks](#)
- [Installing BRM Securely](#)
- [Postinstallation Tasks](#)

For information about installing BRM, see "Installing BRM" in *BRM Installation Guide*.

### Preinstallation Tasks

Perform the following preinstallation tasks:

- The target operating system for BRM should have a default configuration with the following differences:
  - Do not disable X Windows. It is required for local administration and is useful for troubleshooting.
  - Do not disable SSH.
  - By default, the application uses the following ports. Ensure that iptables is configured to allow traffic to these ports and that any unused ports are closed:
    - \* 22 both directions – used for SSH access
    - \* 80 both directions – if using HTTP
    - \* 443 both directions – if using HTTPS
  - Further ports will need to be opened depending upon the ports specified for BRM during the installation process.
- Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer. See the Oracle Database documentation for advanced security configuration parameters. This is required for the BRM installer to make a secured (encrypted) database connection over the network. For more details, see *Oracle Database Advanced Security Administrator's Guide* at: <http://docs.oracle.com>
- Install only the required components. This is true of both the BRM components and any third-party software that is required, such as the operating system and the database. This can be achieved by either carrying out a custom install and only selecting the required components or by removing any extraneous components as a postinstallation step.
- All third-party software should be installed following the security advice given by the vendor. In particular, default values for data such as user names, passwords, and port numbers should be avoided if possible, by either selecting different values during the install or immediately changing the values as a postinstallation step.

## Installing BRM Securely

Follow the steps in *BRM Installation Guide* to install BRM. However, the port numbers, username, password, and database SID should be changed from the default values.

The user name selected must be for an account that is used only for BRM and does not have unnecessary privileges for any other software. In particular, the account should not have root access privileges.

## Postinstallation Tasks

Perform the following tasks after installing BRM:

- [Lock and Expire Default User Accounts](#)
- [Change Default User Passwords](#)
- [Use Strong Passwords for BRM User Schema](#)
- [Enable SSL/TLS for SQL\\*NET](#)
- [Use Secure TLS Connections](#)
- [Enforce Password Management](#)
- [Tighten File Permissions](#)
- [Configure Maximum Number of Invalid Login Attempts](#)
- [Log Customer Service Representative Activities](#)
- [Integrate Paymentech](#)

## Lock and Expire Default User Accounts

Oracle Database installs with many default (preset) database server user accounts. Upon the successful creation of a database server instance, the Database Configuration Assistant automatically locks and expires most of the default database user accounts.

### Note:

If you use Oracle Universal Installer or Database Configuration Assistant, you are prompted for new SYS and SYSTEM passwords.

After the database is installed, lock the SYS and SYSTEM accounts, and use AS SYSDBA for administrator access. Specify administrative passwords individually.

This account (AS SYSDBA) tracks the operating system user name, maintaining accountability. If you need access only for database startup and shutdown, use AS SYSOPER instead. SYSOPER has fewer administrative privileges than SYS, but enough to perform basic operations such as startup, shutdown, mount, backup, archive, and recover.

## Change Default User Passwords

Security is most easily broken when a default database server user account still has a default password even after installation. The following steps fix this:

- Change the default passwords of administrative users immediately after installing the database server.
- In any Oracle environment (production or test), assign strong, secure passwords to the SYS and SYSTEM user accounts immediately upon successful installation of the database server. Under no circumstances should the passwords for SYS and SYSTEM retain their default values. Similarly, for production environments, do not use default passwords for any administrative accounts, including SYSMAN and DBSNMP.

## Use Strong Passwords for BRM User Schema

BRM requires one or more database users and database schema to store subscriber data. You must assign unique and complex passwords for each user and grant enough database privileges to perform the required BRM operations.

## Enable SSL/TLS for SQL\*NET

Configure Oracle Database to communicate over secure sockets layer (SSL) or transport layer security (TLS) channels to secure the data transmitted between the BRM server and the Oracle database.

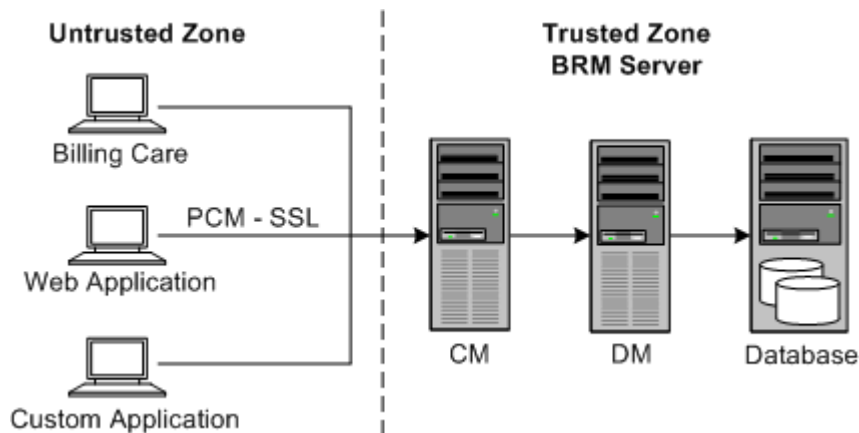
## Use Secure TLS Connections

You can configure BRM to communicate between the various components using encrypted TLS sockets by setting the **enable\_ssl** entry in the CM's **pin.conf** configuration file. When this configuration is enabled, BRM uses TLS sockets for any communication between its components, such as Oracle Data Manager (DM) (**dm\_oracle**), Payload Generator EM (also called the EAI Java Server or **eai\_js**), or Paymentech DM (**dm\_fusa**).

For example, you can configure BRM client applications or any client tier module, such as Web Services Manager or JCA Resource Adapter, to use encrypted TLS sockets to connect to the BRM server.

BRM provides sample CA certificates and trusted client certificates. You must replace the sample CA certificate with your own CA certificate or use a CA certificate from a third party.

[Figure 2-1](#) shows secure communications between BRM components using TLS.

**Figure 2-1 Secure Communications Using TLS**

See "Enabling Secure Communication between BRM Components" in *BRM System Administrator's Guide* for more information.

## Enforce Password Management

You must apply basic password management rules, such as password length, history, and complexity, to all user passwords.

You can configure complex rules by modifying the `PCM_OP_CUST_POL_VALID_PASSWD` policy opcode. See "Customizing Passwords" in *BRM Opcode Guide* for more information.

## Tighten File Permissions

You must ensure that all the installed files have their permission tightened to the maximum possible allowed that does not impact the operation of the software.

## Configure Maximum Number of Invalid Login Attempts

You must set the `MaxLoginAttempts` parameter in the `bus_params_act.xml` configuration file to a value corresponding with internal security policies for the enterprise. It is set to a default value of **5**.

The `pin_bus_params` utility is used to apply any changes to this configuration file.

See "Configuring the Maximum Number of Invalid Login Attempts" in *BRM System Administrator's Guide* for more information.

## Log Customer Service Representative Activities

Customer service representatives (CSRs) need to be given special privileges to carry out their roles. It is important to monitor their activities to ensure that they are not abusing those privileges.

CSR activities are logged as part of BRM's session event logging functionality that can be enabled by changing the `login_audit` entry in the CM's `pin.conf` configuration file to **1**. The `pin_notify` configuration file lists all those activities that will be logged.

The **pin\_load\_notify** utility is used to apply any changes to this configuration file.

See "Logging Customer Service Representative Activity Events" in *BRM System Administrator's Guide* for more information.

## Integrate Paymentech

If the BRM installation is integrated with Paymentech through the **dm\_fusa** component, Oracle recommends that the connection between BRM and Paymentech is protected using VPN. This encrypts the sensitive customer data being communicated between the two platforms and protects from any snooping attempts.



# 3

## Performing a Secure Pricing Design Center Installation

Learn about the recommended deployment configurations for your Oracle Communications Pricing Design Center (PDC) installation that enhance security.

Topics in this document:

- [Recommended Installation Mode](#)
- [Operating System Security](#)
- [Preinstallation Tasks](#)
- [Installation Tasks](#)
- [Postinstallation Configuration](#)
- [Uninstalling Pricing Design Center](#)
- [About Changing Passwords in the Wallets](#)
- [Implementing Pricing Design Center Security](#)
- [About Authentication](#)
- [About Authorization](#)
- [Configuring Authentication and Authorization by Using OIM](#)
- [Verifying OIM Configuration in WebLogic Server](#)

### Recommended Installation Mode

There are two types of installation modes: silent and secured.

The silent installation is not meant for production environments, and it should be used only in test environments for setting up quickly or backing up the properties for later use in another test environment.

The secured installation is the only recommended option for production environments.

### Operating System Security

PDC is supported on Linux (both Oracle Enterprise Linux and Red Hat Enterprise Linux) and Windows Client. For the supported versions, see "PDC Software Compatibility" in *BRM Compatibility Matrix*. See the following documents for more information about operating system security:

- *Guide to the Secure Configuration of Red Hat Enterprise Linux*
- *Hardening Tips for the Red Hat Enterprise Linux*

## Preinstallation Tasks

Perform the following preinstallation tasks:

- Enable SSL for the target WebLogic server domain, configure the server KeyStore certificate, and then get the client KeyStore trusted certificate. This client KeyStore file should be used in installer to make secured connection during installation.
- If SSL is enabled, ensure that the KeyStore file is created in a secure drive and access is strictly limited to the user account.
- Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer. See the Oracle Database documentation for advanced security configuration parameters. This is required for a PDC installer to make a secured (encrypted) database connection over the network. For more details, see the *Oracle Database Advanced Security Administrator's Guide* documentation.
- Verify that you have the latest supported version of Oracle JDK installed.

## Installation Tasks

Perform the following installation tasks:

- During PDC installation, select SSL mode and provide the client KeyStore certificate for connecting to a WebLogic server over SSL.
- The following logs are generated after the PDC installation.

Location: *Oracle Inventory/logs/*

```
-rw-r----- 1 user1 eng 480058 Aug 15 09:25 installActions2018-08-15_08-06-57AM.log
-rw-r----- 1 user1 eng 2384 Aug 15 10:33 dbScripts2018-08-15_10-32-00AM.log
-rw-r----- 1 user1 eng 124268 Aug 15 10:33 oraInstall2018-08-15_10-27-07AM.err
```

The **installActionsxxxxx.log** and **oraInstallxxxx.err** files will have details in clear text format that were entered in the PDC installation wizard. Passwords that were entered in the installation wizard are not logged in any of the PDC installation log files. Delete these installation log files if you do not need them for future reference. If you do require them, protect them appropriately. These log files are created with the file level permission 640 (owner can read/write, group members can read, others cannot do anything) by default.

## Postinstallation Configuration

- PDC user permissions depend on the group the user belongs to. The following three groups are created in the WebLogic server during PDC installation:
  - Pricing Design Admin
  - Pricing Reviewer
  - Pricing Analyst

The users belonging to Pricing Design Admin group have read and write access and can perform any kind of operation from PDC User Interface.

The users belonging to Pricing Analyst group have read and write access to all pricing components and read only access to setup components.

The users belonging to Pricing Reviewer group have read only access to the pricing and setup components.

None of the users by default is authorized to access PDC. The WebLogic server administrator must create an account for each intended user by creating the user in the WebLogic Server Administration Console and adding the user to one of the above groups depending on the user role.

- Do not use your browser's remember password feature for the WebLogic Server Administrator Console URL. Always enter the WebLogic server user name and password manually in the login page, as a precaution.

## Managing Cookies

Oracle recommends deploying PDC only on SSL, which encrypts sensitive data, thus eliminating problems like session stealing.

## Using Secure Cookies

A common Web security problem is session stealing. This happens when an attacker manages to get a copy of your session cookie, generally while the cookie is being transmitted over the network. This can only happen when the data is being sent in clear-text; that is, the cookie is not encrypted.

WebLogic Server allows a user to securely access HTTPS resources in a session that was initiated using HTTP, without loss of session data.

To use secure cookies:

1. Open the **config.xml** file.
2. Add **AuthCookieEnabled="true"** to the WebServer element.

```
<WebServer Name="myserver" AuthCookieEnabled="true"/>
```

You can also set this entry using the WebLogic Server Administration Console:

1. Log in to the Oracle WebLogic Server Administration Console.  
The Home page appears.
2. In the **Domain Configurations** section, under **Domain**, click **Domain**.  
The Settings for *Domain\_Name* page appears.
3. Click the **Web Applications** tab.
4. Verify that the **Auth Cookie Enabled** check box is selected.
5. Click **Save**.

By default, the **Auth Cookie Enabled** check box is selected, but it is not present in the **config.xml** file. If you deselect it, the **<AuthCookieEnabled>** element is added to the **config.xml** file.

Setting **AuthCookieEnabled** to **true**, which is the default setting, causes the WebLogic Server instance to send a new secure cookie, **\_WL\_AUTHCOOKIE\_JSESSIONID**, to the browser when authenticating via an HTTPS connection. After the secure cookie is set, the

session is allowed to access other security-constrained HTTPS resources only if the cookie is sent from the browser.

Oracle recommends keeping cookies settings enabled in the browser. Disabling cookies in the browser disables several features, such as Help.

## Configuring the Session Timeout

The default session timeout in PDC is 10 minutes. Your WebLogic Server administrator can change this value after deployment by doing the following:

1. Log in to WebLogic Server Administration Console.
2. In the **Domain Structure** section, click **Deployments**.
3. Click on the application **PricingDesignCenter** deployed as type Enterprise Application.  
The deployment settings for **PricingDesignCenter** appears.
4. Click the **Configuration** tab.
5. Set **Session Timeout (in seconds)** to the new timeout value, in seconds.
6. Click the **Overview** tab.
7. In the Modules and Components table, click **PricingDesignCenter**.
8. Click the **Configuration** tab.
9. Set **Session Timeout (in seconds)** to the same timeout value, in seconds, set in step 5.
10. Click **Save**.

If no deployment plan is created, WebLogic Server creates one with above changes and prompts you to save deployment plan. Provide the name and path for the deployment plan and click **OK**.

11. In the **Domain Structure** section, click **Deployments**.
12. Select the application **PricingDesignCenter** deployed as Enterprise Application.  
The **Update** button is enabled.
13. Click **Update**.
14. Select **Update this application in place with new deployment plan changes**.
15. Set **Deployment plan path** to the deployment plan created in step 10. Use **Change Path** button to browse to the file.
16. Click **Next**.
17. Click **Finish**.
18. Restart WebLogic Server.
19. Verify your changes by doing the following:
  - a. Log in to WebLogic Server Administration Console.
  - b. In the **Domain Structure** section, click **Deployments**.
  - c. Click on the application **PricingDesignCenter** deployed as type Enterprise Application.  
The deployment settings for **PricingDesignCenter** appears.

- d. Click the **Configuration** tab.
- e. Verify that **Session Timeout (in seconds)** is set to the value you have provided.

For more information about deployment plans, including an example of using one while updating session timeout, see "[Configuring Applications for Production Deployment](#)" in *Oracle Fusion Middleware Deploying Applications to Oracle WebLogic Server*.

## Managing File Permissions

- Following is the default permissions set for the installed files:
  - rw----- 600 (for all non executable files)
  - rwx----- 700 (for all executable files)

Permissions are set to the lowest possible level, and the WebLogic Server administrator can add or revoke permissions. Oracle recommends keeping the permissions as restrictive as possible, as per your business needs.

- The WebLogic configuration (JMS, JDBC, etc) file, **config.xml**, in the domain's configuration directory should be protected with proper permissions.
- Output files generated by the export utility should be stored in a protected directory because it may contain sensitive pricing information.

## Uninstalling Pricing Design Center

The following files remain in the system after uninstalling PDC:

- Install logs:

Location: *Oracle Inventory/logs/*

```
-rw-r----- 1 user1 eng 480058 Aug 15 09:25 installActions2018-08-15_08-06-57AM.log
-rw-r----- 1 user1 eng      0 Aug 15 10:27 oraInstall2018-08-15_10-27-07AM.out
-rw-r----- 1 user1 eng  2384 Aug 15 10:33 dbScripts2018-08-15_10-32-00AM.log
-rw-r----- 1 user1 eng 124268 Aug 15 10:33 oraInstall2018-08-15_10-27-07AM.err
```

- **PDC\_home\oui\data.properties**: This file is used to auto-populate the data during re-installs.

Delete these files manually if you do not need them or protect them appropriately if they are required for further references.

These files are created with the file permission 640 (owner can read/write, group members can read, others cannot do anything) by default.

## About Changing Passwords in the Wallets

PDC stores the passwords for the WebLogic Server domain, PDC user, cross-reference database, and Oracle Communications Billing and Revenue Management (BRM) database in PDC and BRM Integration Pack wallets.

To change the password in the wallets, you must encrypt the new password manually and update the entry in the appropriate wallet. See "Changing Passwords in the Wallet" in *BRM System Administrator's Guide* for more information.

# Implementing Pricing Design Center Security

This section describes how to implement the security capabilities in PDC by using Oracle Identity Management (IDM).

PDC uses IDM for authenticating and authorizing PDC users. Each instance of PDC requires an appropriately configured instance of IDM to enable these functions.

For information about installing PDC, see *PDC Installation Guide*.



## Note:

If you have configured IDM, you must authorize PDC users by using IDM only.

## About Authentication

Within IDM, Oracle Identity Manager (OIM) provides a mechanism for managing user password policies. You must configure OIM to authenticate and authorize PDC users. See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

## About Authorization

Authorization refers to granting appropriate privileges to users and denying access to other functionality based on their job functions. The users with the following roles can access PDC by using IDM:

- **Pricing Design Admin:** Can import and export all pricing and setup components in PDC.
- **Pricing Analyst:** Can import only pricing components. However, the user with this role can export pricing and setup components.
- **Pricing Reviewer:** Can only export all pricing and setup components.
- **Migration Admin:** Can migrate pricing data from the BRM database to the PDC database.
- **JDGroup:** Can manually trigger job dispatcher to put transformation jobs in the work item queue.

## Configuring Authentication and Authorization by Using OIM

OIM enables enterprises to manage the entire user life cycle across all enterprise resources within and beyond a firewall.

To configure OIM to authenticate and authorize users in PDC:

1. Configure OAM in WebLogic Server. See "[Configuring OAM in WebLogic Server](#)".
2. Add users and assign roles in OIM. See "[Adding Users and Assigning Roles in OIM](#)".

## Configuring OAM in WebLogic Server

To configure Oracle Access Manager (OAM) in WebLogic server:

1. Log in to the Oracle WebLogic Server Administration Console.  
The Home page appears.
2. On the left panel, under the **Change Center**, click **Lock and Edit**.
3. On the left panel, under the **Domain Structure**, click the **Security Realms** link.  
The Summary of Security Realms page appears.
4. Under the **Name**, click **myrealm**.  
The Settings for myrealm page appears.
5. Click **Providers** and under **Authentications providers**, click **New**.  
The Create a New Authentication Provider page appears.
6. Enter the name as **OAM Identity Asserter**.
7. Select the type as **OAMIdentityAsserter**.
8. Click **OK**.  
The Settings page appears.
9. Repeat the steps 3 and 4 to navigate to the Settings for myrealm page.
10. Click the **OAMIdentityAsserter** link.
11. In the **Control Flag** row, select **REQUIRED**.
12. Click **Save**.  
The Settings updated successfully message appears.
13. Click **New**.  
The Create a New Authentication Provider page appears.
14. In the **Name** field, enter **OID Authenticator**.
15. In the **Type** field, enter **IPlanetAuthenticator**.
16. Click **OK**.  
The Settings for OID Authenticator page appears.
17. In the **Control Flag** row, select **SUFFICIENT**.
18. Click **Provider Specific** and provide Oracle Unified Directory (OID) connection details.
19. Click **Save**.
20. Click **Reorder**.  
The Reorder Authentication Providers page appears.  
Reorder the authentication provider names in the following order:
  - OAMIdentityAsserter
  - OID Authenticator
  - DefaultAuthenticator

- DefaultIdentityAsserter
21. Click **OK**.
  22. Click the default authenticator and then modify the **Control Flag** of DefaultAuthenticator to **SUFFICIENT** and click **Save**.
  23. In the **Change Center**, click **Activate Changes**.
  24. Restart the WebLogic server.

## Adding Users and Assigning Roles in OIM

To add users and assign roles in OIM to access PDC:

1. Log in to Oracle Identity Self Service.  
The Oracle Identity Self Service home page appears.
2. Create new users (if required) by performing the following steps:
  - a. Click **Manage**.
  - b. Click **Users**.  
The Users page appears.
  - c. Click **+ Create**.  
The Create Users page appears.
  - d. Enter the required information.  
For more information on creating users, see the discussion about creating and managing users in the Oracle Identity Manager Administrative and User Console Guide.
3. Select a user.
4. Click **+ Request Roles**.
5. In the **Search** field, enter the name of the role and click **Search**.  
See "[About Authentication](#)" for the supported roles.  
The search results appear.
6. Select a role from the list under Categories.
7. Click **+ Add to Cart**.
8. Click **Next** and click **Submit**.  
Now, the users can access PDC.

## Verifying OIM Configuration in WebLogic Server

To verify the OIM configuration in the WebLogic server:

1. Log in to the Oracle WebLogic Server Administration Console.  
The Home page appears.
2. On the left panel, under the **Domain Structure**, click the **Security Realms** link.  
The Summary of Security Realms page appears.



3. Under **Name**, click **myrealm**.  
The Settings for myrealm page appears.
4. Click **Users and Groups** tab.  
The list of users created in OIM appears.

# 4

## Performing a Secure ECE Installation

Learn how to create a secure Oracle Communications Elastic Charging Engine (ECE) installation.

Topics in this document:

- [About Deploying ECE into a Secure Environment](#)
- [Installing ECE](#)
- [About ECE Security](#)
- [About Oracle Coherence Security](#)
- [About Oracle Database Security](#)
- [About Oracle NoSQL Database Security](#)
- [About Cluster Security](#)
- [About the KeyStore Files and SSL Considerations](#)
- [About Trusted Host Information](#)
- [About JMX Security](#)
- [Postinstallation Security Tasks](#)

### About Deploying ECE into a Secure Environment

Deploy ECE into a secure environment. For example, ensure that:

- ECE is deployed in a closed networked environment in which any public access to the network is denied.
- All ECE hosts are connected to a single switch or in a parallel switch configuration.
- No external processes are run on the hosts running ECE and its constituents.
- Access to the ECE infrastructure is restricted.

You can further harden ECE security by following the instructions in this chapter.

### Installing ECE

By default, ECE is installed in a secure mode. ECE uses security measures such as cluster security and host authorization.

When you install ECE, you will be prompted to select your preferred security configuration, such as whether to enable secure socket layer (SSL) configuration. Based on the security configuration you select in the installer, ECE sets parameters in the relevant Oracle Coherence and ECE configuration files for enabling the following security levels:

- **JMX security.** Clients require a JMX user name and password to connect to ECE JMX Management servers. For example, Elastic Charging Controller (ECC) can use a JMX user name and password to be authenticated to log in to the cluster.

- **Authorized host list.** A process that joins the Coherence cluster will have access to ECE services only if it is running on a host defined in the authorized host list.
- **Coherence node authentication.** ECE nodes are required to authenticate themselves when trying to join the Coherence cluster. The node credentials are stored in a key store file that must be deployed on the ECE nodes.
- **SSL encryption** (intra-cluster communication). Communication across ECE nodes in the Coherence cluster will be encrypted.

## About ECE Security

Access to ECE files is controlled by creating user accounts and groups and granting specific permissions. The file permissions are granted using Linux commands in a Linux shell. After you have created user accounts and groups and set permissions, users can use ECC to manage ECE files. ECC requires that you set up a password-less SSH. You use the ECE user, a Linux account, for setting up password-less SSH. See "Setting Up and Managing Elastic Charging Engine Security" in *BRM System Administrator's Guide*.

## About Oracle Coherence Security

To restrict access to the ECE Coherence cluster, set up an authorized hosts list. You can optionally enable SSL for intra-cluster communication, in which case you must also enable Well Known Addresses (WKA). See "Setting Up Cluster Security" in *BRM System Administrator's Guide*.

## About Oracle Database Security

If you are using Oracle Database for data persistence, configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer. See the Oracle Database documentation for advanced security configuration parameters. This is required for the ECE installer to make a secured (encrypted) database connection over the network. For more details, see *Oracle Database Advanced Security Administrator's Guide*.

## About Oracle NoSQL Database Security

If you are using Oracle NoSQL Database for data persistence, install Oracle NoSQL Database in a secure location where physical and network access to the store is restricted to trusted users. For this reason, Oracle NoSQL Database's security model is designed to prevent accidental access to the data. It is not designed to prevent malicious access or denial-of-service attacks.

You can access the KVStore and its data in two different ways. Access to data is possible through the Java API. Administrative access is performed by using a command line interface or a browser-based graphical user interface. System administrators use these interfaces to perform the few administrative actions that are required by Oracle NoSQL Database. You can also monitor the store using these interfaces.

## About Cluster Security

ECE uses a file based credentials store or a KeyStore to keep node credentials that are required to join the cluster and that are used for enabling encryption of cluster communication. The KeyStore is in the `ECE_home/occeserver/config/server.jks` file. Though the ECE installer creates a `server.jks` file, you can create your own as well if required. If you create a JKS file of your own, make sure it has very limited permissions so that unauthorized access is not allowed.

ECE uses Oracle wallet to store passwords required to connect to boundary systems such as Oracle Communications Billing and Revenue Management (BRM) and Oracle Communications Pricing Design Center (PDC).

When you install ECE, you enter the following information:

- The account alias for Coherence cluster security
- The key password for Coherence cluster security (the password for the alias)
- The key password for the boundary system alias
- The password for accessing the KeyStore (the certificate store password)
- DName details

The DName value specifies the authorization of users for what they can do regarding cluster security.

The DName is used for authorization as defined in `ECE_home/occeserver/config/permissions.xml`.

See *ECE Installation Guide* for more information.

## About the KeyStore Files and SSL Considerations

ECE maintains the `server.jks` KeyStore file, which stores credentials for cluster node authentication. The file is also used for encrypting intra-cluster communication over SSL.

KeyStore passwords for SSL are stored by default in the `ECE_home/occeserver/config/charging-coherence-override-secure-prod.xml` file. These can, however, be overridden by defining their respective system properties in the `ECE_home/occeserver/config/defaultTuningProfile.properties` file.



### Note:

Oracle strongly recommends not overriding the default `ECE_home/occeserver/config/charging-coherence-override-secure-prod.xml` file.

### Installation Settings when SSL Is Enabled

When you select the SSL options during installation, the following are set:

- In `ECE_home/occeserver/config/ece.properties`:
  - `tangosol.coherence.override=charging-cache-config-secure-prod.xml`

- The WKA list in the **charging-cache-config-secure-prod.xml** file  
This should contain the WKA host list provided during the installation.
- In *ECE\_home/occeserver/config/charging-coherence-override-secure-prod.xml*:
  - `-Dtangosol.coherence.ssl.keypassword=keypassword`
  - `-Dtangosol.coherence.ssl.storepassword=storepassword`where *keypassword* and *storepassword* are the key and store passwords given during installation.

## About Trusted Host Information

The ECE caches contain your subscribers' data. To restrict access to this data, you must specify the machines or processes that you trust and allow to be part of the cluster.

Obtain the IP addresses or host names of all machines or processes that are allowed to access the cluster. Trusted hosts include all of the server machines across which the Coherence cluster is deployed and any other machine that is to be part of the cluster. Include the server machine that runs the Elastic Charging Controller (ECC), and if you use Oracle Enterprise Manager, include the JMX client host running it.

See "Installing Elastic Charging Engine" in *ECE Installation Guide* for more information.

## About JMX Security

JMX security is based on standard Java guidelines, as discussed in "[Security](#)" in *Java Platform, Standard Edition Java Management Extensions Guide*.

For ECE, JMX can be secured by setting the following system parameters:

- In *ECE\_home/occeserver/config/ece.properties*:

```
com.sun.management.jmxremote.authenticate=true
```
- In *ECE\_home/occeserver/config/defaultTuningProfile.properties*:

```
-Dcom.sun.management.jmxremote.password.file=./config/  
jmxremote.password
```

The file permission of **jmxremote.password** must be set to **400**; otherwise, Elastic Charging Server nodes will not start up.

ECE bundles a **jmxremote.password** password file in the *ECE\_home/occeserver/config* directory and contains two default accounts for JMX credentials as defined in *JRE\_home/lib/management/jmxremote.password.template*:

- `monitorRole` with read-only permissions
- `controlRole` with read and write permissions

Passwords for these two accounts can be set in the **jmxremote.password** file bundled in *ECE\_home/occeserver/config*. If more accounts need to be added, add those accounts in the **jmxremote.password** file as well. See "[Monitoring and](#)

"[Management Using JMX Technology](#)" in *Java Platform, Standard Edition Monitoring and Management Guide* for more information about using the `jmxremote.password` file.

Because the JMX passwords are human readable in `jmxremote.password`, the file permission must be set to **400**.

 **Note:**

The `jmxremote.password` file is used for more than JMX. This file is also used for storing passwords required to authenticate cluster nodes and required to encrypt and decrypt passwords for JMS notification services. See "About Managing External Application Passwords" in *BRM System Administrator's Guide* for more information.

All of the Elastic Charging Controller (ECC) shell commands are JMX aware: if JMX is made secure, you must provide a user name and password with the command that starts ECE services.

If JMX is secured, commands like **start server** or starting a single node, such as **start ecs1**, **start configLoader**, and so on must provide a user name and password. For example:

```
start server username=controlRole password=password_as_defined
```

In secured mode, Oracle recommends using the ECC shell in an interactive mode (all commands are run within the shell and not as arguments to the ECC script). The ECC command sets the file permissions of the file that saves the history of the commands that have been run to **600**. This protects unauthorized access to old commands to retrieve passwords typed in the command line.

In applications such as JConsole, jVisualVM, or other JMX client applications, you must specify the user name and password when a connection is made.

## Postinstallation Security Tasks

For the most part, the Oracle Universal Installer requests you to enter security information that takes care of postinstallation steps typically required for security.

After installation, verify the following in the `ECE_home/occeserver/config/permissions.xml` file:

- The **principal** section has the same DName information as was defined during the installation process for creating the `server.jks` file.
- A complete access to all resources is allowed for an authenticated user.
- If the `secure.access.name` system property is set, the `tangosol.coherence.security` system property must be set to **true**. If the `tangosol.coherence.security` system property is set to **false**, the `secure.access.name` system property should not be set.

# 5

## Managing BRM Security

Learn how to manage security in Oracle Communications Billing and Revenue Management (BRM).

Topics in this document:

- [The Security Model](#)
- [Configuring and Using Authentication](#)
- [Configuring and Using Access Control](#)
- [Configuring and Using Security Audit](#)
- [Monitoring Login Attempts](#)
- [Encryption](#)
- [Securing Sensitive Customer Data](#)
- [Using Credit Card Tokenization](#)
- [Masking Sensitive Data in Log Files](#)
- [Securing BRM Network Ports](#)
- [About Managing ECE Security](#)

### The Security Model

BRM security requirements arise from the need to protect data: first, from accidental loss and corruption, and second, from deliberate unauthorized attempts to access or alter that data. Secondary concerns include protecting against undue delays in accessing or using data or even against interference to the point of denial of service. The global costs of such security breaches run up to billions of dollars annually, and the cost to individual companies can be severe, sometimes catastrophic.

The critical security features that provide these protections are:

- **Authentication:** Ensures that only authorized individuals get access to the system and data.
- **Authorization:** Ensures access control to system privileges and data. Authorization builds on authentication to ensure that individuals get only appropriate access.
- **Audit:** Allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control.
- **Encryption:** Ensures that data cannot be read without being adequately decrypted.

BRM enables TLS by default to secure communication between applications. See "Enabling Secure Communication between BRM Components" in *BRM System Administrator's Guide* for more information.

## Configuring and Using Authentication

BRM requires two levels of authentication within its operation:

- [Authentication of Applications](#)
- [Authentication of Accounts](#)

Both levels of authentication use Oracle Wallet.

By default, the BRM installer stores configuration entries, including sensitive information (such as TLS certificates and database and account passwords), in the Oracle wallet. BRM applications retrieve the data from the Oracle wallet unless the configuration entries are also stored in the **Infranet.properties** and **pin.conf** configuration files. The entries in the configuration files take precedence.

### Authentication of Applications

Each component in the application tier must authenticate itself against an account to be allowed to send requests to the BRM server. The user name is stored in the application's configuration file. By default, the password is stored in the Oracle wallet, but the application may be configured so that the password is encrypted using AES and stored in the application's configuration file.

Application account information is stored in the BRM database. All passwords are hashed and encrypted before being stored in the database. When the application connects, the password is hashed and the hash is compared with the hashed password in the database.

### Authentication of Accounts

Users requesting permission to carry out a transaction must be authenticated against the account information stored in the BRM database. All passwords are hashed and encrypted before being stored in the database. The user name and password are typed in by the user, and then the password is hashed and the hash is compared with the hashed password in the database.

## Configuring and Using Access Control

Configure and use access control in BRM.

### Permissions

Permissions determine which tasks a user can perform with BRM applications.

It is possible to restrict activities in applications, such as Customer Center and Pricing Center, by assigning CSRs to a role and setting permissions for that role. For example, it is possible to specify which CSRs can change a password, apply credits, and give refunds. See "Setting Up Permissions in BRM Applications" in *BRM System Administrator's Guide* for more information.

In most cases, only a person with root access, such as a system administrator, is granted permission to change CSR permissions.



See "Managing ECE Permissions" in *BRM System Administrator's Guide* for more information.

## Roles

A set of permissions defines a role. A role represents a set of actions that a person holding a particular job or position can perform. Roles are used to configure permissions for a group of CSRs based on the tasks they need to perform. For example, it is possible to create different types of CSRs and assign them to different kinds of roles:

- *Manager CSRs* can create new roles, assign CSRs to roles, change permission settings, change credit limits, give refunds, and change account status. A manager can also validate the work that junior CSRs perform, for example, by making sure that new accounts are created correctly and have all the necessary information.
- *Junior CSRs* can check customer account balances, check and change billing information, and answer common customer questions.

For example, CSRs A and B can be assigned to the role Manager, and CSRs C and D can be assigned to the role Lead-CSR, where:

- CSRs A and B have read-write permissions for customer credit card information.
- CSRs C and D have read-only permissions for customer credit card information.

It is also possible to create roles with higher levels of permissions. For example, you can create roles that include permissions to create and manage roles using Permissioning Center.

Roles can also be set up to access one or more client applications. In addition, a CSR can be assigned to multiple roles. For example, a CSR can be assigned to a Manager role in Permissioning Center and to a Junior-CSR role in Pricing Center.

Roles can be hierarchical, by creating child roles and associating them with a parent role. At each level above the bottom of the hierarchy, the child roles can also be parent roles. A child role inherits all permission settings that are associated with its parent role.

See "About Managing Roles" in *BRM System Administrator's Guide* for more information.

## Managing CSR Passwords

To improve security features and provide access to BRM client applications, the following password policies are included in Permissioning Center:

- **Ability to set password expiry limits:** The duration of time that a password is valid until the system prevents a user from logging in or forces the password to be changed.
- **Ability to define temporary passwords:** The ability to force CSRs to change their passwords after accessing the application the first time or after a new CSR account has been set up by an administrator.
- **Password content validation:** The ability to validate the contents of the password to make sure that certain characters are or are not included, such as numbers.

See "Managing CSR Passwords" in *BRM System Administrator's Guide* for more information.

## Account Lockout

Users are locked out of the system after a specified number of invalid login attempts. See "Configuring the Maximum Number of Invalid Login Attempts" in *BRM System Administrator's Guide* for instructions for changing the default number of attempts allowed.

Once users are locked out of the system, manual intervention is required to reenable the accounts. See "Unlocking a Locked CSR Account" in *BRM System Administrator's Guide* for instructions for unlocking the accounts.

## Automatic Logout

BRM provides the functionality to force a user to reauthenticate after a given amount of idle time. However, if the password is present in the configuration file, the authentication is automated. This facility should not be used to allow automated reauthentication of CSR accounts.

You can configure the interval for the session to time out by setting the `cm_timeout` parameter. See "Setting the CM Time Interval between Opcode Requests" in *BRM System Administrator's Guide* for detailed instructions.

## Access Control in BRM Web Services Manager

BRM Web Services Manager enables BRM opcodes to be exposed through Web services.

You can use access control capabilities to restrict Web services to certain user roles. Multiple roles can be created, each with a different set of privileges. You define access restrictions for Web services in security policies in WebLogic Server. See "Configuring WebLogic Security Policy on BRM Web Services for JAX-WS in WebLogic Server" in *BRM Web Services Manager* for more information.

Web Services Manager uses the OAuth 2.0 protocol to authenticate a client application's identity and to authorize the client application to access BRM Web services. See "Securing Web Services Manager with OAuth2" in *BRM Web Services Manager* for more information.

## Configuring and Using Security Audit

BRM provides support for auditing any object in the BRM database so that a record is kept of every version of the object for future reference. This can be used to track changes to customer profiles, customer payment information, and so on. An audit trail can also be used to track internal changes, such as changes to your pricing components.

Specific fields within objects can be requested to be audited. However, because there is a performance overhead, auditing should be switched on only for those fields where there is felt to be a security risk.

## Monitoring Login Attempts

You can see both successful and unsuccessful login attempts in the Connection Manager (CM) log file, which is located in the *BRM\_home/sys/cm* directory.

Search for the text "login attempt" in the log file. The PIN\_FLD\_RESULT field in the result from the PCM\_OP\_ACT\_FIND\_VERIFY opcode indicates whether the login attempt was successful.

## Encryption

By default, BRM encrypts the passwords stored in the BRM database.

However, this can be extended to encrypt fields that contain sensitive customer information, such as credit card numbers, to guarantee privacy and prevent unauthorized use. The fields to be encrypted must be in string format. You set up encryption with the BRM Storable Class Editor, which will add a flag attribute in the meta-data defining the field in the BRM data dictionary (PIN\_FLD\_ENCRYPTABLE).

BRM encrypts the fields marked for encryption when storing them in the database and automatically decrypts the fields when retrieving them from the database.

See "About Encrypting Data" in *BRM System Administrator's Guide* for more information.

## Using Oracle ZT Encryption Scheme

Each instance of BRM has a unique root encryption key. This root key is used for all encryption/decryption processes in BRM. You can use an instance-specific root encryption key to assign different keys for development, test, pre-production, and production instances of BRM.

When different root keys are used for each instance, the sensitive subscriber data and other credentials, such as subscriber passwords, cannot be copied from one instance to another and decrypted in the other system.

The encryption scheme adds a random initial vector for each plain block of text to be encrypted. This prevents pattern-based attacks.

See "Generating a Root Encryption Key" in *BRM Developer's Guide* for more information.

## Securing Sensitive Customer Data

Protect subscriber data by masking values contained in system responses to clients and logging.

See "Masking Sensitive Customer Data" in *BRM Managing Customers*.

## Using Credit Card Tokenization

Credit card tokenization is a secure method of storing credit and debit card data. It replaces the credit and debit card numbers with random identifiers, referred to as tokens. You can use tokens for any BRM-initiated payments instead of the actual card numbers. The actual card numbers and their mapping to the tokens are stored securely in Paymentech. Tokens are

valid only between the merchant system and the credit card processor. You can use tokens to transmit safely without the risk of exposing credit or debit card data.

See "Masking Credit Card Numbers by Using Tokens" in *BRM Configuring and Collecting Payments* for more information.

You can migrate previously stored credit card numbers to tokens by using the provided migration application. See "Replacing Credit Card Numbers with Tokens" in *BRM Configuring and Collecting Payments* for more information.

You can use tokens generated outside BRM for credit and debit cards by sending the token into the application in the PCM\_OP\_CUST\_COMMIT\_CUSTOMER opcode. See *BRM Opcode Flist Reference* for more information about PCM\_OP\_CUST\_COMMIT\_CUSTOMER.

You can prevent users from entering any credit card information in Billing Care by removing the **creditCard** entry from the **paymentTypes** key in the Billing Care **CustomConfigurations.xml** file. See "Editing the Billing Care Configuration File" in *Billing Care SDK Guide* for more information about the **CustomConfigurations.xml** file.

## Masking Sensitive Data in Log Files

BRM comes preconfigured to store sensitive data in an encrypted format. However, because encryption and decryption are done in the Data Manager to ensure that the business logic has access to the real value, these fields should also be marked as masked so that their values do not appear in any of the BRM log files.

See "Defining Masked Fields" in *BRM Developer's Guide* for more information.

## Securing BRM Network Ports

The BRM PCM protocol cannot enforce access control to any of the command line applications or other custom C or Java applications. Therefore, operating system and network security measures must be used to secure access to the BRM network ports:

- Enable TLS to secure the BRM PCM communications. See "Enabling SSL/TLS for C and C++ PCM Clients" and "Enabling SSL/TLS for Java PCM Clients", both in *BRM System Administrator's Guide*, for more information.
- The Connection Manager (CM) port must be blocked to prevent any connections from any desktops that do not have a business justification to run any BRM client application.
- BRM DM port: The BRM DM port must be blocked to prevent any connections other than from servers that are running an instance of the CM that is to be allowed access to the DM.

## About Managing ECE Security

To manage ECE security, you perform the following tasks:

- Set up user accounts and user groups, and grant permissions. After creating user groups and setting permissions, users can log in to the system, use ECE, and manage the ECE cluster.

You can assign permissions for users who run and manage ECE processes, manage rated event files, and manage the ECE file systems. Restrict permissions as much as possible. You can create either a single administrative user with all permissions who runs ECE core processes and manages the rated event files and other directories, or create multiple users with specific permissions to carry out these tasks.

See "Configuring Specific File Permissions" in *BRM System Administrator's Guide* for a list of the files that you need to restrict access to.

- Manage passwords. Linux accounts protected by passwords must be created for ECC. Besides the Linux accounts, you need to create non-Linux accounts to access external applications like Oracle Communications Billing and Revenue Management (BRM) and Oracle Communications Pricing Design Center (PDC). BRM and PDC are used to load customer and pricing data respectively into ECE. For secure communication between ECE and these systems, credentials stored in ECE are encrypted and stored in the KeyStore.
- Set up cluster security. To restrict access to the ECE Coherence cluster, you must set up an authorized hosts list. You can optionally enable SSL for intra-cluster communication, in which case you must also enable Well Known Addresses (WKA).
- Set up passwordless Secure Shell SSH between driver and server machines. You must set up passwordless SSH between driver and server machines for ECC to work. Passwordless SSH allows servers to connect to the driver and synchronize ECE files.

# 6

## Security Considerations for Developers

Learn how developers can extend Oracle Communications Billing and Revenue Management (BRM) without compromising security.

Topics in this document:

- [Using the BRM SDK](#)
- [Security Considerations for ECE Developers](#)

### Using the BRM SDK

The frameworks provided in the BRM SDK have the same level of security built into them as exists in the standard BRM product. All extensions developed for BRM should use the framework to ensure the security features detailed in this guide are included in the extensions' design.

### Security Considerations for ECE Developers

ECE requires that all Java processes that join its cluster have a correct set of configuration settings. When using the ECE secure mode, having the correct Coherence properties is not sufficient to join the cluster. Any direct access to Coherence APIs should not be used by developers engaged in writing any extensions of plug-ins to ECE. They must use the Spring and Template framework provided by ECE. Any direct access to Coherence resources including its caches will throw security exceptions.

# 7

## Billing Care Security

Learn how to install and implement Oracle Communications Billing Care and its components in a secure configuration.

Topics in this document:

- [About Installing Billing Care Securely](#)
- [Implementing Billing Care Security](#)
- [Developing Secure Applications for Billing Care](#)
- [Storing Billing Care Passwords in Oracle Wallet](#)
- [Storing Configuration Entries in the Billing Care Wallet](#)

### About Installing Billing Care Securely

Before installing Billing Care, you must properly install and configure several Oracle products, including Java, Oracle WebLogic Server, and Oracle Communications Billing and Revenue Management (BRM). For Billing Care installation instructions, including all required products and related tasks, such as setting up KeyStores and SSL for WebLogic Server, see "Installing Billing Care" in *Billing Care Installation Guide*.

Oracle Platform Security Services (OPSS) and Oracle Identity Manager provide authentication and authorization capabilities for Billing Care. These products are also required in a Billing Care implementation. See *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite* and *Oracle Fusion Middleware Administrator's Guide for Oracle Platform Security Services*.

### Encrypting OAP Entries in Infranet.properties

If you are using Oracle Analytics Publisher for invoicing, you must add the BIP user ID, the OAP password, and the OAP URL in the Billing Care wallet. For a secure installation, you must encrypt the OAP password. You use Oracle WebLogic Server to perform the encryption. For more information, see "[Storing Configuration Entries in the Billing Care Wallet](#)".

### Securing Web Cookies

A common web security problem is the stealing of Web cookies. This happens when an attacker manages to get a copy of your web cookie, generally while it is being transmitted over insecure channels such as HTTP.

You use a WebLogic Server variable to ensure that your Billing Care cookies are sent only through encrypted channels, such as SSL.

To secure your Billing Care Web cookies:

1. Open the *BillingCare\_home/setup/plan.xml* file in a text editor.  
where *BillingCare\_home* is the directory in which you installed Billing Care.

2. Set the `SECURE_COOKIE` variable to **true**:

```
<variable-definition>
  <variable>
    <name>SECURE_COOKIE</name>
    <value>>true</value>
  </variable>
</variable-definition>
```

3. Add a variable assignment for `SECURE_COOKIE`:

```
<module-override>
  <module-name>BillingCare.war</module-name>
  <module-type>war</module-type>
  <module-descriptor external="true">
    <root-element>weblogic-web-app</root-element>
    <uri>WEB-INF/weblogic.xml</uri>
    <variable-assignment>
      <name>SECURE_COOKIE</name>
      <xpath>/weblogic-web-app/session-descriptor/cookie-secure</
xpath>
    </variable-assignment>
  </module-descriptor>
</module-override>
```

4. Save and close the file.
5. Log in to the Oracle WebLogic Server Administration Console.
6. In the **Domain Structure** section, click **Deployments**.
7. In the **Configuration** tab, select the **BillingCare** check box and then click **Update**.  
The Update Application Assistant screen appears.
8. In Deployment plan path, click **Change Path** and enter the path to your Billing Care deployment file.
9. Click **Finish**.

## Implementing Billing Care Security

Billing Care supports stringent authorization, authentication, and audit requirements. This section describes how to implement the security capabilities supported by Billing Care.

### About Identity Management Suite

Oracle Identity Management (IDM) is a primary component for authorization and authentication. Each instance of Billing Care requires a properly configured instance of IDM to enable these functions.

For information about installing Billing Care, see *Billing Care Installation Guide*.



## About Authentication

Billing Care supports the following security for authentication:

- Authenticating Billing Care users against an LDAP-based user ID repository
- Enabling Single Sign-On capabilities
- Supporting user's password policies

Oracle Identity Manager manages user password policies. For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

## About Authorization

Authorization refers to granting users privileges appropriate for their job functions while denying access to other functionality. OPSS handles all authorization tasks for Billing Care. This section provides an overview of setting up and maintaining entitlements for Billing Care plus strategies for mapping enterprise users to those entitlements.

The following terms are used in authorization:

- **Resource Type:** Contains the action definitions, for example, **AdjustmentCurrencyResourceType**.
- **Resource:** Represents a piece of functionality being secured, for example, **AdjustmentResource**. It must always be of a known resource type.
- **Action:** Combined with a resource, defines operations permissible for an application's functionality, for example, **AdjustmentResource** and **make**.
- **Obligation:** Stores transaction limits. Some operations impose transaction limits, such as the maximum payment amount. Obligations are the property of Authorization Policy.
- **Authorization Policy:** Comprises the resources, actions, and obligations that combine to form a logical grouping, for example, an entire set of application functions for the regular CSR.
- **Enterprise (External) Role:** Represents the job functions for the users at your company. You make OPSS aware of roles by mapping them to the Billing Care policies. If you do not map enterprise roles in the authorization policy, you must map to each user.

Billing Care includes an OPSS seed file containing all the resource types, resources, actions, and obligations and few sample authorization policies (Regular CSR, Super CSR, ReadOnly CSR, Auditor, Billing Analyst, and WriteOff).

For instructions on importing the seed file, see *Oracle Fusion Middleware Administering Oracle Platform Security Services*.



### Note:

Unless you are customizing Billing Care, do not change the seed file.

To deploy the seed file, use the **jps-config.xml** file located in **SDK\_home\references\AuthorizationDataModel**.

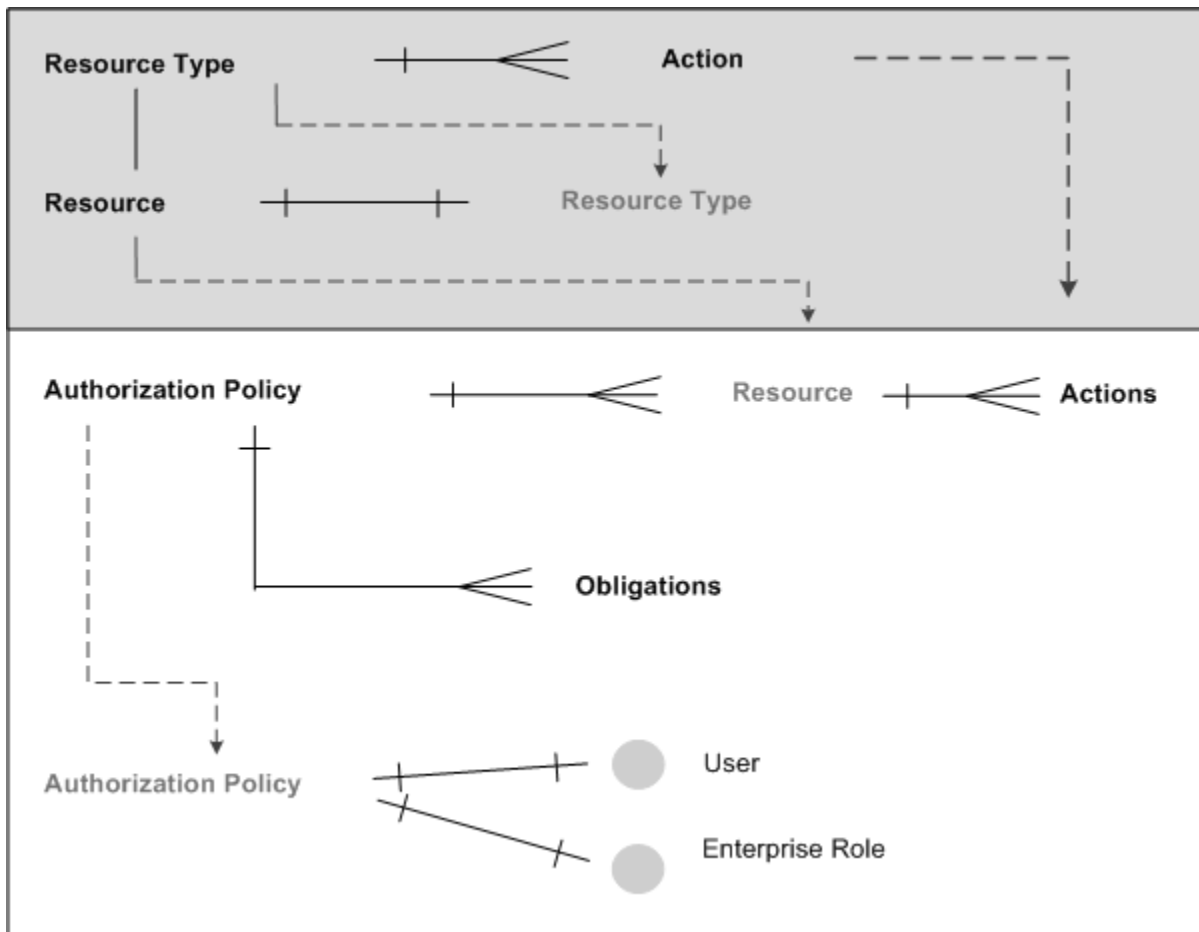
[Figure 7-1](#) describes the authorization flow:

1. The shaded area refers to areas defined in the OPSS seed file. (You load the seed file before performing the configuration).
2. The lower area represents how an authorization policy is mapped to one or more resources in OPSS. A resource may have one or more actions.
3. The authorization policy is mapped to obligations.
4. The authorization policy is associated with a user (individual) or an enterprise role (function).

The authorization policy is mapped to obligations, which are listed in [Table 7-2](#).

Any changes made in OPSS must be redeployed (or distributed).

**Figure 7-1 Developing Authorization Policies for User and Enterprise Roles**



## About Billing Care Authorization Resources

A user who does not have a resource grant is denied access to Billing Care. This behavior is targeted for deployments where a central user identity repository, storing all enterprise users, authenticates Billing Care sign-in requests. The authorization scheme allows access only to users granted resources in OPSS.

[Table 7-1](#) shows the Billing Care Authorization Resources. Resources grant permission to perform general CSR tasks or more advanced A/R tasks.

Table 7-1 Authorization Resources

Resource Type	Resource	Actions	Description
SuperUserType	SuperUserResource	Any	Enables you to create users free of restrictions, including when the user's profile contains other resources.  The only exception is the ReadOnlyType, which takes precedence over all other resource types.
ReadOnlyType	ReadOnlyResource	Any	Causes <b>Save</b> and <b>Apply</b> buttons on overlays to be displayed as read-only. Users are allowed only to read operations even if they have other resources or entitlements.
AccountResourceType	AccountResource	Make, Modify, Search, Transition, View	<b>Make:</b> Allows the user to create accounts. <b>Modify:</b> Allows the user to add, delete, or save customer contact information. <b>Search:</b> Allows the user to access search functionality. <b>Transition:</b> Enables changing the account status. <b>View:</b> Enables the user to view account profile and other customer information.
AdjustmentCurrencyResourceType	AdjustmentResource	Allocate, Make	<b>Allocate:</b> Allows the user to allocate currency adjustments. <b>Make:</b> Allows the user to make adjustments.  Uses a policy that constrains the maximum payment amount as a function of CSRs access level. See <a href="#">Table 7-2</a> for transaction limits.

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
AdjustmentNonCurrencyResourceType	AdjustmentNonCurrencyResource	Make	<b>Make:</b> Gives noncurrency adjustments their own resource type because they cannot be allocated (unlike currency resources). Policy on the minimum and maximum noncurrency amount applies. See <a href="#">Table 7-2</a> for transaction limits.
BillResourceType	BillResource	BillNow	<b>BillNow:</b> Allows the user to perform Bill Now operations.
BillUnitResourceType	BillUnitResource	Add, BalanceTransfer, Delete, Modify, ModifyValidity, SetLimit	<b>Add:</b> Allows the user to create bill units. Allows the user to move services between bill units. <b>BalanceTransfer:</b> Allows the user to transfer balances to another bill unit. <b>Delete:</b> Reserved for future use. <b>Modify:</b> Allows the user to change the bill unit. <b>ModifyValidity:</b> Allows the user to modify the validity of noncurrency balances. <b>SetLimit:</b> Allows the user to set credit limit and thresholds for noncurrency resources.
CancelInstallmentResourceType	CancelInstallmentResource	Add, Cancel	<b>Add:</b> Allows the user to cancel an open installment. <b>Cancel:</b> Allows the user to undo an installment cancellation.

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
ChargeSharingResourceType	ChargeSharingResource	Add, Delete, Modify, AddMember, DeleteMember, ModifyMember, ModifyPriority	<p><b>Add:</b> Allows the user to create a charge sharing group.</p> <p><b>Delete:</b> Allows the user to remove a charge sharing group.</p> <p><b>Modify:</b> Allows the user to modify the charge sharing group.</p> <p><b>AddMember:</b> Allows the user to add a member to a charge sharing group.</p> <p><b>DeleteMember:</b> Allows the user to remove members from a charge sharing group.</p> <p><b>ModifyMember:</b> Allows the user to change members in a charge sharing group.</p> <p><b>ModifyPriority:</b> Allows the user to modify the order of priority when a member is part of multiple discount or charge sharing groups.</p>

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
CollectionsResourceType	CollectionsResource	Search, Delete, AddAction, ModifyAction, Replace, Perform, Promise, Exit, Exempt, ReassignHandler, AddMember, DeleteMember	<p><b>Search:</b> Allows the user to access collections.</p> <p><b>Delete:</b> Allows the user to delete a collection group from an owner account.</p> <p><b>AddAction:</b> Allows the user to add a collection action on a bill unit in collections.</p> <p><b>ModifyAction:</b> Allows the user to modify a collections action for a bill unit.</p> <p><b>Replace:</b> Allows the user to replace a scenario with another scenario in collections.</p> <p><b>Perform:</b> Allows the user to perform collections actions.</p> <p><b>Promise:</b> Allows the user to manage promise-to-pay agreements in collections.</p> <p><b>Exit:</b> Allows the user to exit a bill unit of an account from collections.</p> <p><b>Exempt:</b> Allows the user to exempt a bill unit from collections.</p> <p><b>ReassignHandler:</b> Gives the user the collections manager role. It allows the user to assign collections agents to bill units in collections.</p> <p><b>AddMember:</b> Allows the user to add members to a collections group.</p> <p><b>DeleteMember:</b> Allows the user to delete members from a collections group.</p>

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
ConfigurationsArtifactsType	ConfigurationArtifactsResource	View	<b>View:</b> Allows the user to read all configuration-related REST APIs (for example, authorization profiles).
CustomerDepositResourceType	CustomerDepositResource	Add, View	<b>Add:</b> Allows the user to add and create deposits for a customer. <b>View:</b> Allows the user to view your customers' deposit.
DeferredActionResourceType	DeferredActionResource	Edit, Delete, Execute	<b>Edit:</b> Allows the user to modify a deferred action. <b>Delete:</b> Allows the user to remove a deferred action. <b>Execute:</b> Allows the user to run a deferred action.
DepositPaymentResourceType	DepositPaymentResource	Add	<b>Add:</b> Allows the user to accept and enter deposit payments for your customers.
DepositRefundResourceType	DepositRefundResource	Add, View	<b>Add:</b> Allows the user to refund deposits to your customers. <b>View:</b> Allows the user to view deposit refunds.
DepositReleaseResourceType	DepositReleaseResource	Add	<b>Add:</b> Allows the user to release deposits back to customers.
DepositResourceType	DepositResource	View	<b>View:</b> Allows the user to view customer deposits.
DepositReversalResourceType	DepositReversalResource	Add	<b>Add:</b> Allows the user to perform deposit reversals.
DepositSpecProfileResourceType	DepositSpecProfileResource	Add, View, Modify	<b>Add:</b> Allows the user to create deposit specification profiles. <b>View:</b> Allows the user to view deposit specification profiles. <b>Modify:</b> Allows the user to modify deposit specification profiles.

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
DepositSpecResourceType	DepositSpecResource	Add, View, Modify, Delete	<p><b>Add:</b> Allows the user to create deposit specifications.</p> <p><b>View:</b> Allows the user to view deposit specifications.</p> <p><b>Modify:</b> Allows the user to modify deposit specifications.</p> <p><b>Delete:</b> Allows the user to delete deposit specifications.</p>
DepositTransactionResourceType	DepositTransactionResource	View	<p><b>View:</b> Allows the user to view all transactions that have been performed on an account.</p>
DepositTransferResourceType	DepositTransferResource	Add	<p><b>Add:</b> Allows the user to transfer a deposit to another account.</p>
DiscountSharingResourceType	DiscountSharingResource	Add, Delete, Modify, AddMember, DeleteMember, ModifyMember, ModifyPriority	<p><b>Add:</b> Allows the user to create a discount sharing group.</p> <p><b>Delete:</b> Allows the user to remove a discount sharing group.</p> <p><b>Modify:</b> Allows the user to change the member details in a discount sharing group.</p> <p><b>AddMember:</b> Allows the user to add a member to a discount sharing group.</p> <p><b>DeleteMember:</b> Allows the user to delete members from a discount sharing group.</p> <p><b>ModifyMember:</b> Allows the user to change members in a discount sharing group.</p> <p><b>ModifyPriority:</b> Allows the user to modify the order of priority when a member is part of multiple discount sharing groups.</p>



Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
DisputeResourceType	DisputeResource	Raise, Settle	<b>Raise:</b> Allows the user to raise bill and item-level and event-level disputes. <b>Settle:</b> Allows the user to settle bill and item-level disputes. Policy on the maximum dispute amount applies. See <a href="#">Table 7-2</a> for transaction limits.
InstallmentProposalResourceType	InstallmentProposalResource	Add	<b>Add:</b> Allows the user to add installment proposals.
InstallmentResourceType	InstallmentResource	View	<b>View:</b> Allows the user to view a customer's individual installments.
InstallmentScheduleResourceType	InstallmentScheduleResource	Add, View	<b>Add:</b> Allows the user to add an installment schedule. <b>View:</b> Allows the user to view a customer's installment schedules.
InstallmentScheduleSpecResourceType	InstallmentScheduleSpecResource	Add, View, Modify	<b>Add:</b> Allows the user to add installment schedule specifications. <b>View:</b> Allows the user to view installment schedule specifications. <b>Modify:</b> Allows the user to modify installment schedule specifications.
InvoiceImageType	InvoiceImageResource	View	<b>View:</b> Allows the user to view invoices.
LoanResourceType	LoanResource	ApplyLoan	<b>ApplyLoan:</b> Allows the user to perform a loan for customers.
NoteResourceType	NoteResource	Comment	<b>Comment:</b> Allows the user to add comments to notes.
NotificationEventResourceType	NotificationEventResource	View	<b>View:</b> Allows the user to view notification events.
NotificationResourceType	NotificationResource	View	<b>View:</b> Allows the user to view notifications.

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
NotificationSpecResourceType	NotificationSpecResource	Add, View, Modify	<p><b>Add:</b> Allows the user to create a notification specification.</p> <p><b>View:</b> Allows the user to view notifications specifications.</p> <p><b>Modify:</b> Allows the user to change notification specifications.</p>
PaymentMethodResourceType	PaymentMethodResource	Add, Delete, Modify	<p><b>Add:</b> Allows the user to add payment methods.</p> <p><b>Delete:</b> Allows the user to delete payment methods.</p> <p><b>Modify:</b> Allows the user to change payment methods.</p>

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
PaymentResourceType	PaymentResource	Allocate, Audit, BatchProcess, Make, ReassignHandler, Reverse, SuspenseAccess, SuspenseAllocate, SuspenseMake, SuspenseMove, SuspenseReverse	<p><b>Allocate:</b> Allows the user to allocate payments.</p> <p><b>Audit:</b> Allows the user to view audit information in the Payment Details dialog box. (Audit information in the <b>Payment Suspense</b> screen is always visible).</p> <p><b>BatchProcess:</b> Displays the <b>Batch Payment</b> button on the landing page.</p> <p><b>Make:</b> Allows the user to make payments.</p> <p><b>ReassignHandler:</b> Allows the user to assign an authorized handler to manage suspended payments.</p> <p><b>Reverse:</b> Allows the user to reverse payments.</p> <p><b>SuspenseAccess:</b> Allows the user to access the <b>Payment Suspense</b> button on the landing page.</p> <p><b>SuspenseAllocate:</b> Allows the user to allocate suspended payments partially or fully to an account.</p> <p><b>SuspenseMake:</b> Allows the user to make suspended payments.</p> <p><b>SuspenseMove:</b> Allows the user to move posted payments into suspended status.</p> <p><b>SuspenseReverse:</b> Allows the user to reverse suspended payments.</p> <p>Returned as an obligation; OPSS returns a number, which is interpreted as</p>

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
			a limit. See <a href="#">Table 7-2</a> for transaction limits.
ProfileResourceType	ProfileResource	View, Add, Delete, Modify	<p><b>View:</b> Allows the user to view an account's profile.</p> <p><b>Add:</b> Allows the user to create an account profile.</p> <p><b>Delete:</b> Allows the user to remove an account profile.</p> <p><b>Modify:</b> Allows the user to change an account profile.</p>
ProfileSharingResourceType	ProfileSharingResource	Add, Delete, Modify, AddMember, DeleteMember, ModifyMember	<p><b>Add:</b> Allows the user to create a profile sharing group.</p> <p><b>Delete:</b> Allows the user to remove a user from a profile sharing group.</p> <p><b>Modify:</b> Allows the user to change the member details in a profile sharing group.</p> <p><b>AddMember:</b> Allows the user to change the member details in a profile sharing group.</p> <p><b>DeleteMember:</b> Allows the user to remove a member from a profile sharing group.</p> <p><b>ModifyMember:</b> Allows the user to modify members in a profile sharing group.</p>
RefundResourceType	RefundResource	Make	<p><b>Make:</b> Allows the user to perform account-level and bill unit-level refunds.</p>

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
RequestInfoResourceType	RequestInfoResource	Add, View, Delete	<p>Use this resource to help record failed REST requests, along with their headers and payloads, in the BRM database.</p> <p><b>Add:</b> Allows the user or client application to use the Billing Care REST API to record failed requests.</p> <p><b>View:</b> Allows the user or client application to use the Billing Care REST API to retrieve failed REST API requests.</p> <p><b>Delete:</b> Allows the user or client to use the Billing Care REST API to delete failed REST API requests.</p>

Table 7-1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
ServiceResourceType	ServiceResource	Cancel, Edit, Inactivate, Make, Reactivate, OfferInactivate, OfferTerminate, OfferReactivate, Terminate, Associate, EditOfferCustomization	<p><b>Cancel:</b> Allows the user to cancel services.</p> <p><b>Edit:</b> Gives the user access to the Asset Details page.</p> <p><b>Inactivate:</b> Allows the user to inactivate services.</p> <p><b>Make:</b> Allows the user to access the <b>Select</b> and <b>Configure</b> pages of the customer creation wizard. It also exposes the <b>Purchase</b> button.</p> <p><b>OfferInactivate:</b> Allows the user to inactivate product and discount offers.</p> <p><b>OfferReactivate:</b> Allows the user to reactivate product and discount offers.</p> <p><b>OfferTerminate:</b> Allows the user to terminate product and discount offers.</p> <p><b>Reactivate:</b> Allows the user to reactivate services.</p> <p><b>Terminate:</b> Allows the user to terminate services.</p> <p><b>Associate:</b> Allows the user to search and associate devices.</p> <p><b>EditOfferCustomization:</b> Allows the user to modify rate customizations.</p>
SubscriptionResourceType	SubscriptionResource	Transit	<p><b>Transit:</b> Allows the user to transition packages or bundles.</p>

**Table 7-1 (Cont.) Authorization Resources**

Resource Type	Resource	Actions	Description
TaxExemptionResourceType	TaxExemptionResource	Add, Delete, Modify	<b>Add:</b> Allows the user to add tax exemptions whether account has or does not have prior tax exemptions. <b>Delete:</b> Allows the user to delete tax exemptions. <b>Modify:</b> Allows the user to save changes to tax exemption attributes.
WriteoffResourceType	WriteoffResource	Make	<b>Make:</b> Allows the user to write off accounts, bills, and items. Policy on the minimum and maximum write-off amount applies. See <a href="#">Table 7-2</a> for transaction limits.

## Policies on Transaction Limits

Some of the resources listed in [Table 7-1](#) work in combination with transaction limits. For example, a CSR can be authorized to make adjustments but not over a certain amount. System administrators must configure the limits with OPSS.

[Table 7-2](#) lists the attributes that require system administrators to configure transaction limits (values).

**Table 7-2 Listing of Transaction Limits (Obligations)**

Attribute	Type
Maximum Currency Adjustment Amount	Integer
Minimum Currency Adjustment Amount	Integer
Maximum Noncurrency Adjustment Amount	Integer
Minimum Noncurrency Adjustment Amount	Integer
Maximum Payment Amount	Integer
Maximum Dispute Amount (applies to settle as well)	Integer
Maximum Write-off Amount	Integer
Maximum Refund Issues Amount	Integer
Maximum Refund Settle Amount	Integer

## About Auditing

The BRM server software handles auditing of Billing Care activities. The BRM event notification framework captures the audit trail records inside the **`/user_activity`** storable class.

Each audit trail record links the activity with its creator, date, and time. In the audit trail, the identity of the person creating the record is the user name entered in Billing Care at sign-in.

To capture new activity in the audit trail, include the event corresponding to the relevant activity using the **pin\_notify** file in BRM. The same instructions apply when excluding events from the audit trail.

[Table 7-3](#) lists all activities preserved in BRM by default. The list is from the **/config/pin\_notify** storable class. You can add to or delete from this list.

**Table 7-3 Audited List from /config/pin\_notify**

Task	BRM Event Name (Activity)
Account creation	/event/notification/account/create
Subscription purchase	/event/billing/product/action/purchase
Subscription modification	/event/billing/product/action/modify
Subscription cancellation	/event/billing/product/action/cancel
Updates to bill info (for example, BDOM [billing day of month], billing frequency, accounting type changes)	/event/customer/billinfo/modify
Event adjustment	/event/billing/adjustment/event
Item adjustment	/event/billing/adjustment/item
Account adjustment	/event/billing/adjustment/account
Top up	/event/billing/vouchertopup
Dispute issue	/event/billing/dispute
Dispute settled	/event/billing/settlement/event
Refund	/event/billing/refund
Write-off operation	/event/billing/writeoff
Payment	/event/billing/payment
Credit limit changes	/event/billing/limit, /event/billing/credit
Bill Now	/event/notification/billing/start
Charge sharing group life-cycle operations	/event/group/sharing/charges/create /event/group/sharing/charges/modify /event/group/sharing/charges/delete
Discount sharing group life-cycle operations	/event/group/sharing/discounts/create /event/group/sharing/discounts/modify /event/group/sharing/discounts/delete
Profile (for example, Friends and Family) life-cycle operations	/event/group/sharing/profiles/create /event/group/sharing/profiles/modify /event/group/sharing/profiles/delete
Credit Monitors life-cycle operations	/event/group/sharing/monitor/modify /event/group/sharing/monitor/delete /event/group/sharing/profiles/delete
Account hierarchy operations	/event/group/parent /event/group/member



For information on logging events, including changing the events logged, see "Logging CSR Activity Events" in *BRM System Administrator's Guide*.

## Developing Secure Applications for Billing Care

To develop secure applications for Billing Care or extend Billing Care without compromising security, you must control users' access to resources by:

- Adding security controls over new UI features.
- Controlling who can access REST services and the limitations of that access.

When users sign in, Billing Care calls OPSS and then OPSS provides authorization if appropriate. Additionally, OPSS determines the restraints or obligations of the authorization.

The developer needs to create a web project in Netbeans for the Billing Care custom REST APIs.

### Creating a Resource Type with OPSS

To develop secured custom REST APIs or UIs, you need OPSS resource types for authorization. For more information, see "Importing the Billing Care Security Policies to OPSS" in *Billing Care Installation Guide*.

### About REST API Authorization

To control the access of custom REST services and operations to authenticated users, define resource types in OPSS as described in "[Creating a Resource Type with OPSS](#)".

In custom REST resource operations that require authorization, call **EnforcementUtil.checkAccess()** by passing the required **subject**, **applicationName**, **action**, **resourceType**, **resource**, **Error**, and optional **UIRequestValue** objects as parameters.

**UIRequestValue** parameters are optional and are used for handling obligations.

For more information, see "Performing Authorization on the REST Framework" in *Billing Care SDK Guide*.

### About UI Authorization

After a user successfully signs in to Billing Care, it fetches the grants of all resources and sets it into the global variable **authorizationJSON**.

When opening a page or dialog box, Billing Care gets the grants of resources through the available authorization custom-bindings and then applies the bindings in the respective view model or overlay view model.

For more information, see "Performing Authorization on the UI" in *Billing Care SDK Guide*.

### Adding New Resource Types

To add new resource types:

1. In the **CustomConfigurations.xml** file, add the new OPSS resource types:  
In this example, the new resource type **CreditProfileResourceType** is added.

 **Note:**

Do not change key values.

```

<keyvals>
  <key>authorizationResourceTypes/key>
  <value>CreditProfileResourceType</value>
  <desc>Add comma separated OPSS Resource Types (values) for authorization.
    Also these resource types must be defined in OPSS.
    Do not change the keys here.
  </desc>
</keyvals>

```

**2.** Redeploy the customization.

For more information, see "Packaging and Deploying Customizations" in *Billing Care SDK Guide*.

## Storing Billing Care Passwords in Oracle Wallet

By default, the Billing Care installer stores sensitive information such as passwords in the Oracle wallet, and the Billing Care application retrieves the passwords from the Oracle wallet. However, if the passwords are also stored in configuration files, the Billing Care application retrieves the passwords from the configuration files. The Billing Care application automatically decrypts the encrypted passwords when retrieving them from the configuration files.

By default, passwords in configuration files are encrypted in the Oracle ZT PKI format. For more information, see "Encrypting Data" in *BRM Developer's Guide*.

 **Note:**

To encrypt passwords that are associated with customizations, use the **pin\_crypt\_app** utility. For details, see "About Encrypting Passwords" in *BRM Developer's Guide*.

## Storing Configuration Entries in the Billing Care Wallet

To store a configuration entry for the Billing Care wallet:

1. Go to the `SDK_home/BillingCareSDK/samples/Wallet` directory, where `SDK_home` is the Billing Care SDK installation directory.
2. Do one of the following:
  - On Linux, run the following command:

```

java -cp
'.:oraclepkiLocation:osdtCertLocation:osdtCoreLocation:cetLocation:'com.p
ortal.cet.ConfigEditor -setconf -wallet clientWalletLocation -parameter
configEntry -value value

```

where:

- *oraclepkiLocation* is the path to the **oraclepki.jar** file which contains the APIs that are required for the **wallet.oraclepki.jar** is stored in the *SDK\_home/BillingCareSDK/samples/Wallet* directory.
- *osdtCertLocation* is the path to the **osdt\_cert.jar** file, which contains the JARs that are used by the JAVA PCM library for establishing a TLS connection to BRM. The **osdt\_cert.jar** file is stored in the *SDK\_home/BillingCareSDK/samples/Wallet* directory.
- *osdtCoreLocation* is the path to the **osdt\_core.jar** file, which contains the JARs that are used by the JAVA PCM library for establishing a TLS connection to BRM. The **osdt\_core.jar** file is stored in the *SDK\_home/BillingCareSDK/samples/Wallet* directory.
- *cetLocation* is the **cet.jar** file, which contains the APIs that are required for the wallet. The **cet.jar** file is stored in the *SDK\_home/BillingCareSDK/samples/Wallet* directory.
- *clientWalletLocation* is the path to the Billing Care wallet.
- *configEntry* is the configuration entry in the Billing Care wallet.
- *value* is the appropriate value for the respective entry in the Billing Care wallet.

For example, running the following command with the **-value** parameter stores the **infranet.log.level** as **1** in the Billing Care wallet. If the value exists in the wallet, it will be overwritten:

```
java -cp
'..:oraclepki.jar:osdt_cert.jar:osdt_core.jar:cet.jar:'com.portal.cet.ConfigEdit
or -setconf -wallet "/scratch/pin11/wallet" -parameter infranet.log.level -
value 1
```

If you run the command without the **-value** parameter, it prompts for the values for the **infranet.connection** entries and stores them in the Billing Care wallet. At the command prompt, enter the values listed in [Table 7-4](#).

**Table 7-4 BRM Connection Information**

Field	Description
<b>User Name</b>	The user name for connecting to BRM.
<b>Password</b>	The BRM user's password.
<b>Host Name</b>	The IP address or the host name of the machine on which the primary BRM Connection Manager (CM) or CM Master Process (CMMP) are running.
<b>Port Number</b>	The TCP port number of the CM or CMMP on the host computer.
<b>Service Type</b>	The BRM service type.
<b>Service POID Id</b>	The POID of the BRM service.

- On Windows, run the following command:

```
java -cp "..:oraclepkiLocation:osdtCertLocation:osdtCoreLocation:cetLocation"
com.portal.cet.ConfigEditor -setconf -wallet clientWalletLocation -parameter
configEntry -value value
```

For example, running the following command with the **-value** parameter stores the **infranet.log.level** as **1** in the Billing Care wallet:

```
java -cp ".;C:\Program Files (x86)\Portal  
Software\BillingCare\lib\oraclepki.jar;C:\Program Files (x86)\Portal  
Software\BillingCare\lib\osdt_cert.jar;C:\Program Files (x86)\Portal  
Software\BillingCare\lib\osdt_core.jar;C:\Program Files (x86)\Portal  
Software\BillingCare\lib\cet.jar" com.portal.cet.ConfigEditor -setconf -  
wallet "C:\Program Files (x86)\Portal  
Software\BillingCare\wallet\client" -parameter infranet.log.level -value  
1
```

If you run the command without the **-value** parameter, it prompts for the values for the **infranet.connection** entries and stores them in the Billing Care wallet. At the command prompt, enter the values listed in [Table 7-4](#).

**3.** Enter the Billing Care client wallet password.

The value is stored in the Billing Care wallet.

For retrieving stored configuration entries, see "About Oracle Wallet" in *BRM System Administrator's Guide*.

# 8

## Billing Care REST API Security

Learn how to implement the security capabilities supported by Billing Care REST API. The Oracle Communications Billing Care REST API supports stringent authorization and authentication requirements.

Topics in this document:

- [About Authentication and Authorization](#)
- [Setting Up OAuth with Oracle Identity Cloud Service](#)
- [Setting Up OAuth with Oracle Access Management](#)

For more information, see *REST API Reference for Billing Care*.

### About Authentication and Authorization

The Billing Care REST API uses the OAuth 2.0 protocol to authenticate a client application's identity and to authorize the client application to access its REST API. It does this by validating an OAuth access token that is passed in the header of the client's HTTP/HTTPS request to the Billing Care REST API.

Your client must pass this OAuth access token in the header of every HTTP/HTTPS request sent to the Billing Care REST API.

To set up authentication and authorization for your client, you can use either Oracle Identity Cloud Service (IDCS) or Oracle Access Management.

### Setting Up OAuth with Oracle Identity Cloud Service

You can set up your client application to use OAuth authentication to access the Billing Care REST API. The client application uses the resource owner's credentials to access the resource server.

The high-level steps for setting up OAuth authentication using Oracle Identity Cloud Service (IDCS) includes the following:

1. [Creating a Confidential OAuth Application for the Resource Server](#)
2. [Creating a Confidential OAuth Application for Your Client Application](#)
3. [Encoding the Client's Credentials in Base64 Format](#)
4. [Configuring OAuth Settings Using IDCS](#)
5. [Storing the Resource Server's Credentials in the Wallet](#)

Afterwards, you must request an access token for each client application that will submit REST requests to the Billing Care REST API. See "[Requesting an OAuth Access Token](#)".

**Note:**

Authentication is required for production systems only. In test systems, you can submit requests without configuring authentication.

## Creating a Confidential OAuth Application for the Resource Server

When you create a confidential OAuth application in Oracle Identity Cloud Service (IDCS), it provides you with a client ID and client secret. Your client will need the client ID and client secret to request OAuth access tokens for accessing the Billing Care REST API.

To create a confidential OAuth application in IDCS:

1. In the Identity Cloud Service console, expand the **Navigation Drawer** and then click **Applications**.
2. Click **Add application**.  
The Add Application page appears.
3. Select **Confidential Application** and then click **Launch workflow**.  
The Add Confidential Application page appears.
4. In the **Name** field, enter a name for your application, such as **BCREST**.
5. Click **Next**.
6. In the Resource server configuration section, do the following:
  - a. Select the **Configure this application as a resource server now** option.
  - b. In the **Access token expiration** field, enter how long in seconds the access token remains valid.
  - c. In the **Primary audience** field, enter the primary recipient where the access token of your confidential application is processed.
  - d. Select the **Add scopes** option.
  - e. In the Scopes table, click **Add**.  
The Add Scope dialog box appears.
  - f. In the **Scope** field, enter **BillingCare**.
  - g. Click **Add**.
7. In the Client configuration section, select the **Configure this application as a client now** option.
8. In the Authorization section, do the following:
  - a. In the **Allowed Grant Types** field, select the **Client credentials** option.
  - b. In the **Client Type** field, select the **Confidential** option.
  - c. In the **Allowed Operations** field, select the **Introspect** check box.
9. Click **Next**.
10. Under Web tier policy, select the **Skip and do later** option.

11. Click **Finish**.
12. In the Application Added pop-up window, make note of the client ID and client secret. You will provide this to the person who needs to generate the OAuth access token.
13. Click **Activate** and then click **Activate application** to confirm the activation.

## Creating a Confidential OAuth Application for Your Client Application

When you create a confidential OAuth application in Oracle Identity Cloud Service (IDCS), it provides you with a client ID and client secret. Your client will need the client ID and client secret to request OAuth access tokens for accessing the Billing Care REST API.

To create a confidential OAuth application in IDCS for your client application:

1. In the Identity Cloud Service console, expand the **Navigation Drawer** and then click **Applications**.
2. Click **Add application**.  
The Add Application page appears.
3. Select **Confidential Application** and then click **Launch workflow**.  
The Add Confidential Application page appears.
4. In the **Name** field, enter a name for your application, such as **BCRESTClient1**.
5. Click **Next**.
6. In the Resource server configuration section, select the **Skip for later** option.
7. In the Client configuration section, select the **Configure this application as a client now** option.
8. In the Authorization section, do the following:
  - a. In the **Allowed Grant Types** field, select the **Client credentials** option.
  - b. In the **Client Type** field, select the **Confidential** option.
  - c. Select the **Add resources** option.
  - d. In the Resources table, click **Add scope**.  
The Add Scope dialog box appears.
  - e. In the **Resource** field, enter **ResourceServerBillingCare**.
  - f. Click **Add**.
9. Click **Next**.
10. Under Web tier policy, select the **Skip and do later** option.
11. Click **Finish**.
12. In the Application Added pop-up window, make note of the client ID and client secret. You will provide this to the person who needs to generate the OAuth access token.
13. Click **Activate** and then click **Activate application** to confirm the activation.

## Encoding the Client's Credentials in Base64 Format

To request OAuth access tokens for accessing the Billing Care REST API, your client application will need the client ID and client secret encoded in Base64 format. Generate a

Base64-encoded value of your client ID and client secret joined by a single colon (*ClientID:ClientSecret*).

You pass the Base64-encoded value in the header of your HTTP/HTTPS request for an OAuth access code.

## Configuring OAuth Settings Using IDCS

To configure OAuth to connect to your BRM server using IDCS:

1. Open the *User\_home/Infranet.properties* file in a text editor, where *User\_home* is the domain administrative user's home directory.
2. Add this entry:

```
idp.vendor=IDCS
idp.url=IDCS_hostname:port
idp.resource_server.scope=ResourceserverScopename
```

where:

- *IDCS\_hostname:port* is the host and port number of the IDCS Server that is running your application.
- *ResourceserverScopename* is the name of the resource server concatenated with the name of the scope.

### Note:

You entered the resource server name in the **Primary Audience** field of step 6, and you entered the scope name in the **Scope** field of step 6.

3. Save and close the file.

## Storing the Resource Server's Credentials in the Wallet

IDCS needs your resource server's client credentials to validate OAuth authentication requests. To improve security, store the resource server's client ID and client secret in the Oracle wallet so IDCS can retrieve it when needed.

To store the resource server's client credentials in the Oracle wallet:

1. Go to the *BRM\_home/bin* directory.
2. Store the client ID by running this command:

```
java -cp "JarLocationUnderInstallHome/
oraclepki.jar:JarLocationUnderInstallHome/
osdt_cert.jar:JarLocationUnderInstallHome/
osdt_core.jar:JarLocationUnderInstallHome/cet.jar"
com.portal.cet.ConfigEditor -setconf -wallet WalletLocation -parameter
idp.client.id -value "ClientIdValue"
```

where:

- *JarLocationUnderInstallHome* is the directory in which Java is installed in your Billing Care REST API installation.



- *WalletLocation* is the directory in which the Oracle wallet resides.
  - *ClientIdValue* is the client ID.
3. At the **Enter password for the wallet** prompt, enter your client wallet password.
  4. Store the client secret by running this command:

```
java -cp "JarLocationUnderInstallHome/oraclepki.jar:JarLocationUnderInstallHome/osdt_cert.jar:JarLocationUnderInstallHome/osdt_core.jar:JarLocationUnderInstallHome/cet.jar" com.portal.cet.ConfigEditor -setconf -wallet WalletLocation -parameter idp.client.secret [-pwd]
```

5. At the **Enter password for the wallet** prompt, enter your client wallet password.
6. At the **Enter the value** prompt, enter the client secret to store in the wallet.

## Requesting an OAuth Access Token

To request an OAuth access token, use cURL to send an HTTP/HTTPS request to the Billing Care REST API authorization endpoint. For example:

```
curl --location --request GET 'http://hostname:port/bcws/webresources/v1.0/authentication/queryAccessToken' \
  --header 'Authorization: Basic credentials'
```

where:

- *hostname:port* is the IP address or host name and port of the Billing Care REST API server.
- *credentials* is the Base64-encoded value of your IDCS administrator user name and password joined by a single colon (*username:password*).

If the request is successful, the token type and access token are returned. For example:

```
{
  "token_type": "Bearer",
  "access_token": "accessToken"
}
```

Your client must pass this OAuth access token in the header of every HTTP/HTTPS request sent to the Billing Care REST API.

## Setting Up OAuth with Oracle Access Management

The Oracle Communications Billing Care REST API uses OAuth 2.0 to authenticate requests from clients. Perform the following one-time tasks to configure OAuth and Oracle WebLogic Server for authentication:

1. [Configuring OAuth Services](#)
2. [Configuring WebLogic Server to Access LDAP Server](#)
3. [Configuring OAuth Settings Using Oracle Access Management](#)

Afterwards, you must request an access token for each client application that will submit REST requests to the Billing Care REST API. See "[Requesting an OAuth Access Token](#)".

 **Note:**

Authentication is required for production systems only. In test systems, you can submit requests without configuring authentication.

## Configuring OAuth Services

To use OAuth 2.0 for authentication, configure your Billing Care REST API services and then register your client application as a trusted client on Oracle Access Manager.

To configure OAuth services using Oracle Access Manager:

1. Create an identity domain, which controls the authentication and authorization of your client applications. It also controls which features your client application can access in relation to the service.

To create an identity domain, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL. For example:

```
curl -i
  -H "Content-Type: application/json"
  -H "Accept: application/json"
  -H "Authorization:Basic credentials"
  -X POST
  http(s)://hostname:port/oam/services/rest/ssa/api/v1/
  oauthpolicyadmin/oauthidentitydomain
  -d '{
    "name": "identityDomain",
    "description": "Description for Billing Care REST API
Identity Domain",
    "tokenSettings": [
      {
        "tokenType": "ACCESS_TOKEN",
        "tokenExpiry": tokenExpiry
      }
    ]
  }'
```

where:

- *credentials* is the Base64-encoded value of your Oracle Access Manager administrator user name and password joined by a single colon (*username:password*).
- *hostname:port* is the host and port of the Oracle Access Manager Administration Server.
- *identityDomain* is the name of the Oracle Access Manager identity domain that you want to create.
- *tokenExpiry* is the number of seconds before the token expires, such as 3600 for one hour.

See ["Add a new OAuth Identity Domain"](#) in *REST API for OAuth in Oracle Access Manager* for more information.

2. Create a resource server, which hosts protected resources and accepts and responds to protected resource requests using access tokens.

To create and configure your resource server, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL. For example:

```
curl -i
  -H "Content-Type: application/json"
  -H "Authorization:Basic credentials"
  -X POST
  http(s)://hostname:port/oam/services/rest/ssa/api/v1/
  oauthpolicyadmin/application
  -d '{
    "name": "resourceServer",
    "idDomain": "identityDomain",
    "description": "Billing Care REST API Resource Server",
    "scopes": [
      {
        "scopeName": "scopeName",
        "description": "All Access"
      }
    ]
  }'
```

where:

- *resourceServer* is the name of your resource server, such as BillingCare.
- *scopeName* is the name of the scope, such as All.

See ["Add a new Resource Server"](#) in *REST API for OAuth in Oracle Access Manager* for more information.

3. Create a client application that makes protected resource requests on behalf of the resource owner and with the resource owner's authorization. Billing Care REST API clients are web applications with an OAuth 2.0 client type of Confidential Client. Clients must use a grant type of Client Credentials for requesting access to Billing Care REST API resources.

To create a client application, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL. For example:

```
curl -i
  -H "Content-Type:application/json"
  -H "Authorization:Basic credentials"
  -X POST
  http(s)://hostname:port/oam/services/rest/ssa/api/v1/
  oauthpolicyadmin/client
  -d '{
    "secret": "client_secret",
    "id": "client_id",
    "name": "clientName",
    "scopes": [
      "resourceServer.scopeName"
    ],
    "clientType": "CONFIDENTIAL_CLIENT",
    "idDomain": "identityDomain",
  }'
```

```

        "description": "Description of client of Billing Care REST
API Server",
        "grantTypes": [
            "CLIENT_CREDENTIALS"
        ],
        "defaultScope": "resourceServer.scopeName",
        "redirectURIs": [
            {
                "url": "http(s)://BillingCareHost:BillingCarePort/
bcws",
                "isHttps": isHttps
            }
        ]
    }'

```

where:

- *client\_secret* is the password for your client.
- *client\_id* is the client ID for your client. It will be generated automatically if not specified.
- *clientName* is the name of your client.
- *BillingCareHost:BillingCarePort* is the host and port of the Billing Care REST API Server.
- *isHttps* is a Boolean value that specifies whether the URL is accessed over HTTPS (**true**) or HTTP (**false**).

See ["Add a new OAuth Client"](#) in *REST API for OAuth in Oracle Access Manager* for more information.

## Configuring WebLogic Server to Access LDAP Server

To configure your WebLogic Server to access user details on the LDAP server:

1. Update your Java policy store configuration for the Billing Care REST API to access the LDAP server.

You deploy Billing Care on a JRF-enabled Oracle WebLogic Server domain configured as an Oracle Platform Security Services (OPSS) client domain. Create a JRF-enabled domain in Oracle WebLogic Server and configure an application domain policy that controls access to the Billing Care application.

You deploy Billing Care on a JRF-enabled Oracle WebLogic Server domain configured as an Oracle Platform Security Services (OPSS) client domain. Create a JRF-enabled domain in Oracle WebLogic Server and configure an application domain policy that controls access to the Billing Care application.

For creating the domain and configuring the domain policy, see ["Configuring the Oracle Fusion Middleware Infrastructure Domain"](#) in *Oracle Fusion Middleware Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

- 2.

3. In the **config.xml** file, set this entry to **false**. This configures WebLogic Server to skip basic authentication.

```
<domain>
  <security-configuration>
    <!-- Other configurations -->
    <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-
auth-credentials>
  </security-configuration>
</domain>
```

## Configuring OAuth Settings Using Oracle Access Management

To configure OAuth to connect to your BRM server using Oracle Access Management:

1. Open the *User\_home/Infranet.properties* file in a text editor, where *User\_home* is the domain administrative user's home directory.
2. Add this entry:

```
idp.vendor=OAM
idp.url=OAM_hostname:port
idp.resource_server.scope=ResourceServer.ScopeName
idp.identity_domain=IdentityDomain
```

where:

- *OAM\_hostname:port* is the host and port number of the Oracle Access Manager Managed Server that is running the **oam\_server** application.
  - *Resourceserver.Scopename* is the name of the resource server followed by the name of the scope.
  - *IdentityDomain* is the name of your identity domain.
3. Save and close the file.

## Requesting an OAuth Access Token

To request an OAuth access token, use cURL to send an HTTP/HTTPS request to the Billing Care REST API authorization endpoint. For example:

```
curl --location --request GET 'http://hostname:port/bcws/webresources/v1.0/
authentication/queryAccessToken' \
  --header 'Authorization: Basic credentials'
```

where:

- *hostname:port* is the IP address or host name and port of the Billing Care REST API server.
- *credentials* is the Base64-encoded value of your IDCS administrator user name and password joined by a single colon (*username:password*).

If the request is successful, the token type, expiry time, and access token are returned. For example:

```
{
  "expires_in": 3600,
```

```
"token_type": "Bearer",  
"access_token": "accessToken"  
}
```

The token expires after the number of seconds shown in **expires\_in**. This value is set while setting up the OAuth identity domain as described in "[Configuring OAuth Settings Using Oracle Access Management](#)". After the token expires, you must request a new one.

You use the token in the Authorization header for each REST request with the following format:

```
-H "Authorization: Bearer accessToken"
```

# 9

## BRM REST Services Manager Security

Learn how to implement the security capabilities supported by BRM REST Services Manager. Oracle Communications Billing and Revenue Management (BRM) REST Services Manager supports stringent authorization and authentication requirements.

Topics in this document:

- [About Authentication and Authorization](#)
- [Setting Up OAuth with Oracle Identity Cloud Service](#)
- [Setting Up OAuth using Oracle Access Management](#)
- [Scopes and Roles for Accessing REST Services Manager](#)

For more information, see *REST Services Manager API for Billing and Revenue Management*.

### About Authentication and Authorization

BRM REST Services Manager uses the OAuth 2.0 protocol to authenticate a client application's identity and to authorize the client application to access its REST API and SDK. It does this by validating an OAuth access token that is passed in the header of the client's HTTP/HTTPS request to BRM REST Services Manager.

Your client must pass this OAuth access token in the header of every HTTP/HTTPS request sent to BRM REST Services Manager.

To set up authentication and authorization for your client, you can use either Oracle Identity Cloud Service or Oracle Access Management.

### Setting Up OAuth with Oracle Identity Cloud Service

You can set up your client application to use two-legged or three-legged OAuth authentication to access the BRM REST Services Manager API. Three-legged OAuth authentication allows the resource owner to give the client application access to the resource server without sharing its credentials. In two-legged authentication, the client application uses the resource owner's credentials to access the resource server.

To set up three-legged OAuth authentication using Oracle Identity Cloud Service, perform all of the following steps. To set up two-legged OAuth authentication, skip steps 2 and 3.

1. [Creating Confidential OAuth Applications](#)
2. [Assigning Users to Groups \(3-Legged OAuth Only\)](#)
3. [Generating an Authorization Code \(3-Legged OAuth Only\)](#)
4. [Encoding the Client ID and Client Secret in Base64 Format](#)
5. [Requesting an OAuth Access Token](#)

If you are using three-legged OAuth authentication, you can refresh your access token after it expires. See "[Refreshing OAuth Access Tokens \(3-Legged OAuth Only\)](#)".

## Creating Confidential OAuth Applications

When you create a confidential OAuth application in Identity Cloud Service, it provides you with a client ID and client secret. Your client will need the client ID and client secret to request OAuth access tokens for accessing the BRM REST Services Manager API.

To create a confidential OAuth application in Identity Cloud Service:

1. In the Identity Cloud Service console, expand the **Navigation Drawer** and then click **Applications**.
2. Click **Add**.
3. In the **Add Application** page, click **Confidential Application**.
4. In the **App Details** page, enter a name for your application, such as **MyClient**, and then click **Next**.
5. In the **Client** page, select **Configure this application as a client now**.
6. In the Authorization section, enter the following information:
  - In the **Allowed Grant Types** field, select **Client Credentials**, **JWT Assertion**, **Refresh Token**, and **Authorization Code**.
  - Select the **Allow non-HTTPS URLs** option.
  - In the **Redirect URL** field, enter the application URL where the user is redirected after authentication.
  - In the **Client Type** field, select **Confidential**.
  - In the **Allowed Operations** field, select **Introspect**.

This figure shows how to set the fields in the Authorization section:

Allowed Grant Types  Resource Owner  Client Credentials  JWT Assertion  SAML2 Assertion  Refresh Token  Authorization Code  Implicit  Device Code

Allow non-HTTPS URLs

\* Redirect URL

Logout URL

Post Logout Redirect URL

\* Client Type  Trusted  Confidential  Public


Certificate

Allowed Operations  Introspect  On behalf Of

Bypass Consent

7. In the Token Issuance Policy section, do the following:
  - a. In the **Authorized Resources** field, select **Specific**.
  - b. Under **Grant the client access to Identity Cloud Service Admin APIs**, select **Add**.
  - c. In the Add App Role dialog box, select the following:
    - **Application Administrator**
    - **Identity Domain Administrator**



- **User Administrator**
- d. Click **Add**.
  8. Click **Next**.
  9. In the **Resources** page, select **Configure this application as a resource server now**.
  10. In the Configure application APIs that need to be OAuth protected section, do the following:
    - a. In the **Access Token Expiration** field, enter how long (in seconds) the access token remains valid. For example, enter **3600** for 1 hour.
    - b. Select the **Is Refresh Token Allowed** option.
    - c. In the **Refresh Token Expiration** field, enter how long (in seconds) the refresh token, which is returned with your access token and is associated with your confidential application, remains valid.
    - d. In the **Primary Audience** field, enter the primary recipient where the access token of your confidential application is processed.
    - e. Next to **Scopes**, click **Add**.
    - f. In the Add Scope dialog box, add these scopes: **BillingAgent** and **BillingViewer**.
  11. Click **Back** to return to the **Resources** page.
  12. In the Token Issuance Policy section of the **Resources** page, do the following:
    - a. Under Resources, click **Add Scope**.
    - b. In the Select Scope dialog box, next to the name of your application, select the  icon.
    - c. Select the **BillingAgent** and **BillingViewer** scopes.
    - d. Click **Add**.
  13. Click **Next** to advance to the **Resources** page.
  14. Click **Next** again to advance to the **Authorization** page.
  15. Click **Finish**.
  16. In the **Application Added** pop-up window, make note of the client ID and client secret. You will provide this to the person who needs to generate the OAuth access token.
  17. Click **Close**.
  18. At the top right of the application page, select **Activate** and then click **OK** to confirm the activation.
  19. Provide the following to the person who needs to generate the OAuth access token:
    - The Identity Cloud Service URLs for generating authorization codes and requesting access tokens. For example:

```
https://idcs_hostname/oauth2/v1/authorize
```

```
https://idcs_hostname/oauth2/v1/token
```

where *idcs\_hostname* is the hostname of the server of your Identity Cloud Service instance

- The redirect URL to send authorization codes and access tokens to
- The client ID and client secret

## Assigning Users to Groups (3-Legged OAuth Only)

If your client application is using three-legged OAuth authentication, users are granted access to the BRM REST Services Manager API through Oracle Identity Cloud Service groups. To grant users access, you first create the groups in Identity Cloud Service and then assign users to those groups.

To create the **Billing Viewer** and **Billing Agent** groups in Identity Cloud Service:

1. In the Identity Cloud Service console, expand the **Navigation Drawer** and then click **Groups**.
2. In the top left, click **Add**.
3. In the Add Group dialog box, in the **Name** field, enter **Billing Agent**.
4. Click **Finish**.
5. In the top left, click **Add** again.
6. In the Add Group dialog box, in the **Name** field, enter **Billing Viewer**.
7. Click **Finish**.

To assign users to the appropriate group for accessing the BRM REST Services Manager API:

1. In the Identity Cloud Service console, expand the **Navigation Drawer** and then click **Users**.
2. Select a user that needs access to the BRM REST Services Manager API.
3. In the user's page, select **Groups** at the top left.
4. In the Groups page, click **Assign**.
5. In the Assign Groups dialog box, select **Billing Agent**, **Billing Viewer**, or both. For more information about the groups, see "[Scopes and Roles for Accessing REST Services Manager](#)".
6. Click **OK**.

## Generating an Authorization Code (3-Legged OAuth Only)

If you are using three-legged OAuth authentication, you must include an authorization code in your request for an OAuth access token. To generate an authorization code, use a browser to send an HTTP/HTTPS request to the Identity Cloud Service URL:

```
https://idcs_hostname/oauth2/v1/authorize?  
client_id=client_id&response_type=code&redirect_uri=redirect_url&scope=  
BillingAgent BillingView all offline_access
```

where:

- *idcs\_hostname* is the hostname of your Identity Cloud Service instance.
- *client\_id* is the client ID generated by Identity Cloud Service when you create a confidential application.

- `redirect_url` is the URL for your application.

The authorization code is returned with the parameter named "code" in the redirect URL. Make a note of the authorization code so it can be used to request OAuth access tokens.

For more information, see "[Generate Authorization Code and Identity Token \(3-legged OAuth Flow\)](#)" in *REST API for Oracle Identity Cloud Service*.

## Encoding the Client ID and Client Secret in Base64 Format

Before you can request an OAuth access code, you must encode your client ID and client secret in Base64 format. Generate a base64-encoded value of your client ID and client secret joined by a single colon (*ClientID:ClientSecret*).

You pass the base64-encoded value in the header of your HTTP/HTTPS request for an OAuth access code.

## Requesting an OAuth Access Token

To request an OAuth access token, use cURL to send an HTTP/HTTPS request to the Identity Cloud Service URL. The cURL syntax you use depends on whether you are using two-legged or three-legged OAuth authentication.

- For two-legged OAuth authentication, use this cURL syntax:

```
curl -i
-H "Authorization: Basic encoded_client"
-H "Content-Type: application/x-www-form-urlencoded;charset=UTF-8"
--request POST https://idcs_hostname/oauth2/v1/token
-d 'grant_type=client_credentials&scope=BillingAgent BillingView all'
```

- For three-legged OAuth authentication, include the authorization code in your HTTP/HTTPS request:

```
curl -i
-H "Authorization: Basic encoded_client"
-H "Content-Type: application/x-www-form-urlencoded;charset=UTF-8"
--request POST https://idcs_hostname/oauth2/v1/token
-d
"redirect_uri=redirect_url&grant_type=authorization_code&code=authorizatio
n_code"
```

where:

- `encoded_client` is the base64-encoded client ID and client secret that you created in "[Encoding the Client ID and Client Secret in Base64 Format](#)".
- `idcs_hostname` is the hostname of your Identity Cloud Service instance.
- `redirect_url` is the URL for your application.
- `authorization_code` is the authorization code returned in "[Generating an Authorization Code \(3-Legged OAuth Only\)](#)".

After you submit the request, Identity Cloud Service returns an OAuth access token.

Identity Cloud Service also returns a refresh token if the following are true:

- You are using three-legged OAuth authentication.
- Your OAuth client allows the **Refresh Token** grant type.
- You included the **offline\_access** scope in your request for an authorization code.

The OAuth access token and refresh token returned from the request follows this syntax:

```
{
  "access_token":"access_token",
  "token_type":"Bearer","expires_in":3600,
  "refresh_token":"refresh_token"
}
```

For more information, see ["Generate Access Token and Other OAuth Runtime Tokens to Access the Resource"](#) in *REST API for Oracle Identity Cloud Service*.

## Refreshing OAuth Access Tokens (3-Legged OAuth Only)

If you are using three-legged OAuth authentication, you can refresh your access token. To do so, use cURL to send an HTTP/HTTPS request to the Identity Cloud Service URL:

```
curl -H 'Authorization: Basic encoded_client' -H "Content-Type:application/x-www-form-urlencoded;charset=UTF-8"
--request POST https://idcs_hostname/oauth2/v1/token -d
'grant_type=refresh_token&refresh_token=refresh_token'
```

where:

- *encoded\_client* is the base64-encoded client ID and client password that you created in ["Encoding the Client ID and Client Secret in Base64 Format"](#).
- *idcs\_hostname* is the hostname of your Identity Cloud Service instance.
- *refresh\_token* is the refresh token that was returned when you requested an access token in ["Requesting an OAuth Access Token"](#).

For more information, see ["Generate Access Token and Other OAuth Runtime Tokens to Access the Resource"](#) in *REST API for Oracle Identity Cloud Service*.

## Setting Up OAuth using Oracle Access Management

Setting up OAuth using Oracle Access Management involves these high-level steps:

1. Installing the Oracle Access Management software. For the list of supported versions, see "Additional BRM Software Requirements" in *BRM Compatibility Matrix*.  
For more information about installing the Oracle Access Management software, see [Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management](#).
2. Installing the Oracle Unified Directory software with the HTTP port enabled. For the list of supported versions, see "Additional BRM Software Requirements" in *BRM Compatibility Matrix*.

For more information about installing Oracle Unified Directory, see [Oracle Fusion Middleware Installing Oracle Unified Directory](#).

3. [Enabling OAuth Services](#)
4. [Creating an OAuth Identity Domain](#)
5. [Creating a Resource Server](#)
6. [Creating an OAuth Client](#)
7. Create an access token using either two-legged or three-legged OAuth authentication:
  - [Using Two-Legged OAuth to Create an Access Token](#)
  - [Using Three-Legged OAuth to Create an Access Token](#)



#### Note:

If you use both BRM REST Services Manager and PDC REST Services Manager, you must set up separate OAuth identity domains, resource servers, and clients for each component.

## Enabling OAuth Services

To enable OAuth services in Oracle Access Manager:

1. In the Oracle Access Manager Console, click **Configuration** at the top of the window.
2. Click **Available Services**.
3. Confirm that the **Access Manager** service is enabled.
4. In the **OAuth Service** row, click **Enable Service**.
5. In the **OpenIDConnect Service** row, click **Enable Service**.

For more information, see "[Managing Common Services and Certificate Validation](#)" in *Oracle Fusion Middleware Administering Oracle Access Management*.

## Creating an OAuth Identity Domain

You create an OAuth identity domain to control the authentication and authorization of users who can sign in to BRM REST Services Manager, and what features they can access. You create all artifacts, such as the resource server and OAuth client, under the identity domain.

To create an identity domain, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL:

```
curl -i --header 'Content-Type: application/json'
--header 'Authorization:Basic encoded_admin'
--header 'Cookie:
JSESSIONID=Ax_wYZQ2svzaTYpH5Gwz4KTwqfD2toL1tEi2hzkuTSAK8KVuf0aw!642164469'
--request POST http://:oam_host:oam_port/oam/services/rest/ssa/api/v1/
oauthpolicyadmin/oauthidentitydomain
--data-raw
'{"name":"identity_domain","identityProvider":"identity_store","description":
"My Identity Domain",
```

```
{ "tokenType": "AUTHZ_CODE", "tokenExpiry": 3600, "lifeCycleEnabled": false, "refreshTokenEnabled": false, "refreshTokenExpiry": 86400, "refreshTokenLifeCycleEnabled": false },
{ "tokenType": "SSO_LINK_TOKEN", "tokenExpiry": 3600, "lifeCycleEnabled": false, "refreshTokenEnabled": false, "refreshTokenExpiry": 86400, "refreshTokenLifeCycleEnabled": false }'
```

where:

- *encoded\_admin* is the base64-encoded format of the Oracle Access Management administrator user name and password.
- *oam\_host:oam\_port* is the host name and port for the Oracle Access Management server.
- *identity\_domain* is the name of the Oracle Access Management identity domain that you want to create.
- *identity\_store* is set to your Oracle Unified Directory.

The following shows an example cURL command for creating an identity domain named **TMF\_ID\_Domain** with the identity store set to **ODU**:

```
curl -i --header 'Content-Type: application/json'
--header 'Authorization: Basic encoded_admin'
--header 'Cookie:
JSESSIONID=Ax_wYZQ2svzaTYpH5Gwz4KTWqfD2toL1tEi2hzkuTSAK8KVuf0aw!
642164469'
--request POST 'http://oam_host:oam_port/oam/services/rest/ssa/api/v1/
oauthpolicyadmin/oauthidentitydomain'
--data-raw
'{"name": "TMF_ID_Domain", "identityProvider": "ODU", "description": "My
Identity Domain",
"tokenSettings":
[{"tokenType": "ACCESS_TOKEN", "tokenExpiry": 3600, "lifeCycleEnabled": false, "refreshTokenEnabled": false, "refreshTokenExpiry": 86400, "refreshTokenLifeCycleEnabled": false},
{"tokenType": "AUTHZ_CODE", "tokenExpiry": 3600, "lifeCycleEnabled": false, "refreshTokenEnabled": false, "refreshTokenExpiry": 86400, "refreshTokenLifeCycleEnabled": false},
{"tokenType": "SSO_LINK_TOKEN", "tokenExpiry": 3600, "lifeCycleEnabled": false, "refreshTokenEnabled": false, "refreshTokenExpiry": 86400, "refreshTokenLifeCycleEnabled": false}],
"errorPageURL": "/oam/pages/servererror.jsp", "consentPageURL": "/oam/
pages/consent.jsp"}'
```

If the identity domain was created successfully, you will see a response similar to this:

```
Successfully created entity - OAuthIdentityDomain, detail - OAuth
Identity Domain :: Name - TMF_ID_Domain, Id -
19f85bc53b49561ea52f039474c2c4b, Description - My
Identity Domain, TrustStore Identifiers - TMF_ID_Domain, Identity
Provider - ODU, TokenSettings -
[{"tokenType": "ACCESS_TOKEN", "tokenExpiry": 3600, "lifeCycleEnabled": false, "refreshTokenEnabled": false, "refreshTokenExpiry": 86400, "refreshTokenLifeCycleEnabled": false},
```

```

{"tokenType":"AUTHZ_CODE","tokenExpiry":3600,"lifeCycleEnabled":false,"refreshTokenEnabled":false,"refreshTokenExpiry":86400,"refreshTokenLifeCycleEnabled":false},
{"tokenType":"SSO_LINK_TOKEN","tokenExpiry":3600,"lifeCycleEnabled":false,"refreshTokenEnabled":false,"refreshTokenExpiry":86400,"refreshTokenLifeCycleEnabled":false}],
ConsentPageURL - /oam/pages/consent.jsp, ErrorPageURL - /oam/pages/servererror.jsp, CustomAttrs - null

```

## Creating a Resource Server

A resource server hosts the protected resources. It must be capable of accepting and responding to resource requests using OAuth access tokens.

To create a resource server, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL:

```

curl -k -u wls_admin:password -H 'Content-Type: application/json' 'http://oam_host:oam_port/oam/services/rest/ssa/api/v1/oauthpolicyadmin/application' -d '{"name":"resource_server","description":"TestResourceServer", "scopes":[{"scopeName":"scope1","description":"Scope1 description"}, {"scopeName":"scope2","description":"Scope2 sescription"}, {"scopeName":"scope3","description":"Scope3 description"}], "tokenAttributes":[{"attrName":"sessionId","attrValue":"$session.id","attrType":"DYNAMIC"}, {"attrName":"resSrvAttr","attrValue":"RESOURCECONST","attrType":"STATIC"}],"idDomain":"TestDomain1","audienceClaim":{"subjects":["ab0"]}}'

```

where:

- *wls\_admin:password* is the Admin user name and password for WebLogic Server.
- *resource\_server* is the name of the resource server that you want to create.
- *scopeN* is the name of a scope. After the scopes are defined under the resource server, refer to them as *resource\_server.scope*. For example: *TMFResourceServer.BillingAgent*. For information about the scopes, see ["Scopes and Roles for Accessing REST Services Manager"](#).

The following shows an example of creating a resource server named **TMFResourceServer** with the **BillingAgent** and **BillingViewer** scopes, an identity domain named **TMF\_ID\_Domain**, and static and dynamic customer attributes:

```

curl -k -u wls_admin:password -H 'Content-Type: application/json' 'http://oam_host:oam_port/oam/services/rest/ssa/api/v1/oauthpolicyadmin/application' -d '{"name":"TMFResourceServer","description":"Resource Server", "scopes":[{"scopeName":"BillingAgent","description":"Scope for CSR with BillingAgent Role"}, {"scopeName":"BillingViewer","description":"Scope for CSR with BillingViewer Role"}], "tokenAttributes":[{"attrName":"sessionId","attrValue":"$session.id","attrType":"DYNAMIC"}, {"attrName":"resSrvAttr","attrValue":"RESOURCECONST","attrType":"STATIC"}],"idDomain":"TMF_ID_Domain","audienceClaim":{"subjects":["ab0"]}}'

```

If the resource server is created successfully, you will see a response similar to this:

```
Sucessfully created entity - OAuthResourceServer, detail -
IdentityDomain="TMF_ID_Domain",Name="TMFResourceServer",Description="Re
source Server",
resourceServerId="4953a4f4-8c3f-41fd-99b5-837cfa9f9ecb",resourceServerN
amespacePrefix="TMFResourceServer.",audienceClaim="{\"subjects\":
[\"ab0\"]}",
resServerType="CUSTOM_RESOURCE_SERVER",Scopes="[{"scopeName":"BillingAg
ent","description":"Scope for CSR with BillingAgent Role"},
{"scopeName":"BillingAgent","description":"Scope for CSR with
BillingAgent Role"}, {"scopeName":"BillingViewer","description":"Scope
for CSR with BillingViewer Role"},}],
tokenAttributes="[{"attrName":"sessionId","attrValue":"$session.id","at
trType":DYNAMIC},
{"attrName":"resSrvAttr","attrValue":"RESOURCECONST","attrType":STATIC}
]
```

## Creating an OAuth Client

To create an OAuth client, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL:

```
curl -k -u wls_admin:password -H 'Content-Type: application/json'
'http://oam_host:oam_port/oam/services/rest/ssa/api/v1/
oauthpolicyadmin/client'
-d {"attributes":
[{"attrName":"custom_attribute","attrValue":"custom_value","attrType":"
static"}],
"secret":"client_secret","id":"clientID","scopes":
["resource_server.scopel1"],"clientType":"CONFIDENTIAL_CLIENT",
"idDomain":"identity_domain","description":"Client
Description","name":"client_name","grantTypes":
["PASSWORD","CLIENT_CREDENTIALS","JWT_BEARER","REFRESH_TOKEN","AUTHORIZ
ATION_CODE"],
"defaultScope":"resource_server.scopel1","redirectURIs":[{"url":"http://
redirect_host:redirect_port/Sample.jsp","isHttps":true}]}
```

where:

- *custom\_attribute* and *custom\_value* are custom attribute names and values. You can optionally define a set of static and dynamic custom attributes, which will then be added as custom attributes to the OAuth access token.
- *client\_id* and *client\_secret* are the client ID and client secret.
- *client\_name* is the name of the OAuth client that you want to create.
- *redirect\_host:redirect\_port* is the URL for your client application.

The following shows an example cURL request for creating a confidential OAuth client named **TMFClient** with the **TMFResourceServer:BillingAgent** (default) and



**TMFResourceServer:BillingViewer** scopes, and an identity domain named **TMF\_ID\_Domain**.

```
curl -k -u wls_admin:password -H 'Content-Type: application/json' 'http://
oam_host:oam_port/oam/services/rest/ssa/api/v1/oauthpolicyadmin/client'
-d '{"attributes": [{"attrName": "customAttribute1", "attrValue": "Custom
Value1", "attrType": "static"},
{"attrName": "customAttribute2", "attrValue": "Custom
Value2", "attrType": "static"}],
"secret": "client_secret", "id": "client_id", "scopes":
["TMFResourceServer.BillingAgent", "TMFResourceServer.BillingViewer"], "clientT
ype": "CONFIDENTIAL_CLIENT",
"idDomain": "TMF_ID_Domain", "description": "Client entry for identity
domain", "name": "TMFClient", "grantTypes":
["PASSWORD", "CLIENT_CREDENTIALS", "JWT_BEARER", "REFRESH_TOKEN", "AUTHORIZATION_
CODE"]},
"defaultScope": "TMFResourceServer.BillingAgent", "redirectURIs":
[{"url": "http://redirect_host:redirect_port/oauth/
callback", "isHttps": true}]}'
```

If the client is created successfully, the response will be similar to this:

```
Successfully created entity - OAuthClient, detail - OAuth Client - uid =
4b37dd63-08dd-45b5-b5a5-c1e788cb2ff2, name = TMFClient, id = TMFClientId,
identityDomain = TMF_ID_Domain, description = Client entry for TMF OAuth
Domain, secret = TMFPassword, clientType = CONFIDENTIAL_CLIENT, grantTypes =
[PASSWORD,
CLIENT_CREDENTIALS, JWT_BEARER, REFRESH_TOKEN, AUTHORIZATION_CODE],
attributes =
[{"attrName": "customAttribute1", "attrValue": "Custom
Value1", "attrType": STATIC},
{"attrName": "customAttribute2", "attrValue": "Custom
Value2", "attrType": STATIC},
{"attrName": "sessionId", "attrValue": "session.id", "attrType": DYNAMIC},
{"attrName": "resSrvAttr", "attrValue": "RESOURCECONST", "attrType": STATIC}],
scopes =
[TMFResourceServer.BillingAgent, TMFResourceServer.BillingViewer],
defaultScope = TMFResourceServer.BillingAgent, redirectURIs =
[{"url": "http://redirect_host:redirect_port/oauth/callback", "isHttps": true}]
```

## Using Two-Legged OAuth to Create an Access Token

You create an access token for two-legged OAuth authentication by using the Oracle Access Management OAuth REST API. You submit a request by using its **Create Access Token Flow** endpoint. For more information, see [REST API for OAuth in Oracle Access Manager](#).

To request an OAuth access token, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL:

```
curl -i --header 'Authorization: Basic encoded_admin' \
--header "Content-Type: application/x-www-form-
urlencoded; charset=UTF-8" \
--header "X-OAUTH-IDENTITY-DOMAIN-NAME: identity_domain" \
```

```
--request POST http://oam_host:oam_port/oauth2/rest/token \
--data-
urlencode "grant_type=CLIENT_CREDENTIALS&scope=resource_server.scope"
```

The following shows an example cURL request for creating a creating OAuth access token for the **TMF\_ID\_Domain** identity domain, **TMFResourceServer** resource server, and **BillingAgent** scope:

```
curl --location --header 'Authorization: Basic encoded_admin' \
--header "Content-Type: application/x-www-form-
urlencoded;charset=UTF-8" \
--header "X-OAUTH-IDENTITY-DOMAIN-NAME: TMF_ID_Domain" \
--request POST http://oam_host:oam_port/oauth2/rest/token \
--data-urlencode
"grant_type=CLIENT_CREDENTIALS&scope=TMFResourceServer.BillingAgent"
```

If the request is successful, Oracle Access Management returns something similar to this:

```
{
  "access_token":"access_token",
  "token_type":"Bearer",
  "expires_in":3600
}
```

Your client must pass this OAuth access token in the header of every HTTP/HTTPS request sent to the BRM REST Services Manager.

## Using Three-Legged OAuth to Create an Access Token

You create an access token for three-legged OAuth authentication by doing the following:

1. Creating protected resources in the Oracle Access Management server. See ["Creating Resources in the Oracle Access Management Server"](#).
2. Modifying the WebGate `mod_wl_ohs.conf` file so the Oracle HTTP server can connect to the WebLogic Server. See ["Configuring the Oracle HTTP Server"](#).
3. Generating an OAuth access token. See ["Generating the OAuth Access Token"](#).

## Creating Resources in the Oracle Access Management Server

In three-legged OAuth authentication, you must create resources in the Oracle Access Management server for protecting the consent page and approval page. If you customize the consent page, it must be protected by a Webgate.

To create resources on your Oracle Access Management server:

1. In the Oracle Access Management Console, click **Application Security**.
2. In the Application Security console, click **Application Domains**.
3. Search for and open your application domain.
4. Click the **Resources** tab.

5. Create a protected resource named **/oauth2/rest/approval**. This has to be protected by WebGate.  
Click **Create**, do the following in the **Create Resource** screen, and then click **Apply**:
  - **Resource URL**: Enter **/oauth2/rest/approval**.
  - **Operations Available**: Select **POST**.
  - **Protection Level**: Select **Protected**.
  - **Authentication Policy**: Select **Protected HigherLevel Policy**.
  - **Authorization Policy**: Select **Protected Resource Policy**.
6. Create a protected resource named **/oam/pages/consent.jsp**. If you are using a custom consent page, it needs to be protected by Webgate and the appropriate resource has to be added here.  
Click **Create**, do the following in the **Create Resource** screen, and then click **Apply**:
  - **Resource URL**: Enter **/oam/pages/consent.jsp**.
  - **Operations Available**: Select **GET**.
  - **Protection Level**: Select **Protected**.
  - **Authentication Policy**: Select **Protected Resource Policy**.
  - **Authorization Policy**: Select **Protected Resource Policy**.
7. Create an excluded resource named **/oauth2/rest/\*\***.  
Click **Create**, do the following in the **Create Resource** screen, and then click **Apply**:
  - **Resource URL**: Enter **/oauth2/rest/\*\***.
  - **Protection Level**: Select **Excluded**.
8. Create an excluded resource named **/oam/\*\***.  
Click **Create**, do the following in the **Create Resource** screen, and then click **Apply**:
  - **Resource URL**: Enter **/oam/\*\***.
  - **Operations Available**: Select **ALL**.
  - **Protection Level**: Select **Excluded**.

## Configuring the Oracle HTTP Server

To configure the Oracle HTTP Server for WebLogic Server, modify the WebGate **mod\_wl\_ohs.conf** file:

1. Open the **OHS\_home/user\_projects/domains/base\_domain/config/fmwconfig/components/OHS/OHS\_InstanceName/mod\_wl\_ohs.conf** file in a text editor.

where:

- **OHS\_home** is the path to the Oracle HTTP Server directory.
  - **OHS\_InstanceName** is the name of your Oracle HTTP Server instance.
2. Add the following entries to the file:

```
<Location /oauth2>
  SetHandler weblogic-handler
  WebLogicHost ManagedServerHostName
```

```

    WebLogicPort ManagedServerPort
    ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
</Location>

<Location /oam>
    SetHandler weblogic-handler
    WebLogicHost ManagedServerHostName
    WebLogicPort ManagedServerPort
    ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
</Location>

```

3. Save and close the file.

## Generating the OAuth Access Token

Generating an OAuth access token is a two-step process. First, you retrieve an authorization code from Oracle Access Manager. Then, you include the authorization code in a request to the Oracle Access Manager REST API for an OAuth access token.

To generate an OAuth access token:

1. Open the following URL in a browser:  
**`http://OHS_host:OHS_port/oauth2/rest/authorize?response_type=code&domain=identity_domain&client_id=client_name&scope=resource_server.BillingAgent&state=code1234&redirect_uri=http://redirect_host:redirect_port/oauth/callback`**
2. Enter your user credentials in the Oracle Access Manager login screen.
3. Click **Allow**.
4. Copy the authorization code from the browser URL.
5. Generate the OAuth access token by submitting a cURL request to the **Create Access Token Flow** endpoint in the Oracle Access Manager OAuth REST API. For example:

```

curl --location --request POST 'http://oam_host:oam_port/14100/oauth2/rest/token' \
  --header 'X-OAUTH-IDENTITY-DOMAIN-NAME: identity_domain' \
  --header 'Authorization: Basic encoded_admin' \
  --header 'Content-Type: application/x-www-form-urlencoded' \
  --data-urlencode 'grant_type=AUTHORIZATION_CODE' --data-urlencode 'code=authorization_code' \
  --data-urlencode 'redirect_uri=http://redirect_host:redirect_port/oauth/callback'

```

For more information, see [REST API for OAuth in Oracle Access Manager](#).

## Scopes and Roles for Accessing REST Services Manager

For two-legged OAuth authentication, use the scopes in [Table 9-1](#) to control access to the REST Services Manager API and SDK.

**Table 9-1 Scopes for BRM REST Services Manager**

Scope Name	Description
<b>BillingAgent</b>	Authorizes access to all BRM REST Services Manager APIs.
<b>BillingViewer</b>	Authorizes only GET requests for all BRM REST Services Manager endpoints.

For three-legged OAuth authentication, use the roles (groups) listed in [Table 9-2](#) to control access to the REST Services Manager API and SDK.

**Table 9-2 Roles for BRM REST Services Manager**

Role Name	Description
<b>Billing Agent</b>	Authorizes access to all BRM REST Services Manager APIs.
<b>Billing Viewer</b>	Authorizes only GET requests for all BRM REST Services Manager endpoints.

# PDC REST Services Manager Security

Learn how to set up security for Oracle Communications Pricing Design Center (PDC) REST Services Manager.

Topics in this document:

- [About PDC REST Services Manager Security](#)
- [Setting Up OAuth for PDC REST Services Manager with Oracle Identity Cloud Service](#)
- [Setting Up OAuth for PDC REST Services Manager with Oracle Access Management](#)
- [Securing Inbound Communications](#)
- [Securing Outbound Requests to PDC](#)
- [Encrypting Sensitive Data](#)
- [PDC REST Services Manager Security Configuration Reference Information](#)

For more information, see *PDC REST Services Manager Integration Guide*.

## About PDC REST Services Manager Security

PDC REST Services Manager uses the following security protocols to secure inbound and outbound requests:

- **OAuth 2.0:** Authenticates your enterprise product catalog's identity and authorizes it to access the PDC REST Services Manager API by validating an OAuth access token that is passed in the header of every HTTP/HTTPS request to the PDC REST Services Manager API.  
You can enable OAuth for PDC REST Services Manager using either Oracle Identity Cloud Service or Oracle Access Management.
- **TLS:** Secures communication from your enterprise product catalog to PDC REST Services Manager.
- **T3S:** Secures communication from PDC REST Services Manager to PDC.

Setting up PDC REST Services Manager security involves these tasks:

1. One of the following, depending on your OAuth provider:
  - [Setting Up OAuth for PDC REST Services Manager with Oracle Identity Cloud Service](#)
  - [Setting Up OAuth for PDC REST Services Manager with Oracle Access Management](#)
2. [Securing Inbound Communications](#)
3. [Securing Outbound Requests to PDC](#)

You can also encrypt sensitive data, such as passwords, by using the **RestServicesManager.sh** script. See "[Encrypting Sensitive Data](#)".

# Setting Up OAuth for PDC REST Services Manager with Oracle Identity Cloud Service

Setting up OAuth for PDC REST Services Manager with Oracle Identity Cloud Service involves these tasks:

1. [Creating Confidential OAuth Applications for PDC REST Services Manager](#)
2. [Setting Up Security with Oracle Identity Cloud Service in the PDC REST Services Manager Configuration File](#)
3. [Requesting an OAuth Access Token from Oracle Identity Cloud Service](#)

## Creating Confidential OAuth Applications for PDC REST Services Manager

Add your enterprise product catalog as a confidential application to IDCS by following the instructions in "[Add a Confidential Application](#)" in *Administering Oracle Identity Cloud Service*. When adding the confidential application, ensure that you:

- Select **Confidential** for the **Client Type** option.
- Add a scope named **pubevent** for accessing the Publish Event endpoint in PDC REST Services Manager.
- Add a scope named **metrics** for accessing the Metrics endpoint in PDC REST Services Manager.

After you add the confidential application, Oracle Identity Cloud Service provides you with the following information. You will need it when requesting an OAuth access token and when configuring inbound communication to PDC REST Services Manager:

- The Oracle Identity Cloud Service URL for requesting OAuth access tokens. For example:

```
https://idcs_hostname/oauth2/v1/token
```

where *idcs\_hostname* is the hostname of the server of your Oracle Identity Cloud Service instance

- The primary audience URL
- The client ID and client secret. Encode these in base-64 before using them to request OAuth access tokens.

## Setting Up Security with Oracle Identity Cloud Service in the PDC REST Services Manager Configuration File

To set the Oracle Identity Cloud Service details in the PDC REST Services Manager **application.yaml** file:

1. Open the *PDC\_RSM\_home/apps/conf/application.yaml* file in a text editor, where *PDC\_RSM\_home* is the directory in which you installed PDC REST Services Manager.

- Set the keys under **security** as shown in [Table 10-1](#).

**Table 10-1 Security Keys in the application.yaml File**

Key	Description
<b>config.require-encryption</b>	Controls whether requests require encryption using <b>client_id</b> and <b>client_secret</b> . Set this to <b>true</b> .
<b>enabled</b>	Enables or disables security. Enable security in production environments by setting this to <b>true</b> .
<b>properties.idcs-uri</b>	The base URL of your Oracle Identity Cloud Service instance in this format: <b>https://idcs-TenantID.identity.oraclecloud.com</b>
<b>properties.idcs-client-id</b>	The client ID for your confidential application.
<b>properties.idcs-client-secret</b>	The Base64-encrypted client secret obtained from your Oracle Identity Cloud Service application. For security purposes, do not store the client secret in plain-text. To encrypt the client secret, see " <a href="#">Encrypting Sensitive Data</a> ".
<b>properties.frontend-uri</b>	The base URL of your confidential application when run. For example: <b>http://localhost:8080</b>
<b>properties.audience</b>	The primary audience as provisioned for the PDC REST Services Manager application in Oracle Identity Cloud Service. For example: <b>http://localhost:8080/</b> <b>Note:</b> Ensure that you include the trailing slash in the URL.
<b>properties.proxy-host</b>	The hostname of the proxy server, if required.
<b>web-server.paths.&lt;0&gt;.abac.scopes</b>	The scope defined in Oracle Identity Cloud Service for protecting the TMF620 <b>publishEvent</b> endpoint.
<b>web-server.paths.&lt;1&gt;.abac.scopes</b>	The scope defined in Oracle Identity Cloud Service for protecting the <b>metrics</b> endpoint.

- In the providers section, ensure that the **oidc** and **abac** providers are not commented out. Comment out the **oamoidc** provider.
- In the **app.httpClients.security** section, set the keys based on the type of authentication required by your enterprise product catalog. These keys allow you to secure outbound requests from PDC REST Services Manager to your enterprise product catalog. See:
  - [OAuth Configuration Properties for Outbound Requests](#)
  - [Basic Authentication Configuration Properties for Outbound Requests](#)
- Save and close the **application.yaml** file. See "[Example application.yaml Security Configuration with Oracle Identity Cloud Service](#)" for a sample file showing the appropriate properties.
- Restart PDC REST Services Manager by running the following command from the **PDC\_RSM\_home/apps/bin** directory:  
**./RestServicesManager.sh restart**



## Requesting an OAuth Access Token from Oracle Identity Cloud Service

Request an OAuth access token from Oracle Identity Cloud Service to include in requests to the PDC REST Services Manager APIs. For more information, see ["Generate Access Token and Other OAuth Runtime Tokens to Access the Resource"](#) in *REST API for Oracle Identity Cloud Service*.

To request an OAuth access token using cURL, use the following format for your HTTP/HTTPS request to the Oracle Identity Cloud Service URL:

```
curl -i
-H "Authorization: Basic encoded_credentials"
-H "Content-Type: application/x-www-form-urlencoded;charset=UTF-8"
--request POST https://idcs\_hostname/oauth2/v1/token
-d 'grant_type=client_credentials&scope=https://primaryAudience/scope'
```

where:

- *encoded\_credentials* is either the client ID and client secret (*clientID:clientSecret*) or user name and password (*username:password*) in Base64-encoded format.
- *idcs\_hostname* is the host name of your Oracle Identity Cloud Service instance.
- *primaryAudience* is the host name and port of your confidential application.
- *scope* is one of the following:
  - **pubevent**: Authorizes access to the Publish Event endpoint.
  - **metrics**: Authorizes access to the Metrics endpoint.

After you submit the request, Oracle Identity Cloud Service returns an OAuth access token. Your client must pass this OAuth access token in the header of every HTTP/HTTPS request sent to the PDC REST Services Manager.

## Setting Up OAuth for PDC REST Services Manager with Oracle Access Management

Setting up OAuth for PDC REST Services Manager using Oracle Access Management involves these high-level steps:

1. Installing the Oracle Access Management software. For the list of supported versions, see "Additional BRM Software Requirements" in *BRM Compatibility Matrix*.  
For more information about installing the Oracle Access Management software, see [Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management](#).
2. Installing the Oracle Unified Directory software with the HTTP port enabled. For the list of supported versions, see "Additional BRM Software Requirements" in *BRM Compatibility Matrix*.  
For more information about installing Oracle Unified Directory, see [Oracle Fusion Middleware Installing Oracle Unified Directory](#).

3. [Enabling OAuth Services for PDC REST Services Manager](#)
4. [Creating an OAuth Identity Domain for PDC REST Services Manager](#)
5. [Creating a Resource Server for PDC REST Services Manager](#)
6. [Creating an OAuth Client for PDC REST Services Manager](#)
7. [Setting Up Security with Oracle Access Management in the PDC REST Services Manager Configuration File](#)
8. [Requesting an OAuth Access Token from Oracle Access Management](#)



#### Note:

If you use both BRM REST Services Manager and PDC REST Services Manager, you must set up separate OAuth identity domains, resource servers, and clients for each component.

## Enabling OAuth Services for PDC REST Services Manager

Enable OAuth services in Oracle Access Management as described in "[Managing Common Services and Certificate Validation](#)" in *Oracle Fusion Middleware Administering Oracle Access Management*. Ensure that the following services are enabled:

- Access Manager
- OAuth
- OpenIDConnect

## Creating an OAuth Identity Domain for PDC REST Services Manager

You create an OAuth identity domain to control the authentication and authorization of users who can sign in to PDC REST Services Manager, and what features they can access. You create all artifacts, such as the resource server and OAuth client, under the identity domain.

To create an identity domain, submit a request to the **Add a new OAuth Identity Domain** endpoint of the Oracle Access Manager OAuth REST API. See "[Add a new OAuth Identity Domain](#)" in *REST API for OAuth in Oracle Access Manager* for more information about this endpoint.

The following shows an example cURL command for creating an identity domain named **PDC\_RSM\_Domain**, with the **OUD** identity provider (for Oracle Unified Directory):

```
curl -i --header 'Content-Type: application/json'
--header 'Authorization:Basic encoded_admin'
--request POST http://:oam_host:oam_port/oam/services/rest/ssa/api/v1/
oauthpolicyadmin/oauthidentitydomain
--data-raw
'{"name":"PDC_RSM_Domain","identityProvider":"OUD","description":"Identity
Domain for PDC REST Services Manager","tokenSettings":[
{"tokenType":"ACCESS_TOKEN","tokenExpiry":3600,"lifeCycleEnabled":false,"refr
eshTokenEnabled":false,"refreshTokenExpiry":86400,"refreshTokenLifeCycleEnabl
ed":false}]}'
```

where:

- *encoded\_admin* is the base64-encoded format of the Oracle Access Management administrator user name and password.
- *oam\_host:oam\_port* is the host name and port for the Oracle Access Management server.

If the identity domain was created successfully, you will see a response similar to this:

```
Successfully created entity - OAuthIdentityDomain, detail - OAuth
Identity Domain :: Name - PDC_RSM_Domain, Id -
19f85bc53b49561ea52f039474c2c4b,
Description - Identity Domain for PDC REST Services Manager,
TrustStore Identifiers - PDC_RSM_Domain, Identity Provider - OUD,
TokenSettings -
[{"tokenType":"ACCESS_TOKEN","tokenExpiry":3600,"lifeCycleEnabled":false,
"refreshTokenEnabled":false,"refreshTokenExpiry":86400,"refreshTokenLifeCycleEnabled":false}],
ConsentPageURL - /oam/pages/consent.jsp, ErrorPageURL - /oam/pages/
servererror.jsp, CustomAttrs - null
```

## Creating a Resource Server for PDC REST Services Manager

A resource server hosts the protected resources. It must be capable of accepting and responding to resource requests using OAuth access tokens.

To create a resource server, submit a request to the **Add a new Resource Server** endpoint of the Oracle Access Management OAuth REST API. See ["Add a new Resource Server"](#) in *REST API for OAuth in Oracle Access Manager* for more information about this endpoint.

The following shows an example of creating a resource server named **PDCRSMResourceServer** with the **all** and **read** scopes, an identity domain named **PDC\_RSM\_Domain**, and static and dynamic customer attributes:

```
curl -k -u wls_admin:password -H 'Content-Type: application/json'
'http://oam_host:oam_port/oam/services/rest/ssa/api/v1/
oauthpolicyadmin/application'
-d '{"name":"PDCRSMResourceServer","description":"Resource server for
PDC REST Services Manager",
"scopes":[{"scopeName":"all","description":"All permissions"},
{"scopeName":"read","description":"Read permissions"}],
"tokenAttributes":
[{"attrName":"sessionId","attrValue":"$session.id","attrType":"DYNAMIC"
},
{"attrName":"resSrvAttr","attrValue":"RESOURCECONST","attrType":"STATIC"
}], "idDomain":"PDC_RSM_Domain","audienceClaim":{"subjects":["ab0"]}]'
```

where:

- *wls\_admin:password* is the administrator user name and password for Oracle WebLogic Server.
- *resource\_server* is the name of the resource server that you want to create.
- *scopeN* is the name of a scope.

After the scopes are defined under the resource server, refer to them as *resource\_server.scope* for subsequent tasks, such as creating the OAuth client and requesting an OAuth token. For example, **PDCRSMResourceServer.all**.

If the resource server is created successfully, you will see a response similar to this:

```
Successfully created entity - OAuthResourceServer, detail -
IdentityDomain="PDC_RSM_Domain",Name="PDCRSMResourceServer",Description="Resource server for PDC REST Services Manager",
resourceServerId="4953a4f4-8c3f-41fd-99b5-837cfa9f9ecb",resourceServerNameSpacePrefix="PDCRSMResourceServer.",audienceClaim={"subjects":["ab0"]},
resServerType="CUSTOM_RESOURCE_SERVER",Scopes=[{"scopeName":"all","description":"All permissions"},{"scopeName":"read","description":"Read permissions"}],
tokenAttributes=[{"attrName":"sessionId","attrValue":"$session.id","attrType":DYNAMIC},
{"attrName":"resSrvAttr","attrValue":"RESOURCECONST","attrType":STATIC}]
```

## Creating an OAuth Client for PDC REST Services Manager

You create an OAuth client for PDC REST Services Manager to authenticate requests.

To create an OAuth client, submit a request to the **Add a new OAuth Client** endpoint of the Oracle Access Management OAuth REST API. See ["Add a new OAuth Client"](#) in *REST API for OAuth in Oracle Access Manager* for more information about this endpoint.

The following shows an example cURL request for creating a confidential OAuth client named **PDCRSMClient** with the **PDCRSMResourceServer.all** and default **PDCRSMResourceServer.read** scopes, an identity domain named **PDC\_RSM\_Domain**, and some custom attributes.

```
curl -k -u wls_admin:password -H 'Content-Type: application/json' 'http://oam_host:oam_port/oam/services/rest/ssa/api/v1/oauthpolicyadmin/client'
-d '{"attributes":[{"attrName":"customAttribute1","attrValue":"Custom Value1","attrType":"static"},
{"attrName":"customAttribute2","attrValue":"Custom Value2","attrType":"static"}],
"secret":"client_secret","id":"client_id","scopes":
["PDCRSMResourceServer.all","PDCRSMResourceServer.read"],"clientType":"CONFIDENTIAL_CLIENT",
"idDomain":"PDC_RSM_Domain","description":"PDC RSM OAuth client","name":"PDCRSMClient","grantTypes":["CLIENT_CREDENTIALS"],
"defaultScope":"PDCRSMResourceServer.read","redirectURIs":[{"url":"http://redirect_host:redirect_port/oauth/callback","isHttps":true}]}'
```

where:

- *client\_id* and *client\_secret* are the client ID and client password.
- *redirect\_host:redirect\_port* is the URL for your client application.

If the client is created successfully, the response will be similar to this:

```
Successfully created entity - OAuthClient, detail - OAuth Client - uid =
4b37dd63-08dd-45b5-b5a5-c1e788cb2ff2, name = PDCRSMClient, id =
```

```

PDCRSMClientId,
identityDomain = PDC_RSM_Domain, description = PDC RSM OAuth client,
secret = PDCRSMPassword, clientType = CONFIDENTIAL_CLIENT, grantTypes
= [CLIENT_CREDENTIALS],
attributes = [{"attrName":"customAttribute1","attrValue":"Custom
Value1","attrType":STATIC},
{"attrName":"customAttribute2","attrValue":"Custom
Value2","attrType":STATIC},
{"attrName":"sessionId","attrValue":"session.id","attrType":DYNAMIC},
{"attrName":"resSrvAttr","attrValue":"RESOURCECONST","attrType":STATIC}
], scopes =
[PDCRSMResourceServer.all, PDCRSMResourceServer.read], defaultScope =
PDCRSMResourceServer.read, redirectURIs = [{"url":"http://
redirect_host:redirect_port/oauth/callback","isHttps":true}]

```

## Setting Up Security with Oracle Access Management in the PDC REST Services Manager Configuration File

To set the Oracle Access Management details in the PDC REST Services Manager **application.yaml** file:

1. Open the `PDC_RSM_home/apps/conf/application.yaml` file in a text editor, where `PDC_RSM_home` is the directory in which you installed PDC REST Services Manager.
2. Set the keys under **security** as shown in [Table 10-2](#).

**Table 10-2 Security Keys in the application.yaml File**

Key	Description
<b>enabled</b>	Enables or disables security. Enable security in production environments by setting this to <b>true</b> .
<b>config.require-encryption</b>	Controls whether requests require encryption using <b>client_id</b> and <b>client_secret</b> . Set this to <b>false</b> .
<b>properties.token-endpoint-uri</b>	The URL for requesting an OAuth token from Oracle Access Management. For example, <b>http://oam_host.oam_port/oauth2/rest/token</b>
<b>properties.introspect-endpoint-uri</b>	The URL for validating an OAuth token from Oracle Access Management. For example, <b>http://oam_host.oam_port/oauth2/rest/token/info</b>
<b>properties.oauth-identity-domain-name</b>	The name of the OAuth identity domain that you created in <a href="#">"Creating an OAuth Identity Domain for PDC REST Services Manager."</a> For example, <b>PDC_RSM_Domain</b> .
<b>properties.authorization-endpoint-uri</b>	The URL for authorizing role-based access. PDC REST Services Manager does not support role-based access, so this will not be used. For example, <b>http://oam_host.oam_port/oauth2/authorize</b>

Table 10-2 (Cont.) Security Keys in the application.yaml File

Key	Description
<code>properties.frontend-uri</code>	The URL for the OAuth client you created in "Creating an OAuth Client for PDC REST Services Manager." For example, <code>http://oam_host:oam_port</code>
<code>properties.proxy-host</code>	The URL for your proxy server, if needed.
<code>properties.audience</code>	The name of the OAuth resource server that you created in "Creating a Resource Server for PDC REST Services Manager." For example, <code>PDCRSMResourceServer</code> .
<code>properties.scope-audience</code>	The primary audience for PDC REST Services Manager in the Oracle Access Management resource, used for error handling. This is the same as <code>properties.frontend-uri</code> , ending with <code>/</code> . For example, <code>http://oam_host:oam_port/</code>
<code>providers.oamoidc.validate_with_jwk</code>	Whether to validate with JSON web keys. Set this to <code>false</code> .
<code>providers.oamoidc.token-endpoint-uri</code>	The URL for requesting an OAuth token from Oracle Access Management. For example, <code>http://oam_host:oam_port/oauth2/rest/token</code>
<code>providers.oamoidc.authorization-endpoint-uri</code>	The URL for authorizing role-based access. PDC REST Services Manager does not support role-based access, so this will not be used. For example, <code>http://oam_host:oam_port/oauth2/authorize</code>
<code>providers.oamoidc introspect-endpoint-uri</code>	The URL for validating an OAuth token from Oracle Access Management. For example, <code>http://oam_host:oam_port/oauth2/rest/token/info</code>
<code>providers.oamoidc.scope-audience</code>	The primary audience for PDC REST Services Manager in the Oracle Access Management resource. Set this to <code>"\${ALIAS=security.properties.scope-audience}"</code> .
<code>providers.oamoidc.audience</code>	The name of the OAuth resource server that you created in "Creating a Resource Server for PDC REST Services Manager." For example, <code>PDCRSMResourceServer</code> .
<code>providers.oamoidc.proxy-host</code>	The URL for your proxy server, if needed. Set this to <code>"\${ALIAS=security.properties.proxy-host}"</code> .
<code>providers.oamoidc.frontend-uri</code>	The URL for your application. Set this to <code>"\${ALIAS=security.properties.frontend-uri}"</code> .
<code>providers.oamoidc.cookie-use</code>	Whether to use cookies. Set this to <code>false</code> .
<code>providers.oamoidc.header-use</code>	Whether to use headers. Set this to <code>true</code> .
<code>providers.oamoidc.redirect</code>	Whether to use a redirect URL. Set this to <code>false</code> .
<code>providers.oamoidc.oidc-metadata-well-known</code>	Whether to use OpenID Connect Discovery metadata. Set this to <code>false</code> .
<code>providers.oamoidc.oauth-identity-domain-name</code>	The name of the OAuth identity domain that you created in "Creating an OAuth Identity Domain for PDC REST Services Manager." For example, <code>PDC_RSM_Domain</code> .

**Table 10-2 (Cont.) Security Keys in the application.yaml File**

Key	Description
<b>web-server.paths.methods</b>	The methods allowed for the endpoint. <ul style="list-style-type: none"> <li>For the projectPublishEvent endpoint, set this to ["get", "post"].</li> <li>For the metrics endpoint, set this to ["get"].</li> </ul>
<b>web-server.paths.authenticate</b>	Whether authentication is enabled for the endpoint. Set this to <b>true</b> .
<b>web-server.paths.authorize</b>	Whether authorization is enabled for the endpoint. Set this to <b>true</b> .
<b>web-server.paths.abac.scopes</b>	The scopes that control access to the endpoint. Use the scopes that you configured in <a href="#">Creating a Resource Server for PDC REST Services Manager</a> , without the resource server name. For example, <b>read</b> or <b>all</b> .

- In the providers section, ensure that the **oamoidc** and **abac** providers are not commented out. Comment out the **oidc** provider.
- In the **app.httpClientSecurity** section, set the keys based on the type of authentication required by your enterprise product catalog. These keys allow you to secure outbound requests from PDC REST Services Manager to your enterprise product catalog. See:
  - [OAuth Configuration Properties for Outbound Requests](#)
  - [Basic Authentication Configuration Properties for Outbound Requests](#)
- Save and close the **application.yaml** file. See "[Example application.yaml Security Configuration with Oracle Access Management](#)" for a sample file showing the appropriate properties.
- Restart PDC REST Services Manager by running the following command from the **PDC\_RSM\_home/apps/bin** directory:

```
./RestServicesManager.sh restart
```

## Requesting an OAuth Access Token from Oracle Access Management

You create an access token for OAuth authentication by submitting a request to the **Create Access Token Flow** endpoint of the Oracle Access Management OAuth REST API. For more information, see "[Create Access Token Flow](#)" in *REST API for OAuth in Oracle Access Manager*.

To request an OAuth access token, use cURL to send an HTTP/HTTPS request to the Oracle Access Management URL:

```
curl -i --header 'Authorization: Basic encoded_admin'
--header "Content-Type: application/x-www-form-
urlencoded;charset=UTF-8"
--header "X-OAUTH-IDENTITY-DOMAIN-NAME: identity_domain"
--request POST http://oam_host:oam_port/oauth2/rest/token
--data-
urlencode "grant_type=CLIENT_CREDENTIALS&scope=resource_server.scope"
```

where:

- *encoded\_admin* is the base64-encoded format of the Oracle Access Management administrator user name and password.
- *identity\_domain* is the name of the OAuth identity domain created in Oracle Access Management for PDC REST Services Manager.
- *oam\_host:oam\_port* is the host name and port for the Oracle Access Management server.
- *resource\_server* is the name of the Oracle Access Management resource server created for PDC REST Services Manager.
- *scope* is the name of a scope.

The following shows an example cURL request for creating an OAuth access token for the **PDC\_RSM\_domain** identity domain, **PDCRSMResourceServer** resource server, and **all** scope:

```
curl --location --header 'Authorization: Basic encoded_admin'
--header "Content-Type: application/x-www-form-urlencoded;charset=UTF-8"
--header "X-OAUTH-IDENTITY-DOMAIN-NAME: PDC_RSM_Domain"
--request POST http://oam_host:oam_port/oauth2/rest/token
--data-urlencode
"grant_type=CLIENT_CREDENTIALS&scope=PDCRSMResourceServer.all"
```

If the request is successful, Oracle Access Management returns something similar to this:

```
{"access_token":"access_token",
"token_type":"Bearer","expires_in":3600}
```

Your client must pass this OAuth access token in the header of every HTTP/HTTPS request sent to the PDC REST Services Manager.

## Securing Inbound Communications

You secure communications sent from your enterprise product catalog to the PDC REST Services Manager APIs by enabling TLS in PDC REST Services Manager.

To secure inbound communications to PDC REST Services Manager:

1. Create a PKCS12 certificate file.
2. Copy the PKCS12 certificate file to a location that is accessible by PDC REST Services Manager, such as **~/certs**.
3. Edit the following entries in the *PDC\_RSM\_home/apps/conf/application.yaml* file:
  - **server.ssl.private-key.keystore-path**: Set this to the file system path of the PKCS12 file containing the X.509 certificate and private key.
  - **server.ssl.private-key.keystore-passphrase**: Set this to the password for the PKCS12 file. For example, if you used OpenSSL to create the PKCS12 certificate file, set it to the export password. For security, encrypt the password so it is not stored in clear text. See ["Encrypting Sensitive Data"](#) for more information.



 **Note:**

Set the **server.ssl.private-key.keystore-passphrase** key only if the PKCS file was created using a password.

For example:

```
server:
  ...
  ssl:
    private-key:
      keystore-path: "/scratch/ri-user-1/certs/certificate.p12"
      keystore-passphrase: "${passPhrase}"
```

4. Restart PDC REST Services Manager by running the following command from the *PDC\_RSM\_home/apps/bin* directory:

```
./RestServicesManager.sh restart
```

## Securing Outbound Requests to PDC

During installation, the PDC REST Services Manager installer prompts you for the information required to connect PDC REST Services Manager to PDC. To secure the communications from PDC REST Services Manager to PDC, enable the T3S protocol in PDC REST Services Manager.

To enable T3S in PDC REST Services Manager:

1. Go to the *PDC\_RSM\_home/apps/conf* directory.
2. In the **application.yaml** file, set the **app.pdc.url** key to the T3S protocol and a secure PDC port.

For example:

```
app:
  pdc:
    url: "t3s://pdc.example.com:8002"
```

3. Restart PDC REST Services Manager by running the following command from the *PDC\_RSM\_home/apps/bin* directory:

```
./RestServicesManager.sh restart
```

If you want to change it to use the insecure T3 protocol, set the **app.pdc.url** key to the T3 protocol and an insecure PDC port. For example:

```
app:
  pdc:
    url: "t3://pdc.example.com:8001"
```

## Encrypting Sensitive Data

You can encrypt sensitive data, such as passwords, by using the **RestServicesManager.sh** script.

To encrypt sensitive data:

1. Go to the `PDC_RSM_home/apps/bin` directory, where `PDC_RSM_home` is the directory in which you installed PDC REST Services Manager.

2. Run the following command:

```
./RestServicesManager.sh hash
```

The **Enter value to hash** prompt appears.

3. Enter the sensitive information that you want to encrypt.

The encrypted password is displayed.

## PDC REST Services Manager Security Configuration Reference Information

The following topics contain reference information about PDC REST Services Manager security configuration properties and sample **application.yaml** configuration files:

- [OAuth Configuration Properties for Outbound Requests](#)
- [Basic Authentication Configuration Properties for Outbound Requests](#)
- [Example application.yaml Security Configuration with Oracle Identity Cloud Service](#)
- [Example application.yaml Security Configuration with Oracle Access Management](#)

### OAuth Configuration Properties for Outbound Requests

[Table 10-3](#) describes the keys to configure when your enterprise product catalog uses an OAuth 2.0 authentication type. All keys are nested under **app.httpClients.security.oauth2**.

**Table 10-3** OAuth 2.0 Keys

Key	Description
<b>tokenEndpoint</b>	The URL for requesting an OAuth token. For example, <b>http://host.port/oauth2/rest/token</b> .
<b>clientId</b>	The client ID used to authenticate the request from PDC REST Services Manager.
<b>clientSecret</b>	The encrypted client secret used to authenticate the request from PDC REST Services Manager. To encrypt the client secret, see " <a href="#">Encrypting Sensitive Data</a> ".
<b>scope</b>	The scopes required by the enterprise product catalog. If you are using Oracle Access Management, use the format <i>resourceServerName.scope</i> . For example, <b>ResourceServer.read</b> . If you are using Oracle Identity Cloud Service, use the format <b>urn:opc:resource:consumer::scope</b> .

**Table 10-3 (Cont.) OAuth 2.0 Keys**

Key	Description
<b>grantType</b>	The grant type to be used for the OAuth flow: <b>client_credentials</b> or <b>password</b> . If you are using Oracle Access Management, only <b>client_credentials</b> is supported.
<b>username</b>	The user name required for accessing the enterprise product catalog. Set this only when <b>grantType</b> is <b>password</b> .
<b>password</b>	The encrypted password required for accessing the enterprise product catalog. To encrypt the password, see " <a href="#">Encrypting Sensitive Data</a> ". Set this only when <b>grantType</b> is <b>password</b> .
<b>domainId</b>	The Oracle Access Management Identity domain. Set this only when using Oracle Access Management.

The following shows an example configuration when **grantType** is **client\_credentials**.

```
app:
  httpClients:
    - urlRegex: "local.*:8889"
      security:
        oauth2:
          tokenEndpoint: "http://host:port/oauth2/v1/token"
          clientId: "ClientID"
          clientSecret: "EncryptedClientSecret"
          scope: "https://hostnameurn:opc:resource:consumer::all"
          grantType: "client_credentials"
```

The following shows an example configuration when **grantType** is **password**:

```
app:
  httpClients:
    - urlRegex: "local.*:8889"
      security:
        oauth2:
          tokenEndpoint: "http://host:port:8889/oauth2/v1/token"
          clientId: "ClientID"
          clientSecret: "EncryptedClientSecret"
          scope: "https://hostnameurn:opc:resource:consumer::all"
          grantType: "password"
          username: "ApplicationUsername"
          password: "EncryptedApplicationPassword"
```

## Basic Authentication Configuration Properties for Outbound Requests

**Table 10-4** describes the keys to configure when your enterprise product catalog uses a Basic authentication type. All keys are nested under **app.httpClients.security.basicAuth**.

**Table 10-4 basicAuth Keys**

Key	Description
<b>username</b>	The user name required for accessing the enterprise product catalog.
<b>password</b>	The password required for accessing the enterprise product catalog.

The following shows an example configuration for Basic authentication:

```
app:
  httpClients:
    - urlRegex: "local.*:8889"
      security:
        basicAuth:
          username: "ApplicationUsername"
          password: "ApplicationPassword"
```

## Example application.yaml Security Configuration with Oracle Identity Cloud Service

The following shows sample entries in the **application.yaml** file for configuring PDC REST Services Manager OAuth security with Oracle Identity Cloud Service:

```
security:
  config.require-encryption: true
  enabled: true
  properties:
    idcs-uri: "idcsURI"
    idcs-client-id: "clientId"
    idcs-client-secret: "${clientSecret}"
    frontend-uri: "http://localhost:8080"
    audience: "http://localhost:8080/"
    proxy-host: ""
  providers:
    - abac:
      # Adds ABAC Provider - it does not require any configuration
    - oidc:
      validate-with-jwk: false
      client-id: "${ALIAS=security.properties.idcs-client-id}"
      client-secret: "${ALIAS=security.properties.idcs-client-secret}"
      identity-uri: "${ALIAS=security.properties.idcs-uri}"
      realm: "pdcrsm"
      audience: "${ALIAS=security.properties.audience}"
      proxy-host: "${ALIAS=security.properties.proxy-host}"
      redirect: false
      cookie-use: false
      header-use: true
    #- oamoidc:
      # validate-with-jwk: false
      # token-endpoint-uri: "http://oam_host:oam_port/oauth2/rest/token"
      # authorization-endpoint-uri: "http://oam_host:oam_port/oauth2/
authorize"
```

```

# introspect-endpoint-uri: "http://oam_host:oam_port/oauth2/
rest/token/info"
# scope-audience: "${ALIAS=security.properties.scope-audience}"
# audience: "PDCRSMResourceServer"
# proxy-host: "${ALIAS=security.properties.proxy-host}"
# frontend-uri: "${ALIAS=security.properties.frontend-uri}"
# redirect: false
# cookie-use: false
# header-use: true
# oidc-metadata-well-known: false
# oauth-identity-domain-name: "PDC_RSM_Domain"
# Comment/Uncomment/Override for protection of resources
web-server:
  paths:
    - path: "/productCatalogManagement/v1/projectPublishEvent[/{*}]"
      methods: ["get", "post"]
      authenticate: true
      authorize: true
      abac:
        scopes: ["pubevent"]
    - path: "/metrics[/{*}]"
      methods: ["get"]
      authenticate: true
      authorize: true
      abac:
        scopes: ["metrics"]
  ...
app:
  httpClients:
    - urlRegex: "http://catalog_host:catalog_port/*"
      security:
        oauth2:
          tokenEndpoint: "http://hostname/oauth2/v1/token"
          clientId: "ClientID"
          clientSecret: "EncryptedClientSecret"
          scope: "https://hostnameurn:opc:resource:consumer::all"
          grantType: "client_credentials"
  pdc:
    url: "t3s://pdc_host:secure_pdc_port"
  ...
server:
  ...
  ssl:
    private-key:
      keystore-path: "file_path/certificate.p12"
      keystore-passphrase: "${passPhrase}"

```

## Example application.yaml Security Configuration with Oracle Access Management

The following shows sample entries in the **application.yaml** file for configuring PDC REST Services Manager OAuth security with Oracle Access Management:

```
security:
  config.require-encryption: false
  enabled: true
  properties:
    token-endpoint-uri: "http://oam_host:oam_port/oauth2/rest/token"
    introspect-endpoint-uri: "http://oam_host:oam_port/oauth2/rest/token/
info"
    oauth-identity-domain-name: "PDC_RSM_Domain"
    authorization-endpoint-uri: "http://oam_host:oam_port/oauth2/authorize"
    frontend-uri: "http://localhost:8080"
    proxy-host: ""
    audience: "PDCRSMResourceServer"
    scope-audience: "http://localhost:8080/"
  providers:
    - abac:
      # Adds ABAC Provider - it does not require any configuration
    #- oidc:
      #   validate-with-jwk: false
      #   client-id: "${ALIAS=security.properties.idcs-client-id}"
      #   client-secret: "${ALIAS=security.properties.idcs-client-secret}"
      #   identity-uri: "${ALIAS=security.properties.idcs-uri}"
      #   realm: "pdcrsm"
      #   audience: "${ALIAS=security.properties.audience}"
      #   proxy-host: "${ALIAS=security.properties.proxy-host}"
      #   redirect: false
      #   cookie-use: false
      #   header-use: true
    - oamoidc:
      validate-with-jwk: false
      token-endpoint-uri: "http://oam_host:oam_port/oauth2/rest/token"
      authorization-endpoint-uri: "http://oam_host:oam_port/oauth2/authorize"
      introspect-endpoint-uri: "http://oam_host:oam_port/oauth2/rest/token/
info"
      scope-audience: "${ALIAS=security.properties.scope-audience}"
      audience: "PDCRSMResourceServer"
      proxy-host: "${ALIAS=security.properties.proxy-host}"
      frontend-uri: "${ALIAS=security.properties.frontend-uri}"
      redirect: false
      cookie-use: false
      header-use: true
      oidc-metadata-well-known: false
      oauth-identity-domain-name: "PDC_RSM_Domain"
      # Comment/Uncomment/Override for protection of resources
  web-server:
    paths:
      - path: "/productCatalogManagement/v1/projectPublishEvent[/{*}]"
        methods: ["get", "post"]
```

```

        authenticate: true
        authorize: true
        abac:
            scopes: ["read", "all"]
- path: "/metrics[/{*}]"
  methods: ["get"]
  authenticate: true
  authorize: true
  abac:
    scopes: ["read", "all"]
...
app:
  httpClients:
    - urlRegex: "http://catalog_host:catalog_port/*"
      security:
        oauth2:
          tokenEndpoint: "http://oam_host:oam_port/oauth2/rest/token"
          clientId: "EncryptedClientID"
          clientSecret: "EncryptedClientSecret"
          scope: "ResourceServer.all"
          grantType: "client_credentials"
          domainId: "OAM_Domain"

  pdc:
    url: "t3s://pdc_host:secure_pdc_port"
...
server:
  ...
  ssl:
    private-key:
      keystore-path: "file_path/certificate.p12"
      keystore-passphrase: "${passPhrase}"

```

# Business Operations Center Security

Learn how to install and implement Oracle Communications Business Operations Center and its components in a secure configuration.

Topics in this document:

- [About Installing Business Operations Center](#)
- [About Implementing Business Operations Center Security](#)
- [Storing Business Operations Center Passwords in Oracle Wallet](#)
- [Storing Configuration Entries in the Business Operations Center Wallet](#)

## About Installing Business Operations Center

Before installing Business Operations Center, you must properly install and configure several Oracle products, including Java, Oracle WebLogic Server, Oracle Identity and Access Management components, and Oracle Communications Billing and Revenue Management.

For installation instructions, including all the required products and related tasks, such as setting up KeyStores and SSL for WebLogic Server, see "Installing Business Operations Center" in *Business Operations Center Installation Guide*.

## About Implementing Business Operations Center Security

Business Operations Center supports stringent authorization and authentication requirements. This section describes how to implement the security capabilities supported by Business Operations Center.

## About Identity and Access Management

To authenticate users when they log in and to control user access to functionality, Business Operations Center uses the following Oracle Identity and Access Management components in a production environment:

- Oracle Identity Cloud Service (IDCS)
- Oracle Identity Manager for authentication
- Oracle Platform Security Services (OPSS) for authorization

These components are required in a Business Operations Center implementation.

For more information, see the following documentation:

- Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager
- Oracle Fusion Middleware Administrator's Guide for Oracle Platform Security Services



## About Authentication

Authentication is the process of verifying the identity of a user. The Business Operations Center authentication scheme is designed for deployments in which a central user identity repository, storing all enterprise users, authenticates Business Operations Center sign-in requests.

Business Operations Center supports the following security for authentication:

- Authenticating users against an LDAP-based user ID repository
- Enabling single-sign-on capabilities
- Supporting user's password policies

Oracle Identity Manager manages user password policies. For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

## About Authorization

Authorization is the process of granting users access to privileges (entitlements) appropriate for their job functions while denying access to other functionality. Oracle Platform Security Services handles all authorization tasks for Business Operations Center.

A user who has not been granted any entitlements in Oracle Platform Security Services is denied access to Business Operations Center.

To grant entitlements, you use authorization policies, which contain a collection of the following components combined to form a logical entitlement:

- **Resource type:** Specifies the full scope of traits for a resource, such as job execution history, and defines all actions that can be performed on the resource.
- **Resource:** Represents the aspect of an application's functionality being secured, such as billing, payment collection, and invoicing. Each resource must belong to a resource type.
- **Action:** Represents an operation that can be performed on a resource, such as view, create, modify, delete, history, and timeline.

You map authorization policies to enterprise (external) roles, which represent job functions for the users in your company. If you do not map enterprise roles to authorization policies, you must map each user to an authorization policy.

For more information about authorization policies and enterprise roles, see *Oracle Fusion Middleware Administrator's Guide for Oracle Platform Security Services*.

Business Operations Center includes an authorization policy component file (**system-jazn-data.xml**), which defines all the resource types, resources, and actions available for Business Operations Center authorization policies (see [Table 11-1](#)).

**Table 11-1 Business Operations Center Authorization Policy Components**

Resource Type	Resource	Action	Description
Metrics	Subscribers	View	Permits users to view subscriber metrics.

Table 11-1 (Cont.) Business Operations Center Authorization Policy Components

Resource Type	Resource	Action	Description
Metrics	Subscriptions	View	Permits users to view subscription metrics.
Metrics	Billed Revenue	View	Permits users to view billed-revenue metrics.
Metrics	Payments Received	View	Permits users to view payments-received metrics.
Metrics	AR	View	Permits users to view accounts receivable in the dashboard.
Job	Billing GL Invoicing PaymentCollection PricingSync Refund Workflow	Create View Modify Delete Timeline History	<b>Create:</b> You can create a new job. <b>View:</b> You can view job categories and the jobs for this category. <b>Modify:</b> You can edit a job, deactivate or reactivate jobs. <b>Delete:</b> You can delete jobs. <b>Timeline:</b> You can view the timeline. <b>History:</b> You can view jobs in history.
PaymentFailures	PaymentFailures	View Resolve	<b>View:</b> You can view realtime checkpoints, unresolved batches and unresolved payments, and failure report for Payment Collections jobs. <b>Resolve:</b> You can resolve unresolved payments.
BlackoutPeriod	BlackoutPeriod	View Create Delete	<b>View:</b> You can view the blackout period in the timeline. <b>Create:</b> You can create the blackout period in the timeline. <b>Delete:</b> You can remove the blackout period in the timeline.
Job	Custom	Create View Modify Delete	<b>Create:</b> You can create custom categories in Business Operations Center. <b>View:</b> You can only view custom categories in Business Operations Center.
Job	VirtualTime	View Modify	<b>View:</b> You can view the modified pin virtual time in the Manage Virtual Time banner. <b>Modify:</b> You can change the pin virtual time and date from the jobs actions menu or manage the virtual time banner.
Any	Any	Any	Permits users to perform all operations.

**Table 11-1 (Cont.) Business Operations Center Authorization Policy Components**

Resource Type	Resource	Action	Description
Job	<p><b>category_customcategory1_resource</b></p> <p>Where:</p> <ul style="list-style-type: none"> <li><b>category</b> is a prefix you should add for each resource name.</li> <li><i>customcategory1</i> is the name of the resource of the custom category entered when you create a new category.</li> <li><b>resource</b> is the suffix that you should add to the resource name.</li> </ul> <p>For example, category_custom_billing_resource</p> <p>For information about creating a resource name, see "Defining a Custom Category" in <i>Business Operations Center Online Help</i>.</p>	<p>Create</p> <p>View</p> <p>Modify</p> <p>Delete</p> <p>Timeline</p> <p>History</p>	<p><b>Create:</b> You can create a new job.</p> <p><b>View:</b> You can view job categories and the jobs for this category.</p> <p><b>Modify:</b> You can edit a job, deactivate or reactivate jobs.</p> <p><b>Delete:</b> You can delete jobs.</p> <p><b>Timeline:</b> You can view the timeline.</p> <p><b>History:</b> You can view jobs in history.</p>

The **system-jazn-data.xml** file also includes the following sample authorization policies:

- OperationsAdminPolicy
- FinancialsAdminPolicy
- FullAdminPolicy

The file is located in the *Domain\_home/lib/oes\_config* directory, where *Domain\_home* is the WebLogic Server domain home directory location of the Oracle Platform Security Services client domain in which Business Operations Center is deployed.



**Note:**

Do not change the **system-jazn-data.xml** file.

## Creating Authorization Policies for Business Operations Center

To create authorization policies for Business Operations Center:

1. Import the Business Operations Center authorization policy component file:  
*Domain\_home/lib/oes\_config/system-jazn-data.xml*

For detailed instructions, see "Importing the Business Operations Center Operations Security Policies into OPSS" in *Business Operations Center Installation Guide*.

2. In Oracle Platform Security Services (OPSS), map an authorization policy to one or more resources, which may have one or more actions.

For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Platform Security Services*.

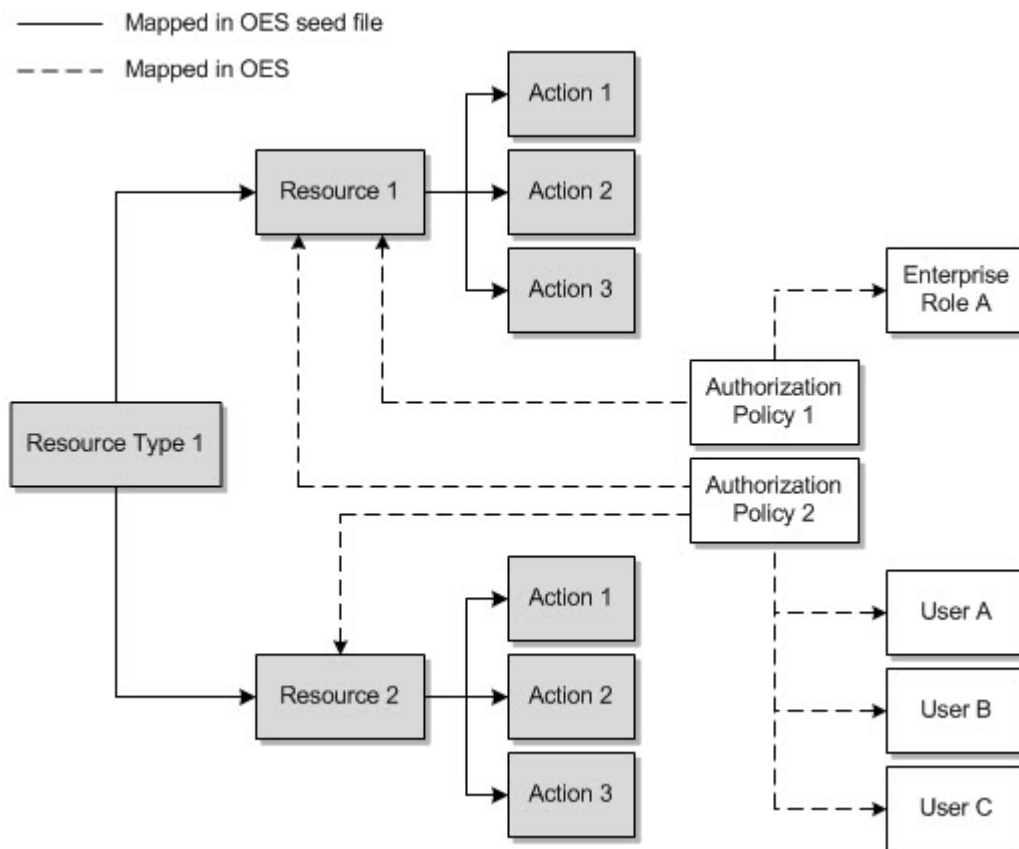
3. Associate the authorization policy with a user or an enterprise role.

For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Platform Security Services*.

4. Redeploy all changes made in OPSS.

Figure 11-1 shows how authorization policies are mapped to resources and enterprise roles or users:

**Figure 11-1 Mapping Authorization Policies to Resources and Enterprise Roles or Users**



## Storing Business Operations Center Passwords in Oracle Wallet

By default, the Business Operations Center Installer stores sensitive information such as passwords in the Oracle wallet and the Business Operations Center application retrieves the passwords from the Oracle wallet. However, if the passwords are also stored in the configuration files, the Business Operations Center application retrieves the passwords from

the configuration files. The Business Operations Center application automatically decrypts the encrypted passwords when retrieving them from the configuration files.

By default, the passwords in the configuration files are encrypted in the Oracle ZT PKI format. For more information, see "Encrypting Data" in *BRM Developer's Guide*.



#### Note:

To encrypt passwords that are associated with customizations, use the **pin\_crypt\_app** utility. For details, see "About Encrypting Passwords" in *BRM Developer's Guide*.

## Storing Configuration Entries in the Business Operations Center Wallet

To store a configuration entry for the Business Operations Center wallet:

1. Go to the *BOC\_home/wallet/client* directory, where *BOC\_home* is the directory in which Business Operations Center is installed.
2. Do one of the following:
  - On Linux, run the following command:

```
java -cp
'.:oraclepki.jar_location:osdt_cert.jar_location:osdt_core.jar_location:
cet.jar_location' com.portal.cet.ConfigEditor -setconf -wallet
clientWalletLocation -parameter configEntry -value value
```

where:

- *oraclepki.jar\_location* is the path to the **oraclepki.jar** file, which contains the APIs that are required for the wallet. The **oraclepki.jar** file is stored in the *BOC\_home/lib* directory.
- *osdt\_cert.jar\_location* is the path to the **osdt\_cert.jar** file, which contains the JARs that are used by the JAVA PCM library for establishing a TLS connection to BRM. The **osdt\_cert.jar** file is stored in the *BOC\_home/lib* directory.
- *osdt\_core.jar\_location* is the path to the **osdt\_core.jar** file, which contains the JARs that are used by the JAVA PCM library for establishing a TLS connection to BRM. The **osdt\_core.jar** file is stored in the *BOC\_home/lib* directory.
- *cet.jar\_location* is the path to the **cet.jar** file, which contains the APIs that are required for the wallet. The **cet.jar** is stored in the *BOC\_home/lib* directory.
- *clientWalletLocation* is the path to the Business Operations Center wallet.
- *configEntry* is the configuration entry in the Business Operations Center wallet.
- *value* is the appropriate value for the respective entry in the Business Operations Center wallet.

For example, running the following command with the **-value** parameter stores the **infranet.log.level** as **1** in the Business Operations Center wallet. If the value exists in the wallet, it will be overwritten:

```
java -cp '.:oraclepki.jar:osdt_cert.jar:osdt_core.jar:cet.jar:'
com.portal.cet.ConfigEditor -setconf -wallet "/scratch/pin11/wallet" -
parameter infranet.log.level -value 1
```

If you run the command without the **-value** parameter, it prompts for the values for the **infranet.connection** entries and stores them in the Business Operations Center wallet. At the command prompt, enter values listed in [Table 11-2](#).

**Table 11-2 BRM Connection Information**

Field	Description
<b>User Name</b>	The user name for connecting to BRM.
<b>Password</b>	The BRM user's password.
<b>Host Name</b>	The IP address or the host name of the machine on which the primary BRM Connection Manager (CM) or CM Master Process (CMMP) are running.
<b>Port Number</b>	The TCP port number of the CM or CMMP on the host computer.
<b>Service Type</b>	The BRM service type.
<b>Service POID Id</b>	The POID of the BRM service.

- On Windows, run the following command:

```
java -cp
".;oraclepki.jar_location:osdt_cert.jar_location:osdt_core.jar_location:cet.jar
_location" com.portal.cet.ConfigEditor -setconf -wallet clientWalletLocation -
parameter configEntry -value value
```

For example, running the following command with the **-value** parameter stores the **infranet.log.level** as **1** in the Business Operations Center wallet:

```
java -cp ".;C:\Program Files (x86)\Portal
Software\BOC_HOME\lib\oraclepki.jar;C:\Program Files (x86)\Portal
Software\BOC_HOME\lib\osdt_cert.jar;C:\Program Files (x86)\Portal
Software\BOC_HOME\lib\osdt_core.jar;C:\Program Files (x86)\Portal
Software\BOC_HOME\lib\cet.jar" com.portal.cet.ConfigEditor -setconf -wallet
"C:\Program Files (x86)\Portal Software\BOC_HOME\wallet\client" -parameter
infranet.log.level -value 1
```

If you run the command without the **-value** parameter, it prompts for the values for the **infranet.connection** entries and stores them in the Business Operations Center wallet. At the command prompt, enter values listed in [Table 11-2](#).

3. Enter the Business Operations Center client wallet password.

The value is stored in the Business Operations Center wallet.

For retrieving stored configuration entries, see "About Oracle Wallet" in *BRM System Administrator's Guide*.

# A

## Secure Deployment Checklist

Learn how to use checklists to install Oracle Communications Billing and Revenue Management (BRM) and Oracle Communications Pricing Design Center (PDC) securely.

Topics in this appendix:

- [BRM Checklist](#)
- [PDC Checklist](#)

### BRM Checklist

The following security checklist lists guidelines to help you secure BRM and its components.

1. Install only what is required.
2. Lock and expire default user accounts.
3. Enforce password management.
4. Practice the principle of least privilege.
  - Grant only the necessary privileges.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
5. Enforce access controls effectively and authenticate clients stringently.
6. Restrict network access.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Monitor who accesses your systems.
  - Check network IP addresses.
7. Apply all security patches and workarounds.
8. Contact Oracle Security Products if you come across a vulnerability in Oracle Database.

### PDC Checklist

Follow this checklist to deploy PDC securely.

1. Preinstallation steps:
  - a. Enable SSL for the target Oracle WebLogic Server domain.
  - b. Configure the server KeyStore certificate and get the client KeyStore trusted certificate.
  - c. Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer.

- d. Ensure that the latest supported version of Oracle JDK is installed and configured with your PDC or WebLogic installation.
2. Installation steps:
    - Select SSL mode and provide the client KeyStore certificate (**.jks** file) for connecting to a WebLogic server over SSL.
  3. Postinstallation steps:
    - a. If you do not need the installation log files, make sure to delete them.
    - b. The WebLogic Server administrator will need to create PDC users based on the roles and privileges.
    - c. Do not use your browser's remember password feature for the WebLogic Server Administration Console URL.
    - d. Enable secure cookies.
    - e. Verify that file permissions for the installed files are 600 for all nonexecutable files and 700 for all executable files.
  4. Un-installation steps:
    - Delete the log files in *OracleInventory/logs/* manually if you do not need them or protect them appropriately if they are required for further reference. These log files have file permission 640 (owner can read/write, group members can read, others cannot do anything) by default.