Oracle® Communications
Billing and Revenue Management
Security Guide
Release 12.0
E51031-03

April 2019
Contents

Preface ................................................................................................................................................................... vii
  Audience ....................................................................................................................................................... vii
  Accessing Oracle Communications Documentation .................................................................................. vii
  Documentation Accessibility .................................................................................................................... vii
  Related Documents ................................................................................................................................ vii
  Document Revision History ....................................................................................................................... vii

1 BRM Security Overview ................................................................................................................................. 1-1
  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 ........................................................................................................... 2-1
  Pre-Installation Tasks ............................................................................................................................... 2-1
  Installing BRM Securely ........................................................................................................................... 2-2
  Post-Installation Tasks ............................................................................................................................... 2-2
    Lock and Expire Default User Accounts ............................................................................................... 2-2
    Change Default User Passwords ........................................................................................................... 2-2
    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 ........................................................................................................................... 2-4

3 Performing a Secure Pricing Design Center Installation .............................................................................. 3-1
  Recommended Installation Mode ................................................................................................................. 3-1
  Operating System Security ........................................................................................................................ 3-1
  Installing Pricing Design Center ................................................................................................................. 3-1
    Pre-Installation ...................................................................................................................................... 3-1
    Installation ............................................................................................................................................... 3-2
Post-Installation Configuration .................................................................................................................. 3-2
    Managing Cookies ................................................................................................................................. 3-3
    Using Secure Cookies ........................................................................................................................... 3-3
    Configuring the Session Timeout .......................................................................................................... 3-3
    Managing File Permissions ...................................................................................................................... 3-4
Uninstalling Pricing Design Center ........................................................................................................ 3-5
About Changing Passwords in the Wallets ............................................................................................ 3-5
Performing a Secure ECE Installation ..................................................................................................... 3-6
    About ECE Security ............................................................................................................................ 4-1
    About Oracle Coherence Security ......................................................................................................... 4-2
    About Oracle Database Security ........................................................................................................... 4-2
    About Oracle NoSQL Database Security .............................................................................................. 4-2
    About Cluster Security .......................................................................................................................... 4-2
    About the Keystore Files and SSL Considerations .............................................................................. 4-3
    About Trusted Host Information ........................................................................................................ 4-3
    About JMX Security ............................................................................................................................... 4-4
    Post-Installation Security Tasks .......................................................................................................... 4-5
4  Performing a Secure ECE Installation
    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 .......................................................................................................................... 4-2
    About the Keystore Files and SSL Considerations .............................................................................. 4-3
    About Trusted Host Information ........................................................................................................ 4-3
    About JMX Security ............................................................................................................................... 4-4
    Post-Installation Security Tasks .......................................................................................................... 4-5
5  Managing BRM Security
    The Security Model ............................................................................................................................... 5-1
    Configuring and Using Authentication ................................................................................................. 5-1
        Authentication of Applications ........................................................................................................... 5-1
        Authentication of Accounts ............................................................................................................... 5-2
    Configuring and Using Access Control ............................................................................................... 5-2
        Permissions ....................................................................................................................................... 5-2
        Roles .................................................................................................................................................. 5-2
        Managing CSR Passwords .................................................................................................................. 5-3
        Automatic Logout ............................................................................................................................. 5-3
        Access Control in BRM Web Services Manager ............................................................................. 5-3
    Configuring and Using Security Audit ................................................................................................. 5-3
    Encryption ............................................................................................................................................. 5-3
        Using Oracle ZT Encryption Scheme ................................................................................................. 5-4
    Securing Sensitive Customer Data ....................................................................................................... 5-4
    Using Credit Card Tokenization ........................................................................................................... 5-4
    Masking Sensitive Data in Log Files ..................................................................................................... 5-4
    Securing BRM Network Ports ................................................................................................................. 5-5
    About Managing ECE Security .............................................................................................................. 5-5
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 BIP Entries in Infranet.properties ......................... 7-1
   Implementing Billing Care Security ......................................... 7-1
   About Identity Management Suite ........................................... 7-1
   About Authentication .................................................................. 7-2
   About Authorization ..................................................................... 7-2
   About Billing Care Authorization Resources ............................. 7-3
      Policies on Transaction Limits .............................................. 7-9
   About Auditing .......................................................................... 7-10
   Security Considerations for Developers .................................... 7-11
   About Secure Development .................................................... 7-11
   Creating a Resource Type with OPSS ..................................... 7-11
   About REST API Authorization .............................................. 7-12
   About UI Authorization ........................................................ 7-12
   Adding New Resource Types .................................................. 7-12
   Storing Passwords in Oracle Wallet ........................................ 7-12
   Storing Configuration Entries in the Billing Care Wallet ............. 7-13

8 Business Operations Center Security
   About Installing Business Operations Center ............................ 8-1
   About Implementing Business Operations Center Security ........ 8-1
   About Identity and Access Management ................................... 8-1
   About Authentication ............................................................ 8-1
   About Authorization .............................................................. 8-2
   Creating Authorization Policies for Business Operations Center ... 8-3
   Storing Passwords in Oracle Wallet ........................................ 8-4
   Storing Configuration Entries in the Business Operations Center Wallet 8-4

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.

Accessing Oracle Communications Documentation

Product documentation is located on Oracle Help Center:

- [http://docs.oracle.com](http://docs.oracle.com)

Documentation Accessibility


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](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) or visit [http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) if you are hearing impaired.

Related Documents

For information on implementing system security in BRM, PDC, and ECE, see *BRM System Administrator’s Guide*.

Document Revision History

The following table lists the revision history for this document:
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E51031-01</td>
<td>December 2017</td>
<td>Initial release.</td>
</tr>
<tr>
<td>E51031-02</td>
<td>September 2018</td>
<td>Documentation updates for Billing Care 12.0 Patch Set 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Updated the following section:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ About Billing Care Authorization Resources</td>
</tr>
<tr>
<td>E51031-03</td>
<td>April 2019</td>
<td>Documentation updates for ECE 12.0 Patch Set 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Added the following chapter:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Performing a Secure ECE Installation</td>
</tr>
</tbody>
</table>
This document provides an overview of Oracle Communications Billing and Revenue Management (BRM) 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. This guide assumes that the BRM maintenance level is 7.5 Patch Set 10 or later.

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

  It is particularly important for system administrators to adopt this policy for software dependencies for which upgrades are generally related to security rather than focused 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 tier and the Data tier 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 upon IP address. Restricting database access by IP address often causes 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 its equivalent.

- **Limit privileges as much as possible.** Give users only as much access as necessary to perform their work. User privileges should be reviewed 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 the "Critical Patch Updates and Security Alerts" article on the Oracle Technology Web site:


### 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**

See the following documents:

- *Guide to the Secure Configuration of Red Hat Enterprise Linux 7*
- *Hardening Tips for the Red Hat Enterprise Linux 7*

**Oracle Database Security**

See *Oracle Database Security Guide*. 

Performing a Secure BRM Installation

This document describes recommended installation steps for Oracle Communications Billing and Revenue Management (BRM).

For information about installing BRM, see BRM Installation Guide.

Pre-Installation Tasks

Perform the following pre-installation 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 post-installation 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 post-installation 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.

Post-Installation Tasks

Perform the following tasks after installing BRM:

- Lock and Expire Default User Accounts
- Change Default User Passwords
- 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, and the defaults change_on_install or manager are not accepted.

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
Post-Installation Tasks

Performing a Secure BRM Installation

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`), Synchronization Queue Manager DM (`dm_aq`), 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 BRM server.

BRM provides sample CA certificate 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 the discussion about 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 the discussion about PCM_OP_CUST_POL_VALID_PASSWD 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 the discussion about 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 the discussion about logging CSR activities 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.
Performing a Secure Pricing Design Center Installation

This document describes recommended deployment configurations for your Oracle Communications Pricing Design Center (PDC) installation that enhance security.

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. See “Installing Pricing Design Center” for more information.

Operating System Security

PDC is supported on Linux 7UL2+ (both Oracle Enterprise Linux and Red Hat Enterprise Linux), Oracle Solaris for SPARC (11 Update 3+), and Windows 8.1 or 10 Client. See the following documents for more information:

- Guide to the Secure Configuration of Red Hat Enterprise Linux 7
- Hardening Tips for the Red Hat Enterprise Linux 7
- Oracle Solaris 11.3 System Hardening References

Installing Pricing Design Center

This section describes the security configurations during pre-installation and installation of PDC.

Pre-Installation

Perform the following pre-installation tasks:

- Enable SSL for the target WebLogic server domain, configure the server keystore certificate, and then get the client keystore trusted certificate (.jks file). 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 12c Release 2* documentation.

Verify that you have the latest supported version of Oracle JDK installed.

**Installation**

During PDC installation, select SSL mode and provide the client keystore certificate (.jks file) 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 installActions2011-08-15_08-06-57AM.log
-rw-r----- 1 user1 eng 2384 Aug 15 10:33 dbScripts2011-08-15_10-32-00AM.log
-rw-r----- 1 user1 eng 124268 Aug 15 10:33 oraInstall2011-08-15_10-27-07AM.err
```

*installActionsxxxxx.log* and *oraInstallxxxx.err* will have details in clear text form entered in the PDC installation wizards. Passwords entered in wizard are not logged in any of the PDC installation logs. Delete these installation log files if you do not need them for future reference, otherwise protect them appropriately if you do require them. 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.

**Post-Installation 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.

   ```xml
   <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.

For more information, see the "Using Secure Cookies to Prevent Session Stealing" article on the Oracle Help Center Web site:

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/security/thin_-client.html#wp1053780

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. The 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**.


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, see the "Configuring Applications for Production Deployment" article on the Oracle Help Center Web site:
http://download.oracle.com/docs/cd/E12840_01/wls/docs103/deployment/config.html

### Managing File Permissions

- Following is the default permissions set for the installed files:
Implementing Pricing Design Center Security

- `rw------- 600` (for all non executable files)
- `rwx------- 700` (for all executable files)

Permissions are set to 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 installActions2011-08-15_08-06-57AM.log`
  - `rw-r-----  1 user1 eng       0 Aug 15 10:27 oraInstall2011-08-15_10-27-07AM.out`
  - `rw-r-----  1 user1 eng    2384 Aug 15 10:33 dbScripts2011-08-15_10-32-00AM.log`
  - `rw-r-----  1 user1 eng  124268 Aug 15 10:33 oraInstall2011-08-15_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 the discussion about changing passwords in the wallets 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 and System Administration 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 information.

### 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 **OUD Authenticator**.

15. In the **Type** field, enter **IPlanetAuthenticator**.

16. Click **OK**.

   The Settings for OUD Authenticator page appears.

17. In the **Control Flag** row, select **SUFFICIENT**.

18. Click **Provider Specific** and provide Oracle Unified Directory (OUD) connection details.

19. Click **Save**.

20. Click **Reorder**.

   The Reorder Authentication Providers page appears.

   Reorder the authentication provider names in the following order:

   - OAMIdentityAsserter
   - OUD 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:
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.
Performing a Secure ECE Installation

This document provides an overview of Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) security and instructions for installing a secure ECE system.

ECE should be deployed into a secured environment; for example,

- ECE is deployed in a closed networked environment in which any public access to the network is denied.
- All ECE hosts are ideally 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.

ECE security can be further hardened by following the instructions in this chapter. See BRM ECE Installation Guide for information about installing ECE.

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 UNIX commands in a UNIX shell. Once 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 UNIX account, for setting up password-less SSH. See the discussion about managing security in BRM System Administrator’s Guide for information about the ECE user.

About Oracle Coherence 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). See the information about managing 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 at:

http://docs.oracle.com

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/cocesserver/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/occeceserver/config/permissions.xml`.

See BRM ECE Installation Guide for more information.

About the Keystore Files and SSL Considerations

ECE maintains the `server.jks` keystore file.

The `server.jks` file stores credentials for cluster node authentication details. The `server.jks` file is also used for encrypting intra-cluster communication over SSL.

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

**Important:** Oracle strongly recommends not overriding the default `ECE_Home/occeceserver/config/charging-coherence-override-secure-prod.xml` file.

Installation Settings when SSL Is Enabled

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

- In `ECE_Home/occeceserver/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/occeceserver/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 the installation.

About Trusted Host Information

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.
About JMX Security

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 BRM ECE Installation Guide for more information.

About JMX Security

JMX can be secured by setting the following system parameters:

- In `ECE_Home/oceceserver/config/ece.properties`:
  
  ```
  com.sun.management.jmxremote.authenticate=true
  ```

- In `ECE_Home/oceceserver/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.

JMX security is based on Java's standard guidelines as documented at:

http://docs.oracle.com/javase/1.5.0/docs/guide/management/agent.html

ECE bundles a `jmxremote.password` password file in the `ECE_Home/oceceserver/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/oceceserver/config`. If more accounts are to be added, then those accounts should be added in the `jmxremote.password` file as well. Refer to the following document for information about setting up authorizations for the new accounts:

http://docs.oracle.com/javase/1.5.0/docs/guide/management/agent.html

Because the JMX passwords are human readable in the `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 the discussion 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 pricingLoader`, `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, it is recommended to use 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 executed 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, the user name and password must be specified when a connection is made.

**Post-Installation Security Tasks**

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

After installation, verify the following in the `ECE_HOME/oceceserver/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.
This document describes how to manage security in Oracle Communications Billing and Revenue Management (BRM).

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: ensuring that only authorized individuals get access to the system and data.
- Authorization: access control to system privileges and data. This 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 properly decrypted.

Configuring and Using Authentication

BRM requires two levels of authentication within its operation:

- Authentication of Applications
- Authentication of Accounts

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 and password for this account are kept in the application's configuration file. By default, the password is encrypted using AES and stored.

The account authenticated against is held in the BRM database. As a result, the mechanics of the authentication are identical to that of the authenticating an account.
Authentication of Accounts

Users requesting permission to carry out a transaction must be authenticated against the account in the BRM database. All passwords are encrypted and stored in the BRM 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 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.

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

See the discussion about setting up permissions in BRM applications 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 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 the discussion 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 the discussion about managing CSR passwords in *BRM System Administrator’s Guide* for more information.

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.

See the discussion about automatic logout in *BRM System Administrator’s Guide* for more information.

Access Control in BRM Web Services Manager

BRM Web Services Manager enables BRM opcodes to be exposed through Web services. Web Services Manager uses the Apache Axis framework to support SOAP 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.

See "Configuring Security for Web Services Manager" 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.

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 the discussion about protecting BRM passwords 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 "Configuring the Data Manager for Oracle ZT PKI Encryption" 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 "About Securing Sensitive Customer Data with Masking" in *BRM Managing Customers* for more information on setting up data masking.

**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 the credit or debit card data.

See "About Replacing Credit Card Numbers with 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 "About Migrating Credit Card Information from Legacy Databases" in *BRM Configuring and Collecting Payments* for more information.

**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:

- 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 you have created user groups and set permissions, users can log in to the system and 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 may choose to 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 BRM System Administrator’s Guide for a list of the files that you need to restrict access to.

- Manage passwords. UNIX accounts protected by passwords must be created for ECC. Besides the UNIX accounts, you need to create non-UNIX 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 (the keystore.jks file).

- 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.
Security Considerations for Developers

This document provides information for developers about how to extend Oracle Communications Billing and Revenue Management (BRM) without compromising security.

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.
This chapter provides information about installing and implementing Oracle Communications Billing Care and its components in a secure configuration.

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 Oracle Communications 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 BIP Entries in Infranet.properties

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

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 Oracle Communications 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 BillingCareSDK\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 permissions to perform general CSR or more advanced A/R tasks, for example.
## Table 7–1  Authorization Resources

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource</th>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuperUserType</td>
<td>SuperUserResource</td>
<td>Any</td>
<td>Enables you to create users free of restrictions, including when the user’s profile contains other resources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The only exception is the ReadOnlyType, which takes precedence over all other resource types.</td>
</tr>
<tr>
<td>ReadOnlyType</td>
<td>ReadOnlyResource</td>
<td>Any</td>
<td>Causes Save and Apply buttons on overlays to be displayed as read-only. Users are allowed only read operations even if they have other resources or entitlements.</td>
</tr>
<tr>
<td>PaymentResourceType</td>
<td>PaymentResource</td>
<td>Allocate, Audit, BatchProcess,</td>
<td>Allocate: Allows user to allocate payments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Make, ReassignHandler, Reverse,</td>
<td>Audit: Allows user to view audit information on Payment Details overlay. (Audit information in payment suspense screen is always visible.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SuspenseAccess, SuspenseAllocate,</td>
<td>BatchProcess: Displays the Batch Payment button on the landing page. Make: Allows user to make payments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SuspenseMake, SuspenseMove,</td>
<td>ReassignHandler: Prevents user from assigning and reassigning batch payment handlers to suspended payments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SuspenseReverse</td>
<td>Reverse: Allows user to reverse payments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SuspenseAccess: Prevents user from accessing any payment suspense functionality.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SuspenseAllocate: Allows user to allocate suspended payments partially or fully to an account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SuspenseMake: Prevents user from making suspended payments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SuspenseMove: Allows user to move posted payments into suspended status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SuspenseReverse: Allows user to reverse suspended payments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Returned as an obligation; OPSS returns a number, which is interpreted as a limit. See Table 7–2 for transaction limits.</td>
</tr>
</tbody>
</table>
### Table 7–1 (Cont.) Authorization Resources

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource</th>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceResourceType</td>
<td>ServiceResource</td>
<td>Cancel, Edit, Inactivate, Make, Reactivate, OfferInactivate, OfferTerminate, OfferReactivate, Terminate, Associate, EditOfferCustomization</td>
<td>Cancel: Prevents user from canceling services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Edit: Gives user read-only access to the Asset Details page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Make: Blocks user’s access to the Select and Configure pages of the customer creation wizard. Hides the Purchase button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inactivate: Prevents user from inactivating services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OfferInactivate: Prevents user from inactivating product and discount offers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OfferReactivate: Prevents user from reactivating product and discount offers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OfferTerminate: Prevents user from terminating product and discount offers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reactivate: Prevents user from reactivating services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Terminate: Prevents user from terminating services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Associate: Allows user to search and associate devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EditOfferCustomization: Allows user to modify rate customizations.</td>
</tr>
<tr>
<td>AdjustmentCurrencyResourceType</td>
<td>AdjustmentResource</td>
<td>Allocate, Make</td>
<td>Allocate: Prevents user from allocating currency adjustments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Make: Prevents users from making adjustments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Uses a policy that constrains the maximum payment amount as a function of CSRs access level. See Table 7–2 for transaction limits.</td>
</tr>
<tr>
<td>WriteoffResourceType</td>
<td>WriteoffResource</td>
<td>Make, Reverse</td>
<td>Make: Prevents user from writing off accounts, bills, and item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy on the minimum and maximum write-off amount applies. See Table 7–2 for transaction limits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reverse: Allows user to reverse the accounts write-off.</td>
</tr>
</tbody>
</table>
### Table 7–1 (Cont.) Authorization Resources

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource</th>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdjustmentNonCurrencyResourceType</td>
<td>AdjustmentNonCurrencyResource</td>
<td>Make</td>
<td>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 Table 7–2 for transaction limits.</td>
</tr>
<tr>
<td>DisputeResourceType</td>
<td>DisputeResource</td>
<td>Raise, Settle</td>
<td>Raise: Allows user to raise bill and item-level and event-level disputes. Settle: Allows user to settle bill and item-level disputes. Policy on the maximum dispute amount applies. See Table 7–2 for transaction limits.</td>
</tr>
<tr>
<td>RefundResourceType</td>
<td>RefundResource</td>
<td>Make</td>
<td>Make: Allows user to perform account-level and bill unit-level refunds.</td>
</tr>
<tr>
<td>ConfigurationsArtifactsType</td>
<td>ConfigurationArtifactsResource</td>
<td>View</td>
<td>Allows user to read all configuration-related REST APIs (for example, authorization profiles).</td>
</tr>
<tr>
<td>InvoiceImageType</td>
<td>InvoiceImageResource</td>
<td>View</td>
<td>Allows user to view invoices.</td>
</tr>
<tr>
<td>NoteResourceType</td>
<td>NoteResource</td>
<td>Comment</td>
<td>Allows user to make comments.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Resource</td>
<td>Actions</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PaymentMethodResourceType</td>
<td>PaymentMethodResource</td>
<td>Add, Delete, Modify</td>
<td>Add: Allows user to add payment method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Delete: Allows user to delete payment method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Modify: Allows user to change payment method.</td>
</tr>
<tr>
<td>TaxExemptionResourceType</td>
<td>TaxExemptionResource</td>
<td>Add, Delete, Modify</td>
<td>Add: Allows user to add tax exemptions whether account has or does not have prior tax exemptions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Delete: Allows user to delete tax exemptions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Modify: Allows user to save changes to tax exemption attributes.</td>
</tr>
<tr>
<td>BillUnitResourceType</td>
<td>BillUnitResource</td>
<td>Add, Delete, Modify, ModifyValidity, SetLimit</td>
<td>Add: Allows user to create bill units and allows user to move services between bill units.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Delete: Reserved for future use.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Modify: Allows user to change the bill unit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ModifyValidity: Allows user to modify the validities for non-currency balances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SetLimit: Allows user to set credit limit and thresholds for non-currency resources.</td>
</tr>
<tr>
<td>BillResourceType</td>
<td>BillResource</td>
<td>BillNow, Correct</td>
<td>BillNow: Allows user to perform Bill Now operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Correct: Allows user to produce corrective bill.</td>
</tr>
</tbody>
</table>
### Table 7-1 (Cont.) Authorization Resources

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource</th>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CollectionResourceType</td>
<td>CollectionResource</td>
<td>Add, Modify, Search, Delete, AddAction, ModifyAction, Replace, Promise, Exit, Exempt, AddMember, DeleteMember</td>
<td>Add: Allows user to create a collection group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modify: Allows user to modify a collection group in an owner account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Search: Allows user to access collections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete: Allows user to delete a collection group from an owner account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddAction: Allows user to add a collection action on a bill unit in collections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ModifyAction: Allows user to modify a collections action for a bill unit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replace: Allows user to replace a scenario with another scenario in collections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Promise: Allows user to cancel promise-to-pay agreement in collections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exit: Allows user to exit a bill unit of an account from collections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exempt: Allows user to exempt a bill unit from collections.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddMember: Allows user to add members to a collections group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteMember: Allows user to delete members from a collections group.</td>
<td></td>
</tr>
<tr>
<td>ChargeSharingResourceType</td>
<td>ChargeSharingResource</td>
<td>Add, Delete, Modify, AddMember, DeleteMember, ModifyMember, ModifyPriority</td>
<td>Add: Allows user to create a charge sharing group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete: Allows user to remove a charge sharing group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modify: Allows user to modify the charge sharing group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddMember: Allows user to add a member to a charge sharing group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteMember: Allows user to remove members from a charge sharing group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ModifyMember: Allows user to change members in a charge sharing group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ModifyPriority: Allows user to modify the order of priority when a member is part of multiple discount or charge sharing groups.</td>
<td></td>
</tr>
</tbody>
</table>
Implementing Billing Care Security

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>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource Type</th>
<th>Resource Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiscountSharingResourceType</td>
<td>DiscountSharingResource</td>
<td>Add, Delete, Modify, AddMember, DeleteMember, ModifyMember, ModifyPriority</td>
<td>Add: Allows user to create a discount sharing group. Delete: Allows user to remove a discount sharing group. Modify: Allows user to change the member details in a discount sharing group. AddMember: Allows user to add a member to a discount sharing group. DeleteMember: Allows user to delete members from a discount sharing group. ModifyMember: Allows user to change members in a discount sharing group. ModifyPriority: Allows user to modify the order of priority when a member is part of multiple discount sharing groups.</td>
</tr>
<tr>
<td>ProfileSharingResourceType</td>
<td>ProfileSharingResource</td>
<td>Add, Delete, Modify, AddMember, DeleteMember, ModifyMember</td>
<td>Add: Allows user to create a profile sharing group. Delete: Allows user to remove a user from a profile sharing group. Modify: Allows user to change the member details in a profile sharing group. AddMember: Allows user to change the member details in a profile sharing group. DeleteMember: Allows user to remove a member from a profile sharing group. ModifyMember: Allows user to modify members in a profile sharing group.</td>
</tr>
<tr>
<td>SubscriptionResourceType</td>
<td>SubscriptionResource</td>
<td>Transit</td>
<td>Transit: Allows user transition packages or bundles.</td>
</tr>
<tr>
<td>DeferredActionResourceType</td>
<td>DeferredActionResource</td>
<td>Edit, Delete, Execute</td>
<td>Edit: Allows user to modify a deferred action. Delete: Allows user to remove a deferred action. Execute: Allows user to execute a deferred action.</td>
</tr>
</tbody>
</table>
Table 7–2 lists the attributes that require system administrators to configure transaction limits (values).

### Table 7–2  Listing of Transaction Limits (Obligations)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Currency Adjustment Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Minimum Currency Adjustment Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum Non-currency Adjustment Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Minimum Non-currency Adjustment Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum Payment Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum Dispute Amount (applies to settle as well)</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum Write-off Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum Refund Issues Amount</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum Refund Settle Amount</td>
<td>Integer</td>
</tr>
</tbody>
</table>

### 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 configure the capture of 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. For more information, see Oracle Communications Billing and Revenue Management System Administrator’s Guide.

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

<table>
<thead>
<tr>
<th>Task</th>
<th>BRM Event Name (Activity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account creation</td>
<td><code>/event/notification/account/create</code></td>
</tr>
<tr>
<td>Subscription purchase</td>
<td><code>/event/billing/product/action/purchase</code></td>
</tr>
<tr>
<td>Subscription modification</td>
<td><code>/event/billing/product/action/modify</code></td>
</tr>
<tr>
<td>Subscription cancellation</td>
<td><code>/event/billing/product/action/cancel</code></td>
</tr>
<tr>
<td>Updates to bill info</td>
<td><code>/event/customer/billinfo/modify</code></td>
</tr>
<tr>
<td>Event adjustment</td>
<td><code>/event/billing/adjustment/event</code></td>
</tr>
<tr>
<td>Item adjustment</td>
<td><code>/event/billing/adjustment/item</code></td>
</tr>
<tr>
<td>Account adjustment</td>
<td><code>/event/billing/adjustment/account</code></td>
</tr>
<tr>
<td>Top up</td>
<td><code>/event/billing/vouchertopup</code></td>
</tr>
<tr>
<td>Dispute issue</td>
<td><code>/event/billing/dispute</code></td>
</tr>
<tr>
<td>Dispute settled</td>
<td><code>/event/billing/settlement/event</code></td>
</tr>
</tbody>
</table>
Security Considerations for Developers

This chapter explains how to create secure applications for Oracle Communications Billing Care and how to extend Billing Care without compromising security.

About Secure Development

Secure development in Billing Care requires controlling access to users who can access the resource that you want to control. You must do the following:

- Add security controls over new UI features.
- Control who can access the REST service and the limits of that access.

On user sign in, Billing Care calls OPSS, and 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>BRM Event Name (Activity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refund</td>
<td>/event/billing/refund</td>
</tr>
<tr>
<td>Write-off operation</td>
<td>/event/billing/writeoff</td>
</tr>
<tr>
<td>Payment</td>
<td>/event/billing/payment</td>
</tr>
<tr>
<td>Credit limit changes</td>
<td>/event/billing/limit, /event/billing/credit</td>
</tr>
<tr>
<td>Bill Now</td>
<td>/event/notification/billing/start</td>
</tr>
<tr>
<td>Charge sharing group life-cycle operations</td>
<td>/event/group/sharing/charges/create, /event/group/sharing/charges/modify, /event/group/sharing/charges/delete</td>
</tr>
<tr>
<td>Discount sharing group life-cycle operations</td>
<td>/event/group/sharing/discounts/create, /event/group/sharing/discounts/modify, /event/group/sharing/discounts/delete</td>
</tr>
<tr>
<td>Profile (for example, Friends and Family) life-cycle operations</td>
<td>/event/group/sharing/profiles/create, /event/group/sharing/profiles/modify, /event/group/sharing/profiles/delete</td>
</tr>
<tr>
<td>Credit Monitors life-cycle operations</td>
<td>/event/group/sharing/monitor/modify, /event/group/sharing/monitor/delete, /event/group/sharing/profiles/delete</td>
</tr>
<tr>
<td>Account hierarchy operations</td>
<td>/event/group/parent /event/group/member</td>
</tr>
</tbody>
</table>

Table 7--3 (Cont.) Audited List from /config/pin_notify

For information on logging events, including changing the events logged, see the sections on logging customer service representative activities in Oracle Communications Billing and Revenue Management System Administrator’s Guide.
For more information on importing the existing policies, see "Importing the Billing Care Security Policies to OPSS" in *Oracle Communications 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 *Oracle Communications Billing Care SDK Guide*.

### About UI Authorization

On successful sign in to Billing Care, the grants of all resources are fetched and set 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 *Oracle Communications 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.

   ```xml
   <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>
   ```

   **Note:** Do not change key values.

2. Redeploy the customization.

   For more information, see *Oracle Communications Billing Care SDK Guide*.

### Storing 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 the 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, 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" and "Encrypting Passwords Manually" 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 Unix:**
   - 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:
     - `SDK_home` is the directory in which you installed the Billing Care SDK.
     - `oraclepki.jar location` 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.
     - `osdt_cert.jar location` is the path to the osdt_cert.jar file which contains the jars that are used by JAVA PCM library for establishing TLS connection to BRM. The `osdt_cert.jar` is stored in the `SDK_home/BillingCareSDK/samples/Wallet` 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 TLS connection to BRM. The `osdt_core.jar` is stored in the `SDK_home/BillingCareSDK/samples/Wallet` directory.
     - `cet.jar location` is the cet.jar file which contains the APIs that are required for the wallet. The `cet.jar` 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:

```
"/scratch/pin11/wallet" -parameter infranet.log.level -value 1

For example, running the following command without the -value parameter prompts for the values for the infranet.connection entries and stores them in the Billing Care wallet:

```
"/scratch/pin11/wallet" -parameter infranet.connection
```

At the command prompt, enter values listed in Table 7–4 BRM.

### Table 7–4  BRM Connection Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name for connecting to BRM.</td>
</tr>
<tr>
<td>Password</td>
<td>The BRM user’s password.</td>
</tr>
<tr>
<td>Host Name</td>
<td>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.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The TCP port number of the CM or CMMP on the host computer.</td>
</tr>
<tr>
<td>Service Type</td>
<td>The BRM service type.</td>
</tr>
<tr>
<td>Service POID Id</td>
<td>The POID of the BRM service.</td>
</tr>
</tbody>
</table>

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 Billing Care wallet:

```java
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
```

For example, running the following command without the -value parameter prompts for the values for the infranet.connection entries and stores them in the Billing Care wallet:

```java
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 infranet.connection
```

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.
This chapter provides information about installing and implementing Oracle Communications Billing and Revenue Management (BRM) Business Operations Center and its components in a secure configuration.

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 Oracle Communications 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 Manager for authentication
- Oracle Platform Security Services (OPSS) for authorization

Oracle Identity Manager and Oracle Platform Security Services 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 those access 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, define, modify, and delete.

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 8–1).

---

**Table 8–1  Business Operations Center Authorization Policy Components**

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Execution History</td>
<td>Billing</td>
<td>View</td>
<td>Permits users to view the run history of billing jobs.</td>
</tr>
<tr>
<td>Job Execution History</td>
<td>Payment Collection</td>
<td>View</td>
<td>Permits users to view the run history of payment-collection jobs.</td>
</tr>
<tr>
<td>Job Execution History</td>
<td>Invoicing</td>
<td>View</td>
<td>Permits users to view the run history of invoicing jobs.</td>
</tr>
<tr>
<td>Job Execution History</td>
<td>G/L</td>
<td>View</td>
<td>Permits users to view the run history of general ledger (G/L) jobs.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Subscribers</td>
<td>View</td>
<td>Permits users to view subscriber metrics.</td>
</tr>
</tbody>
</table>
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.

**Important:** 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 8–1 shows how authorization policies are mapped to resources and enterprise roles or users:

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics</td>
<td>Subscriptions</td>
<td>View</td>
<td>Permits users to view subscription metrics.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Billed Revenue</td>
<td>View</td>
<td>Permits users to view billed-revenue metrics.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Payments Received</td>
<td>View</td>
<td>Permits users to view payments-received metrics.</td>
</tr>
<tr>
<td>Metrics</td>
<td>A/R</td>
<td>View</td>
<td>Permits users to view accounts receivable (A/R) metrics.</td>
</tr>
<tr>
<td>Job</td>
<td>Jobs</td>
<td>Any</td>
<td>Permits users to view, create, modify, and delete any type of job.</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Permits users to perform all operations.</td>
</tr>
</tbody>
</table>
Storing 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" and "Encrypting Passwords Manually" 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 Unix:

- 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 JAVA PCM library for establishing 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 TLS connection to BRM. The osdt_core.jar file is stored in the BOC_HOME/lib directory.
  - `cet.jar_location` is the cet.jar file which contains the APIs that are required for the wallet. The cet.jar is stored in the BOC homeowner 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:

  ```
  ```

  For example, running the following command without the `-value` parameter 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 8–2 BRM.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name for connecting to BRM.</td>
</tr>
<tr>
<td>Password</td>
<td>The BRM user’s password.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The IP address or the host name of the machine on which the primary BRM</td>
</tr>
<tr>
<td></td>
<td>Connection Manager (CM) or CM Master Process (CMMP) are running.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The TCP port number of the CM or CMMP on the host computer.</td>
</tr>
</tbody>
</table>
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
  ```

  For example, running the following command without the `-value` parameter prompts for the values for the infranet.connection entries and stores them in the Business Operations Center wallet:

  ```
  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 infranet.connection
  ```

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*. 

---

**Table 8–2 (Cont.) BRM Connection Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>The BRM service type.</td>
</tr>
<tr>
<td>Service POID Id</td>
<td>The POID of the BRM service.</td>
</tr>
</tbody>
</table>
Secure Deployment Checklist

This document provides checklists for installing Oracle Communications Billing and Revenue Management (BRM) and Pricing Design Center (PDC) securely.

**BRM Checklist**

The following security checklist lists guidelines to help you secure Oracle Communications Billing and Revenue Management (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 your Oracle Communications Pricing Design Center (PDC) securely.

1. Pre-installation 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. Post-installation 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 references. These log files have file permission 640 (owner can read/write, group members can read, others cannot do anything) by default.