Oracle® Communications Billing and Revenue Management

Security Guide

Release 7.5

E39919-07

April 2016

ORACLE®

Oracle Communications Billing and Revenue Management Security Guide, Release 7.5

E39919-07

Contents

Preface

This guide provides guidelines and recommendations for managing security in Oracle Communications Billing and Revenue Management (BRM). It also describes how to install BRM securely.

Audience

This guide is intended for developers and system administrators.

Related Documents

For information on implementing system security in BRM, see *BRM System Administrator's Guide*.

Accessing Oracle Communications Documentation

BRM documentation and additional Oracle documentation; such as Oracle Database documentation, is available from Oracle Help Center:

http://docs.oracle.com

Additional Oracle Communications documentation is available from the Oracle software delivery Web site:

https://edelivery.oracle.com

Documentation Accessibility

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

Access to Oracle Support

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

Document Revision History

The following table lists the revision history for this document:

Version	Date	Description
E39919-01	March 2013	Initial release.
E39919-02	August 2014	Documentation updates for BRM 7.5 Patch Set 9. ■ Added an entry for "Securing Sensitive Customer Data".
E39919-03	January 2015	Documentation updates for BRM 7.5 Patch Set 11. ■ Updated "Basic Security Considerations".
E39919-04	June 2015	Documentation updates for BRM 7.5 Patch Set 12. ■ Updated the following section: Pre-Installation Tasks ■ Added the following sections: Use Strong Passwords for BRM User Schema. Enable SSL/TLS for SQL*NET. Use Secure TLS Connections. Enforce Password Management. Access Control in BRM Web Services Manager. Using Oracle ZT Encryption Scheme. Using Credit Card Tokenization. Masking Sensitive Data in Log Files. Securing BRM Network Ports.
E39919-05	August 2015	Documentation updates for BRM 7.5 Maintenance Patch Set 1. ■ Updated the following section: Use Secure TLS Connections
E39919-06	December 2015	Documentation updates for BRM 7.5 Patch Set 14. ■ Updated the following section: Using Oracle ZT Encryption Scheme
E39919-07	April 2016	Documentation updates for BRM 7.5 Patch Set 15. ■ Added the following chapter: Business Operations Center Security

1

BRM Security Overview

This chapter 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 focussed 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:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

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?**

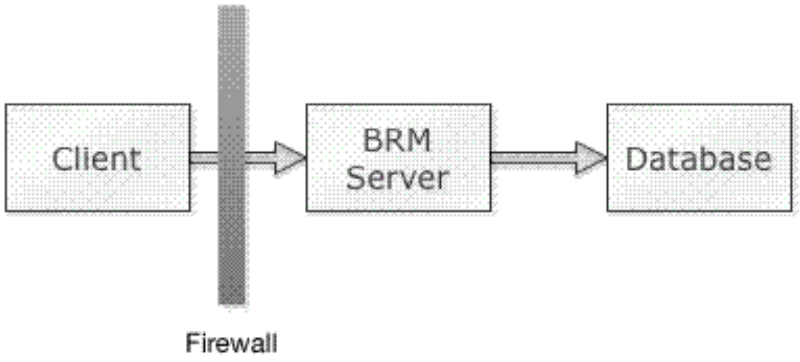
  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource helps you protect it properly.

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 5
- Hardening Tips for the Red Hat Enterprise Linux 5

Oracle Database Security

See *Oracle Database Security Guide*.

2

Performing a Secure BRM Installation

This chapter 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.
  - Enable remote console access to run various operational processes such as billing and reporting. Do not use Telnet or rlogin, which do not encrypt passwords.
  - Do not disable SSH. Use SSH for remote console access to prevent password sniffing.
  - Disable file transfer protocol (FTP) or other remote file transfer services if there are no operations requiring them. For example, if there are no usage records, you do not need file transfer services enabled. If file transfer services are required, use secure FTP (SFTP) instead of FTP.
  - 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, user name, 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
- Use Strong Passwords for BRM User Schema
- Enable SSL/TLS for SQL*NET
- Use Secure TLS Connections
- Enforce Password Management
- Tighten File Permissions
- Configure Maximum Number of Invalid Login Attempts
- Log Customer Service Representative Activities
- Configure Session Timeout
- Integrate Paymentech
- Mask Sensitive Customer Data

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 the 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.
- Change the default password of the root customer service representative's (CSR's) account (user name root-0.0.0.1) immediately after installation.
- In any Oracle environment (production or test), assign strong, secure passwords to the SYS and SYSTEM user accounts immediately upon successful installation of the database server. Under no circumstances should the passwords for SYS and SYSTEM retain their default values. Similarly, for production environments, do not use default passwords for any administrative accounts, including SYSMAN and DBSNMP.
- In any Oracle development or test environment that is using real-world data for analysis, assign the same level of security as a production environment.

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

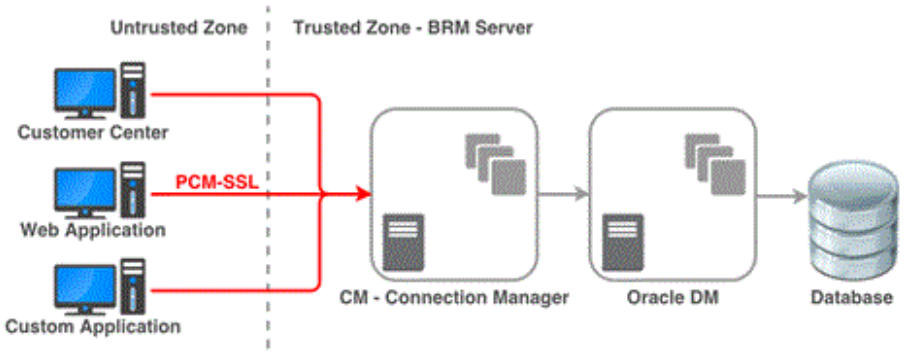
You can configure BRM to communicate between the various components using encrypted TLS sockets by setting the **enable_ssl** entry in the CM's **pin.conf** configuration file. When this configuration is enabled, BRM uses TLS sockets for any communication between its components such as Oracle Data Manager (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 such as Customer Center, Payment Tool 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



Note: BRM pipeline batch rating engine and BRM real-time pipeline used for advanced discounting do not support SSL/TLS connections. Therefore, the communication between BRM CM and BRM real-time pipeline is not encrypted.

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.

With BRM 7.5 Patch Set 6, a policy implementation for enforcing the password complexity rules was introduced. However, by default, these password complexity rules are not enabled. You enable these rules by modifying the PCM_OP_CUST_POL_VALID_PASSWD policy opcode.

See the discussion about PCM_OP_CUST_POL_VALID_PASSWD in *BRM Developer's Reference* 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.

If the maximum number of consecutive unsuccessful login attempts is reached, the user account is locked. Use the **pin_unlock_service** utility to unlock the account and reset the password of the locked account.

See the discussion about unlocking a locked CSR account in *BRM System Administrator's Guide* for more information.

Log Customer Service Representative Activities

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.

Configure Session Timeout

You can set a time interval in minutes after which the child process or thread terminates by using the **cm_timeout** entry in the CM's **pin.conf** file. If your BRM installation has multiple CMs, you must set the **cm_timeout** entry in the **pin.conf** file of each CM.

If a BRM connection reaches the maximum idle duration specified in the **cm_timeout** entry, the BRM server closes the connection.

Integrate Paymentech

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

Mask Sensitive Customer Data

You can mask sensitive customer data such as financial payment information and passwords in system responses and logs. You can configure masking of sensitive data fields stored in string format in system responses to clients and logging to protect subscriber information.

See "About Securing Sensitive Customer Data with Masking" in *BRM Managing Customers* for more information on setting up data masking.

3

Managing BRM Security

This chapter 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 BRM 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 Customer Center, Pricing Center, and other 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.

Permissions can be set up using both Permissioning Center and Customer Center. However, the user adding, changing, or deleting permissions must have the correct permissions to do so. In most cases, only a person with root access, such as a system administrator, is granted permission to change CSR permissions.

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

Roles can be hierarchical, by creating child roles and associating them with a parent role. At each level above the bottom of the hierarchy, the child roles can also be parent

roles. A child role inherits all permission settings that are associated with its parent role.

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

Managing CSR Passwords

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

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

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

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 "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 class 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 price list.

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 Storable Class Editor, which will add a flag attribute in the metadata defining the field in the BRM data dictionary (PIN_FLD_ENCRYPTABLE).

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

See "About Encrypting Information" in *BRM Developer'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.

Customers upgrading to BRM 7.5 Patch Set 10 or later may 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.

4

Security Considerations for Developers

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

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.

5

Business Operations Center Security

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 Entitlements Server for authorization

Oracle Identity Manager and Oracle Entitlements Server 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 Entitlements Server*

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 Entitlements Server handles all authorization tasks for Business Operations Center.

A user who has not been granted any entitlements in Oracle Entitlements Server 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 Entitlements Server*.

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 5–1).

Table 5–1 Business Operations Center Authorization Policy Components

Resource Type	Resource	Action	Description
Job Execution History	Billing	View	Permits users to view the run history of billing jobs.
Job Execution History	Payment Collection	View	Permits users to view the run history of payment-collection jobs.
Job Execution History	Invoicing	View	Permits users to view the run history of invoicing jobs.
Job Execution History	G/L	View	Permits users to view the run history of general ledger (G/L) jobs.
Metrics	Subscribers	View	Permits users to view subscriber metrics.
Metrics	Subscriptions	View	Permits users to view subscription metrics.

Table 5–1 (Cont.) Business Operations Center Authorization Policy Components

Resource Type	Resource	Action	Description
Metrics	Billed Revenue	View	Permits users to view billed-revenue metrics.
Metrics	Payments Received	View	Permits users to view payments-received metrics.
Metrics	A/R	View	Permits users to view accounts receivable (A/R) metrics.
Job	Jobs	Any	Permits users to view, create, modify, and delete any type of job.
Any	Any	Any	Permits users to perform all operations.

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 Entitlements Server 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 Security Policies into OES" in *Business Operations Center Installation Guide*.

2. In Oracle Entitlements Server, 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 Entitlements Server*.

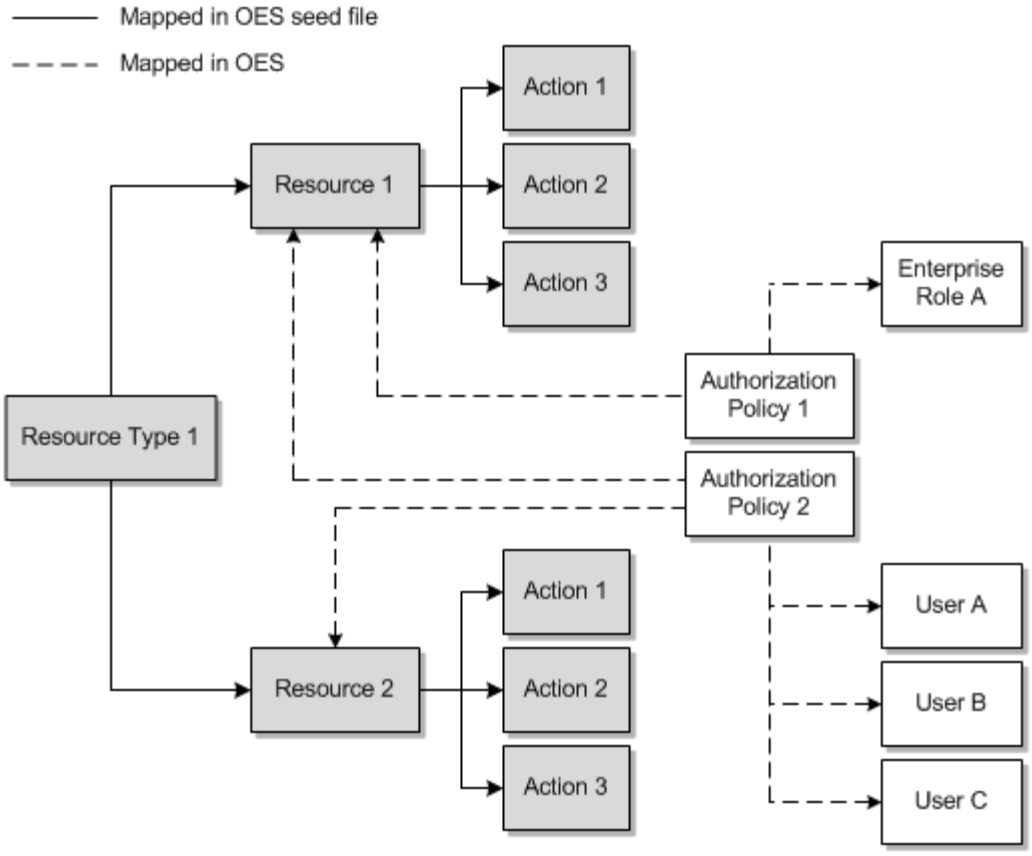
3. Associate the authorization policy with a user or an enterprise role.

   For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*.

4. Redeploy all changes made in Oracle Entitlements Server.

Figure 5–1 shows how authorization policies are mapped to resources and enterprise roles or users:

Figure 5–1 Mapping Authorization Policies to Resources and Enterprise Roles or Users



A

Secure Deployment 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. Mask sensitive customer data in system responses and logging.
9. Contact Oracle Security Products if you come across a vulnerability in Oracle Database.