Oracle® Communications Billing Care

Security Guide

Release 7.5

E39517-04

December 2016

ORACLE®

Oracle Communications Billing Care Security Guide, Release 7.5

E39517-04

Contents

Preface

This guide provides guidelines and recommendations for installing, configuring, and customizing Oracle Communications Billing Care and its components in a secure configuration.

Audience

This document is intended for system administrators, application administrators, and developers.

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.

Related Documents

For more information, see the following documents regarding Billing Care and some of other the Oracle products that are referred to in this guide.

- *Oracle Communications Billing Care Installation Guide*
- *Oracle Communications Billing and Revenue Management System Administrator's Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*
- *Administering Security for Oracle WebLogic Server*

1

Billing Care Security Overview

This chapter provides guidelines and recommendations for setting up Oracle Communications Billing Care components in a secure configuration.

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.
- 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. Refer to the "Critical Patch Updates and Security Alerts" Web site:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`
- Limit privileges as much as possible. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically.

  Refer to "Implementing Billing Care Security" for more information.
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Install software securely. For example, use firewalls and secure passwords.

  Refer to *Oracle Communications Billing Care Installation Guide* for more information.
- Learn about and use the Billing Care security features.

  Refer to "Implementing Billing Care Security" for more information.
- Use secure development practices. For example, take advantage of existing security functionality instead of creating your own application security. Refer to "Security Considerations for Developers" for more information.
- Avoid using the option to have an application remember passwords for admin logins and passwords. For example, do not select the **Remember Password** check box in a login screen.
- Apply the latest patch set for JDK to ensure that your running JDK has the latest security fixes.

2

Installing Billing Care

This chapter provides an overview of some aspects of secure installation Oracle Communications Billing Care.

About Installing Billing Care

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. Refer to *Oracle Communications Billing Care Installation Guide* for Billing Care installation instructions, including all the required products and related tasks, for example, setting up keystores and SSL for WebLogic Server.

Oracle Entitlement Server and Oracle Identity Manager provide authentication and authorization capabilities for Billing Care. These products are also required in a Billing Care implementation. Refer to *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite* and *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server* for general information about these products.

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 **Infranet.properties** file. For a secure installation, you must encrypt the BIP password. You use Oracle WebLogic Server to perform the encryption. Refer to *Oracle Communications Billing Care Installation Guide* for more information.

3

Implementing Billing Care Security

This chapter describes how to implement Oracle Communications Billing Care security.

Introduction to 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, refer to *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, refer to *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. Oracle Entitlement Server (OES) handles all authorization tasks for Billing Care. This section provides an overview for setting up and maintaining the 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 application's functionality being secured, for example, **AdjustmentResource**, 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, for example, the maximum payment amount. Obligations are the property of Authorization Policy.
- Authorization Policy: a collection of 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 OES 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 OES seed file containing all of the resource types, resources, actions, obligations, and four sample authorization policies (regular CSR, senior CSR, auditor, and billing admin).

For instructions on importing the seed file, refer to *Oracle Fusion Middleware Administering Oracle Entitlements Server*.

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\OESDataModel**.

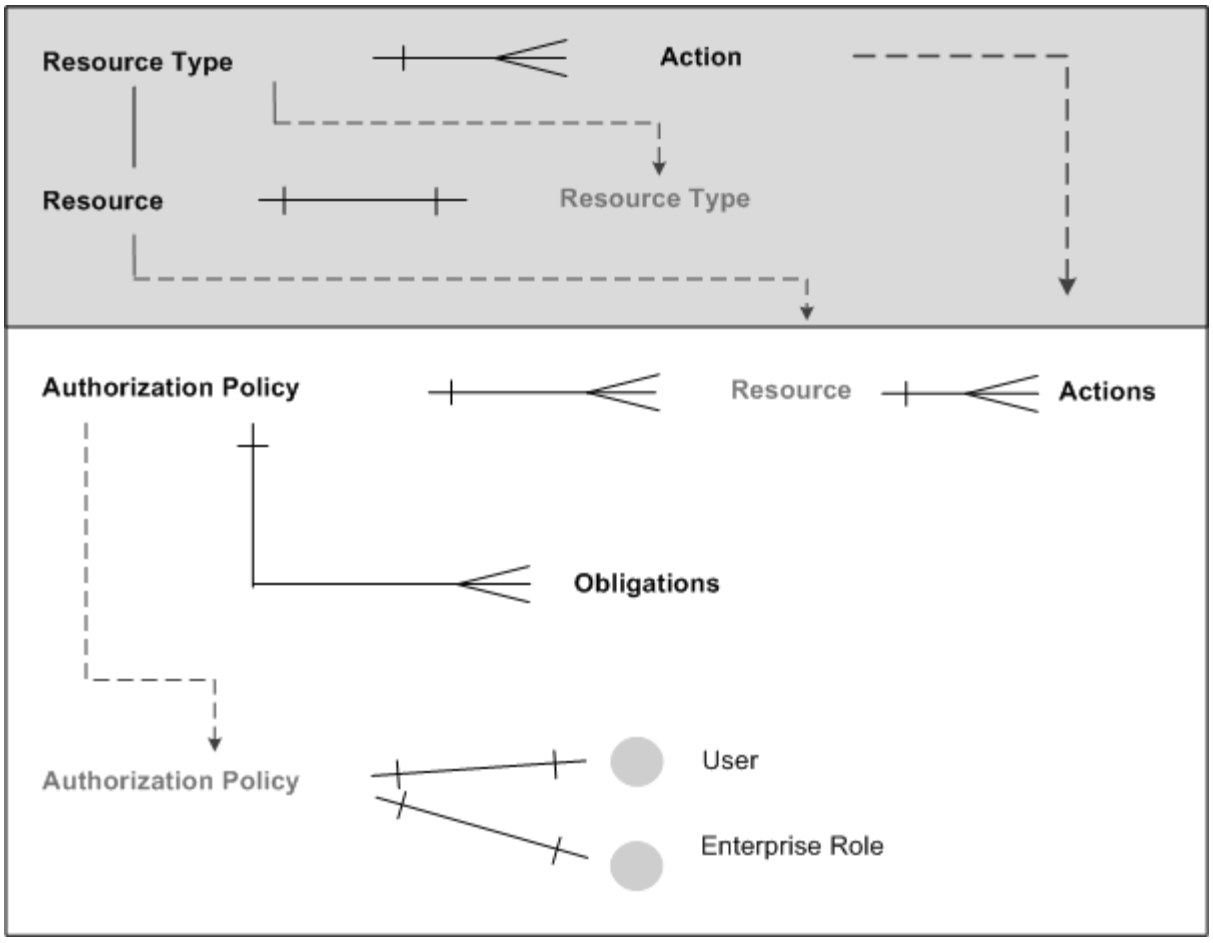
Figure 3–1 describes the authorization flow:

1. The shaded area refers to areas defined in the OES seed file. (You load the seed file before performing the configuration.)
2. The lower area represents how in OES, an authorization policy is mapped to one or more resources, which 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 3–2.

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

Figure 3–1 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 of the enterprise users, authenticates Billing Care sign in requests. The authorization scheme allows access only to users that been granted resources in OES.

Table 3–1 shows the Billing Care Authorization Resources. Resources grant permissions to perform general CSR or more advanced A/R tasks, for example.

Table 3–1 Authorization Resources

Resource Type	Resource	Actions	Description
SuperUserType	SuperUserResource	Any	Enables you to create users free of restrictions, including when the user's profile contains other resources. The only exception is the ReadOnlyType, which takes precedence over all other resource types.

Table 3–1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
ReadOnlyType	ReadOnlyResource	Any	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.
PaymentResourceType	PaymentResource	Allocate, Audit, BatchProcess, Make, ReassignHandler, Reverse, SuspenseAccess, SuspenseAllocate, SuspenseMake, SuspenseMove, SuspenseReverse	Allocate: Allows user to allocate payments. Audit: Allows user to view audit information on Payment Details overlay. (Audit information in payment suspense screen is always visible.) BatchProcess: Displays the Batch Payment button on the landing page. Make: Allows user to make payments. ReassignHandler: Prevents user from assigning and reassigning batch payment handlers to suspended payments. Reverse: Allows user to reverse payments. SuspenseAccess: Prevents user from accessing any payment suspense functionality. SuspenseAllocate: Allows user to allocate suspended payments partially or fully to an account. SuspenseMake: Prevents user from making suspended payments. SuspenseMove: Allows user to move posted payments into suspended status. SuspenseReverse: Allows user to reverse suspended payments. Returned as an obligation; OES returns a number, which is interpreted as a limit. See Table 3–2 for transaction limits.

Table 3–1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
ServiceResourceType	ServiceResource	Cancel, Edit, Inactivate, Make, Reactivate, OfferInactivate, OfferTerminate, OfferReactivate, Terminate	Cancel: Prevents user from canceling services. Edit: Gives user read-only access to the Asset Details page. Make: Blocks user's access to the Select and Configure pages of the customer creation wizard. Hides the Purchase button. Inactivate: Prevents user from inactivating services. OfferInactivate: Prevents user from inactivating product and discount offers. OfferReactivate: Prevents user from reactivating product and discount offers. OfferTerminate: Prevents user from terminating product and discount offers. Reactivate: Prevents user from reactivating services. Terminate: Prevents user from terminating services.
AdjustmentCurrencyResourceType	AdjustmentResource	Allocate, Make	Allocate: Prevents user from allocating currency adjustments. Make: Prevents users from making adjustments. Uses a policy that constrains the maximum payment amount as a function of CSRs access level. See Table 3–2 for transaction limits.
WriteoffResourceType	WriteoffResource	Make	Prevents user from writing off accounts. Policy on the minimum and maximum write-off amount applies. See Table 3–2 for transaction limits.
AdjustmentNonCurrencyResourceType	AdjustmentNonCurrency Resource	Make	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 3–2 for transaction limits.

Table 3–1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
DisputeResourceType	DisputeResource	Raise, Settle	Raise: Disables bill dispute functionality. Settle: Disables bill dispute settlement functionality. Policy on the maximum dispute amount applies. See Table 3–2 for transaction limits.
RefundResourceType	RefundResource	Make	Allows user to refund bills.
AccountResourceType	AccountResource	Make, Modify, Search Transition, View	Make: Allows user to create accounts. Modify: Prevents user from adding, deleting, or saving contact information. Search: Allows user to access search functionality. Transition: Enables changing account status. View: Enables user to view account profile and other customer information.
ConfigurationsArtifactsType	ConfigurationArtifactsResource	View	Allows user to read all configuration-related REST APIs (for example, authorization profiles).
InvoiceImageType	InvoiceImageResource	View	Allows user to view invoices.
NoteResourceType	NoteResource	Comment	Allows user to make comments.
PaymentMethodResourceType	PaymentMethodResource	Add, Delete, Modify	Add: Allows user to add payment method. Delete: Allows user to delete payment method. Modify: Allows user to change payment method.

Table 3–1 (Cont.) Authorization Resources

Resource Type	Resource	Actions	Description
TaxExemptionResourceType	TaxExemptionResource	Add, Delete, Modify	Add: Allows user to add tax exemptions whether account has or does not have prior tax exemptions. Delete: Allows user to delete tax exemptions. Modify: Allows user to save changes to tax exemption attributes.
BillUnitResourceType	BillUnitResource	Add, Delete, Modify	Add: Allows user to create bill units. Delete: Reserved for future use. Modify: Allows user to change the bill unit.
BillResourceType	BillResource	BillNow	BillNow: Allows user to perform Bill Now operations.

Policies on Transaction Limits

Some of the resources listed in Table 3–1 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 Oracle Entitlement Server.

Table 3–2 lists the attributes that require system administrators to configure transaction limits (values).

Table 3–2 Listing of Transaction Limits (Obligations)

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

About Auditing

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

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

To 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, refer to *Oracle Communications Billing and Revenue Management System Administrator's Guide*.

Table 3–3 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 3–3 Audited List from /config/pin_notify

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

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

Task	BRM Event Name (Activity)
Account hierarchy operations	/event/group/parent /event/group/member

For information on logging events, including changing the events logged, see the sections on logging customer service representative activities *Oracle Communications Billing and Revenue Management System Administrator's Guide*.

4

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 Oracle Entitlement Server (OES), and OES provides authorization if appropriate. Additionally, OES 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 OES

To develop secured custom REST APIs or UIs, you need (OES) resource types for authorization.

To create a resource type with OES:

1. Log in to Oracle Entitlements Server.
2. Select the **Billing Care** application.
3. Create a resource type with the relevant actions.
4. Create a resource from the resource type.
5. Create the authorization policy and add the external roles as principals and resource as targets by checking the required grants (actions) on resource.
6. Click the triangle symbol on Applications in the left side panel.
7. Double click **Billing Care**.
8. Click the **Policy Distribution** tab.
9. Expand the WebLogic Server Security Module for the **Billing Care** application binding.
10. Click **Distribute**, and then click the refresh icon.

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

About REST API Authorization

To control the access of custom REST services and operations to authenticated users, define resource types in OES as described in "Creating a Resource Type with OES".

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 OES resource types:

   In this example, the new resource type **CreditProfileResourceType** is added.

   Note: Do not change key values.

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

2. Redeploy the customization.

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