Oracle® Communications Billing and Revenue Management

Billing Care Installation Guide



Release 16.26.0
G54439-01
October 2026

ORACLE

Oracle Communications Billing and Revenue Management Billing Care Installation Guide, Release 16.26.0

G54439-01

Copyright © 2017, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

About This Content

1 Billing Care Installation Overview

About Installing Billing Care 1
Overview of the Billing Care Installation Steps 1
Ensuring a Successful Billing Care Installation 2

2 Planning Your Billing Care Installation

About Planning Your Billing Care Installation 1

3 Installing Billing Care

Downloading the Billing Care Installer 1
Running the Billing Care Installer 1
About Installation Logs 8

4 Configuring Billing Care

About Billing Care Configuration Files 1
Configuring Billing Care Application Settings 2
Configuring BRM Connections 3
Configuring SSL or TLS for Billing Care 5
Configuring OIDC Authentication 7
Configuring Role Mapping 8
- Using LDAP 9
- Using Keycloak or IDCS 11
- Using a Static User List 12
- Using Users Configured for Basic Authentication 12
- Matching Users to Assignment Roles 13

Configuring Billing Care Authorization 14
Configuring the Oracle Analytics Publisher Connection 15
- Using the Signed-In User’s Access Token 16

Copyright © 2017, 2026, Oracle and/or its affiliates.

Using an OAuth Service Client 17
Using Basic Authentication 18
Configuring Certificate Trust and Credentials 19

5 Verifying the Billing Care Installation

Starting and Stopping Billing Care 1
Logging In to Billing Care 1

Copyright © 2017, 2026, Oracle and/or its affiliates.

About This Content

This guide provides instructions for installing Oracle Communications Billing Care.

Audience

This guide is intended for system administrators, database administrators, and developers who install and configure Billing Care. Billing Care requires Oracle Database and Oracle Identity and Access Management Suite products. See the documentation for those products for additional installation and configuration instructions.

Copyright © 2017, 2026, Oracle and/or its affiliates.

1

Billing Care Installation Overview

Learn about the Oracle Communications Billing Care installer.

Topics in this document:

- About Installing Billing Care
- Overview of the Billing Care Installation Steps
- Ensuring a Successful Billing Care Installation

About Installing Billing Care

Billing Care installation should be performed only by experienced system administrators. You must be familiar with the Linux operating system and installing Java-related packages before you begin the installation.

The Billing Care installer does one or more of the following, depending on which one you choose during the installation process:

- Installs the Billing Care UI
- Installs the Billing Care Migration Utility
- Installs the Billing Care SDK
- Installs the Billing Care REST API

Overview of the Billing Care Installation Steps

Installing Billing Care involves the following steps:

1. Plan your installation. Determine the scale of your implementation, identify the required hosts and components, and plan the system topology.

   See "Planning Your Billing Care Installation ".

2. Review requirements and gather configuration information, such as:
   - Hardware requirements, such as disk space and physical RAM.
   - Software requirements, such as operating system (OS) versions.
   - Information requirements, such as IP addresses, administrative user credentials, host names, and port numbers.
3. Install Billing Care. Use Oracle Universal Installer (OUI) to select the required components and configure the installation settings.

   See "Installing Billing Care".

4. Complete the configuration. Review the settings that the installer creates and configure any additional settings required for your environment.

   See "Configuring Billing Care".

Copyright © 2017, 2026, Oracle and/or its affiliates.

5. Start Billing Care. Run **start_billingcare.sh** from *Oracle_home*/**billingcare_rest/bin**, where *Oracle_home* is the Oracle Home directory you select during installation.

   See "Starting and Stopping Billing Care".

6. Verify the installation.

   See "Verifying the Billing Care Installation".

Ensuring a Successful Billing Care Installation

Before you install Billing Care, verify the system requirements and obtain the configuration values required by the installer.

To prepare for installation:

- Verify that your system meets the hardware and software requirements.
- Gather the required host names, port numbers, and BRM connection details.
- For installations that require authentication, ask your security administrator to configure an OpenID Connect (OIDC) identity provider and provide the client ID, client secret, and other required connection settings. See "Configuring OIDC Authentication".
- If you enable SSL/TLS, obtain the required keystore and truststore files and their access details. See "Configuring SSL or TLS for Billing Care".
- Record configuration values for use during installation. Store passwords and client secrets securely.

Copyright © 2017, 2026, Oracle and/or its affiliates.

2

Planning Your Billing Care Installation

Learn how to plan for your Oracle Communications Billing Care installation.

Topics in this document:

- About Planning Your Billing Care Installation

About Planning Your Billing Care Installation

Before you install Oracle Communications Billing Care, plan the deployment capacity, connections, and security settings required for your environment.

- **Deployment capacity:** Determine the number of Billing Care hosts required for your expected user count and transaction volume. Verify the hardware and software requirements in *BRM Compatibility Matrix*.
- **Network connections:** Identify the host names and ports required for Billing Care to communicate with BRM and any optional services, such as an LDAP directory or Oracle Analytics Publisher.
- **Authentication and authorization:** Production installations require authentication and authorization. Choose an OpenID Connect (OIDC) identity provider for authentication and single sign-on. Your security administrator configures the provider using its product documentation and supplies the connection details required by the Billing Care installer. Determine the roles and permissions users require. For authentication and authorization guidance, see "Billing Care Security" in *BRM Security Guide*.
- **Secure communication:** Prepare the certificates, keystores, truststores, and credentials required to secure Billing Care application and administration connections and communication with BRM. Select the corresponding SSL options during installation. Restrict access to the Billing Care hosts.

Copyright © 2017, 2026, Oracle and/or its affiliates.

3

Installing Billing Care

Learn how to install Oracle Communications Billing Care.

Topics in this document:

- Downloading the Billing Care Installer
- Running the Billing Care Installer
- About Installation Logs

Downloading the Billing Care Installer

You can download the Billing Care software from one of the following locations:

- For Billing Care 16.26.0 or any 16.26.0.*x* maintenance release: From the Oracle software delivery website (https://edelivery.oracle.com)
- For any 16.26.0.*x*.*y* patch set release: From the Oracle support website (https://support.oracle.com)

Search for and download the **Oracle Communications Billing Care 16.26.0.*x*.*y*.0** software, where *x* refers to the maintenance release and *y* refers to the patch set release of BRM that you are installing.

The Zip archive includes the installer: **BillingCare_generic.jar**

Running the Billing Care Installer

Run the Billing Care installer as a user who has permissions to write to the **oraInventory** directory.

To install Billing Care:

1. Verify that your Java Development Kit (JDK) is installed correctly. Ensure that you set your **JAVA_HOME** environment variable and that the **$JAVA_HOME/bin** directory is in your path.
2. Download the Billing Care installer. See "Downloading the Billing Care Installer" for more information.
3. From the location where you extracted the downloaded software package, run the following command to start the Billing Care installer:

   ```
   java -jar BillingCare_generic.jar
   ```

   If you are using an existing or custom Oracle inventory location, include the **-invPtrLoc** flag and an Oracle Inventory path location in the Java command that starts the Billing Care installer, for example:

   ```
   java -jar BillingCare_generic.jar -invPtrLoc invPath/oraInst.loc
   ```

   where *invPath* is the Oracle Inventory path.
4. In the Welcome window, click **Next**.

Copyright © 2017, 2026, Oracle and/or its affiliates.

5. In the Installation Location window, enter or browse to your Oracle Home directory and then click **Next**.
6. In the Feature Sets Selection window, select the components to install from the list in Table 3-1 and then click **Next**.

Table 3-1 Feature Sets Details

Option	Description
Billing Care UI	Installs the Billing Care UI. Selecting this component automatically selects the Billing Care REST API, which is required by the UI.
Billing Care REST API	Installs the Billing Care REST API and its configuration. This component provides the services used by the Billing Care UI and integrations.
Billing Care SDK	Installs the Billing Care Software Development Kit (SDK). Use the SDK to develop and package supported customizations and extensions for Billing Care.
Billing Care Migration Utility	Installs the Billing Care Migration Utility, a command-line tool for migrating Billing Care customizations to the Helidon-based runtime. It supports migration of the following: • authorization policy and UI authorization • customer configuration and configuration code • SDK-based customizations • localization code and bundle • Java Util Logging analysis It also includes an extension endpoint-catalog sample.

If you select **Billing Care UI**, **Billing Care REST API** is selected automatically. You cannot install the UI without the REST API, but you can install the REST API without the UI.

7. In the Server Details window, enter the details listed in Table 3-2 and then click **Next**.

Table 3-2 Server Details

Field	Description
Host Name	Enter the host name or IP address of the system where you are installing the **Billing Care REST API**. **Note:** The installer always installs **Billing Care** on the local system where it is run. Ensure that the specified host name or IP address is configured on the local system. If you do not, the application may fail to start because it cannot bind to the specified address. This field is mandatory. The default value is **localhost**.
Port Number	Enter an available port number for the Billing Care application. This field is mandatory. The default value is **8082**.
SSL Enabled	Select an SSL option: • To use one-way SSL, select **Yes - One Way**. • To use two-way SSL, select **Yes - Two Way**. • To deploy Billing Care without SSL, select **No**. You do not need to enter any values in the keystore and truststore fields in this window. This field is mandatory. The default value is **Yes - One Way**.
Keystore Type	The only type of keystore file to use to establish the SSL connection is **PKCS12**.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 3-2 (Cont.) Server Details

Field	Description
Keystore Location	Enter the name and path of your PKCS12 keystore file for SSL connection. The file must have a **.p12** extension. Otherwise, a validation warning is displayed. This field is mandatory when one-way or two-way SSL is enabled.
Keystore Password	Enter the password used to establish the SSL connection. This field is mandatory when one-way or two-way SSL is enabled.
Keystore Alias	Enter the alias used to access the specific certificate in the keystore. This field is mandatory only if an alias was specified when the keystore was created.
Truststore Type	The only type of truststore file to use to establish the SSL connection is **PKCS12**.
Truststore Location	Enter the name and path of your truststore file for SSL authentication. Select a file with a **.p12** extension. Otherwise, a warning message is displayed. This field is mandatory if **SSL Enabled** is set to **Yes - Two Way** and optional if **SSL Enabled** is set to **Yes - One Way**. It has no default value.
Truststore Password	Enter the password used to establish the SSL connection. This field is mandatory if **SSL Enabled** is set to **Yes - Two Way** or if **SSL Enabled** is set to **Yes - One Way** and **Truststore Location** is set. It has no default value.
Wallet Password	Enter the password for the Billing Care application wallet. This field is mandatory. It has no default value.
Confirm Wallet Password	Reenter the Billing Care application wallet password for confirmation. This field is mandatory. It has no default value.

8. In the Management and Observability window, view the details listed in Table 3-3 and then click **Next**.

   This screen enables you to configure the settings required for Billing Care administrative operations, management, and monitoring. It is automatically populated based on the configuration specified in the previous Server Details window. You can modify the value if required.

Table 3-3 Management and Observability

Field	Description
Admin Port Number	Enter an available port number for the Billing Care application to use for administrative operations. This field is mandatory. The default value is **8084**.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 3-3 (Cont.) Management and Observability

Field	Description
SSL Enabled	Select an SSL option for administrative operations. It is populated with the selection from the Server Details window. • To use one-way SSL, select **Yes - One Way**. • To use two-way SSL, select **Yes - Two Way**. • To deploy Billing Care without SSL, select **No**. You do not need to enter any values in the keystore and truststore fields in this window. This field is mandatory. The default value is **Yes - One Way**.
Keystore Type	The only type of keystore file to use to establish the SSL connection is **PKCS12**.
Keystore Location	Enter the name and path of your PKCS12 keystore file for SSL authentication. The file must have a **.p12** extension. Otherwise, a validation warning is displayed. This field is mandatory when one-way or two-way SSL is enabled.
Keystore Password	Enter the password used to establish the SSL connection for administrative operations. This field is mandatory if you are using PKCS12-type SSL. It has no default value.
Keystore Alias	Enter the alias used to access the specific certificate in the keystore for administrative operations. This field is mandatory only if an alias was specified when the keystore was created.
Truststore Type	The only type of truststore file to use to establish the SSL connection for administrative operations is **PKCS12**.
Truststore Location	Enter the name and path of your truststore file for SSL authentication for administrative operations. Select a file with a **.p12** extension. Otherwise, a warning message is displayed. This field is mandatory when one-way or two-way SSL is enabled.
Truststore Password	Enter the password used to establish the SSL connection for administrative operations. This field is mandatory if **SSL Enabled** is set to **Yes - Two Way** or if **SSL Enabled** is set to **Yes - One Way** and **Truststore Location** is set. It has no default value.
Enable Metrics	Select this option to enable metrics collection for Billing Care administrative operations.

> **Note**
>
> The Billing Care installer does not proceed until it verifies that the information you entered is valid.

9. In the BRM Connection Details window, enter the details listed in Table 3-4 and then click **Next**.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 3-4 BRM Connection Details

Field	Description
Host Name	Enter the IP address or host name of the system on which the primary BRM Connection Manager (CM) or CM Master Process (CMMP) is running. This field is mandatory. The default value is **localhost**.
Port Number	Enter the TCP port number of the CM or CMMP on the host system. This field is mandatory. The default value is **11960**.
User Name	Enter the username for connecting to BRM. This field is mandatory. The default value is **bc_client.0.0.0.1**.
Password	Enter the BRM user's password. This field is mandatory. It has no default value.
Service Type	Enter the BRM service type. This field is mandatory. The default value is **/service/admin_client**.
Service POID Id	Enter the Portal object ID (POID) of the BRM service. This field is mandatory. The default value is **416**.
SSL Wallet Location	Enter the location of the SSL wallet to use for the BRM connection. You must enter a wallet location if you want Billing Care to communicate with BRM using SSL. This field is optional. If it is not specified, SSL connection to BRM is disabled.

10. In the Batch Payment Details window, enter the details listed in Table 3-5 and then click **Next**.

Table 3-5 Batch Payment Details

Field	Description
Batch Payment Files Location	Enter the directory in which batch payment files are placed for uploading and processing by Billing Care. The installer creates these folders in the directory you specify: **error**, **processed**, **processing**, and **unprocessed**. This field is mandatory. The default value is *Oracle_home*/**billingcare_rest/batch_payments/data_files**.
Batch Payment Templates Location	Enter the directory in which payment file templates are installed. This field is mandatory. The default value is *Oracle_home*/**billingcare_rest/batch_payments/template_files**.

11. In the Security Details window, select whether to configure Billing Care security and then click **Next**.

    - Select **Yes** to configure an OpenID Connect (OIDC) security provider. Always select this option for a production or staging environment. You can also select it for a development or testing environment. This option is the default.

> **Note**
>
> You must select **Yes** if you want to use LDAP to retrieve customer-service representative (CSR) details.

Copyright © 2017, 2026, Oracle and/or its affiliates.

- Select **No** if you do not want to configure an OIDC security provider. You may select this option for a development or testing environment. If you select this option, go to step 13.

12. In the OpenID Connect Security Provider window, enter the details listed in Table 3-6 and then click **Next**.

Table 3-6 OpenID Connect Security Provider

Field	Description
Identity URL	Enter the identity URL of an Identity Provider. This field is mandatory. It has no default value.
Scope Audience	Enter the primary audience for the confidential OAuth application. This field is mandatory. It has no default value.
Audience	Enter a secondary audience if it is configured. Otherwise, reenter the value from the **Scope Audience** field. This field is mandatory. It has no default value.
Client ID	Enter the client ID of the confidential OAuth application created for Billing Care in the Identity Provider. This field is mandatory. It has no default value.
Client Secret	Enter the client secret of the confidential OAuth application. This field is mandatory. It has no default value.
Cookie Encryption Password	Enter the cookie encryption password used by the application or OIDC component to protect security-sensitive information stored in browser cookies.

13. In the LDAP Connection Details window, if you want to use LDAP to retrieve customer service representative (CSR) agent logins, enter the details in Table 3-7. Otherwise, select **Skip LDAP Configuration**. Then click **Next**.

> **Note**
>
> You must select **Skip LDAP Configuration** if you did not configure security using OpenID Connect. You cannot use LDAP services without OpenID Connect.

Table 3-7 LDAP Connection Details

Field	Description
Host Name	Enter the host name or IP address of the LDAP server. This field is mandatory if you did not select **Skip LDAP Configuration**. The host name is auto-populated from the Server Details window.
Port Number	Enter the number of the port on which the LDAP server is listening. This field is mandatory if you did not select **Skip LDAP Configuration**. The default value is **1389**.
Admin User Name	Enter the distinguished name (DN) of the LDAP user to use to connect to the LDAP server. This field is mandatory if you did not select **Skip LDAP Configuration**. The default value is **cn=Directory Manager**.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 3-7 (Cont.) LDAP Connection Details

Field	Description
Admin Password	Enter the password for the LDAP connection user. This field is mandatory if you did not select **Skip LDAP Configuration**. It has no default value.
User Base DN	Enter the base DN of the tree in the LDAP directory that contains users. This field is mandatory if you did not select **Skip LDAP Configuration**. The default value is **ou=people,dc=example,dc=com**.
User Name Filter	Enter the LDAP search filter used to locate a user based on the specified user name. This field is mandatory if you did not select **Skip LDAP Configuration**. The default value is **(&(uid={username}) (objectClass=person))**.
Group Base DN	Enter the base DN of the tree in the LDAP directory that contains groups. This field is mandatory if you did not select **Skip LDAP Configuration**. The default value is **ou=groups,dc=example,dc=com**.
Group Name Filter	Enter the LDAP search filter used to locate a group based on the specified group name. This field is mandatory if you did not select **Skip LDAP Configuration**. The default value is **(&(cn={group})(| (objectClass=groupOfNames) (objectClass=groupOfUniqueNames)))**.

14. If you selected **Skip LDAP Configuration** in the previous step, a confirmation message is displayed. Click **OK** to continue.
15. In the Installation Summary window, confirm your Billing Care installation summary and click **Install**.

    The Installation Progress window appears.
16. When installation completes, click **Next**.

    The Installation Complete window appears.
17. Make note of the Billing Care links, including the Oracle Home location, log file location, OpenID Connect redirect URL (if applicable), and the link for accessing Billing Care.
18. Click **Finish**.

    The Billing Care installer exits.
19. Review the settings described in "Configuring Billing Care" and complete any additional configuration required for your environment.
20. Start Billing Care by running the **start_billingcare.sh** script from the *Oracle_home*/**billingcare_rest/bin** directory. See "Starting and Stopping Billing Care".

See "Verifying the Billing Care Installation" for information about verifying the successful installation of Billing Care.

See "About Installation Logs" for information about the Billing Care installer logs.

Copyright © 2017, 2026, Oracle and/or its affiliates.

About Installation Logs

You use installation log files to help you debug your Billing Care installation. You can check the log files in the **oraInventory/logs** directory. The default location of the **oraInventory** directory is in the **/etc/oraInst.loc** file.

You use the following log files to monitor the installation and postinstallation process:

- **installAction***TimeStamp***.log**
- **oraInstall***TimeStamp***.err**
- **oraInstall***TimeStamp***.out**
- **launcher***TimeStamp***.log**

Copyright © 2017, 2026, Oracle and/or its affiliates.

4

Configuring Billing Care

Learn how to configure additional settings for Oracle Communications Billing Care.

The Billing Care installer creates the configuration files and configures the required settings based on the options you select during installation. After installation, you can modify these files to configure optional integrations and customize supported settings for your environment.

Topics in this document:

- About Billing Care Configuration Files
- Configuring Billing Care Application Settings
- Configuring BRM Connections
- Configuring SSL or TLS for Billing Care
- Configuring OIDC Authentication
- Configuring Role Mapping
- Configuring Billing Care Authorization
- Configuring the Oracle Analytics Publisher Connection

About Billing Care Configuration Files

Billing Care uses YAML configuration files to define server settings, application behavior, BRM connections, and security settings. During installation, the Billing Care installer creates these files and populates them with the values you specify. After installation, you can edit the files to configure additional supported settings for your environment.

The installer creates the Billing Care configuration files in the *Oracle_home*/**billingcare_rest/config** directory, where *Oracle_home* is the Oracle Home directory you specify during installation.

Table 4-1 describes the configuration files.

Table 4-1 Billing Care Configuration Files

File	Description
application.yaml	Defines server settings, including the host, application and administration ports, and SSL/TLS configuration. Includes LDAP connection settings when you configure LDAP.
brm-connection.yaml	Defines BRM connection settings under the **infranet** configuration root, including connection pool settings, timeouts, logging, and SSL wallet settings.
configurations.yaml	Defines Billing Care application settings, including batch payment directories, role mapping, and overrides for supported product settings.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 4-1 (Cont.) Billing Care Configuration Files

File	Description
authentication.yaml	Defines authentication settings, including the OpenID Connect (OIDC) identity provider, client information, and session cookie settings. You can reference sensitive values, such as the client secret, from the Billing Care application wallet.
authorization.yaml	Defines authorization settings for Billing Care endpoints under the **server.features.security** configuration root.
meta-config.yaml	Identifies the configuration sources that Billing Care loads, including external YAML files and packaged application defaults. When you enable security, these sources include the authentication and authorization configuration files.

Billing Care combines settings from multiple configuration sources in the following order, from highest to lowest priority:

1. Java system properties
2. Environment variables
3. External configuration files
4. Packaged application defaults

When a setting appears in multiple configuration sources, Billing Care uses the value from the source with the highest priority. You can override individual settings without copying the entire configuration. When you override an array, the new array replaces the inherited array. Include all entries that you want to retain.

To override a supported Billing Care application setting, add or update the corresponding key under **billingcare.configuration** in the **configurations.yaml** file. These changes do not require an SDK customization.

> **Note**
>
> Do not store passwords, client secrets, or other credentials under **billingcare.configuration**. Billing Care sends the settings under this configuration root to authenticated Billing Care UI clients. For configuration properties that support wallet references, store credentials in the Billing Care application wallet and reference them from the appropriate configuration file.

Configuring Billing Care Application Settings

You configure Billing Care application settings, such as account search size and session idle timeout, in the **configurations.yaml** file.

To configure Billing Care application settings:

1. Open the *Oracle_home*/**billingcare_rest/config/configurations.yaml** file.
2. Add or update the settings under **billingcare.configuration**. If the file already contains the **billingcare** and **configuration** sections, preserve the other settings in the file.

Copyright © 2017, 2026, Oracle and/or its affiliates.

For example, the following configuration sets the account search size to 100 and the session idle timeout to 15 minutes:

```
billingcare:
  configuration:
    fetch-sizes:
      accounts: 100
    timing:
      session-idle-timeout: PT15M
```

3. Include only supported settings that you want to override. Billing Care uses the packaged defaults for other settings unless a higher-priority configuration source overrides them. Billing Care rejects unrecognized application settings.

> **Note**
>
> Do not store passwords, client secrets, or other credentials under **billingcare.configuration**. Billing Care sends the settings under this configuration root to authenticated Billing Care UI clients.

4. Save the file.
5. Start or restart Billing Care. See "Starting and Stopping Billing Care".

   Billing Care validates the application settings during startup. If invalid settings prevent startup, correct the settings and start Billing Care again.
6. Sign in to Billing Care again or reload the browser page to use the updated settings.

   Verify that the application reflects your changes.

Configuring BRM Connections

Billing Care uses **brm-connection.yaml** to configure communication with BRM. The file contains **Infranet** settings for connection pooling, timeouts, logging, and SSL.

The installer configures the initial connection using the information you enter on the BRM Connection Details screen. If you specify an SSL Wallet Location, the installer enables SSL communication with BRM. If you leave this field blank, the installer configures the connection without SSL.

To update the BRM connection settings:

1. Open *Oracle_home*/**billingcare_rest/config/brm-connection.yaml**.
2. Update the applicable settings under **infranet**. Preserve the existing values for settings that you do not change.

   Table 4-2 lists the settings for connecting Billing Care to BRM.

Table 4-2 BRM Connection Parameters

Setting	Description
PcmTimeoutInMsecs	Specifies the PCM timeout in milliseconds.
connectionpool.minsize	Specifies the minimum connection pool size.
connectionpool.maxsize	Specifies the maximum connection pool size.
log.level	Specifies the PCM logging level.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 4-2 (Cont.) BRM Connection Parameters

Setting	Description
log.file	Specifies the path to the PCM log file.
pcp.ssl.enabled	Enables or disables SSL communication with BRM.
pcp.ssl.wallet.location	Specifies the directory that contains the BRM SSL wallet.
pcp.ssl.wallet.filename	Specifies the BRM SSL wallet filename, such as **cwallet.sso**.
wallet.location	Specifies the Billing Care application wallet directory. This setting applies to both SSL-enabled and SSL-disabled connections.

3. Configure SSL to match your BRM environment.
   - To enable SSL, set **pcp.ssl.enabled** to **true** and specify the directory and filename of a valid BRM SSL wallet in **pcp.ssl.wallet.location** and **pcp.ssl.wallet.filename**.
   - To disable SSL, set **pcp.ssl.enabled** to **false**. Keep **wallet.location** set to the Billing Care application wallet directory in either case.
4. Save the file.
5. Start or restart Billing Care. See "Starting and Stopping Billing Care".
6. Sign in to Billing Care and open an existing account to verify that Billing Care retrieves account information from BRM.

The following examples show the configuration for each SSL option. They use **/opt/oracle/billingcare** as the Oracle Home directory and **/opt/oracle/brm-ssl-wallet** as the BRM SSL wallet directory. Replace these paths with the paths for your installation. The numeric values illustrate a sample configuration; retain the values appropriate for your environment.

For a connection with SSL disabled:

```
infranet:
  PcmTimeoutInMsecs: 15000
  connectionpool:
    minsize: 25
    maxsize: 50
  login:
    type: 1
  log:
    level: 2
    file: /opt/oracle/billingcare/billingcare_rest/logs/javapcm-billingcare-rest.pinlog
  pcp:
    ssl:
      enabled: false
  wallet:
    location: /opt/oracle/billingcare/billingcare_rest/wallet
```

For a connection with SSL enabled:

```
infranet:
  PcmTimeoutInMsecs: 15000
  connectionpool:
    minsize: 25
    maxsize: 50
  login:
    type: 1
  log:
    level: 2
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

```
    file: /opt/oracle/billingcare/billingcare_rest/logs/javapcm-billingcare-rest.pinlog
  pcp:
    ssl:
      enabled: true
      wallet:
        location: /opt/oracle/brm-ssl-wallet
        filename: cwallet.sso
  wallet:
    location: /opt/oracle/billingcare/billingcare_rest/wallet
```

Configuring SSL or TLS for Billing Care

You configure SSL/TLS in the **application.yaml** file to secure connections to the Billing Care application and administration ports. Billing Care supports the following SSL/TLS authentication modes:

- **One-way SSL**: The client verifies the Billing Care server certificate.
- **Two-way SSL (mutual TLS)**: The client verifies the server certificate, and Billing Care requires and verifies a client certificate.

The Billing Care installer configures SSL/TLS using the values you enter on the **Server Details** and **Management and Observability** screens. You can update the connection settings after installation in the **application.yaml** file.

Before you configure SSL/TLS, complete the following prerequisites for each connection:

- Prepare a PKCS12 keystore that contains the server's private key and certificate chain. Ensure that the certificate matches the host name that clients use.
- Configure clients to trust the server's certificate authority.
- For two-way SSL, prepare a PKCS12 truststore containing trusted client certificate authorities. Configure clients with their certificates and private keys.
- Ensure that Billing Care can read each configured keystore and truststore file.

Store the keystore and truststore passwords in the Billing Care application wallet using the following aliases:

- **server-ssl-keystore-password**: Application keystore password
- **server-ssl-truststore-password**: Application truststore password
- **admin-ssl-keystore-password**: Administration keystore password
- **admin-ssl-truststore-password**: Administration truststore password

Configuring SSL/TLS Connections

To configure the SSL/TLS connections for Billing Care:

1. Open *Oracle_home*/**billingcare_rest/config/application.yaml**.
2. Configure the connection settings under **server**. Table 4-3 lists the entries to use based on the connection type. You can use a different SSL/TLS authentication mode for each connection.

   Use the following examples as guidelines for configuring the connection settings:

   - Configuring One-Way SSL Example
   - Configuring Two-Way SSL Example

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 4-3 SSL and TLS Configuration Locations

Connection	Port	SSL/TLS configuration
Application	**server.port**	**server.tls**
Administration	**server.sockets.admin.port**	**server.sockets.admin.tls**

3. If you enable HTTPS for an installation that uses OIDC authentication, update the registered redirect and logout URLs as required and set **cookie-secure** to **true** in the OIDC provider configuration. See "Configuring OIDC Authentication".
4. Save your configuration changes and restart Billing Care. See "Starting and Stopping Billing Care".
5. Verify that clients can connect to both configured HTTPS ports without certificate errors. For two-way SSL, verify that connections succeed with a trusted client certificate and fail without one.

Configuring One-Way SSL Example

The following example configures one-way SSL for both application and administration connections:

> **Note**
>
> Each **key.alias** setting must identify the private-key entry in the corresponding keystore.

```
server:
   host: billingcare.example.com
   port: 8082
   tls:
      enabled: true
      client-auth: NONE
      private-key:
         keystore:
            type: PKCS12
            passphrase: "${wallet=server-ssl-keystore-password}"
            key:
               alias: billingcare
            resource:
               path: "/opt/billingcare/certs/server.p12"
   sockets:
      admin:
         port: 8084
         tls:
            enabled: true
            client-auth: NONE
            private-key:
               keystore:
                  type: PKCS12
                  passphrase: "${wallet=admin-ssl-keystore-password}"
                  key:
                     alias: billingcare-admin
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

```
      resource:
         path: "/opt/billingcare/certs/admin.p12"
```

Configuring Two-Way SSL Example

When configuring two-way SSL, keep the keystore settings from the one-way SSL configuration. For each connection that requires two-way SSL, change **client-auth** to **REQUIRED** and add a **trust** section.

The following example shows the two-way SSL settings for both application and administration connections. Merge these settings into the existing configuration and retain the **enabled** and **private-key** settings.

```
server:
   tls:
      client-auth: REQUIRED
      trust:
         keystore:
            type: PKCS12
            trust-store: true
            passphrase: "${wallet=server-ssl-truststore-password}"
            resource:
               path: "/opt/billingcare/certs/server-truststore.p12"
   sockets:
      admin:
         tls:
            client-auth: REQUIRED
            trust:
               keystore:
                  type: PKCS12
                  trust-store: true
                  passphrase: "${wallet=admin-ssl-truststore-password}"
                  resource:
                     path: "/opt/billingcare/certs/admin-truststore.p12"
```

Configure browsers, API clients, and administration tools that connect to these ports to present trusted client certificates.

> **Note**
>
> Two-way SSL does not replace Billing Care authentication or authorization. Users must still sign in and have permission to perform the requested operations.

Configuring OIDC Authentication

Before you begin, obtain the identity-provider URL, client ID, and audience values for the Billing Care application.

Billing Care uses OpenID Connect (OIDC) to authenticate users through an identity provider. The installer configures OIDC when you select **Yes** on the **Security Details** screen and enter your OIDC provider information. You can review or update these settings after installation in the **authentication.yaml** file.

Copyright © 2017, 2026, Oracle and/or its affiliates.

To configure OIDC authentication:

1. Register the Billing Care redirect URL with your identity provider.

   Use the redirect URL that the Billing Care installer displays when installation completes. For an HTTPS deployment, the URL has the following format: **https://***hostname***:***port***/bc/oidc/redirect**.

   Use the host name and port through which users access Billing Care.

2. Open *Oracle_home***/billingcare_rest/config/authentication.yaml**.

3. Under **security.providers**, locate the **oidc** entry and update the settings listed in Table 4-4.

   Table 4-4 Identity Provider Settings

Setting	Description
identity-uri	Specifies the identity-provider URL.
client-id	Specifies the client ID of the confidential OAuth application you configure for Billing Care in the identity provider.
scope-audience	Specifies the primary audience for the confidential OAuth application.
audience	Specifies the secondary audience, if you configure one. Otherwise, use the same value as **scope-audience**.
client-secret	References the client secret in the Billing Care application wallet through **${wallet=oidc-client-secret}**.
cookie-encryption-password	References the cookie encryption password through **${wallet=oidc-cookie-encryption-password}**.
cookie-secure	Controls whether the browser sends the session cookie only over HTTPS. Set this value to **true** when Billing Care uses HTTPS.

   Ensure that the Billing Care application wallet contains the client secret that matches your identity-provider application and the cookie encryption password. Retain the wallet references in **authentication.yaml**.

   Preserve the installer-generated redirect and logout paths, including **/bc/oidc/redirect**, **/bc/logout**, and **/bc**.

4. Save and close the file.

5. Open *Oracle_home***/billingcare_rest/config/meta-config.yaml** and verify that its configuration sources include **authentication.yaml** and **authorization.yaml**.

   Preserve the other configuration sources and their order.

6. Start or restart Billing Care. See "Starting and Stopping Billing Care".

7. Access the Billing Care URL in a new browser session and verify that Billing Care redirects you to the identity provider.

8. Sign in with a valid user and verify that the browser returns to Billing Care.

Configuring Role Mapping

Billing Care uses a role mapper to retrieve the users available for Collections and Payment Suspense assignments. The role mapper retrieves users from a directory, an identity provider, or a list that you configure.

Copyright © 2017, 2026, Oracle and/or its affiliates.

You select the role mapper in the **configurations.yaml** file. Billing Care uses the roles allowed for the assignment operation in the **authorization.yaml** file to determine which groups to retrieve.

> **Note**
>
> Adding a user to an assignment list does not create a login account or grant access permissions. Configure authentication and authorization separately.

To configure role mapping:

1. Open *Oracle_home*/**billingcare_rest/config/configurations.yaml**.
2. Locate **billingcare.role-mapper** and set type to one of the following values:
   - **ldap**: Users in an LDAP directory.
   - **keycloak**: Members of Keycloak groups.
   - **idcs**: Members of Oracle Identity Cloud Service (IDCS) groups.
   - **static**: Users you list under **billingcare.role-mapper.static.fixed-members**.
   - **basic**: Users and roles configured in the global **http-basic-auth** provider in **authentication.yaml**.

   For example, to use LDAP, specify:

   ```
   billingcare:
     role-mapper:
       type: ldap
   ```

   Update the existing **billingcare** section and preserve its other settings.
3. Configure one of the following selected user sources:
   - Using LDAP
   - Using Keycloak or IDCS
   - Using a Static User List
   - Using Users Configured for Basic Authentication
4. Verify that the group names or configured role names match the assignment roles in **authorization.yaml**. See “Matching Users to Assignment Roles”.
5. Save and close the files.
6. Start or restart Billing Care. See "Starting and Stopping Billing Care".
7. Sign in as an authorized user and open the Collections and Payment Suspense assignment lists. Verify that the expected users appear.

Using LDAP

Use the LDAP role mapper to retrieve users from directory groups for Collections and Payment Suspense assignments. Select **ldap** as the role-mapper type in **configurations.yaml**, then configure the directory connection in **application.yaml**.

The installer creates the connection settings when you enter information on the **LDAP Connection Details** screen. You can update these settings after installation. Billing Care supports LDAP and SSL/TLS-enabled LDAP (LDAPS) connections.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Ensure that the configured bind user can read the groups and their member entries. Group members must have **uid** values that identify their login user names. The LDAP mapper retrieves only direct group members.

To configure the directory connection:

1. Open *Oracle_home*/**billingcare_rest/config/application.yaml**.
2. Locate the **ldap** section and update the settings in Table 4-5.

Table 4-5 LDAP Settings

Setting	Description
urls	Specifies the LDAP server address and port.
bind.dn	Specifies the distinguished name (DN) of the directory user that Billing Care uses to connect to the LDAP server.
bind.password	Specifies the credential for the directory connection. Retain the existing credential setting when you update other connection details.
users.base-dn	Specifies the base DN of the directory tree that contains users.
users.user-from-name-filter	Specifies the search filter that locates a user by user name.
groups.base-dn	Specifies the base DN of the directory tree that contains groups.
groups.group-from-name-filter	Specifies the search filter that locates a group by group name.

Configure the base DNs and filters to match your directory structure. Keep **{username}** and **{group}** as placeholders in the corresponding filters.

3. For an LDAPS connection, configure the directory server to accept LDAPS connections and set **ldap.urls** to the server's LDAPS address, such as ldaps://ldap.example.com:1636. Make a PKCS12 truststore containing the required trusted CA certificates available on the Billing Care host. Ensure that Billing Care can read the file.

   Under **ldap.tls**, configure the settings in Table 4-6.

Table 4-6 LDAPS Settings

Setting	Description
mode	Set to **LDAPS**.
trust-store.path	Specifies the path to the truststore file on the Billing Care host.
trust-store.type	Set to **PKCS12** for a PKCS12 truststore.
trust-store.password	Specifies the credential for accessing the truststore. Use the supported wallet reference for this credential.

After you configure the connection, complete the remaining steps in "Configuring Role Mapping" to save your changes, restart Billing Care, and verify the assignment lists.

The following examples show the **ldap** section in **application.yaml** for LDAP and LDAPS connections. Replace the server addresses, ports, bind DN, base DNs, and truststore path with

Copyright © 2017, 2026, Oracle and/or its affiliates.

the values for your environment. Adjust the filters to match your directory's attributes and object classes.

For an LDAP connection:

```
ldap: &ldapConfig
  urls:
    - "ldap.example.com:1389"
  bind:
    dn: "cn=Directory Manager"
    password: "<existing bind.password value>"
  users:
    base-dn: "ou=people,dc=example,dc=com"
    user-from-name-filter: "(&(uid={username})(objectClass=person))"
  groups:
    base-dn: "ou=groups,dc=example,dc=com"
    group-from-name-filter: "(&(cn={group})(|(objectClass=groupOfNames)
(objectClass=groupOfUniqueNames)))"
```

For an LDAPS connection:

```
ldap: &ldapConfig
  urls:
    - "ldaps://ldap.example.com:1636"
  tls:
    mode: LDAPS
    trust-store:
      path: "/opt/oracle/certificates/ldap-truststore.p12"
      type: "PKCS12"
      password: "<truststore password wallet reference>"
  bind:
    dn: "cn=Directory Manager"
    password: "<existing bind.password value>"
  users:
    base-dn: "ou=people,dc=example,dc=com"
    user-from-name-filter: "(&(uid={username})(objectClass=person))"
  groups:
    base-dn: "ou=groups,dc=example,dc=com"
    group-from-name-filter: "(&(cn={group})(|(objectClass=groupOfNames)
(objectClass=groupOfUniqueNames)))"
```

The examples reference **ldap-admin-password** for the directory bind password and **ldap-truststore-password** for the truststore password. The installer creates the bind-password entry when you configure LDAP. Create the truststore-password entry separately before using the LDAPS configuration. Preserve the other settings in **application.yaml**.

Using Keycloak or IDCS

The Keycloak and IDCS role mappers use the first global **oidc** provider in **authentication.yaml** to obtain a service token and retrieve group members.

Before selecting either mapper:

- Configure OIDC authentication. See "Configuring OIDC Authentication".
- Enable the client credentials grant for the configured client.
- Grant the client permission to read the required groups and their members.
- Verify that Billing Care trusts the certificates used by the token endpoint and directory APIs.

Successful browser sign-in does not verify that the client can retrieve assignment users.

Copyright © 2017, 2026, Oracle and/or its affiliates.

For Keycloak, set **identity-uri** to the realm URL, such as **https://keycloak.example.com/realms/billingcare**.

Create Keycloak groups with names that match the allowed assignment roles. Realm roles and token role claims alone do not provide the group membership that the mapper retrieves.

For IDCS, grant the client access to the required SCIM group and member operations. Ensure that each returned member's **name** contains the login user name. The mapper requests the administrative scope **urn:opc:idm:myscopes**.

These mappers use the global OIDC client settings. They do not provide separate role-mapper settings for a client ID, client secret, token endpoint, or TLS connection.

Using a Static User List

Use **static** to define assignment users directly in **configurations.yaml**.

Under **fixed-members**, add an entry for each allowed role group. For each user, specify:

- **id**: A stable, nonblank user identifier.
- **name**: The user's login user name. Specify the login name, not a display name.

For example:

```
billingcare:
  role-mapper:
    type: static
    static:
      fixed-members:
        super-csr:
          - id: "csr-alice"
            name: "alice"
          - id: "csr-charlie"
            name: "charlie"
        regular-csr:
          - id: "csr-bob"
            name: "bob"
          - id: "csr-charlie"
            name: "charlie"
```

Replace the example groups and users with values for your environment.

If an assignment operation allows both **super-csr** and **regular-csr**, this example returns **alice**, **bob**, and **charlie**. Billing Care removes duplicate login user names from the final assignment list.

Entries with a missing or blank **id** or **name** do not appear in the list. Groups without configured members return no users.

Using Users Configured for Basic Authentication

Use **basic** when the assignment users come from the global **http-basic-auth** provider in the **authentication.yaml** file.

In the **configurations.yaml** file, specify the following:

```
billingcare:
  role-mapper:
    type: basic
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

In the existing global **http-basic-auth** provider, configure each user's **login**, **password**, and **roles**. For example:

```
security:
  providers:
    - abac: {}
    - http-basic-auth:
        realm: BillingCare
        users:
          - login: "alice"
            password: "${wallet=basic-alice-password}"
            roles: [super-csr]
          - login: "bob"
            password: "${wallet=basic-bob-password}"
            roles: [regular-csr]
          - login: "charlie"
            password: "${wallet=basic-charlie-password}"
            roles: [super-csr, regular-csr]
```

Create the referenced wallet entries with the users' passwords. Use HTTPS for requests that use Basic authentication.

> **Note**
>
> This example configures a global authentication provider. Preserve the existing provider list, and change the sign-in configuration only if you intend to change how users authenticate. Selecting type: basic alone does not enable Basic authentication.

The mapper uses **login** as both the user identifier and login user name. It retrieves users from global Basic authentication providers; credentials configured only for an outbound service do not supply assignment users.

Restart Billing Care after changing these users or their roles.

Matching Users to Assignment Roles

Billing Care determines assignment groups based on the roles allowed in the matching endpoint policies defined in the **authorization.yaml** file. Table 4-7 lists the path aliases and HTTP methods for these operations.

Table 4-7 Path Aliases and Methods for Assignment Operations

Assignment Operation	Path Alias	Method
Collections	collections-perform	GET
Payment Suspense	payment-suspense-allocate	POST

Ensure that the allowed role names match the group names or roster keys in your selected user source. For example, an operation that allows **super-csr** requires a corresponding **super-csr** group or roster entry.

Update the existing endpoint policy. If multiple entries have the same path alias and method, Billing Care uses the first matching entry to retrieve assignment groups.

Copyright © 2017, 2026, Oracle and/or its affiliates.

> **Note**
>
> The assignment lookup uses **roles-allowed** to retrieve candidates. It does not evaluate **roles-denied** or other authorization conditions for each candidate. Billing Care still enforces endpoint authorization when a user performs an operation.

If an assignment list is empty, check the matching endpoint policy, its allowed roles, and the corresponding group memberships. For Keycloak and IDCS, also verify that the configured client can obtain a service token and read group members.

Configuring Billing Care Authorization

Billing Care uses authorization rules to control which operations users can perform. You configure these rules in **authorization.yaml** by specifying the roles that can access each REST endpoint. Billing Care also uses these rules to determine which actions users can access in the UI.

Before you configure authorization, configure authentication and ensure that the authenticated user's roles match the role names in your authorization rules. For OIDC authentication, see "Configuring OIDC Authentication".

To configure authorization:

1. Open *Oracle_home*/**billingcare_rest/config/authorization.yaml**.
2. Under **server.features.security.endpoints**, locate the entry for the operation you want to configure. Identify the entry by its **path**, **method**, and **path-alias**.

   Preserve the existing paths, methods, and aliases when you change access permissions. Billing Care uses path aliases for UI access checks and assignment-user lookups.
3. Update the authorization rules using the settings in Table 4-8.

Table 4-8 Endpoint Authorization Settings

Setting	Description
path	Specifies the REST endpoint path.
method	Specifies the HTTP methods covered by the entry, such as **[get]** or **[post]**.
path-alias	Identifies the operation for UI access checks and other authorization lookups.
config.authenticate	Specifies whether the endpoint requires authentication. Retain **true** for protected endpoints.
config.authorize	Specifies whether Billing Care checks authorization for the endpoint. Retain **true** for protected endpoints.
config.authorization-explicit	Specifies whether the endpoint requires explicit authorization configuration. Retain **true** for protected endpoints.
config.abac.rule-validator	Contains the authorization rules for the endpoint. Rules can include role checks and additional policy conditions.
name	Identifies a rule within **rule-validator**.
roles-allowed	Lists the roles that the rule allows.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) Endpoint Authorization Settings

Setting	Description
roles-denied	Lists the roles that the rule denies.

Preserve existing policy conditions, such as amount limits, when you update role permissions. For operations that modify data, preserve applicable restrictions on **read-only-csr**.

4. Save and close the file.
5. Start or restart Billing Care. See "Starting and Stopping Billing Care".
6. Sign in with users who have the affected roles. Verify that permitted operations are available and prohibited operations remain denied. Check REST access as well as UI access.

The following example defines role-based access to the account-details endpoint for **super-csr** and **regular-csr**:

```
server:
  features:
    security:
      endpoints:
        - path: /bcws/webresources/v1.0/accounts/{id}
          method: [get]
          path-alias: account-view
          config:
            authenticate: true
            authorize: true
            authorization-explicit: true
            abac:
              rule-validator:
                - name: super-csr
                  roles-allowed: [super-csr]
                - name: regular-csr
                  roles-allowed: [regular-csr]
```

Update the corresponding entry in your existing **authorization.yaml** file. Preserve the other endpoint entries and any additional conditions that apply to this operation.

> **Note**
>
> Configuration sources can replace an entire YAML list. Do not replace the **endpoints** list with this single-entry example.

Configuring the Oracle Analytics Publisher Connection

Billing Care retrieves invoice PDFs from Oracle Analytics Publisher. Configure the **Publisher** connection in the **application.yaml** file and select an authentication method that Publisher accepts.

Table 4-9 describes the supported authentication methods.

Copyright © 2017, 2026, Oracle and/or its affiliates.

Table 4-9 Supported Authentication Methods

Authentication Method	When to Use
Signed-in user's access token	Publisher accepts the Billing Care user's token and grants report access to that user.
OAuth service client	Publisher requires a service identity to retrieve reports.
Basic authentication	Publisher accepts an account name and password.

Before you configure the connection, obtain the Oracle Analytics Publisher reports service URL and verify that the required BRM invoice reports are available. Ensure that the user or service identity has permission to access these reports.

To configure the connection to Oracle Analytics Publisher, complete the following steps:

1. Open *Oracle_home*/**billingcare_rest/config/application.yaml**.
2. Locate or add the **api-processor.backends.invoice-publisher** configuration entry.
3. Set **base-uri** to the Oracle Analytics Publisher reports service URL. For example, use this reports service URL: https://publisher.example.com:8443/xmlpserver/services/rest/v1/reports.

   Replace the host and port with the values for your environment. Do not include a trailing slash or an individual report path. Billing Care adds the report path when it requests an invoice.
4. Configure one of the following authentication methods:
   - Using the Signed-In User's Access Token
   - Using an OAuth Service Client
   - Using Basic Authentication
5. Configure the certificate trust and wallet entries described in "Configuring Certificate Trust and Credentials".
6. Save and close the configuration files that you modified.
7. Start or restart Billing Care. See "Starting and Stopping Billing Care".
8. Sign in to Billing Care and retrieve an existing invoice.

   Verify that Billing Care displays a valid invoice PDF and that Oracle Analytics Publisher records the expected user or service identity.

Using the Signed-In User's Access Token

Use this method when Publisher accepts the access token of the user signed in to Billing Care. Publisher must accept the token's issuer, audience, and scopes and map the user to the required report permissions.

In the **application.yaml** file, configure the connection as follows:

```
api-processor:
   backends:
      invoice-publisher:
         base-uri: "https://publisher.example.com:8443/xmlpserver/services/
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

```
rest/v1/reports"
         security: {}
```

The empty **security** section enables the connection to use the current request's security context. Retain this section when you use the signed-in user's token.

In the **authentication.yaml** file, locate the existing **oidc** provider under **security.providers** that Billing Care uses for user authentication. Add **outbound-type**, **propagate**, and **outbound** to that provider, as shown below:

```
security:
  providers:
    - oidc:
        # Existing authentication settings remain here.
        outbound-type: USER_JWT
        propagate: true
        outbound:
          - name: publisher-user-token
            hosts: ["publisher.example.com"]
            transports: ["https"]
            propagate: true
          - name: other-targets
            propagate: false
```

This example shows only the settings for forwarding the token. Update the existing OIDC provider; do not create another provider or replace its authentication settings. Preserve other providers and any approved outbound destinations.

Replace **publisher.example.com** with the Publisher host name, without a scheme or port. Keep approved destinations before the final **other-targets** entry, which prevents token forwarding to unmatched hosts.

Billing Care forwards the access token associated with the request. It does not forward the browser cookie or obtain a replacement token for Publisher.

Using an OAuth Service Client

Use an OAuth service client when Oracle Analytics Publisher requires a service identity. Register an OAuth client with the identity provider. Obtain the client's ID and secret, the identity provider's token endpoint, and the scope required for Publisher access.

In the **application.yaml** file, configure the OAuth service client under **api-processor.backends.invoice-publisher.security** as shown in the following example:

```
api-processor:
   backends:
      invoice-publisher:
         base-uri: "https://publisher.example.com:8443/xmlpserver/services/rest/v1/reports"
         security:
            providers:
               - oidc:
                    client-id: "<publisher-service-client-id>"
                    client-secret: "${wallet=bip.oidc.client.secret}"
                    identity-uri: "https://<publisher-identity-provider>"
                    token-endpoint-uri: "https://<publisher-identity-provider>/oauth2/v1/
token"
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

```
token-endpoint-auth: CLIENT_SECRET_BASIC
outbound-type: CLIENT_CREDENTIALS
propagate: true
outbound:
   - name: publisher-service-token
     hosts: ["publisher.example.com"]
     transports: ["https"]
     propagate: true
   - name: other-targets
     propagate: false
client-credentials:
   scope: "<publisher-scope>"
redirect: false
cookie-use: false
cookie-encryption-enabled: false
```

Replace the example values with the values for your environment and registered service client. The **/oauth2/v1/token** path is an IDCS example. Use the token endpoint published by your identity provider. Table 4-10 describes the OAuth service client settings for authenticating the service client, obtaining an access token, and forwarding the token to Oracle Analytics Publisher.

Table 4-10 OAuth Service Client Settings

Setting	Description
client-id	Identifies the registered Publisher service client.
client-secret	References the wallet entry that contains the client secret.
identity-uri	Specifies the identity provider's base or issuer URI.
token-endpoint-uri	Specifies the published token endpoint.
token-endpoint-auth	Specifies how the client authenticates to the token endpoint. The example uses **CLIENT_SECRET_BASIC**.
outbound-type	Specifies **CLIENT_CREDENTIALS** as the outbound authentication type used to obtain a service token.
client-credentials.scope	Specifies the exact scope registered for Publisher access.
outbound	Restricts token forwarding to the configured Publisher host.

Oracle Analytics Publisher receives the resulting bearer token. The **CLIENT_SECRET_BASIC** value specifies how the service client authenticates to the token endpoint.

The service client can use the same identity provider as Billing Care or a different provider. Keep the OAuth service client configuration inside the **invoice-publisher** backend and preserve the global Billing Care sign-in provider in **authentication.yaml**.

Using Basic Authentication

Use this method when Publisher accepts an account name and password.

In the **application.yaml** file, use the following:

```
api-processor:
   backends:
      invoice-publisher:
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

```
         base-uri: "https://publisher.example.com:8443/xmlpserver/services/
rest/v1/reports"
         security:
            providers:
               - http-basic-auth:
                    outbound:
                       - name: publisher-basic
                         hosts: ["publisher.example.com"]
                         transports: ["https"]
                    username: "<publisher-account>"
                    password: "${wallet=invoice.publisher.password}"
```

Replace the host name and account name with your values. Store the account password in the **invoice.publisher.password** wallet entry.

Grant the account permission to access the required invoice reports. This provider authenticates the Publisher connection; Billing Care sign-in continues to use its existing authentication configuration.

Configuring Certificate Trust and Credentials

Configure certificate trust for each HTTPS connection. Billing Care may require separate trust settings for Oracle Analytics Publisher and the identity provider that issues access tokens. Table 4-11 lists the truststore configuration locations for each connection type.

Table 4-11 Certificate Trust Configuration Locations

Connection	Configuration Location
Publisher reports service	**api-processor.backends.invoice-publisher.tls** in **application.yaml**
Identity provider for the signed-in user's token	**webclient.tls** under the global **oidc** provider in **authentication.yaml**
Identity provider for the service client	**webclient.tls** under the **oidc** provider in the **invoice-publisher** backend

If the existing Java trust configuration validates a server certificate, you can omit custom trust settings for that connection.

In the **application.yaml** file, add **tls** alongside **base-uri** and **security** under **api-processor.backends.invoice-publisher** to configure a custom Publisher truststore:

```
tls:
   trust:
      keystore:
         type: PKCS12
         trust-store: true
         passphrase: "${wallet=publisher-truststore-password}"
         resource:
            path: "/opt/billingcare/certs/publisher-truststore.p12"
```


Copyright © 2017, 2026, Oracle and/or its affiliates.

To configure a custom truststore for the service client's identity provider, add the following **webclient** settings under the service client's **oidc** entry:

```
webclient:
   tls:
      trust:
         keystore:
            type: PKCS12
            trust-store: true
            passphrase: "${wallet=publisher-oidc-truststore-password}"
            resource:
               path: "/opt/billingcare/certs/publisher-oidc.p12"
```

Replace the example paths with paths to truststore files that Billing Care can read on its host. Populate the truststores with approved CA certificates. Use server URLs whose host names match the names in the corresponding server certificates. Keep hostname verification enabled.

For the global OIDC provider, preserve its existing trust configuration. If you add a custom truststore for that provider, specify its path and the corresponding wallet reference.

Table 4-12 lists the Billing Care wallet aliases used in the configuration examples for the Publisher account password, OAuth service client secret, and truststore passwords.

Table 4-12 Wallet Entries Used in the Examples

Wallet alias	Value
invoice.publisher.password	Publisher account password for Basic authentication.
bip.oidc.client.secret	OAuth service client secret.
publisher-truststore-password	Password for the Publisher truststore.
publisher-oidc-truststore-password	Password for the service client's identity-provider truststore.

Create only the entries required for your selected configuration. The Billing Care installer does not create these wallet entries automatically.

Set **BILLINGCARE_REST_HOME** to *Oracle_home*/**billingcare_rest** and use the Java runtime configured by **bin/setenv.sh**. For example, run the following command to add the service client secret:

```
java -cp "$BILLINGCARE_REST_HOME/libs/*" \
   oracle.security.pki.OracleSecretStoreTextUI \
   -wrl "$BILLINGCARE_REST_HOME/wallet" \
   -createEntry bip.oidc.client.secret
```

The command prompts you to enter the service client secret and any required wallet password. Use **-modifyEntry** to update an existing wallet entry. Preserve the existing wallet and its auto-login configuration.

Copyright © 2017, 2026, Oracle and/or its affiliates.

5

Verifying the Billing Care Installation

Learn how to verify the Oracle Communications Billing Care installation by starting the application and signing in.

Topics in this document:

- Starting and Stopping Billing Care
- Logging In to Billing Care

Starting and Stopping Billing Care

To start Billing Care:

1. Change to the Billing Care scripts directory.

   cd *BC_home*/**billingcare_rest/bin**

   where *BC_home* is the directory into which you installed Billing Care.

2. Run the following command to start Billing Care:

   sh start_billingcare.sh

   The system will respond with the following messages:

   ```
   Command Executed Successfully
   See log file: BC_home/billingcare_rest/logs/billingcare-rest.log
   ```

To stop Billing Care:

1. Change to the Billing Care scripts directory.

   cd *BC_home*/**billingcare_rest/bin**

   where *BC_home* is the directory into which you installed Billing Care.

2. Run the following command to stop Billing Care:

   sh stop_billingcare.sh

   The system will respond with the following message:

   ```
   Stopping BillingCare REST: Successful
   ```

Logging In to Billing Care

To log in to Billing Care:

1. In a supported browser, access the URL provided by the Billing Care installer at the end of the installation. For the list of supported browser versions, see *BRM Compatibility Matrix*. The URL will look something like this:

   `https://hostname:port/bc`

   where *hostname* and *port* refer to the values you configured when installing Billing Care.

Copyright © 2017, 2026, Oracle and/or its affiliates.

The Billing Care login window appears.

2. Do the following:
   a. In the **User Name** field, enter the user name of a valid user that exists in your Oracle Unified Directory server.
   b. In the **Password** field, enter the password.

   The Billing Care home page appears, verifying that Billing Care is installed successfully.

Copyright © 2017, 2026, Oracle and/or its affiliates.