Oracle® Communications Billing and Revenue Management

Billing Care Installation Guide

Release 15.0
F86197-02
June 2024

Oracle Communications Billing and Revenue Management Billing Care Installation Guide, Release 15.0

F86197-02

Contents

Preface

This guide provides instructions for installing Oracle Communications Billing Care.

This guide has been updated to include changes and new feature content added for release 15.0.1.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Billing Care Installation Overview

Learn about the Oracle Communications Billing Care installer.

Topics in this document:

About Installing Billing Care

Billing Care installation should be performed only by experienced system administrators. You must be familiar with the following before you begin the installation:

- Linux operating system
- Oracle WebLogic Server
- Oracle Enterprise Database
- (Optional) Oracle Identity Management (IDM) components, including:
  - Oracle Access Management (OAM)
  - Oracle Identity Governance
  - Oracle Unified Directory (OUD)

Additionally, you should have experience installing Java-related packages.

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

- Deploys Billing Care to a WebLogic server domain and installs the Billing Care SDK.
- Installs the Billing Care REST API.

Overview of the Billing Care Installation Steps

The following is an overview of the Billing Care installation steps:

1. Plan your installation. Planning your installation involves:
   - Determining the scale of your implementation (for example, whether you are installing a small test system or a large production system).

> **Note:**
>
> You can install a test or development installation for using Billing Care without Oracle Platform Security Services (OPSS) security. Do not use these installations in production environments. See "About Test Installations and Production Installations" for more information.

- Assessing how many physical computers you need and which software components to install on which computers.
- Planning the system topology.

2. Review system requirements. System requirements include:
   - Hardware requirements, such as disk space and physical RAM.
   - Software requirements, such as operating system (OS) versions and OS patch requirements, OS kernel tuning requirements, required Oracle software, including:
     - Enterprise Database
     - WebLogic Server
     - (Optional) IDM components, such as:
       * Oracle Access Management (OAM)
       * Oracle Identity Governance
       * Oracle Unified Directory (OUD)
     - Java Development Kit (JDK)

     See "Billing Care System Requirements" for required versions.
   - Information requirements, such as IP addresses, administrative user credentials, host names, and port numbers.
3. Prepare your foundation by completing the preinstallation tasks.

   See "Billing Care Preinstallation Tasks" for more information.
4. Use the Oracle Universal Installer (OUI) to either install Billing Care and the Billing Care SDK or install the Billing Care REST API.

   See "Installing Billing Care" for more information.
5. Perform the required postinstallation configuration tasks.

   See "Billing Care Postinstallation Tasks" for more information.
6. Verify the installation.

   See "Verifying the Billing Care Installation" for more information.

Ensuring a Successful Billing Care Installation

Billing Care uses additional Oracle software products including Enterprise Database, WebLogic Server, and IDM (optional). Familiarize yourself with these products and their installation procedures before installing Billing Care.

> **Note:**
>
> IDM has important preinstallation requirements including kernel tuning, operating system configuration files editing (for example, editing **limits.conf**), and tuning database parameters. If you are using IDM components, ensure that these requirements have been met when completing the preinstallation tasks before running the Billing Care installer so that your installation is successful. See *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* for detailed information.

Consult additional product documentation on the Oracle Help Center for required information at: https://docs.oracle.com.

To ensure that the Billing Care installation is successful, follow these guidelines:

- As you install each component (for example, the Enterprise Database and WebLogic Server), verify that the component installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing the application, ensure that your system has the required base software and meets the minimum technical requirements. In addition, ensure that you know all the required configuration values, such as host names and port numbers.
- Make a note of any new configuration values as you create them. You will be required to enter configuration values later in the procedure.

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

When planning a Billing Care installation, consider how many physical servers are required to support the Oracle Enterprise Database, Oracle WebLogic Server domains, and Oracle Identity Management (IDM) components (optional) needed in your environment.

Consider the security and networking requirements necessary for securing Billing Care communications with your Oracle Communications Billing and Revenue Management (BRM) system in addition to software and hardware requirements.

See "Billing Care System Requirements" for information about required hardware and software.

About Test Installations and Production Installations

Install Billing Care either as a test or production installation depending on your required environment.

About Test Installations

Use test installations when setting up internal development or testing Billing Care instances. Test installation gives you the option to use Billing Care without Oracle Platform Security Services (OPSS) security. The deployed Billing Care application in your test WebLogic Server domain connects directly to your BRM system using native WebLogic Server user management.

Test installations include the following components:

- WebLogic Server
- WebLogic Server domain to host Billing Care with Billing Care security disabled
- Deployed Billing Care application WAR

This guide includes information on installing test installations. It is not mandatory to perform the IDM preinstallation steps for test installations.

About Production Installations

Use production installations when setting up secure Billing Care instances using security. Production installations require user authentication and authorization for securing access to Billing Care. This guide provides general guidelines for installing and configuring IDM components. It does not contain detailed information on configuring IDM components. Consult the respective product documentation using the references provided in this guide for more information on configuring IDM components.

Production installations include the following components:

- Enterprise Database
- Database creation with Oracle Repository Creation Utility (RCU)
- WebLogic Server
- OPSS JRF-enabled WebLogic domain
- (Optional) IDM components, including:
  - Oracle Access Management (OAM) for single sign-on (SSO) configuration
  - Oracle Identity Governance for user management
  - Oracle Unified Directory (OUD) for user directory management

Database Planning

Billing Care production installations require an Enterprise Database for storing OPSS schema. This database is in addition to your BRM server database. Database sizing requirements depend on the number of Billing Care users in your environment.

See "Installing and Configuring Oracle Enterprise Database" for information on setting up the required database for Billing Care.

Authentication and Authorization Planning

When planning a Billing Care installation, consider the requirements carefully. Each OPSS JRF-enabled domain hosts a deployed instance of Billing Care and connects to OPSS for authorization. Determine how many OPSS JRF-enabled domains are needed to support the Billing Care deployments required by your transaction volume.

For authentication, you can use Security Assertion Markup Language (SAML) for SSO or the IDM components and Oracle HTTP Server Webgate for user authentication, SSO, and user directory management.

If you are using SAML, see the SAML documentation for information on sizing and installation.

If you are using IDM components, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for more information on sizing and installation.

About Installing a Secure System

In production environments, you must ensure that communication between components and access to the system servers are secure. The Billing Care installer prompts you to select security options. After you install Billing Care, enable SSL communication between Billing Care

and BRM. For information about securing Billing Care, see "Billing Care Security" in *BRM Security Guide*.

3

Billing Care System Requirements

Learn how to ensure that your system meets the minimum software and hardware requirements before you install Oracle Communications Billing Care.

Topics in this document:

Software Requirements

Billing Care is deployed on the Oracle Platform Security Services (OPSS) JRF-enabled WebLogic Server domain. See the Oracle Platform Security Services documentation for more information.

You need the following software for installing Billing Care:

- Oracle Enterprise Database for storing authentication and authorization policies and user information.
- Oracle WebLogic Server installed using the Oracle Fusion Middleware Infrastructure installer.
- OPSS JRF-enabled WebLogic Server domain for deploying Billing Care.

> **Note:**
>
> You configure OPSS when you create the JRF-enabled WebLogic domain. No additional steps are required for configuring OPSS.

Optionally, you can install Oracle Identity Management (IDM) components for authentication and authorization based on your requirements:

- Oracle Access Management (OAM) for single sign-on (SSO) configuration.
- Oracle Unified Directory (OUD) for user directory management.
- Oracle Identity Governance for connecting to OUD and managing users.

For information on supported operating systems, additional software requirements, and compatible software versions, see "Billing Care Software Compatibility" in *BRM Compatibility Matrix*.

Hardware Requirements

The number and configuration of the hosts used for your Billing Care installation depend on your requirements. For example, large transaction volumes, multiple geographical locations, or fail-over requirements affect the amount of required hardware.

Table 3-1 lists the recommended hardware requirement for a single server production Billing Care installation containing all components. See *Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management* for more information on IDM component hardware and sizing.

Table 3-1 Billing Care Single Server Minimum Hardware Requirements

Component	Requirement
Hard disk	200 GB of free disk space **Note:** A minimum of 1.5 GB should be free in the domain home.
Processor	Oracle recommends using 6 or more cores, each running at 1.5 GHz or greater.
Memory	A minimum of 35 GB physical memory and 16 GB swap. If you plan on installing the required database on the same server, see *Checking the Hardware Requirements* for more information about required memory. For more information on calculating required memory in your environment, see *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management*.

See *Product-Specific Memory and Disk Space Requirements* in *Oracle Fusion Middleware System Requirements and Specifications* for more information on the requirements.

Also, see the information about hardware and software requirements for the database in the "Install and Upgrade" section of the Oracle Database documentation for the appropriate version of the database software.

About IPv4 and IPv6 Support for Fusion Middleware Products

For information on network considerations, including support for IPv6 addresses, see Oracle Fusion Middleware System Requirements and Specifications.

4

Billing Care Preinstallation Tasks

Learn about prerequisite tasks, such as installing your Oracle database, that you perform before installing the Oracle Communications Billing Care software.

Topics in this document:

Overview of Production Preinstallation Tasks

In production installations, the Billing Care installer deploys Billing Care on a running Oracle Platform Security Services (OPSS) JRF-enabled domain. The installer assumes that the following required software preinstallation tasks, including applying patches and workarounds, have already been completed successfully.

> **Note:**
>
> A test installation without OPSS security can be performed on a basic WebLogic domain. Do not use a test installation in production.

Preinstallation tasks for Billing Care consist of the following steps:

1. Installing and Configuring Oracle Enterprise Database
2. Installing and Configuring Oracle WebLogic Server
3. (Optional) Installing and Configuring Oracle Unified Directory
4. (Optional) Installing and Configuring Oracle Access Management
5. (Optional) Installing and Configuring Oracle Identity Governance

Installing and Configuring Oracle Enterprise Database

Billing Care requires Oracle Enterprise Database for storing authentication and authorization policies and user information. If you are using Oracle Identity Management (IDM) for user authentication and authorization, you must install the database before you install and deploy IDM components.

Oracle recommends that an experienced database administrator install and configure your database. To install and configure Oracle Database, see the Oracle Database installation documentation at: https://docs.oracle.com/en/database/.

Installing and Configuring Oracle WebLogic Server

Billing Care requires a JRF-enabled WebLogic Server domain for deploying Billing Care. You must download and install Oracle WebLogic Server using the Fusion Middleware Infrastructure installer.

If you are using IDM for user authentication and authorization, download and install WebLogic Server before installing IDM.

See Installing and Configuring Oracle WebLogic Server and Coherence for information about installing WebLogic Server.

In a production environment, Oracle recommends using the SSL protocol for sending and receiving messages

For more information about configuring SSL in WebLogic Server, see "Configuring SSL" in *Administering Security for Oracle WebLogic Server*.

Billing Care supports TLS versions 1.2 and 1.3. For information about setting the protocol version, see "Specifying the SSL/TLS Protocol Version" in *Administering Security for Oracle WebLogic Server*.

Configuring the OPSS JRF-Enabled Billing Care Application Domain

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

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

Installing and Configuring Oracle Unified Directory

Download and install the Oracle Unified Directory software. For more information, see "Installing the Oracle Unified Directory Software" in *Oracle Fusion Middleware Installing Oracle Unified Directory*.

Configuring Oracle Unified Directory as Authentication Provider

After installing OUD, configure the OPSS Administration Server to use OUD as the authentication provider.

See "Configuring Authentication Providers" in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server* for information on setting up OUD as your authentication provider.

See "Introduction to Oracle Unified Directory" in *Oracle Fusion Middleware Administering Oracle Unified Directory* for information on setting up OUD, including how to synchronize OUD with existing directories that you may already have.

Installing and Configuring Oracle Access Management

Download and install the Oracle Access Management (OAM) software. For more information, see the information about installing and configuring Oracle Access Management at:

https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/index.html

Configuring the Oracle Access Manager Billing Care Application Domain

Create a Billing Care application domain in Oracle Access Manager (OAM) and configure an application domain policy that controls access to the Billing Care application.

To create your Billing Care application domain in OAM, complete the following steps:

1. Creating the Billing Care Application Domain
2. Defining Billing Care Resources
3. Configuring Billing Care Authentication Modules
4. Creating a Billing Care Authentication Scheme
5. Creating the Billing Care Authentication Policy and Adding Resources
6. Creating the Billing Care Authorization Policy and Adding Resources
7. Configuring and Restarting the Oracle HTTP Server

For more information about application domains and policies, see *Oracle Fusion Middleware Administering Oracle Access Management*.

Creating the Billing Care Application Domain

To create the Billing Care application domain:

1. Log in to your OAM web console at **http://***hostname***:***port***/oamconsole**, where *hostname* and *port* are the server name or IP address and port for your OAM instance.
2. Click **Application Domains** in the **Access Manager** frame.
3. Click **Create Application Domain**.
4. In the **Name** field, enter a name for your application domain.
5. (Optional) Provide **Description**, **Session Idle Timeout (minutes)**, **Allow OAuth Token**, and **Allow Session Impersonation** values.
6. Click **Apply**.

   The Billing Care application domain is created.

See "Creating a New Application Domain" in *Oracle Fusion Middleware Administering Oracle Access Management* for more information.

Defining Billing Care Resources

Define the **/bc****, **/bc***, and **/**** resources for your Billing Care application domain. Repeat steps 1 through 4 for each of these resources.

To define Billing Care resources in your Billing Care application domain:

1. Click **Application Domains** in the **Access Manager** frame.

2. Click the link for your Billing Care application domain.

   The **Summary** tab for your Billing Care application domain is shown.

3. Click the **Resources** tab.

4. Enter or select the following values listed in Table 4-1.

Table 4-1 Billing Care Protected Resource Creation Values

Field	Value
Type	**HTTP**
Description	(Optional) Enter text description
Host Identifier	**IAMSuiteAgent**
Protection Level	**Protected**
Authentication Policy	**Protected Policy**
Resource URL (String)	**/bc***, **/bc***, or **/***

Define an excluded resource for **/fav.ico**.

To define the excluded resource, repeat steps 1 through 4 using the values listed in Table 4-2.

Table 4-2 Billing Care Excluded Resource Creation Values

Field	Value
Type	**HTTP**
Description	(Optional) Enter text description
Host Identifier	**IAMSuiteAgent**
Protection Level	**Excluded**
Resource URL (String)	**/favicon.ico**

See "Adding and Managing Policy Resource Definitions" in *Oracle Fusion Middleware Administering Oracle Access Management* for more information on creating resources in OAM console.

Configuring Billing Care Authentication Modules

Create an **OIMIDStore** authentication model in OAM for authenticating Billing Care users.

To create the required authentication model in OAM:

1. Click **Authentication Modules** in the **Access Manager** frame.

   The **Authentication Modules** node is shown.

2. Click the **Create Authentication Module** menu and select **Create LDAP Authentication Module**.

3. In the **Name** field, provide a name for your authentication module.

4. In **User Identity Store**, select **OIMIDStore**.

5. Click **Apply**.

See "Managing Native Authentication Modules" in *Oracle Fusion Middleware Administering Oracle Access Management* for more information on creating an authentication module in OAM console.

Creating a Billing Care Authentication Scheme

The authentication module you previously created must be added to an authentication scheme in your Billing Care application domain.

To create an authentication scheme and add the authentication module to it:

1. Click **Authentication Schemes** in the **Access Manager** frame.

   The **Authentication Schemes** node is shown.
2. Click **Create Authentication Scheme**.
3. Enter or select the following values listed in Table 4-3.

Table 4-3 Billing Care Authentication Scheme Creation Values

Field	Value
Name	Billing Care LDAP Scheme name
Description	(Optional) Enter text description
Authentication Level	**2**
Challenge Method	**FORM**
Challenge Redirect URL	**/oam/server**
Authentication Module	Select the authentication module created in the previous step
Challenge URL	**/pages/login.jsp**
Context Type	**default**
Context Value	**/oam**

4. Click **Apply**.

See "Creating an Authentication Scheme" in *Oracle Fusion Middleware Administering Oracle Access Management* for more information.

Creating the Billing Care Authentication Policy and Adding Resources

Create an authentication policy that the Billing Care application domain uses to manage the resources, authentication module, and authentication scheme previously created.

To create an authentication policy:

1. Click **Application Domains** in the **Access Manager** frame.

   The **Application Domain** tab is shown.
2. In the **Search** field, enter the name of your Billing Care application domain and press enter.
3. In **Search Results**, click the name of your Billing Care application domain.
4. Click the **Authentication Policies** tab.

   The **Authentication Policy** node is shown.

5. Click **Create Authentication Policy**.
6. Enter or select the following values listed in Table 4-4.

Table 4-4 Billing Care Authentication Policy Creation Values

Field	Value
Name	Billing Care authentication policy name
Description	(Optional) Enter text description
Authentication Scheme	Select the authentication scheme created in the previous step

7. Click **Apply**.

To add your Billing Care resources to your authentication policy:

1. In the **Authentication Policy** node for your previously created policy, click the **Resources** tab.
2. Click **Add**.
3. Select all of the Billing Care resources created in "Defining Billing Care Resources".
4. Click **Apply**.

See "Defining Authentication Policies for Specific Resources" in *Oracle Fusion Middleware Administering Oracle Access Management* for more information on creating an authentication policy and adding resources in OAM console.

Creating the Billing Care Authorization Policy and Adding Resources

Create an authorization policy and add resources to this policy for the Billing Care application domain.

To create the Billing Care application domain authorization policy:

1. Click **Application Domains** in the **Access Manager** frame.

   The **Application Domain** tab is shown.
2. In the **Search** field, enter the name of your Billing Care application domain and press enter.
3. In **Search Results**, click the name of your Billing Care application domain.
4. Click the **Authorization Policies** tab.
5. Enter or select the following values listed in Table 4-5.

Table 4-5 Billing Care Authorization Policy Creation Values

Field	Value
Name	Billing Care authorization policy name
Description	(Optional) Enter text description
Success URL	The redirect URL to be used upon successful authorization
Failure URL	The redirect URL to be used upon failed authorization

6. Click **Apply**.

7. Click the **Resources** tab.
8. Click **Add**.
9. Select all of the Billing Care resources created in "Defining Billing Care Resources".
10. Click **Apply**.

See "Creating an Authorization Policy and Specific Resources" in *Oracle Fusion Middleware Administering Oracle Access Management* for more information on creating an authorization policy and adding resources in OAM console.

Configuring and Restarting the Oracle HTTP Server

After configuring the required Billing Care OAM components, edit the Oracle HTTP Server (OHS) **idm.conf** file in your OAM instance to specify the handler, host, and port for the **/bc** resource. Restart your OHS instance after editing this file.

To configure the **/bc** resource in the OHS **idm.conf** file:

1. Open a secure shell or terminal window to your OAM host as a user with administrative permissions.
2. Change to the *Middleware_home***/config/OHS/***OHS_Instance***/moduleconf** directory, where *Middleware_home* is the middleware home directory of the OAM WebLogic Server instance and *OHS_Instance* is the OHS instance where OAM is hosted.
3. Append the following entry into the **idm.conf** file before the **</VirtualHost>** closing tag:

```
<Location /bc>
     SetHandler weblogic-handler
     WebLogicHost host name or IP address of your OPSS Administration Server
     WeblogicPort port number the WebLogic host is listening on
</Location>
```

4. Save the file.
5. Change to the *OHS_home***/bin** directory, where *OHS_home* is the Oracle home directory of your OHS installation.
6. Restart OHS with the following commands:

   ./opmnctl status

   ./opmnctl stopall

   ./opmnctl startall

See "Using the idm.conf File" in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite* for more information on the OHS **idm.conf** file.

Installing and Configuring Oracle Identity Governance

Download and install the Oracle Identity Governance software. For more information, see the information about installing and configuring Oracle Identity Governance at:

https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/index.html.

5

Installing Billing Care

Learn how to install Oracle Communications Billing Care for a test or production system.

Topics in this document:

Downloading the Billing Care Installer

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

- For Billing Care 15.0.0 or any 15.0.*x* maintenance release: From the Oracle software delivery website (https://edelivery.oracle.com)
- For any 15.0.*x*.*y* patch set release: From the Oracle support website (https://support.oracle.com)

Search for and download the **Oracle Communications Billing Care 15.0.*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**

Installing Billing Care for Testing

Billing Care test installations do not use Oracle Identity Management (IDM) security. The installer deploys the application to a basic Oracle WebLogic domain with Billing Care authorization disabled. Use test installations for internal development and testing only.

To install Billing Care for testing:

1. Disable Billing Care authorization in the WebLogic domain. See "Configuring WebLogic Server for a Test Installation" for more information.
2. Run the Billing Care installer without specifying IDM host details and confirming that authorization is not being used. See "Running the Billing Care Installer for Testing" for more information.

Configuring WebLogic Server for a Test Installation

You can use a WebLogic domain that is not configured as an OPSS JRF-enabled domain when installing test installations of Billing Care. Test installations are not supported in production environments. For a secure Billing Care installation, use an OPSS JRF-enabled domain.

See "Billing Care Security" in *BRM Security Guide* for more information about securing your installation.

To configure a WebLogic domain for a test Billing Care installation:

1. On the WebLogic Server, add the following property to the **JAVA_OPTIONS** parameter in the **setDomainEnv.sh** configuration script located in *Middleware_home***/user_projects/domains/***billingcaredomain***/bin** directory, where *Middleware_home* is the directory where WebLogic Server is installed and *billingcaredomain* is the directory containing the test installation domain you want to install Billing Care:

   ```
   -DdisableBillingCareAuthorization=true
   ```

   For example:

   ```
   JAVA_OPTIONS="${JAVA_OPTIONS} ${JAVA_PROPERTIES} -Dwlw.iterativeDev=$
   {iterativeDevFlag} -Dwlw.testConsole=${testConsoleFlag} -
   Dwlw.logErrorsToConsole=${logErrorsToConsoleFlag} -
   DdisableBillingCareAuthorization=true"
   ```

2. Restart the WebLogic Server domain.
3. Run the Billing Care installer.

Running the Billing Care Installer for Testing

To install a Billing Care test installation in a basic domain:

1. Verify that your Java Development Kit is installed correctly. Ensure that you set your **JAVA_HOME** environment variable and that the *Java_home***/bin** directory is in your path.
2. Start the Oracle WebLogic Server basic domain administration server or the managed server on which you want to deploy Billing Care.
3. Download the Billing Care installer. See "Downloading the Billing Care Installer" for more information.
4. Run the following command, which launches the Billing Care installer:

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

   > **Note:**
   >
   > Specify the **-invPtrLoc** flag and an Oracle Inventory path location in the java command for launching the Billing Care installer if you are using an existing or custom Oracle inventory location for maintaining your installed Oracle products and installation logs.

5. In the Welcome window, click **Next**.
6. In the Installation Location window, enter or browse to your Oracle Home directory and then click **Next**.
7. In the Installation Type window, select the **Billing Care Application** and **Billing Care REST API** components, and then click **Next**.
8. In the Feature Sets Selection window, select to install one or both of the following components. Click **Next**.
   - Billing Care Application
   - Billing Care SDK

9. In the WebLogic Server Details window, enter the details listed in Table 5-1 for the WebLogic Server domain in which you want to deploy Billing Care, and then click **Next**.

Table 5-1 WebLogic Server Details

Field	Description
Host Name	IP address or the host name of the computer on which the WebLogic Server domain is configured.
Port Number	Port number assigned to the WebLogic Server domain administration server.
User Name	WebLogic Server domain administrator user name.
Password	Password for the WebLogic Server domain administrator user.
WebLogic Home	Path of the directory in which the WebLogic Server software is installed.
Use SSL?	Whether to use SSL. Deselect the checkbox for test installations.
KeyStore Type	The type of KeyStore file used in the WebLogic domain for SSL: **JKS** or **PKCS12**.
KeyStore Location	The path to your KeyStore file, which is used for authentication through SSL.
KeyStore Password	The password required to access the certificates from the KeyStore.

> **Note:**
>
> The Billing Care installer will not proceed until it verifies that the information you entered is valid. The domain must be in a **RUNNING** state.

10. In the Target Server window, select the server on which to deploy Billing Care and then click **Next**.

    The target server list includes the administration server, any managed servers, and any clusters. For example, the target list might include:

    - admin-server:RUNNING
    - managed-server1:RUNNING
    - managed-server2:RUNNING
    - managed-server3:SHUTDOWN
    - cluster-1:RUNNING

    In this example, cluster-1 is formed by managed-server1, managed-server2, and managed-server3.

> **Note:**
>
> - You can deploy Billing Care on managed servers that are in an offline state.
> - When a cluster is selected as the target, all managed servers in the cluster are targets.
> - Oracle recommends that you deploy Billing Care on a WebLogic Server managed server or cluster. If you select a WebLogic Server managed server, ensure that the WebLogic Server managed server and the node manager are running.
> - If you deploy Billing Care on a WebLogic Cluster, you must enable sticky sessions in your load balancer.

A warning appears confirming that the domain is not configured as an Oracle Platform Security Services (OPSS) Oracle Java Required Files (JRF)-enabled Domain.

11. In the BRM Connection Details window, enter the details listed in Table 5-2 and then click **Next**.

Table 5-2 BRM Connection Details

Field	Description
User Name	The user name for connecting to BRM.
Password	The BRM user's password.
Host Name	The IP address or the host name of the machine on which the primary BRM Connection Manager (CM) or CM Master Process (CMMP) are running.
Port Number	The TCP port number of the CM or CMMP on the host computer. The default value is **11960**.
Service Type	The BRM service type. The default value is **/service/admin_client**.
Service POID ID	The POID of the BRM service. The default value is **1**.
Use SSL?	Whether to use SSL: • If you have not enabled SSL for BRM, deselect the **Use SSL?** checkbox. • If you have enabled SSL for BRM, leave the **Use SSL?** checkbox selected.
Wallet Password	The password for the Billing Care wallet.
Confirm Wallet Password	Enter the password for the Billing Care wallet again.

12. In the Authenticator and Asserter window, select **Skip Authenticator and Asserter** and then click **Next**.
13. In the Batch Payment Details window, enter the details in Table 5-3 and then click **Next**.

Table 5-3 Batch Payment Details

Field	Description
Batch Payment Files Location	The directory where 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**.
Batch Payment Templates Location	The directory where payment file templates are installed.

14. In the Installation Summary window, confirm your installation selections and then click **Install**.
15. The Installation Progress window appears. When installation completes, click **Next**.
16. The Installation Complete window appears. Make note of the Billing Care links, including the Oracle Home location, log file location, and link for accessing Billing Care.

> **Note:**
>
> If the target server is an offline managed server or a cluster, the Billing Care link will be a template link.

17. Click **Finish**.

    The Billing Care installer exits.

Installing Billing Care for Production

The Billing Care installer must be run from the computer hosting the Oracle Platform Security Services (OPSS) Client domain on which you deploy Billing Care. Billing Care installation must be performed by a user who has permissions to write to the **oraInventory** directory and the *Middleware_home***/user_projects/domains** directory, where *Middleware_home* is the directory in which you installed the Oracle Middleware components.

To install Billing Care on your OPSS JRF-enabled domain:

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. Copy the **oamAuthnProvider.jar** file from *Middleware_home***/oracle_common/modules/oracle.oamprovider_11.1.1**, where *Middleware_home* is the WebLogic Server directory containing your OPSS JRF-enabled domain (for example, /u01/app/Oracle/Middleware) to *Middleware_home***/wlserver_12.2/server/lib/mbeantypes**.
3. Start the Oracle WebLogic Server domain administration server or the managed server on which you want to deploy Billing Care. The domain must be configured with the OPSS WebLogic Server Security Module.
4. Download the Billing Care installer. See "Downloading the Billing Care Installer" for more information.
5. Run the following command, which launches the Billing Care installer:

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

> **Note:**
>
> Include the **-invPtrLoc** flag and an Oracle Inventory path location in the Java command for launching the Billing Care installer if you are using an existing or custom Oracle inventory location for maintaining your installed Oracle products and installation logs.

6. In the Welcome window, click **Next**.
7. In the Installation Location window, enter or browse to your Oracle Home directory and then click **Next**.
8. In the Installation Type window, select to install one or both of the following components and then click **Next**.
   - **Billing Care Application**
   - **Billing Care REST API**

> **Note:**
>
> If you select **Billing Care Application**, the Feature Sets Selection window appears next. Otherwise, the WebLogic Server Details window appears next.

9. In the Feature Sets Selection window, select to install one or both of the following components and then click **Next**.
   - **Billing Care Application**
   - **Billing Care SDK**
10. In the WebLogic Server Details window, enter the details listed in Table 5-4 for the WebLogic Server domain in which you want to deploy Billing Care, and then click **Next**.

Table 5-4 WebLogic Server Details

Field	Description
Host Name	The IP address or the name of the machine on which the WebLogic Server domain is configured.
Port Number	The port number assigned to the WebLogic Server domain administration server.
User Name	The WebLogic Server domain administrator user name.
Password	The password for the WebLogic Server domain administrator user.
WebLogic Home	The path to the directory in which the WebLogic Server software is installed.
Use SSL?	Whether to use SSL. Select this checkbox for production installations. Billing Care requires JSSE-based SSL enabled in your OPSS JRF-enabled domain. For more information, see "Using the JSSE-Based SSL Implementation" in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.
KeyStore Type	The type of KeyStore file used in the WebLogic domain for SSL: **JKS** or **PKCS12**.

Table 5-4 (Cont.) WebLogic Server Details

Field	Description
KeyStore Location	The path to your KeyStore file, which is used for authentication through SSL.
KeyStore Password	The password required to access certificates from the KeyStore.

> **Note:**
>
> The Billing Care installer will not proceed until it verifies that the information you entered is valid. The domain must be in a **RUNNING** state.

11. In the Target Server window, select the server on which to deploy Billing Care and then click **Next**.

    The target server list includes the Administration Server, any managed servers, and any WebLogic clusters. For example, the target list might include:

    - admin-server:RUNNING
    - managed-server1:RUNNING
    - managed-server2:RUNNING
    - managed-server3:SHUTDOWN
    - cluster-1:RUNNING

    In this example, cluster-1 is formed by managed-server1, managed-server2, and managed-server3.

> **Note:**
>
> - You can deploy Billing Care on managed servers that are in an offline state.
> - When a cluster is selected as the target, all managed servers in the cluster are targets.
> - Oracle recommends that you deploy Billing Care on a managed server or cluster. If you select a WebLogic Server managed server, ensure that the WebLogic Server managed server and the node manager are running.
> - If you deploy Billing Care on a WebLogic Cluster, you must enable sticky sessions in your load balancer.

12. In the BRM Connection Details window, enter the details listed in Table 5-5 and then click **Next**.

Table 5-5 BRM Connection Details

Field	Description
User Name	The user name for connecting to BRM.
Password	The BRM user's password.

Table 5-5 (Cont.) BRM Connection Details

Field	Description
Host Name	The IP address or host name of the machine on which the primary BRM Connection Manager (CM) or CM Master Process (CMMP) are running.
Port Number	The TCP port number of the CM or CMMP on the host machine. The default value is **11960**.
Service Type	The BRM service type. The default value is **/service/admin_client**.
Service POID Id	The POID of the BRM service. The default value is **1**.
Use SSL?	Whether to use SSL: • If you have not enabled SSL for BRM, deselect the **Use SSL?** checkbox. • If you have enabled SSL for BRM, leave the **Use SSL?** checkbox selected.
Wallet Password	The password for the Billing Care wallet.
Confirm Wallet Password	Enter the password for the Billing Care wallet again.

13. In the Authenticator and Asserter window, enter the details listed in Table 5-6 to connect to the Oracle Unified Directory (OUD) authenticator and then click **Next**.

Table 5-6 Authenticator and Asserter

Field	Description
Skip Authenticator and Asserter	Select this option to skip the creation of the authenticator and asserter.
Provider Name	The OUD Authentication provider you configured in your OPSS Administration Server.
Host Name	The host name or IP address of the LDAP server.
Port Number	The port number on which the LDAP server is listening.
Admin User Name	The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server.
Admin Password	The credential (usually a password) used to connect to the LDAP server.
User Base DN	The base distinguished name (DN) of the tree in the LDAP directory that contains users. For example: `cn=Users,dc=example,dc=com`
Group Base DN	The base distinguished name (DN) of the tree in the LDAP directory that contains groups. For example: `cn=Groups,dc=example,dc=com`
Asserter Name	The name of OAM Identity Asserter. enter a name to use during Billing Care deployment. A new asserter is created if a **OAMIdentityAsserter** type does not exist in your OPSS JRF-enabled domain already.

14. In the Batch Payment Details window, enter the details listed in Table 5-7 for processing batch payments and then click **Next**.

Table 5-7 Batch Payment Details

Field	Description
Batch Payment Files Location	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**.
Batch Payment Templates Location	The directory in which payment file templates are installed.

15. In the Installation Summary window, review your Billing Care installation summary and correct any errors. Click **Install**.
16. The Installation Progress window appears. When the installation completes, click **Next**.
17. The Installation Complete window appears. Make note of the Billing Care links, including the Oracle Home location, log file location, and link for accessing Billing Care.

> **Note:**
>
> If the target server is an offline managed server or a cluster, the Billing Care link will be a template link.

18. Click **Finish**.

    The Billing Care installer exits.

See "Billing Care Postinstallation Tasks" for required tasks to complete after the Billing Care installer exits.

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

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

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**

6

Billing Care Postinstallation Tasks

Learn about postinstallation tasks, such as importing security policies into OPSS, that you perform after installing the Oracle Communications Billing Care software.

Topics in this document:

Postinstallation Tasks

After installing a Billing Care test or production installation, do the following on each domain host where Billing Care is deployed:

1. If your BRM installation uses Oracle Analytics Publisher to view invoices, encrypt and add the Oracle Analytics Publisher credentials for accessing Oracle Analytics Publisher in the **Infranet.properties** file on each domain host where Billing Care is deployed. See "Encrypting and Adding Oracle Analytics Publisher Connection Information in the Wallet".
2. Adjust your BRM connection pool settings and enable logging in the **Infranet.properties** file for your Billing Care environment. You can customize the Billing Care connection pool settings by adding additional entries in the Billing Care **Infranet.properties** configuration file. See "Configuring Additional Settings in the Infranet.properties File".

> **Note:**
>
> During installation, the Billing Care installer copies the Billing Care **Infranet.properties** configuration file to the domain administrative user's home directory on each domain server where Billing Care is deployed. You can update the **Infranet.properties** file in this location.
>
> You can also copy the **Infranet.properties** file in the domain administrative user's home directory to the *domain_home* directory if required. In this case, the **Infranet.properties** file in the *domain_home* directory takes precedence over the **Infranet.properties** file in the domain administrative user's home directory.

For production installations, also do the following:

1. Import the Billing Care OPSS Administration Server policy configuration. The Billing Care SDK includes a default policy configuration file that must be imported into your OPSS Administration Server.
2. If you are using OUD, configure the Billing Care OPSS JRF-enabled domain to connect to the LDAP directory used by Oracle Identity Management (IDM) to store Billing Care users. See "Configuring OPSS JRF-Enabled Domain LDAP Server Connection".
3. If you are using Security Assertion Markup Language (SAML) for single sign-on (SSO), configure SAML. See "Configuring SAML 2.0 for SSO Using a Service Provider".

About Encryption

Encrypting your BRM and Oracle Analytics Publisher passwords and using SSL increases the security of your Billing Care deployment. See "Billing Care Security" in *BRM Security Guide* for more information about securing your Billing Care environment.

Encrypting and Adding Oracle Analytics Publisher Connection Information in the Wallet

You must configure the connection details for your Oracle Analytics Publisher server in each domain server hosting a Billing Care deployment, if Oracle Analytics Publisher is used in your environment.

> **Note:**
>
> Billing Care application supports multiple BRM servers. When a user login to Billing Care application, the application uses the Billing Care wallet and the **Infranet.properties** file from the available BRM servers.

To encrypt your Oracle Analytics Publisher password and store connection credentials in the Billing Care wallet:

1. Log in to your domain server using a secure shell or console terminal session.
2. Use the WebLogic Server **encrypt** Java utility to encrypt your Oracle Analytics Publisher user's password.

   See "encrypt" in *Command Reference for Oracle WebLogic Server* for information about encrypting passwords.
3. Store the following information listed in Table 6-1 in the Billing Care wallet.

   See "Storing Configuration Entries in the Billing Care Wallet" in *BRM Security Guide* for more information.

Table 6-1 Oracle Analytics Publisher Connection Information

Field	Description
BIP_USERID	Oracle Analytics Publisher user with web access
BIP_PASSWORD	Encrypted Oracle Analytics Publisher user's password
BIP_URL	URL address to access the Oracle Analytics Publisher instance

4. For production installations, if not already done, enable SSL for the OPSS JRF-enabled domain where Billing Care is deployed.
5. Restart the domain where Billing Care is deployed.

Configuring Additional Settings in the Infranet.properties File

Billing Care uses the default connection pool settings for your BRM instance. You can customize Billing Care connection pool settings by adding additional entries in the Billing Care **Infranet.properties** configuration file. You can also enable logging by adding optional entries or changing the BRM connection details in the Billing Care **Infranet.properties** file.

> **Note:**
>
> You can update the BRM connection details in the Billing Care **Infranet.properties** file or in the Billing Care wallet. However, it is recommended to update sensitive information (such as BRM user password) only by using the Billing Care wallet.

See "About Connection Pooling" in *BRM System Administrator's Guide* for more information about changing the default connection pool.

See "Optional Entries in the Infranet.properties File" in *BRM Developer's Guide* for more information about enabling logging for Billing Care connections to BRM.

Importing the Billing Care Security Policies to OPSS

The Billing Care SDK includes the **system-jazn-data.xml** file, which contains default policies, resource types, resources, and actions. You must import this file into your OPSS Administration Server to set up the initial Billing Care OPSS configuration.

The **system-jazn-data.xml** file is located in the *Middleware_home***/BillingCare_SDK/reference/AuthorizationDataModel** directory created during the Billing Care SDK installation, where *Middleware_home* is the WebLogic Middleware home directory containing the OPSS JRF-enabled domain on which Billing Care is deployed.

To migrate the **system-jazn-data.xml** file into your OPSS Administration Server:

1. Open a secure shell or terminal session on the server where you installed the Billing Care SDK.
2. Go to the *Middleware_home***/BillingCare_SDK/reference/AuthorizationDataModel** directory.
3. Open the **jps-config.xml** file and modify the following parameters:
   - **sourceContext**. Specify the location of the **system-jazn-data.xml** file, which contains the policies to be migrated to the database. The **system-jazn-data.xml** file is in the same location as the **jps-config.xml** file.

     ```
     <serviceInstance name="src.xml" provider="policystore.xml.provider"
     location="location of the system-jazn-data.xml file">
        <description>File-Based Policy Store Service Instance</description>
     </serviceInstance>
     ```

   - **destinationContext**. Enter the credentials for the Oracle Platform Security Services (OPSS) database schema.

> **Note:**
>
> Add the **property name** entries (shown in bold) if you enabled one-way or two-way SSL authentication for connections with the OPSS database schema.

```
<serviceInstance name="policystore.db.destination"
provider="policystore.provider">
   <description>DB Based Policy Store Service Instance</description>
   <property name="policystore.type" value="DB_ORACLE"/>
   <property name="jdbc.driver" value="oracle.jdbc.driver.OracleDriver"/>
   <property name="security.principal" value="OPSS_SchemaName"/>
   <property name="security.credential" value="OPSS_SchemaPassword"/>
   <property name="oracle.security.jps.ldap.root.name" value="cn=opssroot"/>
   <property name="oracle.security.jps.farm.name" value="cn=opssSecurityStore"/>

   <!--Add this property if SSL is NOT enabled for connections with the OPSS
database schema-->
   <property name="jdbc.url" value="jdbc:oracle:thin:@dbhost:dbport:SID"/>

   <!--Add the following properties for both one-way and two-way SSL
authentication-->
   <property name="javax.net.ssl.trustStore" value="walletFileNameAndPath"/>
   <property name="javax.net.ssl.trustStoreType" value="SSO_or_PKCS12"/>
   <property name="javax.net.ssl.trustStorePassword"
value="passwordForPKCS12_Only"/>
   <property name="security.providers.3"
value="oracle.security.pki.OraclePKIProvider"/>
   <property name="jdbc.url"
value="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=dbhost)
(PORT=dbport))(CONNECT_DATA=(SERVICE_NAME=SID)))"/>

   <!--Also add the following properties for two-way SSL authentication-->
   <property name="javax.net.ssl.keyStore" value="walletFileNameAndPath"/>
   <property name="javax.net.ssl.keyStoreType" value="SSO_or_PKCS12"/>
   <property name="javax.net.ssl.keyStorePassword"
value="passwordForPKCS12_Only"/>
</serviceInstance>
```

- **jpsContext**. Specify the source context and the destination context.

```
<jpsContext name="sourceContext">
   <serviceInstanceRef ref="src.xml"/>
</jpsContext>
<jpsContext name="destinationContext">
   <serviceInstanceRef ref="policystore.db.destination"/>
</jpsContext>
```

4. Save the file.
5. Run the **migrateSecurityStore** utility to migrate the Billing Care policy into your OPSS Administration Server.
6. Restart the OPSS JRF-enabled domain.

See *Oracle Fusion Middleware Administrator's Guide* for detailed information on how to import the Billing Care **system-jazn-data.xml** file into your OPSS Administration Server.

Configuring OPSS JRF-Enabled Domain LDAP Server Connection

If you are using OUD or third-party LDAP directory server products, each OPSS JRF-enabled domain must be configured with connection details to OUD, as the LDAP identity store, in the **jps-config.xml** file so that Billing Care can retrieve users from the directory.

> **Note:**
>
> Additional LDAP servers, including Oracle Internet Directory and third-party LDAP directory server products, can be configured for use with Billing Care using the process described below. See "Configuring the Identity Store Service" in *Oracle Fusion Middleware Application Security Guide* for more information on using other LDAP servers.

To configure Billing Care's connection to OUD, on each OPSS JRF-enabled domain server where Billing Care is deployed:

1. Open a secure shell or terminal session on the server where the OPSS JRF-enabled domain is located.
2. Go to the *Domain_home***/config/fmwconfig/jps-config.xml** directory.
3. In the **<servicesInstances>** section of the **jps-config.xml** file, add the following identity store service entry containing your OUD server connection information.

   ```
   <serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
      <description>LDAP Identity Store Service Instance</description>
      <property name="idstore.type" value="IPLANET"/>
      <property name="subscriber.name" value="subscriber.name"/>
      <property name="cleartext.ldap.credentials" value="ldap_credentials"/>
      <property name="ldap.url" value="ldap:ldap_url:port"/>
   </serviceInstance>
   ```

   where:

   - *idstore.ldap* is the name of your LDAP authenticator.
   - *subscriber.name* includes the LDAP domain components for Billing Care users. For example:

     ```
     dc=billingcare, dc=com
     ```

   - *ldap_credentials* is an authentication string in clear text containing the required principal and password for accessing the LDAP server. For example:

     ```
     cn=Directory Manager,cn=Root DNs,cn=config:password
     ```

     where *password* is a valid credential for the common name user accessing the LDAP server.

   - *ldap_url:port* is the LDAP server URL and port number.
4. In the **<jpsContext name="default">** section of the **jps_config.xml** file, add the following entry to reference the identity store instance configured in the previous step:

   ```
   <serviceInstanceRef ref="idstore.ldap"/>
   ```

where *idstore.ldap* is the **serviceInstance** name you configured in the step above.

5. Save the file.

Enabling Logging and Configuring the WebLogic Server Deployment

Billing Care writes log messages using the Java Logging API. See Oracle Fusion Middleware Configuring Log Files and Filtering Log Messages for Oracle WebLogic Server for more information about enabling Billing Care logging.

Since Billing Care is a web application that is deployed on WebLogic Server, refer to the WebLogic Server documentation for information about overriding timeouts, cookie attributes, and so on. See "web.xml Deployment Descriptor Elements" and "weblogic.xml Deployment Descriptor Elements" in *Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server* for more information about these configurations.

Configuring SAML 2.0 for SSO Using a Service Provider

You can use SAML 2.0 for enabling SSO in Billing Care. SSO allows you to log in to applications using a single user name and password combination.

You can configure SAML authentication in a Billing Care domain using an Oracle Access Management service provider or an Oracle Identity Cloud Service (IDCS) service provider.

To configure SAML for SSO:

1. Create a SAML2 assertion provider. See "Creating a SAML2 Assertion Provider".
2. Create a SAML2 authenticator. See "Creating a SAML2 Authenticator".
3. Configure the SAML2 general information. See "Configuring SAML2 General Information".
4. Configure your SAML2 service provider. See "Configuring the SAML2 Service Provider".
5. Create a SAML2 application in IDCS or Oracle Access Management.
6. Update your deployment plan to define the cookie name and path. See "Updating the Deployment Plan of Billing Care".
7. (IDCS only) In your Billing Care **Infranet.properties** file, set the SSO_SIGNOUT_URL parameter:

   SSO_SIGNOUT_URL=https://*hostname*:*port*/sso/v1/user/logout

   where *hostname*:*port* is the hostname and port for the IDCS logout URL.

Creating a SAML2 Assertion Provider

To create a SAML2 assertion provider:

1. Log in to WebLogic Server Administration Console.
2. In the **Domain Structure** section, click the **Security Realms** link.

   The Summary of Security Realms page appears.
3. Click the **myrealm** link.

   The Settings for myrealm page appears.

4. Click the **Providers** tab, the **Authentication** subtab, and then **New**.

   The Create a New Authentication Provider page appears.
5. In the **Name** field, enter **samlBCAsserter**.
6. From the **Type** list, select **SAML2IdentityAsserter**.
7. Click **OK**.
8. Restart WebLogic Server.
9. In the **Authentication** subtab, click the **samlBCAsserter** link.

   The Settings for samlBCAsserter page appears.
10. Click the **Management** tab.
11. Click **New** and then click **New Web Single Sign-On Identity Provider Partner**.

    The Create a SAML 2.0 Web Single Sign-On Identity Provider Partner page appears.
12. In the **Name** field, enter **WebSSO-IdP-Partner**.
13. In the **Path** field, enter the path to the XML file that contains the identity provider's metadata, such as **metadata.xml**.
14. Click **OK**.
15. In the Settings for samlBOCAsserter page, click the **Management** tab and then click the **WebSSO-IdP-Partner-0** link.
16. In the **General** tab, select the **Enabled**, **Virtual User**, and **Process Attributes** check boxes.
17. In the **Redirect URIs** field, enter **/bc/***.
18. Click **Save**.

Creating a SAML2 Authenticator

To create a SAML2 authenticator:

1. Log in to WebLogic Server Administration Console.
2. In the **Domain Structure** section, click the **Security Realms** link.

   The Summary of Security Realms page appears.
3. Click the **myrealm** link.

   The Settings for myrealm page appears.
4. Click the **Providers** tab, the **Authentication** subtab, and then **New**.

   The Create a New Authentication Provider page appears.
5. In the **Name** field, enter **samlBCAuthenticator**.
6. From the **Type** list, select **SAMLAuthenticator**.
7. Click **OK**.
8. In the Authentication Providers table, click the **samlBCAuthenticator** link and change the **Control Flag** to **SUFFICIENT**.
9. Click **Save**.
10. In the Authentication Providers table, click the **DefaultAuthenticator** link, and change the **Control Flag** to **SUFFICIENT**.

11. Click **Save**.
12. In the Authentication Providers table, click **Reorder**.

    The Reorder Authentication Providers page appears.
13. Reorder the providers in the following order:
    - **samlBCAuthenticator**
    - **samlBCAsserter**
    - **DefaultAuthenticator**
    - **DefaultIdentityAsserter**
14. Click **OK**.

Configuring SAML2 General Information

To configure SAML 2.0 general information:

1. In the **Domain Structure** section, expand **Environment** and then click **Servers**.

   The Summary of Servers page appears.
2. In the Servers table, click the **AdminServer** link.

   The Settings for AdminServer page appears.
3. Select the **Configuration** tab, the **Federation Services** subtab, and then the **SAML 2.0 General** subtab.
4. In the **Published Site URL** field, enter **http://***BillingCare_hostname***:***port***/saml2**.

   where:
   - *BillingCare_hostname* is either the Billing Care application host name or the load balancer host name.
   - *port* is the port on which Billing Care is listening on.
5. In the **Entity ID** field, enter **samlBCAsserter**.
6. Click **Save**.

Configuring the SAML2 Service Provider

To configure the SAML2 service provider:

1. Log in to WebLogic Server Administration Console.
2. In the Domain Structure section, expand **Environment** and then click **Servers**.

   The Summary of Servers page appears.
3. In the Servers table, click the **AdminServer** link.

   The Settings for AdminServer page appears.
4. Select the **Configuration** tab, the **Federation Services** subtab, and then the **SAML 2.0 Service Provider** subtab.
5. Select the **Enabled** check box.
6. From the **Preferred Binding** list, select **POST**.
7. In the **Default URL** field, enter **http://***BillingCare_hostname***:***port***/bc/login.html**.

where:

- *BillingCare_hostname* is the Billing Care application host name or load balancer name.
- *port* is the port on which Billing Care is listening on.

8. Restart WebLogic Server.

Updating the Deployment Plan of Billing Care

To update the deployment plan of Billing Care:

1. Merge the following contents with your existing Billing Care deployment plan:

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan
http://xmlns.oracle.com/weblogic/deployment-plan/1.0/deployment-plan.xsd"
global-variables="false">
   <application-name>BillingCare.war</application-name>
   <variable-definition>
      <variable>
         <name>cookie-name</name>
         <value>JSESSIONID</value>
      </variable>
      <variable>
         <name>cookie-path</name>
         <value>/bc</value>
      </variable>
   </variable-definition>
   <module-override>
      <module-name>BillingCare.war</module-name>
      <module-type>war</module-type>
      <module-descriptor external="true">
         <root-element>weblogic-web-app</root-element>
         <uri>WEB-INF/weblogic.xml</uri>
         <variable-assignment>
            <name>cookie-name</name>
            <xpath>/weblogic-web-app/session-descriptor/cookie-name</xpath>
            <operation>replace</operation>
         </variable-assignment>
         <variable-assignment>
            <name>cookie-path</name>
            <xpath>/weblogic-web-app/session-descriptor/cookie-path</xpath>
            <operation>remove</operation>
         </variable-assignment>
      </module-descriptor>
   </module-override>
</deployment-plan>
```

2. Log in to the Oracle WebLogic Server Administration Console.
3. In the **Domain Structure** section, click **Deployments**.
4. In the **Configuration** tab, select the **BillingCare** check box and then click **Update**.

   The Update Application Assistant window appears.
5. In Deployment plan path, click **Change Path** and enter the path to your Billing Care deployment file.
6. Click **Finish**.

7

Verifying the Billing Care Installation

Learn how to verify that Oracle Communications Billing Care is installed by checking the state of all installed components or by logging in to Billing Care.

To check the state of all installed components:

1. Log in to the WebLogic Server Administration Console of the domain where Billing Care is deployed.
2. In the **Domain Structure** section, click **Deployments**.

   The Summary of Deployments window appears.
3. Ensure that all of the managed servers are running.
4. Ensure that **BillingCare** appears in **Active** state.
5. For successful REST API Deployment, ensure that **Billing Care REST** appears in **Active** state.

To log in to Billing Care:

1. Open a browser window.
2. Enter the URL provided by the Billing Care installer at the end of the installation.
3. Click **Go**.

   The Billing Care login window appears.
4. 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.