Copyright © 2017, 2019, Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.
Contents

Preface

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

1 Billing Care Installation Overview

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

2 Planning Your Billing Care Installation

About Planning Your Billing Care Installation 2-1
About Test Installations and Production Installations 2-1
  About Test Installations 2-1
  About Production Installations 2-1
Database Planning 2-2
Authentication and Authorization Planning 2-2
About Installing a Secure System 2-2

3 Billing Care System Requirements

Software Requirements 3-1
Hardware Requirements 3-1
About IPv4 and IPv6 Support for Fusion Middleware Products 3-2

4 Billing Care Pre-Installation Tasks

Overview of Production Pre-Installation Tasks 4-1
Installing and Configuring Oracle Enterprise Database 4-1
Installing and Configuring Oracle WebLogic Server 4-2
  Configuring the OPSS JRF-Enabled Billing Care Application Domain 4-2
Installing and Configuring Oracle Unified Directory 4-2
  Configuring Oracle Unified Directory as Authentication Provider 4-2
Installing and Configuring Oracle Access Management 4-2
  Configuring the Oracle Access Manager Billing Care Application Domain 4-3
    Creating the Billing Care Application Domain 4-3
    Defining Billing Care Resources 4-3
    Configuring Billing Care Authentication Modules 4-4
    Creating a Billing Care Authentication Scheme 4-5
    Creating the Billing Care Authentication Policy and Adding Resources 4-5
    Creating the Billing Care Authorization Policy and Adding Resources 4-6
    Configuring and Restarting the Oracle HTTP Server 4-7
Installing and Configuring Oracle Identity Governance 4-8
  Information Requirements 4-8
    OPSS JRF-enabled Domain Information 4-8
    BRM Connection Information 4-8
    Oracle Unified Directory Information 4-9
    Oracle Database Connection Information 4-10
    Oracle Identity and Access Management Console URLs 4-10
    BIP Connection Information 4-10

5 Installing Billing Care

  Downloading the Billing Care Installer 5-1
  Installing Billing Care for Testing 5-2
    Configuring WebLogic Server for a Test Installation 5-2
    Running the Billing Care Installer for Testing 5-2
  Installing Billing Care for Production 5-5
  About Installation Logs 5-9

6 Billing Care Post-Installation Tasks

  Post-Installation Tasks 6-1
    About Encryption 6-2
    Encrypting and Adding BIP Connection Information in the Wallet 6-2
    Configuring Additional Settings in the Infranet.properties File 6-2
    Importing the Billing Care Security Policies to OPSS 6-3
    Configure OPSS JRF-Enabled Domain LDAP Server Connection 6-4
    Configuring Internet Explorer for Billing Care 6-5
    Enabling Logging 6-6
7 Verifying the Billing Care Installation
Preface

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, 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.

Related Documents

The following documents contains related information and are referenced in this guide:

- Administering Security for Oracle WebLogic Server
- Oracle Communications Billing and Revenue Management Developer's Guide
- Oracle Communications Billing and Revenue Management System Administrator's Guide
- Oracle Database Online Documentation 12c Release 2
- Oracle Fusion Middleware Administrator's Guide for Oracle Access Management
- Oracle Fusion Middleware Deploying Applications to Oracle WebLogic Server
- Oracle Fusion Middleware Domain Template Reference
- Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management
- Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite
- Oracle Fusion Middleware Securing Oracle WebLogic Server
Accessing Oracle Communications Documentation

Billing Care documentation and additional Oracle documentation, such as Oracle Database, WebLogic, and Identity and Access Management documentation, is available from Oracle Help Center:

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

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

- [https://edelivery.oracle.com](https://edelivery.oracle.com)

Document Revision History

The following table lists the revision history for this guide:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E91359-01</td>
<td>December 2017</td>
<td>Initial release.</td>
</tr>
<tr>
<td>E91359-02</td>
<td>September 2018</td>
<td>Documentation updates for Billing Care 12.0 Patch Set 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional Software Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloading the Billing Care Installer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Post-Installation Tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring Additional Settings in the Infranet.properties File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Importing the Billing Care Security Policies to OPSS</td>
</tr>
<tr>
<td>E91359-03</td>
<td>August 2019</td>
<td>Documentation updates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the following chapters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Billing Care System Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Billing Care Pre-Installation Tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planning Your Billing Care Installation</td>
</tr>
<tr>
<td>E91359-04</td>
<td>September 2019</td>
<td>Documentation updates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the following chapters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Billing Care System Requirements</td>
</tr>
</tbody>
</table>
Billing Care Installation Overview

This chapter provides an overview of Oracle Communications Billing Care components and installation process.

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:

- UNIX/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 deploys Billing Care to a WebLogic server domain, installs the Billing Care SDK, or performs both actions.

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 pre-installation tasks:
   See "Billing Care Pre-Installation Tasks " for more information.

4. Install Billing Care and the Billing Care SDK (if required) using the Oracle Universal Installer (OUI) Billing Care installer.
   See "Installing Billing Care " for more information.

5. Perform the required post-installation configuration tasks.
   See "Billing Care Post-Installation 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 pre-installation 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 pre-installation 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.
Planning Your Billing Care Installation

This chapter provides information on planning your Oracle Communications Billing Care installation.

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 pre-installation 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 in 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 Guide*.
Billing Care System Requirements

This chapter describes Oracle Communications Billing Care software and hardware requirements.

Software Requirements

Billing Care is deployed on the Oracle Platform Security Services (OPSS) JRF-enabled WebLogic Server domain. See Oracle Platform Security Services or OPSS in Fusion Middleware Identity Management 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 Preparing to Install in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management for more information on IdM component hardware and sizing.
Table 3-1  Billing Care Single Server Minimum Hardware Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 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, Oracle Database Hardware Requirements and Software Requirements in Oracle Database Online Documentation 12c Release 1 /Installing and Upgrading for more information on the database requirements.

About IPv4 and IPv6 Support for Fusion Middleware Products

For information on network considerations, including support for IPv6 addresses, see Configuring IPv4 and IPv6 for Fusion Middleware Products in Oracle Fusion Middleware System Requirements and Specifications.
Billing Care Pre-Installation Tasks

This chapter describes the tasks that you must perform before running the Oracle Communications Billing Care installer. The procedures include links to relevant documentation in related product documentation.

Overview of Production Pre-Installation 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 pre-installation 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.

Pre-installation 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 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/

Record your database details in Table 4-9.
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 "Obtaining the Oracle Fusion Middleware Software in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management" for more information on downloading 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 "Configuring your 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 (OUD) 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 an Authentication Provider for Oracle Unified Directory" in Oracle Fusion Middleware Securing 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.

Record your OUD details in Table 4-8.

Installing and Configuring Oracle Access Management

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

See "Introduction to Application Domain and Policy Creation" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management for more information on application domains and policies.

Creating the Billing Care Application Domain

To create the Billing Care application domain:

1. Log into your OAM web console at http://Host:port/oamconsole where Host 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.

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>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>HTTP</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter text description</td>
</tr>
<tr>
<td><strong>Host Identifier</strong></td>
<td>IAMSuiteAgent</td>
</tr>
<tr>
<td><strong>Protection Level</strong></td>
<td>Protected</td>
</tr>
<tr>
<td><strong>Authentication Policy</strong></td>
<td>Protected Policy</td>
</tr>
<tr>
<td><strong>Resource URL (String)</strong></td>
<td>/bc*, /bc*, or /**</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>HTTP</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter text description</td>
</tr>
<tr>
<td><strong>Host Identifier</strong></td>
<td>IAMSuiteAgent</td>
</tr>
<tr>
<td><strong>Protection Level</strong></td>
<td>Excluded</td>
</tr>
<tr>
<td><strong>Resource URL (String)</strong></td>
<td>/favicon.ico</td>
</tr>
</tbody>
</table>


### 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**.
Creating a Billing Care Authentication Scheme

The authentication module you previously created must be added to a 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>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Billing Care LDAP Scheme name</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter text description</td>
</tr>
<tr>
<td>Authentication Level</td>
<td>2</td>
</tr>
<tr>
<td>Challenge Method</td>
<td>FORM</td>
</tr>
<tr>
<td>Challenge Redirect URL</td>
<td>/oam/server</td>
</tr>
<tr>
<td>Authentication Module</td>
<td>Select the authentication module created in the previous step</td>
</tr>
<tr>
<td>Challenge URL</td>
<td>/pages/login.jsp</td>
</tr>
<tr>
<td>Context Type</td>
<td>default</td>
</tr>
<tr>
<td>Context Value</td>
<td>/oam</td>
</tr>
</tbody>
</table>

4. Click Apply.


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>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Billing Care authentication policy name</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter text description</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>Select the authentication scheme created in the previous step</td>
</tr>
</tbody>
</table>

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**.


**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>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Billing Care authorization policy name</td>
</tr>
</tbody>
</table>
Table 4-5 (Cont.) Billing Care Authorization Policy Creation Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Enter text description</td>
</tr>
<tr>
<td>Success URL</td>
<td>The redirect URL to be used upon successful authorization</td>
</tr>
<tr>
<td>Failure URL</td>
<td>The redirect URL to be used upon failed authorization</td>
</tr>
</tbody>
</table>

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 Administrator's Guide for Oracle Access Manager 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
   ```

Installing and Configuring Oracle Identity Governance

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


Information Requirements

This section describes the information that you will be required to provide during and after the Billing Care installation procedure. You define some of these configuration values when you complete the previous steps. After you have completed all of the pre-installation steps, see "Installing Billing Care" for information on running the Billing Care installer to install Billing Care.

Note:
Oracle recommends that you print the tables and record the values for when you run the Billing Care installer.

OPSS JRF-enabled Domain Information

Table 4-6 lists the details for the OPSS JRF-enabled domain that are required during Billing Care installation. Use the Value column to record your environment's details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The IP address or the host name of the computer on which the OPSS JRF-enabled domain is configured.</td>
<td>-</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number assigned to the OPSS JRF-enabled domain administration server.</td>
<td>-</td>
</tr>
<tr>
<td>User Name</td>
<td>The OPSS JRF-enabled domain administrator user name.</td>
<td>-</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the OPSS JRF-enabled domain administrator user.</td>
<td>-</td>
</tr>
<tr>
<td>WebLogic Home</td>
<td>The path of the directory in which the WebLogic Server software is installed on the OPSS JRF-enabled domain server.</td>
<td>-</td>
</tr>
</tbody>
</table>

BRM Connection Information

Table 4-7 lists the details for connecting to BRM. Use the Value column to record your environment's details.
### Table 4-7  BRM Connection Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name for connecting to BRM.</td>
<td>-</td>
</tr>
<tr>
<td>Password</td>
<td>The BRM user's password.</td>
<td>-</td>
</tr>
<tr>
<td>Host Name</td>
<td>The IP address or the host name of the machine on which the primary BRM Connection Manager (CM) or CM Master Process (CMMP) are running.</td>
<td>-</td>
</tr>
<tr>
<td>Port Number</td>
<td>The TCP port number of the CM or CMMP on the host computer. The default value is 11960.</td>
<td>-</td>
</tr>
<tr>
<td>Service Type</td>
<td>The BRM service type. The default value is /serv ide/admin_client</td>
<td>-</td>
</tr>
<tr>
<td>Service POID Id</td>
<td>The POID of the BRM service. The default value is 1.</td>
<td>-</td>
</tr>
<tr>
<td>Use SSL?</td>
<td>Whether to use SSL.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>If you have not enabled SSL for BRM, deselect the Use SSL? check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you have enabled SSL for BRM, leave the Use SSL? check box selected.</td>
<td></td>
</tr>
<tr>
<td>Wallet Password</td>
<td>The password for the Billing Care wallet</td>
<td>-</td>
</tr>
</tbody>
</table>

### Oracle Unified Directory Information

Table 4-8 lists the details for the Oracle Unified Directory (OUD) authentication provider that are required during Billing Care installation. This information is required only if you are using OUD for authentication. Use the Value column to record your environment's details.

### Table 4-8  Oracle Unified Directory Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
<td>Name of OUD Authentication provider.</td>
<td>-</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host name or IP address of the LDAP server.</td>
<td>-</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number on which the LDAP server is listening.</td>
<td>-</td>
</tr>
<tr>
<td>Admin User Name</td>
<td>The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server.</td>
<td>-</td>
</tr>
<tr>
<td>Admin Password</td>
<td>The credential (usually a password) used to connect to the LDAP server.</td>
<td>-</td>
</tr>
<tr>
<td>User Base DN</td>
<td>The base distinguished name (DN) of the tree in the LDAP directory that contains use.</td>
<td>-</td>
</tr>
<tr>
<td>Group Base DN</td>
<td>The base distinguished name (DN) of the tree in the LDAP directory that contains group.</td>
<td>-</td>
</tr>
<tr>
<td>Asserter Name</td>
<td>The name of the OAM Identity Asserter.</td>
<td>-</td>
</tr>
</tbody>
</table>
Oracle Database Connection Information

Table 4-9 lists the database details that are required during response file configuration for silent installation. Use the Value column to record your environment's details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The IP address or the host name of the computer on which the database is configured.</td>
<td>-</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number assigned to the database service.</td>
<td>-</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name of the database administrator.</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>This user should have the following capabilities on the database: create user, grant any role, grant any privileges, and select any table for Enterprise edition.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>The database administrator's password.</td>
<td>-</td>
</tr>
<tr>
<td>Service Name</td>
<td>The name of the database service.</td>
<td>-</td>
</tr>
</tbody>
</table>

Oracle Identity and Access Management Console URLs

Table 4-10 lists the Oracle Identity Management (IdM) Console URLs which are required to complete Billing Care pre-installation and configuration if you are using IdM. The Host is the server name or IP address of your OPSS Administration Server. Default values are provided for the ports. Use the Value column to record your environment's details.

<table>
<thead>
<tr>
<th>Web Application URL</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://Host:7778/identity">http://Host:7778/identity</a></td>
<td>Oracle Identity Management console</td>
<td>-</td>
</tr>
<tr>
<td><a href="http://Host:7777/oamconsole">http://Host:7777/oamconsole</a></td>
<td>Oracle Access Management console</td>
<td>-</td>
</tr>
<tr>
<td><a href="http://Host:7001/console">http://Host:7001/console</a></td>
<td>Oracle WebLogic Administration Console</td>
<td>-</td>
</tr>
</tbody>
</table>

BIP Connection Information

Table 4-11 lists the Oracle Business Intelligence Publisher (BIP) details, if used, that are required after the Billing Care installation. Use this information to configure the BIP instance to which Billing Care connects to.

See "Encrypting and Adding BIP Connection Information in the Wallet" for more information on how to configure Billing Care to BIP connections in each OPSS JRF-enabled domain on which Billing Care is deployed. Use the Value column to record your environment's details.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BIP_PASSWORD</strong></td>
<td>Encrypted BIP user's password</td>
<td>-</td>
</tr>
<tr>
<td><strong>BIP_USERID</strong></td>
<td>BIP user with web access</td>
<td>-</td>
</tr>
<tr>
<td><strong>BIP_URL</strong></td>
<td>URL address to access BIP instance</td>
<td>-</td>
</tr>
</tbody>
</table>
Installing Billing Care

This chapter describes how to install Oracle Communications Billing Care. Before installing Billing Care, read the following chapters:

- Billing Care Installation Overview
- Planning Your Billing Care Installation
- Billing Care System Requirements
- Billing Care Pre-Installation Tasks

Billing Care supports test and productions installations. For more information on test and production installations, see "Installing Billing Care for Testing" and "Installing Billing Care for Production" respectively.

Downloading the Billing Care Installer

To download the Billing Care installer:

1. Create a temporary directory (temp_dir).
2. Go to the Oracle support Web site:
   https://support.oracle.com
3. Sign in with your user name and password.
4. Click the Patches & Updates tab.
5. From the list, select Patch Name or Number.
6. In the text field, enter PatchNumber and click Search, where PatchNumber is patch number of Oracle Communications Billing and Revenue Management (BRM) 12.0 patch set that includes the Billing Care software.
   
   See BRM 12.0 Patch Set Installation Guide for more information about the patch number.
   
   The Patch Search Results page appears.
7. Click the patch name.
   
   The patch details appear.
8. From the Platform list, select platform and click Download, where platform is linux or solaris.
   
   The File Download dialog box appears.
9. Download the appropriate pPatchNumber_12v_Generic.zip software pack to temp_dir, where v is the patch version. For example, it is 1 for Billing Care 12.0 Patch Set 1 and 2 for Billing Care 12.0 Patch Set 2.
    
    The package includes the BillingCare_generic.jar installer.
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 Oracle Communications Billing Care 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 your Java Development Kit is installed correctly, including setting 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 on how to download the installer.

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.

   The Welcome screen appears.

   5. Click **Next**.

   The Installation Location screen appears. Enter your Oracle Home directory path in **Oracle Home** or click **Browse** to select a directory.

   6. Click **Next**.

   The Features Sets Selection screen appears.

   This screen displays the available Billing Care components. Select either the **Billing Care Application** or the **Billing Care REST API** components.

   If you select Billing Care Application, the next screen displays the component selection screen for the Billing Care Application and the Billing Care SDK.

   7. Click **Next**.

   The WebLogic Server Details screen appears.

   8. Enter the following details for the WebLogic Server OPSS JRF-enabled domain in which you want to deploy Billing Care, see Table 4-6 for more information:

   a. In the **Host Name** field, enter the IP address or the host name of the computer on which the WebLogic Server domain is configured.

   b. In the **Port Number** field, enter the port number assigned to the WebLogic Server domain administration server.

   c. In the **User Name** field, enter the WebLogic Server domain administrator user name.

   d. In the **Password** field, enter the password for the WebLogic Server domain administrator user.

   e. In the **WebLogic Home** field, enter the path of the directory in which the WebLogic Server software is installed.

   **Note:**
   The Billing Care installer does not proceed until it verifies that the information you entered is valid. The domain must be in a **RUNNING** state.
f. Deselect the **Use SSL?** check box.

g. Click **Next**.

The Target Server screen appears.

9. Select the server on which to deploy Billing Care. The target server list includes the AdminServer and any managed servers managed by the AdminServer.

**Note:**

Oracle recommends that you deploy Billing Care on a WebLogic Server managed server. If you select a WebLogic Server managed server, ensure that the WebLogic Server managed server and the node manager are running.

10. Click **Next**.

The BRM Connection Details screen appears.

11. Enter the following details for connecting to BRM, see Table 4-7 for more information:

   a. In the **User Name** field, enter the user name for connecting to BRM.

   b. In the **Password** field, enter the BRM user's password.

   c. In the **Host Name** field, enter 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.

   d. In the **Port Number** field, enter the TCP port number of the CM or CMMP on the host computer. The default value is **11960**.

   e. In the **Service Type** field, enter the BRM service type. The default value is `/servide/admin_client`.

   f. In the **Service POID Id** field, enter the POID of the BRM service. The default value is **1**.

   g. Do one of the following:

      If you have not enabled SSL for BRM, deselect the **Use SSL?** check box.

      If you have enabled SSL for BRM, leave the **Use SSL?** check box selected.

   h. In the **Wallet Password** field, enter the password for the Billing Care wallet.

   i. In the **Confirm Wallet Password** field, enter the password for the Billing Care wallet again.

12. Click **Next**.

The Authenticator and Asserter screen appears.

13. Select **Skip Authenticator and Asserter**.

14. Click **Next**.

The Batch Payment Details screen appears.

15. Enter the following file locations used for processing batch payments:

   a. In the **Batch Payment Files Location** field, enter the directory where batch payment files are placed for uploading and processing by Billing Care. The
installer creates unprocessed, processed, and failure folders in this directory for managing batch payment files.

b. In the **Batch Payment Templates Location** field, enter the directory where payment file templates are installed.

16. Click **Next**.
   The Auto Updates screen appears.

17. Select your Auto Updates preferences.

18. Click **Next**.
   The Installation Summary screen appears.

19. Review your Billing Care installation summary and correct any errors.

20. Click **Install**.
   The Installation Progress screen appears.

21. When the Installation completes, Click **Next**.
   The Installation Complete screen appears. Make note of the Billing Care Links.

22. 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 your Java Development Kit is installed correctly, including setting 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/wlsServer_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 on how to download the installer.

5. 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.

The Welcome screen appears.

6. Click Next.

The Installation Location screen appears. Enter your Oracle Home directory path in Oracle Home or click Browse to select a directory.

7. Click Next.

The Installation Type screen appears.

This screen displays the available Billing Care components. Select the Billing Care Application or the Billing Care REST API.

8. Click Next.

Based on the selection in the previous screen, appropriate Feature Set Selection screen appears.

9. Click Next.

The WebLogic Server Details screen appears.

10. Enter the following details for the WebLogic Server OPSS JRF-enabled domain in which you want to deploy Billing Care, see Table 4-6 for more information:

   a. In the Host Name field, enter the IP address or the host name of the computer on which the WebLogic Server domain is configured.

   b. In the Port Number field, enter the port number assigned to the WebLogic Server domain administration server.

   c. In the User Name field, enter the WebLogic Server domain administrator user name.

   d. In the Password field, enter the password for the WebLogic Server domain administrator user.

   e. In the WebLogic Home field, enter the path of the directory in which the WebLogic Server software is installed.

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.

f. Do one of the following:

   If the server does not support SSL, deselect the Use SSL? check box.
Billing Care requires JSSE-Based SSL enabled in your OPSS JRF-enabled domain. See "Using the JSSE-Based SSL Implementation" in Oracle Fusion Middleware Securing Oracle WebLogic Server for more information on using JSEE-Based SSL.

If you have configured SSL in your OPSS JRF-enabled domain, leave the Use SSL? check box selected, and, in the KeyStore Location field, enter the path of the client-side keystore file generated from the exported public certificate using the keytool utility.

For information on generating a keypair and root certificate for your encrypted password, and storing the certificate, using the Java keytool utility, see:

https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html

See "Configuring SSL" in Oracle Fusion Middleware Securing Oracle WebLogic Server for more information on using SSL in your domain.

g. Click Next.

The Target Server screen appears.

11. Select the server on which to deploy Billing Care. The target server list includes the AdminServer and any managed servers managed by the AdminServer.

Note:
Oracle recommends that you deploy Billing Care on a WebLogic Server managed server. If you select a WebLogic Server managed server, ensure that the WebLogic Server managed server and the node manager are running.

12. Enter the following details for connecting to BRM, see Table 4-7 for more information:

   a. In the User Name field, enter the user name for connecting to BRM.

   b. In the Password field, enter the BRM user's password.

   c. In the Host Name field, enter 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.

   d. In the Port Number field, enter the TCP port number of the CM or CMMP on the host computer. The default value is 11960.

   e. In the Service Type field, enter the BRM service type. The default value is /servide/admin_client.

   f. In the Service POID Id field, enter the POID of the BRM service. The default value is 2.

   g. Do one of the following:

      If you have not enabled SSL for BRM, deselect the Use SSL? check box.

      If you have enabled SSL for BRM, leave the Use SSL? check box selected.

   h. In the Wallet Password field, enter the password for the Billing Care wallet.


i. In the **Confirm Wallet Password** field, enter the password for the Billing Care wallet again.

13. Click **Next**.
   
   The Authenticator and Asserter screen appears.

14. Enter the following information required to connect to the Oracle Unified Directory (OUD) authenticator, see Table 4-8 for more information:

   <Note>
   Select **Skip Authenticator and Asserter** if you are not using OUD.
   </Note>

   a. In the **Provider Name** field, enter the OUD Authentication provider you configured in your OPSS Administration Server.
   
b. In the **Host Name** field, enter the host name or IP address of the LDAP server.
   
c. In the **Port Number** field, enter the port number on which the LDAP server is listening.
   
d. In the **Admin User Name** field, enter the Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server.
   
e. In the **Admin Password** field, enter the credential (usually a password) used to connect to the LDAP server.
   
f. In the **User Base DN** field, enter the base distinguished name (DN) of the tree in the LDAP directory that contains users. For example:

   `cn=Users,dc=example,dc=com`

   g. In the **Group Base DN** field, enter the base distinguished name (DN) of the tree in the LDAP directory that contains groups. For example:

   `cn=Groups,dc=example,dc=com`

   h. In the **Asserter Name** field, 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.

15. Click **Next**.
   
   The Batch Payment Details screen appears.

16. Enter the following file locations used for processing batch payments:

   a. In the **Batch Payment Files Location** field, enter the directory where batch payment files are placed for uploading and processing by Billing Care. The installer creates unprocessed, processed, and failure folders in this directory for managing batch payment files.
   
b. In the **Batch Payment Templates Location** field, enter the directory where payment file templates are installed.

17. Click **Next**.
   
   The Auto Updates screen appears.

18. Select your Auto Updates preferences.

19. Click **Next**.
The Installation Summary screen appears.

20. Review your Billing Care installation summary and correct any errors.

21. Click **Install**.
   The Installation Progress screen appears.

22. When the Installation completes, Click **Next**.
   The Installation Complete screen appears. Make note of the Billing Care Links.

23. Click **Finish**.
   The Billing Care installer exits.

See "Billing Care Post-Installation 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**

The installation logs are used for debugging purposes. 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 installation and post-installations:

- `installAction TIMESTAMP.log`
- `oraInstall TIMESTAMP.err`
- `oraInstall TIMESTAMP.out`
- `dbScripts TIMESTAMP.log` (for the scripts executed using SQL*Plus and JDBC)
- `silentInstall TIMESTAMP.log` (for silent mode installation)

where `TIMESTAMP` is the date and time the log file was created.
Billing Care Post-Installation Tasks

This chapter provides instructions for Oracle Communications Billing Care post-installation tasks.

Post-Installation Tasks

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

• If your BRM installation uses Oracle Business Intelligence Publisher (BIP) to view invoices, encrypt and add the BIP credentials for accessing BIP in the `Infranet.properties` file on each domain host where Billing Care is deployed. See "Encrypting and Adding BIP Connection Information in the Wallet" for more information.

• 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" for more information.

  **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.

• If you are using Internet Explorer, configure the browser cache refresh setting to retrieve new data on each page visit. See "Configuring Internet Explorer for Billing Care" for more information.

For production installations:

• 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.

• 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 "Configure OPSS JRF-Enabled Domain LDAP Server Connection" for more information.
• If you are using Security Assertion Markup Language (SAML) for single sign-on (SSO), configure SAML. See "Configuring SAML for SSO" for more information.

About Encryption

Encrypting your BRM and BIP passwords and using SSL increases the security of your Billing Care deployment. See Oracle Communications Billing Care Security Guide for more information about securing your Billing Care environment.

Encrypting and Adding BIP Connection Information in the Wallet

You must configure the connection details for your BIP server in each domain server hosting a Billing Care deployment, if BIP 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 BIP 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 BIP user’s password.
   See "encrypt" in Oracle Fusion Middleware Command Reference for Oracle WebLogic Server for information on encrypting passwords.
3. Store the following information listed in Table 6-1 in the Billing Care wallet.
   See "Storing Configuration Entries for Billing Care" in BRM Security Guide for information on storing the BIP connection information in the Billing Care wallet.

Table 6-1 BIP Connection Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIP_USERID</td>
<td>BIP user with web access</td>
</tr>
<tr>
<td>BIP_PASSWORD</td>
<td>Encrypted BIP user’s password</td>
</tr>
<tr>
<td>BIP_URL</td>
<td>URL address to access BIP instance</td>
</tr>
</tbody>
</table>

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 the 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 by updating the entries 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 the sensitive information (such as BRM user password) only by using the Billing Care wallet.

See "Configuring the Connection Pool" in BRM System Administrator's Guide for more information on customizing the default connection pool.

See "Optional Entries in the Infranet.properties File" in BRM Developer's Guide for more information on 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 containing default policies, resource-types, resource, 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 following directory created during the Billing Care SDK installation:

Middleware_home/BillingCare_SDK/reference/AuthorizationDataModel

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. Change 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.

   ```xml
   <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 Oracle Platform Security Services (OPSS) schema.

   ```xml
   <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.url" value="jdbc:oracle:thin:@dbhost:dbport:SID"/>
   ```
Configure 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. Change to the `DOMAIN_HOME/config/fmwconfig/jps-config.xml` directory.
3. In the `<servicesInstances>` section of the `jps-config.xml` file, add the following identify store service entry containing your OUD server connection information. See Table 4-8 in "Billing Care Pre-Installation Tasks" for the list of required values from your OUD instance.

```
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
    <description>LDAP Identity Store Service Instance</description>
```

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 "Migrating From XML to Database" in 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.
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 a 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 step 3 above.

5. Save the file.

### Configuring Internet Explorer for Billing Care

Internet Explorer browser users must change the default cache configuration for Billing Care to properly refresh Billing Care data.

To configure Internet Explorer to refresh Billing Care data on each page visit in Internet Explorer, on each client where Internet Explorer is installed:

1. Open Internet Explorer.
2. Click the gear options menu.
3. Click **Internet Options**.

   The **Internet Options** window opens.

4. In the **General** tab, under **Browsing History**, click **Settings**.

   The **Website Data Settings** window opens.

5. In the **Temporary Internet Files** tab, select **Every time I visit the webpage** for the **Check for newer versions of stored pages** option.

6. Click **OK**.

   The **Website Data Settings** window closes.

7. Click **OK** to close the **Internet Options** window.
Enabling Logging

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

Configuring SAML for SSO

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.

To configure SAML for SSO, do the following:

1. Creating SAML Assertion Provider
2. Creating SAML Authenticator
3. Specifying General Information
4. Configuring the SAML Service Provider
5. Publishing the Service Provider Metadata
6. Updating the Deployment Plan of Billing Care

Creating SAML Assertion Provider

To create a SAML 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.
5. Click the Authentication subtab.
6. Click New.
   The Create a New Authentication Provider page appears.
7. In the Name field, enter samlBC.
8. From the Type list, select SAML2IdentityAsserter.
9. Click OK.
11. In the Authentication subtab, click samlBC link to view the settings for samlBC.
12. Click the Management tab.
   The Create a Web Single Sign-On Identity Provider Partner page appears.
14. In the Name field, enter WebSSO-IdP-Partner-1.
15. In the Path field, enter the path to the XML file that contains the identity provider’s metadata.

16. Click OK.

17. Click WebSSO-IdP-Partner-1 link.

18. Ensure that the identity provider details are displayed in the Site Info and Single Sign-On Signing Certificate tabs.

19. In the General tab, select the Enabled, Virtual User, and Process Attributes check box.

20. In the Redirect URIs field, enter /bc/*.

21. Click Save.

Creating SAML Authenticator

To create a SAML authenticator:

1. Log in to WebLogic Server Administration Console.

2. In the Domain Structure section, click the Security Realms link.

3. Click the myrealm link.

4. Click the Providers tab.

5. Click the Authentication subtab.

6. Click New.

7. In the Name field, enter samlBCAuth.

8. From the Type list, select SAMLAuthenticator.

9. Click OK.

10. Click the samlBCAuth link and modify the Control Flag to SUFFICIENT.

11. Click Save.

12. Click the DefaultAuthenticator link and modify the Control Flag to SUFFICIENT.

13. Click Save.

14. Reorder the providers in the following order:

   • samlBCAuth
   • samlBC
   • DefaultAuthenticator
   • DefaultIdentityAssertion

15. Click OK.

Specifying General Information

To specify the SAML general information:
1. Log in to WebLogic Server Administration Console.
2. In the Domain Structure section, click Environment > Servers > AdminServer.
3. In the Settings for AdminServer page, select Configuration > Federation Services > SAML 2.0 General.
4. In the Published Site URL field, enter http://billingcare_hostname:port/saml2.
   where:
   • billingcare_hostname is the Billing Care application host.
   • port is the port on which Billing Care is listening on.
5. In the Entity ID field, enter samlBC.
6. Click Save.

Configuring the SAML Service Provider

To configure the SAML service provider:
1. Log in to WebLogic Server Administration Console.
2. In the Domain Structure section, click Environment > Servers > AdminServer.
3. In the Settings for AdminServer page, select Configuration > Federation Services > SAML 2.0 Service Provider.
4. Select the Enabled checkbox.
5. Select POST from the Preferred Binding list.
   where:
   • billingcare_hostname is the Billing Care application host.
   • port is the port on which Billing Care is listening on.
7. Restart WebLogic Server.

Publishing the Service Provider Metadata

To publish the service provider metadata:
1. Log in to WebLogic Server Administration Console.
2. In the Domain Structure section, click Environment > Servers > AdminServer.
3. In the Settings for AdminServer page, select Configuration > Federation Services > SAML 2.0 General.
4. Click Publish Meta Data.
   The Publish SAML 2.0 Meta Data page appears.
5. In the Path field, enter the full path and filename of the metadata file. For example, C:\mydomain\myserver\sppmeta.xml.
6. Click OK.
Updating the Deployment Plan of Billing Care

To update the deployment plan of Billing Care:

1. Create an XML file with the deployment plan:

   ```xml
   <?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-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>
     </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 Control tab, select BillingCare in the Deployments table.
5. Click Update.
6. In the Update Application Assistant screen, select Redeploy this application using the following deployment files:
7. Click Change Path next to the Deployment plan path.
8. Enter or browse to the directory in which the XML file that you created is stored and click Next.
9. Click Finish.

Verifying SAML Configuration

To verify the SAML configuration:

   where:
   - `billingcare_hostname` is the Billing Care application host.
- *port* is the port on which Billing Care is listening on.
  The login page of the identity provider is displayed.

2. Enter the login credentials.
   The Billing Care home page appears.
Verifying the Billing Care Installation

You can 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 screen appears.
3. Ensure that all of the managed servers are running.
4. For successful REST API Deployment, **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 page 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.