Oracle® Communications Billing and Revenue Management

Business Operations Center Installation Guide



Release 16.26.0
G54443-01
October 2026

ORACLE

Oracle Communications Billing and Revenue Management Business Operations Center Installation Guide, Release 16.26.0

G54443-01

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

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

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

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

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

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

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

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

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

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

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

Contents

About This Content

1 Business Operations Center Installation Overview

About Installing Business Operations Center 1
Overview of the Business Operations Center Installation Steps 1
Ensuring a Successful Business Operations Center Installation 2

2 Planning Your Business Operations Center Installation

About Planning Your Business Operations Center Installation 1
About Test Installations and Production Installations 1
About Test Installations 1
About Production Installations 2
Database Planning 2
Authentication and Authorization Planning 2
About Installing a Secure System 3

3 Business Operations Center Requirements

Software Requirements 1
About IPv4 and IPv6 Support for Fusion Middleware Products 1

4 Business Operations Center Preinstallation Tasks

Connecting to Oracle BRM 1
Installing and Configuring Oracle Enterprise Database 2
Configuring SSL for the Oracle Enterprise Database 2
Downloading the JDBC Driver 2
Creating the Business Operations Center User 2
Installing and Configuring Oracle WebLogic Server 3
Configuring the OPSS JRF-Enabled Business Operations Center Application Domain 4
Installing and Configuring Oracle Unified Directory 4
Installing and Configuring Oracle Access Management 4

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

Configuring the Oracle Access Manager Business Operations Center Application Domain 5
Creating the Business Operations Center Application Domain 5
Configuring and Restarting the Oracle HTTP Server 6
Installing and Configuring Oracle Identity Governance 6

5 Installing Business Operations Center

Downloading the Business Operations Center Installer 1
Installing Business Operations Center for Testing 1
Installing Business Operations Center for Production 6
About Installation Logs 11

6 Business Operations Center Postinstallation Tasks

Enabling Logging 1
Configuring Additional Settings in Infranet.properties 2
Creating the Business Operations Center WebLogic Server Data Source 3
Configuring the SSL-Enabled Business Operations Center Data Source 4
Importing the Business Operations Center Security Policies into OPSS 5
Configuring SAML for SSO 7
Creating a SAML2 Assertion Provider 7
Creating a SAML2 Web Single Sign-On Identity Provider Partner 8
Creating a SAML2 Authenticator 8
Configuring SAML2 on the Administration Server 9
Configuring the SP metadata.xml file for the Identity Provider 10
Updating the Deployment Plans for Business Operations Center 10

7 Verifying the Business Operations Center Installation

8 Upgrading Business Operations Center

About Upgrading Business Operations Center 1
Upgrading Business Operations Center 1
Upgrading Your Business Operations Center Database Schema Manually 4

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

About This Content

This guide provides instructions for installing Oracle Communications Billing and Revenue Management Business Operations Center.

Audience

This guide is intended for system administrators, database administrators, and developers who install and configure Business Operations Center. Business Operations Center requires Oracle Database, Oracle WebLogic Server, and Oracle Identity Management Suite products in production environments. Additionally, Business Operations Center requires Billing and Revenue Management Revenue Assurance Manager, an optional component, to be installed in your Billing and Revenue Management environment.

See the documentation for those products for additional installation and configuration instructions.

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

1

Business Operations Center Installation Overview

Learn about the Oracle Communications Billing and Revenue Management (BRM) Business Operations Center installation process.

Topics in this document:

- About Installing Business Operations Center
- Overview of the Business Operations Center Installation Steps
- Ensuring a Successful Business Operations Center Installation

About Installing Business Operations Center

Business Operations Center 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 Communications Billing and Revenue Management (BRM)
  - BRM Revenue Assurance Manager
- Oracle WebLogic Server
- Oracle Enterprise Database
- (Optional) Oracle Identity Management (IDM) components, including:
  - Oracle Access Management (OAM)
  - Oracle Identity Governance
  - Oracle Unified Directory

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

The Business Operations Center installer creates the required schema in the BRM database and deploys Business Operations Center to a WebLogic server domain.

Overview of the Business Operations Center Installation Steps

The high-level tasks for installing Business Operations Center include:

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

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

> **Note**
>
> You can install a test or development installation of Business Operations Center without IDM. Do not use these installations in production environments. See "About Test Installations and Production Installations".

- Assessing how many physical computers you need and which software components to install on which computers.
- Planning the system topology (for example, determining whether you want a standalone deployment or a clustered deployment).

2. Reviewing system requirements, which includes:
   - 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, and the following required Oracle software:
     - Enterprise Database
     - WebLogic Server
     - (Optional) IDM components, such as:

       Oracle Access Management (OAM)

       Oracle Identity Governance

       Oracle Unified Directory
     - Java Development Kit (JDK)

     See "Business Operations Center Software Compatibility" in *BRM Compatibility Matrix* for required versions.
   - Information requirements, such as IP addresses, host names, and port numbers
   - BRM Server including installation of Revenue Assurance Manager

     See "Installing Revenue Assurance Manager" in *BRM Collecting Revenue Assurance Data*.
3. Preparing your foundation by completing the preinstallation tasks.

   See "Business Operations Center Preinstallation Tasks".
4. Installing Business Operations Center using the Oracle Universal Installer (OUI).

   See "Installing Business Operations Center".
5. Performing the required postinstallation configuration tasks.

   See "Business Operations Center Postinstallation Tasks".
6. Verifying the installation.

   See "Verifying the Business Operations Center Installation".

Ensuring a Successful Business Operations Center Installation

Business Operations Center uses additional Oracle software products, such as Enterprise Database, WebLogic Server, and IDM (optional). Familiarize yourself with these products and their installation procedures before installing Business Operations Center.

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

> **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 Business Operations Center installer so that your installation is successful.
>
> See *Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management* for detailed information.

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

To ensure that the Business Operations Center installation is successful, follow these guidelines:

- As you install each component (for example, the Enterprise Database and WebLogic Server), verify that the component is 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.

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

2

Planning Your Business Operations Center Installation

Learn how to plan your Oracle Communications Billing and Revenue Management (BRM) Business Operations Center installation.

Topics in this document:

- About Planning Your Business Operations Center Installation
- About Test Installations and Production Installations
- Database Planning
- Authentication and Authorization Planning
- About Installing a Secure System

About Planning Your Business Operations Center Installation

When planning a Business Operations Center installation, consider how many physical servers are required to support the Oracle WebLogic Server domains and Oracle Identity Management (IDM) components needed in your environment. High-availability requirements may increase the number of hosts.

Consider the security and networking requirements necessary for securing Business Operations Center communications with your BRM system in addition to software and hardware requirements.

See "Business Operations Center Requirements" and *BRM Compatibility Matrix* for information about required software. See "Business Operations Center Security" in *BRM Security Guide* for information about securing Business Operations Center.

About Test Installations and Production Installations

Install Business Operations Center either as a test or production installation depending on your required environment. Both test and production Business Operations Center installations must connect to a BRM system with Revenue Assurance Manager installed. See *BRM Collecting Revenue Assurance Data* for more information.

About Test Installations

Use test installations when setting up internal development or testing Business Operations Center instances. Test installations allow users to use Business Operations Center without IDM security. The deployed Business Operations Center 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

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

- WebLogic Server domain to host Business Operations Center with Business Operations Center security disabled
- Deployed Business Operations Center application WAR
- Creation of Business Operations Center schema in the BRM database

This guide includes information on installing test installations. You do not need to perform the IDM preinstallation steps for test installations. See "Installing Business Operations Center for Testing" for more information on test installations.

About Production Installations

Use production installations when setting up secure Business Operations Center instances using IDM security. Production installations require user authentication and authorization for securing access to Business Operations Center. 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 links 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
- Deployed Business Operations Center application WAR on each Oracle Platform Security Services (OPSS) domain
- Creation of the Business Operations Center schema in the BRM database
- (Optional) Oracle Identity Management (IDM) components, including:
  - Oracle Access Management (OAM) for single sign-on (SSO) configuration
  - Oracle Unified Directory for user directory management
  - Oracle Identity Governance for connecting to Oracle Unified Directory and managing users

Database Planning

Business Operations Center production installations require an Enterprise Database. This database is in addition to your BRM server database used for the Business Operations Center schema and OPSS schema. Database sizing requirements depend on the number of Business Operations Center users in your environment.

See "Installing and Configuring Oracle Enterprise Database" for information on setting up the required database for Business Operations Center.

Authentication and Authorization Planning

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

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

You can use the IDM components and Oracle HTTP Server Webgate for user authentication, SSO, and user directory management. See *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for more information on sizing and installation.

See *Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management* for more information about sizing your IDM host requirements.

About Installing a Secure System

In production environments, you must ensure that communication between components and access to the system servers are secure. The Business Operations Center installer prompts you to select security options. After you install Business Operations Center, enable SSL communication between Business Operations Center and BRM. For information about securing Business Operations Center, see "Business Operations Center Security" in *BRM Security Guide*.

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

3

Business Operations Center Requirements

Learn about the software requirements for the Oracle Communications Billing and Revenue Management (BRM) Business Operations Center software.

Topics in this document:

- Software Requirements
- About IPv4 and IPv6 Support for Fusion Middleware Products

Software Requirements

Business Operations Center is deployed on the Oracle Platform Security Services (OPSS) JRF-enabled WebLogic Server domain.

The following software is required for installing Business Operations Center:

- OPSS JRF-enabled WebLogic Server domain for deploying Business Operations Center.

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

- Oracle WebLogic Server installed using the Oracle Fusion Middleware Infrastructure installer.

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 for user directory management.
- Oracle Identity Governance for connecting to Oracle Unified Directory and managing users.

Business Operations Center is supported only on the software listed in these sections. You must install and connect all required software components for a secure installation.

For information about supported operating systems, additional software requirements, and compatible software versions, see *BRM Compatibility Matrix*.

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*.

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

4

Business Operations Center Preinstallation Tasks

Learn about the tasks that you must perform before running the Oracle Communications Billing and Revenue Management (BRM) Business Operations Center installer.

In production installations, the Business Operations Center installer deploys Business Operations Center 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 Business Operations Center consist of the following steps:

1. Connecting to Oracle BRM
2. Installing and Configuring Oracle Enterprise Database
3. Downloading the JDBC Driver
4. (Optional) Creating the Business Operations Center User
5. Installing and Configuring Oracle WebLogic Server
6. Configuring the OPSS JRF-Enabled Business Operations Center Application Domain
7. (Optional) Installing and Configuring Oracle Unified Directory
8. (Optional) Installing and Configuring Oracle Access Management
9. (Optional) Installing and Configuring Oracle Identity Governance

Connecting to Oracle BRM

Business Operations Center connects to BRM when retrieving operational data and submitting job requests. The connected BRM instance must have Revenue Assurance Manager installed. The Business Operations Center installer connects to the BRM database and creates the required schema.

See *BRM Installation Guide* for information on installing BRM.

See "Installing Revenue Assurance Manager" in *BRM Collecting Revenue Assurance Data* for more information.

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

Installing and Configuring Oracle Enterprise Database

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.

Configuring SSL for the Oracle Enterprise Database

You can configure secure sockets layer (SSL) for the Oracle Enterprise Database by creating the necessary wallets for storing certificates and then modifying the following configuration files to point to the appropriate wallet:

- **sqlnet.ora**
- **tnsnames.ora**
- **listener.ora**

You can use the **Orapki** utility to create the wallets.

Downloading the JDBC Driver

Download the JDBC driver file and save it in a directory on the machine on which you want to install BRM. Note the path to this directory; you are required to specify this path in the Specify Prerequisite Libraries Location window during the BRM installation. The correct file to download is:

- If you are using Oracle Database version 19, download the latest version of **ojdbc8.jar** for the version 19 database.
- If you are using Oracle Database version 23, download the latest version of **ojdbc11.jar** for the version 23 database.

You can download **ojdbc8.jar** or **ojdbc11.jar** from the following location:

https://www.oracle.com/database/technologies/appdev/jdbc-downloads.html

Creating the Business Operations Center User

The Business Operations Center installer provides the option to automatically create the Business Operations Center user for you. If you want the installer to create the user, you can skip this step.

If you want to create the user manually before you install Business Operations Center, do the following:

1. Log in to your database as user **sysdba**:

   ```
   sqlplus system/@databaseAlias as sysdba
   Enter password: password
   ```

   where:

   - *databaseAlias* is the Oracle system database alias.
   - *password* is the Oracle system database user password.

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

2. Create the default tablespaces for Business Operations Center:

```
SQL> CREATE TABLESPACE BOCtablespace DATAFILE 'BOCtablespaceDataFile' size
1000 M REUSE autoextend on next 50M extent management local;
SQL> CREATE TEMPORARY TABLESPACE BOCtempTablespace TEMPFILE
'BOCtempDataFile' size 1000 M REUSE autoextend on next 50M extent
management local;
```

   where:

   - *BOCtablespace* is the name of the data tablespace.
   - *BOCtablespaceDataFile* is the name and location of the data file for the data tablespace.
   - *BOCtempTablespace* is the name of the temporary tablespace.
   - *BOCtempDataFile* is the name and location of the data file for the temporary tablespace.

3. Create your Business Operations Center user:

```
SQL> CREATE BOCuser IDENTIFIED BY BOCpassword DEFAULT tablespace
BOCtablespace TEMPORARY tablespace BOCtempTablespace;
SQL> ALTER USER BOCuser quota unlimited ON BOCtablespace;
```

   where *BOCuser* is the name of your Business Operations Center user, and *BOCpassword* is the password for the Business Operations Center user.

4. Grant permissions to your Business Operations Center user:

```
SQL> GRANT CONNECT, RESOURCE TO BOCuser;
SQL> GRANT CREATE SEQUENCE TO BOCuser;
SQL> GRANT CREATE VIEW TO BOCuser;
SQL> GRANT CREATE TYPE TO BOCuser;
SQL> GRANT CREATE TRIGGER TO BOCuser;
SQL> GRANT CREATE ANY PROCEDURE TO BOCuser;
SQL> GRANT CREATE ANY TABLE TO BOCuser;
SQL> GRANT CREATE ANY CONTEXT TO BOCuser;
SQL> GRANT EXECUTE ANY TYPE TO BOCuser;
SQL> GRANT CREATE ANY JOB TO BOCuser;
SQL> GRANT MANAGE SCHEDULER TO BOCuser;
SQL> GRANT EXECUTE ON DBMS_SCHEDULER TO BOCuser;
SQL> GRANT SELECT ON DBA_USERS TO BOCuser;
SQL> GRANT SELECT ON DBA_SEGMENTS TO BOCuser;
SQL> GRANT CREATE SESSION TO BOCuser;
SQL> GRANT CREATE TABLE TO BOCuser;
SQL> GRANT EXECUTE ON SYS.DBMS_LOCK TO BOCuser;
SQL> GRANT EXECUTE ON dbms_crypto TO BOCuser;
```

Installing and Configuring Oracle WebLogic Server

Business Operations Center requires a preexisting Oracle WebLogic Server middleware home directory. You must download and install Oracle WebLogic Server using the Fusion Middleware Infrastructure installer.

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

If you are using Oracle Identity Management (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*.

Business Operations Center 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 Business Operations Center Application Domain

You deploy Business Operations Center 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 Business Operations Center application.

For information about creating the domain and configuring the domain policy, see "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*.

After installing Oracle Unified Directory, configure the OPSS Administration Server to use Oracle Unified Directory as the authentication provider. For information about:

- Setting up Oracle Unified Directory as your authentication provider, see "Configuring Authentication Providers" in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.
- Setting up Oracle Unified Directory, including how to synchronize Oracle Unified Directory with existing directories that you may already have, see "Introduction to Oracle Unified Directory" in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

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

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

Configuring the Oracle Access Manager Business Operations Center Application Domain

Create a Business Operations Center application domain in OAM and configure an application domain policy that controls access to the Business Operations Center application.

To create your Business Operations Center application domain in OAM, complete the following steps:

1. Creating the Business Operations Center Application Domain
2. 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 Business Operations Center Application Domain

Create the Business Operations Center application domain by following the instructions in "Creating a New Application Domain" in *Oracle Fusion Middleware Administering Oracle Access Management*.

As you create the application domain, ensure that you do the following:

1. Define the following resources for your Business Operations Center application domain:
   - The **/opsdashboard****, **/opsdashboard***, and **/**** resources:
     - Type: **HTTP**
     - Host Identifier: **IdMSuiteAgent**
     - Protection Level: **Protected**
     - Authentication Policy: **Protected Policy**
     - Resource URL (String): **/opsdashboard***, **/opsdashboard***, or **/****
   - The **/favicon.ico** resource:
     - Type: **HTTP**
     - Host Identifier: **IdMSuiteAgent**
     - Protection Level: **Excluded**
     - Resource URL (String): **/favicon.ico**

   For more information, see "Adding and Managing Policy Resource Definitions" in *Oracle Fusion Middleware Administering Oracle Access Management*.
2. Create an LDAP authentication module for authenticating Business Operations Center users. Set its user identity store to **OIMIDStore**.

   For more information, see "Managing Native Authentication Modules" in *Oracle Fusion Middleware Administering Oracle Access Management*.
3. Add the LDAP authentication module to an authentication scheme in your Business Operations Center application domain. The authentication scheme should include these values:
   - Authentication Level: **2**
   - Challenge Method: **Form**

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

- Challenge Redirect URL: **/oam/server**
- Challenge URL: **/pages/login.jsp**
- Context Type: **default**
- Context Value: **/oam**

For more information, see "Creating an Authentication Scheme" in *Oracle Fusion Middleware Administering Oracle Access Management*.

4. Create an authentication policy and then add the resources you created in step 1 and the authentication scheme you created in step 3 to it.

   For more information, see "Defining Authentication Policies for Specific Resources" in *Oracle Fusion Middleware Administering Oracle Access Management*.

5. Create an authorization policy and then add the resources you created in step 1 to it.

   For more information, see "Creating an Authorization Policy and Specific Resources" in *Oracle Fusion Middleware Administering Oracle Access Management*.

Configuring and Restarting the Oracle HTTP Server

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

To configure the **/opsdashboard** 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. Go 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. In the **idm.conf** file, append the following entry before the **</VirtualHost>** closing tag:

```
<Location /opsdashboard>
     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. Go 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
```

For more information about the OHS **idm.conf** file, see "Using the idm.conf File" in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

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:

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

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

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

5

Installing Business Operations Center

Learn how to install Oracle Communications Billing and Revenue Management (BRM) Business Operations Center using a GUI installer or a silent, command-line installer.

Topics in this document:

- Downloading the Business Operations Center Installer
- Installing Business Operations Center for Testing
- Installing Business Operations Center for Production
- About Installation Logs

Downloading the Business Operations Center Installer

You can download the Business Operations Center software from one of the following locations:

- For Business Operations Center 16.26.0.0 or any 16.26.0.*x* maintenance release: From the Oracle software delivery website (https://edelivery.oracle.com)
- For any 16.26.0.*x*.*y* patch set release: From the Oracle support website (https://support.oracle.com)

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

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

Installing Business Operations Center for Testing

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

To install a Business Operations Center test installation in a basic domain:

1. Verify that your Java Development Kit is installed correctly, including setting your **JAVA_HOME** environment variable and confirming that the *Java_home***/bin** directory is in your path.
2. Start the Oracle WebLogic Server basic domain administration server, managed server, or cluster on which you want to deploy Business Operations Center.
3. Run the following command, which launches the Business Operations Center installer:

   ```
   java -jar BusinessOperationsCenter_generic.jar
   ```


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

> **Note**
>
> - Specify the **-invPtrLoc** flag and an Oracle Inventory path location in the Java command for launching the Business Operations Center installer if you are using an existing or custom Oracle inventory location for maintaining your installed Oracle products and installation logs.
> - Business Operations Center requires postinstallation configuration of an Oracle WebLogic Server data source. By default, the installer uses the value **bocdb** for this data source's name. To use a custom data source name, specify the name by passing the following flag when launching the installer:
>
>   ```
>   DS_NAME="new_value"
>   ```
>
>   For example:
>
>   ```
>   java -jar BusinessOperationsCenter_generic.jar DS_NAME=''name''
>   ```
>
>   where *name* is the name of the WebLogic Server data source.
>
>   See "Creating the Business Operations Center WebLogic Server Data Source" for more information on configuring the WebLogic data source after installation completes.

4. In the Welcome window, click **Next**.
5. In the Installation Inventory window, select an **Inventory Directory** and **Operating System Group** and then click **Next**.
6. In the Installation Location window, enter or browse to your Oracle Home directory and then click **Next**.
7. In the Feature Sets Selection window, select **Business Operation Center Components** and then click **Next**.
8. In the Prerequisite Libraries Location window, enter the full path or browse to the directory in which the JDBC driver is located and then click **Next**. See "Downloading the JDBC Driver" for more information.
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 Business Operations Center, 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.

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

Table 5-1 (Cont.) WebLogic Server Details

Field	Description
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 Business Operations Center 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 Business Operations Center 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 Business Operations Center 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 Business Operations Center 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 Business Operations Center 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 Authentication and Asserter window, select **Skip Authenticator and Asserter**. A warning appears confirming that the Authenticator and Asserter will not be configured. Click **OK** and then click **Next**.
12. In the Database User Details window, enter the details in Table 5-2 and then click **Next**.

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

Table 5-2 Database User Details

Field	Description
Host Name	The IP address or the host name of the machine on which the BRM database is installed.
Port Number	The port number assigned to the BRM database. For example: **1521**.
Service Name	The database service name. For example: **orcl**.
User Name	The name of the Business Operations Center database user. For example: **boc**.
Password	The Business Operations Center user's password.
Confirm Password	Enter the Business Operations Center user's password again.
SSL Enabled	The type of connection required to connect to the database: • **Yes-One Way**: One-way SSL authentication is required. • **Yes-Two Way**: Two-way SSL authentication is required. • **No**: SSL authentication is not required.
Store Type	The type of TrustStore and KeyStore file that is used for the SSL connection: **SSO** or **PKCS12**.
Truststore Location	The directory in which your TrustStore file is located. This file is used for authentication through SSL.
Truststore Password	The password required to access the certificates from the TrustStore.
Keystore Location	The directory in which your KeyStore file is located. This file is used for authentication through SSL.
Keystore Password	The password required to access the certificates from the KeyStore.

The installer checks whether the Business Operations Center database user and Business Operations schema already exist, and then does one of the following:

- **If the user already exists but the schema does not**: The installer will create the Business Operations Center schema. Proceed to step 14.
- **If both the user and schema already exist**: The installer displays a warning. Click **OK** to have Business Operations Center reuse the existing schema. Proceed to step 14.
- **If the user does not exist**: The installer displays a warning. Click **OK** to have the installer create the user and schema for you. You will need to provide the database administrator credentials in the next window. Proceed to the next step.

13. In the Database Administrator Details window, enter the database administrator and tablespace details listed in Table 5-3.

Table 5-3 Database Administrator Details

Field	Description
User Name	The database administrator user name.
Password	The password for the database administrator user.
Role	The role of the database administrator user, such as **sysdba**.
Default Tablespace	The default tablespace for the Business Operations Center schema.
Temp Tablespace	The temporary tablespace for the Business Operations Center schema.

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

The installer checks whether the default and temp tablespaces already exist, and then does one of the following:

- If they do not exist, the installer displays a warning. Click **OK** to have the installer create the tablespaces for you.
- If they already exist, the installer uses the existing tablespaces.

14. In the User Interface Details window, enter the user details listed in Table 5-4 and then click **Next**.

Table 5-4 Business Operations Center User Interface Details

Field	Description
Billing Care URL	The URL of the Billing Care instance configured for use with your BRM Server if installed. Leave blank if Billing Care is not installed in your environment.
Logout URL	The redirect URL where Business Operations Center sends a user after logout and session termination.
Help URL	The URL of the Business Operations Center Online Help Guide located on the Oracle Help Center.
Timeout Warning Duration	The number of session idle seconds before Business Operations Center displays a timeout warning to a user (default value is 90 seconds).

15. 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.
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**.
SSL Wallet Location	The location of the SSL wallet to use for the BRM connection. You must enter a wallet location if you want Business Operations Center to communicate with BRM using SSL. If it is left empty, the SSL connection to BRM is disabled.
Wallet Password	The password for the Business Operations Center wallet.
Confirm Wallet Password	Enter the password for the Business Operations Center wallet again.

16. In the Web Services Details window, enter the details listed in Table 5-6 and then click **Next**.

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

Table 5-6 Business Operations Center Web Services Details

Field	Description
BRM Server Timezone	The Time Zone (TZ) value of the server operating system on which the BRM is running.

17. In the Auto Updates window, select an auto update option and then click **Next**.
18. In the Installation Summary window, confirm your installation selections and then click **Install**.

    The installation proceeds and runs postinstallation scripts to complete the Business Operations Center installation.

Installing Business Operations Center for Production

For production installations, run the Business Operations Center installer from the computer hosting the OPSS JRF-enabled domain on which you deploy Business Operations Center. The 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 Business Operations Center on your OPSS JRF-enabled domain:

1. Verify that your Java Development Kit is installed correctly, including setting your **JAVA_HOME** environment variable and confirming that the *Java_home***/bin** directory is in your path.
2. Start the Oracle WebLogic Server basic domain administration server, managed server, or cluster on which you want to deploy Business Operations Center.
3. Run the following command, which launches the Business Operations Center installer:

   ```
   java -jar BusinessOperationsCenter_generic.jar
   ```

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

4. In the Welcome window, click **Next**.
5. In the Installation Inventory window, select an **Inventory Directory** and **Operating System Group**, and then click **Next**.
6. In the Installation Location window, enter or browse to your Oracle Home directory path and then click **Next**.
7. In the Features Sets Selection window, select **Business Operation Center Components** and then click **Next**.
8. In the Prerequisite Libraries Location window, enter the full path or browse to the directory in which the JDBC driver is located and then click **Next**. See "Downloading the JDBC Driver" for more information.

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

9. In the WebLogic Server Details window, enter the details listed in Table 5-7 for the WebLogic Server domain in which you want to deploy Business Operations Center. Click **Next**.

Table 5-7 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. Select the check box for production installations.
KeyStore Type	The type of KeyStore file that is used for the SSL connection: **JKS** or **PKCS12**.
Keystore Location	The directory in which your KeyStore file is located. This file is used for authentication through SSL.
Keystore Password	The password required to access the certificates from the KeyStore.

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

10. Enter the required SSL information and then click **Next**.

    Business Operations Center 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*.

    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 about using the Java **keytool** to generate a key pair and root certificate for your encrypted password and to store the certificate, see: https://docs.oracle.com/en/java/javase/21/docs/specs/man/keytool.html.

    See "Configuring SSL" in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server* for more information about using SSL in your domain.

11. In the Target Server window, select the server on which to deploy Business Operations Center 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

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

- 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 Business Operations Center 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 Business Operations Center 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 Business Operations Center 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.

12. In the Authenticator and Asserter window, do one of the following and then click **Next**.
    - If you are not using Oracle Unified Directory, select **Skip Authenticator and Asserter**. A warning appears confirming that the Authenticator and Asserter will not be configured. Click **OK**.
    - Enter the information listed in Table 5-8 for connecting to the Oracle Unified Directory authenticator.

Table 5-8 Authentication and Asserter Details

Field	Description
Provider Name	Oracle Unified Directory Authentication provider you configured in your OPSS JRF-enabled domain administration server.
Host Name	Host name or IP address of the LDAP server.
Port Number	Port number on which the LDAP server is listening.
Admin User Name	Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server.
Admin Password	Credential (usually a password) used to connect to the LDAP server.
User Base DN	Base distinguished name (DN) of the tree in the LDAP directory that contains users. For example: `cn=Users,dc=example,dc=com`

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

Table 5-8 (Cont.) Authentication and Asserter Details

Field	Description
Group Base DN	Base distinguished name (DN) of the tree in the LDAP directory that contains groups. For example: `cn=Groups,dc=example,dc=com`
Asserter Name	Name to use during Business Operations Center deployment. A new asserter is created if a **OAMIdentityAsserter** type does not exist in your OPSS JRF-enabled domain already.

13. In the Database User Details window, enter the details in Table 5-9 and then click **Next**.

Table 5-9 Database User Details

Field	Description
Host Name	The IP address or the host name of the machine on which the BRM database is installed.
Port Number	The port number assigned to the BRM database. For example: **1521**.
Service Name	The database service name. For example: **orcl**.
User Name	The name of the Business Operations Center database user. For example: **boc**.
Password	The Business Operations Center user's password.
Confirm Password	Enter the Business Operations Center user's password again.
SSL Enabled	The type of connection required to connect to the database: • **Yes-One Way**: One-way SSL authentication is required. • **Yes-Two Way**: Two-way SSL authentication is required. • **No**: SSL authentication is not required.
Store Type	The type of TrustStore and KeyStore file that is used for the SSL connection: **SSO** or **PKCS12**.
Truststore Location	The directory in which your TrustStore file is located. This file is used for authentication through SSL.
Truststore Password	The password required to access the certificates from the TrustStore.
Keystore Location	The directory in which your KeyStore file is located. This file is used for authentication through SSL.
Keystore Password	The password required to access the certificates from the KeyStore.

The installer checks whether the Business Operations Center database user and Business Operations schema already exist, and then does one of the following:

- **If the user already exists but the schema does not**: The installer will create the Business Operations Center schema. Proceed to step 15.
- **If both the user and schema already exist**: The installer displays a warning. Click **OK** to have Business Operations Center reuse the existing schema. Proceed to step 15.
- **If the user does not exist**: The installer displays a warning. Click **OK** to have the installer create the user and schema for you. You will need to provide the database administrator credentials in the next window. Proceed to the next step.

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

14. In the Database Administrator Details window, enter the database administrator and tablespace details listed in Table 5-10.

Table 5-10 Database Administrator Details

Field	Description
User Name	The database administrator user name.
Password	The password for the database administrator user.
Role	The role of the database administrator user, such as **sysdba**.
Default Tablespace	The default tablespace for the Business Operations Center schema.
Temp Tablespace	The temporary tablespace for the Business Operations Center schema.

The installer checks whether the default and temp tablespaces already exist, and then does one of the following:

- If they do not exist, the installer displays a warning. Click **OK** to have the installer create the tablespaces for you.
- If they already exist, the installer uses the existing tablespaces.

15. In the User Interface Details window, enter the user details listed in Table 5-11 and then click **Next**.

Table 5-11 User Interface Details

Field	Description
Billing Care URL	URL of the Billing Care instance configured for use with your BRM Server if installed. Leave blank if Billing Care is not installed in your environment.
Logout URL	Redirect URL where Business Operations Center sends a user after logout and session termination.
Help URL	URL location of the Business Operations Center Online Help Guide located on the Oracle Help Center.
Timeout Warning Duration	Number of session idle seconds before Business Operations Center displays a timeout warning to a user (default value is 90 seconds).

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

Table 5-12 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.
Service Type	The BRM service type, such as **/service/admin_client**.
Service POID ID	The POID of the BRM service. The default value is **1**.

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

Table 5-12 (Cont.) BRM Connection Details

Field	Description
SSL Wallet Location	The location of the SSL wallet to use for the BRM connection. You must enter a wallet location if you want Business Operations Center to communicate with BRM using SSL. If it is left empty, the SSL connection to BRM is disabled.
Wallet Password	The password for the BOC wallet.
Confirm Wallet Password	Enter the password for the BOC wallet again.

17. In the Web Services Details window, enter the details listed in Table 5-13 and then click **Next**.

Table 5-13 Web Services Details

Field	Description
BRM Server Timezone	Time Zone (TZ) value of the server operating system on which the BRM is running.

18. In the Installation Summary window, confirm your installation selections and then click **Install**.

    The installation proceeds and runs post install scripts to complete the Business Operations Center installation.

19. Click **Finish** to complete the installation.

See "Business Operations Center Postinstallation Tasks" for required tasks to complete after the Business Operations Center installer exits.

See "Verifying the Business Operations Center Installation" for information on verifying the successful installation of Business Operations Center.

See "About Installation Logs" for information on the Business Operations Center 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 the installation and postinstallation process:

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

where *TimeStamp* is the date and time the log file was created.

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

6

Business Operations Center Postinstallation Tasks

Learn how to perform postinstallation tasks, such as enabling encryption and logging, after installing the Oracle Communications Billing and Revenue Management (BRM) Business Operations Center software.

After installing Business Operations Center, complete the following steps on each domain host where it is deployed:

1. Enable logging. See "Enabling Logging".
2. Adjust your BRM connection pool settings and configure logging for your Business Operations Center environment. See "Configuring Additional Settings in Infranet.properties".
3. Create an Oracle WebLogic Server data source for use with Business Operations Center. See "Creating the Business Operations Center WebLogic Server Data Source".
4. If you are setting up a test installation, perform the following additional steps:
   a. Create the following Business Operations Center groups in Oracle WebLogic Server and add Business Operations Center users to these groups:
      - **BOC_ADMIN**
      - **BOC_FINANCE**

      For more information about creating groups and adding the users in Oracle WebLogic Server, see "Users and Groups" in *Oracle WebLogic Remote Console Online Help*.
   b. If you want to enable **pin_virtual_time** in BRM and use virtual time when running Business Operations Center jobs, set the **ENABLE_PVT_TEST** property to **true** in the *Domain_home***/lib/bocws-config.properties** file. Then, restart your domain for the configuration change to take effect.
5. If you are setting up a production installation, also do the following:
   - Import the Business Operations Center Oracle Platform Security Services (OPSS) Administration Server policy configuration. See "Importing the Business Operations Center Security Policies into OPSS".
   - If you are using Security Assertion Markup Language (SAML) for single sign-on (SSO), configure SAML. See "Configuring SAML for SSO".

Enabling Logging

Business Operations Center writes log messages using the Log4j library. See *Oracle Fusion Middleware Configuring Log Files and Filtering Log Messages for Oracle WebLogic Server* for more information on enabling Business Operations Center logging.

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

Configuring Additional Settings in Infranet.properties

Business Operations Center uses the default connection pool settings for your BRM instance. You can customize the connection pool settings or configure logging by adding entries to the application's **Infranet.properties** file.

> **Note**
>
> You can update the connection details in the **Infranet.properties** file or in the Business Operations Center wallet. It is recommended to update sensitive information (such as the BRM user password) only by using the Business Operations Center wallet.

To customize the connection pool and logging settings, do the following:

1. Open the Business Operations Center **Infranet.properties** file in a text editor.

   > **Note**
   >
   > - During installation, the **Infranet.properties** file is copied to the *Oracle_home***/setup** directory, and this path will be added to the **INFRANET_PROPERTIES_FILE_LOCATION** property in the *Domain_home***/lib/bocws-config.properties** file. You can update the **Infranet.properties** file in this location.
   > - The **Infranet.properties** file is copied to the *Domain_home* directory, and this path will be added to the **INFRANET_PROPERTIES_FILE_LOCATION** property in the *Domain_home***/lib/bocws-config.properties** file.

2. Edit the connection pool entries in Table 6-1.

Table 6-1 Configurable Connection Pool Properties

Parameter	Description
infranet.connectionpool.maxsize	The maximum number of connections the connection pool maintains.
infranet.connectionpool.minsize	The minimum number of connections the connection pool maintains. **Note:** When you first start the connection pool, it may have fewer connections than the *minsize* value. When the *minsize* number of connections is reached, the number of connections will not fall below this count.
infranet.connectionpool.timeout	The time *in milliseconds* that a connection request will wait in the pending request queue for a free connection before it times out. If a pending request doesn't receive a connection during this time, an exception is thrown.

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

Table 6-1 (Cont.) Configurable Connection Pool Properties

Parameter	Description
infranet.connectionpool.maxidletime	The time *in milliseconds* that an idle (unused) connection remains in the connection pool before it is removed. **Important:** If the value is set too low, connections might be removed and restored too frequently. This can degrade system performance.

3. Configure the logging entries in Table 6-2.

Table 6-2 Optional Entries in Infranet.properties

Entry	Description
Infranet.log.file	The file path. The default value is **javapcm.log**.
Infranet.log.logallebuf	Boolean. If **true**, forces all **EbufException** exceptions to be logged automatically.
Infranet.log.level	Specifies how much information the application should log: • **0**: No logging • **1**: Log ERROR messages • **2**: Log ERROR and WARNING messages • **3**: Log ERROR, WARNING, and DEBUG messages
Infranet.pcp.debug.enabled	Boolean. If **true**, enables debug mode.
Infranet.pcp.debug.flags	Specifies what to log: • **0**: Log nothing • **1**: Log errors only • **0x1fff**: Log all messages
Infranet.log.opcodes.enabled	Boolean. If **true**, enables a log that records the input and output flist for every opcode called by all client applications that support this feature.
Infranet.log.opcodes.file	The file path.

4. Save and close the file.

Creating the Business Operations Center WebLogic Server Data Source

Configure a JDBC data source in the Business Operations Center WebLogic Server domain. The deployed Business Operations Center application uses this data source to connect to the database schema created by the installer.

By default, Business Operations Center uses a value of **bocdb** for the WebLogic Server data source. If you did not specify a custom name for your Business Operations Center database when launching the installer, create a data source named **bocdb** using the WebLogic Remote Console. See "Configuring WebLogic JDBC Resources" in *Oracle Fusion Middleware Administering JDBC Data Sources for Oracle WebLogic Server* for information on creating the required data source for Business Operations Center.

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

If you specified a custom name for your Business Operations Center database schema during installation, create the WebLogic Server data source using that name. Additionally, you must edit the **quartz.properties** file with your data source's name.

To edit the **quartz.properties** file data source name:

1. Open the *Domain_home*/**lib/quartz.properties** file where *Domain_home* is the WebLogic Server domain home directory of the domain in which Business Operations Center is deployed.
2. In the **DS_NAME** parameter, change the value to your custom data source name.
3. Save the file.
4. Restart the domain.

Configuring the SSL-Enabled Business Operations Center Data Source

You can configure a Secure Sockets Layer (SSL)-enabled JDBC data source in the Business Operations Center WebLogic Server domain for secured communications.

To configure the data source:

1. Create a truststore and then add the root certificate (which you created while configuring SSL for the Oracle database) as a trusted certificate to the truststore.
2. Log in to WebLogic Remote Console.
3. Click **Edit Tree**, then **Services**, and then **Data Sources**.

   A page with information about JDBC data source objects appears.
4. Select the Business Operations Center WebLogic Server Data Source for which you want to enable SSL. The default data source is for Business Operations Center **bocdb**.
5. Click the **Connection Pool** tab.
6. In the **General** tab, modify the **Url** field:

   ```
   jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST = hostname)
   (PORT = ssl-port))(CONNECT_DATA=(SERVICE_NAME=SID)))
   ```

   Where:

   - *hostname* is the name of the machine on which the Oracle database is installed.
   - *ssl-port* is the SSL-enabled port used for connecting to the Oracle database.
   - *SID* is the unique name of the Oracle database.
7. Click **Save**.
8. Click the same data source in the tree in the left pane.
9. Click **Properties** under the data source you are updating in the tree in the left pane.
10. For each of the properties in Table 6-3, perform the following steps. Note that some properties are only necessary if you require client authentication (two-way authentication):

    Perform the following steps for each property:

    a. Click **New**.
    b. In the **Name** field, enter the property name.
    c. Click **Create**.

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

A window that allows you to add a value to the new property appears.

d. In the **Value** field, enter the value as described in Table 6-3 for the specific property you want to add.

e. Click **Save**.

Table 6-3 Data Source Connection Properties

Property Name	Value Description
javax.net.ssl.keyStore	(For client/two-way authentication only) Path to the client-side KeyStore file generated from the exported public certificate using the **keytool** utility.
javax.net.ssl.keyStoreType	(For two-way authentication only) **JKS**
javax.net.ssl.keyStorePassword	(For two-way authentication only) Password of the KeyStore.
javax.net.ssl.trustStoreType	Path to the directory in which the truststore created in step 1 is stored.
javax.net.ssl.trustStoreType	**JKS**
javax.net.ssl.trustStorePassword	Password of the truststore.
oracle.jdbc.sendBooleanAsNativeBoolean **Note**: You only need to add this property if you are using the Oracle 23ai Database.	**false**

11. Click the shopping cart at the top right, and then click **Commit Changes** to commit your changes.
12. Restart the WebLogic Server domain.

    Your data source is now configured to use SSL.
13. Test and verify the connection.

See "SSL-Enabling a Data Source" in *Oracle Administering Oracle Fusion Middleware* for detailed information.

Importing the Business Operations Center Security Policies into OPSS

Business Operations Center includes the **system-jazn-data.xml** file, which contains default OPSS policies, resource-types, resource, and actions. You must import this file into your OPSS Administration Server to set up the initial Business Operations Center OPSS configuration. Complete this procedure once for each OPSS Administration Server.

The **system-jazn-data.xml** file is located in the *Domain_home***/lib/oes_config** directory, where *Domain_home* is the WebLogic domain home directory location of the OPSS JRF-enabled domain in which Business Operations Center is deployed.

To import 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 Business Operations Center.
2. Change to the *Domain_home***/lib/oes_config** directory.

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

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 Oracle Platform Security Services (OPSS) schema.

     > **Note**
     >
     > Add the last five **property name** entries (shown in bold) if you enabled one-way or two-way SSL authentication in Business Operations Center.

     ```
     <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"/>
        <property name="jdbc.driver"
     value="oracle.jdbc.driver.OracleDriver"/>
        <property name="security.principal" value="OPSS Schema
     Name(Ex:CC_OPSS)"/>
        <property name="security.credential" value="OPSSSchemaPassword"/>
        <property name="oracle.security.jps.ldap.root.name"
     value="cn=opssroot"/>
        <property name="oracle.security.jps.farm.name"
     value="cn=opssSecurityStore"/>
        <property name="jdk.tls.client.protocols" value="TLSv1.2"/>
        <property name="javax.net.ssl.trustStore" value="/scratch/ri-user-1/
     wallet/cwallet.sso"/>
        <property name="javax.net.ssl.trustStoreType" value="SSO"/>
        <property name="javax.net.ssl.keyStore" value="/scratch/ri-user-1/
     wallet/cwallet.sso"/>
        <property name="javax.net.ssl.keyStoreType" value="SSO"/>
     </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.

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

5. Run the **migrateSecurityStore** utility to import the Business Operations Center policy into your OPSS Administration Server.

See *Oracle Fusion Middleware Administrator's Guide* for detailed information on how to import files into your OPSS Administration Server.

Configuring SAML for SSO

You can use SAML 2.0 for enabling single sign-on (SSO) in Business Operations Center. SSO allows users to log in to applications using a single user name and password combination.

You can configure SAML authentication in a Business Operations Center domain using an Oracle Access Manager 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 web single sign-on identity provider partner. See "Creating a SAML2 Web Single Sign-On Identity Provider Partner"
3. Create a SAML2 authenticator. See "Creating a SAML2 Authenticator".
4. Configure SAML2 on the administration server. See "Configuring SAML2 on the Administration Server".
5. Configure a SP **metadata.xml** file for the identity provider. See "Configuring the SP metadata.xml file for the Identity Provider"
6. Create a SAML2 application in IDCS or Oracle Access Management.
7. Update your deployment plan to define the cookie name and path. See "Updating the Deployment Plans for Business Operations Center".
8. In your *Domain_home***/lib/bocws-config.properties** file, set the LOGOUT_URL parameter:

   ```
   LOGOUT_URL=IDP's Single logout URL
   ```

Creating a SAML2 Assertion Provider

To create a SAML2 assertion provider:

1. Log in to WebLogic Server Remote Console.
2. Click **Edit Tree**, then **Security**, and then **Realms**.

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

   The myrealm configuration page appears.
4. Click **Authentication Providers** in the tree in the left pane.

   A page with an Authentication Providers table appears.
5. Click **New**.

   The Create a New Authentication Provider page appears.
6. In the **Name** field, enter **samlBOCAsserter**.
7. From the **Type** list, select **SAML2IdentityAsserter**.

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

8. Click **Create**.
9. Restart WebLogic Server.

Creating a SAML2 Web Single Sign-On Identity Provider Partner

To create a SAML2 web single sign-on identity provider partner:

1. Log in to WebLogic Server Remote Console.
2. Click **Security Data Tree** and then **Realms**.

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

   The myrealm configuration page appears.
4. Click **Authentication Providers** in the tree in the left pane.

   A page with an Authentication Providers table appears.
5. In the table, select **samlBOCAsserter**.

   The configuration page for samlBOCAsserter appears.
6. Click **Partners** in the tree in the left pane.
7. Click **New**.

   The Create a new Identity Provider Partner page appears.
8. In the **Name** field, enter **WebSSO-IdP-Partner**.
9. From the **Type** list, select **Web Single Sign-On Identity Partner**.
10. In the **Meta Data File Name** field, enter the name and the path to the XML file that contains the identity provider's metadata.
11. Click **Create**.
12. Click **WebSSO-IdP-Partner** in the tree in the left pane.
13. Click the **General** tab.
14. In the **General** tab, turn on **Enabled**, **Virtual User**, and **Process Attributes**.
15. In the **Redirect URIs** Field, enter **/opsdashboard/***.
16. Click **Save**.

Creating a SAML2 Authenticator

To create a SAML2 authenticator:

1. Log in to WebLogic Server Remote Console.
2. Click **Edit Tree**, then **Security**, and then **Realms**.

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

   The myrealm configuration page appears.
4. Click **Authentication Providers** in the tree in the left pane.

   A page with an Authentication Providers table appears.
5. Click **New**.

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

6. In the **Name** field, enter **samlBOCAuthenticator**.
7. From the **Type** list, select **SAMLAuthenticator**.
8. From the **Control Flag** list, select **SUFFICIENT**.
9. Click **Create**.
10. In the Authentication Provider table, arrange the providers in the following order using the **Move Down** and **Move Up** buttons.
    - **Trust Service Identity Asserter**
    - **samlBOCAuthenticator**
    - **samlBOCAsserter**
    - **DefaultAuthenticator**
    - **DefaultIdentityAsserter**
11. Restart the Weblogic Server.

Configuring SAML2 on the Administration Server

To configure SAML2 on the Administration Server:

1. Log in to WebLogic Server Remote Console.
2. Click **Edit Tree**, then **Environment**, and then **Servers**.

   The Summary of Servers page appears.
3. In the Servers table, click the administration server.

   A page containing settings for the administration server appears.
4. Click the **Security** subtab, and then the **SAML 2.0 General** subtab.
5. In the **Published Site URL** field, enter **http://***BusinessOperationsCenter_hostname***:***port***/saml2**.

   where:
   - *BusinessOperationsCenter_hostname* is the Business Operations Center application host.
   - *port* is the port on which Business Operations Center is listening on.
6. In the **Entity ID** field, enter **samlBOCAsserter**.
7. Click **Save**.
8. Click the **SAML 2.0 Service Provider** subtab.
9. Turn on **Enabled**.
10. Turn on **POST Binding Enabled**.
11. From the **Preferred Binding** list, select **HTTP/POST**.
12. In the **Default URL** field, enter **http://***BusinessOperationsCenter_hostname***:***port***/opsdashboard**.

    where:
    - *BusinessOperationsCenter_hostname* is the Business Operations Center application host.
    - *port* is the port on which Business Operations Center is listening on.

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

13. Click **Save**.
14. Restart WebLogic Server.

Configuring the SP metadata.xml file for the Identity Provider

To configure SP **metadata.xml** file for identity provider:

1. Log in to WebLogic Server Remote Console.
2. Click **Monitoring Tree**, then **Environment**, and then **Servers**.

   The Summary of Servers page appears.
3. In the Servers table, click the administration server.

   A page containing settings for the administration server appears.
4. Click **SAML 2.0** subtab.
5. Click **Publish metadata**.
6. In the **File Name** field, enter the full path and the name of the file.
7. Click **Done**.

Updating the Deployment Plans for Business Operations Center

To update the deployment plans for Business Operations Center:

1. Merge the following contents with your existing Business Operations Center service and UI deployment plans:
   a. Merge the following contents with your existing Business Operations Center service 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>BusinessOperationCenter_Service</application-name>
    <variable-definition>
        <variable>
            <name>cookie-name</name>
            <value>JSESSIONID</value>
        </variable>
        <variable>
            <name>cookie-path</name>
            <value>/opsdashboard</value>
        </variable>
    </variable-definition>
    <module-override>
        <module-name>boc-service.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>
```


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

```
                <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>
```

b. Merge the following contents with your existing Business Operations Center UI 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>BusinessOperationCenter_UI</application-name>
    <variable-definition>
        <variable>
            <name>cookie-name</name>
            <value>JSESSIONID</value>
        </variable>
        <variable>
            <name>cookie-path</name>
            <value>/opsdashboard</value>
        </variable>
    </variable-definition>
    <module-override>
        <module-name>boc-ui.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>
```


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

```
    </module-override>
</deployment-plan>
```

> **Note**
>
> For SAML SSO, the **JSESSIONID** cookie must use the root path (/) for both the BOC UI and BOC Service applications. Do not retain an application-specific cookie path, such as **/opsdashboard**, in the deployment plan. Remove the **cookie-path** session-descriptor override so that WebLogic uses /, and then redeploy BOC.

2. Log in to WebLogic Server Remote Console.
3. Click **Monitoring Tree**, then **Deployments**, and then **Application Management**.

   A page with a list of installed Java EE applications and standalone application modules appears.
4. In the table, select **boc#1.0**.
5. Click **Update/Redeploy** and do one of the following:
   - If your updated deployment plan is located on the server containing WebLogic Server, select **Update Deployment Plan on Server** and enter the location of the file in the **Plan Path** field.
   - If your updated deployment plan is located on your local machine, select **Update Deployment Plan on Local Machine** and click Choose File to browse to the file or enter the file name in the **Plan** field.
6. Click **Done**.

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

7

Verifying the Business Operations Center Installation

Learn how to verify that Oracle Communications Billing and Revenue Management (BRM) Business Operations Center is installed by checking the state of all installed components or by logging in to Business Operations Center.

To check the state of all installed components:

1. Log in to the Administration Server managing your Business Operations Center Oracle Platform Security Services (OPSS) JRF-enabled domain servers.
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. If Business Operations Center is installed successfully, the Business Operations Center deployment appears in **Active** state.

To log in to Business Operations Center:

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

   The Business Operations Center 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 Business Operations Center home page appears, verifying that Business Operations Center is installed successfully.

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

8

Upgrading Business Operations Center

Learn how to upgrade your Oracle Communications Business Operations Center system.

See the following topics for more information about upgrading Business Operations Center:

- About Upgrading Business Operations Center
- Downloading the Business Operations Center Installer
- Upgrading Business Operations Center
- Upgrading Your Business Operations Center Database Schema Manually

About Upgrading Business Operations Center

The Business Operations Center installer allows you to do a full installation of the software or to do an upgrade of the software. The installer determines which one to perform based on the *Oracle_home* directory specified during the installation process. If you specify an empty *Oracle_home* directory, the installer automatically performs a full installation. If you specify an existing *Oracle_home* directory, the installer automatically performs an upgrade.

During the upgrade process, the Business Operations Center installer does the following:

- Replaces the existing Business Operations Center application WAR file that is deployed in your WebLogic application server with the latest version.
- Copies your existing **Infranet.properties** file and Oracle wallet to the *Domain_home* directory.
- Adds new entries to your Business Operations Center configuration files, such as **bocui-config.properties** and **bocws-config.properties**, retaining any custom values that were in the files.
- Updates your Business Operations Center wallet, retaining any custom values that were in it.
- Upgrades your Business Operations Center database schema to the latest release.

  The Business Operations Center installer can automatically upgrade the database schema for you, or you can choose to upgrade the database schema manually at a later time. See "Upgrading Your Business Operations Center Database Schema Manually".

Upgrading Business Operations Center

To upgrade to the latest Business Operations Center release:

1. Make a backup of your existing Business Operations Center installation. If the upgrade process fails, it does not roll back any changes that it made.
2. Ensure that you have upgraded Oracle Database Server to the latest supported version. For the list of supported versions, see *BRM Compatibility Matrix*.
3. Ensure that you have installed the appropriate new version of the Java Development Kit (JDK). For the list of supported versions, see *BRM Compatibility Matrix*.

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

Then, set your **JAVA_HOME** environment variable to the new version, and add the *Java_home***/bin** directory in your path.

4. Install the appropriate new version of Oracle WebLogic Server, ensuring that you are using the new version of Java. For the list of supported versions, see *BRM Compatibility Matrix*.
5. Upgrade your WebLogic Server domain. See Reconfiguring WebLogic Domains in *Upgrading Oracle WebLogic Server* for information.
6. Start the Oracle WebLogic Server domain administration server or the managed server on which Business Operations Center is deployed.
7. Run the following command, which launches the Business Operations Center installer:

   ```
   Java_home/bin/java -jar -invPtrLoc OracleInventoryPath
   BusinessOperationsCenter_generic.jar
   ```

   where:

   - *Java_home* is the directory in which you installed the latest compatible Java version.
   - *OracleInventoryPath* is the path to your *existing* Oracle Inventory location.
8. In the Welcome window, click **Next**.
9. In the Installation Location window, enter or browse to the location of your *existing* Oracle Home directory for Business Operations Center and then click **Next**.

   > ⚠ **Caution**
   >
   > If you enter a *new* Oracle Home directory, the installer does a full installation of Business Operations Center.

10. In the Features Set Selection window, select **Business Operation Center Components** and then click **Next**.
11. In the Prerequisite Libraries Location window, enter the full path or browse to the directory in which the JDBC driver is located and then click **Next**. See "Downloading the JDBC Driver" for more information.
12. In the WebLogic Server Details window, enter the details listed in Table 8-1 for the WebLogic Server domain in which Business Operations Center is already deployed and then click **Next**.

Table 8-1 WebLogic Server Details

Field	Description
Host Name	The IP address or the host 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 of the directory in which the WebLogic Server software is installed.
Use SSL?	Whether to use SSL (deselect for test installations).

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

Table 8-1 (Cont.) WebLogic Server Details

Field	Description
KeyStore Type	The type of TrustStore and KeyStore file that is used for the SSL connection: **JKS** or **PKCS12**.
Keystore Location	The directory in which your KeyStore file is located. This file is used for authentication through SSL.
Keystore Password	The password required to access the certificates from the KeyStore.

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

13. In the Database User Details window, enter the details listed in Table 8-2 and then click **Next**.

Table 8-2 Database User Details

Field	Description
Host Name	The IP address or the host name of the machine on which the BRM database is installed.
Port Number	The port number assigned to the BRM database. For example: **1521**.
Service Name	The database service name. For example: **orcl**.
User Name	The name of the Business Operations Center database user. For example: **boc**.
Password	The Business Operations Center user's password.
SSL Enabled	Select the type of connection required to connect to the database: • **Yes-One Way**: One-way SSL authentication is required. • **Yes-Two Way**: Two-way SSL authentication is required. • **No**: SSL authentication is not required.
Store Type	Select the type of TrustStore and KeyStore file that is used for the SSL connection: **SSO** or **PKCS12**.
Truststore Location	Enter or browse to the directory in which your TrustStore file is located. This file is used for authentication through SSL.
Truststore Password	Enter the password required to access the certificates from the TrustStore.
Keystore Location	Enter or browse to the directory in which your KeyStore file is located. This file is used for authentication through SSL.
Keystore Password	Enter the password required to access the certificates from the KeyStore.

14. In the BOC Schema Upgrade window, do one of the following and then click **Next**.
    - Deselect the **Skip Schema Upgrade** check box: The Business Operations Center installer upgrades the database schema for you. This is the default.

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

- Select the **Skip Schema Upgrade** check box: The Business Operations Center installer copies the database schema upgrade scripts to the *Oracle_home***/scripts/upgrade** directory so you can upgrade the schema later. See "Upgrading Your Business Operations Center Database Schema Manually".

15. In the Installation Summary window, confirm your installation selections and then click **Install**.
16. The Installation Progress window appears. When installation completes, click **Next**.

> **Note**
>
> After the installation begins, if you click **Stop installation**, the installation process stops, but the files that are already copied are not removed.

17. In the Installation Complete window, click **Finish** to complete the installation.

Upgrading Your Business Operations Center Database Schema Manually

If you chose to skip the automatic upgrade of your Business Operations Center database schema, the installer copied the upgrade scripts and a **README.txt** file that explains how to perform the upgrade to your *Oracle_home***/scripts/upgrade** directory.

To upgrade your Business Operations Center database schema manually, go to the *Oracle_home***/scripts/upgrade** directory and run this command:

```
Java_home/bin/java -cp .:OJDBC_path/OJDBC_file:Oracle_home/lib/BOCActions.jar
com.oracle.installer.boc.BOCActions upgrade DatabaseHost DatabasePort
ServiceName BOCSchemaUser BOCSchemaPassword Oracle_home
```

where:

- *Java_home* is the directory in which you installed the latest compatible Java version. See *BRM Compatibility Matrix*.
- *OJDBC_path* is the directory in which you installed the Oracle JDBC driver.
- *OJDBC_file* is the name of the Oracle JDBC driver file, either **ojdbc8.jar** or **ojdbc11.jar**. See "Downloading the JDBC Driver" for more information.
- *DatabaseHost* is the IP address or the host name of the machine on which the BRM database is installed.
- *DatabasePort* is the port number assigned to the BRM database.
- *ServiceName* is the database service name.
- *BOCSchemaUser* is the Business Operations Center database schema user name.
- *BOCSchemaPassword* is the password for the Business Operations Center database schema user.

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