16.1.3

Installation Guide (GlassFish)

December 2016

Trademarks	LINUX is a registered trademark of Linus Torvalds. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Open Service Catalog Manager is a registered trademark of FUJITSU LIMITED. Oracle, GlassFish, Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates. Apache Ant, Ant, and Apache are trademarks of The Apache Software Foundation. UNIX is a registered trademark of the Open Group in the United States and in other countries. VMware vSphere is a registered trademark of VMware in the United States and in other countries. Other company names and product names are trademarks or registered trademarks of their respective owners.

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, FUJITSU (or other affiliate's name) shall not be liable against the Customer and/or any third party for any claims or damages arising in connection with the High Safety Required Use of the Product.

Export Restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Contents

About this Manual

This manual describes how to install and uninstall Open Service Catalog Manager (OSCM).

The manual is structured as follows:

Chapter	Description
Introduction on page 8	Provides an overview of OSCM, its architecture, and the distribution media.
Prerequisites and Preparation on page 11	Describes the prerequisites that must be fulfilled and the preparations you need to take before installing and deploying OSCM.
Installation on page 15	Describes how to install OSCM with the help of the utilities which are shipped with the software.
Update Installation on page 26	Describes how to update OSCM.
Uninstallation on page 31	Describes how to uninstall OSCM.
Application Server Resources on page 32	Describes the resources required for OSCM on the application server.
Configuration Settings on page 35	Describes the OSCM configuration settings.

Readers of this Manual

This manual is directed to operators who install and maintain OSCM in their environment.

It assumes that you are familiar with the following:

- Administration of the operating systems in use, including the adaption and execution of batch files or shell scripts.
- Java EE technology, particularly as to the deployment on application servers.
- Relational databases and their administration, in particular, the PostgreSQL database.
- OSCM concepts as explained in the *Overview* manual.
- Installation and administration of Web servers.
- Installation and administration of the GlassFish application server.

Notational Conventions

This manual uses the following notational conventions:

Add	The names of graphical user interface elements like menu options are shown in boldface.
`init`	System names, for example command names and text that is entered from the keyboard, are shown in Courier font.
`<variable>`	Variables for which values must be entered are enclosed in angle brackets.

`[option]`	Optional items, for example optional command parameters, are enclosed in square brackets.
`one | two`	Alternative entries are separated by a vertical bar.
`{one | two}`	Mandatory entries with alternatives are enclosed in curly brackets.

Abbreviations

This manual uses the following abbreviations:

API	Application Programming Interface
DBMS	Database Management System
EJB	Enterprise JavaBeans
IdP	SAML Identity Provider
JMS	Java Message Service
LDAP	Lightweight Directory Access Protocol
OSCM	Open Service Catalog Manager
PaaS	Platform as a Service
PSP	Payment Service Provider
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
STS	Security Token Service
WSDL	Web Services Description Language
WSIT	Web Services Interoperability Technologies

The term "Windows" is used to denote the different Microsoft Windows operating systems supported by OSCM. "UNIX" stands for the supported UNIX operating systems, "Linux" for the supported Linux systems.

Available Documentation

The following documentation on OSCM is available:

- *Overview:* A PDF manual introducing OSCM. It is written for everybody interested in OSCM and does not require any special knowledge.
- *Online Help:* Online help pages describing how to work with the administration portal of OSCM. The online help is intended for and available to everybody working with the administration portal.
- *Installation Guide (GlassFish):* A PDF manual describing how to install and uninstall OSCM. It is intended for operators who set up and maintain OSCM in their environment.
- *Operator's Guide:* A PDF manual for operators describing how to administrate and maintain OSCM.

- *Technology Provider's Guide:* A PDF manual for technology providers describing how to prepare applications for usage in a SaaS model and how to integrate them with OSCM.
- *Supplier's Guide:* A PDF manual for suppliers describing how to define and manage service offerings for applications that have been integrated with OSCM.
- *Reseller's Guide:* A PDF manual for resellers describing how to prepare, offer, and sell services defined by suppliers.
- *Broker's Guide:* A PDF manual for brokers describing how to support suppliers in establishing relationships to customers by offering their services on a marketplace.
- *Marketplace Owner's Guide:* A PDF manual for marketplace owners describing how to administrate and customize marketplaces in OSCM.
- *Developer's Guide:* A PDF manual for application developers describing the public Web services and application programming interfaces of OSCM and how to integrate applications and external systems with OSCM.
- *ServerView Resource Orchestrator Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual platforms and servers controlled by FUJITSU ServerView Resource Orchestrator through services in OSCM.
- *Amazon Web Services Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual servers controlled by the Amazon Elastic Compute Cloud Web service through services in OSCM.
- *OpenStack Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual systems controlled by OpenStack through services in OSCM.
- *VMware vSphere Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual machines provisioned on a VMware vSphere server through services in OSCM.
- Javadoc and YAML documentation for the public Web services and application programming interfaces of OSCM and additional resources and utilities for application developers.

1 Introduction

Open Service Catalog Manager (OSCM) is a set of services which provide all business-related functions and features required for turning on-premise applications and tools into "as a Service" (aaS) offerings and using them in the Cloud. This includes ready-to-use account and subscription management, online service provisioning, billing and payment services, and reporting facilities.

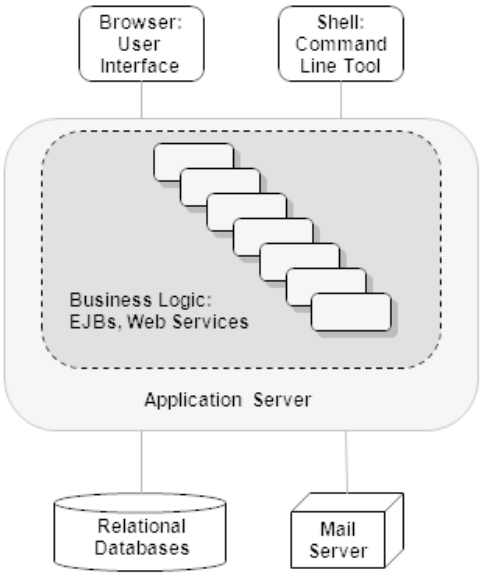
With its components, OSCM covers all the business-related aspects of a Platform as a Service (PaaS) or Cloud platform. It supports software vendors as well as their customers in leveraging the advantages of Cloud Computing.

OSCM is typically operated in data centers on servers providing for optimum performance, scalability, and non-stop operation. The applications integrated with OSCM and their data may be hosted in the same data centers as OSCM or in different locations.

1.1 OSCM Architecture

OSCM is implemented in Java, using Java Platform, Enterprise Edition (Java EE) technology. It is deployed on an application server supporting this technology.

The following figure provides an overview of the architecture:



OSCM has a three-tier architecture:

- The **presentation layer** in the application server's Web container includes the **user interface** (administration portal and marketplaces), realized as JavaServer Faces. Users access the user interface in Web browsers. In addition, OSCM provides a **command line tool**, which operators can install to carry out their tasks from a command shell instead of the administration portal.

- The **business logic** is implemented in Enterprise JavaBeans (EJB). Both the Enterprise JavaBeans and the **public Web services** are available in the application server's EJB container. The public Web services and their interfaces are mainly used for integrating applications and external systems with OSCM. However, they can also be employed for accessing OSCM functionality from a Web service client. HTTPS must be used for communication with the public Web services.
- OSCM **persists** its data through the Java Persistence API in **relational databases**.

For informing users about relevant issues (e.g. their registration or assignment to a subscription), OSCM must have access to a mail server.

1.2 Distribution Media

OSCM is distributed in the following packages:

- **Installation Package, `oscm-install-pack.zip`:**

  Contains the OSCM software and documentation for installation and deployment in a data center. The package includes:

  - **`databases/bes_db`** subdirectory:

    Configuration files for setting up the databases used by OSCM.

  - **`doc`** subdirectory:

    PDF manuals providing installation and operation instructions, an overview of OSCM, and information on new features and compatibility issues when upgrading a OSCM installation.

  - **`domains/bes_domain`** subdirectory:

    Configuration files for setting up the application server resources for the domain to which OSCM is to be deployed, as well as the archive files that make up OSCM.

  - **`domains/indexer_domain`** subdirectory:

    Configuration files for setting up the application server resources for the domain to which the search indexer application is to be deployed, as well as the archive file that makes up the search indexer application.

  - **`install`** subdirectory:

    XML files that support you in setting up the databases and application server resources for OSCM.

  - **`licences`** subdirectory:

    License files of third-party software used by OSCM.

  - **`oscm-operatorclient.zip`**: The command line tool.

  The subsequent chapters of this manual describe the installation and deployment in detail.

- **Integration Package, `oscm-integration-pack.zip`:**

  Contains the public Web services and application programming interfaces of OSCM, their documentation as well as additional resources, templates, samples, and utilities. Developers and technology providers can use this package for integrating applications and external systems with OSCM. This is described in detail in the *Technology Provider's Guide* and the *Developer's Guide*.

- **Payment Service Provider Integration Package, `oscm-integration-psp-pack.zip`:**

Contains the public Web service interface as well as additional resources and documentation for integrating a payment service provider (PSP) with OSCM.

- **Integration Package for Asynchronous Provisioning, `oscm-integration-app-pack.zip`:**
  Contains the asynchronous provisioning platform (APP) as well as samples and documentation. APP is a framework which provides a provisioning service, an operation service, as well as functions, data persistence, and notification features which are always required for integrating applications with OSCM in asynchronous mode.
- **ROR Integration Package, `oscm-ror-install-pack.zip`:**
  Contains all the components required for integrating FUJITSU ServerView Resource Orchestrator (ROR) with OSCM as well as the related documentation.
- **AWS Integration Package, `oscm-aws-install-pack.zip`:**
  Contains all the components required for integrating the Amazon Elastic Compute Cloud Web service with OSCM as well as the related documentation.
- **OpenStack Integration Package, `oscm-openstack-install-pack.zip`:**
  Contains all the components required for integrating OpenStack services with OSCM as well as the related documentation.
- **vSphere Integration Package, `oscm-vmware-install-pack.zip`:**
  Contains all the components required for integrating VMware vSphere with OSCM as well as the related documentation.

2 Prerequisites and Preparation

The following sections describe the prerequisites that must be fulfilled and the preparations you need to take before installing and deploying OSCM.

2.1 Hardware and Operating Systems

OSCM as a Java application does not rely on specific hardware or operating systems. It can be deployed on any platform supported by the application server and the database management system.

OSCM without any data requires about 150 MB of disk space.

Apart from this, OSCM does not have specific requirements as to the power, performance, capacity, or configuration of CPUs, memory, and disks. OSCM is usually deployed as part of a Cloud platform for which the most powerful and efficient hardware is used anyway.

2.2 Java and Ant

OSCM requires a Java Development Kit (JDK), version 7, 64 bit. Deployment with JDK 7, Update 45 has been tested and is recommended.

Due to a CORBA library change which is incompatible with Oracle GlassFish Server version 3.1.2.2, deployment with JDK 7, Update 55 and higher is not supported.

In order to be able to execute the installation scripts, you need to install the Apache Ant 1.8 (or higher) open source software. In the subsequent sections, `<ANT_HOME>` is the installation directory of Apache Ant.

2.3 Application Server

OSCM must be deployed on an application server compatible with Java EE version 6. The following application server is supported:

Oracle GlassFish Server, version 3.1.2.2.

Note:	Before installing GlassFish, make sure that the `JAVA_HOME` environment variable points to a Java Development Kit (JDK), version 7, 64 bit.

Proceed as follows:

1. Install the application server as described in its documentation, and configure it as required by your environment.

Note:	Make sure that the path of the GlassFish installation directory does not contain blanks.

2. After you have configured GlassFish, make a backup copy of the GlassFish installation.
3. Make sure that GlassFish is running in a JDK 7 environment. Also, make sure that no other applications (e.g. Tomcat) are running on your GlassFish ports.

OSCM requires two domains in the application server:

- One for the actual OSCM application (`bes-domain`).
- One for the search indexer application (`master-indexer-domain`). OSCM applies a master/slave search architecture: Every slave node delegates its index-related work to the master

node. The slave node is where the OSCM application runs; the master node is where the search indexer application runs.

Both domains can be created by running the OSCM installation scripts.

In the subsequent sections, `<GLASSFISH_HOME>` is the installation directory of GlassFish.

Note:	OSCM can be operated in a multi-node environment: You can install several OSCM domains communicating with one search indexer application domain. In this case, a load balancer must be configured for handling and distributing the load on the various nodes. In case you want to set up a multi-node environment, refer to the relevant documentation (application server, load balancer).

2.4 Relational Databases

OSCM stores its data in relational databases. The following database management system (DBMS) is supported:

PostgreSQL, version 9.1.12.

Install the DBMS as described in its documentation.

It is recommended that you use a separate machine for the OSCM databases.

Setup and Configuration

Edit the file

`<postgres_dir>/data/postgresql.conf`

as follows (`<postgres_dir>` is the PostgreSQL installation directory):

1. Set the `max_prepared_transactions` property value to `50`.
2. Set the `max_connections` property value to `210`.

   This property determines the maximum number of concurrent connections to the database server.

   Note the following: This setting is used in combination with the JDBC pool size settings for the domains on your application server. If you change the JDBC pool size, you might need to adapt the `max_connections` setting. Refer to the OSCM *Operator's Guide*, section *Tuning Performance*, for details.
3. Set the `listen_addresses` property value:

   Specify the IP addresses of all application servers on which the database server is to listen for connections from client applications. If you use the entry `'*'`, which corresponds to all available IP addresses, you must be aware of possible security holes.
4. Save the file.

If you use a server name in all configuration files instead of `localhost` during installation, edit the file

`<postgres_dir>/data/pg_hba.conf`

as follows (`<postgres_dir>` is the PostgreSQL installation directory):

1. Add the IP address of the application server that is to host the OSCM application.

   For example:

```
host all all 123.123.12.1/32 md5
```

Also add the application server's IPv6 address.

For example:

```
host all all fe80::cdfb:b6ed:9b38:cf17/128 md5
```

There are authentication methods other than `md5`. For details, refer to the PostgreSQL documentation.

2. Save the file.

Restart your PostgreSQL server for the changes to take effect.

2.5 Mail Server

To inform users about relevant issues (e.g. their registration or assignment to a subscription), OSCM requires a mail server in its environment. You can use any mail server that supports SMTP.

The settings for addressing the mail server are defined in the `glassfish.properties` file for the `bes-domain` domain of OSCM. Refer to *GlassFish Configuration Settings for the OSCM Domain* on page 36 for details.

2.6 Web Browsers

The OSCM user interface supports the following Web browsers:

- Google Chrome 42.0, 43.0
- Microsoft Internet Explorer 9.0, 10.0, or 11.0; Microsoft Edge
- Mozilla Firefox 31.0 - 38.0

Note: Using the administration portal of OSCM as well as marketplaces requires to have cookies enabled.

2.7 Authentication Mode

Before starting to install OSCM, you must decide on how users and Web services are to be authenticated.

The following sections explain the supported scenarios.

INTERNAL Authentication Mode

OSCM is installed as a platform for public access from anywhere in the Internet. Users are authenticated with OSCM and can be managed in OSCM or an existing LDAP system of an organization. Web service calls are authenticated in OSCM either by providing a user key or ID and a password in their header, or by certificates.

It is recommended to use the INTERNAL authentication mode if Web browser single sign-on is not required, and if your customers are to be able to register themselves.

SAML_SP Authentication Mode

OSCM is installed as a SAML 2.0 service provider. SAML (Security Assertion Markup Language) is an XML-based protocol that uses SAML assertions to pass information about a user between a SAML IdP and a SAML service provider (OSCM). With SAML 2.0, Web browser single sign-on within a company is provided.

All users and Web service calls are authenticated against the authentication system underlying the IdP, for example, OpenAM, Cloudminder, or Active Directory Federation Service (ADFS). The IdP provides a Web browser single sign-on profile (SSO profile) and a Security Token Service (STS). This is a Web service that issues security tokens as defined in the WS-Security/WS-Trust specification. A connection to the IdP is always established by the client (Web browser or Web service application), not by OSCM. The client sends a request for a SAML assertion. The IdP returns an assertion authenticating the calling user.

Single logout support can also be configured: When a user logs out of a OSCM marketplace or the administration portal, a `logout` request is sent to the single logout service of the IdP system and the sessions in OSCM and in the IdP system are invalidated. The user is directed to a Web page that depends on settings in the IdP system and in OSCM, and he can log in again.

The user data is managed in the IdP. Additionally, all users who are to work with OSCM must be registered explicitly in OSCM.

It is recommended to use the SAML_SP authentication mode if you want to operate OSCM in a company network and use existing authentication mechanisms that support the SAML 2.0 standard. Customer self-registration is not supported in this case, and should thus be disabled.

Required Information From the IdP

When using OSCM in SAML_SP mode, additional configuration settings in OSCM are necessary. For this, you require the following:

- A contractual relationship with the IdP operator so that the IdP can allow for Web browser SSO and secure of Web service calls using a Security Token Service (STS).
- Information on the following service endpoints. Ask the IdP operator for the following information:
  - For Web browser SSO: the SAML Redirect URL of the IdP as well as the URL of the single logout service endpoint.
  - For STS communication: STS service endpoint URL as well as the URL pointing to the MEX address (Issuer Metadata Exchange) of the STS.

  In a multi-tenancy environment and when several tenants are associated with one and the same IdP, one service endpoint per tenant must be defined and communicated.
- The entity ID of the IdP system. The IdP administrator can find out the ID by retrieving the federation metadata on his IdP system.
- Length of the encryption key used by the IdP.
- Information on whether the IdP can process `GET` or `POST` authentication requests.
- For Web browser SSO: the public key certificate from the IdP. Request this certificate from the IdP operator.

Required Information by the IdP

When using OSCM in SAML_SP mode, the administrator of the IdP system that is to be used for authenticating users requires the following information so that the IdP system can be configured correctly:

- A unique identifier for OSCM. The IdP uses this ID for identifying incoming authentication requests from OSCM.
- The unique identifier of the default tenant as specified when installing OSCM. You create this ID by specifying the corresponding configuration value in the configuration settings when installing the system.
- The OSCM signature verification certificate. The IdP system needs this certificate for handling logout requests.

3 Installation

The installation of OSCM consists of the following main steps:

1. Preparing the OSCM software and setup utilities. Refer to *Preparing the Software and Setup Utilities* on page 15.
2. Adapting configuration files. Refer to *Configuring OSCM* on page 16.
3. Setting up the databases. Refer to *Setting up the Databases* on page 18.
4. Setting up the resources in the application server and deploying the OSCM archives. Refer to *Setting up the Application Server Resources* on page 18.
5. Logging in to OSCM, creating users, and checking the configuration of OSCM. Refer to *Next Steps* on page 22.
6. When installing OSCM in SAML_SP authentication mode, additional steps are required. Refer to *Configuration Steps Required for IdP Communication* on page 24.

The descriptions in the subsequent sections assume that you are using the OSCM setup utilities for setting up the databases and the application server resources. This is the easiest way and suitable for most environments, particularly when you are using a database management system and application server installation solely for OSCM.

In specific situations, however, you may have to set up some or all of the resources manually. This is the case, for example, if you want to integrate the OSCM resources in an existing environment on an application server.

The resources required by OSCM on the application server are described in detail in *Application Server Resources* on page 32. Details of how to set up the resources properly can best be obtained from the XML files which are provided for the automated installation and described in the sections below.

3.1 Preparing the Software and Setup Utilities

The OSCM software and setup utilities are provided in the OSCM installation package, `oscm-install-pack.zip`. The contents of the installation package need to be made available in your environment as follows:

Extract the contents of the OSCM installation package, `oscm-install-pack.zip`, to a separate temporary directory on the system from where you want to install and deploy OSCM.

In the following sections, this directory is referred to as `<install_pack_dir>`.

After extraction, the following directories are available:

- **`databases/bes_db`**

  Configuration files for setting up the databases used by OSCM.

- **`doc`**

  PDF manuals providing installation and operation instructions, an overview of OSCM, and information on new features and compatibility issues when upgrading a OSCM installation.

- **`domains/bes_domain`**

  Configuration files for setting up the application server resources for the domain to which OSCM is to be deployed. The **`domains/bes_domain/applications`** subdirectory contains the archive files that make up OSCM:

  - `oscm.ear`: The OSCM platform.
  - `oscm-portal.war`: The OSCM administration portal and marketplace.

  - `oscm-portal-help.war`. The online help for the administration portal and the marketplaces.

- **`domains/indexer_domain`**

  Configuration files for setting up the application server resources for the domain to which the search indexer application (`oscm-search.ear`) is to be deployed. The **`domains/indexer_domain/applications`** subdirectory contains the `oscm-search.ear` file.

- **`install`**

  XML files that support you in setting up the databases and application server resources for OSCM.

- **`licenses`**

  License files of third-party software used by OSCM.

- **`oscm-operatorclient.zip`**: The command line tool.

Note: The `<install_pack_dir>/install` directory contains a properties file, `parallel-execution.properties`. Do not change the content of this file!

3.2 Configuring OSCM

The OSCM software and setup utilities require a number of settings. These settings are provided in the following subdirectories and files of `<install_pack_dir>`:

- **`databases/bes_db`**
  - `db.properties`: Settings for the database setup and access.
  - `configsettings.properties`: Configuration settings for the OSCM services.

    The initial installation stores these settings in the `bss` database, where you can change them later, if required. An update installation only adds new settings to the database but does not overwrite existing ones.

  - `sso.properties`: Configuration setting for creating the first platform operator in OSCM (`ADMIN_USER_ID`). Only required when installing OSCM in SAML_SP authentication mode.

- **`domains/bes_domain`**

  The configuration settings for setting up the application server domain to which the OSCM applications will be deployed are provided in the following files:
  - `glassfish.properties`: Configuration settings for the application server.
  - `glassfishJMSBroker.properties`: Configuration settings for the Java Message Service (JMS) in the application server.

- **`domains/indexer_domain`**

  The configuration settings for setting up the application server domain to which the search indexer application will be deployed are provided in the following files:
  - `glassfish.properties`: Configuration settings for the application server.
  - `glassfishJMSBroker.properties`: Configuration settings for the Java Message Service (JMS) in the application server.

Additional configuration files contained in other subdirectories are used internally and must not be changed.

You need to adapt the settings in the files above to your environment. In particular, server names, ports, paths, user IDs, and passwords require adaptation. If installed in SAML_SP authentication mode, additional settings are required.

Proceed as follows to view and adjust the configuration settings:

1. Open each of the configuration files listed above with an editor.
2. Check the settings in each file and adapt them to your environment.

   For details on the individual settings, refer to *Configuration Settings* on page 35.
3. Save the files to their original location in `<install_pack_dir>/<subdirectory>`. For future reference, it is a good idea to create a backup of the files.

Observe the following configuration issues:

- The specified ports are suggestions and work with the default settings used in the files.
- If you install everything on the local system, use either the server name or `localhost` in all configuration files for all URLs that need to be resolved by OSCM.

  Do not mix the specification of server names and `localhost`.

  The `BASE_URL_HTTPS` setting, and, if specified, the `BASE_URL` setting in the `configsettings.properties` file must be resolved by clients. They always require the specification of the server name.

  Specify the settings as follows:

```
BASE_URL_HTTPS=https://<host>:<port>/oscm-portal
BASE_URL_HTTP=http://<host>:<port>/oscm-portal
```

- On Windows, in the `glassfish.properties` files, double-escape the colon in the drive specification of the path to the search indexer application (`hibernate.search.shared.sourceBase`). Otherwise the search indexer application may not work properly. The directory you specify for the search indexer application is created automatically.

  Example:

```
hibernate.search.shared.sourceBase=
C\\:/glassfish/masterSourceBase
```

- The following settings in the `configsettings.properties` file are mandatory when installing OSCM in **SAML_SP** authentication mode:
  - `AUTH_MODE`
  - `SSO_DEFAULT_TENANT_ID`
  - `SSO_ISSUER_ID`
  - `SSO_IDP_URL`
  - `SSO_IDP_AUTHENTICATION_REQUEST_HTTP_METHOD`
  - `SSO_SAML_ASSERTION_ISSUER_ID`
  - `SSO_STS_URL`
  - `SSO_STS_METADATA_URL`
  - `SSO_STS_ENCKEY_LEN`
  - `SSO_IDP_TRUSTSTORE`
  - `SSO_IDP_TRUSTSTORE_PASSWORD`

3.3 Setting up the Databases

OSCM requires and stores its data in the following PostgreSQL databases:

- The OSCM database (`bss`). This database is used for the actual business data, as well as for resources and configuration settings, for example, timer data.
- The JMS database (`bssjms`). This database is used for storing JMS data.

The databases are created by executing installation scripts. They need to be initialized with the appropriate schema and settings.

Proceed as follows:

1. Make sure that the database server is running.
2. Open the command prompt (Windows) or a terminal session (UNIX/Linux).
3. Set the following environment variable for your current session:

   `DB_INTERPRETER`: The absolute path and name of the `psql` executable of PostgreSQL. The executable is usually located in the `bin` subdirectory of the PostgreSQL installation directory.

   Example (Unix/Linux):

   ```
   export DB_INTERPRETER="/opt/PostgreSQL/9.1/bin/psql"
   ```

   Example (Windows):

   ```
   set DB_INTERPRETER="C:\Program Files\PostgreSQL\9.1\bin\psql"
   ```

4. Create the OSCM databases by executing the `build-db.xml` file in `<install_pack_dir>/install` as follows:

   ```
   <ANT_HOME>/bin/ant -f build-db.xml initDB
   ```

   If you set a password other than `postgres` for the PostgreSQL user account (`postgres`) when installing the database management system, you have to specify the password with the call to the `build-db.xml` file as follows:

   ```
   <ANT_HOME>/bin/ant -f build-db.xml initDB
      -Ddb.admin.pwd=<password>
   ```

Note: It may be required to enclose the `-Ddb.admin.pwd=<password>` command in double or single quotes depending on the operating system.

If the setup of the databases fails with errors, proceed as follows:

1. Check and correct the configuration files.
2. Execute the `build-db.xml` file in `<install_pack_dir>/install` as follows:

   ```
   <ANT_HOME>/bin/ant -f build-db.xml DROP.dbsAndUsers
   ```

3. Repeat the setup.

3.4 Setting up the Application Server Resources

OSCM requires specific settings and resources in the application server, such as a data source and JMS queues. For details on the resources, refer to *Application Server Resources* on page 32.

Before starting to install OSCM, make sure that the application server ports you want to use are available. The GlassFish domain creation reserves some ports using the following rules based on the port base principle. For example, when using port base 8000:

Portbase + 48: admin port: `8048`

Portbase + 80: HTTP listener: `8080`

Portbase + 81: HTTP listener: `8081`

Portbase + 86: JMX port: `8086`

Portbase + 76: JMS broker port: `8076`

Portbase + 37: IIOP listener: `8037`

Portbase + 38: IIOP listener: `8038`

Portbase + 39: IIOP listener: `8039`

By default, the OSCM installation assumes the following ports:

`8048`: admin port of the OSCM domain.

`8448`: admin port of the search indexer application domain.

You can specify the port numbers in the `glassfish.properties` configuration files.

Proceed as follows to create the resources and make the required settings in the application server:

1. Open the command prompt (Windows) or a terminal session (UNIX/Linux).
2. Execute the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-glassfish.xml SETUP
```

Note: The `<install_pack_dir>/domains` directory contains a properties file, `InstallationOrder.properties`. Do not change the content of this file! The search indexer application domain must always be installed before the OSCM domain.

Results of the Build Script Execution

The execution of the `SETUP` target defined in the `build-glassfish.xml` file has the following results:

1. **Domains and resources**:
   - The `master-indexer-domain` domain is created and started.
   - The search indexer application (`oscm-search.ear`) is deployed to the `master-indexer-domain` domain.
   - The `bes-domain` domain is created and started.
   - The following applications are deployed to the `bes-domain` domain:

     `oscm.ear`

     `oscm-portal.war`

     `oscm-portal-help.war`
   - The `oscm-security.jar`, the `postgresql-9.1-903.jdbc4.jar`, and the `commons-codec-1.7.jar` files are copied from the directory to which you extracted the

OSCM installation package (`<install_pack_dir>/domains/bes_domain/lib`) to the `lib` directory of the `bes-domain` domain.

- The `javax.faces.jar` file is copied from the directory to which you extracted the OSCM installation package (`<install_pack_dir>/install/lib`) to the `<GLASSFISH_HOME>/modules` directory.
- The required resources, email settings, JMS queues, data sources are created in the application server. Refer to *Application Server Resources* on page 32 for details.
- The directory traversal is disabled for both domains, `bes-domain` and `master-indexer-domain`: The directory listing parameter is set to `false` in the `default-web.xml` file in the domain directories you are using for OSCM.

2. **JVM options set for the `master-indexer-domain` domain** during the installation:

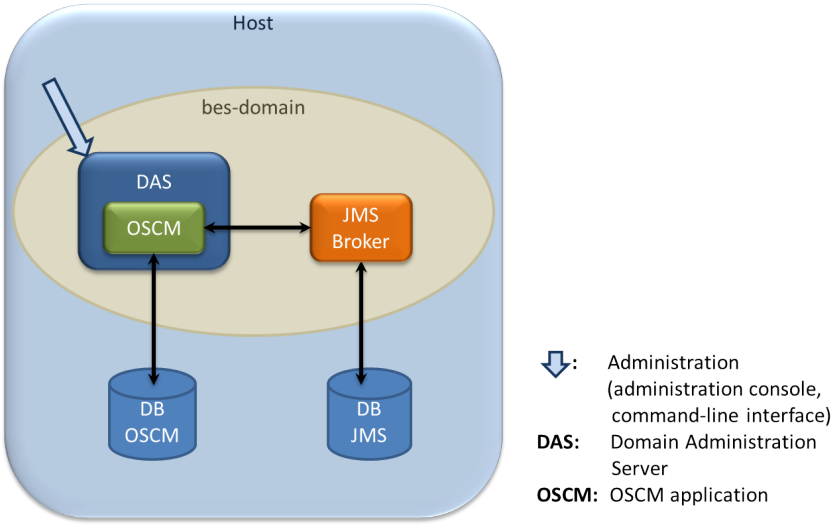
```
-Dfile.encoding=UTF8
-Duser.language=en
-Dorg.glassfish.jms.EagerStartup=true
-XX:MaxPermSize=512m
-Dhibernate.search.default.directory_provider=
   org.hibernate.search.store.impl.FSMasterDirectoryProvider
-Dhibernate.search.default.indexBase=${com.sun.aas.instanceRoot}/
   masterIndexBase
-Dhibernate.search.default.sourceBase=
${hibernate.search.shared.sourceBase}
-Dhibernate.search.default.refresh=${hibernate.search.default.refresh}
-Dorg.apache.catalina.loader.WebappClassLoader.
   ENABLE_CLEAR_REFERENCES=false
```

3. **JVM options set for the `bes-domain` domain** during the installation:

```
-Dfile.encoding=UTF8
-XX:MaxPermSize=512m
-Dsun.java2d.print.polling=false
-Dsun.net.inetaddr.ttl=3600
-Duser.language=en
-Dhibernate.search.default.directory_provider=
   org.hibernate.search.store.impl.FSSlaveDirectoryProvider
-Dhibernate.search.indexing_strategy=manual
-Dhibernate.search.default.indexBase=${com.sun.aas.instanceRoot}/
   slaveIndexBase
-Dhibernate.search.default.sourceBase=
${hibernate.search.shared.sourceBase}
-Dhibernate.search.default.refresh=${hibernate.search.default.refresh}
-Dorg.apache.catalina.loader.WebappClassLoader.
   ENABLE_CLEAR_REFERENCES=false
```

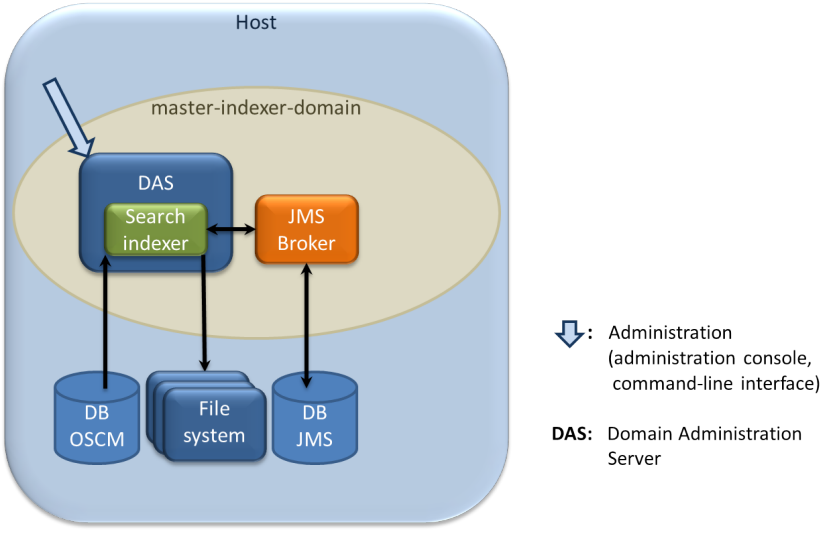
After a successful deployment, you have two domains with the following setup:

1. OSCM domain (`bes-domain`)



Host is the machine where your application server is installed. The `bes-domain` domain has a Domain Administration Server (DAS) which is used for domain administration and the hosting of the OSCM application. Configuration information and actual business data is stored in the OSCM database (`bss`). The JMS broker administers the JMS queues used for processing asynchronous tasks, such as the sending of emails, synchronization of indexing data, or execution of process triggers. The JMS messages are stored in the JMS database. The domain is administered using the standard administration facilities of the application server.

2. Search indexer application domain (`master-indexer-domain`)



Host is the machine where your application server is installed. The `master-indexer-domain` domain has a Domain Administration Server (DAS) which is used for domain administration and the hosting of the search indexer application. Data for indexing is read from the OSCM database

(bss) and written to a shared directory on the file system. This directory hosts the search index for the master indexer node. It is specified by the hibernate.search.shared.sourceBase configuration setting in the glassfish.properties files of both domains. The JMS broker administers the JMS queue used for processing indexing jobs. The JMS messages are stored in the JMS database. The domain is administered using the standard administration facilities of the application server.

If the setup of the application server resources fails with errors, proceed as follows:

1. Stop the application server domains related to OSCM.
2. Delete the bes-domain domain.
3. Delete the master-indexer-domain domain.
4. Delete the shared directory for the master search index.
5. Repeat the setup.

If you want to set up a single domain:

Add a parameter indicating which domain you want to set up, and execute the build-glassfish.xml file in <install_pack_dir>/install as follows:

For setting up the search indexer application domain:

```
<ANT_HOME>/bin/ant -Ddomain.setup=indexer_domain
   -f build-glassfish.xml SETUP
```

For setting up the OSCM domain:

```
<ANT_HOME>/bin/ant -Ddomain.setup=bes_domain
   -f build-glassfish.xml SETUP
```

Note: It may be required to enclose the -Ddomain.setup=<domain> command in double or single quotes depending on the operating system.

3.5 Next Steps

After you have successfully completed the installation of OSCM, you can deploy BIRT in order to enable reports and optionally change the URL to be used for accessing the OSCM administration portal and the marketplaces. You can then start to set up the OSCM organizations using the OSCM administration portal.

Deploying BIRT

OSCM uses BIRT to generate reports. BIRT is not included in the OSCM packages. To be able to generate reports, you need to obtain and manually deploy BIRT on your own.

Proceed as follows:

1. Download the latest version of Eclipse BIRT runtime, for example, from http://www.eclipse.org.
2. Deploy the birt.war archive to a domain on the application server which you use for OSCM. You can deploy the archive to the bes-domain domain of OSCM or a separate domain.
3. Add the OSCM report designs and localized labels to the folder of the birt application on the application server.

   The OSCM report designs and labels are available in the following archive provided for each release: oscm-reports.zip. Extract the contents of this archive to the root folder of the birt application, <GLASSFISH_HOME>/glassfish/domains/<domain>/applications/birt.

4. Restart `birt`.

Each time you install a new release of OSCM, you should also check for new releases of BIRT and changes in the OSCM report designs and labels and update them as required.

Setting the Context Root

By default, i.e. if you used the OSCM installation scripts, the context root of the URL used for accessing the OSCM administration portal and the marketplaces is `oscm-portal`. You can change this setting in the application server administration console. In addition, you need to adapt the `BASE_URL_HTTPS` configuration setting, and, if specified, the `BASE_URL` configuration setting, in OSCM.

1. In the application server administration console:
   1. Go to **Applications -> oscm-portal -> Edit** and set the **Context Root** as required.
   2. Go to **Applications -> oscm-portal-help -> Edit** and set the **Context Root** analogously to the one for `oscm-portal`.

      Example: If you set the context root for `oscm-portal` to `MyPortal`, set it to `MyPortal-help` for `oscm-portal-help`.

2. In the OSCM administration portal, go to **Operation -> Update Configuration Settings** and change the `BASE_URL_HTTPS` configuration key, and, if specified, the `BASE_URL` configuration key, accordingly. See below for details on accessing OSCM.

Accessing OSCM

You can access the OSCM administration portal in a Web browser using an URL in the following format:

`https://<server>:<port>/<context-root>` or

`http://<server>:<port>/<context-root>`

`<server>` is the host of the application server where OSCM has been deployed. `<port>` is the port to address the application server (default: `8080` for HTTP, `8081` for HTTPS). `<context-root>` is the context root of OSCM (default: `oscm-portal`).

You are prompted for a user ID and password.

Depending on the authentication mode, the initial credentials are the following:

- INTERNAL:

  User ID: `administrator`

  Password: `admin123`

  It is recommended that you change the initial password in the OSCM administration portal (**Change Password** page in the **Account** menu).

- SAML_SP:

  User ID: The ID you specified in the `ADMIN_USER_ID` configuration key in the `sso.properties` configuration file.

  Password: Password as known in the IdP for the above user.

Creating an Additional Operator Account

The creation of an additional operator account for your organization is useful, for example, to be able to delegate operational tasks or to unlock other operator accounts in case the password has been forgotten. Proceed as follows:

In the OSCM administration portal, choose **Register new users** in the **Account** menu. Enter the relevant user data and assign at least the **Operator** role.

Changing the OSCM Configuration

Refer to the *Operator's Guide* in case you need to change the configuration of your OSCM installation.

3.6 Configuration Steps Required for IdP Communication

After having successfully deployed OSCM in SAML_SP authentication mode, the following steps must be performed in the IdP and in OSCM:

1. The IdP operator must ensure that the correct endpoints for the Web UI SSO and STS connections are activated.
2. For STS, the IdP operator must create the relying party for OSCM in the IdP, and all OSCM users must be allowed to access this relying party. The URL of the relying party is usually the URL for accessing the OSCM administration portal.
3. For Web browser SSO, an SSO federation with the IdP must be established in a way that OSCM acts as the relying party.
4. OSCM must be registered with the IdP. One way to achieve this is to use OSCM metadata. The minimum data required are a name or ID of OSCM as a service provider (as specified in the `SSO_ISSUER_ID` configuration key) and the URL to which the IdP is to send its responses (as specified in the `BASE_URL` or `BASE_URL_HTTPS` configuration key).

   The IdP operator requires a URL in the following format:

   `http://<host>:<port>/<context-root>/saml2/metadata.jsp`

   where `<host>`, `<port>`, and `<context-root>` point to the OSCM installation.
5. For Web browser SSO: Import the IdP certificate into the application server truststore where OSCM is deployed, and set the **`SSO_IDP_TRUSTSTORE`** and **`SSO_IDP_TRUSTSTORE_PASSWORD`** configuration keys accordingly. Refer to the *Operator's Guide* for details on certificate handling.
6. For using the STS for authenticating Web service calls, the IdP operator requires the OSCM domain certificate. He has to import this certificate into the truststore of the application server where the STS is deployed. Refer to the *Operator's Guide* for details on certificate handling.
7. For Web browser SSO and for STS, the assertions returned to OSCM must contain user IDs and the corresponding tenant ID for each user. This is required for OSCM to map the users to the OSCM user roles (such as administrator, service manager, marketplace manager), and to ensure the uniqueness of user IDs in a multitenancy environment.

   To achieve this, the IdP must be configured such that its assertions contain two `<AttributeStatement>` elements. The first `<Attribute>` subelement must contain a `Name="userid"` property, and the `<AttributeValue>` subelement must specify the user ID that matches the ID of the calling user in OSCM . The second `<Attribute>` subelement must contain a `Name="tenantID"` property, and the `<AttributeValue>` subelement must specify the ID of the tenant associated with the organization the corresponding user belongs to.

   Example:

```
<saml:Assertion ...>
    ...
    <saml:AttributeStatement>
      <saml:Attribute Name="userid">
        <saml:AttributeValue>administrator</saml:AttributeValue>
      </saml:Attribute>
```

```
    <saml:Attribute Name="tenantID">
        <saml:AttributeValue>34ffd098</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
```

4 Update Installation

Before updating your installation of OSCM, read the *Release Notes* of the new release. They contain information on compatibility issues, changes and enhancements, and known restrictions.

Note: An update installation cannot change the authentication mode (INTERNAL or SAML_SP). You can only upgrade from an installation in INTERNAL mode to an installation in INTERNAL mode, or an installation in SAML_SP mode to an installation in SAML_SP mode.

Preparing the Update

Before you start with the update installation, carry out the following steps:

1. In the `bes-domain` and the `master-indexer-domain` domains, check whether all JMS messages have been processed. They are stored in the `bssjms` database. For example, check the JMS broker as follows:

   For the `bes-domain` domain:

   ```
   <GLASSFISH_HOME>/mq/bin/imqcmd.exe -b localhost:8076
      -u admin query bkr
   ```

   For the `master-indexer-domain` domain:

   ```
   <GLASSFISH_HOME>/mq/bin/imqcmd.exe -b localhost:8476
      -u admin query bkr
   ```

   where `8076` or `8476` is the port where the JMS broker is running.

   When executing the above command, you need to specify a password. The default password `admin` is defined in the `password.sample` file in the `<GLASSFISH_HOME>/mq/etc` directory. It is set automatically after the installation of GlassFish. You can also call the above command together with this password file, for example for the `bes-domain` domain:

   ```
   <GLASSFISH_HOME>/mq/bin/imqcmd.exe -b localhost:8076
      -u admin query bkr -passfile ../etc/passfile.sample
   ```

2. Set the following environment variable for your current session:

   `DB_INTERPRETER`: The absolute path and name of the `psql` executable of PostgreSQL. The executable is usually located in the `bin` subdirectory of the PostgreSQL installation directory.

   Example:

   ```
   export DB_INTERPRETER="/opt/PostgreSQL/9.1/bin/psql"
   ```

3. If you are upgrading from a release prior to 16.0.5, check and, if necessary, adapt the value of the `HIDE_PAYMENT_INFORMATION` configuration setting introduced with this release. This setting is evaluated only once and cannot be changed anymore after OSCM has been started.

   The setting is made in the `configsettings.properties` file located in `<install_pack_dir>/databases/bes_db`.

4. If you are running OSCM in SAML_SP mode, add the following configuration setting:

   In the `configsettings.properties` file located in `<install_pack_dir>/databases/bes_db`, add values for the following configuration parameters:

SSO_DEFAULT_TENANT_ID

SSO_SAML_ASSERTION_ISSUER_ID

5. If you are running OSCM in SAML_SP mode and want to update or change STS-related configuration settings:

   In the configsettings.properties file located in <install_pack_dir>/databases/bes_db, change the values for the following configuration parameters as required:

   SSO_STS_ENCKEY_LEN

   SSO_STS_METADATA_URL

   SSO_STS_URL

6. If you are running OSCM in SAML_SP mode and upgrading from a release prior to 16.0.6:

   In the configsettings.properties file located in <install_pack_dir>/databases/bes_db, specify values for the following configuration parameters in order to support single logout:

   SSO_LOGOUT_URL : mandatory for single logout

   SSO_SIGNING_KEY_ALIAS : mandatory for signed logout requests

   SSO_SIGNING_KEYSTORE : mandatory for signed logout requests

   SSO_SIGNING_KEYSTORE_PASS : mandatory for signed logout requests

7. Proceed with updating your installation in the following sequence:
   1. Update the database.
   2. Update the master-indexer-domain domain.
   3. Update the bes-domain domain.
   4. Restart both domains.

   See below for details.

Updating the Database

Proceed with updating the database as follows:

1. Check whether the file

   postgresql-9.1-903.jdbc4.jar

   is contained in the following directories of the application server:

   - lib directory of the bes-domain domain
   - <GLASSFISH_HOME>/mq/lib/ext

   If this is not the case, copy the file from the <install_pack_dir>/install/lib directory to the location where it is missing.

2. Create a backup of the bss database using the standard PostgreSQL commands. The database backup must be compatible with PostgreSQL 9.1.12. Make sure to also have a backup of any customizations to marketplaces.

Note: Creating a backup of search index data is not required. The index will be automatically rebuilt when OSCM is operational again.

3. Update the following configuration files so that the settings match your current installation:
   - db.properties located in <install_pack_dir>/databases/bes_db
   - configsettings.properties located in <install_pack_dir>/databases/bes_db

4. Start the `bss` database.
5. Update the schema and configuration settings of the `bss` database by executing the `build-db.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-db.xml updateDatabase
```

Note: Make sure that Ant runs in a Java 7 runtime environment when calling the `build-db.xml` file.

Updating the `master-indexer-domain` Domain

1. Start the `master-indexer-domain` domain.
2. Undeploy the search indexer application, `oscm-search`.
3. Set the following setting in the **JVM Options** of the application server to `false`:
   `-Dorg.apache.catalina.loader.WebappClassLoader.ENABLE_CLEAR_REFERENCES=false`
4. Stop the `master-indexer-domain` domain.
5. Check for `.glassfishStaleFiles` files. If there are any, delete them. The files are located in
   `<domain>/applications/<application name>/.glassfishStaleFiles`
   For example:
   `master-indexer-domain/applications/oscm-search/.glassfishStaleFiles`
6. Delete any existing index directories in the index base of the `master-indexer-domain` domain:
   `master-indexer-domain/masterIndexBase/*`
7. Start the `master-indexer-domain` domain.
8. Deploy the search indexer application (`oscm-search` located in `<install_pack_dir>/domains/indexer_domain/applications`).

Updating the `bes-domain` Domain

1. Start the `bes-domain` domain.
2. Undeploy the following applications:
   - `oscm`
   - `oscm-portal`
   - `oscm-portal-help`
   - Optionally: Your own branding package `.war` file, if you have customized the layout of the marketplaces and created your own branding package.
3. Set the following setting in the **JVM Options** of the application server to `false`:
   `-Dorg.apache.catalina.loader.WebappClassLoader.ENABLE_CLEAR_REFERENCES=false`
4. Stop the `bes-domain` domain.
5. Check for `.glassfishStaleFiles` files. If there are any, delete them. The files are located in
   `<domain>/applications/<application name>/.glassfishStaleFiles`
   For example:
   `bes-domain/applications/oscm/.glassfishStaleFiles`
6. Check for an `eclipse-birt-runtime` directory. If there is one, delete it.

7. Delete any existing index directories in the index base of the `bes-domain` domain:
   `bes-domain/slaveIndexBase/*`
8. Copy the `javax.faces.jar` file from the `<install_pack_dir>/install/lib` directory to the `<GLASSFISH_HOME>/modules` directory.
9. Copy the `oscm-security.jar` and `commons-codec-1.7.jar` files from the `<install_pack_dir>/domains/bes_domain/lib` directory to the `lib` directory of the `bes-domain` domain.
10. Start the `bes-domain` domain.
11. Deploy the OSCM applications located in `<install_pack_dir>/domains/bes_domain/applications` in the following sequence:
    1. `oscm`

       If you are running OSCM in SAML_SP mode, you need to update the WSIT files contained in the `oscm.ear` archive. If you want to update or change STS-related configuration settings, you must change the respective settings in the `configsettings.properties` located in `<install_pack_dir>/databases/bes_db` file first.

       Execute the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

       ```
       <ANT_HOME>/bin/ant
          -DpatchProps.path=../domains/bes_domain/installer
          -f build-glassfish.xml patchApplication
       ```

       Note: It may be required to enclose the `-DpatchProps.path=<path>` command in double or single quotes depending on the operating system.

       The configuration setting values are read from the `configsettings.properties` file and written to the WSIT files contained in the `oscm.ear` archive. During the execution of the above command, a `tmp` subdirectory is created in `<install_pack_dir>/domains/bes_domain` to which the updated `oscm.ear` archive is saved. Proceed with manually deploying the `tmp/oscm.ear` archive to the `bes-domain` domain.

    2. `oscm-portal`

       This archive contains the properties files for the user interface resources (user interface and email texts, platform objects). Be aware that with a new release or fix, new keys may have been added to the system, others may have been changed or deleted.

       If you have not customized the texts, existing texts in English, German, and Japanese are overwritten by an upgrade. If you have customized these texts, they are not overwritten. Make sure to have a backup of your changes. After having deployed the `oscm-portal`, check whether existing texts, for example, mail messages have changed as compared to the previous release. You may need to customize the texts again.

    3. `oscm-portal-help`

       This archive contains the online help and FAQ files in English, German, and Japanese. You can customize these resources. When upgrading the system with a fix for this release, make sure to have a backup of any such customizations. Merge the customized files into the `oscm-portal-help` archive, before deploying it again. Otherwise they will no longer be available after the upgrade.

       If you added additional languages to the system, also include the corresponding help and FAQ file structures into the `oscm-portal-help` archive before deploying it again. Refer to the *Operator's Guide* for details.

4. Optionally: Your own branding package `.war` file

Updating the Command Line Tool

The current version of the command line tool is provided in the OSCM installation package, `oscm-install-pack.zip`, as `oscm-operatorclient.zip`. If you want to use the command line tool with your updated installation, delete and install it again when finished with the update. For details on how to set up the tool, refer to the *Operator's Guide*.

5 Uninstallation

The uninstallation of OSCM consists of the following steps:

1. Stop the application server domains related to OSCM.
2. Delete the `bes-domain` domain.
3. Delete the `master-indexer-domain` domain.
4. Delete the shared directory for the master search index.
5. Delete the databases, `bss` and `bssjms`, and uninstall the database management system and the application server, if you no longer need them for other purposes.

For details on how to proceed, refer to the documentation of the database management system and the application server.

Appendix A: Application Server Resources

The following sections provide an overview of the resources which must be provided to OSCM on the application server.

For details and hints on how to create these resources, refer to the `build-glassfish.xml` file located in the `<install_pack_dir>/install` directory.

A.1 OSCM Domain

The following sections give an overview of the resources which must be provided for the OSCM domain (`bes-domain`) on the application server.

Data Source

A JDBC data source with a corresponding connection pool is required for the relational databases where OSCM stores its data.

Name	`BSSDS`
Class name	`org.postgresql.xa.PGXADataSource`
Resource type	`javax.sql.XADataSource`
Database schema	As distributed with OSCM.

JMS Queues

The following JMS queues and corresponding connection factories are required for asynchronous processing:

1. **Trigger queue:**
   Queue name: `jms/bss/triggerQueue`
   Connection factory name: `jms/bss/triggerQueueFactory`
2. **Task queue:**
   Queue name: `jms/bss/taskQueue`
   Connection factory name: `jms/bss/taskQueueFactory`
3. **Indexer queue:**
   Queue name: `jms/bss/indexerQueue`
   Connection factory name: `jms/bss/indexerQueueFactory`
4. **Master indexer queue:**
   Queue name: `jms/bss/masterIndexerQueue`
   Connection factory name: `jms/bss/masterIndexerQueueFactory`

All queues and connection factories mentioned above use the following settings:

Initial and minimum pool size	`1` connection
Maximum pool size	`250` connections
Pool resize quantity	`2` connections

Idle timeout	`600` seconds
Max wait time	`60000` milliseconds
On any failure	`Close all connections`
Transaction support	`XATransaction`
Connection validation	`Required`
UserName	`jmsuser`
Password	`jmsuser`

The master indexer queue / connection factory requires the following additional setting:

AddressList	`<master-indexer-host-name>:<port>`, where `port` is the port number of the search indexer application domain. Default: `8476`

Java Mail Session

A Java Mail Session is required for the application server to automatically send emails in case of specific user actions.

JNDI Name	`mail/BSSMail`
Store Protocol	`imap`
Transport Protocol	`smtp`
mail-smtp-auth	`false`
mail-user	`saas`
mail-smtp-port	`25`
mail-smtp-password	`password`

The settings are retrieved from the `glassfish.properties` file located in `<install_pack_dir>/domains/bes_domain` when running the installation scripts. The **JNDI Name**, **Store Protocol**, and **Transport Protocol** are mandatory and must not be changed.

Realm

OSCM comes with a custom realm implementation in the `oscm-security.jar` archive (located in `<install_pack_dir>/domains/bes_domain/lib`), which is included in the installation package. The realm must be configured as follows:

Name	`bss-realm`
JAAS context	`bssRealm`
Implementation class	`org.oscm.security.ADMRealm`

Certificate Realm

The certificate realm of the application server must be assigned the role `CLIENTCERT`.

Default File Encoding

Ensure that the default file encoding of the application server's Java virtual machine is UTF-8. This can be achieved by setting the `file.encoding` system property to `UTF8`.

A.2 Search Indexer Application Domain

The following sections provide an overview of the resources which must be provided for the search indexer application domain (`master-indexer-domain`) on the application server.

Data Source

A JDBC data source with a corresponding connection pool is required for the relational databases where OSCM stores its data.

Name	`BSSDS`
Class name	`org.postgresql.xa.PGXADataSource`
Resource type	`javax.sql.XADataSource`
Database schema	As distributed with OSCM.

JMS Queue

A JMS queue and a corresponding connection factory are required for asynchronous processing.

Queue name	`jms/bss/masterIndexerQueue`
Connection factory name	`jms/bss/masterIndexerQueueFactory`
Initial and minimum pool size	`1` connection
Maximum pool size	`250` connections
Pool resize quantity	`2` connections
Idle timeout	`600` seconds
Max wait time	`60000` milliseconds
On any failure	`Close all connections`
Transaction support	`XATransaction`
Connection validation	`Required`
UserName	`jmsuser`
Password	`jmsuser`

Default File Encoding

Ensure that the default file encoding of the application server's Java virtual machine is UTF-8. This can be achieved by setting the `file.encoding` system property to `UTF8`.

Appendix B: Configuration Settings

The configuration settings for OSCM are provided in the following files in subdirectories of the directory to which you extracted the `oscm-install-pack.zip` file (`<install_pack_dir>`):

- `domains/indexer_domain/glassfish.properties`
- `domains/bes_domain/glassfish.properties`
- `domains/indexer_domain/glassfishJMSBroker.properties`
- `domains/bes_domain/glassfishJMSBroker.properties`
- `databases/bes_db/db.properties`
- `databases/bes_db/configsettings.properties`
- `databases/bes_db/sso.properties`

This appendix describes the settings in detail.

B.1 GlassFish Configuration Settings for the Search Indexer Application Domain

The `glassfish.properties` file located in `<install_pack_dir>/domains/indexer_domain` contains the configuration settings for the GlassFish application server. The settings are required for configuring the domain where the search indexer application is deployed.

Below you find a detailed description of the settings.

GLASSFISH_HOME

The absolute path and name of the GlassFish installation directory.

JDBC_DRIVER_JAR_NAME

The name of the PostgreSQL JDBC driver jar file as available after installation.

Example: `postgresql-9.1-903.jdbc4.jar`

glassfish.domain.portbase

Mandatory. The base number for all ports used by the domain of the search indexer application. Make sure that the port base setting differs from the `glassfish.domain.portbase` setting for the `bes_domain` domain by at least 200.

Example: `8400`

glassfish.domain.jms.port

Mandatory. The port of the JMS broker used by the domain of the search indexer application.

Example: `8476`

glassfish.domain.portadmin

Mandatory. The administration port of the search indexer domain.

Example: `8448`

glassfish.domain.name

Mandatory. The name of the domain for the search indexer application.

Default: `master-indexer-domain`

glassfish.domain.admin.user

Mandatory. The user name of the search indexer application domain administrator.

Default: `admin`

glassfish.domain.admin.pwd

Mandatory. The password of the search indexer application domain administrator.

Default: `adminadmin`

glassfish.domain.admin.master.pwd

Mandatory. The master password required for accessing the keystore and truststore files of the application server domain.

Default: `changeit`

hibernate.search.shared.sourceBase

Mandatory. The shared directory hosting the search index for the master indexer node and the slave nodes, if any. From this directory, the master search index is replicated to the slave nodes, if any.

On Windows, double-escape the colon in the drive specification of the path to the shared directory.

Example: `C\\:/glassfish/masterSourceBase`

hibernate.search.default.refresh

Mandatory. The interval in seconds between refresh operations. At this interval, the search index is replicated and copied to the shared directory hosting the search index for the master indexer node.

Default: `300`

glassfish.domain.stop.waitSeconds

Mandatory. The time in seconds the application server waits until a stop domain operation is executed.

Default: `60`

glassfish.domain.start.maxWaitSeconds

Mandatory. The maximum time in seconds the application server waits until it checks whether a domain is started.

Default: `600`

B.2 GlassFish Configuration Settings for the OSCM Domain

The `glassfish.properties` file located in `<install_pack_dir>/domains/bes_domain` contains the configuration settings for the GlassFish application server. The settings are required for configuring the domain where the OSCM application is deployed.

Below you find a detailed description of the settings.

GLASSFISH_HOME

The absolute path and name of the GlassFish installation directory.

JDBC_DRIVER_JAR_NAME

The name of the PostgreSQL JDBC driver jar file as available after installation.

Example: `postgresql-9.1-903.jdbc4.jar`

MAIL_HOST

The host name or IP address of your mail server.

MAIL_RESPONSE_ADDRESS

The email address used by the server as the sender of emails.

Example: `saas@yourcompany.com`

MAIL_PORT

The port of your mail server.

Default: `25`

MAIL_USE_AUTHENTICATION

Optional. Defines whether mails can be sent only to users authenticated against the SMTP mail system.

Allowed values: `true`, `false`

Default: `false`

MAIL_USER

Mandatory if `MAIL_USE_AUTHENTICATION=true`. Specifies the name of the user to be used for authentication against the SMTP mail system.

MAIL_PWD

Mandatory if `MAIL_USE_AUTHENTICATION=true`. Specifies the password of the user to be used for authentication against the SMTP mail system.

MAIL_TIMEOUT

Optional. The time interval in milliseconds for sending email messages, i.e. until a socket I/O timeout occurs.

Allowed values: Any value between `0` and `4924967296`

Default: `30000`

MAIL_CONNECTIONTIMEOUT

Optional. The time interval in milliseconds for establishing the SMTP connection, i.e. until a socket connection timeout occurs.

Allowed values: Any value between `0` and `4924967296`

Default: `30000`

glassfish.domain.portbase

Mandatory. The base number for all ports used by the domain of the OSCM application. Make sure that the port base setting differs from the `glassfish.domain.portbase` setting for the `master_indexer_domain` domain by at least 200.

Example: `8800`

glassfish.domain.portadmin

The administration port of the domain used for OSCM.

Example: `8848`

glassfish.domain.name

The name of the domain where OSCM is deployed.

Example: `bes-domain`

glassfish.domain.admin.user

The user name of the OSCM domain administrator.

Default: `admin`

glassfish.domain.admin.pwd

The password of the OSCM domain administrator.

Default: `adminadmin`

glassfish.domain.remote.jms.host

Mandatory. The host name or IP address of the server where the domain for the search indexer application is deployed.

Example: `MyHibernateMasterIndexerHostName`

glassfish.domain.remote.jms.port

Mandatory. The port of the JMS broker used by the domain of the search indexer application.

Example: `8476`

glassfish.domain.admin.master.pwd

Mandatory. The master password required for accessing the keystore and truststore files of the application server domain.

Default: `changeit`

glassfish.domain.WS_PORT

The port used for an HTTP listener for Web service connections of the application server.

Example: `8082`

hibernate.search.default.refresh

Mandatory. The interval in seconds between index data refresh operations. At this interval, the search index is read from the shared directory hosting the search index for the master indexer node and written to the index directory on the slave node.

Example: `300`

hibernate.search.shared.sourceBase

Mandatory. The shared directory hosting the search index for the master indexer node and the slave nodes, if any. From this directory, the master search index is replicated to the slave nodes, if any.

On Windows, double-escape the colon in the drive specification of the path to the shared directory.

Example: `C\\:/glassfish/masterSourceBase`

glassfish.domain.stop.waitSeconds

Mandatory. The time in seconds the application server waits until a stop domain operation is executed.

Default: `60`

glassfish.domain.start.maxWaitSeconds

Mandatory. The maximum time in seconds the application server waits until it checks whether a domain is started.

Default: `600`

B.3 GlassFish JMS Configuration Settings

The `glassfishJMSBroker.properties` file contains the configuration settings for the Java Message Service (JMS) in the application server. It is required for both domains, `master-indexer-domain` and `bes-domain`, and thus available in the following directories:

`<install_pack_dir>/domains/indexer_domain`

`<install_pack_dir>/domains/bes_domain`

Note: If you are using OSCM in a multi-node installation, make sure to change the default setting `imq.brokerid=broker1` to a value that is unique for every node.

For details, refer to the *Sun GlassFish Message Queue 4.4 Administration Guide*.

B.4 Database Configuration Settings

The `db.properties` file located in `<install_pack_dir>/databases/bes_db` contains the configuration settings for database access. This configuration is used for the initial setup and schema updates.

db.driver.class

The Java class of the JDBC driver.

Default: `org.postgresql.Driver`

db.host

The database host.

Default: `localhost`

db.port

The database port.

Default: `5432`

db.name

The name of the database.

Default: `bss`

db.user

The name of the user to connect to the database.

Default: `bssuser`

db.pwd

The password of the user to connect to the database.

Default: `bssuser`

db.type

The type of the database.

Default: `postgresql`

B.5 OSCM Configuration Settings

The `configsettings.properties` file located in `<install_pack_dir>/databases/bes_db` contains the configuration settings for the OSCM services.

AUDIT_LOG_ENABLED

Optional. Specifies whether user operations related to subscriptions, marketable services, and price models are logged and stored in the database. If set to `true`, the operator can export audit log data to retrieve information on the user operations.

Allowed values: `true`, `false`

Default: `false`

AUDIT_LOG_MAX_ENTRIES_RETRIEVED

Optional. Specifies how many log entries are retrieved in one export of audit log data. If this number is exceeded, a warning is displayed asking the operator to change his filter criteria and start the export again. This setting is required to keep the number of SQL requests to the database low when audit log data is exported. Too many requests may lead to a decrease in system performance.

Allowed values: Any value between `1` and `1000`

Default: `100`

AUTH_MODE

Mandatory. Specifies whether OSCM is used for user authentication or whether it acts as a SAML service provider. This configuration setting is evaluated at the first startup of OSCM and can no longer be changed after OSCM has been started for the first time. It cannot be changed by an upgrade installation either.

Allowed values: `INTERNAL` (OSCM user authentication is used) or `SAML_SP` (OSCM shall act as SAML service provider, and users are to be authenticated against an Identity Provider (IdP) system.

Default: `INTERNAL`

BASE_URL

Optional. The base URL is used to access the OSCM home page if OSCM does not require HTTPS for communication. If left empty, the `BASE_URL_HTTPS` setting is used.

Syntax: `http://<host>:<port>/<context-root>`

The default for `<context-root>` is `oscm-portal`.

Note: If the SSL/HTTPS port was changed, then this setting must also be updated.

BASE_URL_HTTPS

Mandatory. The base URL is used to access the OSCM home page and to create the URL for accessing services via HTTPS.

Syntax: `https://<host>:<port>/<context-root>`

The default for `<context-root>` is `oscm-portal`.

Note: If the SSL/HTTPS port was changed, then this setting must also be updated.

CUSTOMER_SELF_REGISTRATION_ENABLED

Optional. Specifies whether customer organizations can register on a marketplace. If set to `false`, the operator needs to create an organization for the customer who wants to register, or a seller (supplier, broker, reseller) needs to register the customer.

Allowed values: `true`, `false`

Default: `true`

DECIMAL_PLACES

Optional. Specifies the number of decimal places in which usage charges are calculated. This setting is needed only when migrating from OSCM V14.1 to a higher version.

Allowed values: `2`, `3`, `4`, `5`, `6`

Default: `2`

HIDDEN_UI_ELEMENTS

Optional. Specifies user interface elements to be hidden from the OSCM administration portal and the marketplaces operated on your platform. You can use this setting to hide user interface elements both from the marketplaces and the administration portal.

Marketplaces

If you want to hide a menu option from the **Account** menu of the marketplaces operated on your platform, enter one of the following values:

- `marketplace.navigation.Profile`: **Profile** menu
- `marketplace.navigation.Payment`: **Payment** menu
- `marketplace.navigation.Subscriptions`: **Subscriptions** menu
- `marketplace.navigation.Users`: **Users & Units** menu
- `marketplace.navigation.Reports`: **Reports** menu
- `marketplace.navigation.Processes`: **Processes** menu
- `marketplace.navigation.Operations`: **Operations** menu

To hide several options from the **Account** menu, separate the options by a comma.

Administration Portal

If you want to hide a specific page from the OSCM administration portal, you can find out which value needs to be specified here as follows:

1. Open the respective page at the administration portal.
2. Display the online help for this page.
3. Have a look at the name of the online help HTML page.
4. Omit the file extension `.htm` and replace the underscore by a dot.

Example:

You want to hide the **Manage VAT rates** page. The online help HTML page name is `organization_manageVats.htm`. Thus, the respective administration portal page is `organization.manageVats`. You need to set the configuration key as follows:

```
HIDDEN_UI_ELEMENTS=organization.manageVats
```

To hide several pages from the administration portal, separate the entries by a comma.

Below, you find some more examples of values that can be used to hide a specific page. The list is not complete.

- `organization.edit`: **Edit profile** page
- `shop.editSkin`: **Customize layout** page
- `techService.edit`: **Update service definition** page

To hide a complete menu from the administration portal, enter one of the following values:

- `navigation.myAccount`: **Account** menu
- `navigation.customer`: **Customer** menu
- `navigation.operator`: **Operation** menu
- `navigation.techService`: **Technical service** menu
- `navigation.service`: **Marketable service** menu
- `navigation.priceModel`: **Price model** menu
- `navigation.marketplace`: **Marketplace** menu

Note:	The **Update configuration settings** page in the **Operation** menu is the default page the operator is directed to when logging in. If you hide the page from the menu or hide the complete menu, you are still directed to the **Update configuration settings** page where you can make changes, if required.

HIDE_PAYMENT_INFORMATION

Optional. Determines whether customers need to specify payment information for subscribing to services that use the native billing system of OSCM and are not free of charge. If set to `true`, the dialogs and options for specifying payment types and billing addresses are hidden on the marketplaces, and customer payment information does not appear in billing and payment preview reports. In the administration portal, suppliers and resellers cannot manage payment types for their customers. Billing runs and payment processing are not affected by the setting.

The setting is evaluated only once when OSCM is installed or updated. The value can no longer be changed after OSCM has been started, not even with a further update installation.

Allowed values: `true`, `false`

Default: `false`

HTTP_PROXY

Optional. The proxy to be used for PSP-related HTTP connections, if any.

Example: `proxy.domain` or the proxy server IP address.

HTTP_PROXY_PORT

Optional. The proxy port to be used for PSP-related HTTP connections, if any.

Allowed values: Any value between `1` and `65535`

Default: `1080`

IDP_ASSERTION_EXPIRATION

Deprecated.

IDP_ASSERTION_VALIDITY_TOLERANCE

Deprecated.

IDP_PRIVATE_KEY_FILE_PATH

Deprecated.

IDP_PUBLIC_CERTIFICATE_FILE_PATH

Deprecated.

LDAP_SEARCH_LIMIT

Optional. The maximum number of entries that will be returned by an LDAP query in case an organization uses an external LDAP system for user management.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `100`

LOG_CONFIG_FILE

Optional. The path to the `log4j` configuration file of OSCM.

Default:

`./log4j.properties` in the `<GLASSFISH_HOME>/glassfish/domains/bes-domain/config` directory

LOG_FILE_PATH

Mandatory. The path to the OSCM log files.

Default:

`../logs`, which is the `<GLASSFISH_HOME>/glassfish/domains/bes-domain/logs` directory

If you change this setting, you need to restart OSCM.

LOG_LEVEL

Optional. The log level for OSCM. This setting applies to all logging classes if it is not overridden by the content of the `log4j.properties` file.

Allowed values: `ERROR`, `WARN`, `INFO`, `DEBUG`

Default: `INFO`

If you change this setting, you need to restart OSCM.

MAIL_JA_CHARSET

Optional. Special character encoding for emails sent in Japanese.

Default: `UTF-8`

MAX_NUMBER_ALLOWED_USERS

Mandatory. The maximum number of users that can be registered within the OSCM installation.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `10`

MAX_NUMBER_LOGIN_ATTEMPTS

Optional. The maximum number of allowed login attempts to OSCM. If a user does not log in successfully with this number of attempts, his account is locked.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `3`

MP_ERROR_REDIRECT_HTTP

Optional. The URL of a Web page that is to be displayed in case a visitor tries to access a marketplace without a valid marketplace ID by HTTP. This Web page will be shown instead of the default error message.

Syntax: `http://<your Web page>`

Make sure to specify a valid URL that does not exceed a maximum of 255 characters.

MP_ERROR_REDIRECT_HTTPS

Optional. The URL of a Web page that is to be displayed in case a visitor tries to access a marketplace without a valid marketplace ID by HTTPS. This Web page will be shown instead of the default error message.

Syntax: `https://<your Web page>`

Make sure to specify a valid URL that does not exceed a maximum of 255 characters.

PERMITTED_PERIOD_INACTIVE_ON_BEHALF_USERS

Optional. The time in milliseconds after which a user who logged in on behalf of a customer and was inactive will be removed from the system.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `604800000`, i.e. 7 days

PERMITTED_PERIOD_UNCONFIRMED_ORGANIZATIONS

Optional. The maximum time in milliseconds until an organization's initial administrative account must be confirmed. When this time has passed, the account is removed.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `604800000`, i.e. 7 days

PSP_USAGE_ENABLED

Mandatory. Specifies whether PSP integration is used for the current environment.

Allowed values: `true`, `false`

Default: `false`

If you change this setting, you need to restart OSCM.

REPORT_ENGINEURL

Mandatory if you want to use the OSCM reports. The URL template of the report engine. If you do not specify a correct URL template, OSCM will not be able to generate any reports, since the Report Web service cannot be called correctly.

If your installation is configured to use HTTP access, the required value is:

```
http://<host IP address>:<port>/birt/frameset?
   __report=${reportname}.rptdesign&SessionId=${sessionid}
   &__locale=${locale}&WSDLURL=${wsdlurl}&SOAPEndPoint=${soapendpoint}
   &wsname=Report&wsport=ReportPort
```

If your installation is configured to use HTTPS access, the required value is:

```
https://<host IP address>:<port>/birt/frameset?
   __report=${reportname}.rptdesign&SessionId=${sessionid}
   &__locale=${locale}&WSDLURL=${wsdlurl}&SOAPEndPoint=${soapendpoint}
   &wsname=ReportSecure&wsport=ReportSecurePort
```

Note: The above value must be used as indicated. Do not change this value.

If the SSL/HTTPS port is changed and the BIRT report engine is running on the same domain as OSCM, then this setting must also be updated.

REPORT_SOAP_ENDPOINT

Mandatory if you want to use the OSCM reports. The SOAP end point of the Report Web service. All report data is retrieved via a call to the Report Web service. If you do not specify a correct value, OSCM will not be able to generate any reports, since the Report Web service cannot be called correctly.

If your installation is configured to use HTTP access, the required value is:

```
http://<host IP address>:<port>/Report/ReportingServiceBean
```

If your installation is configured to use HTTPS access, the required value is:

`https://<host IP address>:<port>/ReportSecure/ReportingServiceSecureBean`

Note:	The above value must be used as indicated. Do not change this value. If the SSL/HTTPS port is changed and the BIRT report engine is running on the same domain as OSCM, then this setting must also be updated.

REPORT_WSDLURL

Mandatory if you want to use the OSCM reports. The URL of the WSDL file of the Report Web service. All report data is retrieved via a call to the Report Web service. If you do not specify a correct value, OSCM will not be able to generate any reports, since the Report Web service cannot be called correctly.

If your installation is configured to use HTTP access, the required value is:

`http://<host IP address>:<port>/Report/ReportingServiceBean?wsdl`

If your installation is configured to use HTTPS access, the required value is:

`https://<host IP address>:<port>/ReportSecure/ReportingServiceSecureBean?wsdl`

Note:	The above value must be used as indicated. Do not change this value. If the SSL/HTTPS port is changed and the BIRT report engine is running on the same domain as OSCM, then this setting must also be updated.

SEARCH_INDEX_MASTER_FACTORY_NAME

Mandatory. The name of the search indexer application's JMS connection factory. Stay with the entry `jms/bss/masterIndexerQueueFactory` and do not change it.

SEARCH_INDEX_MASTER_QUEUE_NAME

Mandatory. The name of the search indexer application's JMS queue. Stay with the entry `jms/bss/masterIndexerQueue` and do not change it.

SSO_DEFAULT_TENANT_ID

Mandatory if you install OSCM in SAML_SP authentication mode.

The unique ID of the default tenant. The default tenant is associated with the IdP that all users registered with OSCM are authenticated against when they access a marketplace or the administration portal.

It must consist of exactly 8 characters. No special characters or blanks are allowed. The platform operator may specify any value in the configuration settings.

The default tenant ID must be communicated to the IdP administrator. The IdP administrator must set this ID as an attribute for SAML assertions. For example, in OpenAM, where OSCM has been registered as Service Provider (SP), the IdP administrator selects this SP, and enters `tenantID="<the 8 characters>"` as an assertion processing attribute.

If you need to change this setting after the first exchange of data between OSCM and the IdP, you must change it both in OSCM and the IdP system. The IdP administrator must be informed accordingly.

SSO_IDP_AUTHENTICATION_REQUEST_HTTP_METHOD

Mandatory if you install OSCM in SAML_SP authentication mode. The method used for HTTP authentication requests. Depending on the IdP, `GET` or `POST` requests can be used.

Required for Web browser SSO.

Default: `POST`

If you change this setting, you need to restart OSCM.

SSO_SAML_ASSERTION_ISSUER_ID

Mandatory if you install OSCM in SAML_SP authentication mode.

The entity ID of the IdP system. This ID is unique for the IdP system and has to be communicated between the platform operator and the IdP administrator. It is required so that the platform can ensure that the authentication information returned from the IdP system actually comes from the IdP system that is configured for authenticating users.

The IdP administrator can find out the ID by retrieving the federation metadata on his IdP system.

Examples:

On the OpenAM server, the federation metadata can be retrieved in a Web browser as follows:

`https://<OpenAM_server>/openam/saml2/jsp/exportmetadata.jsp?entityid=`

On the ADFS server, look for the following file:

`http://<ADFShost>/FederationMetadata/2007-06/FederationMetadata.xml`

In the XML file, the issuer ID is known as `entityID`, for example;

`entityID="http://example.adfs.com/adfs/services/trust"`

SSO_IDP_TRUSTSTORE

Mandatory if you install OSCM in SAML_SP authentication mode. The path and file name of the application server truststore file holding the public key certificate of the IdP.

Required for Web browser SSO.

Default: `<path>/cacerts.jks`

As soon as another IdP system, for example, OpenAM, Cloudminder, or Active Directory is installed and used, this setting might need to be changed. In this case, you need to restart OSCM.

SSO_IDP_TRUSTSTORE_PASSWORD

Mandatory if you install OSCM in SAML_SP authentication mode. The password of the application server truststore holding the public key certificate of the IdP.

Required for Web browser SSO.

GlassFish default password: `changeit`

The spelling of the password is case-sensitive and must be identical to the output of the IdP.

If you change this setting, you need to restart OSCM.

SSO_IDP_URL

Mandatory if you install OSCM in SAML_SP authentication mode. The SAML Redirect URL for the IdP service endpoint.

Required for Web browser SSO.

For security and confidentiality reasons, it is recommended to use the HTTPS protocol.

Syntax: `https://<host>:<port>/<RedirectServiceEndpoint>`

If you change this setting, you need to restart OSCM.

SSO_ISSUER_ID

Mandatory if you install OSCM in SAML_SP authentication mode. A unique identifier for OSCM. The IdP uses this ID for identifying incoming SAML authentication requests from OSCM.

Required for Web browser SSO.

If you need to change this setting after the first exchange of data between OSCM and the IdP, you must change it both in OSCM and the IdP system. It may be required to send a new metadata exchange file to the IdP operator.

Default: `CT_MG`

If you change this setting, you need to restart OSCM.

SSO_LOGOUT_URL

Mandatory if you install OSCM in SAML_SP authentication mode and want to make use of single logout.

The URL of the endpoint of the IdP system's single logout service. Logout and invalidate session requests from OSCM are sent to this address.

Required for Web browser SSO.

For security and confidentiality reasons, it is recommended to use the HTTPS protocol.

Syntax: `https://<host>:<port>/<LogoutServiceEndpoint>`

If you change this setting, you need to restart OSCM.

Note: In the IdP system, a URL must be specified to which the response to the logout request is sent and the user is redirected by the logout. We recommend you use the following default marketplace address of OSCM: `https://<host>:<port>/oscm-portal/marketplace/index.jsf`. In case of problems, the user can be automatically redirected from this page to another one specified in the `MP_ERROR_REDIRECT_HTTPS` configuration setting.

SSO_SIGNING_KEY_ALIAS

Mandatory if you install OSCM in SAML_SP authentication mode, want to make use of single logout, and the IdP system's single logout service requires signed requests, as, for example, in Microsoft Active Directory Federation Services.

The alias of the private key of OSCM to be used for signing logout requests. The IdP system needs the corresponding certificate of OSCM in its truststore for verifying the signature.

Required for Web browser SSO.

Example: `s1as`

If you change this setting, you need to restart OSCM.

SSO_SIGNING_KEYSTORE

Mandatory if you install OSCM in SAML_SP authentication mode, want to make use of single logout, and the IdP system's single logout service requires signed requests, as, for example, in Microsoft Active Directory Federation Services.

The path and name of the application server's keystore where the private key of OSCM specified in the `SSO_SIGNING_KEY_ALIAS` setting is stored.

Required for Web browser SSO.

Example: `/opt/glassfish-3.1.2.2/glassfish/domains/bes-domain/config/keystore.jks`

If you change this setting, you need to restart OSCM.

SSO_SIGNING_KEYSTORE_PASS

Mandatory if you install OSCM in SAML_SP authentication mode, want to make use of single logout, and the IdP system's single logout service requires signed requests, as, for example, in Microsoft Active Directory Federation Services.

The password for accessing the keystore specified in the `SSO_SIGNING_KEYSTORE` setting.

Required for Web browser SSO.

Example: `changeit`

If you change this setting, you need to restart OSCM.

SSO_STS_ENCKEY_LEN

Mandatory if you install OSCM in SAML_SP authentication mode. The length of the encryption key as used by the IdP.

Required for STS communication.

Default: `128`

This setting is an installation property and cannot be changed in the administration portal. If you need to change the encryption key length, proceed as follows:

1. Stop the `bes-domain` domain.
2. Edit the `configsettings.properties` file and change the value for `SSO_STS_ENCKEY_LEN` as required.
3. Execute the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant
   -DpatchProps.path=../domains/bes_domain/installer
   -f build-glassfish.xml patchAndRedeployApplication
```

   `<ANT_HOME>` is the installation directory of Apache Ant.

Note: It may be required to enclose the `-DpatchProps.path=<path>` command in double or single quotes depending on the operating system.

   The modified configuration parameter value is read from the `configsettings.properties` file and written to the WSIT files contained in the `oscm.ear` archive. The updated archive is redeployed to the `bes-domain` domain.

   During the execution of the above command, a `tmp` subdirectory is created in `<install_pack_dir>/domains/bes_domain` to which the updated `oscm.ear` archive is saved.

4. Redeploy the `oscm-portal.war` file to the `bes-domain` domain.
5. Restart the `bes-domain` domain.

SSO_STS_METADATA_URL

Mandatory if you install OSCM in SAML_SP authentication mode. The URL of the MEX address (Issuer Metadata Exchange) of the STS.

Required for STS communication.

For security and confidentiality reasons, it is recommended to use the HTTPS protocol.

Syntax: `https://<host>:<port>/<MEXAddress>`

This setting is an installation property and cannot be changed in the administration portal. If you need to change the URL, proceed as follows:

1. Stop the `bes-domain` domain.
2. Edit the `configsettings.properties` file and change the value for `SSO_STS_METADATA_URL` as required.
3. Execute the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant
   -DpatchProps.path=../domains/bes_domain/installer
   -f build-glassfish.xml patchAndRedeployApplication
```

`<ANT_HOME>` is the installation directory of Apache Ant.

Note: It may be required to enclose the `-DpatchProps.path=<path>` command in double or single quotes depending on the operating system.

The modified configuration parameter value is read from the `configsettings.properties` file and written to the WSIT files contained in the `oscm.ear` archive. The updated archive is redeployed to the `bes-domain` domain.

During the execution of the above command, a `tmp` subdirectory is created in `<install_pack_dir>/domains/bes_domain` to which the updated `oscm.ear` archive is saved.

4. Redeploy the `oscm-portal.war` file to the `bes-domain` domain.
5. Restart the `bes-domain` domain.

SSO_STS_URL

Mandatory if you install OSCM in SAML_SP authentication mode. The URL of the STS endpoint.

Required for STS communication.

For security and confidentiality reasons, it is recommended to use the HTTPS protocol.

Syntax: `https://<host>:<port>/<ServiceEndpoint>`

This setting is an installation property and cannot be changed in the administration portal. If you need to change the URL, proceed as follows:

1. Stop the `bes-domain` domain.
2. Edit the `configsettings.properties` file and change the value for `SSO_STS_URL` as required.
3. Execute the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant
   -DpatchProps.path=../domains/bes_domain/installer
   -f build-glassfish.xml patchAndRedeployApplication
```

`<ANT_HOME>` is the installation directory of Apache Ant.

Note: It may be required to enclose the `-DpatchProps.path=<path>` command in double or single quotes depending on the operating system.

The modified configuration parameter value is read from the `configsettings.properties` file and written to the WSIT files contained in the `oscm.ear` archive. The updated archive is redeployed to the `bes-domain` domain.

During the execution of the above command, a `tmp` subdirectory is created in `<install_pack_dir>/domains/bes_domain` to which the updated `oscm.ear` archive is saved.

4. Redeploy the `oscm-portal.war` file to the `bes-domain` domain.
5. Restart the `bes-domain` domain.

SUPPLIER_SETS_INVOICE_AS_DEFAULT

Optional. Specifies whether invoice is to be used as the default payment type for all customers.

Allowed values: `true`, `false`

Default: `false`

TAGGING_MAX_TAGS

Mandatory. The maximum number of tags composing the tag cloud.

The tag cloud is the area of a marketplace containing defined search terms (tags). The more often a tag is used in services, the bigger the characters of the tag are displayed. Customers can use the tags to search for services, provided that the tag cloud is enabled for the marketplace by the marketplace owner.

Allowed values: Any value between `0` and `2147483647`

Default: `20`

TAGGING_MIN_SCORE

Mandatory. The minimum number of times a tag must be used in services to be shown in the tag cloud.

The tag cloud is the area of a marketplace containing defined search terms (tags). The more often a tag is used in services, the bigger the characters of the tag are displayed. Customers can use the tags to search for services, provided that the tag cloud is enabled for the marketplace by the marketplace owner.

Allowed values: Any value between `1` and `2147483647`

Default: `1`, i.e. a tag must have been used at least once so that it is shown in the tag cloud.

TIME_ZONE_ID

Optional. The time zone to be used for display.

Allowed values: All time zones supported by Java. This can be an abbreviation such as `PST`, a full name such as `America/Los_Angeles`, or a custom ID such as `GMT-8:00`. For a list of IDs, refer to `java.util.TimeZone`.

Default: `GMT`

TIMER_INTERVAL_BILLING_OFFSET

Optional. The offset in milliseconds for the timer for billing runs calculating subscription usage costs (customer billing data) or revenue share data. The interval for this timer is one day and cannot be changed. If no offset is defined, the default offset of 4 days is applied.

Customer billing data is calculated for a period of one month (billing period). Suppliers and resellers can define individual start days for their billing periods. Revenue share data is always calculated for the past month on the first day of a month.

The offset for the billing run timer defines the following:

- Number of days after which the billing run calculating the customer billing data or the revenue share data is executed.
- Time the timer for the daily billing runs expires on the current day.

Example:

A supplier defines the 10th of a month as the billing period start date. The offset is set to 4 days and 4 hours. The billing run that calculates the customer billing data for the past billing period of this supplier is started on the 14th of the following month at 04:00:00.000. The revenue share data is calculated on the 5th of the following month at 04:00:00.000. The daily check whether a billing period of any supplier has ended is started at 04:00:00.000 every day.

Allowed values: Any value between `0` and `2419200000` (28 days)

Default: `345600000`, i.e. 4 days.

TIMER_INTERVAL_DISCOUNT_END_NOTIFICATION_OFFSET

Optional. The offset in milliseconds for the timer for terminating the discounts for all organizations. The timer interval is one day and cannot be changed.

Allowed values: Any value between `0` and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_INACTIVE_ON_BEHALF_USERS

Optional. The time interval in milliseconds at which a check for non-existing users acting on behalf of another organization is executed. A value of 0 indicates that this timer is disabled.

A technical service definition may contain a flag (`allowingOnBehalfActing`) to indicate that an organization can act in the name of another organization. The organization must be a customer of the other organization, which must have both the technology provider and supplier role. Additionally, the customer organization must have allowed the other organization to log in on its behalf. This is achieved via a subscription whose underlying technical service has the `allowingOnBehalfActing` flag set to `true`.

When an organization acts in the name of another organization, an artificial user ID is generated.

Cleaning up the OSCM database from time to time to remove such users who no longer exist might be required since it cannot be ensured that a technical service always removes such users itself.

Allowed values: `0` and any value between `10000` (10 seconds) and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_INACTIVE_ON_BEHALF_USERS_OFFSET

Optional. The offset in milliseconds for the timer for removing inactive "on behalf" users.

Allowed values: Any value between `0` and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_ORGANIZATION

Optional. The time interval in milliseconds at which tasks related to organizations are executed. A value of 0 indicates that this timer is disabled.

Allowed values: `0` and any value between `10000` (10 seconds) and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_ORGANIZATION_OFFSET

Optional. The offset in milliseconds for the timer for organization-related tasks.

Allowed values: Any value between `0` and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_SUBSCRIPTION_EXPIRATION

Optional. The time interval in milliseconds at which a check for expired subscriptions is executed. This timer cannot be disabled, i.e. it cannot be set to 0.

Allowed values: Any value between `10000` (10 seconds) and `9223372036854775807`

Default: `86400000`, i.e. 1 day

TIMER_INTERVAL_SUBSCRIPTION_EXPIRATION_OFFSET

Optional. The offset in milliseconds for the timer for subscription expiration checks.

Allowed values: Any value between `0` and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_TENANT_PROVISIONING_TIMEOUT

Optional. The time interval in milliseconds at which a check for timed-out subscriptions is executed. A value of 0 indicates that this timer is disabled.

Allowed values: `0` and any value between `10000` (10 seconds) and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_TENANT_PROVISIONING_TIMEOUT_OFFSET

Optional. The offset in milliseconds for the timer for pending subscription checks.

Allowed values: Any value between `0` and `9223372036854775807`

Default: `0`

TIMER_INTERVAL_USER_COUNT

Mandatory. The time interval in milliseconds at which the amount of users registered with the platform is checked. This timer cannot be disabled, i.e. it cannot be set to 0.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `43200000`, i.e. 12 hours

WS_TIMEOUT

Mandatory. The timeout for outgoing Web service calls in milliseconds. After this time has passed, a timeout exception is thrown by the JAX-WS framework.

An outgoing Web service call is a call initiated by OSCM. A typical example is the invocation of the `createUsers` method of the `ProvisioningService` interface, which is implemented by an

application. If the timeout is reached before the Web service call returns, the operation is aborted and an exception is thrown.

Allowed values: Any value between `1` and `9223372036854775807`

Default: `30000`, i.e. 30 seconds

Note:	Make sure that timeouts set in the GlassFish application server, e.g. request timeouts, do not conflict with or overrule the timeouts defined in the OSCM configuration settings.

B.6 SAML_SP Configuration Setting

The `sso.properties` file located in `<install_pack_dir>/databases/bes_db` contains the configuration setting for creating the first platform operator in OSCM when installing OSCM in SAML_SP authentication mode.

ADMIN_USER_ID

Mandatory if you install OSCM in SAML_SP authentication mode. The ID of the user who is to become the first OSCM operator. This user must relate to an existing user in the IdP.

User IDs are restricted to 100 characters and must not contain any of the following characters:

```
! " # $ % & ' * + , / : ; < = > ? \ ^ `
```