

Oracle® Secure Enterprise Search

Release Notes

11g Release 2 (11.2.2.2)

E35074-53

November 2017

Release Notes

This document contains important information for Oracle Secure Enterprise Search 11g Release 2 (11.2.2.2) that is not included in the regular documentation.

This document may be updated after it is released. To check for updates to this document and to view other Oracle SES documentation, refer to the Oracle Help Center (OHC) website https://docs.oracle.com/cd/E35215_01/index.html.

This document contains the following topics:

- [Mandatory Software Patches](#) (page 1)
- [Oracle Security Patch Certification Information](#) (page 2)
- [Supported Java Development Kit \(JDK\) Versions](#) (page 4)
- [Mandatory Upgrade to either Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2](#) (page 4)
- [Changed Features](#) (page 8)
- [Desupported Features](#) (page 10)
- [Open Bugs](#) (page 12)
- [Documentation Corrections and Additions](#) (page 18)
- [Implementing High Availability for Oracle SES](#) (page 25)
- [Documentation Accessibility](#) (page 26)

Mandatory Software Patches

After installing the Oracle SES 11.2.2.2 software, you must install the following mandatory patches by downloading them from the My Oracle Support (MOS) website <https://support.oracle.com>. First install the bundle patch and then install the overlay patches.

- [Bundle Patch 7](#) (patch # 23138553)

 **Note:**

When installing bundle patch 7, specify the installer to rollback the earlier installed bundle patch 6. This will deinstall bundle patch 6 as well as all the overlay patches that are already installed on the system before proceeding with the bundle patch 7 installation.

- Overlay Patches

Patch Number	Description
24490617	This is a generic patch (for all platforms) having the SES release number 11.2.2.2.7. Note: Apply this patch only if you are using a Siebel 8 data source and using Oracle Access Manager (OAM) for single sign-on (SSO) authentication for Oracle SES.
25165361	This is a generic patch (for all platforms) having the SES release number 11.2.2.2.7.
25505741	This is a generic patch (for all platforms) having the SES release number 11.2.2.2.7.
23511737	This is a generic patch (for all platforms) having the FMW release number 11.1.1.6.0.
19468532	This is a platform-specific patch having the SES release number 11.2.2.2.0. Note: This patch is currently available for Linux, Windows, AIX, and Solaris x86 operating systems. This patch will be available for Solaris SPARC operating system shortly.

Oracle Security Patch Certification Information

Oracle SES is certified with the following Oracle security patches (PSU).

Oracle SES Installation Mode	Operating System	PSU
Oracle SES installed along with the database and the middle tier	Linux, Windows, AIX, and Solaris	<ul style="list-style-type: none">• Oracle WebLogic Server 10.3.6 (Oracle Fusion Middleware) - Jan 2017 PSU• Oracle Database Server 12.1.0.2 - Jan 2017 PSU• Oracle Database Server 11.2.0.4 - April 2016 PSU
Oracle SES installed on an existing database and an existing middle tier	Linux	<ul style="list-style-type: none">• Oracle WebLogic Server 10.3.6 (Oracle Fusion Middleware) - Jan 2017 PSU• Oracle Database Server 12.1.0.2 - Jan 2017 PSU

After applying a PSU for Oracle WebLogic Server, you must execute the following steps:

1. Start the Oracle Enterprise Manager Console using the URL:

```
http://host:port/em
```

where, *host* and *port* are host name and port of the WebLogic Server middle tier.

2. Navigate to **Weblogic Domain > ses_domain_name**.

Here, **ses_domain_name** is the WebLogic Server domain used by Oracle SES.

3. Select the menu **Security > System Policies**.
4. Click the **Create** button to add a new system security grant.
5. Click the **Add** button to add a new permission.
6. On the pop-up page, select the option **Select here to enter details for a new permission** and enter the following permission details:

```
permission class: oracle.security.jps.JpsPermission  
resource name: AppSecurityContext.setApplicationID.*
```

7. Click **OK**.

8. Enter the following information in the **Codebase** field:

```
file:MW_HOME/patch_wls1036/patch_jars/*
```

where, *MW_HOME* is the absolute directory path of the WebLogic Server middle tier.

Example:

```
file:/u00/oracle/middleware/patch_wls1036/patch_jars/*
```

9. Click **OK**.
10. Execute the following steps, if the user `searchsys` is not already added to the role `SearchAdminSuperUserRole`:
 - a. Navigate to **Weblogic Domain > ses_domain_name**.
Here, **ses_domain_name** is the WebLogic Server domain used by Oracle SES.
 - b. Select the menu **Security > Application Roles**.
 - c. Select the Application Stripe **search**.
 - d. Click the arrow next to the **Role Name** field.
 - e. Add the user `searchsys` to the role `SearchAdminSuperUserRole`.

 **Note:**

- Oracle SES does the certification with Oracle WebLogic Server 10.3.6 PSU on quarterly basis.
- If Oracle SES is to be installed on an existing middle tier, then the middle tier must have WebLogic Server version 10.3.6.0.x. If the existing middle tier contains any Oracle Fusion Middleware (FMW) product, then the FMW product version must be 11.1.1.6.0 (PS5). If the FMW product version is greater than 11.1.1.6.0 (PS5), then the recommended and supported topology is to install Oracle SES into a separate Fusion Middleware home.

Supported Java Development Kit (JDK) Versions

Oracle SES 11.2.2.2 supports JDK 6 and JDK 7.

 **Note:**

- Oracle SES 11.2.2.2 does not support JDK version 8 and later, because these JDK versions do not ship with the `sun.*` packages, which are required for proper functioning of Oracle WebLogic Server 10.3.6.0.x.
See the Oracle Technology Network (OTN) article at <http://www.oracle.com/technetwork/java/faq-sun-packages-142232.html> for more information about Oracle's desupport for the `sun.*` packages.
- If you want to use Transport Layer Security (TLS) protocol version 1.2 (TLSv1.2), then you must install JDK 7 update 95 (JDK 7u95) or later.

 **See Also:**

- [Fusion Middleware Securing Oracle WebLogic Server](#)
- [JDK 7 Release Notes](#)

Mandatory Upgrade to either Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2

Oracle SES support for Oracle Database 11.2.0.3 ends on August 27, 2015. You must upgrade to either Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2 before the support ends for Oracle Database 11.2.0.3 in August 2015.

 **Note:**

- After the end of extended support for Oracle Database 11.2.0.3 in August 2015, Oracle SES installer will still install Oracle Database 11.2.0.3 when the option of installing Oracle SES along with the database and the middle tier is selected. In order to receive support from Oracle, you must manually upgrade to either Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2 before the support ends for Oracle Database 11.2.0.3 in August 2015.
- Premier support for Oracle Database 11.2.0.4 ends on January 31, 2016. If you are having Oracle Database 11.2.0.4 license without any extended support contract, then you must upgrade to Oracle Database 12.1.0.2 before the Premier support ends for Oracle Database 11.2.0.4 in January 2016.

To upgrade to Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2:

1. Stop all the running crawler schedules:
 - a. In the Oracle SES Administration GUI, navigate to **Home > Schedules**.
 - b. Select each schedule and click **Stop**.
2. Stop the index optimizer:
 - a. In the Oracle SES Administration GUI, navigate to **Global Settings > Index Optimization**.
 - b. Click **Stop Index Optimizer**.
3. Shut down Oracle SES middle tier:

- a. Shut down Oracle ESS managed servers using the following command on Linux and UNIX systems:

```
wls_domain_home/ses_domain_name/bin/stopManagedWebLogic.sh ess_server_name  
admin_URL user_name password
```

On Windows system, use the command:

```
wls_domain_home\ses_domain_name\bin\stopManagedWebLogic ess_server_name  
admin_URL user_name password
```

The parameters *admin_URL*, *user_name*, and *password* are optional parameters.

- b. Shut down Oracle SES managed servers using the following command on Linux and UNIX systems:

```
wls_domain_home/ses_domain_name/bin/stopManagedWebLogic.sh ses_server_name  
admin_URL user_name password
```

On Windows system, use the command:

```
wls_domain_home\ses_domain_name\bin\stopManagedWebLogic ses_server_name  
admin_URL user_name password
```

The parameters *admin_URL*, *user_name*, and *password* are optional parameters.

- c. Shut down WebLogic Server using the following command on Linux and UNIX systems:

```
wls_domain_home/ses_domain_name/bin/stopWebLogic.sh
```

On Windows system, use the command:

```
wls_domain_home\ses_domain_name\bin\stopWebLogic
```

4. Shut down Oracle Enterprise Manager. You can skip this step, if you have installed Oracle SES 11.2.2.2 software along with the database and the middle tier.

To check if Oracle Enterprise Manager is running or not, execute the following command on Linux and UNIX systems:

```
ORACLE_HOME/bin/emctl status dbconsole
```

On Windows system, use the following command:

```
ORACLE_HOME\bin\emctl status dbconsole
```

If the output of this command contains the text "Oracle Enterprise Manager 11g is running.", then execute the following command to shut down Oracle Enterprise Manager on Linux and UNIX systems:

```
ORACLE_HOME/bin/emctl stop dbconsole
```

On Windows system, use the command:

```
ORACLE_HOME\bin\emctl stop dbconsole
```

5. Shut down Oracle SES database instance using the SQL*Plus `shutdown` command after logging in as `sys` user.

On Linux and UNIX systems, connect to the database as `sys` user using the command:

```
ORACLE_HOME/bin/sqlplus "sys/password as sysdba"
```

On Windows system, use the command:

```
ORACLE_HOME\bin\sqlplus "sys/password as sysdba"
```

Shutdown the database instance using the command:

```
SQL> shutdown;
```

6. Upgrade to Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2.

 **Note:**

While upgrading to Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2, specify the listener port of the old database instance, that is of the Oracle Database 11.2.0.3 instance.

Note that if you select "perform typical configuration" on the Oracle Net Configuration Assistant Welcome page during the database upgrade, the upgraded Oracle Database instance will use a different database listener port than that of the old Oracle Database instance. In this case, you will have to manually configure the database listener port to the one used by the old Oracle Database instance.

 **See Also:**

- To upgrade to Oracle Database 11.2.0.4, see [Oracle Database 11.2.0.4 Upgrade Guide](#)
- To upgrade to Oracle Database 12.1.0.2, see [Oracle Database 12.1.0.2 Upgrade Guide](#)

7. Apply the Oracle Database patches.

- For Oracle Database 11.2.0.4 upgrade:
 - For Linux and UNIX systems, install the Oracle Text 11.2.0.4 patches 20882647, 13073613, and 19249319. Apply these patches using the Oracle OPatch utility.
 - For Windows system, install the Windows DB bundle patch 11.2.0.4.8 (patch 19192715).
- For Oracle Database 12.1.0.2 upgrade:
 - For Linux and UNIX systems, install the Oracle Database 12.1.0.2 patches 20551194, 19441649, 19542097, and PSU 12.1.0.2.3 (patch 20299023) or later. Apply these patches using the Oracle OPatch utility.
 - For Windows system, install the Oracle Database 12.1.0.2 patches 21551086, 19441649, and PSU 12.1.0.2.7 (patch 21126814) or later. Apply these patches using the Oracle OPatch utility.

8. Apply the Oracle SES 11.2.2.2 patches mentioned in the section "[Mandatory Software Patches](#) (page 1)".

9. If you have installed Oracle SES 11.2.2.2 along with the database and the middle tier, and if you have performed out-of-place upgrade for Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2, then execute the following steps.

- a. On Linux and UNIX systems, open the file `ses_home/bin/searchctl` in a text editor.

On Windows system, open the file `ses_home\bin\searchctl.bat` in a text editor.

- b. Replace the value for `DB_ORACLE_HOME` parameter with the full directory path of Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2 installation, that is, with the value of `ORACLE_HOME` environment variable.

Example:

- For Oracle Database 11.2.0.4 upgrade, replace the value for `DB_ORACLE_HOME` parameter with `/host/app/oracle/product/11.2.0/sesdb_11.2.0.4`.
- For Oracle Database 12.1.0.2 upgrade, replace the value for `DB_ORACLE_HOME` parameter with `/host/app/oracle/product/12.1.0/sesdb_12.1.0.2`.

10. If you had shut down Oracle Enterprise Manager in step 4, then restart it. You can skip this step, if you have installed Oracle SES 11.2.2.2 software along with the database and the middle tier.

On Linux and UNIX systems, use the command:

```
ORACLE_HOME/bin/emctl start dbconsole
```

On Windows system, use the command:

```
ORACLE_HOME\bin\emctl start dbconsole
```

11. Start Oracle SES 11.2.2.2 instance.



See Also:

Section “Starting and Stopping Oracle SES Instance” in the [Oracle Secure Enterprise Search Installation and Upgrade Guide](#) for the appropriate platform.

Changed Features

This section describes changed features in this release. This section contains the following topics:

- [Supported Document Types](#) (page 8)
- [Architectural Enhancements](#) (page 9)
- [Using searchctl Command](#) (page 10)
- [Administrator User Name](#) (page 10)
- [Oracle SES and Oracle WebCenter](#) (page 10)

Supported Document Types

The following document types are *not* supported in this release, because there is no MIME media types associated with these document type formats as published by Internet Assigned Numbers Authority (IANA) on its website <https://www.iana.org/assignments/media-types/media-types.xhtml>.

- IBM Lotus Symphony 1.2 (Documents, Presentations, Spreadsheets)
- IBM Lotus Notes Domino XML Language DXL

 **See Also:**

[Oracle Text Reference](#) for the complete list of document types supported by Oracle SES.

Architectural Enhancements

- You can install Oracle SES 11.2.2.2 software using either the Oracle Universal Installer (OUI) or the command line installer (silent installation) in one of the following three modes:
 - **Install Oracle SES along with the database and the middle tier**

This option installs Oracle SES 11.2.2.2, Oracle Database 11.2.0.3.0, and Oracle WebLogic Server 10.3.6.0.0 middle tier on a system.
 - **Install Oracle SES along with the middle tier on an existing database**

This option installs Oracle SES 11.2.2.2 and Oracle WebLogic Server 10.3.6.0.0 middle tier on a system. You must have already installed Oracle Database 11.2.0.3.x (Enterprise Edition) or Oracle Database 11.2.0.4.x (Enterprise Edition) or Oracle Database 12.1.0.2 (Enterprise Edition) on a system in the same network where Oracle SES is installed.
 - **Install Oracle SES on an existing database and a middle tier**

This option installs only Oracle SES 11.2.2.2 on a system. You must have already installed the following software:

 - * Oracle WebLogic Server 10.3.6.0.x version installed on the same system where Oracle SES is installed.
 - * Oracle Database 11.2.0.3.x (Enterprise Edition) or Oracle Database 11.2.0.4.x (Enterprise Edition) or Oracle Database 12.1.0.2 (Enterprise Edition) installed on a system in the same network where Oracle SES is installed.
- The Oracle SES middle tier is not installed under the Oracle Database home directory in this release.

 **See Also:**

Section “Important Oracle SES Directories” in the [Oracle Secure Enterprise Search Installation and Upgrade Guide](#) for the appropriate platform for more information about the locations of various important directories of the Oracle SES software.

- Oracle SES 11.2.2.2 supports open architecture, that is, an Oracle SES application can have multiple middle tier components across multiple systems.

Therefore, you must ensure that the custom plug-in jar files are accessible across all the Oracle SES instance middle tiers.

In the earlier Oracle SES release, a custom plug-in jar file was required to be stored in the `ses_home/search/lib/plugins` directory, but this is not required in the current Oracle SES release. You can now store a custom plug-in jar file in any directory, but you must refer it using its absolute file path in the Oracle SES application.

Using searchctl Command

You can now use the `searchctl` command only when both the Oracle Database and the WebLogic Server middle tier are installed as part of the Oracle SES software installation.

Administrator User Name

Oracle SES administrator user name is `SEARCHSYS` in this release. For the earlier Oracle SES release (11.1.2.2), the administrator user name was `EQSYS`.

Oracle SES and Oracle WebCenter

Oracle WebCenter includes a limited use license of Oracle SES. In the context of Oracle WebCenter, Oracle SES has also been certified with Oracle Unified Directory (OUD).



See Also:

[Oracle Fusion Middleware 11g Release 1 Certification Matrix](#)

Desupported Features

This section describes the features and functionality that is desupported in this release. This section contains the following topics:

- [Deprecated Configuration Files](#) (page 10)
- [Deprecated Data Sources](#) (page 11)
- [Backup and Recovery Using Administration GUI](#) (page 11)
- [Changing the Administrator Password Using Administration GUI](#) (page 12)
- [Deploying Oracle SES Instance as a Portlet](#) (page 11)
- [Disk Space Management](#) (page 11)

Deprecated Configuration Files

The following configuration files that were used in the earlier Oracle SES release (11.1.2.2) are no longer used in this release, and you can now configure these settings using either the Administration GUI or the Administration API:

- crawler.dat
- search.properties
- drivers.properties
- ranking.xml
- QueryPlan.xml

Deprecated Data Sources

The following data sources are not supported in this release:

- FileNet Content Engine
- FileNet Image Services
- Hummingbird
- IBM DB2
- Open Text Livelink
- EMC Documentum eRoom

Backup and Recovery Using Administration GUI

The Oracle SES Administration GUI does not provide backup and recovery operations in this release.



See Also:

Section "Performing Backup and Recovery" of *Oracle Secure Enterprise Search Administrator's Guide* for more information about the backup and recovery functionality provided by Oracle SES.

Deploying Oracle SES Instance as a Portlet

Oracle SES instance cannot be deployed as a portlet in this release.

Disk Space Management

The Oracle SES crawler log directory and the cache directory cannot be configured in this release. The pre-seeded storage area entries for these directories are not supported. The Administration API objects for disk space management - `alert`, `spaceCalculator`, and `tasks` - are also not supported in this release.

Changing the Administrator Password Using Administration GUI

In this release, Oracle SES administrator is a WebLogic Server identity store user, and hence the administrator password can be changed only by using the standard interface provided by the WebLogic Server. You now cannot change the administrator password using the Oracle SES Administration GUI.

See Also:

Section "Changing the Administrator Password" of *Oracle Secure Enterprise Search Administrator's Guide*

Open Bugs

This section provides the description and workaround for the known bugs in this Oracle SES release.

23222475: SES 11.2.2.2 INTALLATION ON WINDOWS 2012 R2 FAILS WITH "UNSUPPORTED OS DISTRIBUTION" ERROR

SES 11.2.2.2 installation on Windows 2012 R2 fails with the following error message:

```
Environment does not meet minimum requirements: Unsupported OS distribution.  
CAUSE: Minimum requirements were not met for this environment
```

Workaround: Run the SES 11.2.2.2 installer on Windows 2012 R2 system using the following command:

```
setup.exe -ignorePrereq -ignoreSysPreReqs -debug
```

7294661: CRAWLER FAILS WHILE PROCESSING LHA FORMAT FILES

Crawling of LHA format files is supported in this release. The crawler fails while processing the LHA format files when it cannot find the libraries for processing the LHA format content.

Workaround: You must download and deploy the libraries that can process the LHA format content.

14386424: ERROR WHILE QUERING E-MAIL SOURCE AND MAILING LIST SOURCE

The search results are not displayed properly while querying E-mail source and Mailing List source.

Workaround:

- For E-mail source: The E-mail archive directory specified during E-mail source creation must be accessible to the database system as well as to the middle tier system.

- For Mailing List source: You must create the directory `data/cache/mail` under Oracle home on the system where database is installed.

16771801: MAILING LIST E-MAILS ARE NOT SEARCHABLE AFTER FORCE RECRAWL

When the Crawler Recrawl Policy for source of Mailing List type is configured to Processing All Documents, then after the crawl of this source, all previously crawled e-mails are not available for searching.

Workaround: Contact Oracle Support to get the patch for this issue. The patch must be applied before running the crawl for a mailing list source in FORCE recrawl mode.

17010559: ORACLE SES 11.2.2.2 UPGRADED ENVIRONMENT SHOWS SEARCHABLE DATA AS 0 MB

After you upgrade from Oracle SES 11.1.2.2 to Oracle SES 11.2.2.2, the query truncation and instance statistics computation may not execute as scheduled if its original job status is not `SCHEDULED`.

Workaround: Execute the following steps:

1. Connect to the Oracle SES 11.2.2.2 database as Oracle SES administrator using `sqlplus`.

```
oracle_home/bin/sqlplus searchsys/SES_admin_password
```

2. Run the following SQL script, which will clean up and reset the Oracle SES jobs:

```
col ji_process_status format a15

select JI_ID,JI_TYPE,JI_JOB_NO,ji_process_status from eq$job_info order
byji_type;
begin
  eq_adm.use_instance(1);
  -- drop obsolete jobs
  for j in (select ji_id from eq$job_info where ji_type in (6,12,13,14,16))
  loop
    eq_job.drop_job(j.ji_id);
  end loop;
  -- reset all jobs
  for j in (select ji_id,ji_process_status from eq$job_info where ji_typenot in
(1,3))
  loop
    eq_job.disable_job(j.ji_id);
    -- enable jobs that are not disabled
    if j.ji_process_status<> 'DISABLED' then
      eq_job.enable_job(j.ji_id);
    end if;
  end loop;
exception
  when others then
    eq_err.text_on_stack(sqlerrm);
    raise;
end;
/
select JI_ID,JI_TYPE,JI_JOB_NO,ji_process_status from eq$job_info order
byji_type;
```

17672708: INSTALLATION ERROR FOR CERTAIN PASSWORD VALUE PATTERNS SPECIFIED FOR ORACLE SES DATABASE SCHEMA

Oracle SES software installation fails if the Oracle SES database schema password specified during the software installation contains any of the following characters:

- Multi-byte character
- Starting with number or special character and containing alphabetical character. For example: 123abc, #abc, and 123dc\$.
- Character other than alphabetical character, number, and special character. For example: >, @, and space character.

The following is the error message that is displayed in the log file in this scenario:

```
ORA-00922: missing or invalid option
```

Workaround: Avoid using the above mentioned characters in the Oracle SES database schema password.

See Also:

Oracle Database Security Guide for guidelines for specifying Oracle Database schema password

18141781: QUERY WEB SERVICE API OracleSearchResult.getAltKeywords DOES NOT RETURN MULTIPLE KEYWORDS FORMAT STRING

The multiple alternative keywords feature is disabled by default in Oracle SES and the configuration setting `ses.qapp.multiple_alternate_keywords` cannot be used to enable this feature in the current SES release.

Workaround: To enable multiple alternative keywords feature in Oracle SES, log into the Oracle SES database as `searchsys` user using SQL Plus, and run the following commands:

```
SQL> exec eq_adm.use_instance(1);
SQL> exec eq_query_adm.set_sys_admin_param('SA_MULTIPLE_ALT_KEYWORDS','true');
SQL> exec eq_query_adm.increment_sequence_version(eq_adm.METADATA_VER,1);
```

18302520: DOCUMENT NOT INDEXED ON ERROR PROCESSING AN ATTACHMENT

If there is any error while processing one or more attachments of a document being crawled, then that document is not indexed in Oracle SES database, and hence it is not available for searching.

Workaround: The information about the cause of error while processing the attachment for the document being crawled is logged in the crawler log file. Rectifying this error by analyzing the log error message and then re-crawling the document will resolve this issue.

18451275: FILE SYSCTL.CONF MUST HAVE READ ACCESS FOR THE USER PERFORMING THE SES INSTALLATION ON LINUX SYSTEM

When installing Oracle SES on a Linux system, the Oracle SES installer reads the `/etc/sysctl.conf` file for determining the OS kernel parameters that are prerequisites for Oracle SES software installation. If the user installing Oracle SES software does not have read permission for this file, then the Oracle SES installer will not be able to execute these prerequisite checks.

Workaround: Before installing Oracle SES software on a Linux system, provide read permission to the file `/etc/sysctl.conf` to the user who is going to install the Oracle SES software.

18554945: INVALID FACET PATH ERROR WHILE SEARCHING FOR STRING TYPE FACET

After upgrading to Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2, faceted search for string type facet does not work, if the facet value contains a space character at the end.

Workaround: There is no workaround for this issue.

19679982: CANNOT APPLY WEBLOGIC SERVER PSU PATCH 18040640 (T5F1)

Patch conflict occurs when applying the WebLogic Server PSU patch 18040640 (T5F1) on the WebLogic Server instance for Oracle SES 11.2.2.2. This patch conflict occurs because the WebLogic Server shipped along with the Oracle SES 11.2.2.2 software has SLMA patch that conflicts with the PSU patch 18040640 (T5F1).

Workaround: WebLogic Server PSU patch 18040640 (T5F1) is a super set of WebLogic Server SLMA patch. Hence, you must first rollback the SLMA patch and then apply the PSU patch 18040640 (T5F1) for the Oracle Server instance on Oracle SES 11.2.2.2 installation. The following are the steps to achieve this:

1. Go to `MW_HOME/utils/bsu` directory and run the `bsu` script. The Oracle Smart Update window is displayed.
2. Click the **remove** icon for the SLMA patch.
3. Click **OK** on the confirmation dialog box.
4. Apply the WebLogic Server PSU patch 18040640 (T5F1) by following the instructions in the patch readme file.

19679982: CANNOT LOGIN TO ADMINISTRATION GUI AFTER APPLYING THE WEBLOGIC SERVER PSU PATCH 18040640 (T5F1)

After applying the WebLogic Server PSU patch 18040640 (T5F1) on the Oracle WebLogic Server instance for Oracle SES 11.2.2.2, you cannot login to Oracle SES Administration GUI. This issue occurs when the PSU patch 18040640 (T5F1) is not granted appropriate permissions.

Workaround: The following are the steps to grant appropriate permissions to the PSU patch 18040640 (T5F1) using Oracle Enterprise Manager:

1. In the Oracle Enterprise Manager console, expand WebLogic Domain, and select the Oracle SES domain that was created during the Oracle SES 11.2.2.2 installation.

2. In the **Weblogic Domain** list box, select **Security and System Policies**. The page for searching security setup is displayed.
3. In the search security setup page, select **Starts With** and click the arrow icon beside the text box. The list of existing security setups is displayed.
4. Click the **Create** button to create a new security setup entry.
5. For the code base field, specify the location of the patch files for the WebLogic Server instance. For example:

```
file:ORACLE_HOME/patch_wls1036/patch_jars/*
```

Specify the complete directory path for *ORACLE_HOME*.

6. Click the **Add** button.
7. On the popup window, select **Principal** type and click **Select here to enter details for a new permission** link.
8. For the **Permission Class** text box, enter the value `oracle.security.jps.JpsPermission`. For the **Resource Name** text box, enter the value `AppSecurityContext.setApplicationID.*`. Leave the **Permission Action** text box blank.
9. Click **OK**.
10. Restart the Oracle SES instance.

1919928: AFTER APPLYING THE WEBLOGIC SERVER 10.3.6.0.8 PSU, THE ERROR MESSAGE "PERMISSION DENIED" IS DISPLAYED WHEN CREATING A DATA SOURCE

After applying the WebLogic Server 10.3.6.0.8 PSU for Oracle SES 11.2.2.2, you may get the error message "Permission denied" when creating a data source using Administration GUI. This issue occurs when the WebLogic Server 10.3.6.0.8 PSU is not granted appropriate permissions.

Workaround: Execute the steps mentioned as a workaround for the issue "19679982: CANNOT LOGIN TO ADMINISTRATION GUI AFTER APPLYING THE WEBLOGIC SERVER PSU PATCH 18040640 (T5F1)".

20847809: REPOSITORY CREATION UTILITY FAILS WHEN INSTALLING ORACLE SES 11.2.2.2 ALONG WITH THE DATABASE AND THE MIDDLE TIER ON WINDOWS SERVER 2012 R2 SYSTEM

When installing Oracle SES 11.2.2.2 along with the database and the middle tier on a Windows Server 2012 R2 system, the following error message is displayed by the Oracle SES installer:

```
[INS-20802] Repository Creation Utility failed.
```

Workaround: Set the Windows system environment variable `JAVA_TOOL_OPTIONS` to `-Djava.net.preferIPv6Addresses=true` and restart the Oracle SES 11.2.2.2 installation process.

22064792: INDEX FRAGMENTATION VALUES SHOWN ON THE ADMINISTRATION GUI ARE INCONSISTENT

The index fragmentation values shown on the **Global Settings > Index Optimization** page of the Administration GUI vary drastically whenever this page is accessed. This happens when event 10013 is enabled, which makes Oracle SES to calculate the index fragmentation ratio based on few sampled tokens and not all the tokens.

Workaround: Disabling event 10013 makes Oracle SES to calculate the index fragmentation ratio based on all the tokens, thus improving the accuracy of calculating the fragmentation ratio. Note that this may slow down the crawler process and search queries.

21151876: ORACLE SES QUERY FAILS WITH ERROR MESSAGE "NEGATIVE QUERY IS NOT SUPPORTED"

When an Oracle SES query contains a compulsory exclusion operator "-" without any positive search term before it, the query operation fails with the error message "negative query is not supported". For example, the query "A & (-B | C)" is not a valid query and it fails with the error message, because "-B" in this query does not have a positive search term before it. The correct way to write this query is "(A -B) | (A & C)".

Workaround: Write the query in such a way that the compulsory exclusion operator in the query has a positive search term before it.

20018779: ERROR CRAWLING FTP ATTACHMENT FILE WHEN THE FILE NAME CONTAINS NON-ASCII CHARACTERS

If a file attachment has a non-ASCII character in its file name, then Oracle SES crawler fails to retrieve the attachment using FTP protocol if the FTP server does not support UTF-8 character encoding. This issue occurs because the character encoding of FTP connection is automatically set to UTF-8 for the crawler when it is not explicitly set to any value using the event 18006 (that is, when the event 18006 is not enabled).

Workaround: Set the character encoding of FTP connection for the crawler to the same value as that of the FTP server using the event 18006. For example:

```
SQL> exec eq_adm.use_instance(1);
SQL> exec eq_util.set_event('18006', '<character encoding of the FTP server>');
```

Note:

- If the value of 'default' is specified as the character encoding of the FTP connection for the crawler using the event 18006, then the FTP client's default character encoding is used by the crawler to connect to the FTP server.
- The event 18006 can be disabled using the following SQL statements:

```
SQL> exec eq_adm.use_instance(1);
SQL> exec eq_util.set_event(18006, null);
```

In this case, UTF-8 character encoding is used by the crawler.

- Oracle SES uses the Java API method `java.nio.charset.Charset.isSupported()` to determine whether the character encoding specified is a valid value.

 **See Also:**

- [Java SE documentation](#) for the list of valid character encodings
- [Java API documentation](#) for more information about the Java class `java.nio.charset.Charset`

Documentation Corrections and Additions

This section contains corrections to the following Oracle SES documents:

- [Oracle Secure Enterprise Search Administration GUI Online Help](#) (page 18)
- [Oracle Secure Enterprise Search Administrator's Guide](#) (page 20)
- [Oracle Secure Enterprise Search Java API Reference](#) (page 25)

Oracle Secure Enterprise Search Administration GUI Online Help

Configuring Similar Document Handling Settings

The Administration GUI online Help for the **Global Settings - Query UI Configuration** page should include the following information for the **Similar Document Handling** parameter:

Similar Document Handling

Specify how similar documents should be handled. Select one of the following options:

- **Detect:** Similar documents detection is enabled, and search results show similar documents only when the **Similar Documents** link is clicked. Duplicate documents are not shown in search results.
- **Remove:** Similar documents detection is enabled, and similar as well as duplicate documents are not shown in search results.
- **Disabled:** Similar documents detection is disabled. Search results shows all the documents, including similar and duplicate documents. Select this option to minimize the discrepancy between the facet search result count and the normal search result count.

Configuring Relevancy Tuning Option - Forced Ranking

The Administration GUI online Help for the **Search - Relevancy - Forced Ranking** page should include the following information:

Forced Ranking

Specify how similar documents should be handled. Select one of the following options:

- **Detect:** Similar documents detection is enabled, and search results show similar documents only when the **Similar Documents** link is clicked. Duplicate documents are not shown in search results.

- **Remove:** Similar documents detection is enabled, and similar as well as duplicate documents are not shown in search results.
- **Disabled:** Similar documents detection is disabled. Search results shows all the documents, including similar and duplicate documents. Select this option to minimize the discrepancy between the facet search result count and the normal search result count.

Crawler Statistics Displayed on the Crawler Process Summary Page

The Administration GUI online Help for the **Home - Schedules - Crawler Process Summary** page should contain the following information.

- **Documents Processed:** Number of documents retrieved by the crawler. Many of these documents may not have been queued for indexing yet.
- **Documents Discovered:** Total number of documents discovered so far. This is roughly equal to:

$$[\text{documents processed}] + [\text{documents to process}] + [\text{document processing failures}] + [\text{documents excluded}]$$

In an RSS-based connector crawl like UCM, the number of documents or items from a data feed correspond to the number of documents discovered regardless of the operations performed on them. This assumes that all of the data feed items are valid, that is, they have valid display URLs and so on.
- **Documents to Process:** Number of URLs in the queue waiting to be crawled.
- **Documents Deleted:** Number of document deleted during incremental recrawl.
- **Document Processing Failures:** Number of documents whose contents cannot be retrieved by the crawler. This could be due to an inability to connect to the website, slow server response time causing time-outs, or authorization requirements. Problems encountered after successfully fetching the document are not considered here; for example, documents that are too big or duplicate documents that were ignored.
- **Documents Excluded:** Number of URL links encountered but not considered for crawling. The reason for excluding these documents could be due to boundary rules, the robots exclusion rule, the mime type inclusion rule, the crawling depth limit, or the URL rewriter discard directive.
- **Documents Non-Indexable:** Number of documents that cannot be indexed; for example, a file source directory or a document with robots NOINDEX meta-tag.
- **Document Conversion Failures:** Number of binary documents that could not be converted to HTML. Though the filtering operation is failed for these documents, their metadata is submitted to the Oracle SES indexing engine (that is, Oracle Text) for indexing purpose. This document count is included in the "Documents Queued for Index" statistic.
- **Conversion Failures in Archives:** Number of archived/zipped documents with conversion failures. Conversion failure of each document inside a zip file is counted as one document failure.
- **Documents Queued for Index:** Number of documents that are pending to be indexed, that is, number of documents that are submitted to the Oracle SES

indexing engine (that is, Oracle Text) for the indexing purpose and are yet to be indexed.

- **Documents Indexed:** Number of documents that have been indexed.

Oracle Secure Enterprise Search Administrator's Guide

Oracle SES Query Web Service API - targetDocIdList Parameter Values of doOracleFetchSearch API Must Contain a Dot (.) as a Suffix

The Oracle SES Query Web service API `doOracleFetchSearch` has a parameter `targetDocIdList`, which should be assigned a list of document IDs. A document ID has the following format:

<Document ID>.<One or more federation source IDs separated by underscore>

For example, "777.2_3", "316.3", and "721.2". If a document ID represents a document from a non-federated source, then a dot (.) must be added to the document ID as a suffix. For example, "264468."

Oracle SES Query Web Service API - facetPaths parameter of doOracleFacetSearch() and getFacetNodes() methods can be used for specifying per-facet limits

You can specify per-facet limits, such as `returnFacetDocCount`, `minFacetDocCount`, `maxFacetChildren`, and `sortBy` - as comma separated name-value pairs in the facet path string of the `facetPaths` parameter of the Oracle SES Query Web Service API methods - `doOracleFacetSearch()` and `getFacetNodes()`.

For example:

```
facetPaths[0] = Facet=Location, Path=Location/California, minFacetDocCount=1,
maxFacetChildren=5, returnFacetDocCount=true, sortBy=ALPHA_ASC
```

```
facetPaths[1] = Facet=Food, Path=Food/Vegetable/Cabbage, minFacetDocCount=1,
maxFacetChildren=5, returnFacetDocCount=true, sortBy= ALPHA_ASC
```

```
facetPaths[2] = Facet=Author, Path=Author, minFacetDocCount=1, maxFacetChildren=10,
returnFacetDocCount=true, sortBy=COUNT_DES
```

You can also specify per-request facet limits using separate parameters - `returnFacetDocCount`, `minFacetDocCount`, `maxFacetChildren`, and `sortBy` - of the `doOracleFacetSearch()` and `getFacetNodes()` API methods. Per-facet limits take precedence over per-request facet limits. If these facet limits are not specified at per-facet level as well as at per-request level, then default values are used for the facet limits.

 **Note:**

If a facet path parameter value has either character "=" or character "," in it, then that value must be enclosed in double quotes. If a parameter value contains any double quote character, then the backslash character "\" should be used to escape the double quote character.

For example:

```
Facet="Price, \"random\""
```

Configuring Single Sign-On for Oracle SES using Oracle Access Manager 11g

The Oracle SES Administrator's Guide contains information about implementing single sign-on (SSO) authentication for Oracle SES using Oracle Access Manager (OAM) version **10g**. This section describes how to configure Oracle SES for SSO authentication using OAM version **11g**.

 **See Also:**

Oracle Secure Enterprise Search Administrator's Guide for information about implementing SSO authentication for Oracle SES using Oracle Access Manager (OAM) version **10g**

 **Note:**

- If you protect the Oracle SES instance using OAM SSO, then it is recommended to protect both the Oracle SES applications - Administration application and Query application.
- If you chose to protect only one of the Oracle SES applications using OAM SSO, that is, either the Administration application and or the Query application, then you must configure the logout URL parameter for the *unprotected* application using either the Administration GUI or the Administration API.

For example, if the Administration application is *unprotected*, then the Administration URL must be set to be *excluded* from OAM resource, and the Administration Logout URL must be set to a non-SSO logout URL, such as `/search/admin/control/logout.jsp`.

- If you protect the Administration application using OAM SSO and use OID as identity store, then you must either add the `searchsys` user to OID identity store, or grant the `SearchAdminSuperUserRole` role to an existing user in OID identity store. Also, configure the appropriate Administration logout URL for SSO.

Ensure that the following components are installed:

- **Oracle Access Manager 11g**

Install and configure OAM 11g as described in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

To configure OAM 11g to use an external identity store, such as OID, see the "Registering a New User Identity Store" section of the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

- **Oracle HTTP Server (OHS) 11g**

See "Installing and Configuring Oracle Web Tier" section of the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

- **WebGate**

See "Installing and Configuring Oracle HTTP Server 11g Webgate for OAM" section of the *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.

To implement the OAM 11g SSO authentication for Oracle SES, you must configure OHS, Oracle SES, and OAM. Configure OID as well, if it is used as identity store.

To configure OAM 11g SSO for Oracle SES:

1. Execute the following steps described in the section "Configuring Secure Search with Oracle Access Manager Single Sign-On" of *Oracle Secure Enterprise Search Administrator's Guide*:

- a. Add OAM Identity Asserter
- b. Add OID Authenticator, if OID is used as identity store
- c. Configure Oracle HTTP Server
- d. Install and Configure WebGate

2. Register Webgate agent and resources:

- a. Navigate to the directory `<RREG_Home>/input`, where `<RREG_Home>` is `<OAM_ORACLE_HOME>/oam/server/rreg`.
- b. Create SES OAM configuration file `<RREG_HOME>/input/ses.oam.conf` with the following information:

```
#####  
protected_uris  
#####  
/search/query/formlogin.uix  
/search/admin  
#####  
public_uris  
#####  
/monitor  
/search/ohw  
/search/query
```

- c. Create a new file named `SESOAM11gRequest.xml` in the `<RREG_Home>/input` directory to serve as a parameter file to the `oamreg` tool. In the following example, replace `$$oam...$$` with the OAM host and OAM administration

server port. In this example, `SESAccessGate` is the agent name and host identifier. You can provide any other name for it.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
Copyright (c) 2009, 2010, Oracle and/or its affiliates. All rights reserved.
NAME: OAM11GRequest_short.xml - Template for OAM 11G Agent Registration
Request file (Shorter version - Only mandatory values - Default values will
be used for all other fields) DESCRIPTION: Modify with specific values and
pass file as input to the tool.
-->

<OAM11GRegRequest>
<serverAddress>http://$oamhost$$:$oamadminserverport$$</serverAddress>
  <hostIdentifier>SESAccessGate</hostIdentifier>
  <agentName>SESAccessGate</agentName>
  <logOutUrls>
    <url>/oamssso/logout.html</url>
  </logOutUrls>
</OAM11GRegRequest>
```

- d. Navigate to directory `<RREG_Home>` and run the following command:

```
export JAVA_HOME=<JDK Home Directory>
```

where, `<JDK Home Directory>` is the directory where JDK is installed, for example `/etc/jdk6`.

- e. Run the following command:

```
<RREG_Home>/bin/oamreg.sh inband input/SESOAM11gRequest.xml
```

When prompted for agent credentials, enter your OAM administrator credentials and your WebGate password. Enter `yes` when asked whether you want to import a URIs file. Specify the full path of the `<RREG_HOME>/input/ses.oam.conf` file you created earlier. You should see the output similar to the one shown below, when the registration is successful:

```
JAVA_HOME=/ade/aimel_adc00qib/jdk7
CLASSPATH=...
OAM_REG_HOME=/scratch/aimel/work/mw4597/idm9376/oam/server/rreg
-----
Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
Mode: inband
Filename: /scratch/aimel/work/mw4597/idm9376/oam/server/rreg/input/
SESOAM11gRequest.xml
Enter admin username:Username: weblogic
Enter password: Enter password: Password field taken in from System.in was
empty or null.
Webgate password field is empty.
-----
Request summary:
OAM11G Agent Name: SESAccessGate
URL String:null
Registering in Mode:inband
Your registration request is being sent to the Admin server at: http://
example.com:7001
-----
```

Inband registration process completed successfully! Output artifacts are created in the output folder.

- f. Copy the generated files and artifacts (ObAccessClient.xml and cwallet.sso) from the <RREG_Home>/output/SESAccessGate directory to your WebGate instance configuration directory <Webgate_Instance_Directory>/webgate/config. Note that <Webgate_Instance_Directory> should match the instance home of OHS, as shown in the following example:

```
<MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config
```

- g. Verify the following information in the OAM Console:

- i) You should be able to see the following artifacts:

- 11g WebGate agent named SESAccessGate

- 11g host identifier by the same name

- an application domain with the same name containing authentication and authorization policies which in turn contain protected and public policies

- ii) Navigate to **Application Domain > SESAccessGate > Authentication Policies**. You should be able to see the following policies:

- Protected Resource Policy

- Public Resource Policy

- iii) Open the **Protected Resource Policy** and make sure that the **Authentication Scheme** is set to LDAPScheme. The LDAPScheme is configured when OAM is installed.

- h. Restart OHS.

3. Enable the OAM SSO functionality using the Oracle SES Administration GUI by navigating to **Global Settings > Configure Single Sign-On**, selecting the OAM option, and clicking **Activate**.

4. Enter the following parameter values for OAM SSO:

- Admin logout return URL: Specify the URL to display after logging out of the administration application.
- Query invalid session return URL: Specify the URL to display when the query application session expires.
- Query logout return URL: Specify the URL to display after logging out of the query application. Specify this URL format depending upon the WebGate version.

 **Note:**

The format of the logout return URLs for Administration and Query applications must be as follows:

- For **WebGate 10g**, the format of the logout return URL is:

```
/oamsso/logout.html?end_url=return_url
```

where, *return_url* is the page that is displayed after logging out of the application. For example, to return to the Query application page, set *return_url* to */search/query*, and to return to the Administration application page, set *return_url* to */search/admin*.

- For **WebGate 11g**, the format of the logout return URL is:

```
oam_logout_url?end_url=return_url
```

where, *oam_logout_url* is the OAM logout URL. For example, `http://oam_server_host:oam_server_port/oam/server/logout`.

return_url is the page that is displayed after logging out of the application. For example, to return to the Query application page, set *return_url* to `http://ses_host:ses_port/search/query`, and to return to the Administration application page, set *return_url* to `http://ses_host:ses_port/search/admin`.

5. Verify the OAM SSO functionality using the Oracle SES Administration application `http://OHS_HOST:OHS_HTTP_PORT/search/admin`, and Oracle SES Query application `http://OHS_HOST:OHS_HTTP_PORT/search/query`.

 **Note:**

When OAM is configured to use an external identity store, such as OID, then Oracle SES should use the same identity store. Add two additional users to the identity store - `SEARCHSYS` and `FUSION_APPS_SEARCH_APPID`, which are specific to Oracle SES.

Oracle Secure Enterprise Search Java API Reference

OracleSearchService.logUserClick() API Method Not Supported

Oracle SES Java API method `OracleSearchService.logUserClick()` is not supported in this release.

Implementing High Availability for Oracle SES

To implement High Availability for Oracle SES 11.2.2.2, refer to the support note 1611280.1 on My Oracle Support website <https://support.oracle.com>. You can search for this support note on My Oracle Support website by entering the string **1611280.1** in the Global Search text box.

Documentation Accessibility

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

Access to Oracle Support

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

Oracle® Secure Enterprise Search Release Notes, 11g Release 2 (11.2.2.2)
E35074-53

Copyright © 2006, 2017, Oracle and/or its affiliates. All rights reserved.

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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