Oracle Commerce Guided Search Platform Services

Migration Guide

Version 11.2 • October 2015

ORACLE

COMMERCE

Contents

Copyright and disclaimer.....v
Preface.....7
About this guide.....7
Who should use this guide.....7
Conventions used in this guide.....7
Contacting Oracle Support.....8

Chapter 1: Upgrading Platform Services to Version 11.2.....9
About Oracle Commerce Guided Search.....9
About the documentation.....9
Recommended reading.....9
Upgrading from Platform Services 11.1.....10

Chapter 2: Required Changes.....13
Changes from 6.1.2 to 6.1.3.....13
The Endeca Control System is not supported.....13
The VOID ID_LANGUAGE expression is no longer supported.....13

Chapter 3: Behavioral Changes.....15
SSL Protocol Changes in 11.2.....15
Changes from 6.1.0 to 6.1.1.....18

Copyright and disclaimer

for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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

Oracle 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.

Preface

Oracle Commerce Guided Search is the most effective way for your customers to dynamically explore your storefront and find relevant and desired items quickly. An industry-leading faceted search and Guided Navigation solution, Guided Search enables businesses to influence customers in each step of their search experience. At the core of Guided Search is the MDEX Engine™, a hybrid search-analytical database specifically designed for high-performance exploration and discovery. The Oracle Commerce Content Acquisition System provides a set of extensible mechanisms to bring both structured data and unstructured content into the MDEX Engine from a variety of source systems. The Oracle Commerce Assembler dynamically assembles content from any resource and seamlessly combines it into results that can be rendered for display.

Oracle Commerce Experience Manager enables non-technical users to create, manage, and deliver targeted, relevant content to customers. With Experience Manager, you can combine unlimited variations of virtual product and customer data into personalized assortments of relevant products, promotions, and other content and display it to buyers in response to any search or facet refinement. Out-of-the-box templates and experience cartridges are provided for the most common use cases; technical teams can also use a software developer's kit to create custom cartridges.

About this guide

This guide describes the major tasks necessary to upgrade to Platform Services 11.2 from Platform Services 11.1.

Who should use this guide

This guide is intended for developers who are upgrading Oracle Commerce Guided Search, as well as for system administrators managing Oracle Commerce Guided Search on Windows, UNIX, Solaris, or Linux.

Note: Unless otherwise indicated, whenever this document specifies UNIX, it applies to Linux and Solaris as well.

Conventions used in this guide

This guide uses the following typographical conventions:

Code examples, inline references to code elements, file names, and user input are set in `monospace` font. In the case of long lines of code, or when inline monospace text occurs at the end of a line, the following symbol is used to show that the content continues on to the next line: ¬

When copying and pasting such examples, ensure that any occurrences of the symbol and the corresponding line break are deleted and any remaining space is closed up.

Contacting Oracle Support

Oracle Support provides registered users with answers to implementation questions, product and solution help, and important news and updates about Guided Search software.

You can contact Oracle Support through the My Oracle Support site at *https://support.oracle.com*.

Chapter 1

Upgrading Platform Services to Version 11.2

This section describes the steps that you must take to upgrade your version of Platform Services to version 11.2. After you complete the upgrade procedures described in this section, be sure to review this guide for any additional changes that may be required to upgrade your application.

About Oracle Commerce Guided Search

Oracle Commerce Guided Search consists of four primary components:

- Oracle Commerce MDEX Engine
- Oracle Commerce Guided Search Platform Services
- Oracle Commerce Guided Search Tools and Frameworks
- Oracle Commerce Content Acquisition System

Each component is upgraded individually. For more information about these packages, see the *Oracle Commerce Guided Search Getting Started Guide* available on the Oracle Technology Network.

About the documentation

Documentation for all components is available on the Oracle Technology Network (OTN) for viewing or download.

For a complete list of documents associated with each product, refer to the *Oracle Commerce Guided Search Getting Started Guide*, which is available on the Oracle Technology Network (OTN).

Recommended reading

In addition to reading this document, Oracle recommends that you read the following documents for important information about the release.

Release Announcement

The *Release Announcement* provides a brief explanation of the new features that were added in Version 11.2. The *Release Announcement* is available for download from the Oracle Technology Network.

Release Notes

The release notes for each package provide information about new features, changed features, and bug fixes for this release. You can download the release notes (`README.txt`) from the Oracle Technology Network. After installation, release notes are also available in the following location:

- Windows: `C:\Endeca\PlatformServices\<version>\README.txt`
- UNIX: `usr/local/endeca/PlatformServices/<version>/README.txt`

On Windows, you can also access the release notes from **Start > Programs > Endeca > Platform Services > Release Notes**.

Getting Started Guide

The *Oracle Commerce Guided Search Getting Started Guide* gives an overview of components and includes information about configuration scenarios. After installing all the components in your deployment, read this guide for information about how to verify your installation.

Upgrading from Platform Services 11.1

This procedure provides high-level steps needed to upgrade from Platform Services 11.1 to Platform Services 11.2.

The high-level procedure of upgrading a Platform Services 11.1 platform is:

1. Back up your EAC store.
2. Uninstall Platform Services 11.1.
3. Install Platform Services 11.2.
4. Restore the backed-up EAC store.
5. Upgrade other components as required.

Before installing upgraded versions of components, check the appropriate Installation Guide for the version that you are uninstalling for a list of environment variables used by all components, and ensure that any environment variables from previous installations are removed from your servers. This is because, on UNIX, when you uninstall the previous versions, the environment variables from the previous installations are not removed automatically.

Step 1: Back up your existing configuration

The EAC store contains application configuration.

Note: This step is necessary only if you are using EAC scripts to provision your application. Implementations relying on the Deployment Template do not need to back up the EAC store because the information is stored in the Deployment Template's `AppConfig.xml` file.

To back up the EAC store:

1. Stop the Oracle Commerce Guided Search HTTP Service if it is running.
2. Copy the `eacstore` directory from `%ENDECA_CONF%\state` (on Windows) or `$ENDECA_CONF/state/` (on UNIX) to another location.

Step 2: Uninstall Platform Services 11.1

Uninstall the software as documented in the 11.2 version of the *Oracle Commerce Guided Search Platform Services Installation Guide*.

Note: If you have the Oracle Commerce Document Conversion module, uninstall it before uninstalling Platform Services.

Step 3: Install Platform Services 11.2

Install Platform Services 11.2 as documented in the 11.2 version of the *Oracle Commerce Guided Search Platform Services Installation Guide*.

If you have purchased the Oracle Commerce Document Conversion module, install version 11.2.

Step 4: Restore the backed-up EAC store

To restore a backup of the EAC store on the Platform Services 11.1 location:

1. Stop the Oracle Commerce Guided Search HTTP Service if it is running.
2. If there is an `eacstore` directory in `%ENDECA_CONF%\state` (on Windows) or `$ENDECA_CONF/state/` (on UNIX), delete the directory.
3. Copy the backup `eacstore` directory into `%ENDECA_CONF%\state` (on Windows) or `$ENDECA_CONF/state/` (on UNIX).
4. Start the Oracle Commerce Guided Search HTTP Service.

Keep in mind that this step is necessary only if you used EAC scripts to provision your application in 11.1. Implementations relying on the Deployment Template do not need to back up or restore the EAC store.

Step 5: Upgrade other components

After you have upgraded to Platform Services 11.2, check your other components and upgrade them as necessary:

1. Upgrade the MDEX Engine to the latest version. For details, see the *Oracle Commerce Guided Search MDEX Engine Migration Guide* and the *Oracle Commerce Guided Search MDEX Engine Installation Guide*.
2. Upgrade Tools and Frameworks to version 11.2. For details, see the *Oracle Commerce Guided Search Workbench Migration Guide* and *Oracle Commerce Guided Search Workbench Installation Guide*.
3. Upgrade Developer Studio to version 11.2. For details, see the section "Upgrading a Developer Studio project" in this chapter.
4. Upgrade any other Guided Search packages to maintain compatibility among the components.

Chapter 2

Required Changes

You must make the changes specified in this section, if they apply to your application.

Changes from 6.1.2 to 6.1.3

This section describes changes to Platform Services that occurred between version 6.1.2 and 6.1.3.

The Endeca Control System is not supported

As part of the MDEX Engine 6.2.0 release, the Endeca Control System is unsupported. The Endeca Control System includes the Endeca JCD and the Control Interpreter, both of which have been deprecated since Endeca IAP 5.0.

You should use the Endeca Application Controller to control, manage, and monitor components in your implementation. For details, see the *Platform Services Application Controller Guide*.

The *Control System Guide* is no longer included in the Platform Services documentation set.

The `VOID ID_LANGUAGE` expression is no longer supported

The `VOID ID_LANGUAGE` expression was typically used in a Record Manipulator to identify the language of a specified property and then add a language identifier property to a record. This expression is no longer supported.

Chapter 3

Behavioral Changes

This section describes changes that do not require action on the developer's part, but will have an effect on how your application behaves after you upgrade.

SSL Protocol Changes in 11.2

In release 11.2 of Platform Services, the cryptographic protocols TLSv1.1 and TLSv1.2 are enabled by default. These protocols provide protection against serious security threats that have emerged recently. The protocols SSL 3.0 and TLS 1.0 do not provide similar protection and are disabled by default. Note that if you enable SSL 3.0 and TLS 1.0 -- for compatibility or any other reason -- you thereby make your application vulnerable to the serious threats against which TLSv1.1 and TLSv1.2 provide protection.

In `ENDECA_CONF/server.xml`, make sure that any non-SSL connector is commented and uncomment the following SSL connector:

```
<<Connector port="8443" maxHttpHeaderSize="8192" SSLEnabled="true"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="true" sslEnabledProtocols="TLSv1.1,TLSv1.2"
               keystoreFile="C:/Endeca/ToolsAndFrameworks/11.1.0/deployment_tem¬
plate~
                  /ssl_certs_utility/bin/ssl/hostname.ks" keystorePass="eacpass"

             truststoreFile="C:/Endeca/ToolsAndFrameworks/11.1.0/deployment_tem¬
plate~
                /ssl_certs_utility/bin/ssl/TS-hostname.ks" truststorePass="eac¬
pass"
               URIEncoding="UTF-8"/>
```

Steps to enable the SSL 3.0 and TLS 1.0 protocols for Platform Services

Note: If you enable SSL 3.0 and TLS 1.0 -- for compatibility or any other reason -- you thereby make your application vulnerable to the serious threats against which TLSv1.1 and TLSv1.2 provide protection.

To enable the SSL 3.0 protocol, follow these steps:

1. Open `server.xml` at `%ENDECA_TOOLS_ROOT%\server\workspace\conf`.

2. Change `sslEnabledProtocols` to `sslEnabledProtocols="SSLv3.0"` in the SSL connector.

```
<Connector port="8443" SSLEnabled="true"
   protocol="org.apache.coyote.http11.Http11Protocol"
   maxPostSize="0"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="true" sslEnabledProtocols="SSLv3"
   keystoreFile="cert.ks" keystorePass="eacpass"
   truststoreFile="ca.ks" truststorePass="eacpass"
   URIEncoding="UTF-8"
```

3. Open `java.security` file in `%ENDECA_TOOLS_ROOT%/server/j2sdk/jre/lib/security`.
4. Uncomment the `jdk.tls.disabledAlgorithms` property and disable all protocols except `SSLv3`: `"jdk.tls.disabledAlgorithms=TLSv1, TLSv1.1, TLSv1.2"`.
5. Restart the Tools and Frameworks server.

To enable the TLS 1.0 protocol, follow these steps:

1. Open `server.xml` at `%ENDECA_TOOLS_ROOT%\server\workspace\conf`.
2. Change `sslEnabledProtocols` to `sslEnabledProtocols="TLSv1"` in the SSL connector.

```
<Connector port="8443" SSLEnabled="true"
   protocol="org.apache.coyote.http11.Http11Protocol"
   maxPostSize="0"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="true" sslEnabledProtocols="TLSv1"
   keystoreFile="cert.ks" keystorePass="eacpass"
   truststoreFile="ca.ks" truststorePass="eacpass"
   URIEncoding="UTF-8"
```

3. Open `java.security` file in `%ENDECA_TOOLS_ROOT%/server/j2sdk/jre/lib/security`.
4. Uncomment the `jdk.tls.disabledAlgorithms` property and disable all other protocols except `TLSv1`:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1.1, TLSv1.2
```

5. Restart the Tools and Frameworks server.

Steps to enable the SSL 3.0 protocol for Forge

Note: When the SSLv3 protocol is enabled for Forge, it must also be enabled for both Platform Services and Tools and Frameworks.

1. Open `DataIngest.xml` file at *APP_NAME*`/config/script`.
2. Pass extra argument "-sslv3" in "args" argument for Forge component.

```
<forge id="Forge" host-id="ITLHost">
   <properties>
   <property name="numStateBackups" value="10" />
   <property name="numLogBackups" value="10" />
   </properties>
   <directories>
   <directory
    name="incomingDataDir">./data/incoming</directory>
   <directory name="configDir">./config/pipeline</directory>
   <directory
    name="wsTempDir">./data/workbench/temp</directory>
   </directories>
```

```
<args>
<arg>-vw</arg>
<arg>--sslv3</arg>
</args>
<log-dir>./logs/forges/Forge</log-dir>
<input-dir>./data/processing</input-dir>
<output-dir>./data/forge_output</output-dir>
<state-dir>./data/state</state-dir>
<temp-dir>./data/temp</temp-dir>
<num-partitions>1</num-partitions>

<pipeline-file>./data/processing/pipeline.epx</pipeline-file>
<ssl-config bean="sslConfig" ref="globalSslConfig"/>
<!--
<credentials-map>CREDENTIALS_MAP</credentials-map>
<jps-config-path>JPSCONFIG_LOCATION</jps-config-path>
<opss-jars-dir>OPSS_JARS_DIR</opss-jars-dir>
-->
</forge>
```

3. Modify the "globalSslConfig" in *APP_NAME*/config/script/AppConfig.xml file to pass the ciphers that are supported for Forge when SSLv3 protocol is enabled.
4. Verify that the warning message "SSLv3 is enabled" is logged in `apps\`*`APP_NAME`*`\logs\forges\Forge\Forge.log`.

Note: The following ciphers are supported for Forge when the SSLv3 protocol is enabled.

- AES128-sha
- RC4-md5
- RC4-sha

Parallel Forge

To enable SSLv3 during Parallel Forge execution, add `-sslv3` to the arguments while starting Forge as server and Forge as client.

Steps to enable the SSL 3.0 protocol for Log Server

Note: When the SSLv3 protocol is enabled for the Logserver, it must also be enabled for both Platform Services and Tools and Frameworks.

1. Open the `ReportGeneration.xml` file in *APP_NAME*`/config/script`.
2. Specify "-sslv3" in an `<arg>` element:.

```
<logserver id="LogServer" host-id="ReportGenerationHost" port="15010">
   <properties>
     <property name="numLogBackups" value="10" />
     <property name="targetReportGenDir" value="./reports/input" />
    <property name="targetReportGenHostId" value="ReportGenerationHost" />
   </properties>
   <args>
     <arg>
       --sslv3
     </arg>
   <args>
```

```
   <log-dir>./logs/logservers/LogServer</log-dir>
   <output-dir>./logs/logserver_output</output-dir>
   <startup-timeout>120</startup-timeout>
   <gzip>false</gzip>
</logserver>
```

3. Modify the "globalSslConfig" in `APP_NAME/config/script/AppConfig.xml` file to pass the ciphers that are supported for Logserver when the SSLv3 protocol is enabled. These ciphers are:
   - AES128-sha
   - RC4-md5
   - RC4-sha
4. A warning message "SSLv3 is enabled" is logged in apps/*APPNAME*/logs\Logserver\Logserver.log.

Changes from 6.1.0 to 6.1.1

This section describes changes in the behavior of the software that you should be aware of when you upgrade from Platform Services 6.1.0.

DVAL_STATIC_RANK attribute is reinstated in the STATS element

The `DVAL_STATIC_RANK` attribute has been reinstated in the XML Configuration Reference. This attribute specifies whether every dimension value's static rank should be returned as a property on the dimension value. The default value is `FALSE`.

Setting this attribute to `TRUE` causes the MDEX Engine to return the static rank with each dimension value. Like other attributes in the `STATS` element configuration, the value for this attribute can be specified both at the individual dimension level and at the global level.

Note: This attribute is reinstated starting with the MDEX Engine release 6.1.4. However, this attribute has been deprecated in 6.1.0-6.1.3 releases of MDEX Engine. For those releases, the MDEX Engine ignores this attribute and issues a warning about its presence in the file.