

# **Oracle Health Insurance Back Office**

## **Reading, Writing and Authorizing Oracle Health Insurance Application Files and Messages**

Version 1.23

Part number: G49637-01

March 25, 2026

Copyright © 2011, 2026, 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 software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

#### **U.S. GOVERNMENT RIGHTS**

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are “commercial computer software” or “commercial technical data” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.

Where an Oracle offering includes third party content or software, we may be required to include related notices. For information on third party notices and the software and related documentation in connection with which they need to be included, please contact the attorney from the Development and Strategic Initiatives Legal Group that supports the development team for the Oracle offering. Contact information can be found on the Attorney Contact Chart.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

# CHANGE HISTORY

Release	Version	Changes
10.12.2.0.0	1.2	<ul style="list-style-type: none"><li>• Changed examples in Reading output</li></ul>
10.14.2.0.0	1.3	<ul style="list-style-type: none"><li>• Some minor adjustments</li></ul>
10.15.1.0.0	1.4	<ul style="list-style-type: none"><li>• Removed references to Oracle Reports</li></ul>
10.15.3.0.0	1.5	<ul style="list-style-type: none"><li>• No relevant updates, only republished</li></ul>
10.16.1.0.0	1.6	<ul style="list-style-type: none"><li>• No changes</li></ul>
10.16.2.0.0	1.7	<ul style="list-style-type: none"><li>• Some minor textual improvements</li></ul>
10.17.1.0.0	1.8	<ul style="list-style-type: none"><li>• No changes</li></ul>
10.17.2.0.0	1.9	<ul style="list-style-type: none"><li>• No changes</li></ul>
10.18.1.0.0	1.10	<ul style="list-style-type: none"><li>• Added information regarding the isolation of database directories of pluggable databases in database 12.2 through PATH_PREFIX</li></ul>
10.18.2.0.0	1.11	<ul style="list-style-type: none"><li>• Republished with different part nr.</li></ul>
10.19.1.0.0	1.12	<ul style="list-style-type: none"><li>• No changes. Republished with different part nr.</li></ul>
10.19.2.0.0	1.13	<ul style="list-style-type: none"><li>• No changes, republished with different part nr.</li></ul>
10.20.1.0.0	1.14	<ul style="list-style-type: none"><li>• No changes, republished.</li></ul>
10.20.8.0.0	1.15	<ul style="list-style-type: none"><li>• Title adjusted as next to files also messages are involved</li><li>• Content extended for queued output messages</li></ul>
10.21.1.0.0	1.16	<ul style="list-style-type: none"><li>• Added information regarding queued JSON and XML output messages</li><li>• New part number.</li></ul>
10.22.1.0.0	1.17	<ul style="list-style-type: none"><li>• No changes, republished with new part number.</li></ul>
10.23.1.0.0	1.18	<ul style="list-style-type: none"><li>• Changed Introduction, Limited privileges on Database Directories in paragraph "Technical management of database directories"</li><li>• New part number.</li></ul>
10.23.7.0.0	1.19	<ul style="list-style-type: none"><li>• Small corrections</li></ul>
10.24.1.0.0	1.20	<ul style="list-style-type: none"><li>• No changes, republished with new part number.</li></ul>
10.25.1.0.0	1.21	<ul style="list-style-type: none"><li>• No changes, republished with new part number.</li></ul>
10.26.1.0.0	1.22	<ul style="list-style-type: none"><li>• No changes, republished with new part number.</li></ul>
10.26.3.0.0	1.23	<ul style="list-style-type: none"><li>• Remove reference to obsolete <code>ozg_init.env</code></li></ul>

## RELATED DOCUMENTS

A reference in the text (**doc[x]**) is a reference to another document about a subject that is related to this document.

Below is a list of related documents:

**Doc[1]** Oracle Health Insurance Back Office - Installation, Configuration and DBA Manual ([docs.oracle.com](https://docs.oracle.com))

Unless otherwise indicated, these documents can be downloaded from [docs.oracle.com](https://docs.oracle.com).

# CONTENTS

Introduction .....	5
OHI Data .....	5
OHI Documentation .....	5
Requesting output from a batch.....	7
Location of application software .....	7
Naming.....	7
Authorization .....	8
Determining the file location.....	9
Examples .....	12
XML output files .....	14
General functionality.....	14
Technical management of database directories.....	15
JSON and XML messages .....	18
General functionality.....	18
Message format .....	21
Online help information.....	24
Release documentation .....	25

## Introduction

This document deals with the technical and functional aspects of several types of Oracle Health Insurance application files.

Specifically, this document discusses:

- Output of OHI data
  - File output
  - Message output published on a JMS queue
- OHI Documentation
  - OHI Online Help
  - OHI Release information
- OHI batch output files
  - Batch *.out* file
  - Batch *.log* file

## OHI Data

OHI application data can be exported in several ways:

- **File output** from the Oracle Health Insurance application is mostly generated using the so-called *batch or script functionality*. Files often contain many messages for different message topics (policies, claims, etc.) in one and the same file.
- OHI increasingly outputs messages by publishing them on a **JMS queue**. This type of output usually has one message per topic (claim, policy, relation, etc.) and is mainly in XML or JSON format.

The files involved in the file output are either stored on the database server or the application server, in a directory that is to be specified per request or is pre-configured.

The bulk of file output is the XML file output, which is generated by certain batches since the first OHI release in 2005 onwards. You can specify your own file name and 'database directory' (from a pre-defined list) for the XML output (and XSD output if applicable) per script request. The technical log messages from the batch are, however, saved to the regular pre-configured output location on the application server. The system management department of an OHI customer determines the actual locations of these directories and how you can access them.

## OHI Documentation

Online help information stored in files in HTML format is used from within the application. Users can start a menu option within the user interface. This starts a new browser window and requests the files from the OHI web server.

In addition to the online help, users can view the documentation files for the installed (patch) releases in the same way from within the application (the 'releases' window).

---

## Requesting output from a batch

By default a batch script request creates a standard output file. The location and naming of this file is described below.

The output of batches that produce XML output is written to separate files and not to the standard output file for a batch. Please refer to the chapter that deals with this subject in detail for more information.

---

## Location of application software

The Oracle Health Insurance batch scheduler processes the batch requests submitted by the application.

Various types of modules are started to this end, including shell scripts, SQL\*Plus modules, perl scripts, etc.

The "Directory environment" field in the "System/Management/General/System parameters" screen (SYS1010F) specifies the top directory for the application on the Application Server. The modules to be started exist in the specified subdirectory structure. The best practice is to specify environment variable \$OZG\_BASE, but it is possible to specify your own environment variable or hard coded directory.

See the following document for the mandatory directory structure:



Oracle Health Insurance Back Office Installation, Configuration and DBA Manual

---

## Naming

The following conventions apply for naming files produced by Oracle Health Insurance script requests:

### Filename structure

---

The file name is constructed from a batch script request number and an extension:

`<script request number in a maximum of 14 positions> + <extension>`

#### *Example*

10000000041774.out

### Extensions

---

The extension can be one of the following:

#### *.out*

The extension for output, used for statuses "Completed" (script request successfully executed) and "Error" (functional errors have occurred).

#### *.log*

The extension for the log file which is filled on the "Failed" status (technical error).

---

## Authorization

**File authorization** ensures that the output can only be *read*. **System authorization** is used to ensure that this is only done by individuals who are authorized to do so.

---

### File authorization

---

#### *General*

The Oracle Health Insurance Batch Scheduler runs under a specific OS-account (normally 'batch'). All output files are created and saved under this account.

The default properties of the files created are determined by the OS file mode creation mask `umask`. When this is set to `umask 333` (preferably in a (non-interactive) profile for 'batch'), all files created are assigned *read-only* properties.

Note that the owner of the Fusion MiddleWare software needs *read* access to show the \*.out and \*.log files in the browser.

When the setting is used the result is that end users who then open the file at Operating System level can only *read* it. As the basic property of the files is read-only the files *cannot* be changed.

Here it does not matter whether file **browser** functionality (e.g. browsers like MS Internet Explorer or Edge, Chrome) or file **editor** functionality (e.g. vi under UNIX, MS Word, Wordpad, PFE under Windows) is used to display the output.

Even if the files are accessed under Windows (using networking software such as NFS or Samba) through a read-only mounted share they can still only be *read*.

---

### Application authorization

---

Application authorization means that end users can only access the output of batches they submitted from within the application through a created URL, unless he/she has authorizations as an OHI administrator (as registered in the *Maintain functions with roles* screen); in that case they can view the output of other users also.

If an OHI user has administrator authorization he/she can also view script requests from other users.

The algorithm used to determine the location of the output file is therefore as follows:

```
<set generic output directory> +  
<directory-symbol> +  
<file name>
```

Where the following also applies:

```
if not administrator user then the following must apply  
  <current user>=<user that started the script>  
else  
  error message  
end if
```

Beware, this only applies to the standard application functionality. By manipulating a URL, anyone can easily access any batch log and output file in a browser. By protecting the output URLs using e.g. Single Sign-On, it is possible to limit access to those files, but differentiating between files of different users is not possible.

Do not rely on this mechanism to protect sensitive data.

---

## Determining the file location

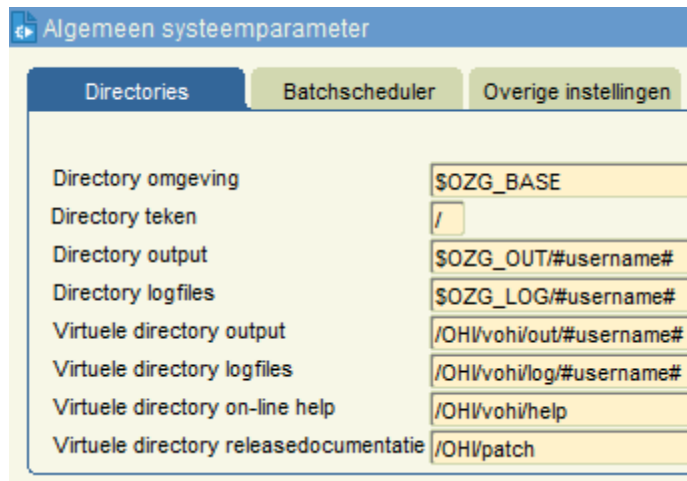
The directory that is used for the creation and retrieval of the batch *.out* and *.log* files is determined at run time.

### Writing output

---

For writing Oracle Health Insurance batch *.out* and *.log* files, the location is determined using the values specified in the “Directory output” and “Directory log files” fields in the SYS1010F screen.

The screen print below shows these fields with an example configuration (and other fields discussed later in this document).



These locations must be accessible directories on the application server. OS environment variables can also be used in the values for these locations.

The batch scheduler must be restarted before changes made in these locations take effect.

Substitution variables (between # symbols) can be used in these values. See below.

#### Example

```
Out-files = /u01/app/oracle/product/OHI/prod/out/#username#/#ado#/#merk#  
Log-files = /u01/app/oracle/product/OHI/prod/log/#username#/#ado#/#merk#
```

or (using environment variables \$OZG\_OUT and \$OZG\_LOG):

```
Out-files = $OZG_OUT/#username#/#ado#/#merk#  
Log-files = $OZG_LOG/#username#/#ado#/#merk#
```

### Reading output

---

For reading Oracle Health Insurance batch *.out* and *.log* files, the location is using the values in the “Virtual directory output” and “Virtual directory log files” fields in the SYS1010F screen.

These locations must be accessible virtual directories (within the configuration of the Oracle HTTP server) on the application server.

OS environment variables *must not* be used in the values for these locations.

Protocol, servername and portnumber are optional, so the value can start with the name of the virtual directory. This last method is called a relative address. Relative addresses are the best practice, because they do not have to be adapted when an OHI environment is moved or cloned.

### *Example*

#### Output

```
http://myhost:7777/OHI/prod/out/#username#/#ado#/#merk#  
or  
/OHI/prod/out/#username#/#ado#/#merk#
```

#### Logfiles

```
http://myhost:7777/OHI/prod/log/#username#/#ado#/#merk#  
or  
/OHI/prod/log/#username#
```

### **Conditions**

---

1. Locations specified must not end in a directory symbol.
2. The #username# substitution variable can be used to mark where the actual username appears in the path.  
The use of substitution variables is optional.
3. Substitution variables are also available for administrative organization, brand and finance company and the source of the claims. The variable names must be in Dutch but for easy understanding the English name is mentioned between brackets:
  - #ado# {#administrative organization#}. The administrative organization for which the output is being generated. The value for the administrative organization is determined from the parameters in the script request or external integration processing. If a script request or external integration processing has no administrative organization parameter then the substitution variable is replaced with an empty string.
  - #merk# {#brand#}. The brand for which output is being generated. The value for the brand is determined from the parameters in the script request or external integration processing. If a script request or external integration processing has no brand parameter then the substitution variable is replaced with an empty string.
  - #finbedrijf# {#finco#}. The finance company for which output is being generated. The value for the finance company is determined from the parameters in the script request or external integration processing. If a script request or external integration processing has no finance company parameter then the substitution variable is replaced with empty.
  - #declaratieherkomst# {#claimsource#}. This variable is only replaced for claims in return media for external integration. This variable is replaced with the source of the claim for which return information is sent.

Oracle Health Insurance determines the values for ado, brand and finance company per script request where possible and if applicable.

The system then replaces the substitution variables with the values that have been determined. Finally, the file is written to the path that has been obtained following substitution.

For each processing of an outgoing medium Oracle Health Insurance

determines the values for ado, brand and finance company where possible and if applicable.

The system then replaces the substitution variables with the values that have been determined.

The batch run is created with a file name matching the path that has been obtained following substitution.

4. A location for saving the files that differs from the default location in the file system can be specified using a medium variable for outgoing or return EI medium versions. The aforementioned substitution variables can be used here too. The name of this medium variable is `<MEDIUM_CODE>_<MEDIUM_VERSIE>_BESTEMMING` `{<MEDIUM_CODE>_<MEDIUM_VERSION>_DESTINATION}`. If the medium version with this name is not filled for a specific outgoing EI medium then the output path contained in the system parameters is used. If the medium variable does have a value then this path is used.
5. Operating system commands that need to be executed by the batch scheduler after a file has been saved can be specified in screen 'Maintain print layouts'. These can be printer commands or shell scripts that execute another process on the output files. The command defined for processing the output report is executed only for the .out file. The command defined for the processing of data files is executed once for every file produced by the script. The directory path is included in the filename. The substitution variables can be used in these commands also. If the substitution variable is empty it will be populated with the value 'null':

```
scriptnaam -A #ado# -M #merk# bestandsnaam {scriptname -A #ado# -M #brand# filename}
```

becomes the following where ado and brand have empty values:

```
scriptnaam -A null -M null bestandsnaam {scriptname -A null -M null filename}
```

6. The batch scheduler retrieves the parameter values for ado, brand and finance company that have been specified by the user. The batch scheduler checks if the value for ado, brand and finance company exist. If not, this value is replaced by an empty string.
7. If there is only a parameter (and therefore a parameter value) for brand then the ado is determined based on this brand.
8. By substituting an empty parameter value, if the brand is not applicable for example, a non-valid pathname can be generated that includes a number of consecutive slashes. Multiple consecutive slashes are always replaced with a single slash.
9. The OHI customer organization itself is responsible for the existence of the complete directory structure that must be present for the substitution variables that are used.
10. The #username# string cannot however be used IN such an environment variable! If there is a requirement to use the username in (the middle of) the path then two environment variables can be used for this:

### **Example**

```
Out-files          = $OZG_OUT_PRE/#username#/$OZG_OUT_POST  
where $OZG_OUT_PRE = /home  
and      $OZG_OUT_POST = out
```

## Examples

### Scenario 1

---

- User JJANSEN submits script request 123 under the Health Insurance subsystem. JJANSEN does not have administrator authorization.
- User member KDIJK submits script request 456 under the Financial subsystem. KDIJK does have administrator authorization.
- The output directory to be used has been set to

```
$OZG_OUT/#username#
```

- When JJANSEN wants to view his own output the following file is opened as per the algorithm above:

```
$OZG_OUT/jjansen/123.out
```

- When KDIJK wants to view his own output the following file is opened:

```
$OZG_OUT/kdijk/456.out
```

- If JJANSEN wants to view KDIJK's output the following applies: JJANSEN is not an administrator user and JJANSEN (=current user) <> KDIJK (user who started the script); therefore, an error message is generated.
- If KDIJK wants to view JJANSEN's output the following applies: KDIJK is an administrator user and the following file is opened:

```
$OZG_OUT/jjansen/123.out
```

### Scenario 2

---

- Out files: `/home/#username#/#ado#/#merk#/#finbedrijf#`  
`{/home/#username#/#ado#/#brand#/#finco#}`

Suppose that Pietersen uses the username PPIETERS to submit a script request for medium ZRG8092E 'Genereren afreken spec. natura/restitutie naar bestand' *{Generate payment spec. in kind/repayment to file}* with parameter value '1' for ado and parameter value 'TOP' for the brand. Following the substitution rules, the batch run will use the filename

```
/home/ppieters/1/top.
```

### Scenario 3

---

- Out files: `/home/#ado#/#merk#/#finbedrijf#/#username#`  
`{/home/#ado#/#brand#/#finco#/#username#}`

Suppose that Pietersen uses the username PPIETERS to submit a script request for medium ZRG8092E 'Genereren afreken spec. natura/restitutie naar bestand' *{Generate payment spec. in kind/repayment to file}* with parameter value '2' for ado and no parameter value for the brand. Following the substitution roles, the batch run will use the filename

```
/home/2/ppieters.
```

#### Scenario 4

---

- Out files: `/home/#ado#/#merk#/#finbedrijf#/#username#`  
`{/home/#ado#/#brand#/#finco#/#username#}`

Suppose that Pietersen uses the username PPIETERS to submit a script request for medium ZRG6055E 'Genereren polisbladen naar bestand' *{Generate policy pages to file}* with the parameter value TOP for the brand (there is no parameter value for ado). The system now determines the associated ado set '1'. Following the substitution roles, the batch run will use the filename

`/home/1/top/ppieters.`

#### Scenario 5

---

- Out files: `/home/#ado#/#merk#/#finbedrijf#/#username#`  
`{/home/#ado#/#brand#/#finco#/#username#}`

Suppose that Pietersen uses the username PPIETERS to submit a script request for medium FIN2020E 'Aanmaken aanmaanbestand externe incasso' *{Create reminder file external collection}* with the parameter value 6 for the finance company. Following the substitution roles, the batch run will use the filename `/home/6/ppieters.`

---

## XML output files

OHI provides a set of batch scripts that produce XML output. If necessary, an associated XSD file can also be created. This functionality is outlined below.

---

### General functionality

A number of default parameters exist for an XML output product. These are described below:

- **XML and/or XSD file**

This parameter is used to specify whether the script request should produce the requested XML file only (this will be the default use) or if the associated XSD file should be created in addition or on its own.

A batch that produces an XML output product can also produce an associated XSD file if required. The file 'describes' the structure of the XML file that is produced. It is, as it were, a 'contract' which must be met by the XML output and can often be used to control and/or direct XML processing programs.

In a script request you can specify whether you want this XSD file created. The content of the XSD file will always be the same for the output product concerned. It is only when a new version of the output product or the underlying object structure is produced that the content may differ in relation to the previous version. The same parameters are used for naming the XSD file (see below) as for the XML file, but the extension .XSD is used instead of .XML.

The content of the XML file depends on the other functional parameters to be specified.

In the unlikely event that you only want to create the XSD file, you still need to specify valid values for the functional parameters. The script request is primarily intended for generating XML output.

NOTE: When you only request XML output a more efficient (much faster) algorithm is used for writing the output to file. Output is then buffered to write larger pieces at once. Therefore, it is wise to only generate the XSD output when required to prevent unnecessary write delays.

- **Name of XML/XSD file**

A file name that you set (without the associated extension) can be specified for XML output products. Specify a meaningful name that can easily be recognized later.

In addition to these files, the default/standard output (.out file) from the script request is saved in the usual manner. This file is identified by the number of the request and contains error messages and information messages.

If an XML file already exists with the name that you specify, the number of the script request is appended behind the name so that it is still unique. The file that already exists is not, therefore, overwritten. Any existing XSD file will be overwritten though (the reason behind this choice is that this will normally be identical or it will be simple to recreate it).

- **File location**

A location or a 'directory' can be selected from a list of pre-defined locations (so called 'database directories') to be set up by the database administrator which have been given a logical name. A list of possible values can be

requested when the script request is entered. Using specific database directories, XML output intended for different purposes can be saved to different locations which can be determined by the organization.

- **Reference date**

For certain, time-valid data which are retrieved when generating the XML output, the situation must be determined as per a specific date. By default the date of creation of the output file (the 'system date') will be used as that date but if necessary a different date can be specified. The date is for example used to determine the marital status for an individual, which is valid on that date.

By changing the default parameter values for a script definition you can influence the standard values for the parameters, possibly making the submission of a script request more efficient.

It is important to realize that creating an XML file is a relatively intensive action: the data that is present in the database is translated into a functional model and this model is 'rich' as far as data is concerned.

The reason for this is that the XML file must contain all data that may be required so that a 'selection' can be made from this when using the XML file. At the same time, the techniques used to generate the XML output are more intensive than those that are used to generate the traditional ASCII output product. And the final reason is, of course, that the size of the XML files is considerably larger than a 'data only' file as every data component has an 'open' and 'close' tag that comprises the name of the data component. An example: <NAME>Smith</NAME>.

Still there is a way to influence the size of the XML output by including or excluding specific data elements. There is a special screen which can be used to view and alter this XML output dynamic content.

---

## Technical management of database directories

Certain 'database directories' have to be created in the database in order to facilitate the creation of XML and any associated XSD output files. These database directories specify a 'logical directory name' that reference a physical file system directory to which the XML output can be written. The files concerned are created by the database processes in file system directories that have been created for this purpose. This means that the OS account that runs the database (usually "oracle") needs write access to the physical file system directory. The OS account "batch" should not need this write access. ("batch" only needs access to directories on the application server).

When generating the XML output products the user can select from a number of database directories that are available to the user account concerned. These database directories can be created in the database using a DBA account and can be granted to the user accounts that are permitted access to them. This does not mean that the OHI application users need READ or WRITE privilege on these database directories. It is sufficient if they have EXECUTE privilege, which cause the directory to be visible in List-Of-Values and selectable as parameter for a batch script request.

You could grant EXECUTE privilege to the OHI BO role "OHI\_ROLE\_ALL" so all Application users automatically inherit this privilege, but this is not compatible with Database Vault.

The following OHI BO application accounts need EXECUTE privilege on database directories:

- OHI\_VIEW\_OWNER

- OHI\_DPS\_USER

A practical way to avoid having to grant EXECUTE privilege to every new application user is to grant EXECUTE to PUBLIC. This is safe, because the only effect this privilege has is related to the creation of external tables. That requires extra privileges, which should not be granted to application users. Executable files should not be placed in the Database Directories used by OHI for input and output anyway.

The only database accounts that need READ and WRITE access on the database directories are

- the application schema owner (usually "OZG\_OWNER" for Back Office; OBD\_OWN for Data Marts)
- the schema owner(s) of custom development schemas, if the custom code needs to manipulate files in the database directory concerned.

If necessary a directory can be granted to a non-OHI role or directly to a non-OHI database account. You as an OHI customer can therefore determine the privileges on directories that reference a file system directory structure completely under your own control.

By default the OZG\_TMP database directory has already been granted and represented in a file system directory that you determined during the initial database side installation of the application. This database directory must remain granted.

A couple of example commands:

```
CREATE DIRECTORY PGB_UITVOER AS '/u01/xml/ozg_uitvoer/pgb';
{translation: CREATE DIRECTORY PGB_OUTPUT AS '/u01/xml/ozg_OUTPUT/pgb'}

GRANT WRITE ON DIRECTORY PGB_UITVOER TO ksmith;
{translation: GRANT WRITE ON DIRECTORY PGB_OUTPUT TO ksmith}

CREATE DIRECTORY NOCLAIM_UITVOER AS '/u01/xml/ozg_noclaim';
{translation: CREATE DIRECTORY NOCLAIM_OUTPUT AS '/u01/xml/ozg_noclaim'}

GRANT WRITE ON DIRECTORY noclaim_uitvoer TO noclaim_gebruikers;
{translation: GRANT WRITE ON DIRECTORY noclaim_output TO noclaim_users}
```

The operating system account that owns the Oracle database software must have write permission on the physical directories concerned.

Logical names for the directories must not begin with OZG\_BASE.

You can only grant READ, WRITE and EXECUTE privilege. WRITE privileges are needed to be able to write XML.

Please consult the SQL Reference Manual for further information in relation to granting object privileges or on creating database directories.



Beware that since database release 12.2 database directories in a pluggable database can be restricted to a specific pre-defined path like for example '/u01/envs/test1'. Database directories need to be relative to such a prefixed path.

In such a way the output from a PDB can be better isolated from other output and it is in no way possible to create a database directory that might reference an Oracle Home folder or a folder where database files are stored.

The PATH\_PREFIX variable can be used to specify this during for example the plugin operation of a pluggable database.



Beware that since database release 18 database directories cannot contain symbolic links anywhere in there physical directory. Trying to use such a database directory results in *ORA-29283: invalid file operation: path traverses a symlink*



**Attention:** If your database server is not also your application server, you may find it useful (for easy access by application managers and users) to centralize the input/output database directories and the output directories on the application server by putting both types of directories on the same shared file system. There is no technical requirement from OHI to do so, however.

---

## JSON and XML messages

The OHI Back Office application offers functionality to 'publish' individual, OHI defined, standard messages for separate intended receivers of such a message (for example an insured member or a health care provider).

This message based output is different than the common file based output, where multiple messages for multiple receivers are typically stored in one or more larger files, containing many individual messages.

Goal is to support a transition over the years from file based output to message based output.

In the current situation standard messages published by OHI Back Office are all published as JMS (Java Message Service) messages on a single OHI queue in the database, named ALG\_OHI\_JMS\_QUEUE.

This might change over time, additional queues may be introduced. Currently it is not supported to publish such a message directly as a file.

These standard messages should be clearly distinguished from 'custom' JMS messages that your organization, using the OHI application, may publish on a separate queue for this purpose, named ALG\_JMS\_QUEUE. The messages on this 'custom' publish queue are not created and published by the OHI application. This queue is only offered (on request of multiple OHI customers) as a standard general purpose queue for publishing custom messages.

For more information how to access the database Advanced Queuing ALG\_OHI\_JMS\_QUEUE as JMS queue please see the relevant Appendix in **Doc[1]**.

---

## General functionality

Different types of messages will be published on the ALG\_OHI\_JMS\_QUEUE. The set of messages that can be published on the queue can be found in the technical OHI Back Office table ALG#TYPE\_QUEUE\_BERICHTEN.

In a future version of the online help information the different messages will be documented including a more detailed description.

The table contains a record per message type, with the following columns:

- HEADERTYPE: The value that identifies the message in the JMS Header as it appears in the JMSType property in the actual messages.
- SOORT\_BERICHT: The OHI type of message. Two types are supported:
  - The value N for notification, meaning a JMS message without payload, only meant to 'signal' to the dequeuer that a certain event has occurred. Such a message will only provide a very limited set of properties.
  - The value B for message ('bericht' in Dutch). This type has some properties that are required for (efficient) processing by the consumer, and a payload with the actual message, typically in XML or JSON format.

- OMS: The description of the message, a short functional description of when the message will be 'published'.

Some additional technical columns are also present.

For a better understanding the figure below shows the standard structure of a JMS message. A JMS message can consist of three parts, the standard JMS header, the additional properties and the payload.

The properties can be separated into three groups as is also shown. For OHI the application related properties differ per message type, so per record as present in the above mentioned table.



JMS messages are published on an Advanced Queuing database queue which supports JMS structured data.

Typically the table behind such a queue looks like:

Name	Type
Q_NAME	VARCHAR2(128)
MSGID	RAW(16)
CORRID	VARCHAR2(128)
PRIORITY	NUMBER
STATE	NUMBER
DELAY	TIMESTAMP(6)
EXPIRATION	NUMBER
TIME_MANAGER_INFO	TIMESTAMP(6)
LOCAL_ORDER_NO	NUMBER
CHAIN_NO	NUMBER
CSCN	NUMBER
DSCN	NUMBER
ENQ_TIME	TIMESTAMP(6)
ENQ_UID	VARCHAR2(128)
ENQ_TID	VARCHAR2(30)
DEQ_TIME	TIMESTAMP(6)
DEQ_UID	VARCHAR2(128)
DEQ_TID	VARCHAR2(30)
RETRY_COUNT	NUMBER
EXCEPTION_QSCHEMA	VARCHAR2(128)
EXCEPTION_QUEUE	VARCHAR2(128)
STEP_NO	NUMBER
RECIPIENT_KEY	NUMBER
DEQUEUE_MSGID	RAW(16)
SENDER_NAME	VARCHAR2(128)
SENDER_ADDRESS	VARCHAR2(1024)
SENDER_PROTOCOL	NUMBER
USER_DATA	SYS.AQ\$_JMS_MESSAGE
USER_PROP	SYS.ANYDATA

Please be aware of the following aspects:

- The technical table for the ALG\_OHI\_JMS\_QUEUE is queue table ALG#OHI\_JMS\_QUEUE\_TAB.
- This table is the store for the queue itself but also for the associated error/exception queue.
- Messages that were processed still remain on the queue to aid in investigating issues. By default, the retention time for the queue is configured as 7 days.
- Message processing can be monitored by querying the queue table: columns ENQ\_TIME and DEQ\_TIME contain the timestamp for when the message was enqueued and dequeued, always in UTC. You can use "enq\_time at local" in queries to get a notation with your local timezone.
- The USER\_DATA column, a SQL type column, contains the standard JMS header properties as separate columns within this SQL type column. The actual application properties are stored in USER\_DATA.HEADER.PROPERTIES as a property list.
- The textual payload itself is stored in USER\_DATA.TEXT\_LOB unless it does not fit within 4000 characters, in which situation it is stored in USER\_DATA.TEXT\_VC.
- The STATE column shows the actual queue processing state of the message.

For an overview of the relevant state values see the table below:

Value	Name	Meaning
0	READY	The message is ready to be processed, i.e., either the delay time of the message has passed or the message did not have a delay time specified
1	WAITING or WAIT	The delay specified by message_properties_t.delay while executing dbms_aq.enqueue has not been reached.
2	RETAINED OR PROCESSED	The message has been successfully processed (dequeued) but will remain in the queue until the retention_time specified for the queue while executing dbms_aqadm.create_queue has been reached.
3	EXPIRED	The message was not successfully processed (dequeued) in either 1) the time specified by message_properties_t.expiration while executing dbms_aq.enqueue or 2) the maximum number of dequeue attempts (max_retries) specified for the queue while executing dbms_aqadm.create_queue.

You can query the queue table to monitor whether expected messages are present and are being dequeued or not.

An example query for a specific message type named 'RESTITUTIEDECLARATIE' where as application and message specific property 'DECLARATIENUMMER' is fetched, next to the actual payload:

```
select t.enq_time    enqueue_tijd
,      t.deq_time    dequeue_tijd
,      t.enq_uid     enqueue_user
,      t.retry_count
,      t.priority
,      (select prp.num_value
        from   table (t.user_data.header.properties) prp
        where  prp.name = 'DECLARATIENUMMER'
       ) declaratie_nr
,      nvl(t.user_data.text_lob
           ,to_clob(t.user_data.text_vc)) bericht
,      t.state
from   alg#ohi_jms_queue_tab t
where  t.user_data.header.type = 'RESTITUTIEDECLARATIE'
order by
       t.enq_time desc
```

---

## Message format

Messages that contain a payload (SOORT\_BERICHT = 'B') are typically formatted as a JSON or XML message.

The messages are created in the same manner and by the same functional code base as which is used for the JSON responses that are created by RESTful web services. This to make sure the structure of a message is identical when returned by a web service call or when published through an OHI JMS queue.

Please note:

- OHI standard messages as published on an OHI JMS queue are created typically by 'get' operations.
- Not each RESTful web service 'get' operation may be used to publish messages on a JMS queue.
- Some messages will only be available by publishing them on the queue. The related web service operation should not be used as it will run too long and the message result will be too large. This typically applies for potentially very large messages.
- For a specific message type OHI will, when publication is activated, publish the message in XML or in JSON format. The customer can configure whether the format should be JSON or XML, as both formats can be produced.
- For the standard XML messages an XSD file is delivered within the \$OZG\_BASE folder that contains the response message definition. The name of such a file is always HSL\_<three character abbreviation>.xsd. This three character abbreviation is the same as used in the modules that are shown when the HSLBOWS deployment is chosen.
- For JSON structured messages the Swagger information as delivered for the REST webservices can be used to determine the format. The Swagger definition is published in the OHI Online Help for each web service.
- One web service definition can contain multiple operations which each can have its own response message.

For JSON structured messages the API and SDK documentation per web service can be used to retrieve a Swagger file containing all the response messages.

For the XML structured messages the link between the list of three character abbreviations and web service names as used in the Online Help may not be clear.

For that reason an association table is shown below:

File name used for XSD	Resource name in Online Help
HSL_BSN	BSN
HSL_C2B	C2B
HSL_CLA	Claim
HSL_FIN	Financial
HSL_NAT	Natura Declaratie
HSL_POL	Policy
HSL_REL	Relation
HSL_ZKR	Zorgkantoor
HSL_ZPN	Zorgplan
HSL_ZZV	Machtiging

Beware, as with the Swagger files one .xsd file name may contain the message definitions for the responses of many operations present in that web service.

At this moment it is still a little hard to determine which response message definition is associated with a certain message published on the OHI JMS message queue. This will be improved in a future release of OHI and as such be documented.

---

## Online help information

In order to access and view the online help information from within the application the "Online help virtual directory" should be set in the SYS1010F screen to the virtual directory in Oracle HTTP server (OHS) containing the online help files.

The virtual directory must point to the physical directory \$OZG\_BASE/help. A double forward slash may be needed in front of the 'help' directory.

### *Example*

<http://myhost:7777/OHI/prod/help> (or <http://myhost:7777/OHI/prod//help>)

---

## Release documentation

In order to access and view the release documentation from within the application, the "Release documentation virtual directory" should be set in the SYS1010F window to the virtual directory containing the release document files.

The virtual directory must point to the physical directory \$OZG\_PATCH.

### *Example*

`http://myhost:7777/OHI/patch`