



One Identity Manager 8.1.1

Process Monitoring and Troubleshooting Guide

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

About this guide	5
Monitoring the process handling	6
Working with Job Queue Info	6
Job Queue Info views	7
Updating the views	8
Customizing the column configuration in the Job Queue Info	8
Changing the program settings in the Job Queue Info	9
Monitoring process execution	9
Details about process handling	11
Details about process step handling	12
Details of the process step parameters	13
OUT parameters	14
Hidden parameters	14
Re-enabling process steps and processes	15
Enabling and disabling the extended logging of process steps	16
Determining the state of the server	17
Processing the DBQueue	18
Job queues sequence	18
Stopping the system (emergency stop)	19
Support for error localization in One Identity Manager	21
Overview of the system configuration and transport history	21
Displaying error messages in the One Identity Manager tools	22
Error message window in the One Identity Manager tools	22
Display error log messages	24
Display system journal messages	27
Displaying the One Identity Manager Service log file	29
Status of a One Identity Manager application server	30
Which authentication module is the current user using?	31
Which system user is the current user using?	31
Which permissions apply to the current user?	32
Which program functions are available to the current user?	33

Configuring logging in One Identity Manager	34
Configuring the retention periods of messages in the system journal	34
Recording process handling errors in the system journal	36
Recording logins and logoffs in the system journal	36
Global configuration of logging with NLog	36
Logging the One Identity Manager components	39
Configuring One Identity Manager Service logging	40
Prerequisites for displaying the log file	40
Configuring the log file	41
Authentication method for displaying the log file	42
Advanced logging in the One Identity Manager Service	43
Extended debugging in One Identity Manager Service	43
Outputting custom messages in the One Identity Manager Service log file	44
Recording messages in the event view	45
HTTPLogPlugins log file	46
Output of extended return values from individual process components	47
Enabling the crash recorder	48
Appendix: One Identity Manager configuration files	49
Application-specific configuration files	49
Global configuration file for One Identity Manager tools	51
About us	53
Contacting us	53
Technical support resources	53
Index	54

About this guide

The One Identity Manager Process Monitoring and Troubleshooting Guide describes the various methods of monitoring processing and of localizing errors in One Identity Manager. It also explains the advanced configurations for logging in One Identity Manager.

It is assumed that you understand the concept and the architecture of One Identity Manager. It is also assumed that you are thoroughly familiar with the One Identity Manager tools.

You can find additional notes about error localization and troubleshooting in the other One Identity Manager guides.

Available documentation

You can access the One Identity Manager documentation in Manager and in Designer by selecting **Help | Search**. The online version of the One Identity Manager documentation is available in the Support-Portal under [Online-Documentation](#). You will find videos with additional information at www.YouTube.com/OneIdentity.

Detailed information about this topic

- [Monitoring the process handling](#) on page 6
- [Support for error localization in One Identity Manager](#) on page 21
- [Configuring logging in One Identity Manager](#) on page 34

Monitoring the process handling

The Job Queue Info program helps you check the current status of the services running in the One Identity Manager network. It enables a detailed and comprehensive overview of the requests in the Job queue and various One Identity Manager Service requests on the servers. This program makes it easier to work with processes, supplies status information during run-time and allows errors to be quickly recognized and debugged.

Detailed information about this topic

- [Monitoring process execution](#) on page 9
- [Details about process handling](#) on page 11
- [Details about process step handling](#) on page 12
- [Details of the process step parameters](#) on page 13
- [Re-enabling process steps and processes](#) on page 15
- [Enabling and disabling the extended logging of process steps](#) on page 16
- [Determining the state of the server](#) on page 17
- [Processing the DBQueue](#) on page 18
- [Job queues sequence](#) on page 18
- [Stopping the system \(emergency stop\)](#) on page 19

Working with Job Queue Info

The Job Queue Info program has several views for the layout of processes and process steps in the job queue. In Job Queue Info, you can:

- Monitor handling of job queue processes.
- Monitor processing of the DBQueue.
- Monitor the status of the Job server and web server.
- Display the One Identity Manager Service log file.
- Display the system journal.

Job Queue Info views

The Job Queue Info has several views for displaying and editing processes and process steps in the Job queue.

Table 1: Job Queue Info Views

View	Description
Job queue	This view shows the contents of the Job queue grouped by processes. In the first level of the hierarchy, all the processes are shown with a process count. If a process node is opened, all the processes are shown with start times. The complete process with its hierarchy is displayed under a process node. Each process step contains its success and failure branches as sub elements.
Job server	This view shows the Job queue contents sorted by executing servers. At the first hierarchy level, all Job servers are displayed, with their counts of the different processes, that exist in the Job queue for the Job server. If a Job server node is opened, the process tasks are listed and the number of process step per process task is shown. The process steps are listed by start time under the process task node.
Process History	The shows the contents of the table JobHistory. The course of the process execution is displayed by sorted processes. You can limit the list of processes in the process history to only processes with errors in the program settings. If you select a failed process step, the entire error message is shown in a tooltip.
Base objects	The process history entries and the current job queue entries are summarized here in this view for the object being processed. If an error occurs during processing and the processing of the process is stopped (Frozen or Overlimit execution status), you can analyze the previous processing sequence in this view. Once all processes have been successfully handled for this object the error messages are removed from the view.
Process	This view gives an overview of how process steps are linked within a process. In this way, the execution sequence of individual process steps for large processes can be monitored better. After selecting a process, all its process steps are displayed.
Process step	In this view detailed information is displayed for each process step. The view shows the data structure for a process step at compilation time. After selecting a process step, specific information from the Job queue is mapped as well as each parameter of the selected process step with its values.
Parameter	After selecting a process step, the passing parameters of the process step are displayed with their names and their values. If the selected node does not represent a process step, the parameter view is cleared.
Affected objects	This view shows all objects that are affected by a process step.

View	Description
Progress	This view displays the number of entries in the Job queue is queried. The current value is represented by a number and inserted, at the same time, into a bar graph. The process step progress state is shown in different colors.
Server state	This view gives you a faster overview of all the Job servers and Web servers available in the network.
DBQueue	Calculation tasks in the table DialogDBQueue used for DBQueue Processor processing are displayed in this view. The number, sort order and name of the queued requests are displayed.
System journal	Displays entries in the system journal.

Updating the views

To update the views in Job Queue Info, choose **F5**. If the view focus is on a base object then the whole display is updated and the hierarchy tree is closed. This update refreshes the contents of all views. This update also refreshes the contents of other views.

The views can only ever display a snap-shot of the queue because the contents of the job queue is continually changing. Therefore, when a node is opened or the view is updated, the necessary information may have already been deleted from the job queue. If this is the case, the corresponding entry in the hierarchical display is deleted or the corresponding element is not shown.

Customizing the column configuration in the Job Queue Info

In some of the program views, you can specify which columns are to be displayed.

To specify which columns to display

- Select a node in the hierarchical display and select **Configure columns** from the context menu.

Select the columns you want to display by moving through the list and accepting with the arrow buttons, then change the order in which they are displayed.

To change the width of the columns on display

- Double-click a column boundary to optimize the column width.
- Use **Shift + double-click** for a column boundary to optimize the width of all columns.

Changing the program settings in the Job Queue Info

To change the program settings

- In the Job Queue Info, select the **Database | Settings** menu.

Table 2: Program settings

Setting	Meaning
Language	Language of the user interface. The changes come into effect after the program has been restarted. This specifies the language globally for all One Identity Manager programs so that the language does not have to set separately in each program.
Result limit	Number of entries to load and display for processes or process steps.
Polling interval	Specifies the number of seconds between data requests. The views are updated at the end of every interval. If the value is 0, the views are not updated. In this case, use F5 to update.
HTTP port of the Job server	HTTP port at which the One Identity Manager Service operates for polling the server state of the Job server. The default value is port 1880.
Status query timeout (s)	Maximum delay for status queries. Job servers that do not respond within this time limit are considered unavailable.
Only show process errors	Limits the process history display to processes with errors. The setting does not effect how the process history is recorded, only how it is displayed.

Monitoring process execution

To monitor the process information

- In the **Job queues** view or the **Base objects** view in Job Queue Info, select a process and select the **Monitor process** context menu entry.

The process information is updated regularly.

TIP: To monitor the complete job queue, select the **Monitor job queue** context menu in the **Job queues** view.

The context menu entry is only available if the logged-in user has the **Option to monitor the Job queue in Job Queue Info** (JobQueue_Monitor) program function.

In order to improve the overview, the execution progress of a process step is mirrored in the color of the text.

Table 3: Job Queue Display - Meaning of the Colors

Color	Meaning	Execution status
Orange	This process step is being processed.	Processing
Yellow	This process step is loaded for processing.	Loaded
Green	This process step is ready for processing.	True
Blue	This process step has already been processed.	Finished
Black	This process step is not ready for processing.	False
Red	The process step being dealt with cannot be processed. You can re-enable process steps with the Frozen execution status and therefore set them again for processing. The error message is shown in a tooltip.	Frozen
Purple	The process step being dealt with cannot be processed. You can re-enable process steps with the Overlimit execution status and therefore set them again for processing. The error message is shown in a tooltip.	Overlimit
Light purple	The process step cannot be found.	Missing

TIP:

- Use **Ctrl + F2** you can mark individual process steps with a bookmark. Use **F2** or **Shift + F2** to switch between the selected process steps.
- To display the objects affected by a process step, use the **Affected objects** view.

Related topics

- [Re-enabling process steps and processes](#) on page 15

Details about process handling

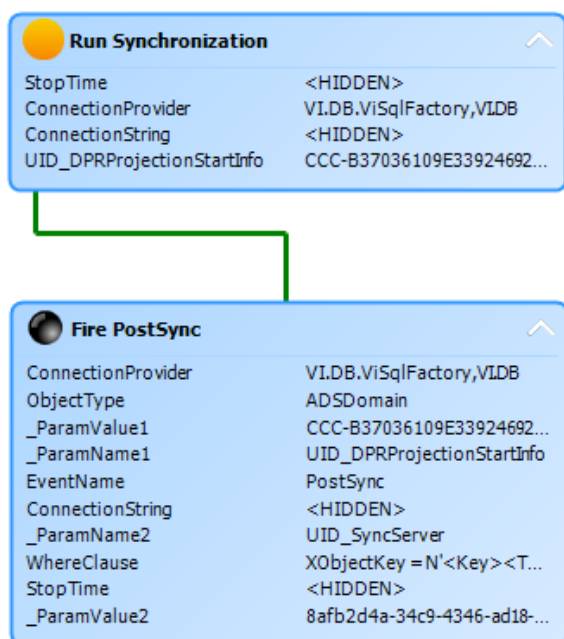
This view gives an overview of how process steps are linked within a process. In this way, the execution sequence of individual process steps for large processes can be monitored better.

To display details of the process handling

- Select a process in Job Queue Info and select the **View | Process** menu.
All the process steps of the selected process are displayed.

The process step and its properties are displayed through a special control element. The process step name is displayed in the control's header. The progress state of the process step is clarified by the use of a color icon (●). All other entries represent the parameters for this process step. You can hide or show the parameter list by clicking on the icon ▼ ▲ in the header of the control element.

Figure 1: The Process View



Each control element entry has a tooltip.

The process step's tooltip displays the following information:

- Name of the executing queue
- Name of the process component
- Name of the process task name
- Execution status

- Start time of the process step
- Error Message

A parameter's tooltip show the following information:

- Parameter name
- Parameter value

Table 4: Displaying Process's Process Steps - Meaning of the Colors

Color	Meaning	Execution status
Orange	This process step is being processed.	Processing
Yellow	This process step is loaded for processing.	Loaded
Green	This process step is ready for processing.	True
Blue	This process step has already been processed.	Finished
Black	This process step is not ready for processing.	False
Red	The process step being dealt with cannot be processed. You can re-enable process steps with the Frozen and Overlimit execution statuses and therefore set them again for processing.	Frozen/Overlimit/unknown

Details about process step handling

In this view detailed information is displayed for each process step. The view shows the data structure for a process step at compilation time. After selecting a process step, specific information from the Job queue is mapped as well as each parameter of the selected process step with its values.




To display details of the process step handling

- Select a process step in Job Queue Info and select the **View | Process step** menu.

Figure 2: Process Step View

Process step	
UID_Job	0A4349C3-454A-46F7-BD32-02386291
BasisObjectKey	
ComponentAssembly	HandleObjectComponent
ComponentClass	VI.JobService.JobComponents.Hand
DeferOnError	False
ErrorNotify	False
ErrorMessages	
ExecutionType	INTERNAL
GenProcID	7BA8D4CF-568F-4EF0-8FBB-E01E587
IgnoreErrors	False
IsRootJob	True
IsSplitOnly	False
IsToFreezeOnError	False
JobChainName	Proc: vid_InsertForHandleObject Obj
LimitationCount	0
MaxInstance	0
MinutesToDefer	0
NotifyAddress	
NotifyAddressSuccess	
NotifyBody	
NotifyBodySuccess	

Table 5: Process Step View - Meaning of Icons

Icon	Meaning
	Selection of a process step and its parameters.
	Displays a column from the Jobqueue table and the value.
	Displays a process step parameter and the value.

TIP: You can copy the data currently selected in the view into the clipboard by pressing **Ctrl + C**. The data format is column name value.

Details of the process step parameters

After selecting a process step, the passing parameters of the process step are displayed with their names and their values. If the selected node does not represent a process step, the parameter view is cleared.

To display process step parameters

- In the Job Queue Info, select a process step and select the **View | Parameter** menu.

TIP: You can copy the data currently selected in the view into the clipboard by pressing **Ctrl + C**. The data format is column name value.

OUT parameters

Parameters of the **OUT** or **INOUT** type are parameters that a process component can use to output a value. This value is then available in all subsequent process steps in the process and can be used as a value for parameters of the **IN** type.

Job Queue Info is not technically capable of determining the point at which or for which process step these parameters are valid. For this reason, OUT parameters are added to the list of parameters of a process step and are highlighted in blue.

They cannot be seen in the view of the process step under <ParamIN> of a process step because this view presents the data structure of every process step at compilation time. However, the OUT parameters are created in the context of the process.

The time at which the process is loaded into Job Queue Info is important. If a parameter is overwritten several times, only the state at the time of data query is displayed.

Example

Step 1	OUT parameter: X=1
Step 2	IN parameter: X=1
	Value changes: X=2
	OUT parameter: X=2
Step 3	IN parameter: X=2

If the process is loaded into Job Queue Info before step 2 is processed, the Job Queue Info displays the **X=1** value for the OUT parameter. If the process is loaded after step 2 is processed, the **X=2** value is displayed for the OUT parameter.

You can find more detailed information about each process step and how the parameters are filled, in the One Identity Manager Service log file.

Related topics

- [Displaying the One Identity Manager Service log file](#) on page 29
- [Output of extended return values from individual process components](#) on page 47

Hidden parameters

Parameters in the One Identity Manager Service log file and in the Job Queue Info program that are not to be displayed are labeled with the **Hidden** option. Values for hidden parameters are shown as <HIDDEN>.

Users with the program function **Option to see the values of hidden parameters in Job Queue Info** (JobQueue_ShowHiddenParameters) can view the hidden parameters in Job Queue Info. Assign the appropriate permissions group to the program function.

Related topics

- [Which program functions are available to the current user?](#) on page 33

Re-enabling process steps and processes

The maximum number of times a process can appear in the Job queue can be limited in order to prevent mass modifications.

If the limit is exceeded, the process steps are set to the **Overlimit** status and are therefore no longer collected for processing. You can re-enable these process steps for execution.

Critical process steps whose processing has failed are set to the **Frozen** execution status. You can also re-enable these processes after correcting the error.

To re-enable process steps

- Select the process step in Job Queue Info and select the **Re-enable process step** context menu.

NOTE: Use **Shift + select** or **Ctrl + select** to select and re-enable multiple process steps.

To re-enable a process step

- Select the process in Job Queue Info and select the **Restart process** context menu.

IMPORTANT: When you restart a process, all process steps are processed again. All previously handled processes up to the the point at which the error occurred are run again. This can lead to data inconsistencies in certain circumstances.

Sometimes a rerun of the failed process step is not desired. This might occur when the action to be carried out by the process has been carried out manually, for example, an expected directory has been manually added in the meantime. Even so, it may just happen that the process should be rerun even though the error has not been fixed, for example, for a rollback of already processed steps. In this case, to continue with the process, the next process step in the success or failure branch can be handled.

To run the subsequent process step

- Select the failed process step and select the **End with success** context menu or the **End with error** context menu.
 - ① **NOTE:** Both context menu entries are only viewable if there is an error/success successor and the process step is in the **Frozen** status.
 - ① **NOTE:** Use **Shift+ select** or **Ctrl + select** to select multiple process steps and start the further processing.

Enabling and disabling the extended logging of process steps

Success and error messages from process handling are written to the One Identity Manager Service log file. In order to test your processes, you can enable logging mode for process steps in the Job Queue Info. In this case, the processing messages of the processing step are written along with the **Debug** level of information into a separate log. You can display the log in Job Queue Info as well as in the log file of the One Identity Manager Service itself.

- ① **NOTE:** The log mode is only available if the logged in user has usage permissions for the program function **Option to selectively set the logging mode of process steps in the Job queue in Job Queue Info** (JobQueue_LogMode).

To enable process step logging mode

- To log the messages on success and on failure, select the process step in the **Job queues** view in Job Queue Info and select the **Execution log | Create always** context menu.
- To log the messages on failure only, select the process step in the **Job queues** view in the Job Queue Info and select the **Execution log | On Error**.
- ① **NOTE:** You can set the log mode by default for separate process steps. To do this, edit the process step in the Designer in Process Editor. For detailed information about editing processes and process steps, see the *One Identity Manager Configuration Guide*.

To display the log in Job Queue Info

- In the **Job queues** view in Job Queue Info, select the process step and select the **Execution log | Display** context menu.

This displays the log in a separate window. If a process step was executed more than once, for example, if it is re-enabled more than once, several log are displayed.

To display the log in the One Identity Manager Service log file

- In the **Server state** view in Job Queue Info, select the Job server and select the **Open in browser** context menu.
- The log is marked with a link entry Log written to Job_<UID_Job>_<yyyymmdd>_<Timestamp>.log. Click the link to display the log.

The files are stored in the One Identity Manager Service log directory.

Repository structure:

```
<Log directory>\JobLogs\<First 4 digits of the UID_Job>\Job_<UID_Job>_<yyyymmdd>_<Timestamp>.log
```

To end log mode

- In the **Job queues** view in Job Queue Info, select the process step and select the **Execution log | Disable** context menu.

Related topics

- [Displaying the One Identity Manager Service log file](#) on page 29
- [Which program functions are available to the current user?](#) on page 33

Determining the state of the server

This view gives you a faster overview of all the Job servers and Web servers available in the network.

- **NOTE:** Set the HTTP port to be queried and the maximum response time in the program settings.

One Identity Manager Service configurations of each Job server stored in the database are used to get more detailed results of Job server status queries. This is especially required if the HTTP server port has been set individually or a Job server processes several queues.

- **NOTE:** In Designer, configure and enable the schedule **Get configuration file from the Job server and write in the Job server configuration** in order to import the One Identity Manager Service configuration of the Job server into the database. For detailed information, see the *One Identity Manager Configuration Guide*.

To query the status of all the existing Job servers in the database

- In Job Queue Info, select the **View | Server state** menu and use **F5**

To query the status of a single Job server

1. In Job Queue Info, select the **View | Server state** menu.
2. Select the Job server and use the **Get status** context menu.

If the server responds, the system time, the One Identity Manager Service version and the One Identity Manager Service account name are determined and displayed. The software update status as well as the current version of the software are also displayed.

TIP: Use **Refresh server list** or **F6** to reload the list of servers.

To display a Job server's services

1. In Job Queue Info, select the **View | Server state** menu.
2. Select the Job server and select the **Open in browser** context menu.

The One Identity Manager Service HTTP server for the Job server is queried and the varying One Identity Manager Service services are displayed.

Related topics

- [Changing the program settings in the Job Queue Info](#) on page 9
- [Prerequisites for displaying the log file](#) on page 40

Processing the DBQueue

Within the One Identity Manager, changes to inheritance-relevant data such as changes to assignments, or changes to specific system data such as changes to the user interface for a system user, necessitate recalculation of the resulting data. These calculations are queued in the DBQueue and processed by the DBQueue Processor.

To display DBQueue entries

- In Job Queue Info, select the **View | DBQueue** menu.

Calculation tasks in the table DialogDBQueue used for DBQueue Processor processing are displayed in this view. The number, sort order and name of the queued requests are displayed. The display is updated at fixed time intervals of 2 seconds.

Job queues sequence

To display the Job queue sequence

- Select the **View | Progress** menu in Job Queue Info.

This queries the number of entries in the Job queue. The current value is represented by a number and inserted, at the same time, into a bar graph. The process step progress state is shown in different colors. The display is updated every 5 seconds. The tooltip shows the timestamp and the number of process steps in the Job queue at this point.

Table 6: Progress View - Meaning of the Colors

Color	Meaning	Execution status
Black	Number of process steps that are not read for processing.	False
Green	Number of process steps ready for processing.	True
Yellow	Number of process steps loaded for processing.	Loaded
Blue	Number of process step that have completed processing	Finished
Red	Number of process steps with an unknown progress state	Frozen/Overlimit/Missing

Stopping the system (emergency stop)

In certain circumstances, situations can occur in the system that require processing by One Identity Manager Service and processing of tasks by the DBQueue Processor to be stopped. Changes in One Identity Manager can, for example, sometimes cause the system to become overloaded by making mass entries in the job queue or the DBQueue.

To analyze this situation and to take the necessary steps to solve the problem where necessary, you can stop the system in Job Queue Info and restart it once the problem has been fixed.

To temporarily halt process handling of a single Job server

1. In Job Queue Info, select the **View | Server state** menu.
2. Select the Job server and select the **Stop processing** context menu.

NOTE: After solving the problem, you can use the **Start processing** context menu to restart processing.

To stop processing entirely

1. In Job Queue Info, select **Help | Emergency stop**.
2. To stop DBQueue processing, click the **DBQueue Processor** button.
From this point on no new calculations are carried out in the database.

NOTE: After the problem is eliminated, you can click the button to restart DBQueue Processor.


3. Click the One Identity Manager Service button to stop collection of process steps for all **One Identity Manager Services**.

Process steps that have already been collected are still processed but no new process step are sent to the services.

NOTE: After the problem is eliminated, you can click the button to restart the running of services.

The following icons are displayed in the status bar of all administration tools to inform the user that DBQueue Processor processing and services have been stopped.

Table 7: Special icon in the status bar for system stop

Icon	Meaning
	The DBQueue Processor has been stopped.
	The server services have been stopped.

Support for error localization in One Identity Manager

At this point, the various possibilities for error localization within the One Identity Manager are explained.

Detailed information about this topic

- [Overview of the system configuration and transport history](#) on page 21
- [Displaying error messages in the One Identity Manager tools](#) on page 22
- [Displaying the One Identity Manager Service log file](#) on page 29
- [Status of a One Identity Manager application server](#) on page 30
- [Which authentication module is the current user using?](#) on page 31
- [Which system user is the current user using?](#) on page 31
- [Which permissions apply to the current user?](#) on page 32
- [Which program functions are available to the current user?](#) on page 33

Overview of the system configuration and transport history

To obtain an overview of the system configuration

- Start Designer or Manager and select **Help | Info**.

The **System information** tab provides an overview of your current system administration and the installed modules with their versions.

IMPORTANT: You will need to provide this information if you contact the Support Team.

NOTE: If you have enabled vendor notification, this report is sent once a month to One Identity.

During a schema installation or schema update using the Configuration Wizard, the migration date and migration version are recorded in the database transport history.

When you import a transport package with the Database Transporter, the import date and description, the database version, and the transport package name are recorded in the transport history of the target database.

To display transport history

- Start Designer and select **Help | Transport history**.

Displaying error messages in the One Identity Manager tools

The One Identity Manager tools offer various possible ways to display error messages.

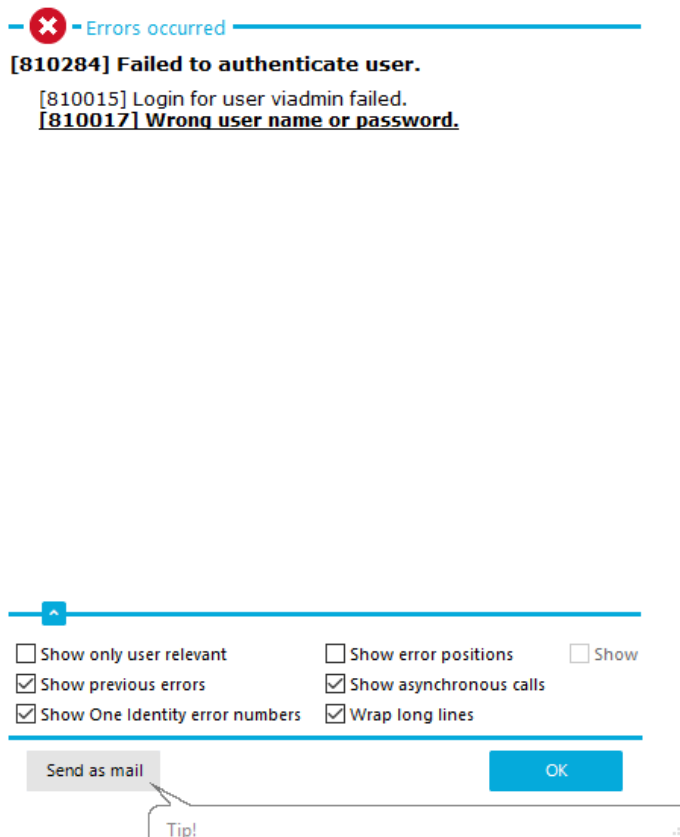
Detailed information about this topic

- [Error message window in the One Identity Manager tools](#) on page 22
- [Display error log messages](#) on page 24
- [Display system journal messages](#) on page 27

Error message window in the One Identity Manager tools

Error messages for the One Identity Manager tools are shown in a separate window. In addition, a more detailed description of the error is displayed.

Figure 3: Error message window



- To send the messages, click on the **Send as mail** button.
This creates a new email message in the default mail program and copies over the error text.
- To copy the messages to the clipboard, open the context menu for the **Send as mail** button and click on **Copy to clipboard**.
- To record the steps taken that gave the error, start the Windows Steps Recorder.
 - Open the context menu for the **Send as mail** button and click on **Create problem report**.
 - Confirm the security prompt with **OK**.

You can now start recording the individual steps. Detailed information about recording the steps taken to reproduce a problem using the Windows Steps Recorder can be found in the [Microsoft documentation](#).

Configure the amount of information to be displayed using the options in the error message window.

To change options


- Open the configuration area for the error messages window with the  button and enable or disable the options you want.

Table 8: Options for Displaying Error Messages



Option	Meaning
Show previous errors	Specifies whether all previous errors that lead to the current error, should also be shown.
Show One Identity error numbers	Specifies whether internal error numbers are shown.
Show error positions	Specifies whether error position are also shown in the program code.
Wrap long lines	Specifies whether long error messages are wrapped.
Show only user relevant	Specifies whether all error messages are to be displayed or only those error messages that are classified as user-relevant.
Show asynchronous calls	Specifies whether error messages in asynchronous method calls are shown.
Show crash report	Specifies whether error messages from the crash recorder are shown.

Related topics

- [Enabling the crash recorder](#) on page 48


Display error log messages

A program's error log, as in the Manager for example, collects all the messages, such as error messages and warnings, that have occurred since the program started. The error log is reinitialized when the program is restarted.

 **NOTE:** In Manager, the  icon in the program's status bar indicates new messages in the error log. Double-click the icon to open the error log.

To display items from the Manager error log

1. In Manager, select **View | Error log**.
2. Enable the  view in the error log toolbar.

You can configure how the messages are displayed in the error log. To do this, switch the error log to advanced mode by clicking  on the right of the column headers. Here you have the possibility to debug individual actions.


TIP: You can apply different filters to limit the information being displayed. Click the arrow in the column header and select a filter. The  icon in the log toolbar shows whether a filter is active.

Figure 4: Simple Error Log (above) and Advanced Error Log (below)

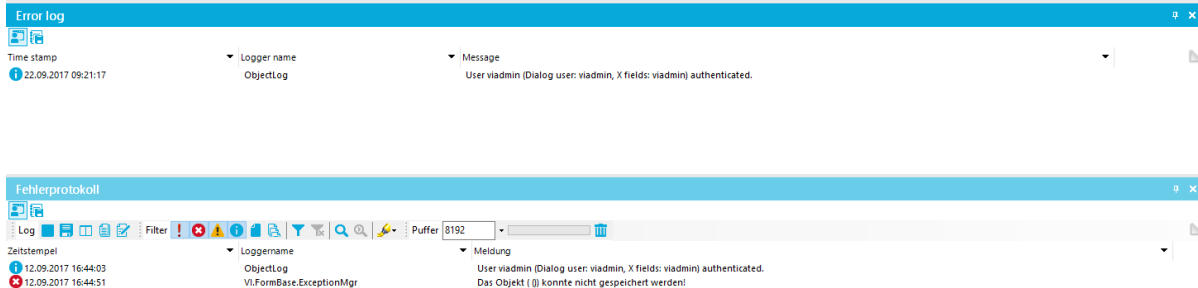




















Table 9: Meaning of Icons in the Error Log

Icon	Meaning
	Logs all critical error messages. (Severity level = Fatal)
	Logs all information. (Severity level = Info)
	Logs all warnings. (Severity level = Warning)
	Logs all error messages. (Severity level = error)
	Logs debugger output. This setting should only be used for testing. (Severity level = Debug)
	Logs highly detailed information. This setting should only be used for analysis purposes. The log file quickly becomes large and cumbersome. (Severity level = Trace)
	Adds a custom filter condition.
	Deletes filter condition.
	Searches for term.
	Searches next term.
	Marks all messages with a specific term.
Buffer size	Sets the message buffer size. The buffer's level is displayed next to the text box.
	Deletes the buffer contents.
	Stops logging.
	Starts logging.

Icon	Meaning
	Saves log to file.
	Specifies which column are displayed in the error log.
	Copies selected messages to the clipboard.
	Opens the error log with a text editor.

The following information is displayed about a message. The range of information depends on the severity level of a message.

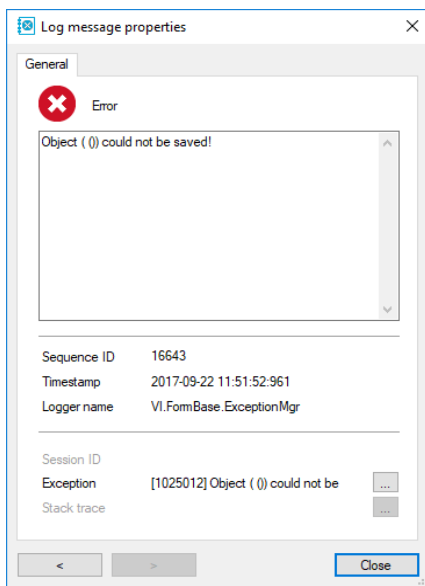
Table 10: Information about a message

Detail	Description
Severity code	Level of information supplied for the message.
Timestamp	Time and date of the log entry.
Logger name	One Identity Manager component from which the message was sent.
Message	Logged message.
Error Message	Detailed error message.
Data	Additional data about the message.
Sequence ID	Number of the line in the error log.
Stack trace	Complete stack trace for the error message.
Session ID	Session identification number.

NOTE: If there is a filter set on the session ID, only the messages for this session are displayed, for example, loading collections and single objects. If the filter is not set, actions outside of the connection, such as loading of table definitions or configuration parameters, are also displayed.

TIP: Double-click a message to display detailed information.

Figure 5: Detailed information about a message




Related topics

- [Logging the One Identity Manager components](#) on page 39

Display system journal messages

The system journal is used to store information, warning and error messages from different components of One Identity Manager, for example, DBQueue Processor, Configuration Wizard, or One Identity Manager Service. Actions in the Job Queue Info program, such as reactivating process steps, are also recorded in the system journal.

To display system journal entries in Manager

1. In Manager, go to **View | Error log**.
2. Enable the  view in the error log toolbar.

To display system journal entries in the Job Queue Info

- In Job Queue Info, select **View | System journal**.





TIP: You can apply different filters to limit the information being displayed. Click the arrow in the column header and select a filter. The  icon in the log toolbar shows whether a filter is active.

Table 11: Displaying messages in the system journal

Icon	Meaning
	Information is written to the error log/system journal.
	A warning has been written to the system journal.
	A error has been written to the system journal.


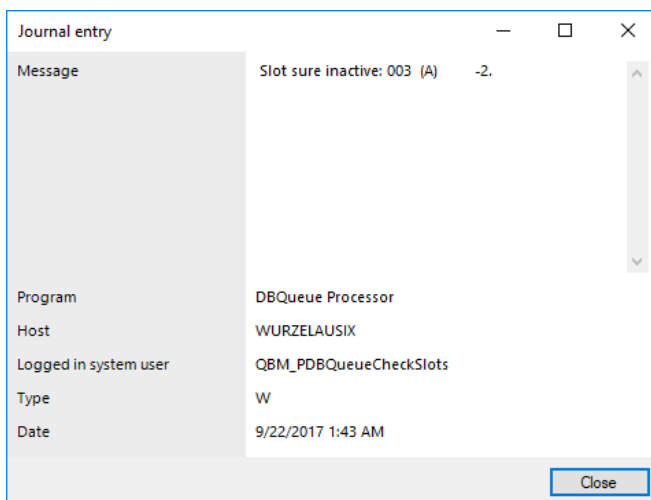
 **TIP:** Double-click a message to display detailed information.

Figure 6: Detailed Information about a Message



The following information is displayed about a message. The range of information depends on the type of message.

Table 12: Information about a message

Detail	Description
Message	Logged message.
Program	One Identity Manager component from which the message was sent.
Host	Computer from which the action was started.
Logged in system user	System user that triggered the action.
Type	Type of message. (W= Warning, I = Info, E = Error, T = Trace)
Date	Time and date of the log entry.

Related topics

- [Recording process handling errors in the system journal](#) on page 36

Displaying the One Identity Manager Service log file

You can use a browser front end to display the One Identity Manager Service log file. You call up the log file with the appropriate URL.

`http://<server name> :<port number>`

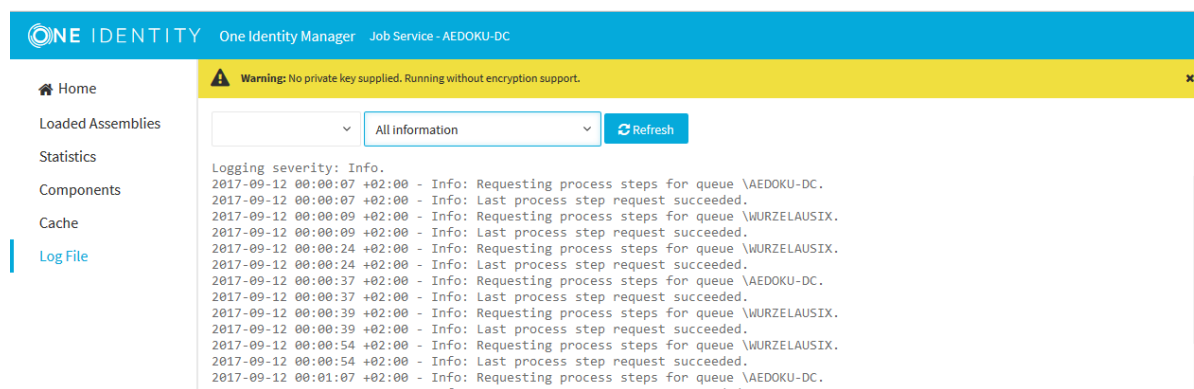
The default value is port 1880.

To open the One Identity Manager Service log file in Job Queue Info

1. Start the Job Queue Info program.
2. In the **Server state** view, select the Job server and select **Open in browser** in the context menu.

The One Identity Manager Service HTTP server for the Job server is queried and the various One Identity Manager Service services are displayed.

Figure 7: The One Identity Manager Service log file



The messages to be displayed on the web page can be filtered interactively. There is a menu on the website for this. Only text contained in the log file can be displayed in this case. If the message type is **Warning**, for example, messages with the **Info** message type cannot also be displayed if the relevant filter is selected.

The log output is color coded to make it easier to identify.

Table 13: Log file color code

Color	Meaning
Green	Processing successful.
Yellow	Warnings occurred during processing.
Red	Fatal errors occurred during processing.

i **NOTE:** If you want to retain the color information to send by mail, you need to save the complete web page.

Related topics

- [Configuring One Identity Manager Service logging](#) on page 40
- [Prerequisites for displaying the log file](#) on page 40

Status of a One Identity Manager application server

You can access the application server from a browser.

Use the appropriate URL for this:

http://<server name>/<application name>

https://<server>/<application name>

i **TIP:** You can open the web server's status display in Job Queue Info. In Job Queue Info, select **View | Server state** in the menu and, on the **Web servers** tab, open the web server status display from the **Open in browser** context menu.

You will see different status information. Status information for the application server is displayed as performance indicators. Users with the program function **Enables log display in the application server** (AppServer_Logs) can see the log. In addition, API documentation is available here.

Related topics

- [Determining the state of the server](#) on page 17

Which authentication module is the current user using?

One Identity Manager uses different authentication modules for logging in to administration tools. Authentication modules identify the system users to be used and load the user interface and database resource editing permissions depending on their permission group memberships.

For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

To identify the current authentication module for the current user

- To display user information, double-click the icon  in the status bar.

The **System user** tab displays the following information about the authentication module used.

Table 14: Information about the user authentication module

Property	Description
Authenticated by	Name of the authentication module used for logging in.
Employee UID (UserUID)	Unique ID for the current user's employee if an employee related authentication module is used to log in.

Related topics

- [Which system user is the current user using?](#) on page 31
- [Which permissions apply to the current user?](#) on page 32
- [Which program functions are available to the current user?](#) on page 33

Which system user is the current user using?

Users log in to the running administration tool using a system ID. Permitted system user IDs are determined by the authentication module you select. When the system user logs in to the One Identity Manager administration tools, the user interface is displayed and editing rights are assigned depending on the permissions groups to which the user belongs.

For detailed information about the One Identity Manager authentication modules and system users, see the *One Identity Manager Authorization and Authentication Guide*.

To identify the current system user for the current user:


- To display user information, double-click the icon  in the status bar.
The **System user** tab displays the following information about the system user.

Table 15: Information about the system user

Property	Description
System user	Name of system user
Dynamic user	Specifies whether the logged in user is using a dynamic system user. Dynamic system users are applied when a role-based authentication module is used.

Related topics


- [Which authentication module is the current user using?](#) on page 31
- [Which permissions apply to the current user?](#) on page 32
- [Which program functions are available to the current user?](#) on page 33

Which permissions apply to the current user?

The user interface displayed to and editing rights available to the current user depend on the permissions groups to which their system user belongs.

For detailed information about permissions in One Identity Manager, see the *One Identity Manager Authorization and Authentication Guide*.

To identify the current permissions rights for the current user:

- To display user information, double-click the icon  in the status bar.
The **Permissions groups** tab lists the user's permissions groups.

NOTE: The **Read only** option on the **System user** tab indicates whether the current system user has read permissions only. If so, the user is not permitted to change data.

To identify which permissions are assigned to the current user for an object:

- Select the object for which you want to see the permissions.
- Select the **Properties** context menu.

On the **Permissions** tab, you can see which permissions groups give you which permissions for an object.

Related topics


- [Which authentication module is the current user using?](#) on page 31
- [Which system user is the current user using?](#) on page 31
- [Which program functions are available to the current user?](#) on page 33

Which program functions are available to the current user?

Some functions in the One Identity Managertools are available only if the program functions are assigned to the current user. This includes data export from the Manager, calling the SQL Editor in the Designer or showing DBQueue Processor information in all programs, as examples.

For detailed information about program functions in the One Identity Manager, see the *One Identity Manager Authorization and Authentication Guide*.

To identify the program functions available to the current user:

- To display user information, double-click the icon  in the status bar.
The **Program functions** tab shows the program functions that are available.

Related topics

- [Which authentication module is the current user using?](#) on page 31
- [Which system user is the current user using?](#) on page 31
- [Which permissions apply to the current user?](#) on page 32

Configuring logging in One Identity Manager

One Identity Manager provides various options for extending its log. The log can be configured for each One Identity Manager component.

Detailed information about this topic

- [Configuring the retention periods of messages in the system journal](#) on page 34
- [Recording process handling errors in the system journal](#) on page 36
- [Recording logins and logoffs in the system journal](#) on page 36
- [Global configuration of logging with NLog](#) on page 36
- [Logging the One Identity Manager components](#) on page 39
- [Configuring One Identity Manager Service logging](#) on page 40
- [Output of extended return values from individual process components](#) on page 47
- [Enabling the crash recorder](#) on page 48

Configuring the retention periods of messages in the system journal

Table 16: Configuration parameters for logging in the system journal

Configuration parameter	Meaning
Common Journal	General parameter for configuring the system journal.
Common Journal LifeTime	Use this configuration parameter to specify the maximum retention period in days for a system journal entry in the database. Older entries are deleted from the database.

Configuration parameter	Meaning
Common Journal LifeTime D	The configuration parameter contains the retention period in days for Debug type messages.
Common Journal LifeTime E	The configuration parameter contains the retention period in days for Error type messages.
Common Journal LifeTime I	The configuration parameter contains the retention period in days for Info type messages.
Common Journal LifeTime T	The configuration parameter contains the retention period in days for Trace type messages.
Common Journal LifeTime W	The configuration parameter contains the retention period in days for Warning type messages.
Common Journal LoginAudit	Logs successful One Identity Manager logins.
Common Journal Delete	This configuration parameter allows configuration of deletion behavior for system messages.
Common Journal Delete BulkCount	This configuration parameter contains the number of entries to be deleted in an operation.
Common Journal Delete TotalCount	This configuration parameter contains the total number of entries to be deleted in any processing run.

Messages in the system journal are regularly deleted by the DBQueue Processor.

To delete log entries in the system journal

- In Designer, enable the **Common | Journal | LifeTime** configuration parameter and enter the maximum retention period for the entries in the system journal. Use the configuration sub parameters to specify the retention period for each warning level.
- If there is a large amount of data, you can specify the number of objects to delete per DBQueue Processor operation and run in order to improve performance. To do this, use the **Common | Journal | Delete | BulkCount** and **Common | Journal | Delete | TotalCount** configuration parameters.

Recording process handling errors in the system journal

To log error in process handling in the system journal

- At the process steps in the Designer, enable the **Log errors to journal** option.

For detailed information about editing processes and process steps, see the *One Identity Manager Configuration Guide*.

Related topics

- [Display system journal messages](#) on page 27

Recording logins and logoffs in the system journal

One Identity Manager logins and One Identity Manager logoffs can be recorded in the system journal.

NOTE: The logins and logoffs are also recorded in the QBM_VDialogJournalLoginAudit table, and can be executed there.

To log successful One Identity Manager logins

- In Designer, enable the **Common | Journal | LoginAudit** configuration parameter.

To record One Identity Manager logoffs

- In the Designer, enable the **Common | Journal | LogoffAudit** configuration parameter.

Related topics

- [Display system journal messages](#) on page 27

Global configuration of logging with NLog

Configuration setting for logging messages are made by NLog in Globallog.config. Globallog.config is referenced in the One Identity Manager component's configuration

files.

- ❶ **IMPORTANT:** The settings for `globallog.config` are global for all One Identity Manager components. Use the application specific configuration file `*.exe.config` to customize individual components.

Use variables to define names, output path and layout of the log files. The variable `appName` is defined in the One Identity Manager component's configuration files.

The `targets` section defines the output targets for the messages. NLog already has predefined targets that you can use in the configuration file.

The `rules` section is used to define rules for logging the messages. For an exact description and functionality of NLog, see the online help (<http://nlog-project.org/>).

Example of file structure

```
<nlog autoReload="true" xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <variable name="companyName" value="One Identity"/>
  <variable name="productTitle" value="One Identity Manager"/>
  <variable name="logBaseDir"
value="${specialfolder:LocalApplicationData}/${companyName}/${productTitle}/${ap
pname}"/>
  <variable name="layout" value="${longdate} ${level:upperCase=true} (${logger}
${event-context:item=SessionId}) : ${event-context:item=Indention}${message}
${exception:format=ToString,StackTrace}" />
  <targets async="true">
    <default-wrapper xsi:type="BufferingWrapper" bufferSize="256"
flushTimeout="2000" />
    <target name="logfile" xsi:type="File"
fileName="${logBaseDir}/${appName}.log" layout="${layout}" encoding="utf-8"
archiveFileName="${logBaseDir}/${appName}.{#.log" maxArchiveFiles="7"
archiveEvery="Day" archiveNumbering="Rolling"/>
  </targets>
  <targets>
    <target name="eventLog" xsi:type="EventLog" source="${companyName}
${productTitle} ${appName}"
layout="${message}${newline}${exception:format=tostring}"/>
  </targets>
  <rules>
    <logger name="*" minlevel="Info" writeTo="logfile"/>
    <logger name="*" level="Fatal" writeTo="eventLog"/>
  </rules>
</nlog>
```

You can enter the severity level through:

- `minlevel=` Messages are logged from this severity level.
- `level=` Message are logged which have exactly this severity level.

Table 17: Permitted severity levels

Severity Level	Description
Trace	Logs highly detailed information. This setting should only be used for analysis purposes. The log file quickly becomes large and cumbersome.
Debug	Logs debug steps. This setting should only be used for testing.
Info	Logs all information.
Warning	Logs all warnings.
Error	Logs all error messages.
Fatal	Logs all critical error messages.

By providing `logger name`, you specify for which One Identity Manager components messages are logged. Messages are logged for all components with the default setting `logger name="*"`. To limit logs to certain components, use the name contained in the log.

Table 18: Logger names of components

Logger name	Description
FrontendLog	Logs actions in front-ends.
JobGenLog	Logs during process generation.
Jobservice	Logs One Identity Manager Service messages.
ObjectLog	Logs object actions through the object level.
ProjectorEngine	Logs messages from the synchronization engine.
SqlLog	Logs database queries
StopWatch	Logs timings.
SystemConnection	Detailed logging of data communication with the system connection during synchronization, including system configuration and system connectors' data communication.
SystemConnector	Logs system connector data communication during synchronization.
Update	Logs update handling.
WebLog	Logs Web service actions.

Logging the One Identity Manager components

In the One Identity Manager default installation, the log files are written to the %LocalAppData%\One Identity\One Identity Manager\<>appName> under the name <appName>.log directory, where appName is the name of the One Identity Manager component.

All messages with a minimum information level of **Info** are recorded in the <appName>.log file. The files are kept for 7 days and backed up daily.

In addition, all messages with a severity level of **Fatal** are recorded in the event log for the One Identity Manager <appName> source.

Each One Identity Manager component supports message logging using the integrated NLog functionality. For an exact description and functionality, see the online help (<http://nlog-project.org/>).

The configuration files of the One Identity Manager component (*.exe.config) contain the nlog section, in which settings for logging by means of NLog are entered. Use the variable appName to pass the One Identity Manager component names.

The configuration of the logs is defined in the global configuration file globallog.config. This file is referenced in the configuration files of the One Identity Manager components.

Example of a Configuration File

```
<configuration>
  <configSections>
    ...
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog"/>
  </configSections>
  ...
  <nlog autoReload="true" xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <variable name="appName" value="Manager"/>
    <include file="{basedir}/globallog.config" ignoreErrors="true"/>
  </nlog>
  ...
</configuration>
```

Related topics

- [Global configuration of logging with NLog on page 36](#)

Configuring One Identity Manager Service logging

Success and error messages from process handling are written to the One Identity Manager Service log file. Messages can also be written to a server's event log. A severity level can be configured for output to this log file.

You can create most of the settings in the One Identity Manager Service configuration file. Use the Job Service Configuration program to do this. For detailed information about working with Job Service Configuration and configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.

Detailed information about this topic

- [Prerequisites for displaying the log file](#) on page 40
- [Advanced logging in the One Identity Manager Service](#) on page 43
- [Extended debugging in One Identity Manager Service](#) on page 43
- [Outputting custom messages in the One Identity Manager Service log file](#) on page 44
- [Recording messages in the event view](#) on page 45
- [HTTPLogPlugins log file](#) on page 46
- [Global configuration of logging with NLog](#) on page 36

Prerequisites for displaying the log file

The One Identity Manager Service log files can be displayed using a HTTP server (`http://<server name>:<port number>`).

- Users require permission to open an HTTP server. The administrator must grant URL approval to the user to do this. This can be executed with the following command line call:

```
netsh http add urlacl url=http://*:<port number>/ user=<domain>\<user name>
```

If the One Identity Manager Service has to run under the Network Service (**NT AUTHORITY\NetworkService**) user account, explicit permissions for the internal web service must be granted. This can be executed with the following command line call:

```
netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"
```

You can check the result with the following command line call:

```
netsh http show urlacl
```

To display the One Identity Manager Service log file, configure the following modules in the One Identity Manager Service configuration file:

- **FileLogWriter** module
Create the log file settings in this module.
- **Configuration** module
Configure the port for displaying the services. The default value is port 1880.
- **HTTP authentication** module
Set up an authentication method to display the log file.

For detailed information about configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.

Detailed information about this topic

- [Configuring the log file](#) on page 41
- [Authentication method for displaying the log file](#) on page 42

Configuring the log file

To generate the log file, customize the **FileLogWriter** module in the One Identity Manager Service configuration file for each One Identity Manager Service.

Table 19: FileLogWriter parameters

Parameter	Description
Log file (OutputFile)	Name of the log file, including the directory name. Log information for the One Identity Manager Service is written to this file. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p>i IMPORTANT: The directory specified for the file must exist. If the file cannot be created, no error output is possible. Error messages then appear under Windows operating systems in the event log or under Linux operating systems in /var/log/messages.</p> </div>
Log rename interval (LogLifeTime)	In order to avoid unnecessarily large log files, the module supports the functionality of exchanging the log file with a history list. The LogLifeTime specifies the maximum life of a log file before it is renamed as backup. If the log file has reached its maximum age, the file is renamed (for example, as JobService.log_20040819-083554) and a new log file is started. Timeout format: day.hour:minutes:seconds
Process step log lifetime (JobLogLifeTime)	Use this parameter to specify the length of time process step logs are kept. After this expires, the logs are deleted. Timeout format: day.hour:minutes:seconds

Parameter	Description
	<p>For test purposes, you can enable logging of individual process steps in the Job Queue Info. The processing messages of the process step is written to a separate log with the Debug NLog severity. The files are stored in the log directory.</p> <p>Repository structure:</p> <p><log directory>\JobLogs\<first 4 digits of the UID_Job>\Job_<UID_Job>_<yyyymmdd>_<Timestamp>.log</p>
Number of history logs (HistorySize)	Maximum number of log files. If several log files exist, the oldest backup file is deleted when a new log file is created so that the limit is not exceeded.
Max. log file size (MB) (MaxLogSize)	Maximum size in MB of the log file. Once the log file has reached the limit, it is renamed as a backup file and a new log file is created.
Max. length of parameters (ParamMaxLength)	Specifies the maximum number of characters a process step parameter is permitted to have in order to be written to the log file.
LogSeverity	Severity levels of the logged messages. The default value is Warning .

Table 20: Severity level of logging

Severity code	Description
Info	All messages are written to the event log. The event log quickly becomes large and confusing.
Warning	Only warnings and exception errors are written to the event log (default)
Serious	Only exception messages are written to the event log.

Add server name (AddServerName)	Specifies whether the server name is to be added to the log entries.
----------------------------------	--

For detailed information about configuring the One Identity Manager Service see the *One Identity Manager Configuration Guide*.

Authentication method for displaying the log file

Use the HTTP authentication module to specify how authentication on the HTTP server works to access the services, for example, to display the log file or status display.

The following module types may be selected:

- BasicHttpAuthentication

With this authentication type, enter a specific user account and the corresponding password for accessing the HTTP server.

- WindowsHttpAuthentication

Use this authentication type to specify an Active Directory group, whose users can be authenticated on the HTTP server. A security ID (SID) or the Active Directory group name in the domain of the Job server can be specified. If Active Directory is not located in the domain of the Job server, the SID must be used.

NOTE: If a module is not specified, authentication is not required. In this case, all users can access the services.

For detailed information about configuring the One Identity Manager Service see the *One Identity Manager Configuration Guide*.

Advanced logging in the One Identity Manager Service

To use advanced logging for the One Identity Manager Service, configure the storage of log files in the One Identity Manager Service configuration file in the **Connection** module.

NOTE: The given directory must exist and the One Identity Manager Service user account must have write permissions to the directory.

Following parameters are available:

- Process generation log directory (JobGenLogDir)

Log files are created in this directory that record process generation instructions from One Identity Manager Service.

For detailed information about configuring the One Identity Manager Service see the *One Identity Manager Configuration Guide*.

Extended debugging in One Identity Manager Service

The **Configuration** module of the One Identity Manager Service configuration file provides two parameters for advanced debugging:

- DebugMode
- ComponentDebugMode

If the **Debug mode** (DebugMode) parameter is enabled, the One Identity Manager Service writes more extensive information into the log file, such as all parameters transferred to a component and the results of the process handling and their Out parameters.

Individual One Identity Manager Service process components can output additional process data to the One Identity Manager Service log file. For this purpose, you can enable the **Component debug mode** (ComponentDebugMode) parameter in the configuration module. You should only use "ComponentDebugMode" for localizing errors because the effect on performance means that it is not recommended for normal use.

For detailed information about configuring the One Identity Manager Service see the *One Identity Manager Configuration Guide*.

Outputting custom messages in the One Identity Manager Service log file

You can use the RaiseMessage and AppData.Instance.RaiseMessage script engine tasks from within process steps to write custom messages to the One Identity Manager Service log file. Use the ScriptComponent process component to run the scripts.

The messages in the log file are marked in color depending on the specified severity (MsgSeverity parameter).

Figure 8: Example output of custom messages to the One Identity Manager Service log file

```
2007-08-10 12:48:58 - Warning: Example warning message
2007-08-10 12:48:58 - Info: Example Info message
2007-08-10 12:48:58 - Serious: Example error message
```

RaiseMessage

The output is consolidated with other messages and logged at the end of processing the process step.

Syntax:

```
RaiseMessage (MsgSeverity, "string")
```

Example:

```
RaiseMessage (MsgSeverity.Warning, "Example warning message")
```

```
RaiseMessage (MsgSeverity.Info, "Example Info message")
```

```
RaiseMessage (MsgSeverity.Serious, "Example error marked message")
```

AppData.Instance.RaiseMessage

The output is issued immediately during processing regardless of whether processing of the process step has ended.

Syntax:

```
AppData.Instance.RaiseMessage (MsgSeverity, "string")
```

Example:

```
AppData.Instance.RaiseMessage (MsgSeverity.Warning, "Example warning message")
```

```
AppData.Instance.RaiseMessage (MsgSeverity.Info, "Example Info message")
```

```
AppData.Instance.RaiseMessage (MsgSeverity.Serious, "Example error marked message")
```

For more examples of One Identity Manager Service log file output, see the script example on the installation medium in the directory `QBM\dvd\AddOn\SDK\ScriptSamples`.

- IMPORTANT:** You should never use the VB.NET functions `Msgbox` and `Inputbox` on servers. Use the functions `VID_Write2Log`, `RaiseMessage` or `AppData.Instance.RaiseMessage`.

Recording messages in the event view

To record messages from the One Identity Manager Service in the server event view, adjust the **EventLogLogWriter** module in the One Identity Manager Service configuration file.

Table 21: EventLogLogWriter parameters

Parameter	Description
EventLog	Name of the event log to which the messages are written. The messages are written to the application log with Application as the default value. NOTE: If more than one One Identity Manager Service write event logs on a server, make sure that the first 8 letters in the log name are unique on the server.
Severity (LogSeverity)	Severity levels of the logged messages. The default value is Warning .

Parameter Description

Table 22: Severity level of logging

Severity code	Description
Info	All messages are written to the event log. The event log quickly becomes large and confusing.
Warning	Only warnings and exception errors are written to the event log (default)
Serious	Only exception messages are written to the event log.

EventID	The ID of the messages written to the event log.
Category	The category of the messages written to the event log.
Source	The name of the source of the messages written to the event log.

Process handling error can also be written to a server's result log. For this purpose, use the LogComponent process component.

For detailed information about configuring the One Identity Manager Service see the *One Identity Manager Configuration Guide*.

HTTPLogPlugins log file

If the **HTTPLogPlugin** plug-in is configured in the One Identity Manager Service configuration file, a log file is generated with the HTTP queries of the One Identity Manager Service. The file is written in Apache HTTP Server Combined Log Format.

Example Entry

```
172.19.2.18 - - [03/Feb/2005:14:55:48 +0100] "GET /resources/JobService.css HTTP/1.x"
OK - "http://<server name>:<port>/status/LogWriter/Config"Mozilla/5.0 (Windows; U;
5.1; en-US; rv:1.7.5) Gecko/20041108Firefox/1.0"
```

Table 23: Meaning of each Entry

Entry	Meaning
172.19.2.18	IP address that sent the request.
-	Client user name using IDENT protocol (RFC 1413).
-	User name of the client according to HTTP authentication.

Entry	Meaning
[03/Feb/2005:14:55:48 +0100]	Time that the request is processed on the server.
GET /resources/JobService.css HTTP/1.x	Request.
OK	Status code.
-	Size of data sent back to the browser.
"http://<server name>:<port>/status/LogWriter/Config"	URL from which the page can be accessed.
"Mozilla/5.0 (Windows; U; Windows NT 5.1; de-DE; rv:1.7.5) Gecko/20041108Firefox/1.0"	Browser name.

For more detailed information about configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.

Output of extended return values from individual process components

Table 24: Configuration Parameter for Outputting Extended Return Values

Configuration parameter	Effect when set
Common Jobservice DoReturnOutput	The entire output of the parameter is written to the One Identity Manager Service log file when a error occurs in the case of process task that supply an extended return value.

Individual process components have process tasks with parameters that supply extended return values (OUT).

The entire output of the parameter is written to the One Identity Manager Service log file when a error occurs. For example, the output text of the listed commands or programs can be returned when you run a command or a program using the `CommandComponent` process component.

To log return values

- In the Designer, enable the **Common | Jobservice | DoReturnOutput** configuration parameter.

Related topics

- [OUT parameters](#) on page 14

Enabling the crash recorder

The crash recorder saves the previous 128 messages starting at **Debug** level and issues these in the error message window. You can configure the crash recorder using the configuration files for the One Identity Manager tools (*.exe.config).

Example for activating the crash recorder in the configuration file

```
<configuration>
  <configSections>
    ...
    <section name="connectionbehaviour" type="System.Configuration.
      NameValueSectionHandler" />
  </configSections>
  ...
  <appSettings>
    <add key="CrashRecorderBuffer" value="128" />
    <add key="CrashRecorderLevel" value="Error" />
  </appSettings>
  <connectionbehaviour>
    ...
  </connectionbehaviour>
  ...
</configuration>
```

If the variable `CrashRecorderBuffer` is set to the value `0`, the crash record functionality is disabled.

Permitted values for `CrashRecorderLevel` are **Debug**, **Error**, **Fatal**, **Info**, **Off**, **Trace** and **Warn**.

Related topics

- [Error message window in the One Identity Manager tools](#) on page 22

Appendix: One Identity Manager configuration files

General configuration settings can be preset in a configuration file. The configuration file is kept in the program directory. Each administration tool can take its settings from a configuration file in NET executable format. Valid global configuration settings can also be defined through a configuration file in One Identity Manager's own format.

Detailed information about this topic

- [Application-specific configuration files](#) on page 49
- [Global configuration file for One Identity Manager tools](#) on page 51

Application-specific configuration files

NOTE: Use the configuration file `globallog.config` for global setting that apply to all One Identity Manager components.

The One Identity Manager components, for example Manager or Designer, have a configuration file for .NET executable's with a predefined format for this. There is a configuration section in the file for each of the different modules of a One Identity Manager component.

NOTE: Entries are case-sensitive.

The root in the XML file is always called `configuration`. All other sections of the configuration file must be in the mandatory section `configSections` and their type must be defined.

Format of the Configuration File using `.exe.config` as an Example

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
```

```

    <section name="formprovider"
    type="System.Configuration.NameValueSectionHandler" />
    <section name="formarchives"
    type="System.Configuration.NameValueSectionHandler" />
    <section name="vicontrols"
    type="System.Configuration.NameValueSectionHandler" />
    <section name="connectionbehaviour"
    type="System.Configuration.NameValueSectionHandler" />
    <section name="dialogplugins"
    type="System.Configuration.NameValueSectionHandler" />
    <section name="consistencychecks"
    type="System.Configuration.NameValueSectionHandler" />
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog"/>
</configSections>
<dialogplugins>
    <add key="ComplianceRuleSimulation"
    value="VI.DialogEngine.Plugins.ComplianceRuleSimulation,
    AE.DialogEngine.Plugins" />
    <add key="ComplianceRuleSimulationSummary"
    value="VI.DialogEngine.Plugins.ComplianceRuleSimulationSummary,
    AE.DialogEngine.Plugins" />
</dialogplugins>
<consistencychecks>
    <add key="AE" value="VI.ConsistencyChecks.AE.dll" />
    <add key="Common" value="VI.ConsistencyChecks.Common.dll" />
</consistencychecks>
<formarchives>
    <add key="Forms" value="archive:.\???.Forms*.vif;10" />
    <add key="CustomForms" value="archive:.\AE.CustomForms*.vif;5" />
    <add key="CommonForms" value="archive:.\Common.Forms*.vif;5" />
</formarchives>
<vicontrols>
    <add key="defaultcontroldesign" value="System" />
</vicontrols>
<nlog autoReload="true" xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <variable name="appName" value="Manager"/>
    <include file="{basedir}/globallog.config" ignoreErrors="true"/>
</nlog>

```

</configuration>

Related topics

- [Global configuration of logging with NLog on page 36](#)
- [Global configuration file for One Identity Manager tools on page 51](#)

Global configuration file for One Identity Manager tools

The Global.cfg is an XML configuration file in One Identity Manager's own simplified format. The advantage of this file is that run-time loading is supported. Each of the different modules has its own section allocated within the file.

NOTE: Entries are case-sensitive. Both the sections and the names of the values must be written in lower case.

You can find an example of a configuration file on the installation medium in directory QBM\dvd\AddOn\SDK\ConfigSample. If the file Global.cfg is in the program directory, it is used when the One Identity Manager tools start up.

The root in the XML file is always called configuration. Each configuration file module and its values are defined in a section category respectively.

Format of Global.cfg

```
<configuration>
  <category name="settings">
    <value name="language">English</value>
    <value name="autoupdateenabled">>true</value>
    <value name="connectiontimeout">15</value>
  </category>
  <category name="connections">
    <value name="database display 1">ConnectionString</value>
    <value name="database display 2">ConnectionString</value>
  </category>
</configuration>
```

TIP: To generate the (ConnectionString) connection parameters, use the Config Encryptor program. You will find this program on the installation medium in the directory QBM\dvd\AddOn\ConfigEncryptor.

Related topics

- [Application-specific configuration files](#) on page 49

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

*

*.exe.config 49

A

application server
 status display 30

C

combined log format 46
configuration
 component debug mode 43
 debug mode 43
connection
 JobGenLogDir 43
crash recorder 48

D

DBQueue
 display 18
DBQueue Processor
 stop 19

E

emergency stop 19
error log 24
error message window 22
EventLogLogWriter
 EventLog 45
 LogSeverity 45

F

FileLogWriter 41
 HistorySize 41
 JobLogLifeTime 41
 LogLifeTime 41
 LogSeverity 41
 MaxLogSize 41
 OutPutFile 41
 ParamMaxLength 41

G

Global.cfg 51
Globallog.config 36

H

HTTP authentication
 BasicHttpAuthentication 42
 WindowsHttpAuthentication 42
HTTPLogPlugin
 log file 46

J

job queue
 sequence 18
Job Queue Info 6
 column configuration 8
 emergency stop 19
 HTTP port 9

- language 9
- One Identity Manager Service
 - log file 29
- polling interval 9
- process history 9
- program setting 9
- stop system 19
- system journal 27
- timeout 9
- update 8
- Job server
 - continue processing 19
 - determine status 17
 - stop processing 19

L

- logger name
 - FrontendLog 36
 - JobGenLog 36
 - Jobservice 36
 - ObjectLog 36
 - ProjectorEngine 36
 - SqlLog 36
 - StopWatch 36
 - SyncLog 36
 - SystemConnection 36
 - SystemConnector 36
 - update 36
 - WebLog 36
- LogWriter
 - FileLogWriter 41

N

- NLog 39
 - information level 36
 - logger name 36

O

- One Identity Manager Service
 - component debug mode 43
 - debug mode 43
 - event view 45
 - FileLogWriter 41
 - HTTP server 40
 - log file 16, 41, 43
 - display 29, 40
 - log file (HTTPLogPlugin) 46
 - NSProviderTrace.log 43
 - out-parameter 47
 - process generation log 43
 - RaiseMessage 44
 - services 40
 - StdioProcessor.log 43
 - stop 19

P

- process
 - frozen 15
 - monitoring 9
 - overlimit 15
 - re-enable 15
 - restart 15
- process component
 - component debug mode 43
 - return value 47

- process handling
 - monitoring 6
- process step
 - details 11-12
 - end with error 15
 - end with success 15
 - execution log 16
 - execution state 11
 - execution status 9
 - frozen 15
 - logging
 - disable 16
 - enable 16
 - logging errors 36
 - overlimit 15
 - parameter 13
 - out-parameter 14, 47
 - parameters
 - hidden 14
 - re-enable 15

S

- script
 - RaiseMessage 44
- server status 17
- system
 - stop 19
- system configuration
 - report 21
- system journal
 - delete 34
 - display 27
 - record logins 36
 - record logoffs 36
 - retention periods 34

U

- user
 - authentication module 31
 - dynamic 31
 - permissions groups 32
 - program function 33
 - system user 31