One Identity Manager 8.1.1

Installation 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.

One Identity Manager Installation Guide
Updated - August 2019
Version - 8.1.1
## Contents

**About this guide** ........................................................................................................... 8

**One Identity Manager overview** ................................................................................. 9
  One Identity Manager editions ......................................................................................... 10
  One Identity Manager architecture .................................................................................... 11
  One Identity Manager tools ............................................................................................... 13
  Which components and front-ends work with an application server? .......................... 18
  One Identity Manager Docker images .............................................................................. 20

**Installation prerequisites** .............................................................................................. 21
  Minimum system requirements for the database server .................................................... 22
    Database server settings and the One Identity Manager database ............................... 23
    Users with granular permission for the One Identity Manager database on an SQL Server ......................................................................................................................... 26
  Requirements for a managed instance in Azure SQL Database ...................................... 30
    Database server settings and the One Identity Manager database in a managed instance in an Azure SQL Database ................................................................. 31
    Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database ................................................................................................. 33
  Minimum system requirements for administrative workstations .................................. 37
  Minimum system requirements for the service server ..................................................... 38
  Minimum system requirements for the web server .......................................................... 39
  Minimum system requirements for the application server ............................................. 40
  Users for One Identity Manager ....................................................................................... 41
  Setting up permissions for creating an HTTP server ...................................................... 43
  Communications ports and firewall configuration ......................................................... 44

**Installing the One Identity Manager** ......................................................................... 45
  Before you start installing One Identity Manager ......................................................... 46
  Installing One Identity Manager components ................................................................ 47
    Installing the One Identity Manager components on a Windows terminal server .... 49
  Installing and configuring a One Identity Manager database ...................................... 50
  Notes on setting up a One Identity Manager database ................................................ 52
  Installing and configuring the One Identity Manager database .................................... 53
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing the One Identity Manager database during setup using the Configuration Wizard</td>
<td>58</td>
</tr>
<tr>
<td>Configuring a One Identity Manager database for testing, development or production</td>
<td>60</td>
</tr>
<tr>
<td>Encrypting database information</td>
<td>61</td>
</tr>
<tr>
<td>Creating a new database key and encrypting the database information</td>
<td>62</td>
</tr>
<tr>
<td>Changing a database key and encrypting the database information</td>
<td>63</td>
</tr>
<tr>
<td>Re-encrypting the database information</td>
<td>64</td>
</tr>
<tr>
<td>Decrypting the database information</td>
<td>65</td>
</tr>
<tr>
<td>Notes on working with an encrypted One Identity Manager database</td>
<td>66</td>
</tr>
<tr>
<td>One Identity Manager vendor notification</td>
<td>67</td>
</tr>
<tr>
<td>Enabling vendor notification</td>
<td>67</td>
</tr>
<tr>
<td>Checking the vendor notification</td>
<td>68</td>
</tr>
<tr>
<td>Disabling vendor notification</td>
<td>68</td>
</tr>
<tr>
<td>Setting up the email notification system</td>
<td>69</td>
</tr>
<tr>
<td><strong>Installing and configuring the One Identity Manager Service</strong></td>
<td>75</td>
</tr>
<tr>
<td>Setting up Job servers</td>
<td>76</td>
</tr>
<tr>
<td>Remote installation of the One Identity Manager Service with the Server Installer</td>
<td>77</td>
</tr>
<tr>
<td>Displaying the One Identity Manager Service log file</td>
<td>80</td>
</tr>
<tr>
<td>Changing the user account or One Identity Manager Service start type</td>
<td>80</td>
</tr>
<tr>
<td>The One Identity Manager Service in a cluster</td>
<td>81</td>
</tr>
<tr>
<td>Registering the One Identity Manager Service in a cluster</td>
<td>82</td>
</tr>
<tr>
<td>Installing and configuring the One Identity Manager Service in a cluster</td>
<td>83</td>
</tr>
<tr>
<td><strong>Automatic updating of One Identity Manager</strong></td>
<td>85</td>
</tr>
<tr>
<td>Basics for automatic software update</td>
<td>85</td>
</tr>
<tr>
<td>Automatic updating of the One Identity Manager tools</td>
<td>87</td>
</tr>
<tr>
<td>User intervention in automatic updating of One Identity Manager tools</td>
<td>88</td>
</tr>
<tr>
<td>Automatic updating of the One Identity Manager Service</td>
<td>88</td>
</tr>
<tr>
<td>Automatic updating of web applications</td>
<td>89</td>
</tr>
<tr>
<td>Implementing the automatic software update</td>
<td>90</td>
</tr>
<tr>
<td>Disabling automatic update</td>
<td>91</td>
</tr>
<tr>
<td><strong>Updating the One Identity Manager</strong></td>
<td>93</td>
</tr>
<tr>
<td>The update process for releasing a new One Identity Manager version</td>
<td>93</td>
</tr>
<tr>
<td>Updating One Identity Manager components</td>
<td>97</td>
</tr>
<tr>
<td>Updating the One Identity Manager database</td>
<td>100</td>
</tr>
</tbody>
</table>
Notes on updating the One Identity Manager database .............................................101
Updating the One Identity Manager database with the Configuration Wizard ...........103
Editing the One Identity Manager database during update with the Configuration Wizard ......................................................................................................................105
Installing a hotfix in the One Identity Manager database .....................................106
  Displaying the contents of a transport package with the Database Transporter ....107
  Importing a transport package with the Database Transporter ..........................108
  Importing files with the Software Loader ..............................................................110

**Installing and updating an application server** ..................................................112
  Advice for installing an application server ...............................................................112
  Installing an application server ..............................................................................113
  Displaying the application server status ...............................................................116
  Updating an application server ..............................................................................117
  Updating the search index on the application server ...........................................118
  Uninstalling an application server .......................................................................118

**Installing the API Server** ..............................................................................120
  Installing the API Server ......................................................................................120
  Installing and accessing HTML5 applications ....................................................124
  Uninstalling the API Server ..................................................................................125

**Installing, configuring and maintaining the Web Portal** ................................126
  Installing the Web Portal ......................................................................................126
  Updating the Web Portal ......................................................................................131
  Uninstalling the Web Portal ..................................................................................132
  Configuring the Web Portal ..................................................................................133
    Configuring the database connection .................................................................134
    Authentication data for the web application ......................................................134
    Logging for the web application .......................................................................136
    Configuring the automatic update for the Web Portal ....................................137
  Advanced web settings .........................................................................................138
  Storing the cache directories ................................................................................139
  Configuring the debugger service .......................................................................139
  Configuring the search service ............................................................................139
  Maintenance of the Web Portal ............................................................................140
  Displaying the Runtime Monitor .......................................................................140
Access permissions for the runtime monitor ......................................................... 141
Log files and exceptions ....................................................................................... 141
Maintenance mode ............................................................................................... 142
Using the performance indicators for monitoring .............................................. 142

Installing and updating the Manager web application ........................................ 144
Installing the Manager web application .............................................................. 144
Displaying the Manager web application ........................................................... 147
Updating the Manager web application .............................................................. 147
Uninstalling the Manager web application ......................................................... 148

Logging in to One Identity Manager tools ......................................................... 150
Logging in to the One Identity Manager database .............................................. 151
Logging in to the One Identity Manager tools using a system ID ...................... 153
Enabling other authentication modules ............................................................. 154
Language settings in One Identity Manager ....................................................... 155
    Enabling other login languages .................................................................... 156
Password expiry .................................................................................................... 156
Checking authentication ...................................................................................... 156

Error handling .................................................................................................... 158
Displaying the transport history and checking the One Identity Manager version .... 158
Error messages when logging into One Identity Manager tools ...................... 159
Error messages when installing and updating the One Identity Manager database .... 160
Database errors when migrating a database in SQL Server AlwaysOn availability groups or database mirroring ................................................................. 162
DBQueue Processor does not process tasks ....................................................... 163
Message: Enter email address in configuration parameter ............................... 164
Operations Support Web Portal is not displayed .............................................. 165
Removing superfluous modules ........................................................................ 165
Log message for search index creation .............................................................. 167

Appendix: Creating a One Identity Manager database for a test or development environment from a database backup ................................................................. 169

Appendix: Extended configuration of the Manager web application .............. 171
General ............................................................................................................... 172
Database connection ......................................................................................... 172
Security ............................................................................................................. 173
About this guide

The One Identity Manager describes the installation and initial commissioning of *One Identity Manager Installation Guide*. It provides an overview of the architecture of One Identity Manager and the functions of the various One Identity Manager tools. It also provides information about the prerequisites you will need before installation of One Identity Manager, and how to set up, install, and update the components of One Identity Manager.

This guide is intended for end users, system administrators, consultants, analysts, and any other IT professionals using the product.

**NOTE:** This guide describes One Identity Manager functionality available to the default user. It is possible that not all the functions described here are available to you. This depends on your system configuration and permissions.

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](http://www.YouTube.com/OneIdentity).
One Identity Manager overview

One Identity Manager simplifies the process of managing user identities, access permissions and security policies. You allow the company control over identity management and access decisions whilst the IT team can focus on their core competence.

With this product, you can:

- Implement group management using self-service and attestation for Active Directory with the One Identity Manager Active Directory Edition
- Simplify access decisions for restructuring data with the One Identity Manager Data Governance Edition
- Realize Access Governance demands cross-platform within your entire company with One Identity Manager

Every one of these scenario specific products is based on an automation-optimized architecture that addresses major identity and access management challenges at a fraction of the complexity, time, or expense of "traditional" solutions.

One Identity Hybrid Subscription

Extend the functional scope of One Identity Manager with a One Identity Hybrid Subscription, which offers a range of additional cloud functions and services. Use the universal Starling Two-Factor Authentication to protect administrative access, to force an additional authentication if you request or approve a critical access, or in order to activate the out-of-brand user verification for password requirements. For an additional charge, these offers can also be extended to further target systems and application scenarios. A single subscription can be used for all your One Identity products.
One Identity Manager editions

One Identity Manager is available in the following editions.

Table 1: One Identity Manager editions

<table>
<thead>
<tr>
<th>Edition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Identity Manager</td>
<td>The edition contains all management modules (IT Shop &amp; workflow, delegation, management of system roles and business roles, role mining, risk assessment, attestation, compliance, company policies, report subscriptions), as well as Unified Namespace and connectors for Active Directory.</td>
</tr>
<tr>
<td>One Identity Manager Active</td>
<td>This edition contains all the functionality required for Active Directory support including connectors for Active Directory, attestation, IT Shop and workflows, and report functions.</td>
</tr>
<tr>
<td>Directory Edition</td>
<td></td>
</tr>
<tr>
<td>One Identity Manager Data</td>
<td>This edition contains the features required for data governance support including the connectors for Active Directory and SharePoint, risk assessment, attestation, compliance, company policies, delegation, report subscriptions, and the Data Governance service.</td>
</tr>
<tr>
<td>Governance Edition</td>
<td></td>
</tr>
</tbody>
</table>
One Identity Manager architecture

Figure 1: Overview of One Identity Manager components

One Identity Manager consists of the following components:

**Database**

The database represents the One Identity Manager kernel. It fulfills the main tasks, which are managing data and calculating inheritance. Object properties can be inherited along the hierarchical structures, such as, departments, cost centers, location or business roles. In the case of data management, the database maps the managed target systems, ERP structures as well as the compliance rules and access permissions.

The database is separated into two logical parts, payload and metadata. The payload contains all the information required to maintaining data, such as information about employees, user accounts, groups, memberships and operating data, approval workflows, attestation, recertification and compliance rules.

The meta data contains the description of the application data model and scripts for formatting roles and templates or conditional interactions. One Identity Manager’s entire system configuration, all the front-end control settings and the queues for asynchronous processing of data and processes are also part of the metadata.

Recalculation of inheritance is started by the database trigger logic. For this purpose, the triggers place processing tasks in a task list known as the DBQueue. The DBQueue Processor processes these tasks and recalculates inheritance of the respective database
objects. A table labeled "JobQueue" is used to store processing orders that are to be executed by the object layer.

SQL Server or a managed instance in Azure SQL Database is used as the database system.

**Server Service**

One Identity Manager uses so called 'processes' for mapping business processes. A process consists of process steps, which represent processing tasks and are joined by predecessor/successor relations. This functionality allows flexibility when linking up actions and sequences on object events. Processes are modeled using process templates. A process generator (Jobgenerator) is responsible for converting script templates in processes and process steps into a concrete process in the 'Job queue'.

The One Identity Manager Service enables the distribution of the information administrated in the One Identity Manager database throughout the network. The One Identity Manager Service performs data synchronization between the database and any connected target systems and executes actions at the database and file level. The One Identity Manager Service retrieves process steps from the JobQueue. Process steps are executed by process components. The One Identity Manager Service also creates an instance of the required process component and transfers the process step parameters. Decision logic monitors the execution of the process steps and determines how processing should continue depending on the results of the executed process components. The One Identity Manager Service enables parallel processing of process steps because it can create several instances of process components.

The One Identity Manager Service is the only One Identity Manager component authorized to make changes in the target system.

**Application server**

Clients connect to an application server storing business logic. The application server provides a connection pool for accessing the database and ensures a secure connection to the database. Clients send their queries to the application server, which processes the objects, for example, by determining values using templates and sending the results back to the clients. The data from the application is sent to the database when an object is saved.

Clients can alternatively work without external application servers, by keeping the object layer themselves and accessing the database layer directly. In this case, only the part of the object layer required for the acquisition process is mapped in the clients.

**Web server**

There is an application running on a web server based on a web page render engine for implemented browser-based user interfaces. Via a web browser, users can access the website that has been dynamically set up and customized for them. Data exchange between database and web server can take place directly or through the application server.
**Front ends**

There are different front-ends for different tasks. For example, a different front-end is used to configure One Identity Manager as that for managing employee data. The contents to be displayed and the extent to which it can be altered is determined in conjunction with the access rights of the respective user through the object layer. Available front-end solutions are client and browser based.

**Figure 2: Overview of One Identity Manager components without application servers**

![Diagram showing the components of One Identity Manager without application servers]

**Related topics**

- One Identity Manager tools on page 13
- Which components and front-ends work with an application server? on page 18

**One Identity Manager tools**

Different tools are provided for different tasks. For example, the tool used to configure One Identity Manager differs from the tool used to manage employee data. The contents to be displayed and the extent to which it can be altered is determined in conjunction with the access rights of the respective user through the object layer.
### Table 2: Overview of One Identity Manager tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Launchpad</strong></td>
<td>Launchpad is the central tool for starting One Identity Manager administration tools and configuration tools. You can use Launchpad to check the existing One Identity Manager installation and start One Identity Manager tools to execute individual tasks. The Launchpad can be customized. You can define your own menu items and action for the Designer in the Launchpad.</td>
</tr>
</tbody>
</table>
| **Web Portal**       | The Web Portal is a web-based application for all One Identity Manager users. The Web Portal provides the stringent workflows in the following areas:  
  - Change employee master data and own password  
  - Edit or enter employee master data for subordinate staff.  
  - Search, request, cancel or renew products in the IT Shop  
  - Delegate user-specific roles.  
  - Edit assigned approvals, attestation cases and rule violations.  
  
In the info system, you see several evaluations, for example, about your own requests and attestation cases, employee numbers, approvals, rule violations, or the Unified Namespace.  

The Web Portal requires a web server. Via a web browser, users can access the website that has been dynamically set up and customized for them. Once the web server has been configured and a web project in Web Designer has been shared, you can start the Web Portal in your own web browser. |
| **Password Reset Portal** | The Password Reset Portal allows users to reset passwords of the user accounts they manage securely.  
To utilize the Password Reset Portal, it must be installed as a dedicated web application. The necessary security is guaranteed by multi-factor authentication. |
| **Operations Support Web Portal** | The Operations Support Web Portal was created with help desk employees in mind, who need support when executing tasks and process steps. You can use the Operations Support Web Portal to monitor the handling of processes and DBQueue tasks. You can also create access codes for your colleagues.  

Before you can use the Operations Support Web Portal, you must install an API Server. |
| **Manager**          | Manager is the main administration tool for setting up information about employees and their identities. It displays and maintains all the data required for the administration of employees, their user accounts, |
permissions, and company-specific roles in a One Identity Manager network. Company resources employees require can be entered and assigned to them.

You can also use Manager to

- Define custom IT policies
- Set up an IT Shop from which company resources and assignments can be requested
- Set up special approval processes for authorizing requests and checking compliance to IT policy
- Set up attestation procedures for regularly testing the correctness of data about employees or roles and their assignments

By implementing One Identity Manager application roles, every One Identity Manager user obtains only those access permissions they require to fulfill necessary administrative duties.

Manager functionality can be provided by web applications.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synchronization Editor</strong></td>
<td>You use the One Identity Manager to connect different target systems to Synchronization Editor. Use this tool to configure data synchronization for any target system and specify which target system data is mapped to the One Identity Manager database. You also define the object properties mapping and the synchronization sequence as a workflow.</td>
</tr>
<tr>
<td><strong>Analyzer</strong></td>
<td>Use the Analyzer to automatically detect and analyze data correlations in the database. This information can be used to replace, for example, direct permissions assignments with indirect assignments, therefore reducing the administration effort.</td>
</tr>
<tr>
<td><strong>Job Queue Info</strong></td>
<td>Job Queue Info helps you to check the current status of the services running in a One Identity Manager network. It displays, in a detailed and comprehensive manner, the tasks in the job queue and the different One Identity Manager Service requests on the servers. The tool provides on-the-fly status information and makes fast error detection possible.</td>
</tr>
</tbody>
</table>
| **Configuration Wizard** | The Configuration Wizard is used to set up the database on a SQL Server for use in a One Identity Manager network. All the One Identity Manager schema tables, data types and database procedures are loaded into the database with the Configuration Wizard. The SQL Server logins and database users with permissions for the One Identity Manager schema are created. Automatic version control is integrated into the One Identity Manager, ensuring that One Identity Manager components are always consistent.
<table>
<thead>
<tr>
<th>Tool</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designer</td>
<td>The Designer is the main tool for configuring the One Identity Manager. The program offers an overview of the entire One Identity Manager data model. It enables the configuration of global system settings, for example, language or configuration parameters, as well as customizing the user interface for the various administration tools. The rights structure for different administrative tasks of individual users and user groups is also set up with the Designer. Another important task is the definition of workflows for technically illustrating the administration procedures in a company. The Designer provides various editors for the One Identity Manager system configuration. The range of functions and the operating methods of the editors are tailored to the differing configuration requirements.</td>
</tr>
<tr>
<td>Web Designer</td>
<td>The Web Designer is used to configure and extend the Web Portal. It includes functions for adapting the Web Portal workflows and developing new workflows.</td>
</tr>
<tr>
<td>Data Import</td>
<td>With the Data Import program, the One Identity Manager offers a simple means of importing data from other systems. Use this program if you want to import company resource data from external sources into your database. The program supports importing from files and importing directly from other database systems. You can import data immediately. You also have the option to import data from customized processes using the import scripts that are created. The import definition is saved so that you can use it for future data imports.</td>
</tr>
<tr>
<td>Crypto Configuration</td>
<td>In certain circumstances it is necessary store encrypted information in the database. Encryption is carried out using the Crypto Configuration program. This program creates a code file and converts the contents of the affected database column. The coded information is stored in the database.</td>
</tr>
<tr>
<td>Database Compiler</td>
<td>The One Identity Manager database must be compiled after changes to configuration data. After a migration package or full custom configuration package is imported, compiling the database is started immediately from the Configuration Wizard or Database Transporter. The Database Compiler compiles the One Identity Manager database after hotfixes are imported or when changes have been made to processes, scripts, formatting rules, object definitions, task definitions, and preprocessor-relevant configuration parameters.</td>
</tr>
<tr>
<td>Report Editor</td>
<td>With the Report Editor, you can group One Identity Manager object data...</td>
</tr>
<tr>
<td>Tool</td>
<td>Short description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>API Loader</strong></td>
<td>Together into reports. You can group, accumulate, and graphically represent this data. Predefined reports are supplied though migration but you can also create your won reports with the Report Editor.</td>
</tr>
<tr>
<td><strong>Schema Extension</strong></td>
<td>The Schema Extension extends the existing application data schema of the One Identity Manager database with customer-specific tables and columns. Using the object technology in the One Identity Manager, it is possible to do this at database level such that these additions are available with full functionality at the object level.</td>
</tr>
<tr>
<td><strong>System Debugger</strong></td>
<td>The System Debugger allows you to process and test scripts. Existing scripts in your One Identity Manager database are imported into a Visual Studio script library. There, you can edit and test the scripts. Subsequently, you decide whether your changes should be transferred to the One Identity Manager database.</td>
</tr>
<tr>
<td><strong>Database Transporter</strong></td>
<td>The Database Transporter transfers objects and custom changes as well as custom database procedures, triggers, functions, and sets from the One Identity Manager database (source) to another One Identity Manager database (target).</td>
</tr>
<tr>
<td><strong>HistoryDB Manager</strong></td>
<td>One Identity Manager historical data is transferred at regular intervals into a One Identity Manager History Database. Therefore, the One Identity Manager History Database provides an archive of change information. The HistoryDB Manager tool displays the data in the One Identity Manager History Database. Use the HistoryDB Manager to set up access to the source databases.</td>
</tr>
<tr>
<td><strong>Job Service Configuration</strong></td>
<td>Job Service Configuration is used to create and customize the configuration file for One Identity Manager Service. One Identity Manager Service and its plugins are configured with this file. The configuration file is necessary both for One Identity Manager Service on a Windows based operating system and also for the Linux daemon.</td>
</tr>
<tr>
<td><strong>License Meter</strong></td>
<td>Using the License Meter, you can track and maintain the licences in your One Identity Manager database. The wizard creates a report with license-relevant information.</td>
</tr>
<tr>
<td><strong>Software Loader</strong></td>
<td>Use the Software Loader to load new or modified files, for example custom form archives, in the One Identity Manager database in order to distribute them to One Identity Manager network workstations and Job servers using automatic software updating.</td>
</tr>
<tr>
<td><strong>Server Installer</strong></td>
<td>Use the Server Installer to install and configure the One Identity Manager Service. The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.</td>
</tr>
</tbody>
</table>
| **API Designer**     | The API Designer allows you to create, record, compile and publish a
REST-API (Representational State Transfer Application Programming Interface) in the quickest way possible. This API is based on the OpenAPI Specification and the One Identity Manager database model. To use the API, you must install an API Server.

API Server

The API Server provides the API that you create in the API Designer. It also provides the Operations Support Web Portal and your HTML5 web applications.

Related topics

- Which components and front-ends work with an application server? on page 18

### Which components and front-ends work with an application server?

The following list tells you which One Identity Manager components can work with an application server. Some front-ends only work have limited functionality to work with an application server.

#### Table 3: One Identity Manager components and application servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Connection through Application Server?</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launchpad</td>
<td>Yes</td>
<td>Certain application, which you can start from the Launchpad, require a direct connection to the database.</td>
</tr>
<tr>
<td>Web Portal</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Password Reset Portal</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Operations Support Web Portal</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td>Yes</td>
<td>The consistency check is not supported. Compliance rule simulation is not supported. Some forms are not supported.</td>
</tr>
<tr>
<td>Manager web application</td>
<td>Yes</td>
<td>Some forms are not supported.</td>
</tr>
<tr>
<td>Component</td>
<td>Connection through Application Server?</td>
<td>Restrictions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Synchronization Editor</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Analyzer</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Job Queue Info</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Configuration Wizard</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Designer</td>
<td>Yes</td>
<td>The consistency check is not supported. Process simulation is not supported. Database compilation is not supported.</td>
</tr>
<tr>
<td>Web Designer</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Data Import</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Crypto Configuration</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Database Compiler</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Report Editor</td>
<td>Yes</td>
<td>SQL query testing is not supported.</td>
</tr>
<tr>
<td>Schema Extension</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>System Debugger</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Database Transporter</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>HistoryDB Manager</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>License Meter</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Software Loader</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SPML web application</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>SOAP Web Service</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>One Identity</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Component | Connection through Application Server? | Restrictions
---|---|---
Manager Service | | 
Server Installer | Yes | 
API Designer | Yes | 
API Server | Yes | 

One Identity Manager Docker images

One Identity provides various Docker images for simple and standardized installation and execution of individual One Identity Manager components in Docker containers. The One Identity Manager Docker images, together with detailed information about the usage and configuration of the individual images are available in the One Identity Docker repository. Videos containing additional information are available in the One Identity Manager Containerization video series available at www.YouTube.com/OneIdentity. For detailed information about Docker, see https://www.docker.com/.

Table 4: Available One Identity Manager Docker images

<table>
<thead>
<tr>
<th>Docker image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oneidentity/oneim-job</td>
<td>This image executes an instance of a One Identity Manager Service. When started, it downloads the necessary files for a specific Job server. This behavior can be controlled using encrypted values and environment variables.</td>
</tr>
<tr>
<td>oneidentity/oneim-appserver</td>
<td>This image executes an instance of the One Identity Manager application server. When started, it downloads the necessary files from the configured One Identity Manager database. This behavior can be controlled using encrypted values and environment variables.</td>
</tr>
<tr>
<td>oneidentity/oneim-web</td>
<td>This image executes an instance of the Web Portal. When started, it downloads the necessary files from the configured One Identity Manager database. This behavior can be controlled using encrypted values and environment variables.</td>
</tr>
<tr>
<td>oneidentity/oneim-installer</td>
<td>This image contains a simple installation program that can be used in derived images to create the file structure for One Identity Manager applications.</td>
</tr>
</tbody>
</table>
Installation prerequisites

The following installation prerequisites represent only the minimum requirements for installing and unlimited operation of One Identity Manager. These prerequisites can be used as a starting point for other planning, depending on the size of the project and which business processes and business transactions are supported. Determining hardware capacities and any further development is part of project planning and dependent on the Identity Management project specification. Particular attention must be paid to I/O performance (in throughput and latency) and in SAN environments in particular, a targeted performance analysis of the specify infrastructure is recommended before implementation. Every One Identity Manager installation can be virtualized. Ensure that performance and resources are available to the respective One Identity Manager component according to system requirements. Ideally, resource assignments for the database server are fixed. Virtualization of a One Identity Manager installation should only be attempted by experts with well-based knowledge of virtualization techniques. For more information about virtual environments, see Product Support Policies.

**NOTE:** Other system requirements for individual One Identity Manager models are listed in the corresponding documentation for those specific modules.

**Detailed information about this topic**

- Minimum system requirements for the database server on page 22
- Requirements for a managed instance in Azure SQL Database on page 30
- Minimum system requirements for administrative workstations on page 37
- Minimum system requirements for the service server on page 38
- Minimum system requirements for the web server on page 39
- Minimum system requirements for the application server on page 40
- Users for One Identity Manager on page 41
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26
- Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33
Minimum system requirements for the database server

A server must meet the following system requirements for installation of a One Identity Manager database. Depending on the number of One Identity Manager modules and the accounts managed in One Identity Manager, the requirements for working memory, hard disk storage, and processors may be significantly greater than the minimum requirements.

Table 5: Minimum system requirements - database server

<table>
<thead>
<tr>
<th>Processor</th>
<th>8 physical cores 2.5 GHz+</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>NOTE:</strong> 16 physical cores are recommended on the grounds of performance.</td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB+ RAM</td>
</tr>
<tr>
<td>Hard drive storage</td>
<td>100 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>• Note the requirements of Microsoft for the version of SQL Server you are using.</td>
</tr>
<tr>
<td></td>
<td>UNIX and Linux operating systems</td>
</tr>
<tr>
<td></td>
<td>• Note the operating system manufacturer’s minimum requirements for SQL Server databases.</td>
</tr>
<tr>
<td>Software</td>
<td>Following versions are supported:</td>
</tr>
<tr>
<td></td>
<td>• SQL Server 2017 Standard Edition (64-bit) with the current cumulative update</td>
</tr>
<tr>
<td></td>
<td>• SQL Server 2016 Standard Edition (64-bit), Service Pack 2 with the current cumulative update</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For performance reasons, the use of SQL Server Enterprise Edition is recommended.</td>
</tr>
<tr>
<td></td>
<td>• SQL Server Management Studio (recommended)</td>
</tr>
</tbody>
</table>
NOTE: In virtual environments, you must ensure that the VM host provides performance and resources to the database server according to system requirements. Ideally, resource assignments for the database server are fixed. Furthermore, optimal I/O performance must be provided, in particular for the database server. For more information about virtual environments, see Product Support Policies.

Related topics

- Database server settings and the One Identity Manager database on page 23
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26

Database server settings and the One Identity Manager database

For installation and operation of a One Identity Manager database, the following database server and database settings are required:

Table 6: Database server settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>English</td>
<td></td>
</tr>
<tr>
<td>Server Collation</td>
<td>Case insensitive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL_Latin1_General_CP1_CI_AS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(empfohlen)</td>
<td></td>
</tr>
<tr>
<td>Extreme transaction processing</td>
<td>True</td>
<td>One Identity Manager uses In-Memory-OLTP (Online Transactional Processing) for memory-optimized data accesses. The database server must support extreme transaction processing (XTP). This function is activated by default in a standard installation. The setting is tested by the Configuration Wizard before installing or updating One Identity Manager database. If XTP is not activated, the installation or update is not started.</td>
</tr>
<tr>
<td>supported (is XTP supported)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Server Agent</td>
<td>Started</td>
<td>Start the SQL Server Agent in the SQL Server Service Management Portal. You can log in on an SQL Server Agent as a domain user with Windows authentication or with a local system account.</td>
</tr>
</tbody>
</table>
The setting is tested by the Configuration Wizard before installing or updating One Identity Manager database. If the SQL Server Agent is not started, the installation or update is not started.

Table 7: Database settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collation</td>
<td>SQL_Latin1_General_CP1_CI_AS</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Recovery model</td>
<td>Simple</td>
<td>The setting is tested by the Configuration Wizard before installing the One Identity Manager database. If the recovery model is not set to the value <strong>Simple</strong>, the installation is not started.</td>
</tr>
<tr>
<td>Compatibility level</td>
<td>SQL Server 2016 (130)</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Auto Create Statistics</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Auto Update Statistics</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Auto Update Statistics Asynchronously</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Arithmetic Abort enabled</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Quoted Identifiers Enabled</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Property</td>
<td>Value</td>
<td>Comment</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Broker Enabled</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Is Read Committed Snapshot On</td>
<td>True</td>
<td>The default setting for transactions is <strong>AutoCommit</strong>. If transactions are required, they are opened explicitly. These settings have proven to provide the best balance between data security and performance for One Identity Manager’s massive parallel processing. Other transaction modes are not supported by One Identity Manager. The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
</tbody>
</table>
| Database file and date file group for memory-optimized tables | Required | One Identity Manager uses In-Memory-OLTP (Online Transactional Processing) for memory-optimized data accesses. For the creation of memory-optimized tables, the following prerequisites must be met:  
  - A database file with the file type **Filestream data** must exist.  
  - A memory-optimized data filegroup must exist.  
  Before installation or update of the One Identity Manager database, the Configuration Wizard checks whether these requirements are fulfilled. In Configuration Wizard, repair methods are offered in order to create the database file and the data file group. The database file is created by the repair method in the directory of the data file (*.mdf). |


Related topics

- Minimum system requirements for the database server on page 22
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26

Users with granular permission for the One Identity Manager database on an SQL Server

The following users are identified for using a One Identity Manager database on an SQL Server with the granular permissions concept. User permissions at server and database level are matched to their tasks.

NOTE: If you want to switch to granular permissions when you update from 8.1.x at a later date, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

- Installation user

  The installation user is needed for the initial installation of a One Identity Manager database using the Configuration Wizard.

  NOTE: If you want to change to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.1, you will also require an installation user.

- Administrative user

  The administrative user is used by One Identity Manager components that require permissions at server and database level, including for example the Configuration Wizard, DBQueue Processor or the One Identity Manager Service.

- Configuration user

  The configuration user can execute configuration tasks within the One Identity Manager, for example, creating customer-specific schema extensions or working with the Designer. Configuration users need permissions at the server and database levels.

- End user

  End users are only assigned permissions at database level in order, for example, to complete tasks with the Manager or the Web Portal.

Permissions for installation users

An SQL Server login and a database user with the following permissions must be provided for the installation user.
SQL Server:

- Member of **dbcreator** server role
  This server role is required if the database is created by the Configuration Wizard and if you are updating from version 7.0.x, 7.1.x or 8.0.x to version 8.1.1.

- Member of **securityadmin** server role
  This server role is required to create the SQL Server logins.

- **Permission view server state and permission alter any connection with the option with grant option**
  These permissions are required to check connections and close these if necessary.

- **alter any server role permission**
  This permission is required to create the server role for the administrative user.

**msdb database:**

- **Select** permission with the option **with grant option** for the **dbo.sysjobs**, **dbo.sysjobschedules**, **dbo.sysjobactivity** and **dbo.sysschedules** tables
  These permissions are required to execute and monitor database schedules.

- **alter any user** permission
  This permission is required to create the necessary database users for the administrative user.

- **Permission alter any role**
  This permission is required to create the necessary database role for the administrative user.

- Member of the **SQLAgentUserRole** database role
  This database role is required for managing database schedules during an update from version 7.0.x, 7.1.x or 8.0.x to version 8.1.1.

**master database:**

- **alter any user** permission
  This permission is required to create the necessary database users for the administrative user.

- **Permission alter any role**
  This permission is required to create the necessary database role for the administrative user.

- **Permission Execute with the option with grant option** for the procedure **xp_readerrorlog**
  This permission is required to find out information about the database server's system status.
One Identity Manager database:

- Member of the **db_owner** database role
  This database role is only required if you wish to use an existing database or a schema update is performed when installing the schema with the Configuration Wizard.

**Permissions for administrative users**

The following principal elements with the permissions are created for the administrative user during the installation of the One Identity Manager database with the Configuration Wizard:

**SQL Server:**

- **OneIMAdminRole_<DatabaseName>** server role
  - **alter any server role** permission
    This permission is required to create the server role for the configuration user.
  - **view any definition** permission
    The permission is required to link the SQL Server logins for the configuration user and the end user with the corresponding database users.

- **<DatabaseName>_Admin** SQL server login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - Permission **view server state** and permission **alter any connection** with the option **with grant option**
    These permissions are required to check connections and close these if necessary.

**msdb database:**

- **OneIMRole_<DatabaseName>** database role
  - Member of the **SQLAgentUserRole** database role
    The database role is required to execute database schedules.
  - **Select** permission for the **dbo.sysjobs**, **dbo.sysjobschedules**, **dbo.sysjobactivity** and **dbo.sysschedules** tables
    The permissions are required to execute and monitor database schedules.

- **OneIM_<DatabaseName>** database user
  - Member of the **OneIMRole_<DatabaseName>** database role
  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.
master database:

- **OneIMRole_<DatabaseName>** database role
  - Permission **Execute** for the procedure `xp_readerrorlog`
    This permission is required to find out information about the database server's system status.

- **OneIM_<DatabaseName>** database user
  - Member of the **OneIMRole_<DatabaseName>** database role
  - The database user is assigned to the `<DatabaseName>_Admin` SQL server login.

One Identity Manager database:

- **Admin** database user
  - Member in **db_owner** database role
    The database role is required to update a database with the Configuration Wizard.
  - The database user is assigned to the `<DatabaseName>_Admin` SQL server login.

**Permissions for configuration users**

The following principal elements with the permissions are created for configuration users during the installation of the One Identity Manager database with the Configuration Wizard:

**SQL Server:**

- **OneIMConfigRole_<DatabaseName>** server role
  - Permission **view server state** and permission **alter any connection**
    These permissions are required to check connections and close these if necessary.

- `<DatabaseName>_Config` SQL login
  - Member of the **OneIMConfigRole_<DatabaseName>** server role

One Identity Manager database:

- **OneIMConfigRoleDB** database role
  - **Create Procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create View**, **Insert**, **Execute**, **Create function** permissions for the database

- **Config** database user
  - Member of the **OneIMConfigRoleDB** database role
  - The database user is connected with the `<DatabaseName>_ConfigSQL Server login.`
Permissions for end users

The following principals are created with the permissions for end users during the installation of the One Identity Manager database with the Configuration Wizard:

SQL Server:

- `<DatabaseName>_User` SQL login

One Identity Manager database:

- `OneIMUserRoleDB` database role
  - `Insert`, `Update`, `Select`, `Delete` permissions for selected tables in the database
  - `View Definition` permission for the database
  - Permissions `Execute` and `References` for individual function, procedures and types
- `User` database user
  - Member of the `OneIMUserRoleDB` database role
  - The database user is connected with the `<DatabaseName>_User` SQL Server login.

Tips for using integrated Windows authentication

Integrated Windows authentication can be used without restriction for the One Identity Manager Service and the web applications. Integrated Windows authentication can be used for FAT clients. Use of Windows groups for logging in is supported. To ensure functionality it is strongly recommended you use SQL Server login.

To implement Windows authentication

- Set up an SQL Server login for the user account on the database server.
- Enter `dbo` as the default schema.
- Assign the required permissions SQL server login.

Requirements for a managed instance in Azure SQL Database

To operate the One Identity Manager database in a managed instance in Azure SQL Database, you require the Business critical tier. For more detailed information, see the Microsoft site under https://azure.microsoft.com/en-us/services/sql-database/.
Related topics

- Database server settings and the One Identity Manager database in a managed instance in an Azure SQL Database on page 31
- Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33

Database server settings and the One Identity Manager database in a managed instance in an Azure SQL Database

For installation and operation of a One Identity Manager database, the following database server and database settings are required:

Table 8: Database server settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>English</td>
<td></td>
</tr>
<tr>
<td>Server Collation</td>
<td>Case insensitive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL_Latin1_General_CP1_CI_AS (empfohlen)</td>
<td></td>
</tr>
<tr>
<td>Extreme transaction processing supported</td>
<td>True</td>
<td>Default setting.</td>
</tr>
<tr>
<td>(is XTP supported)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Server Agent</td>
<td>Started</td>
<td>Default setting.</td>
</tr>
</tbody>
</table>

Table 9: Database settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collation</td>
<td>SQL_Latin1_General_CP1_CI_AS</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Recovery model</td>
<td>Full</td>
<td>Default setting.</td>
</tr>
<tr>
<td>Compatibility level</td>
<td>SQL Server 2016 (130)</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Auto Create Statistics</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Property</td>
<td>Value</td>
<td>Comment</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identity Manager database and adjusted for the database if necessary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Update Statistics</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Auto Update Statistics Asynchronously</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Arithmetic Abort enabled</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Quoted Identifiers Enabled</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Broker Enabled</td>
<td>True</td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Is Read Committed Snapshot On</td>
<td>True</td>
<td>The default setting for transactions is <strong>AutoCommit</strong>. If transactions are required, they are opened explicitly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These settings have proven to provide the best balance between data security and performance for One Identity Manager's massive parallel processing. Other transaction modes are not supported by One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</td>
</tr>
<tr>
<td>Database file and date file group for memory-optimized tables</td>
<td>Required</td>
<td>Default setting.</td>
</tr>
</tbody>
</table>
Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database

The following users are identified for using a One Identity Manager database in a managed instance in the Azure SQL Database with the granular permissions concept. User permissions at server and database level are matched to their tasks.

- Installation user
  The installation user is needed for the initial installation of a One Identity Manager database using the Configuration Wizard.

- Administrative user
  The administrative user is used by One Identity Manager components that require permissions at server and database level, including for example the Configuration Wizard, DBQueue Processor or the One Identity Manager Service.

- Configuration user
  The configuration user can execute configuration tasks within the One Identity Manager, for example, creating customer-specific schema extensions or working with the Designer. Configuration users need permissions at the server and database levels.

- End user
  End users are only assigned permissions at database level in order, for example, to complete tasks with the Manager or the Web Portal.

Permissions for installation users

An SQL Server login and a database user with the following permissions must be provided for the installation user.

SQL Server:

- Member of dbcreator server role
  The server role is only required if the database is created using the Configuration Wizard.

- Member of securityadmin server role
  This server role is required to create the SQL Server logins.

- Permission view server state and permission alter any connection with the option with grant option
  These permissions are required to check connections and close these if necessary.

- alter any server role permission
  This permission is required to create the server role for the administrative user.
msdb database:

- **Select** permission with the option **with grant option** for the `dbo.sysjobs`, `sysjobsteps`, `dbo.sysjobschedules`, `dbo.sysjobactivity` and `dbo.sysschedules` tables
  The permissions are required to execute and monitor database schedules.

- **alter any user** permission
  This permission is required to create the necessary database users for the administrative user.

- **Permission alter any role**
  This permission is required to create the necessary database role for the administrative user.

master database:

- **alter any user** permission
  This permission is required to create the necessary database users for the administrative user.

- **Permission alter any role**
  This permission is required to create the necessary database role for the administrative user.

- **Permission Execute with the option with grant option** for the procedure `xp_readerrorlog`
  This permission is required to find out information about the database server's system status.

- **Execute permissions with the option with grant option** for the `xp_sqlagent_is_starting`, `xp_sqlagent_notify` and `xp_sqlagent_enum_jobs` procedures
  The permissions are required to execute and monitor database schedules.

One Identity Manager database:

- **Member of the db_owner database role**
  This database role is only required if you wish to use an existing database or a schema update is performed when installing the schema with the Configuration Wizard.

Permissions for administrative users

The following principal elements with the permissions are created for the administrative user during the installation of the One Identity Manager database with the Configuration Wizard:
SQL Server:

- **OneIMAdminRole_<DatabaseName>** server role
  - **alter any server role** permission
    This permission is required to create the server role for the configuration user.
  - **view any definition** permission
    The permission is required to link the SQL Server logins for the configuration user and the end user with the corresponding database users.

- **<DatabaseName>_Admin** SQL server login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - Permission **view server state** and permission **alter any connection** with the option **with grant option**
    These permissions are required to check connections and close these if necessary.

msdb database:

- **OneIMRole_<DatabaseName>** database role
  - Member of the **SQLAgentUserRole** database role
    The database role is required to execute database schedules.
  - **Select** permission for the `dbo.sysjobs`, `sysjobsteps`, `dbo.sysjobschedules`, `dbo.sysjobactivity` and `dbo.sysschedules` tables
    The permissions are required to execute and monitor database schedules.

- **OneIM_<DatabaseName>** database user
  - Member of the **OneIMRole_<DatabaseName>** database role
  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

master database:

- **OneIMRole_<DatabaseName>** database role
  - Permission **Execute** for the procedure `xp_readerrorlog`
    This permission is required to find out information about the database server’s system status.
  - **Execute** permission for the `xp_sqlagent_is_starting`, `xp_sqlagent_notify` and `xp_sqlagent_enum_jobs` procedures
    The permissions are required to execute and monitor database schedules.

- **OneIM_<DatabaseName>** database user
  - Member of the **OneIMRole_<DatabaseName>** database role
  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.
One Identity Manager database:

- **Admin** database user
  - Member in **db_owner** database role
    - The database role is required to update a database with the Configuration Wizard.
  - The database user is assigned to the `<DatabaseName>_Admin` SQL server login.

**Permissions for configuration users**

The following principal elements with the permissions are created for configuration users during the installation of the One Identity Manager database with the Configuration Wizard:

**SQL Server:**

- **OneIMConfigRole_<DatabaseName>** server role
  - Permission **view server state** and permission **alter any connection**
    - These permissions are required to check connections and close these if necessary.
- `<DatabaseName>_Config` SQL login
  - Member of the **OneIMConfigRole_<DatabaseName>** server role

One Identity Manager database:

- **OneIMConfigRoleDB** database role
  - **Create Procedure, Delete, Select, Create table, Update, Checkpoint, Create View, Insert, Execute, Create function** permissions for the database
  - **Config** database user
    - Member of the **OneIMConfigRoleDB** database role
    - The database user is connected with the `<DatabaseName>_Config` SQL Server login.

**Permissions for end users**

The following principals are created with the permissions for end users during the installation of the One Identity Manager database with the Configuration Wizard:

**SQL Server:**

- `<DatabaseName>_User` SQL login
One Identity Manager database:

- **OneIMUserRoleDB** database role
  - **Insert, Update, Select, Delete** permissions for selected tables in the database
  - **View Definition** permission for the database
  - Permissions **Execute** and **References** for individual function, procedures and types
- **User** database user
  - Member of the **OneIMUserRoleDB** database role
  - The database user is connected with the `<DatabaseName>_User` SQL Server login.

## Minimum system requirements for administrative workstations

One Identity Manager administration and configuration tools are installed on an administrative workstation in order to edit and display data.

The following system prerequisites must be guaranteed for installing tools on an administrative workstation.

**Table 10: Minimum system requirements - administrative workstations**

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>4 physical cores 2 GHz+</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB+ RAM</td>
</tr>
<tr>
<td>Hard drive storage</td>
<td>1 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>Following versions are supported:</td>
</tr>
<tr>
<td></td>
<td>Windows 10 (32-bit or 64-bit) minimum version 1511</td>
</tr>
<tr>
<td></td>
<td>Windows 8.1 (32-bit or 64-bit) with the current Service Pack</td>
</tr>
<tr>
<td></td>
<td>Windows 7 (32-bit or non-Itanium 64-bit) with the current service pack</td>
</tr>
<tr>
<td>Additional software</td>
<td>Microsoft .NET Framework Version 4.7.2 or later</td>
</tr>
<tr>
<td>Supported browsers</td>
<td>Internet Explorer 11 or later</td>
</tr>
<tr>
<td></td>
<td>Firefox (Release Channel)</td>
</tr>
<tr>
<td></td>
<td>Chrome (Release Channel)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Edge (Release Channel)</td>
</tr>
</tbody>
</table>

Additional: Minimum system requirements for administrative workstations
Minimum system requirements for the service server

The One Identity Manager Service enables the distribution of the information administrated in the One Identity Manager database throughout the network. The One Identity Manager Service performs data synchronization between the database and any connected target systems and executes actions at the database and file level.

The following system prerequisites must be fulfilled to install the One Identity Manager Service on a server.

**Table 11: Minimum system requirements - services server**

<table>
<thead>
<tr>
<th>Processor</th>
<th>8 physical cores 2.5 GHz+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>16 GB RAM</td>
</tr>
<tr>
<td>Hard drive storage</td>
<td>40 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>Following versions are supported:</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later</td>
</tr>
<tr>
<td>Linux operating systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Linux operating system (64-bit), supported by the Mono project, or Docker images provided by the Mono project.</td>
</tr>
</tbody>
</table>

**Additional software**

<table>
<thead>
<tr>
<th>Windows operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft .NET Framework Version 4.7.2 or later</td>
</tr>
</tbody>
</table>

**NOTE:** Take the target system manufacturer’s recommendations for connecting the target system into account.

<table>
<thead>
<tr>
<th>Linux operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mono 5.14 or higher</td>
</tr>
</tbody>
</table>

**Related topics**

- Users for One Identity Manager on page 41
Minimum system requirements for the web server

The following system prerequisites must be fulfilled to install web applications on a web server.

Table 12: System requirements - web server

<table>
<thead>
<tr>
<th>Processor</th>
<th>4 physical cores 1.65 GHz+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>4 GB RAM</td>
</tr>
<tr>
<td>Hard drive storage</td>
<td>40 GB</td>
</tr>
</tbody>
</table>

**Operating system**

Windows operating systems

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later

Linux operating systems

- Linux operating system (64-bit), supported by the Mono project, or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.

**Additional software**

Windows operating systems

- Microsoft .NET Framework Version 4.7.2 or later
- Microsoft Internet Information Services 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and the Role Services:
  - Web Server | Common HTTP Features | Static Content
  - Web Server | Common HTTP Features | Default Document
  - Web Server | Application Development | ASP.NET
  - Web Server | Application Development | .NET Extensibility
  - Web Server | Application Development | ISAPI Extensions
  - Web Server | Application Development | ISAPI Filters
Minimum system requirements for the application server

The application server provides a connection pool for accessing the database and stores business logic. The following system prerequisites must be fulfilled for installation of the application server.

Table 13: System requirements - application server

<table>
<thead>
<tr>
<th>Processor</th>
<th>8 physical cores 2.5 GHz+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>8 GB RAM</td>
</tr>
<tr>
<td>Hard drive storage</td>
<td>40 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>Following versions are supported:</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later</td>
</tr>
</tbody>
</table>

Linux operating systems

- NTP - Client
- Mono 5.14 or higher
- Apache HTTP Server 2.0 or 2.2 with the following modules:
  - mod_mono
  - rewrite
  - ssl (optional)
Linux operating system (64-bit), supported by the Mono project, or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.

Windows operating systems
- Microsoft .NET Framework Version 4.7.2 or later
- Microsoft Internet Information Services 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2 and the Role Services:
  - Web Server | Common HTTP Features | Static Content
  - Web Server | Common HTTP Features | Default Document
  - Web Server | Application Development | ASP.NET
  - Web Server | Application Development | .NET Extensibility
  - Web Server | Application Development | ISAPI Extensions
  - Web Server | Application Development | ISAPI Filters
  - Web Server | Security | Basic Authentication
  - Web Server | Security | Windows Authentication
  - Web Server | Performance | Static Content Compression
  - Web Server | Performance | Dynamic Content Compression

Linux operating systems
- NTP - Client
- Mono 5.14 or higher
- Apache HTTP Server 2.0 or 2.2 with the following modules:
  - mod_mimo
  - rewrite
  - ssl (optional)

**NOTE:** In order to use the application server's REST API, the HTTP request methods POST, GET, PUT and DELETE must be permitted by the web server (IIS/Apache).

## Users for One Identity Manager

### Table 14: Users for One Identity Manager

<table>
<thead>
<tr>
<th>User</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User for</td>
<td>The installation user is needed for the initial installation of a One Identity</td>
</tr>
<tr>
<td>User</td>
<td>Permissions</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>installing One Identity Manager</td>
<td>Manager database using the Configuration Wizard. For detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.</td>
</tr>
<tr>
<td>User for administrative tasks in One Identity Manager</td>
<td>The administrative user is used by components of One Identity Manager that require authorizations at server level and database level, for example, the Configuration Wizard, the DBQueue Processor, or the One Identity Manager Service. For detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.</td>
</tr>
<tr>
<td>User for configuration tasks in One Identity Manager</td>
<td>The configuration user can execute configuration tasks within the One Identity Manager, for example, creating customer-specific schema extensions or working with the Designer. Configuration users need permissions at the server and database levels. For detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.</td>
</tr>
<tr>
<td>End user for One Identity Manager</td>
<td>End users are only assigned permissions at database level in order, for example, to complete tasks with the Manager or the Web Portal. For detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.</td>
</tr>
<tr>
<td>User for Logging into One Identity Manager</td>
<td>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.</td>
</tr>
<tr>
<td>User account for the One Identity Manager Service</td>
<td>The user account for One Identity Manager Service requires rights to carry out operations at file level, for example, assigning user rights and creating and editing directories and files. The user account must belong to the Domain users group. The user account must have the Login as a service extended user right. The user account requires access rights to the internal web service.</td>
</tr>
</tbody>
</table>
NOTE: If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call:

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

The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.

In the default installation the One Identity Manager is installed under:

- %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)
- %ProgramFiles%\One Identity (on 64-bit operating systems)

NOTE: Other target system specific permissions may be required for synchronizing the One Identity Manager with each target system. These permissions are explained in the corresponding guide.

For more information, see Setting up permissions for creating an HTTP server on page 43.

### Setting up permissions for creating an HTTP server

The log files of the One Identity Manager Service can be displayed using an HTTP server (http://<Servername>:\:<Portnumber>).

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
```
Communications ports and firewall configuration

One Identity Manager is made up of several components that can be executed in different network segments. In addition, One Identity Manager requires access to various network services, which can also be installed in different network segments. You must open various ports depending on which components and services you want to install behind the firewall.

The following ports are required:

Table 15: Communications port

<table>
<thead>
<tr>
<th>Default port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>Port for communicating with the One Identity Manager database.</td>
</tr>
<tr>
<td>1880</td>
<td>Port for the HTTP protocol of One Identity Manager Service.</td>
</tr>
<tr>
<td>2880</td>
<td>Port for access tests with the Synchronization Editor, such as in the target system browser or for simulating synchronization.</td>
</tr>
<tr>
<td>80</td>
<td>Port for accessing web applications.</td>
</tr>
<tr>
<td>88</td>
<td>Kerberos authentication system. (if Kerberos authentication is implemented).</td>
</tr>
<tr>
<td>135</td>
<td>Microsoft End Point Mapper (EPMAP) (also, DCE/RPC Locator Service).</td>
</tr>
<tr>
<td>137</td>
<td>NetBIOS Name Service.</td>
</tr>
<tr>
<td>139</td>
<td>NetBIOS Session Service.</td>
</tr>
</tbody>
</table>

Other ports for connecting to target systems are also required. These ports are listed in the corresponding guides.
Installing the One Identity Manager

The following steps are required to install One Identity Manager:

1. Installation of One Identity Manager tools on the administrative workstation on which the One Identity Manager database schema installation will be started.
2. Installing and configuring the One Identity Manager database.
3. Setting up the server, which handles the SQL processes.
   a. The server must be entered in the database as a Job server with the server function SQL processing server.
   b. A One Identity Manager Service with direct access to the One Identity Manager database must be installed and configured on the server.

   NOTE: Multiple SQL processing servers can be set up to spread the load of SQL processes.

4. Setting up an update server for automatic software updating of other servers.
   a. The server must be entered in the database as a Job server with the server function Update server.
   b. A One Identity Manager Service with direct access to the One Identity Manager database must be installed and configured on the server.

   NOTE: You can proceed with setting up an SQL processing server and the update server using the Configuration Wizard.

You can also install the following:

- Install more workstations
- Install more server with One Identity Manager Service
- Install an application server
- Install the Web Portal on a Web server
- Install the Password Reset Portal on a Web server

For more detailed information about installing and configuring the Password Reset Portal, see the One Identity Manager Web Application Configuration Guide.

- Install the Manager web application on a Web server
Install more Web services like SPML Web service or SOAP Web Service.
For detailed information about installing the web services, see the One Identity Manager Configuration Guide.

You can install and update the One Identity Manager using the following methods.

- Use the installation wizard to install the One Identity Manager components on workstations for the first time.
- Use the installation wizards to install the One Identity Manager Service on servers for the first time or remote with the Server Installer.
- To update an existing installation use the auto update software.
- Use the installation wizard to manually update individual workstations and servers.

**Detailed information about this topic**

- Before you start installing One Identity Manager on page 46
- Installing One Identity Manager components on page 47
- Installing and configuring a One Identity Manager database on page 50
- Installing and configuring the One Identity Manager Service on page 75
- Installing an application server on page 113
- Installing the Web Portal on page 126
- Installing and updating the Manager web application on page 144
- Updating the One Identity Manager on page 93

**Before you start installing One Identity Manager**

Before you start installing One Identity Manager:

- Ensure that the workstations and servers meet the minimal hardware and software requirements.
- End all programs and service components otherwise installation cannot begin.

**NOTE:** A separate upgrade package is available for the update from One Identity Manager version 6.x to One Identity Manager version 7.0. For all inquiries, please contact the support desk. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.
Detailed information about this topic

- Installation prerequisites on page 21
- Installing the One Identity Manager on page 45
- Updating the One Identity Manager on page 93

Installing One Identity Manager components

An installation wizard is available to help you through the installation of One Identity Manager components on workstations and servers.

NOTE: Always start installing administration and configuration tools on an administrative workstation if possible.

To install the One Identity Manager components

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. Switch to the Installation tab, select the edition and click Install.
3. This starts the installation wizard. On the start page, select the language for the installation wizard.
4. Confirm the conditions of the license.
5. On the Installation settings page, enter the following information.
   - Installation source: Select the directory containing the installation files.
   - Installation directory: Select the directory in which you want to install the files for One Identity Manager.
     
     NOTE: To make further configuration settings, click on the arrow button next to the input field. Here, you can specify whether you are installing on a 64-bit or a 32-bit operating system. For a standard installation, no further configuration settings are necessary.

   - Select installation modules using the database: Set this option to load the installation data using the existing One Identity Manager database.
     
     NOTE: Leave this option empty to install the workstation on which you start the One Identity Manager schema installation.

   - Add further modules to the selected edition: Set this option to add additional One Identity Manager modules to the selected edition.

6. On the Module selection page, also select the modules to be installed.
7. Enter the database connection data on **Connect to database**.

   **NOTE:** This page is only shown if you have set the **Select installation modules with existing database** option.

a. Select the connection in **Select a database connection**.

   - OR -

   Click on **Add new connection**, select a system type and enter connection data.

### Table 16: SQL Server database connection data

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Database server.</td>
</tr>
<tr>
<td>Windows authentication</td>
<td>Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td>
</tr>
<tr>
<td>User</td>
<td>SQL Server Login name.</td>
</tr>
<tr>
<td>Password</td>
<td>SQL Server login password.</td>
</tr>
<tr>
<td>Database</td>
<td>Database.</td>
</tr>
</tbody>
</table>

b. In the **Authentication method** area, select the authentication module and enter the login data for the system user ID.

Which login data you require depends on the authentication module selected.

8. On the **Assign machine roles** page, define the machine roles.

   **NOTE:** The machine roles appropriate for the One Identity Manager modules are activated. All machine subroles are selected when you select the machine role. You can deselect individual packages.

9. On the **Change service properties** page, you can change the name, display name and the description for installing the One Identity Manager Service.

   **NOTE:** This page is only shown if you have selected the machine role **Server | Job Server**.

10. You can start different programs for further installation on the last page of the install wizard.

    - To perform installation of the One Identity Manager schema, start the Configuration Wizard and follow the instructions of the Configuration Wizard.
NOTE: Perform this step only on the workstation on which you start the installation of the One Identity Manager schema.

- To create the configuration of the One Identity Manager Service, start the program Job Service Configuration.

NOTE: Execute this step only on servers on which you have installed the One Identity Manager Service.

11. Click Finish to close the installation wizard.
12. Close the autorun program.

The One Identity Manager is installed for all user accounts on the workstation or server. In the default installation the One Identity Manager is installed under:

- %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)
- %ProgramFiles%\One Identity (on 64-bit operating systems)

Related topics

- Before you start installing One Identity Manager on page 46
- Installation prerequisites on page 21
- One Identity Manager tools on page 13
- Installing the One Identity Manager components on a Windows terminal server on page 49
- Installing and configuring a One Identity Manager database on page 50
- Installing and configuring the One Identity Manager Service on page 75
- Appendix: Machine roles and installation packages on page 181

Installing the One Identity Manager components on a Windows terminal server

To install One Identity Manager tools on a Windows terminal server you need to ensure that the Windows terminal server has been fully installed and configured. This includes profile handling in particular as well as permissions for Windows terminal server use.

NOTE: Ensure that in an Active Directory Domain, users also have relevant permissions to use the Windows terminal server self.

To install One Identity Manager components on a Windows terminal server

1. Log in with a user account, which has administrator permissions on the Windows terminal server.
Log in through a console connection is recommended. For this call, enter the following command:

Start/Ausführen: mstsc /Console /v:<servername>

where <servername> must be replaced with the server name of the terminal server (without leading ")

2. Open the command line console (CMD.exe) and switch the Windows terminal server into software installation mode with help of the command CHANGE USER /INSTALL.

3. Start the installation wizard and install the One Identity Manager components as described.

4. End the software installation mode on the Windows terminal server with the command CHANGE USER /EXECUTE in the command line console.

After the installation is complete, anyone who is an authorized Windows terminal server user can start the One Identity Manager tools and use them.

For more information about software installation on Windows terminal servers, refer to the Windows operating system documentation you are using.

Related topics

- Installing One Identity Manager components on page 47

## Installing and configuring a One Identity Manager database

To set up the One Identity Manager database, use the Configuration Wizard. The Configuration Wizard executes the following steps.

1. Installs the One Identity Manager schema in a database.
   
   The Configuration Wizard can create a new database and install the One Identity Manager schema. Alternatively, the One Identity Manager schema can be installed in an existing database.

2. Creating the required SQL Server logins and database users with permissions for the administrative user, configuration user and end user.

3. Creates administrative system users and permissions groups.

4. Installing and configuring a One Identity Manager Service with direct access to the database for handling SQL processes and automatic server software updates.

| NOTE: Further steps are executed in One Identity Manager depending on the Edition and Configuration Wizard modules.

Other steps are required to configure the One Identity Manager database following the schema installation:
Configure the database for a test, development or live system.

Other system settings may be required for putting individual functions into operation in One Identity Manager.

Use configuration parameters to configure the behavior of the system’s basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. You can find an overview of all configuration parameters in Base data | General | Configuration parameters in Designer.

In certain circumstances, it is necessary to store encrypted information in the One Identity Manager database. Use the program Crypto Configuration to do this.

You can log changes to data and information from process handling in One Identity Manager. All entries logged in One Identity Manager are initially saved in the One Identity Manager database. The proportion of historical data to total volume of a One Identity Manager database should not exceed 25%. Otherwise performance problems may arise. You must ensure that log entries are regularly removed from the One Identity Manager database and archived.

For more information about process monitoring and process history, see the One Identity Manager Configuration Guide. For more information about archiving data, see the One Identity Manager Data Archiving Administration Guide.

**Detailed information about this topic**

- Notes on setting up a One Identity Manager database on page 52
- Installing and configuring the One Identity Manager database on page 53
- Configuring a One Identity Manager database for testing, development or production on page 60
- Encrypting database information on page 61
- One Identity Manager vendor notification on page 67
- Setting up the email notification system on page 69

**Related topics**

- Minimum system requirements for the database server on page 22
- Requirements for a managed instance in Azure SQL Database on page 30
- Installing One Identity Manager components on page 47
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26
- Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33
Notes on setting up a One Identity Manager database

- The following prerequisites must be fulfilled on the workstation from which you want to start the One Identity Manager database setup:
  - Installing the Configuration Wizard
    Use the install wizard to install the program. To do this, select the **Workstation** machine role and the **Configuration** installation package in the installation wizard.
  - Access to the installation sources
    - **NOTE:** If you copy the installation files to a repository, you must ensure that the relative directory tree remains intact.

- To ensure that HTML applications are be successfully compiled, you must download packages from the NPM repository. Ensure that the workstation you are compiling on, can establish a connection to the website registry.npmjs.org:443.
  - Alternatively, you can download packages from a proxy server and install them manually.

- An installation user with permissions for installing a One Identity Manager database must exist. For detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.

- It is not recommended to select a user with Windows authentication for installing the database. If you decide to use it anyway, ensure that your environment supports Windows authentication. You must use the same user to update the database.

- If you want to install the One Identity Manager schema in an existing database, ensure that the database has the required settings. For more information, see Database server settings and the One Identity Manager database on page 23 and Database server settings and the One Identity Manager database in a managed instance in an Azure SQL Database on page 31.

- Always start Configuration Wizard on an administrative workstation.

- The program executes remote installation of One Identity Manager Service. Remote installation is only supported within a domain or a trusted domain.

- If you start the Configuration Wizard on a server on which you also want to configure a One Identity Manager Service, simply skip the section for installing the service on the local server in the Configuration Wizard. Install the One Identity Manager Service with the installation wizard in this case. For more information, see Installing and configuring the One Identity Manager Service on page 75.

- If you are working with an encrypted One Identity Manager database, see Notes on working with an encrypted One Identity Manager database on page 66.
Installing and configuring the One Identity Manager database

**IMPORTANT:** Always start the Configuration Wizard on an administrative workstation. If you start the Configuration Wizard on a server on which you also want to configure a One Identity Manager Service, simply skip the section for installing the service on the local server in the Configuration Wizard.

To install a database in the Configuration Wizard

1. Start the Configuration Wizard.
2. Select the **Create and install a database** option on the Configuration Wizard home page and click **Next**.
3. To use an existing database, perform the following steps on the **Create administrative connection** page.
   a. Enable **Advanced**.
   b. In the **Advanced options** pane, set the **Use an existing, empty database for installation** option.
   c. Enter the following connection data for the database.
      - **Server**: Database server.
      - (Optional) **Windows Authentication**: Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
      - **User**: SQL Server Login name of the installation user.
      - **Password**: Password for the installation user.
      - **Database**: Select the database.

   - OR -

To install a new database, enter the following database connection data on the **Create administrative connection** page.
   - **Server**: Database server.
   - (Optional) **Windows Authentication**: Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
   - **User**: SQL Server Login name of the installation user.
   - **Password**: Password for the installation user.

4. If you are using an existing database, on the **Create database** page, **Installation source** view, select the directory containing the installation files.

   - OR -

One Identity Manager 8.1.1 Installation Guide
Installing the One Identity Manager
If you are creating a new database, perform the following tasks on the Create database page.

a. In the **Database properties** view, enter the following information about the database.

**Table 17: Database properties**

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database name</td>
<td>Name of the database.</td>
</tr>
<tr>
<td>Data directory</td>
<td>Directory in which the data file is created. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>&lt;browse&gt;: Select a directory using the file browser.</td>
</tr>
<tr>
<td></td>
<td>&lt;directory name&gt;: Directory in which data files are already installed.</td>
</tr>
<tr>
<td>Log directory</td>
<td>Directory in which the transaction log file is created. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>&lt;browse&gt;: Select a directory using the file browser.</td>
</tr>
<tr>
<td></td>
<td>&lt;directory name&gt;: Directory in which transaction log files are already installed.</td>
</tr>
<tr>
<td>Memory tables directory</td>
<td>Directory for data file group and database file for memory-optimized tables. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>&lt;browse&gt;: Select a directory using the file browser.</td>
</tr>
<tr>
<td></td>
<td>&lt;Directory name&gt;: Directory in which data files for memory-optimized tables are already installed.</td>
</tr>
<tr>
<td>Initial size</td>
<td>Initial size of the database files. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>&lt;custom&gt;: User-defined entry.</td>
</tr>
<tr>
<td></td>
<td>Different recommended sizes: Depending on the number of employees being administrated.</td>
</tr>
</tbody>
</table>

b. Select the directory with the installation files in **Installation source**.

5. Select the configuration module on **Select configuration module**.
If you started the Configuration Wizard from the install wizard, the configuration modules for the selected edition are already activated. Check the module selection in this case.

Select the configuration module at this point if you started the Configuration Wizard directly. Dependent configuration modules are selected automatically.

6. On the **Create a new login for administrators** page, decide which SQL server login to use for administrative users. You have the following options:

- **Create new SQL Server logins for the database**: Select this option if you want to set up a new administrative login on the SQL Server. Other SQL Server logins with permissions for system configuration and for end users are created after the database has been migrated.

  Enter the login name, password and password confirmation for the new SQL Server login.

  **NOTE**: The password must meet the Windows policy requirements for passwords.

- **Use the current SQL Server login for the database**: When you select this option, no additional SQL Server logins are created for the database. In this case, you cannot work with the granular permissions concept at SQL level. The user you specified is used to connect to the database.

  **NOTE**: If you want to switch to granular permissions at a later time, contact Support. To access the Support Portal, go to [https://support.oneidentity.com/identity-manager/](https://support.oneidentity.com/identity-manager/).

7. Error that prevent processing the database are displayed on the **Database check** page. Correct the errors before you continue with the installation.

8. The installation steps are shown on the **Processing database** page.

  Installation and configuration of the database is automatically carried out by the Configuration Wizard. This procedure may take some time depending on the amount of data and system performance. Once processing is complete, click **Next**.

  **TIP**: Set **Advanced** to obtain detailed information about processing steps and the migration log.

9. On the **Create SQL server logins** page, enter the login name, the password and password confirmation for the SQL Server logins for configuration users and end users.

  **NOTE**: The password must meet the Windows policy requirements for passwords.

10. On the **System information** page, enter the customer information and create administrative system users for One Identity Manager.
a. In the **Customer information** view, enter the full name of the company.

b. In the **System user** view, you configure the predefined administrative system users and enter your own administrative system users.
   - Enter a password and password confirmation for the predefined system users.
   - To create customer-specific system users, click the + button and enter the name, password and password confirmation.
   - **TIP:** Use the <...> button next to the name of a system user to configure further settings for that system user. You can also adjust these settings in the Designer at a later time.

c. *(Optional)* Create custom permissions groups.
   The Configuration Wizard creates custom permissions groups, which you can use to define permissions for any custom schema extensions you require.
   - For non-role-based login, the permission groups **CCCViewPermissions** and **CCCEditPermissions** are created. Administrative system users are automatically added to these permissions groups.
   - For role-based login, the permission groups **CCCViewRole** and **CCCEditRole** are created.

   **To create additional permissions groups**
   - i. Enable the **Advanced** option and in the **Permissions groups** view, click the + button.
   - ii. Enter the name for the permissions group. Label custom permission groups with the prefix **CCC**.
   - iii. For role-based permissions groups, enable the **Role-based** option.

11. On the **Service installation** page, you can create a Job server for the server on which the One Identity Manager database is installed.
   - **NOTE:** If you do not want to set up a One Identity Manager Service at this stage, select **Skip service installation.**
a. Enter the following information to install the One Identity Manager Service.

**Table 18: Installation data**

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Server on which to install and start the service from.</td>
</tr>
<tr>
<td></td>
<td><strong>To select a server</strong></td>
</tr>
<tr>
<td></td>
<td>- Enter a name for the server.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Select an entry from the list.</td>
</tr>
<tr>
<td>Service account</td>
<td>User account data for the One Identity Manager Service.</td>
</tr>
<tr>
<td></td>
<td><strong>To enter a user account for the service</strong></td>
</tr>
<tr>
<td></td>
<td>- Set the option <strong>Local system account</strong>.</td>
</tr>
<tr>
<td></td>
<td>This starts the One Identity Manager Service under the <strong>NT AUTHORITY\SYSTEM</strong> account.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Enter user account, password and password confirmation.</td>
</tr>
<tr>
<td>Installation account</td>
<td>Data for the administrative user account to install the service.</td>
</tr>
<tr>
<td></td>
<td><strong>To enter an administrative user account for installation</strong></td>
</tr>
<tr>
<td></td>
<td>- Enable <strong>Advanced</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Enable the option <strong>Current user</strong>.</td>
</tr>
<tr>
<td></td>
<td>This uses the user account of the current user.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>- Enter user account, password and password confirmation.</td>
</tr>
<tr>
<td>Machine roles</td>
<td>Specify the machine role. The <strong>Job server</strong> machine role is defined by default. You can add more machine roles.</td>
</tr>
</tbody>
</table>

b. Check the One Identity Manager Service configuration. Enable **Advanced**.

**NOTE:** The initial service configuration is predefined already. If further changes need to be made to the configuration, you can do this later with the Designer. For more detailed information about configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.

c. Click **Next** to start installing the service.

Installation of the service occurs automatically and may take some time.

**NOTE:** The service is entered with the name **One Identity Manager Service** in the server service management.
12. Click **Finish** on the last page of Configuration Wizard.

**Related topics**

- Notes on setting up a One Identity Manager database on page 52
- Error messages when installing and updating the One Identity Manager database on page 160
- Editing the One Identity Manager database during setup using the Configuration Wizard on page 58

**Editing the One Identity Manager database during setup using the Configuration Wizard**

Installation and configuration of the One Identity Manager database is automatically carried out by the Configuration Wizard. The Configuration Wizard can create a new database and install the One Identity Manager schema. Alternatively, the One Identity Manager schema can be installed in an existing database.

The Configuration Wizard performs the following steps when processing the database:

- Creates the required SQL Server logins and database users with permissions for the administrative user, configuration user and end user. For more information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26.

- Installing the One Identity Manager schema.

Before the schema installation can take place the Configuration Wizard tests the database. Error messages are displayed in a separate window. The errors must be corrected manually. The schema installation cannot be started until these are resolved.

All the tables, data types, database procedures that are required are loaded into the database through migration. The selected Editions and configuration modules are enabled. During migration, calculation tasks are queued in the database. These are processed by the DBQueue Processor.

When a schema is installed with the Configuration Wizard, migration date and migration revision are recorded in the database's transport history.

- Compiling the system.

Scripts, templates and processes are declared in the database. The **System user** authentication module with the **viadmin** system user is used for compilation.

- Uploading files for automatic software update.

In order to distribute One Identity Manager files using the automatic software updating mechanism, the files are loaded into the One Identity Manager database.

- Creates administrative system users and permissions groups.
A system user is required for authentication in One Identity Manager. One Identity Manager provides various system users whose permissions are matched to the various tasks. For detailed information about system users, access rights and granting permissions, see the One Identity Manager Authorization and Authentication Guide.

The viadmin system user is the default system user in One Identity Manager. This system user can be used to compile and initialize the One Identity Manager database and for the first user login to the administration tools.

**IMPORTANT:** Do not use the viadmin system user in a live environment. Create your own system user with the appropriate permissions.

Custom system users are created as administrative system users by the Configuration Wizard. Administrative system users are automatically added to all non-role-based permissions groups, and are assigned all permissions of the system user viadmin.

- Installing and configuring a One Identity Manager Service with direct access to the database for handling SQL processes and automatic server software updates.

The One Identity Manager Service handles defined processes. The service has to be installed on the One Identity Manager network server to execute the processes. The server must be declared as a “Job server” in the One Identity Manager database.

During the initial schema installation with the Configuration Wizard, in the One Identity Manager database a Job server is already created for the server on which the One Identity Manager database is installed. This Job server receives the server functions **SQL processing server** and **Update server**.

- The SQL processing server handles SQL processes.
- The update sever ensures that software is updated automatically on other servers.

The SQL processing server and the update server require a direct connection to the One Identity Manager database to handle processes. Use the Configuration Wizard to install the One Identity Manager Service on a server for handling these processes.

The Configuration Wizard executes the following steps.

- Installs the One Identity Manager Service components
- Configuring the One Identity Manager Service
- Starting the One Identity Manager Service

**Related topics**

- Automatic updating of One Identity Manager on page 85
- Displaying the transport history and checking the One Identity Manager version on page 158
## Configuring a One Identity Manager database for testing, development or production

You use the staging level of the One Identity Manager database to specify whether the database is a test database, development database or a live database. A number of database settings are controlled by the staging level. The following database settings are configured when you change the staging level.

### Table 19: Database settings for development, test and live environments

<table>
<thead>
<tr>
<th>Setting</th>
<th>Development Environment</th>
<th>Test Environment</th>
<th>Live Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color of the One Identity Manager tools status bar</td>
<td>none</td>
<td>Green</td>
<td>Yellow</td>
</tr>
<tr>
<td>Maximum DBQueue Processor runtime</td>
<td>20 minutes</td>
<td>40 minutes</td>
<td>120 minutes</td>
</tr>
<tr>
<td>Maximum number of slots for DBQueue Processor</td>
<td>5</td>
<td>7</td>
<td>Maximum number of slots according to the hardware configuration</td>
</tr>
</tbody>
</table>

### To modify a database staging level

1. Open the Launchpad and select **Database staging level**. Starts the Designer.
2. Select the database and change the value of the **Staging level** property to **Test environment**, **Development environment** or **Live environment**.
3. Select **Database | Save to database** and click **Save**.

The DBQueue Processor configuration settings are configured for normal operations and must not be modified normally. The configuration settings are reduced for test environments and development environments because several databases may be located on a server.

If it is necessary to change the settings for testing or development environments for reasons of performance, you must modify the following configuration parameter settings in the Designer.


### Table 20: Configuration parameters for the DBQueue Processor

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QBM</td>
<td>DBQueue</td>
</tr>
<tr>
<td>Exception: Enter a value of 0 for using the maximum number of slots available based on the hardware configuration.</td>
<td></td>
</tr>
</tbody>
</table>

| QBM | DBQueue | KeepAlive | This configuration parameter regulates the maximum runtime of the central dispatcher. Tasks on slots currently in use are still processed when the timeout expires. Then the slot database schedules are stopped and the central dispatches exits. |
| The lowest permitted value for runtime is 5 minutes; the maximum permitted value is 720 minutes. |

### Related topics

- Appendix: Creating a One Identity Manager database for a test or development environment from a database backup on page 169

### Encrypting database information

In certain circumstances, it is necessary to store encrypted information in the One Identity Manager database.

- In Designer, choose the configuration parameter **Common | EncryptionScheme** to define which encryption method to use. Permitted values are:
  - **RSA**: RSA encryption with AES for large data (default).
  - **FIPSCertifiedRSA**: FIPS certified RSA with AES for large data. This method is used if encryption must match the FIPS 1040-2 standard. The local security policy **Use FIPS compliant algorithms for encryption, hashing, and signing** must be enabled.

  **NOTE:** If the configuration parameter **Common | EncryptionScheme** is not set, RSA is used as the method.

- Encryption is carried out using the Crypto Configuration program. With this program an encryption file is created and the contents of the database columns that are effected are converted. The encrypted data is stored in the database table **DialogDatabase**.

  **NOTE:** It is recommended that you create a backup before encrypting the database information in a database. Then you can restore the previous state if necessary.
Creating a new database key and encrypting the database information

**NOTE:** It is recommended that you create a backup before encrypting the database information in a database. Then you can restore the previous state if necessary.

To create a new database key and encrypt the One Identity Manager database

1. Open Launchpad and select Encrypt database. This starts the Crypto Configuration program.
2. Click Next on the start page.
3. On the New database connection page, enter the valid connection data for the One Identity Manager database and click Next.
4. Select Create or change database key on the Select action page and click Next.
5. Select There was no encryption yet on Private key and click Next.
6. Create a new key on New private key.
   a. Click Create key.
   b. Select the directory path for saving the file using the file browser and enter a name for the key file.
   c. Click Save.
      The (*.key) key file is generated. The file browser is closed. The path and filename are displayed under Private key.
   d. Click Next.
      This establishes which data is encrypted.
7. The date to be encrypted is displayed on the Convert database page.
   a. Click Convert.
   b. Confirm the following two security questions with Yes.
      The data encryption is started. Conversion progress is displayed.
   c. Click Next.
8. Click Finish on the last page to end the program.
Related topics

- Changing a database key and encrypting the database information on page 63
- Re-encrypting the database information on page 64
- Decrypting the database information on page 65
- Notes on working with an encrypted One Identity Manager database on page 66

Changing a database key and encrypting the database information

**NOTE:** To change a database key, you need the key file with the old database key. The key is change and saved in a new key file.

**NOTE:** It is recommended that you create a backup before encrypting the database information in a database. Then you can restore the previous state if necessary.

**To change a database key and encrypt the One Identity Manager database**

1. Open Launchpad and select Encrypt database. This starts the Crypto Configuration program.
2. Click Next on the start page.
3. On the New database connection page, enter the valid connection data for the One Identity Manager database and click Next.
4. Select Create or change database key on the Select action page and click Next.
5. Load the existing key on Private key.
   a. Select Encryption was enabled.
   b. Click Load key.
   c. Using the file browser, select the (*.key) file with the old database key.
   d. Click Open.
      The file browser is closed. The path and file name are shown.
   e. Click Next.
6. Create a new key on New private key.
   a. Click Create key.
   b. Select the directory path for saving the file using the file browser and enter a name for the key file.
   c. Click Save.
      The (*.key) key file is generated. The file browser is closed. The path and filename are displayed under Private key.
d. Click **Next**.
   This establishes which data is encrypted.

7. The date to be encrypted is displayed on the **Convert database** page.
   a. Click **Convert**.
   b. Confirm the following two security questions with **Yes**.
      The data encryption is started. Conversion progress is displayed.
   c. Click **Next**.

8. Click **Finish** on the last page to end the program.

**Related topics**
- Creating a new database key and encrypting the database information on page 62
- Re-encrypting the database information on page 64
- Decrypting the database information on page 65
- Notes on working with an encrypted One Identity Manager database on page 66

**Re-encrypting the database information**

Use this method when you mark more database columns with the option **Encrypted** and the database is already encrypted.

**NOTE:** It is recommended that you create a backup before encrypting the database information in a database. Then you can restore the previous state if necessary.

**To repeat One Identity Manager database encryption using an existing database key**

1. Open Launchpad and select **Encrypt database**. This starts the Crypto Configuration program.
2. Click **Next** on the start page.
3. On the **New database connection** page, enter the valid connection data for the One Identity Manager database and click **Next**.
4. Select **Encrypt using existing key** on the **Select action** page and click **Next**.
   This establishes which data is encrypted.
5. The date to be encrypted is displayed on the **Convert database** page.
   a. Click **Convert**.
   b. Confirm the following two security questions with **Yes**.
      The data encryption is started. Conversion progress is displayed.
   c. Click **Next**.
6. Click **Finish** on the last page to end the program.
Related topics

- Creating a new database key and encrypting the database information on page 62
- Changing a database key and encrypting the database information on page 63
- Decrypting the database information on page 65
- Notes on working with an encrypted One Identity Manager database on page 66

Decrypting the database information

**NOTE:** You need the file with the database key for this.

**NOTE:** It is recommended that you create a backup before encrypting the data in a database. Then you can restore the previous state if necessary.

To decrypt the One Identity Manager database

1. Open Launchpad and select **Encrypt database**. This starts the Crypto Configuration program.
2. Click **Next** on the start page.
3. On the **New database connection** page, enter the valid connection data for the One Identity Manager database and click **Next**.
4. Select **Decrypt data** on the **Select action** page and click **Next**.
   This establishes which data is encrypted.
5. The date to be encrypted is displayed on the **Convert database** page.
   a. Click **Convert**.
   b. Confirm the following two security questions with **Yes**.
   c. The data encryption is started. Conversion progress is displayed.
   d. Using the file browser, select the (* .key) file with the database key.
   e. Click **Open**.
      The file browser is closed. The data decryption is started. Conversion progress is displayed.
   f. Click **Next**.
6. Click **Finish** on the last page to end the program.

Related topics

- Creating a new database key and encrypting the database information on page 62
- Changing a database key and encrypting the database information on page 63
- Re-encrypting the database information on page 64
- Notes on working with an encrypted One Identity Manager database on page 66
Notes on working with an encrypted One Identity Manager database

If you encrypt a One Identity Manager database, you must declare the database key to the One Identity Manager Service.

**CAUTION:** If the One Identity Manager Service finds a private key in the installation directory on startup, it places the key in the Windows internal key container of its service account and deletes the file from the hard drive. So save the private key at another location in addition to the service install directory!

**To declare the database key**

- Declare the following information in the One Identity Manager Service configuration file. Use the Job Server Editor in Designer or the Job Service Configuration program to edit the configuration file. For more detailed information, see the One Identity Manager Configuration Guide.

### Table 21: Configuring the One Identity Manager Service for encryption

<table>
<thead>
<tr>
<th>Configuration module</th>
<th>Parameters</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>JobServiceDestination</td>
<td>Encryption method (EncryptionScheme)</td>
<td>Encryption method used</td>
</tr>
<tr>
<td>JobServiceDestination</td>
<td>File with private key (PrivateKey)</td>
<td>Enter the file with the encryption information. The default file is private.key.</td>
</tr>
<tr>
<td>JobServiceDestination</td>
<td>Private key identifier (KeyId)</td>
<td>Identifier of the private key. Use this parameter if you work with several private keys, for example, if One Identity Manager Service data must be exchanged between two encrypted One Identity Manager databases. If no ID is specified, a search is performed for the private.key file.</td>
</tr>
<tr>
<td>File with the private key</td>
<td></td>
<td>Private key identifier and path to private key file. The ID is expected in the JobServiceDestination in the parameter <strong>PrivateKey identifier (KeyId)</strong> The default key has the ID <strong>Default</strong>.</td>
</tr>
</tbody>
</table>
- Save the key file created in the service’s install directory.
- Open the service management and restart the One Identity Manager Service.

**NOTE:** The file with the private key must exist in the server's installation directory on all servers with an active One Identity Manager Service.

**NOTE:** If you change the One Identity Manager Service user account, you must save the key file in the service’s install directory again.

**Detailed information about this topic**
- Encrypting database information on page 61

**One Identity Manager vendor notification**

Give us the opportunity to keep you up-to-date. The interfaces to other systems are being developed continually. Enable vendor notifications to receive news about important program updates for your system.

If vendor notification is enabled, One Identity Manager generates a list of system settings once a month and sends it to One Identity. This list does not contain any personal data. The list will be reviewed by our customer support team who will look for material changes in a proactive effort to identify potential issues before they materialize on your system. The lists may be used by our R&D staff for analysis, diagnosis, and replication for testing purposes. We will keep and refer to this information for as long as your company remains on support for this product.

**NOTE:** You can check the latest system information at any time in the Help | Info menu.

**Detailed information about this topic**
- Enabling vendor notification on page 67
- Checking the vendor notification on page 68
- Disabling vendor notification on page 68

**Enabling vendor notification**

**Prerequisite for Vendor Notification**
- A Job server is configured as SMTP host for sending mail in One Identity Manager.
- The configuration parameters for email notification are configured.
To enable a vendor notification

1. Start the Launchpad and log in on the One Identity Manager database.
   NOTE: You can only configure vendor notification in Launchpad on a One Identity Manager database with the **Live environment** staging level.

2. Select Configure vendor notification and click Start.
   This starts the Designer and opens the Configuration Parameter Editor.

3. Enable the configuration parameter **Common | MailNotification | VendorNotification** and enter the email address of your business contact.
   The email address is used as the return address for notifying vendors.

4. Select Database | Save to database and click Save.

Detailed information about this topic

- Checking the vendor notification on page 68
- Disabling vendor notification on page 68
- Setting up the email notification system on page 69

Checking the vendor notification

NOTE: You can only configure vendor notification in Launchpad on a One Identity Manager database with the **Live environment** staging level.

**To check whether vendor notification is enabled**

- Start the Launchpad and log in on the One Identity Manager database.
  - Look at the **Configure vendor notification** in the installation view to see if the functionality is enabled.

Detailed information about this topic

- Enabling vendor notification on page 67
- Disabling vendor notification on page 68

Disabling vendor notification

NOTE: You can only configure vendor notification in Launchpad on a One Identity Manager database with the **Live environment** staging level.
To disable a vendor notification

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select Configure vendor notification and click Start.
   This starts the Designer and opens the Configuration Parameter Editor.
3. Disable the configuration parameter Common | MailNotification | VendorNotification.
4. Select Database | Save to database and click Save.

Related topics

- Enabling vendor notification on page 67
- Checking the vendor notification on page 68

Setting up the email notification system

The One Identity Manager sends email notifications about various actions taken within the system. Thus, various notifications are sent to requester and approver within the request process. In the same way, notifications about attestation cases are sent or reports delivered by email. Notifications are sent when an actions is successfully or unsuccessfully executed during process handling.

You can implement custom notifications in addition to predefined notification processes.

To use the notification system

1. Use the Job Server Editor to set up a Job server as a SMTP host for mail distribution.
2. Check the configuration parameters for the email notification system in the Base data | General | Configuration parameters category in Designer and customize the values.

   **NOTE:** In addition to the configuration parameters listed in the following, other configuration parameters may be necessary for different notification processes. Some configuration parameters are only available if the module is installed.

Table 22: General configuration parameters for mail notification

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>InternationalEMail</td>
</tr>
</tbody>
</table>
**Configuration parameter** | **Meaning**
--- | ---
*IMPORTANT:* The mail server must also support this function. If necessary, you must override the script VID_IsSMTPAddress

Common | MailNotification | Notification data.

Common | MailNotification | AcceptSelfSignedCert | If this configuration parameter is set, self-signed TLS connection certificates are accepted.

Common | MailNotification | AllowServerNameMismatchInCert | If this configuration parameter is set, server names that do not match are permitted by TLS connection certificates.

Common | MailNotification | DefaultAddress | Default email address (recipient) for sending notifications.

Common | MailNotification | DefaultCulture | Default language that emails are sent in if no language can be determined for a recipient.

Common | MailNotification | DefaultLanguage | Default language for sending messages.

Common | MailNotification | DefaultSender | Default email address (sender) for sending notifications.

Common | MailNotification | Encrypt | Specifies whether emails are encrypted.

Common | MailNotification | Encrypt | ConnectDC | Domain controller to use.

Common | MailNotification | Encrypt | ConnectPassword | User password. This is optional.

Common | MailNotification | Encrypt | ConnectUser | User account for querying Active Directory. This is optional.

Common | MailNotification | Encrypt | DomainDN | Distinguished name of the domain to search through.

Common | MailNotification | Encrypt | EncryptionCertificateScript | Script, which supplies a list of encrypted certificates (default: QBM_GetCertificates).

Common | MailNotification | NotifyAboutWaitingJobs | Specifies whether a message should be sent if the process steps have a particular execution state in the job queue.

Common | MailNotification | SignCertificateThumbprint | SHA1 thumbprint of the certificate to use for the signature. This can be in the computer's or the user's My Store.
<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuration parameter | Meaning
--- | ---
Common | MailNotification | Enables the email address of your company’s contact person. The email address is used as the return address for notifying vendors.

If the configuration parameter is set, One Identity Manager generates a list of system settings once a month and sends the list to One Identity. This list does not contain any personal data. You can check the latest system information at any time by selecting Help | Info in the menu. The list will be reviewed by our customer support team who will look for material changes in a proactive effort to identify potential issues before they materialize on your system. The lists may be used by our R&D staff for analysis, diagnosis, and replication for testing purposes. We will keep and refer to this information for as long as your company remains on support for this product.

### Table 23: Additional parameters for email notifications

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Attestation</td>
</tr>
<tr>
<td>QER</td>
<td>ComplianceCheck</td>
</tr>
<tr>
<td>QER</td>
<td>ITShop</td>
</tr>
<tr>
<td>QER</td>
<td>Policy</td>
</tr>
<tr>
<td>QER</td>
<td>RPS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>Exchange2000</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>ADS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>AzureAD</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>AzureAD</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>CSM</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>EBS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>LDAP</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>NDO</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>SAPR3</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>SharePoint</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>Unix</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>UNS</td>
</tr>
<tr>
<td>TargetSystem</td>
<td>PAG</td>
</tr>
</tbody>
</table>
Related topics

- Setting up Job servers on page 76
- Message: Enter email address in configuration parameter on page 164
Installing and configuring the One Identity Manager Service

The One Identity Manager Service handles defined processes. The service has to be installed on the One Identity Manager network server to execute the processes. The server must be declared as a "Job server" in the One Identity Manager database.

Setting up a Job server requires the following steps:

- Create an entry for the Job server in the One Identity Manager database.
- Specify the machine roles and server functions for the Job server.
  Installation packages to be installed on the Job server are found, depending on the selected machine roles. The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.
- Install the One Identity Manager Service.
- Configure the One Identity Manager Service.
- Start the One Identity Manager Service.

Related topics

- Setting up Job servers on page 76
- Remote installation of the One Identity Manager Service with the Server Installer on page 77
- Displaying the One Identity Manager Service log file on page 80
- Changing the user account or One Identity Manager Service start type on page 81
- The One Identity Manager Service in a cluster on page 81
- Updating the One Identity Manager on page 93
- Appendix: Machine roles and installation packages on page 181
Setting up Job servers

Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using exactly this queue name.

- Enter this queue name in the One Identity Manager Service configuration file.
- A Job server must be known in the One Identity Manager database for each queue.

There are several methods for setting up a Job server:

- For the initial schema installation with the Configuration Wizard, you already set up a Job server with the server functions **SQL processing server** and **Update server**. Use the Configuration Wizard to configure the service and install the service remotely on a server.
- To configure further Job servers, use the Server Installer program.
  Using the Server Installer, you create the Job server with its machine roles and server functions in the database. Use the Server Installer to configure the service and install the service remotely on a server.
- You can create Job servers in the Designer.
  In Designer, you can create a Job server with the machine roles and server functions, configure the service on the server and install the service remotely. For detailed information, see **One Identity Manager Configuration Guide**.
- If a remote installation is not possible, you can install and configure the service locally on a server.
  - Install the service components on the server using the installation wizard.
  - Configure the service using the Job Service Configuration program. For more detailed information about configuring the One Identity Manager Service, see the **One Identity Manager Configuration Guide**.
  - If the configuration parameter **Common | Jobservice | AutoCreateServerFromQueues** is enabled, in response to queries from the One Identity Manager Service for unknown queues, new Job servers are created in the database. Information about machine roles and server functions is transferred to the database.

**NOTE:** If you subsequently change server functions for a Job server in the database, for example using the Designer, the system checks whether the required components are installed on the server, and updates the server if necessary. To enable this, automatic software updates must be active.

Related topics

- **Installing and configuring the One Identity Manager database** on page 53
- **Remote installation of the One Identity Manager Service with the Server Installer** on page 77
Remote installation of the One Identity Manager Service with the Server Installer

**IMPORTANT:** If you are working with an encrypted One Identity Manager database, see Notes on working with an encrypted One Identity Manager database on page 66.

Use the One Identity Manager Service to install the Server Installer. The program executes the following steps:

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of One Identity Manager Service components corresponding to the machine roles.
- Configuration of One Identity Manager Service.
- Starts the One Identity Manager Service.

**NOTE:** The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.

For remote installation of One Identity Manager Service, you require an administrative workstation on which the One Identity Manager components are installed.

**To install and configure One Identity Manager Service remotely on a server**

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the Database connection page.
3. Specify the server on which you want to install One Identity Manager Service on the Server properties page.
   - Select a Job server from the Server menu.
     - OR -
       To create a new Job server, click Add.
   - Enter the following data for the Job server.
### Table 24: Job server properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</td>
</tr>
<tr>
<td>Queue</td>
<td>Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.</td>
</tr>
<tr>
<td>Full server name</td>
<td>Full server name in accordance with DNS syntax. Example: &lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</td>
</tr>
</tbody>
</table>

| NOTE: You can use the Extended option to make changes to other properties for the Job server. You can also edit the properties later with Designer. |

4. Specify which roles the Job server is to have in One Identity Manager on the Machine roles page. Installation packages to be installed on the Job server are found depending on the selected machine role.

5. Specify the function of the server in the One Identity Manager environment on the Server functions page. One Identity Manager processes are handled depending on the server function.
   
   The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.

6. Check the One Identity Manager Service configuration on the Service settings page.
   
   | NOTE: The initial service configuration is predefined already. If further changes need to be made to the configuration, you can do this later with the Designer. For detailed information about configuring the service, see the One Identity Manager Configuration Guide. |

7. To configure remote installations, click Next.

8. Confirm the security prompt with Yes.

9. Select the directory with the install files on Select installation source.

10. Select the file with the private key on the page Select private key file.
   
   | NOTE: This page is only displayed when the database is encrypted. |

11. Enter the service's installation data on the Service access page.
Table 25: Installation data

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Server on which to install and start the service from.</td>
</tr>
<tr>
<td><strong>To select a server</strong></td>
<td>• Enter a name for the server.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>• Select a entry from the list.</td>
</tr>
<tr>
<td>Service account</td>
<td>User account data for the One Identity Manager Service.</td>
</tr>
<tr>
<td><strong>To enter a user account for the One Identity Manager Service</strong></td>
<td>• Set the option Local system account.</td>
</tr>
<tr>
<td></td>
<td>This starts the One Identity Manager Service under the NT AUTHORITY\SYSTEM account.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>• Enter user account, password and password confirmation.</td>
</tr>
<tr>
<td>Installation account</td>
<td>Data for the administrative user account to install the service.</td>
</tr>
<tr>
<td><strong>To enter an administrative user account for installation</strong></td>
<td>• Enable Advanced.</td>
</tr>
<tr>
<td></td>
<td>• Enable Current user.</td>
</tr>
<tr>
<td></td>
<td>This uses the user account of the current user.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>• Enter user account, password and password confirmation.</td>
</tr>
</tbody>
</table>

12. Click **Next** to start installing the service.
   Installation of the service occurs automatically and may take some time.

13. Click **Finish** on the last page of Server Installer.

| NOTE: The service is entered with the name One Identity Manager Service in the server service management. |

**Related topics**

- Minimum system requirements for the service server on page 38
- Users for One Identity Manager on page 41
- Changing the user account or One Identity Manager Service start type on page 81
- Appendix: Machine roles and installation packages on page 181
Displaying the One Identity Manager Service log file

The One Identity Manager Service log file can be displayed in a browser. 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 3: 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 26: Log file color code

<table>
<thead>
<tr>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Processing successful.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Warnings occurred during processing.</td>
</tr>
<tr>
<td>Red</td>
<td>Fatal errors occurred during processing.</td>
</tr>
</tbody>
</table>

NOTE: If you want to retain the color information to send by mail, you need to save the complete web page.
Changing the user account or One Identity Manager Service start type

When One Identity Manager Service is installed the service is already entered in the "Services" on the computer.

To customize login data and the way the service is started

1. Open the service management of the server and select the entry One Identity Manager Service in the list of services.
2. Open service properties with the context menu item Properties.
3. On the General tab, change the start type if necessary.
   The start type Automatic is recommended.
4. Change the user account under which the service runs on the Login tab.
5. Click Apply.
6. Close the service's properties with OK.
7. Start the service from the context menu item Start.
   If the One Identity Manager Service cannot be started, a corresponding message is written to the server event log.

   **NOTE:** If you change the One Identity Manager Service user account, you must save the service’s configuration file in the service’s install directory again.

   **NOTE:** If you are working with an encrypted One Identity Manager database, see Notes on working with an encrypted One Identity Manager database on page 66.

Related topics

- Minimum system requirements for the service server on page 38
- Users for One Identity Manager on page 41

The One Identity Manager Service in a cluster

The idea of a cluster solution is to make the system highly available. The aim is to limit system failure to only a few seconds if a hardware or software component fails. This can be achieved with the installation of a Windows cluster solution (only possible with Enterprise servers). The following diagram shows such a solution.
This cluster is made up of 2 physical computers "Server A" and "Server B" that use the same disk array and have their own individual system hard drive. Every server has a Windows operating system. Both servers are installed identically so that in the case of failure one server can take over from the other.

All redundant system components are managed by the cluster manager. From an external point of view, the cluster is addressed as a single, virtual server "Server C". The service or user that is accessing the service is automatically connected to the physical server that is currently carrying out the work in the cluster.

If one of the servers fails, then the redundant server in the cluster automatically takes over. The virtual server remains the contact partner, only the physical server that is running, changes.

**Detailed information about this topic**

- Registering the One Identity Manager Service in a cluster on page 82
- Installing and configuring the One Identity Manager Service in a cluster on page 83

**Registering the One Identity Manager Service in a cluster**

Once registered, the One Identity Manager Service is governed by cluster handling for site resilience and load balancing. The service is installed on a virtual server which simulates
the cluster. All computer related operations and service data operate, transparently, with the virtual server and not the real computer (cluster nodes). This also applies to clients that contact the service through the server name, for example RPC (ORPC, DCOM), TCP/IP (Winsock, Named Pipes), HTTP.

Because the service is in the context of the virtual server, note the following facts:

- The service-specific settings for the node on which the virtual server is located are replicated to all other nodes. The service, therefore, always has the same configuration independent of the node on which it is actually started.
- The service is always started only on the current node of the virtual server (the virtual server's current node). The service is stopped on all other nodes.
- The service is booted and shutdown with the virtual server. If the cluster is not enabled, the service is stopped on all nodes.
- Services on nodes are brought automatically in the required state (manual or stopped) before registration by the program.

Related topics

- The One Identity Manager Service in a cluster on page 81
- Installing and configuring the One Identity Manager Service in a cluster on page 83

Installing and configuring the One Identity Manager Service in a cluster

The installation of server components from the One Identity Manager installation medium needs to be done on all the physical nodes of the cluster.

| NOTE: | In the configuration of the JobServiceDestination, the parameter Queue must contain the name of the virtual server. |

After saving the configuration, the configuration file in the One Identity Manager Service installation directory needs to be copied to all the physical nodes. Here you must not change the name of the configuration file.

| NOTE: | One Identity Manager Service configuration is not part of a cluster resource. Thus, each node keeps its own configuration. For this reason, it is necessary to ensure that the configuration files on the physical nodes are consistent. If this is not the case, correct functionality cannot be guaranteed after changing cluster nodes. |

Setting up a Cluster Resource for the One Identity Manager Service

In the Cluster Administrator program, set up a new cluster resource for the One Identity Manager Service and make this available online. For information about this procedure, refer to Microsoft Technet under http://technet.microsoft.com/en-us/library/cc787285 (WS.10).aspx. Note the following when creating the cluster resource:
Select the resource type **Generic Service**.

Select the following One Identity Manager Service dependencies.
- Cluster IP address
- Cluster name
- Quorum; for example, disc: D

Do not enter anymore registration keys.

**NOTE:** After setting up the One Identity Manager Service in a cluster system it is advisable to simulate a failover so that possible problems with the cluster do not arise during live operations.

**Storing the One Identity Manager Service log file on a Shared Volume**

- In the Cluster Administrator program, set up a new cluster resource for the and make this available online. Note the following when creating the cluster resource:
  - Select the **File Share** resource type.
  - Select at least the following dependency:
    - One IdentityOne Identity Manager Service

- In the configuration file of the One Identity Manager Service, adapt the directory information in the **Log file** (OutPutFile) parameter of the log writer.

- Copy the configuration file to all the physical cluster nodes in the One Identity Manager Service install directory after you have changed it.

**Related topics**

- The One Identity Manager Service in a cluster on page 81
- Registering the One Identity Manager Service in a cluster on page 82
Automatic updating of One Identity Manager

Particularly local installation and updating of software can prove to be a problem due to the distributed structure of servers and workstations. To help guarantee an acceptable workload for network administrators, a method for updating One Identity Manager automatically has been developed for One Identity Manager. Apart from updating the usual One Identity Manager installation files, new custom files can be simply added to the procedure and are, therefore, distributed to workstations and servers in the One Identity Manager network using the automatic software updating mechanism.

Detailed information about this topic

- Basics for automatic software update on page 85
- Implementing the automatic software update on page 90
- Disabling automatic update on page 91

Basics for automatic software update

All files in a One Identity Manager installation are saved with their name and binary code in QBMFileRevision in the One Identity Manager database. The file size and hash values of each file are stored to identify them. Additionally, each file's affiliation to machine roles and installation packages is entered in the table QBMFileHasDeployTarget.

The necessary files are loaded into the One Identity Manager database and updated when a hotfix, a service pack or a full version update is run.

In the database, a semaphore software revision is maintained. When a file is added, changed or deleted in the database, the semaphore value is recalculated by the DBQueue Processor. In every One Identity Manager installation directory there is a file Softwarerevision.viv. This file is assigned the permissions Read only and Not visible in the file system, and therefore is not normally displayed by the operating system.

The Softwarerevision.viv contains the following information.
The installation revision number
The revision status is determined from the value of the SoftwareRevision semaphore in the database.

The start time of the last modification

As of One Identity Manager version 8.0, the Update.zip file is stored in the QBMFileRevision table. The file plays a central role in automatic updating. The Zip archive contains all the files that are required on the clients or server for updating the product. The Zip archive is not part of the One Identity Manager installation data but is recreated after the database has been updated by the Configuration Wizard and also the Software Loader.

The Zip archive contains the following files:
- Update.exe
- VI.Base.dll
- NLog.dll
- Newtonsoft.Json.dll
- InstallManager.Msi.dll
- InstallManager.Core.dll

The zip archive is extended with all files from the installation data that correspond to the name filter *.Update.dll. This makes it possible for different modules to contribute more functionality to the automatic update.

In addition, the installation directory of all One Identity Manager installations contains the file InstallState.config. This file contains information about the installed machine roles, installation packages and files.

Whether a software update is required, depends on the comparison of semaphore values from the database and the file .softwarerevision.viv If semaphore values vary, machine roles for the computer or server are determined based on the InstallState.config. Each file belonging to a machine role is check to see if the file is known to the database.

If the file exists in the data, the following checks are made:
- Has the file size changed?
  - If this is the case, the file is added to the list of files to be updated.
- Has the hash value changed?
  - If this is the case, the file is added to the list of files to be updated.

New files that have been loaded into the One Identity Manager database through a hotfix, a service pack or a version update are also added to the list. All the files in the list are updated.

All actions are logged in the file update.log. After the update has finished, the current semaphore value is copied from the database to the file softwarerevision.viv.
Related topics

- Automatic updating of the One Identity Manager tools on page 87
- Automatic updating of the One Identity Manager Service on page 88
- Automatic updating of web applications on page 89
- Implementing the automatic software update on page 90
- Disabling automatic update on page 91

Automatic updating of the One Identity Manager tools

When a program starts up, VI.D8.dll creates a connection to the database and carries out the semaphore test. If the file softwarerevision.viv is not found, a new file is added.

If the One Identity Manager installation directory does not have write access, an error message is displayed and the software update continues.

The update program (Updater.exe) expects a login by an administrator when user account control is active, assuming the logged in user does not have administration permissions for the installation directory (for example %ProgramFiles%). If installation takes place in a directory without user account control, the query does not apply. Then the update process is started.

The application then loads the file Update.zip from the database or from the application server, which is unpacked in a temporary directory.

In the first step, the Update.exe informs the main application whether it can run an update or not. Depending on the configuration, the user may still be able to cancel the automatic update at this point.

To prevent further applications from starting during the update, a file called Update.lock is created in the installation directory. The trigger program and the update program (Updater.exe) write their process ID in the file. The Update.lock file is deleted from the installation directory once updating has been successfully completed. The program is then restarted. To ensure that automatic updating is restarted when an application is restarted after quitting unexpectedly, Update.lock files older than two hours are ignored. If none of the processes whose IDs are saved in the Update.lock file exist on the workstation when the application is restarted, the Update.lock file is also ignored and the update is restarted.

Before actually updating, the preparation steps that prepare the installation for the update, are called from the *.Update.dlls. A preparation step might be renaming a machine role, for example.

For the actual update, the Update.exe searches for all the necessary files and saves them in a temporary directory. Communication with the system is established through the client application to be updated because only it has the required permissions for contacting the database or the application server. Once all the required files have been transferred, the Update.exe takes control and starts the data exchange. At this point the user is prompted to quit all running applications that might interfere with the update process. At the same time,
administrator permissions requirements are authorized by user account control, if necessary.

In this update procedure, not only the files are exchanged but other migration steps from the *.Update.dlls are also executed. The functionality in these migration steps is not restricted. Typical examples are customizations in the registry database or configuration files and removal of obsolete program data on the computers. These migration steps are executed after the files have been exchanged.

If all the update steps have been carried out successfully, the Update.exe creates a new SoftwareRevision.viv and restarts the client application. The Update.exe then ends and removes the temporary working directory itself. This software update is thus complete.

The semaphore test is carried out by VI.DB.dll on a cyclical basis during normal operations. If a file is identified for update, the update process is started automatically.

Related topics

- User intervention in automatic updating of One Identity Manager tools on page 88

User intervention in automatic updating of One Identity Manager tools

When the automatic One Identity Manager tool update is detected on a workstation, the user is prompted to close all open programs. Updating starts after the user has closed all the programs.

Whether the users of One Identity Manager tools can decide when their own workstations are updated, is controlled using the configuration parameter Common | AutoUpdate | AllowOutOfTimeApps.

- Users have no possibility to intervene in the update if the configuration parameter is not set. The update is executed immediately.
- If the configuration parameter is set, the logged in user is prompted with a message. The user can decide whether the One Identity Manager tools update takes place on the workstation straight away or at a later time.

**NOTE:** If the user does not want to update immediately, he can continue working. The update is started the next time the program is started.

Automatic updating of the One Identity Manager Service

Automatic software update is the default method for updating the One Identity Manager Service on servers. However, the update method takes into account that it may be essential to exclude certain servers from being updated automatically and to update them manually.
For every query of process steps, the One Identity Manager Service returns the current status of the semaphore software revision. If this value differs from the value in the database, the Job server is labeled with "updating" in the database and no more normal process steps are sent to it.

The Job server is updated depending on the procedure set in the configuration parameter **Common | Autoupdate | ServiceUpdateType**.

First, the start time of the last change is determined from SoftwareRevision.viv. A list is compiled of all files with additional information specifying whether each file is new or not. This list is evaluated on the Job server to be updated and another list is compiled specifying which files will be updated.

To do this, the service receives an Autoupdate process from the server, which loads the file Update.zip and the update process begins.

If updating with the new process cannot be completed because, for example, there is no direct connection to the database or an application server, the files are transfer by process steps in the Job queue (fallback). In this case, any existing update steps from the module library might not be executed.

One Identity Manager Service is restarted if any one of the files has changed on the Job server. After the update is completed, the Job server label is reset in the database.

## Automatic updating of web applications

In principle, web applications support automatic software update. However, a few web applications may require extra configuration to take part in automatic software updating.

The following permissions are required for automatic updating:

- The user account for updating requires write permissions for the application directory.
- The user account for updating requires the local security policy **Log on as a batch job**.
- The user account running the application pool requires the local security policies **Replace a process level token** and **Adjust memory quotas for a process**.

Updating the web application requires restarting the application. The web application is restarted automatically by the web server when it has been idle for a defined length of time. This may take some time or be hindered by continuous user requests. Some web application offer you the option to restart manually.

**NOTE:** To update the Web Portal automatically, use a browser to connect to the runtime monitor http://<servername>/<application>/monitor and start the update of the web application.

If the web application update is identified, new files are copied from the database to a temporary directory on the server.

The application then loads the file Update.zip from the database or from the application server, which is unpacked in a temporary directory.
The `Update.exe` starts, waits until the web application process has shutdown and copies the files from the temporary directory to the web application's directory.

**Related topics**
- Updating an application server on page 117
- Configuring the automatic update for the Web Portal on page 137
- Updating the Manager web application on page 147

## Implementing the automatic software update

The following permissions are required for automatic software updating:

- It is recommended that you apply full access rights to the One Identity Manager installation directory for automatic updating of One Identity Manager tools.
- The service’s user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.

**To implement automatic software updating**

1. Ensure that an update server is set up. This server ensures that the other servers are updated automatically.
   
   - The server must be entered in the database as a Job server with the server function **Update server**.
   - A One Identity Manager Service with direct access to the database must be installed and configured on the server.

2. Check the configuration parameter **Common | Autoupdate** in the Designer.
   
   - If the configuration parameter is set (default), One Identity Manager files, which do not have the current revision status, are updated automatically.
   - If this configuration parameter is deactivated, no automatic update is performed.

3. Use the configuration parameter **Common | AutoUpdate | AllowOutOfTimeApps** to define whether the users of the One Identity Manager tools can decide when the update of their workstation takes place.
   
   - If this configuration parameter is set, users of One Identity Manager tools are prompted to decide whether they want to update now or later.
   - If this configuration parameter is not set, the One Identity Manager tools are updated immediately.

4. In the configuration parameter **Common | Autoupdate | ServiceUpdateType**, determine which procedure is used to update the One Identity Manager Service.
Table 27: Procedure according to configuration parameter Common | Autoupdate | ServiceUpdateType

<table>
<thead>
<tr>
<th>Method</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue</td>
<td>A process that distributes all files is queued in the job queue.</td>
</tr>
<tr>
<td>DB</td>
<td>The files are reloaded directly from the database. Implement this procedure if all Job servers have a direct connection to the database.</td>
</tr>
<tr>
<td>Auto</td>
<td>All root servers are filled directly from the database. A process is set up in the Job queue for all leaf servers. For this process, the root servers must have a direct database connection.</td>
</tr>
</tbody>
</table>

5. Web applications may require some individual configuration settings. Check the configuration settings.

**Related topics**

- Basics for automatic software update on page 85
- Disabling automatic update on page 91

**Disabling automatic update**

**NOTE:** If the configuration parameter **Common | Autoupdate** is deactivated, no automatic update is performed across the system.

Under certain circumstances, it is necessary to exclude individual workstations, server or web applications.

**Disabling Automatic Update on Workstations**

To disable automatic update locally on a workstation, set the registry key `HKEY_CURRENT_USER\Software\One Identity\One Identity Manager\Global\Settings\AutoUpdateEnabled="false"`.

This disables automatic updating completely on this workstation.

**Disabling Job Server Automatic Updating**

Automatic update for Job servers is configured in the server entry. To exclude individual Job servers (for example the update server) from the automatic update, enable the following option for the Job server in Designer: **No automatic software update**.

**Disabling automatic update of the Web Portal**

You can disable Web Portal updates in the database. If the property `QBM\WebApplication.AutoUpdateLevel` is set to the value 1 (inactive), this web application can...
no longer be updated via the automatic software update.

**Configuring Automatic Update of an Application Server**

Configure automatic updating in the application server’s `web.config`. You can adjust the behavior with the following statements:

```xml
<autoupdate>
  <add key="off" value="true"/>
  <add key="checkinterval" value="00:05:00"/>
  <add key="inactivitytime" value="00:00:10"/>
</autoupdate>
```
Updating the One Identity Manager

Updating One Identity Manager tools includes updating the One Identity Manager database and the existing installations on One Identity Manager network workstations and servers. Database updates are necessary when hotfixes and service packs or complete version updates are available for One Identity Manager.

- **Hotfix**
  A hotfix contains corrections to the default configuration of the current main version but no extension of functionality. A hotfix can supply patches for issues solved in synchronization projects.

- **Service pack**
  A service pack contains minimal extensions of functionality and all the modifications since the last main version that were already included in the hotfixes. A service pack can supply patches with new functions for synchronization projects.

- **Version change**
  A version change means that significant extensions of functionality have been made and involves a complete re-installation. A version change can supply milestones for updating synchronization projects. Milestones group together all patches for solved issues and patches required for new features of the previous version.

**Detailed information about this topic**

- The update process for releasing a new One Identity Manager version on page 93
- Automatic updating of One Identity Manager on page 85
- Updating One Identity Manager components on page 97
- Updating the One Identity Manager database on page 100

**The update process for releasing a new One Identity Manager version**

**NOTE:** Read the release notes for possible differing or additional steps for updating One Identity Manager.
To update the One Identity Manager to a new version

1. In Designer, carry out all consistency checks in the Database area.
   a. Start Consistency Editor in Designer by selecting Database | Check data consistency.
   b. In the dialog Test options click the icon ![Test options](image)
   c. Activate all tests in the area Database and click OK.
   d. To start the check, choose the following in the menu Consistency check | Run.
      All database tests must be successful. Correct the errors. Some consistency checks offer repair methods for correcting errors.

2. Update the administrative workstation, on which the One Identity Manager database schema update is started.
   a. Execute the program autorun.exe from the root directory on the One Identity Manager installation medium.
   b. Change to the Installation tab. Select the edition that you installed.
   c. Click Install.
      This starts the installation wizard.
   d. Follow the installation instructions.

   **IMPORTANT:** On the Installation Settings page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.

3. (From version 7.0.x or version 7.1.x) End the One Identity Manager Service on the server that processes direct database queries.
   (From version 8.0.x or version 8.1.x). End the One Identity Manager Service on the update server.

4. Create a back up of the One Identity Manager database.

5. Check whether the database’s compatibility level is set the 130 and change it if necessary.

6. Run a schema update of the One Identity Manager database.
   a. Start the Configuration Wizard on the administrative workstation.
      Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.
      b. Use the same user as you used for initially installing the schema.
      c. If you created an administrative user during schema installation, use that one.
• If you selected a user with Windows authentication to install the schema, you must use the same one for updating.

NOTE: If you want to switch to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.1, you will also require an installation user according to Users with granular permission for the One Identity Manager database on an SQL Server on page 26.

If you want to switch to granular permissions when you update from 8.1.x at a later date, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

7. (From version 7.0.x or version 7.1.x) Update the One Identity Manager Service on the server that processes direct database queries.

(From version 8.0.x or version 8.1.x). Update the One Identity Manager Service on the update server.

a. Execute the program autorun.exe from the root directory on the One Identity Manager installation medium.

b. Change to the Installation tab. Select the edition that you installed.

c. Click Install.

This starts the installation wizard.

d. Follow the installation instructions.

IMPORTANT: On the Installation Settings page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.

8. Check the login information of the One Identity Manager Service. Revert to the original settings if the One Identity Manager Service did not initially use the local system account for logging in. Specify the service account to be used. Specify the service account to use.

9. Start the One Identity Manager Service on the update server.

10. Update other installations on workstations and servers.

You can use the automatic software update method for updating existing installations.

NOTE: In some cases it may be necessary to update the further workstations and Job servers manually. This might be required, for example, if there are a significant number of new changes with a One Identity Manager version update, which do not allow the use of automatic update.

To update synchronization projects to a new version

Any required changes to system connectors or the synchronization engine are made available when you update One Identity Manager. These changes must be applied to existing synchronization projects to prevent target system synchronizations that are already set up, from failing. Patches are made available for this.
NOTE: Some patches are applied automatically. A process that migrates all existing synchronization project is queued in the Job queue to do this. To execute the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

- Check whether the process DPR_Migrate_Shell has been started successfully. If a patch could not be applied, for example because the target system was not available, you can apply the patch manually later.

For more detailed information about applying patches, see the One Identity Manager Target System Synchronization Reference Guide.

To update an application server to a new version

- The application server starts updating automatically after the One Identity Manager database schema update.
- To start the update manually, open the status page for the application in the browser and click on **Update immediately** in the menu for the logged in user.

To update the Web Portal to a new version

NOTE: Ensure that the application server is updated before you update the Web Portal.

- To update the Web Portal automatically, use a browser to connect to the runtime monitor http://<server name>/<application>/monitor and start the update of the web application.
- To manually update the Web Portal, uninstall the existing Web Portal and install the Web Portal again.

To update an API Server to a new version

- After updating the One Identity Manager database schema, restart the API Server. The API Server is updated automatically.

To update the Operations Support Web Portal to a new version

- (As from version 8.1.x) After updating the API Server, compile the HTML application **Operations Support Portal**. For more information, see the One Identity Manager Installation Guide.
- (As from version 8.0.x)
  2. Install an API Server and compile the HTML application **Operations Support Portal**. For more information, see the One Identity Manager Installation Guide.

To update the Manager web application to a new version

1. Uninstall the Manager web application.
2. Reinstall the Manager web application.
3. The Manager default user requires write access to the Internet Information Services web application installation directory so that Manager web applications can be updated automatically. Check that the correct permissions are allocated.

**Detailed information about this topic**

- Automatic updating of One Identity Manager on page 85
- Updating One Identity Manager components on page 97
- Updating the One Identity Manager database on page 100
- Installing and updating an application server on page 112
- Installing, configuring and maintaining the Web Portal on page 126
- Installing and updating the Manager web application on page 144

**Updating One Identity Manager components**

You can use the automatic software update method for updating the workstations and servers.

In some cases it may be necessary to update the workstations and servers manually using the installation wizard. This might be required, for example, if there are a significant number of new changes with a One Identity Manager version update, which do not allow the use of automatic update.

![NOTE:](image)

**NOTE:** When changing versions, use the installation wizard to update the workstation on which the schema installation of the One Identity Manager database is started.

**To update a workstation using the installation wizard**

1. Execute the program autorun.exe from the root directory on the One Identity Manager installation medium.
2. Change to the Installation tab. Select the edition you have installed and click Install.
3. This starts the installation wizard. Select the language for the installation wizard on the start page and click Next.
4. Confirm the conditions of the license.
5. On the Installation settings page, enter the following information.
### Table 28: Settings for the installation

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation source</td>
<td>Select the directory containing the installation files.</td>
</tr>
<tr>
<td>Installation directory</td>
<td>Select the directory of your previous One Identity Manager installation. Otherwise the components are not updated and a new installation is created in the second directory instead.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>To make further configuration settings, click on the arrow button next to the input field. Here, you can specify whether you are installing on a 64-bit or a 32-bit operating system. For a standard installation, no further configuration settings are necessary.</td>
</tr>
<tr>
<td>Select installation modules</td>
<td>Set this option to load the installation information using the existing One Identity Manager database.</td>
</tr>
<tr>
<td>using the database</td>
<td>NOTE: Leave this option empty to install the workstation on which you start the One Identity Manager schema installation.</td>
</tr>
<tr>
<td>Add further modules to the</td>
<td>Set this option to add additional One Identity Manager modules to the selected edition</td>
</tr>
<tr>
<td>selected edition</td>
<td></td>
</tr>
</tbody>
</table>

6. On the **Module selection** page, also select the modules to be installed.

   NOTE: This page is only shown if you set the option **Add more modules to the selected Edition**.

7. Enter the database connection data on **Connect to database**.

   NOTE: This page is only shown if you have set the **Select installation modules with existing database** option.

   a. Select the connection in **Select a database connection**.
   - OR -
   
   Click on **Add new connection**, select a system type and enter connection data.
### Table 29: SQL Server database connection data

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Database server.</td>
</tr>
<tr>
<td>Windows authentication</td>
<td>Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td>
</tr>
<tr>
<td>User</td>
<td>SQL Server Login name.</td>
</tr>
<tr>
<td>Password</td>
<td>SQL Server login password.</td>
</tr>
<tr>
<td>Database</td>
<td>Database.</td>
</tr>
</tbody>
</table>

b. In the **Authentication method** area, select the authentication module and enter the logon data for the system user ID. Which login data you require depends on the authentication module selected.

8. On the **Assign machine roles** page, define the machine roles.

   **NOTE:** The machine roles appropriate for the One Identity Manager modules are activated. All machine subroles are selected when you select the machine role. You can deselect individual packages.

9. You can start different programs for further installation on the last page of the install wizard.

   * To perform installation of the One Identity Manager schema, start the Configuration Wizard and follow the instructions of the Configuration Wizard.
     
     **NOTE:** Perform this step only on the work station on which you start the installation of the One Identity Manager schema.

   * To create the configuration of the One Identity Manager Service, start the program Job Service Configuration.
     
     **NOTE:** Execute this step only on servers on which you have installed the One Identity Manager Service.

10. Click **Finish** to close the installation wizard.

11. Close the autorun program.

### To update the One Identity Manager Service using the installation wizard

1. Open the service management of the server and close the One Identity Manager Service.

2. Update the One Identity Manager components with the installation wizard.

3. Check the login information of the One Identity Manager Service. Revert to the original settings if the One Identity Manager Service did not initially use the local
system account for logging in. Specify the service account to be used. Specify the service account to use.

4. Start the One Identity Manager Service in service management.

Related topics
- Automatic updating of One Identity Manager on page 85

Updating the One Identity Manager database

Automatic version control is integrated into the One Identity Manager, ensuring that One Identity Manager components are always consistent with each other and with the database. If program extensions that change the structure are implemented, for example, table extensions, the database needs to be updated.

You need to update the database if hotfixes and service packs for your installed version of One Identity Manager are available or complete version updates. In addition, customer-specific changes must be transferred from a development database into the test database and into the production system database.

**IMPORTANT:** Test changes in a test system before you load a transport package in a productive system.

The One Identity Manager schema is customized by loading so-called ‘transport packages’. One Identity Manager recognizes the following types of transport packages that can be copied to the database depending on requirements.

Table 30: Transport package

<table>
<thead>
<tr>
<th>Transport Package Type</th>
<th>Description</th>
<th>Tool Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration package</td>
<td>Migration packages are provided by for the initial database schema installation, for service pack and complete version updates. A migration package contains all the necessary tables, data types, database procedures, and the default One Identity Manager configuration.</td>
<td>Configuration Wizard</td>
</tr>
<tr>
<td>Hotfix package</td>
<td>Hotfix packages are provided to load individual corrections to the default configuration such as templates, scripts, processes, or files into the database.</td>
<td>Database Transporter Software Loader</td>
</tr>
</tbody>
</table>

**NOTE:** If a hotfix package only contains changed files, load these files into the database using the Software Loader file.
<table>
<thead>
<tr>
<th>Transport Package Type</th>
<th>Description</th>
<th>Tool Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom configuration package</td>
<td>A custom configuration package is used to exchange customer specific changes between the development, test and productive system database. This transport package is created by the customer and loaded into the database.</td>
<td>Database Transporter</td>
</tr>
</tbody>
</table>

**NOTE:** If more custom configuration adjustments are made to a One Identity Manager database, then create a custom configuration package and import this transport package in the target database with the Database Transporter. There is no support for merging a hotfix package with a custom configuration package into one transport package.

### Related topics
- Updating the One Identity Manager database with the Configuration Wizard on page 103
- Installing a hotfix in the One Identity Manager database on page 106
- Appendix: Creating a One Identity Manager database for a test or development environment from a database backup on page 169

### Notes on updating the One Identity Manager database

- Test changes in a test system before you load a migration package in a production system. Use a copy of the production database for testing.
- Before you update the One Identity Manager schema, ensure that the administrative system user who is going to compile the database has a password. Otherwise the schema update cannot be completed successfully.
- Use the Configuration Wizard to update the One Identity Manager database if you have received a service pack or complete version update. The Configuration Wizard carries out the update of the schema and transfers the current status to the version history.
- For performance reasons, we recommend that you set the database to the Simple restore model during the schema update.
- Start Configuration Wizard on an administrative workstation.
- Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.
• Use the same user as you used for initially installing the schema.
• If you created an administrative user during schema installation, use that one.
• If you selected a user with Windows authentication to install the schema, you must use the same one for updating.

**NOTE:** If you want to switch to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.1, you will also require an installation user according to [Users with granular permission for the One Identity Manager database on an SQL Server](https://support.oneidentity.com/identity-manager/) on page 26.

If you want to switch to granular permissions when you update from 8.1.x at a later date, contact support. To access the Support Portal, go to [https://support.oneidentity.com/identity-manager/](https://support.oneidentity.com/identity-manager/).

• For the period of the update, the database is set to single user mode. Close all existing connections to the database before starting the schema update.
• After the update has completed, the database is automatically switched to multiuser mode. If it is not possible, you receive a message in which you can manually switch to multiuser mode.
• You may experience problems activating single-user mode when using database mirroring.
• During the update, calculation tasks are queued in the database. These are processed by the DBQueue Processor. Processing calculation tasks may take some time depending on the amount of data and system performance.

This is particularly the case, if you save large amounts of historical data in the One Identity Manager database such as change data or data from process handling. Therefore, ensure that you have configured an appropriate procedure for archiving the data before you update the database. For more information about archiving data, see the [One Identity Manager Data Archiving Administration Guide](https://support.oneidentity.com/identity-manager/).

• To ensure that HTML applications are be successfully compiled, you must download packages from the NPM repository. Ensure that the workstation you are compiling on, can establish a connection to the website registry.npmjs.org:443.
  Alternatively, you can download packages from a proxy server and install them manually.

**Detailed information about this topic**

• [Updating the One Identity Manager database with the Configuration Wizard](https://support.oneidentity.com/identity-manager/) on page 103
• [Editing the One Identity Manager database during update with the Configuration Wizard](https://support.oneidentity.com/identity-manager/) on page 105
• [Users with granular permission for the One Identity Manager database on an SQL Server](https://support.oneidentity.com/identity-manager/) on page 26
• [Appendix: Creating a One Identity Manager database for a test or development environment from a database backup](https://support.oneidentity.com/identity-manager/) on page 169
Updating the One Identity Manager database with the Configuration Wizard

**IMPORTANT:** Test changes in a test system before you load a migration package in a productive system. Use a copy of the production database for testing.

**NOTE:** Always start the Configuration Wizard on an administrative workstation!

**To update a database**

1. Start the Configuration Wizard.
2. Select **Update database** on the Configuration Wizard home page and click **Next**.
3. Select the database and install directory on the **Select database** page.
   a. Select the connection in **Select a database connection** Select a user who has at least administrative permissions for the One Identity Manager database.
   b. Select the directory with the installation files in **Installation source**.
4. Configuration modules and version information are shown in the **Product description** page.
   a. Select the module you want to update.
   b. Confirm that you have an up-to-date backup of database.
   c. Confirm that the database consistency checks were executed.
   d. Set **Add other modules** to select other modules.
5. Select the additional module on the **Select configuration modules** page.
   **NOTE:** This page is only shown if you set **Add more modules**.
   **NOTE:** If you add more modules, your custom administrative users obtain the permissions for this module.
6. Other users with existing connections to the database are displayed on the **Active sessions** page.
   - Disconnect the connections on order to start database processing.
7. On the **Create a new login for administrators** page, decide which SQL server login to use for administrative users.
   **NOTE:** This page is only shown when updating a One Identity Manager database with version 7.0.x, 7.1.x or 8.0.x to version 8.1.1.
   If you want to switch to granular permissions when you update from 8.1.x at a later date, contact support. To access the Support Portal, go to [https://support.oneidentity.com/identity-manager/](https://support.oneidentity.com/identity-manager/).

You have the following options:
• **Create new SQL Server logins for the database**: Select this option if you want to set up a new administrative login on the SQL Server. Other SQL Server logins with permissions for system configuration and for end users are created after the database has been migrated.

Enter the login name, password and password confirmation for the new SQL Server login.

• **Use the current SQL Server login for the database**: If you select this option, no other SQL server logins are created for the database. In this case, you cannot work with granular permissions concepts at SQL level. The user you specified is used to connect to the database.

8. Error that prevent processing the database are displayed on the **Database check** page. Correct the error before you continue updating.

9. The installation steps are shown on the **Processing database** page. Installation and configuration of the database is automatically carried out by the Configuration Wizard.

   ![TIP:](image.png)

   Set **Advanced** to obtain detailed information about processing steps and the migration log.

   a. You must login as an administrative user to compile the system.
      
      i. Enter a user name and password for the administrative system user.
      
      ii. Click **Log in**.

   b. Once processing is complete, click **Next**.

10. On the **Create SQL server logins** page, enter the login name, the password and password confirmation for the SQL Server logins for configuration users and end users.

   ![NOTE:](image.png)

   This page is only shown when updating a One Identity Manager database with version 7.0, 7.1 or 8.0 to version 8.1.1.

11. You can configure the vendor notification on the page, **Configure vendor notification**.

   ![NOTE:](image.png)

   This page is only shown of you have not yet enabled vendor notifications.

   If vendor notification is enabled, One Identity Manager generates a list of system settings once a month and sends it to One Identity. This list does not contain any personal data. The list will be reviewed by our customer support team who will look for material changes in a proactive effort to identify potential issues before they materialize on your system. The lists may be used by our R&D staff for analysis, diagnosis, and replication for testing purposes. We will keep and refer to this information for as long as your company remains on support for this product.

   a. To use the function, set **Enable vendor notification** and enter your company's contact email address in **Email address for contact**.
The email address is used as the sender address for notifying vendors.

b. Set **Disable vendor notification** if you do not want to use this functionality.

12. Click **Finish** on the last page of Configuration Wizard.

**Related topics**

- Notes on updating the One Identity Manager database on page 101
- Editing the One Identity Manager database during update with the Configuration Wizard on page 105
- One Identity Manager vendor notification on page 67
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26
- Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33
- Error messages when installing and updating the One Identity Manager database on page 160
- Appendix: Creating a One Identity Manager database for a test or development environment from a database backup on page 169

**Editing the One Identity Manager database during update with the Configuration Wizard**

The One Identity Manager database is updated automatically by the Configuration Wizard. This procedure may take some time depending on the amount of data and system performance.

The Configuration Wizard performs the following steps:

- Updating the One Identity Manager schema.

  Before the schema installation, the Configuration Wizard checks the database. Error messages are displayed in a separate window. The errors must be corrected manually. The schema update cannot be started until these are resolved.

  All the tables, data types, and database procedures that are required are loaded into the database by the schema update. When a transport package is imported into a One Identity Manager database, the following operations are carried out:

<table>
<thead>
<tr>
<th>Table 31: Operations when importing a migration package</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
</tr>
<tr>
<td>Insert</td>
</tr>
<tr>
<td>Operations</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Refresh</td>
</tr>
<tr>
<td>Delete</td>
</tr>
</tbody>
</table>

During a schema update, calculation tasks are queued in the database. These are processed by the DBQueue Processor.

For a schema update with the Configuration Wizard, the migration date and the migration status are recorded in the transport history of the database.

- Compiling the system.
  Scripts, templates and processes are declared in the database. The **System user** authentication module with the specified system user is used for compilation.

- Uploading files for automatic software update.
  In order to distribute One Identity Manager files using the automatic software updating mechanism, the files are loaded into the One Identity Manager database.

- Migration of synchronization projects,
  A process that migrates all existing synchronization project is queued in the Job queue. This updates the One Identity Manager schema and applies automatic patches.

### Related topics

- [Automatic updating of One Identity Manager](#) on page 85
- [Displaying the transport history and checking the One Identity Manager version](#) on page 158

## Installing a hotfix in the One Identity Manager database

1. **IMPORTANT:** Test changes in a test system before you install a hotfix in a productive system.

Hotfix packages contain:

- Transport packages which contain changes to the default configuration, such as templates, scripts, processes in the One Identity Manager database

- Modified files, such as *.exe, *.dll or *.vif

If you receive a transport package using a hotfix package, use the Database Transporter program to update the One Identity Manager database.

If a hotfix contains a modified file, copy the file to the install directory of the test computer for testing. To distribute the files to all workstations and servers using the automatic
software automation, use the program Software Loader to import the files into the One Identity Manager database.

**NOTE:** If more custom configuration adjustments are made to a One Identity Manager database, then create a custom configuration package and import this transport package in the target database with the Database Transporter. There is no support for merging a hotfix package with a custom configuration package into one transport package.

### Detailed information about this topic

- Displaying the contents of a transport package with the Database Transporter on page 107
- Importing a transport package with the Database Transporter on page 108
- Importing files with the Software Loader on page 110
- Displaying the transport history and checking the One Identity Manager version on page 158

### Displaying the contents of a transport package with the Database Transporter

You can display the contents of a transport package with the Database Transporter before you import.

**NOTE:** Always start the Database Transporter on an administrative workstation!

**To display the contents of a transport package**

1. Start the Launchpad and log in on the One Identity Manager database.
2. In Change & Extend, select *Transport custom modifications*. This starts the Database Transporter program.
3. Select *Show transport file*.
4. Select the transport package file browser and click *Open*.
5. Click *Next* on the *Select transport file* page.
6. The contents of the transport file are displayed on the *Show transport file* page.
   - To display the sequence in which the objects are imported
     a. Click + to select an entry in the transport file and select *Sort in import order* from the context menu.
     b. Click *OK* and enter the connection credentials for the database. This step is only required when you established the first in the order.
     The order in which the entry’s objects are imported into the database is found.
c. Repeat this step for all other entries for which you want to determine the import order.

- To display the objects required for an import in the target environment, select the entry for the .xml file and select **Show required objects** from the context menu.

Objects that are dependent on another object that is not part of the transport package are highlighted.

7. To end the program, click **Finish** on the last page.

**TIP:** You can start the import of the transport package from display mode. On the **Show transport file** page, click the name of the transport package and use the **Import** context menu.

Related topics

- Importing a transport package with the Database Transporter on page 108

**Importing a transport package with the Database Transporter**

**NOTE:**

- Test the changes in a test environment before you load a transport package in a production system. Use a copy of the production database for testing.

- To import transport packages with Database Transporter, the user requires the ** Allows transport packages to be imported into the database** (Transport_Import) program function.

- Start Database Transporter on an administrative workstation.

- The database is set to single-user mode for the duration of the import. Close all existing connections to the database before starting the import.

- When you import a transport package with schema extensions, the database is set to maintenance mode. Objects cannot be processed in the database during this time.

- 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 import a transport package**

1. Start the Launchpad and log in on the One Identity Manager database.

2. In **Change & Extend**, select **Transport custom modifications**. This starts the Database Transporter program.

3. Select **Import transport file** on the start page.
4. On the **Select the database connection** page, check the One Identity Manager database connection data and change it if necessary.

5. Select the transport package file browser and click **Open**.

6. Specify your import options on **Select transport file**.

### Table 32: Import options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a log file for the data import</td>
<td>Enable this option to create a log file for the import. The log file is saved in the output directory of the transport file.</td>
</tr>
<tr>
<td>Import objects singly and ignore errors</td>
<td>Enable this option to import options individually. Errors, which might occur during importing are ignored and displayed when importing is complete. If you do not enable this option, the import procedure is canceled when errors occur.</td>
</tr>
<tr>
<td>Ignore default data differences</td>
<td>Enable this option to ignore changes to default data during the import. If you do not enable this option, the import procedure is canceled if changes to default data are included.</td>
</tr>
</tbody>
</table>

7. Import steps and import progress are displayed on the **Importing transport data** page. The import procedure can take some time. Calculation tasks are queued for the DBQueue Processor on termination.

8. If changes have been made to the system configuration, for example, processes or scripts imported, you have to compile the database after the tasks have been processed. Compilation is started automatically once importing is complete.

9. To end the program, click **Finish** on the last page.

**NOTE:** Use the button to save any errors that occur whilst importing.

**Related topics**

- Displaying the contents of a transport package with the Database Transporter on page 107
- Displaying the transport history and checking the One Identity Manager version on page 158
- Appendix: Creating a One Identity Manager database for a test or development environment from a database backup on page 169
Importing files with the Software Loader

**NOTE:**

- Start Software Loader on an administrative workstation.
- When selecting the base directory, ensure that a directory hierarchy is not created unintentionally.
- For web applications, select the installation directory of the web application to ensure that the required subdirectories, for example the bin directory, are detected correctly.
- For detailed information about how to import customer-defined files using the Software Loader, see the *One Identity Manager Operational Guide*.

**To import files into a One Identity Manager database**

1. Start the Launchpad and log in on the One Identity Manager database.
2. In **Change & Extend**, select **Import files for software update**. This starts the Software Loader program.
3. Select **Import into database** on the start page.
4. On the **Connect to database** page, check the One Identity Manager database connection data and change if necessary.
5. Specify the file to be imported on **Select files**.
   a. Select the base directory where the files can be found.
      
      The status and file size of all the files in the selected directory are displayed in the file list.

**Table 33: Meaning of status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version unknown</td>
<td>The file belongs to the known files but has not yet been loaded into the database. There is no version information in the database.</td>
</tr>
<tr>
<td>Unknown file</td>
<td>The file is new. The file is in the list of known files but has not been loaded in the database yet. There is no version information in the database.</td>
</tr>
<tr>
<td>Version OK</td>
<td>The file version matches the version in the database.</td>
</tr>
<tr>
<td>Version modified</td>
<td>The file version has been modified compared with the version in the database.</td>
</tr>
</tbody>
</table>
b. Select the files you want to load into the One Identity Manager database.

**TIP:**
- Click a column in the table header to order the display by the selected column.
- Press **Shift + select** or **Ctrl + select** to select more than one file.
- To quickly select all files with **Changed version** as their status, select **Open all directories** and **Open all modified files** in the context menu. Files in subdirectories are only selected if the higher-level directories have already been opened.

6. On the **Select change label** page, assign a change label to make it easier to exchange files between various databases, such as the test database, development database and productive database.
   a. Select **Assign files to following change label**.
   b. Use the button next to the option to select the change label.

7. The files are loaded straight from the One Identity Manager database.

8. Specify other file settings on **Assign machine roles**.
   a. Assign a computer role to the files.
   b. (Optional) For more file settings, click ... next to the file names.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory source</td>
<td>Directory path in installation source.</td>
</tr>
<tr>
<td>Create backup</td>
<td>A copy must be made of the file during the automatic software update.</td>
</tr>
<tr>
<td>No update</td>
<td>The file is not updated by the automatic software update.</td>
</tr>
</tbody>
</table>

9. Click **Finish** on the last page to end the program.

**Related topics**
- Automatic updating of One Identity Manager on page 85
- Appendix: Machine roles and installation packages on page 181
Installing and updating an application server

The application server provides a connection pool for accessing the database. Clients send their queries to the application server, which processes the objects, for example, by determining values using templates and sending the results back to the clients. The data from the application is sent to the database when an object is saved.

Before installation ensure that the minimal hardware and software prerequisites are fulfilled on the server.

**Detailed information about this topic**

- Minimum system requirements for the application server on page 40
- Advice for installing an application server on page 112
- Installing an application server on page 113
- Displaying the application server status on page 116
- Updating the search index on the application server on page 118
- Updating an application server on page 117
- Uninstalling an application server on page 118

**Advice for installing an application server**

- If you want to run the One Identity Manager Service or the Designer through an application server, the application server requires at least configuration user permissions. Use the SQL Server login for connecting to the One Identity Manager database and for authenticating against the One Identity Manager database when you install the application server.
- To limit permissions for end users, you can make other application servers available,
which use the SQL Server login for end users.

- To use the Web Portal or full text search in the Manager, you need an application server with a search service installed on it.
- Start the application server installation locally on the server.
- Use the configuration parameter **QBM | AppServer | SessionTimeout** to add the timeout in hours, after which inactive application server sessions are closed. The default value is **24** hours. Edit the configuration parameter in the Designer.

### Installing an application server

**IMPORTANT:** Start the application server installation locally on the server.

**To install an application server**

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. Go to the **Installation** tab and select the entry **Web based components** and click **Install**. Starts the Web Installer.
3. Select **Install application server** on the Web Installer and click **Next**.
4. On the **Database connection** page, enter the connection credentials for the One Identity Manager database.
5. Configure the following settings on the **Select setup target** page.

#### Table 35: Settings for the Installation Target

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Name used as application name, as in the title bar of the browser, for example.</td>
</tr>
<tr>
<td>Target in IIS</td>
<td>Internet Information Services web page on which to install the application.</td>
</tr>
<tr>
<td>Enforce SSL</td>
<td>Specifies whether insecure websites are available for installation. If the option is set, only sites secured by SSL can be used for installing. This setting is the default value. If this option is not set, insecure websites can be used for installing.</td>
</tr>
<tr>
<td>URL</td>
<td>The application's Uniform Resource Locator (URL).</td>
</tr>
<tr>
<td>Install dedicated application pool</td>
<td>Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application pool</td>
<td>The application pool to use. This can only be entered if the option <strong>Install dedicated application pool</strong> is not set.</td>
</tr>
<tr>
<td></td>
<td>If you use the default value <strong>DefaultAppPool</strong>, the application pool has the following syntax:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;application name&gt;_POOL</code></td>
</tr>
<tr>
<td>Identity</td>
<td>Permissions for executing an application pool. You can use a default identity or a custom user account.</td>
</tr>
<tr>
<td></td>
<td>If you use the default value <strong>ApplicationPoolIdentity</strong>, the user account has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>IIS APPPOOL&lt;application name&gt;_POOL</td>
</tr>
<tr>
<td></td>
<td>You can authorize another user by clicking ... next to the box, enabling the option <strong>Custom account</strong> and entering the user and password.</td>
</tr>
<tr>
<td>Web authentication</td>
<td>Specifies the type for authentication against the web application. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows authentication (Single Sign-On)</strong></td>
</tr>
<tr>
<td></td>
<td>The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method if Windows authentication is installed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anonymous</strong></td>
</tr>
<tr>
<td></td>
<td>Login is possible without Windows authentication. The user is authenticated against the Internet Information Services and the web application anonymously and the web application is directed to a login page.</td>
</tr>
<tr>
<td>Database authentication</td>
<td>NOTE: You can only see this section if you have selected an SQL database connection on the <strong>Database connection</strong> page.</td>
</tr>
<tr>
<td></td>
<td>Specifies the type for authentication against the One Identity Manager database. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows authentication</strong></td>
</tr>
<tr>
<td></td>
<td>The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>with a user defined user account or a default identity for the application pool.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SQL authentication</strong></td>
</tr>
<tr>
<td></td>
<td>Login is only possible through a user defined user account. Authentication is completed with a user name and password. This access data is saved in the web application configuration as computer specific encrypted.</td>
</tr>
</tbody>
</table>

6. On the **Assign machine roles** page, define the machine roles.

This enables the machine roles for the application server. The machine roles **Search Service** and **Search Indexing Service** are required for indexing the full text search. These machine roles are always used together.

**NOTE:** If you want to use a Web Portal, you will need to use an application server with a search service installed.

7. On the **Set session token certificate** page, you define the certificate for creating and checking session tokens.

**NOTE:** The certificate must have a key length of at least 1024 Bits.

a. To create a new certificate, enter the following information.
   i. **Session token certificate:** Select **Create new certificate**.
   ii. **Certificate issuer:** Enter the issuer of the certificate.
   iii. **Key length:** Specify the key length for the certificate.

   The certificate is entered in the application server's certificate management.

b. To use an existing certificate, enter the following information.
   i. **Session token certificate:** Select the entry **Use existing certificate**.
   ii. **Select certificate:** Select the certificate.

c. To generate a new certificate file, enter the following information.
   i. **Session token certificate:** Select **Generate new certificate file**.
   ii. **Certificate issuer:** Enter the issuer of the certificate.
   iii. **Key length:** Specify the key length for the certificate.
   iv. **Certificate file:** Enter the directory path and name of the certificate file.

   The certificate file is stored in the specified directory in the web application.

8. Specify the user account for automatic updating on the **Set update credentials** page. The user account is used to add or replace files in the application directory.
- Use IIS credentials for update: Set this option to use the user account under which the application pool is executed for the updates.

**Use IIS credentials for update**: Set this option to use the user account under which the application pool is executed for the updates.

- **Use other credentials for updates**: To use a different user account, set this option. Specify the domain, the user name, and the user password.

9. Installation progress is displayed on the **Setup is running** page. The Web Installer generates the web application and the corresponding configuration files (web.config) for each directory. After installation is complete, click **Next**.

10. Click **Finish** on the last page to end the program.

11. Close the autorun program.

ℹ️ **NOTE**: Default values are used for the configuration settings during installation. You can keep these values. It is recommended you check the settings.

**Related topics**

- Minimum system requirements for the application server on page 40
- Advice for installing an application server on page 112
- Displaying the application server status on page 116
- Updating an application server on page 117
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26
- Appendix: Machine roles and installation packages on page 181

### Displaying the application server status

You can access the application server from a browser.

Use the appropriate URL for this:

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

ℹ️ **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.
Updating an application server

1. **NOTE:**
   - We recommend that you perform the automatic update only in specific maintenance windows, in which the application cannot be accessed by users and the application can be manually restarted with no risk.
   - The following permissions are required for automatic updating:
     - The user account for updating requires write permissions for the application directory.
     - The user account for updating requires the local security policy **Log on as a batch job**.
     - The user account running the application pool requires the local security policies **Replace a process level token** and **Adjust memory quotas for a process**.

Configure automatic updating in the application server's *web.config*. You can adjust the behavior with the following statements:

```xml
<autoupdate>
    <!-- <add key="off" value="true" /> -->
    <add key="checkinterval" value="00:05:00"/>
    <add key="inactivitytime" value="00:00:10"/>
</autoupdate>
```

The application is updated automatically. To run an update, first load the files to be updated into the One Identity Manager database. The necessary files are loaded into the One Identity Manager database and updated when a hotfix, a service pack or a full version update is run.

The test is executed when the application starts and then at 5 minute intervals. New files are loaded from the database as they are identified. The files cannot be updated while the application is running. The update waits until the application is restarted.

The application is restarted automatically by the web server when it has been idle for a defined length of time. However, this may take some time or be hindered by continuous user requests.

**To start the update manually**

1. Open the status page for the application server in the browser.
2. In the menu for the currently logged on user, click **Update immediately**.

**Related topics**

- [Displaying the application server status](#) on page 116
- [Automatic updating of One Identity Manager](#) on page 85
Updating the search index on the application server

The searched index is updates when changes are made to a table with indexed columns, to referenced tables or translations.

Use the configuration parameter **Common | Indexing | BatchSize** to define the maximum number of objects that can be indexed in a single indexing run. The default value is **50000**.

The configuration parameter **Common | Indexing | Interval** contains the interval between two indexing runs. The default value is **120** seconds. Once this time interval has elapsed, a new indexing run is started.

You can also update the search index manually.

**To manually update the search index on the application server:**

1. Open the status page for the application server in the browser.
2. In the menu for the currently logged on user, click **Update Index**.
3. Choose whether you want to update all indexes, or only some indexes.

Related topics

- Displaying the application server status on page 116
- Log message for search index creation on page 167

Uninstalling an application server

**To uninstall a web application**

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. On the start page o the installation wizard:
   a. Select the **Installation** tab.
   b. Select **Web-based components** and click **Install**.
      - Starts the Web Installer.
3. On the Web Installer start page, click **Uninstall a One Identity Manager web application** and click **Next**.
4. The **Uninstall a One Identity Manager web application** page displays all installed web applications.
a. Select the web application you want to remove by double-clicking it.
   The icon is displayed in front of the application.

b. In the Authentication method area, select an authentication method and enter the corresponding login data.

c. To start uninstalling the web application(s), click Next.

d. Confirm the security prompt with Yes.

5. The uninstall progress is displayed on the Setup is running page.

6. Once installation is complete, click Next.

7. On the Wizard complete page, click Finish.

8. Close the autorun program.
Installing the API Server

The API Server hosts the API that you have defined in the API Designer. Angular web apps can also be delivered via the API Server.

To make full use of the API Designer, you must first install the API Server. You can use the Web Installer to help install the API Server. Read through the following sections for instructions on how to install the API Server on a Windows server and set it up with the default configuration.

Detailed information about this topic

- Installing the API Server on page 120

Installing the API Server

The following describes how to install the API Server.

- **NOTE:** Before installation ensure that the minimum **hardware and software requirements** are fulfilled on the server.

- **IMPORTANT:** Start the API Server installation locally on the server.

To install the API Server

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. On the start page of the installation wizard, switch to the **installation** tab in the navigation on the left.
3. Click **Install** next to **Web-based components**.
   Starts the Web Installer.
4. On the Web Installer start page, click **Install API Server**.
5. Click **Next**.
6. On the **Database connection** page, do the following:
TIP: One Identity recommends using an AppServer connection.

- To use an existing connection to the One Identity Manager database, select it in the Select a database connection menu.
- OR -
- To create a new connection to the One Identity Manager database, click Add new connection and enter a new connection.

7. Select the authentication method and enter the login data for the database under Authentication method.
8. Click Next.
9. On the Installation source page, do the following:
   - To retrieve the installation data from the database, activate the Database option.
   - OR -
   - To retrieve the installation data from the installation media (e.g. from the hard drive), activate the File system option and enter the path.

10. Configure the following settings on the Select setup target page.

Table 36: Settings for the Installation Target

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Name used as application name, as in the title bar of the browser, for example.</td>
</tr>
<tr>
<td>Target in IIS</td>
<td>Internet Information Services web page on which to install the application.</td>
</tr>
<tr>
<td>Enforce SSL</td>
<td>Specifies, whether the API Server web page can only be opened over an encrypted connection.</td>
</tr>
<tr>
<td>URL</td>
<td>The application's Uniform Resource Locator (URL).</td>
</tr>
<tr>
<td>Install dedicated application pool</td>
<td>Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.</td>
</tr>
<tr>
<td>Application pool</td>
<td>The application pool to use. This can only be entered if the option Install dedicated application pool is not set.</td>
</tr>
<tr>
<td></td>
<td>If you use the default value DefaultAppPool, the application pool has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>&lt;application name&gt;_POOL</td>
</tr>
<tr>
<td>Identity</td>
<td>Permissions for executing an application pool. You can use a default identity or a custom user account.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>If you use the default value <strong>ApplicationPoolIdentity</strong>, the user account has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>IIS APPPOOL&lt;application name&gt; _POOL</td>
</tr>
<tr>
<td></td>
<td>You can authorize another user by clicking ... next to the box, enabling the option <strong>Custom account</strong> and entering the user and password.</td>
</tr>
<tr>
<td>Web authentication</td>
<td>Specifies the type for authentication against the web application. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows authentication (Single Sign-On)</strong></td>
</tr>
<tr>
<td></td>
<td>The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method if Windows authentication is installed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anonymous</strong></td>
</tr>
<tr>
<td></td>
<td>Login is possible without Windows authentication. The user is authenticated against the Internet Information Services and the web application anonymously and the web application is directed to a login page.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can only see this pane if you have selected an SQL database connection on the <strong>Database connection</strong> page.</td>
</tr>
<tr>
<td></td>
<td>Specifies the type for authentication against the One Identity Manager database. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows authentication</strong></td>
</tr>
<tr>
<td></td>
<td>The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible with a user defined user account or a default identity for the application pool.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SQL authentication</strong></td>
</tr>
<tr>
<td></td>
<td>Login is only possible through a user defined user account. Authentication is done using user name and password. This access data is saved in the web application configuration as computer specific encrypted.</td>
</tr>
</tbody>
</table>

11. Click **Next**.
If you have selected a direct database connection in step 4, the page **Select application server** appears. Application server data is required if you want to use full text search. You can enter the application server in the configuration file at a later date.

12. (Optional) Configure the following settings on the **Select application server** page.

   ![NOTE: If you would like to use the full text search, then you must specify an application server. You can enter the application server in the configuration file at a later date.]

   a. Click **Select application server**.
   b. Enter the application server's web address in the **URL** field.
   c. Click **OK**.

13. On the **Select application server** page, click **Next**.

14. On the **Set session token certificate** page, select the certificate for creating and checking session tokens. Perform one of the following tasks:

   - To use an existing certificate:
     a. In the **Session token certificate** list, select **Use existing certificate**.
     b. Select an existing certificate from the **Select certificate** list.

   - To create a new certificate:
     a. In the **Session token certificate** list, select **Create new certificate**.
     b. In the **Certificate issuer** field, the name of the certificate issuer.
     c. Select the key length of the certificate from the **Key length** list.

   - To create a new certificate file:
     a. In the **Session token certificate** list, select **Create new certificate file**.
     b. In the **Certificate issuer** field, the name of the certificate issuer.
     c. Select the key length of the certificate from the **Key length** list.
     d. In the **Certificate file** field, enter the path and file name for the new certificate.

15. Click **Next**.

16. Specify the user account for automatic updating on the **Set update credentials** page by activating one of the following options:

   ![NOTE: The user account is used to add or replace files in the application directory.]

   - **Use IIS credentials for update**: Set this option to use the user account used by the application pool to run updates.
• **Use other credentials for updates:** To use a different user account, set this option. Specify the domain, the user name, and the user password.

17. Click **Next**.

18. On the **Application token** page, enter the application token for the API Server into the input field.

   **TIP:** To use a new token and therefore replace the existing token in the database, activate the option **Replace the application token in the database.** When doing so, please note that the current token will become invalid and every location that uses it must be updated with the new token.

19. Click **Next**.

   The **Setup is running** page opens and shows the progress of each installation step.

20. Once installation is complete, click **Next**.

21. On the **Wizard complete** page, click **Finish**.

22. Close the autorun program.

**Related topics**

- **Uninstalling the API Server** on page 125

### Installing and accessing HTML5 applications

To speed up initial installation, the Operations Support Web Portal is not installed automatically. If you want to provide the Operations Support Web Portal (or any other HTML application), you must follow these steps after installing the API Server.

**To install and compile HTML applications**

1. Start the Designer.
2. Connect to the relevant database.
3. In the navigation, select **Getting Started | Edit configuration parameters**.
4. On the **Configuration parameters** tab, enable the configuration parameter **QBM | HtmlDevelopment | Compiler**.
5. Recompile the database.

   **NOTE:** Ensure that the workstation you are compiling on, can establish a connection to the website registry.npmjs.org:443.
**To access all installed HTML5 applications**

- In a web browser, open the web address (URL) of your API Server. All installed HTML5 applications are displayed.

**Related topics**

- [Installing the API Server](#) on page 120

---

**Uninstalling the API Server**

**To uninstall a web application**

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. On the start page o the installation wizard:
   a. Select the **Installation** tab.
   b. Select **Web-based components** and click **Install**.
      Starts the Web Installer.
3. On the Web Installer start page, click **Uninstall a One Identity Manager web application** and click **Next**.
4. The **Uninstall a One Identity Manager web application** page displays all installed web applications.
   a. Select the web application you want to remove by double-clicking it.
      The icon is displayed in front of the application.
   b. In the **Authentication method** area, select an authentication method and enter the corresponding login data.
   c. To start uninstalling the web application(s), click **Next**.
   d. Confirm the security prompt with **Yes**.
5. The uninstall progress is displayed on the **Setup is running** page.
6. Once installation is complete, click **Next**.
7. On the **Wizard complete** page, click **Finish**.
8. Close the autorun program.

**Related topics**

- [Installing the API Server](#) on page 120
Installing, configuring and maintaining the Web Portal

You can use the Web Installer to install, configure and update the Web Portal. The following describes the steps necessary for installing the Web Portal on a Windows server and for getting the standard version up and running. The configuration settings are explained using their corresponding, possible values.

Detailed information about this topic

- Installing the Web Portal on page 126
- Updating the Web Portal on page 131
- Uninstalling the Web Portal on page 132
- Configuring the Web Portal on page 133
- Maintenance of the Web Portal on page 140

Installing the Web Portal

The following describes how to install the Web Portal. Please note the following information:
NOTES:

- Before installation ensure that the minimum hardware and software prerequisites are fulfilled on the server.
- Prepare an application server on which the search service for the Web Portal is installed.
- Start the Web Portal installation locally on the server.
- If you install the Web Portal with HTTPS, the transfer method for cookies is configured to use HTTPS in the Web Installer.
- If you change the SSL settings for the Web Portal at a later time, you must manually update the value in the Web Portal’s web.config configuration file.
- Default values are used for the configuration settings during installation. You can keep these values. Check the settings using the Web Designer Configuration Editor.

To make a modification

- Example: Enter the value `<httpCookies requireSSL="true"/>` in the web.config under element `<system.web>`.

To install the Web Portal

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. On the start page of the installation wizard, switch to the installation tab in the navigation on the left.
3. Click Install next to Web-based components.
   Starts the Web Installer.
5. Click Next.
6. On the Database connection page, do the following:
   - to use an existing connection to the One Identity Manager database, select it in the Select a database connection menu.
   - OR -
   - to create a new connection to the One Identity Manager database, click Add new connection and enter a new connection. For more information, see Configuring the database connection.
7. Select the authentication method and enter the login data for the database under Authentication method.
8. Click Continue.
9. Configure the following settings on the Select setup target page.
### Table 37: Settings for the Installation Target

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Name used as application name, as in the title bar of the browser, for example.</td>
</tr>
<tr>
<td>Target in IIS</td>
<td>Internet Information Services web page on which to install the application.</td>
</tr>
<tr>
<td>Enforce SSL</td>
<td>Specifies whether insecure websites are available for installation. If the option is set, only sites secured by SSL can be used for installing. This setting is the default value. If this option is not set, insecure websites can be used for installing.</td>
</tr>
<tr>
<td>URL</td>
<td>The application's Uniform Resource Locator (URL).</td>
</tr>
<tr>
<td>Install dedicated application pool</td>
<td>Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.</td>
</tr>
<tr>
<td>Application pool</td>
<td>The application pool to use. This can only be entered if the option <strong>Install dedicated application pool</strong> is not set. If you use the default value <strong>DefaultAppPool</strong>, the application pool has the following syntax: <code>&lt;application name&gt;_POOL</code></td>
</tr>
<tr>
<td>Identity</td>
<td>Permissions for executing an application pool. You can use a default identity or a custom user account. If you use the default value <strong>ApplicationPoolIdentity</strong>, the user account has the following syntax: <code>IIS APPPOOL\&lt;application name&gt;_POOL</code> You can authorize another user by clicking ... next to the box, enabling the option <strong>Custom account</strong> and entering the user and password.</td>
</tr>
<tr>
<td>Web authentication</td>
<td>Specifies the type for authentication against the web application. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows authentication (Single Sign-On)</strong></td>
</tr>
<tr>
<td></td>
<td>The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method is Windows authentication is installed.</td>
</tr>
</tbody>
</table>
### Setting Description

- **Anonymous**
  
  Login is possible without Windows authentication. The user is authenticated against the Internet Information Services and the web application anonymously and the web application is directed to a login page.

Database authentication

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymous</strong></td>
<td>Login is possible without Windows authentication. The user is authenticated against the Internet Information Services and the web application anonymously and the web application is directed to a login page.</td>
</tr>
</tbody>
</table>

**NOTE:** You can only see this section if you have selected an SQL database connection on the Database connection page.

Specifies the type for authentication against the One Identity Manager database. You have the following options:

- **Windows authentication**
  
  The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible with a user defined user account or a default identity for the application pool.

- **SQL authentication**
  
  Login is only possible through a user defined user account. Authentication is completed with a user name and password. This access data is saved in the web application configuration as computer specific encrypted.

10. Click **Next**.

If you have selected a direct database connection in step 4, the page Select application server appears. Application server data is required if you want to use full text search. You can enter the application server in the configuration file at a later date.

11. (Optional) Configure the following settings on the Select application server page.

**NOTE:** If you would like to use the full text search in the Web Portal, then you must specify an application server. You can enter the application server in the configuration file at a later date.

**NOTE:** If using Windows authentication and the application server is located on a different host to that of the Web Portal, or if the application server uses a different user account for the application pool to that used by the Web Portal, then some further Active Directory settings must be configured (e.g. a Kerberos delegation).

a. Click **Select application server**.

b. In the dialog, enter the address of the application server on which the full text
search service is installed into the URL field.

c. Click OK.

12. On the Select application server page, click Next.

13. On the Installation source page, perform one of the following actions in the Installation source area:
   
   - to retrieve the installation data from the database, activate the Load from database option.
   
   - OR -

   - to retrieve the installation data from the installation media (e.g. from the hard drive), activate the Load from local folder option and enter the path.

14. In the Web project list, select the desired web project and enter the authentication data if required:

   a. Click .
   
   b. In the Authentication data dialog, click a red project.
   
   c. Under Authentication method, specify the method and login data you would like to use.
   
   d. Repeat these steps for all other red projects.
   
   e. Click OK.

15. On the Set update credentials page, specify the user account for automatic updating by activating one of the following options:

   a. Click .
   
   b. In the Authentication data dialog, click a red project.
   
   c. Under Authentication method, specify the method and login data you would like to use.
   
   d. Repeat these steps for all other red projects.
   
   e. Click OK.

16. Specify the user account for automatic updating on the Set update credentials page by activating one of the following options:

17. Click Continue.
The Setup is running page opens and shows the progress of each installation step. The Web Installer generates the web application and the corresponding configuration files for each folder.

18. Installation progress is displayed on the Setup is running page. The Web Installer generates the web application and the corresponding configuration files for each folder.

19. Once installation is complete, click Next.

20. On the Validate installation page, test the start of the web application. The base URL is displayed for mail distribution. If you wish to use a different URL, select this from the Change to field.

21. Click Continue.

22. On the Wizard complete page, click Finish.

23. Close the autorun program.

Related topics

- Minimum system requirements for the web server on page 39
- Installing an application server on page 113
- Configuring the Web Portal on page 133
- Authentication data for the web application on page 134

Upgrading the Web Portal

<table>
<thead>
<tr>
<th>NOTE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- We recommend that you perform the automatic update only in specific maintenance windows, in which the application cannot be accessed by users and the application can be manually restarted with no risk.</td>
</tr>
<tr>
<td>- The following permissions are required for automatic updating:</td>
</tr>
<tr>
<td>- The user account for updating requires write permissions for the application directory.</td>
</tr>
<tr>
<td>- The user account for updating requires the local security policy Log on as a batch job.</td>
</tr>
<tr>
<td>- The user account running the application pool requires the local security policies Replace a process level token and Adjust memory quotas for a process.</td>
</tr>
</tbody>
</table>

The configuration settings for the automatic update of the web application are made in the configuration file web.config. You can do this using the Web Designer Configuration Editor.
To update the web application automatically

1. Open the Runtime Monitor in the browser.
2. On the Status tab, select one of the options Update now or Update when all user sessions are closed.

To update a web application manually

- Uninstall the existing Web Portal and re-install the Web Portal.

Note that each write access to the web application’s bin folder causes the web application to restart. This means that all active sessions in the application are closed and all unsaved data is lost. For this reason, you should only perform manual updates of the web application if no active session is running.

Related topics

- Configuring the automatic update for the Web Portal on page 137
- Automatic updating of web applications on page 89
- Installing the Web Portal on page 126
- Displaying the Runtime Monitor on page 140
- Maintenance mode on page 142

Uninstalling the Web Portal

To uninstall a web application

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. On the start page o the installation wizard:
   a. Select the Installation tab.
   b. Select Web-based components and click Install.
      Starts the Web Installer.
3. On the Web Installer start page, click Uninstall a One Identity Manager web application and click Next.
4. The Uninstall a One Identity Manager web application page displays all installed web applications.
   a. Select the web application you want to remove by double-clicking it.
      The icon is displayed in front of the application.
   b. In the Authentication method area, select an authentication method and enter the corresponding login data.
c. To start uninstalling the web application(s), click **Next**.
d. Confirm the security prompt with **Yes**.

5. The uninstall progress is displayed on the **Setup is running** page.
6. Once installation is complete, click **Next**.
7. On the **Wizard complete** page, click **Finish**.
8. Close the autorun program.

### Configuring the Web Portal

Web Portal configuration covers a number of settings. The configuration is saved in the web application configuration files `web.config`, `NLog.config` and `monitor.config`, which are found in the base directory of the web application, and in the table `QBMWebApplication` of the One Identity Manager database.

Use the Web Designer Configuration Editor (`WebDesigner.ConfigFileEditor.exe`) to edit the `web.config` configuration file.

Connection strings and login data are automatically encrypted in the configuration files noted above with the default Microsoft ASP.NET cryptography.

**To configure a web application**

1. Start the program `WebDesigner.ConfigFileEditor.exe` from the installation directory of the web application.
2. Select the configuration file `web.config` in the Open configuration file view and click **Open**.
3. Select the required authentication procedure and log on.

   Make the configuration settings in the individual areas of the Web Designer Configuration Editor.

**Detailed information about this topic**

- Configuring the database connection on page 134
- Authentication data for the web application on page 134
- Logging for the web application on page 136
- Configuring the automatic update for the Web Portal on page 137
- Advanced web settings on page 138
- Storing the cache directories on page 139
- Configuring the debugger service on page 139
- Configuring the search service on page 139
Configuring the database connection

The current connection settings for the Web Portal can be viewed in the Web Designer Configuration Editor in the Database connection view. You can customize the settings as required.

To select a new database connection

1. Open the Web Designer Configuration Editor.
2. In the Database connection area, click Enter new connection.
3. Select the system type and enter the connection data.
   - For the system type SQL Server, enter the following information.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Database server.</td>
</tr>
<tr>
<td>Windows authentication</td>
<td>Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td>
</tr>
<tr>
<td>User</td>
<td>SQL Server Login name.</td>
</tr>
<tr>
<td>Password</td>
<td>SQL Server login password.</td>
</tr>
<tr>
<td>Database</td>
<td>Database.</td>
</tr>
</tbody>
</table>

- For the system type Application server, enter the URL.

**NOTE:** In the Options menu, select either Test connection or Advanced options as required.

Related topics

- Logging in to the One Identity Manager database on page 151

Authentication data for the web application

The authentication data for the web project and subprojects is configured in the Web Designer Configuration Editor in the Web project area. For detailed information about the authentication modules, see the One Identity Manager Authorization and Authentication Guide.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web project</td>
<td>Name of the web project.</td>
</tr>
<tr>
<td>Authentication module</td>
<td>Authentication module for logging on to the web project.</td>
</tr>
<tr>
<td>NOTE: Some authentication modules support single sign-on. In such cases, a corresponding message is shown beneath selection.</td>
<td></td>
</tr>
<tr>
<td>Perform single sign-on, if an error occurs, using the following module.</td>
<td>If the module selected under Authentication module supports single sign-on, you have the option to specify an alternative authentication method here. This authentication method is used as a fallback if single sign-on fails for any reason.</td>
</tr>
<tr>
<td>Debugging</td>
<td>Activate this option if you want to use a debugging environment.</td>
</tr>
<tr>
<td>OAuth</td>
<td>If you use the authentication modules OAuth 2.0 / OpenID Connect or OAuth 2.0 / OpenID Connect (role-based), you make the configuration settings here.</td>
</tr>
<tr>
<td>OAuth 2.0 / OpenID Connect</td>
<td>Select the OAuth 2.0 / OpenID Connect configuration that you want to adjust.</td>
</tr>
<tr>
<td>Client ID for OAuth authentication</td>
<td>ID of the application on the identity provider. Example: urn:OneIdentityManager/Web</td>
</tr>
<tr>
<td>Issuer information for the OAuth certificate</td>
<td>This is used to find the certificate in the certificate store. Either the thumb nail or the issuer of the certificate is required. For example: O=[company name], OU=[organizational unit], CN=[server IP]</td>
</tr>
<tr>
<td>OAuth Resource</td>
<td>Uniform Resource Name (URN) of the resource to be queried. Only required if the identity provider requires this value.</td>
</tr>
<tr>
<td>Fingerprint for the OAuth certificate</td>
<td>Fingerprint of the certificate used to verify the security token. Either the thumb nail or the issuer of the certificate is required.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Uniform Resource Locator (URL) of the certificate end point on the authorization server. For example: <a href="https://certificateServer/certificate.crt">https://certificateServer/certificate.crt</a></td>
</tr>
<tr>
<td>Authentication data for subprojects</td>
<td>Authentication data for subprojects.</td>
</tr>
</tbody>
</table>

**To enter or change authentication data for a sub project**

1. Open the Web Designer Configuration Editor.
2. In the Web project area, next to the Authentication for sub projects is missing message, click ⌺.
3. In the edit view, click on the project marked in red.
4. In the Authentication method area, select the required authentication procedure and enter the required login information.
5. Click OK.

Logging for the web application

The settings for logging the web application are configured in the Web Designer Configuration Editor in the Log area. This view is divided into:

- General
- Application log
- Event log
- Database log

Table 40: General settings for logging

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Name of the web application.</td>
</tr>
<tr>
<td>Company name</td>
<td>Name of the company that uses the web application.</td>
</tr>
<tr>
<td>Product title</td>
<td>Software manufacturer’s product name</td>
</tr>
<tr>
<td>Log directory</td>
<td>Directory in which the log files of the web application are saved.</td>
</tr>
<tr>
<td></td>
<td>The web server process must have write access to this folder.</td>
</tr>
</tbody>
</table>

Table 41: Application log settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity code</td>
<td>Severity level of the log.</td>
</tr>
<tr>
<td>Archive every</td>
<td>Maximum runtime of a log file before it is renamed.</td>
</tr>
<tr>
<td>Archive numbering</td>
<td>Specifies whether the archive files of the application log are numbered</td>
</tr>
<tr>
<td></td>
<td>in ascending or descending order.</td>
</tr>
</tbody>
</table>

Table 42: Event log settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity code</td>
<td>Severity level of the log.</td>
</tr>
</tbody>
</table>
Table 43: Database log settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity code</td>
<td>Severity level of the log.</td>
</tr>
<tr>
<td>Archive every</td>
<td>Maximum runtime of a log file before it is renamed. When a log file has reached its maximum age, the file is renamed and a new log file is started.</td>
</tr>
<tr>
<td>Archive numbering</td>
<td>Specifies whether the archive files of the database log are numbered in ascending or descending order.</td>
</tr>
</tbody>
</table>

Table 44: Permitted severities

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No information is logged.</td>
</tr>
<tr>
<td>Trace</td>
<td>Logs highly detailed information. This setting should only be used for analysis purposes. The log file quickly becomes large and cumbersome.</td>
</tr>
<tr>
<td>Debug</td>
<td>Logs debug steps. This setting should only be used for testing.</td>
</tr>
<tr>
<td>Info</td>
<td>Logs all information.</td>
</tr>
<tr>
<td>Warning</td>
<td>Logs all warnings.</td>
</tr>
<tr>
<td>Errors</td>
<td>Logs all error messages.</td>
</tr>
<tr>
<td>Fatal</td>
<td>Logs all critical error messages.</td>
</tr>
</tbody>
</table>

Configuring the automatic update for the Web Portal

**NOTE:** The following permissions are required for automatic updating:

- The user account for updating requires write permissions for the application directory.
- The user account for updating requires the local security policy **Log on as a batch job**.
- The user account running the application pool requires the local security policies **Replace a process level token** and **Adjust memory quotas for a process**.

The automatic update is configured in the Web Designer Configuration Editor in the **Automatic update** area.
To configure the automatic update of the web application

1. Open the Web Designer Configuration Editor.
2. In the Automatic updates area, set the Enable automatic updates option.
3. Define the user account for the automatic update. The user account is used to add or replace files in the application directory.
   - **Use IIS credentials for update**: Set this option to use the user account under which the application pool is executed for the updates.
   - **Use other credentials for updates**: To use a different user account, set this option. Specify the domain, the user name, and the user password.

Related topics

- Automatic updating of One Identity Manager on page 85
- Automatic updating of web applications on page 89
- Updating the Web Portal on page 131

Advanced web settings

In the Web settings area of the Web Designer Configuration Editor, you configure the following web settings.

Table 45: Web setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML headers</td>
<td>HTTP header lines that the server outputs for every HTTP query.</td>
</tr>
<tr>
<td>After logging off</td>
<td>Page that is displayed after the user has logged off.</td>
</tr>
<tr>
<td>Close session after idle time</td>
<td>Period of inactivity after which the session is closed.</td>
</tr>
<tr>
<td>(minutes)</td>
<td><strong>NOTE</strong>: Enter the value 0 if you want the session to remain open despite being idle.</td>
</tr>
<tr>
<td>Compress HTTP transfer</td>
<td>Specifies whether the HTTP transfer takes place in compressed form.</td>
</tr>
<tr>
<td>Create Windows performance</td>
<td>When you install a web application, performance counters are registered, which provide information about the state of the application. For detailed information, see the Using the performance indicators for monitoring on page 142.</td>
</tr>
<tr>
<td>indicators</td>
<td></td>
</tr>
</tbody>
</table>
Storing the cache directories

The storage of the cache directories is configured in the Web Designer Configuration Editor in the Cache area.

Table 46: Settings for cache directories

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache directory</td>
<td>Full path to the directory used for temporary saving of frequently used application contents.</td>
</tr>
<tr>
<td>Assembly Cache</td>
<td>Full path to the directory for caching assembler files.</td>
</tr>
</tbody>
</table>

Configuring the debugger service

For functions of the web application that support the debugging mode, a Windows Communication Foundation (WCF) connection must be established. The permitted port range for the WCF connection is configured in the Web Designer Configuration Editor in the Debugger Service area.

To restrict the port range of the WCF connection

1. Open the Web Designer Configuration Editor.
2. In the Debugger service area, enable the Limit port range option and define the limits for the port using the connection.

Configuring the search service

Prerequisite for using the Web Portal is an application server installed with the search service.

- If you run the Web Portal directly over an application server installed with the search service, you can use the full text search immediately.
- If you are using the Web Portal with an application server that does not have an installed search service, or with a direct database connection, you will need to enter an application server with an installed search service in the configuration of the web application.

The application server is usually entered during the Web Portal installation. For subsequent changes, use the Web Designer Configuration Editor.
To enter an application server at a later date

1. Open the Web Designer Configuration Editor.
2. In the Search service area, click Select application server.
3. Enter the application server's web address in the URL.
4. Test the connection by selecting Test connection from the Options menu.
5. Edit other optional settings by selecting Advanced settings from the Options menu.
6. To accept the settings, click OK.

Certain important columns are already indexed for full text search in the default installation. You configure more columns for full text searching if you require.

For detailed information about configuring columns for the full text search, see the One Identity Manager Configuration Guide. For detailed information about using the full text search in the Web Portal, see the One Identity Manager Web Portal User Guide.

Related topics

- Installing and updating an application server on page 112
- Installing the Web Portal on page 126

Maintenance of the Web Portal

The following is a list of the maintenance options available for a web application, together with descriptions.

Detailed information about this topic

- Displaying the Runtime Monitor on page 140
- Log files and exceptions on page 141
- Maintenance mode on page 142
- Using the performance indicators for monitoring on page 142

Displaying the Runtime Monitor

The Web Portal includes a runtime monitor for monitoring. The runtime monitor is accessed via a browser front end.

Use the appropriate URL for this:

\[ \text{http://<servername>/<application>/monitor} \]
Access permissions for the runtime monitor

Access to the runtime monitor is configured in the configuration file (monitor.config) of the web application. The default settings enables only members of the group BUILTIN\Administrators to access the runtime monitor.

```xml
<?xml version="1.0"?>
<!-- Permission to use WebDesigner runtime monitor -->
<authorization>
    <allow roles="BUILTIN\Administrators" />
    <deny users="*" />
</authorization>
```

For more information about changing this setting, see the ASP.NET documentation.

Log files and exceptions

The log files are displayed in the Runtime Monitor.

- All log files generated by the web application are displayed on the Log files tab. You can filter these file and search by strings. The log files exist in physical form in the log directory defined by the configuration in the configuration file of the web application, usually ./Logs).
- The Exceptions tab display log messages that contain exception errors. These messages are sorted by exception error and in descending order of frequency. The top exception error in the list is the error that occurs most frequently.

**NOTE:** The Web Installer writes important events to the log file of the application. You can view this log file in the Windows event display.

Related topics

- Logging for the web application on page 136
- Displaying the Runtime Monitor on page 140
Maintenance mode

To carry out maintenance work, switch the web application to maintenance mode. You use maintenance mode, for example, to enable an update at a particular time.

No new sessions are permitted in maintenance mode. Current sessions are not affected. While maintenance work is being performed, users who view the web application are displayed the contents of the Maintenance.html file, which is located in the installation directory of the web application. You can edit this file to display details of the maintenance work for the user.

**To switch the web application to maintenance mode**

1. Open the Runtime Monitor in the browser.
2. On the **Status** tab, click **Start maintenance mode**.

**To end maintenance mode**

1. Open the Runtime Monitor in the browser.
2. On the **Status** tab, click **End maintenance mode**.

Maintenance mode can also be activated by creating the file App_Data\Maintenance.mode in the installation directory of the web application, and terminated by deleting this file.

**Related topics**

- Displaying the Runtime Monitor on page 140

Using the performance indicators for monitoring

When you install a web application, performance counters are registered, which provide information about the state of the application.

Performance indicators can be installed later.

**NOTE:** Prerequisites for this are that the web application is installed on a Windows Server and has sufficient permissions to offer performance indicators. It may be necessary to add the application pool user account to the local group **Performance monitoring user** for this. Apart from this, the web application must be running in order to select the performance indicators.

**To post-install performance indicators**

1. Open the Web Designer Configuration Editor.
2. Click **Web settings** and **Create Windows performance counters**.
After this is successfully completed, an installation prompt is displayed.

3. Confirm the prompt with **OK**.

**To view performance counters**

1. Log in to the server on which the web application is installed.
3. In the dialog on the left-hand side, select **Performance monitoring**.
4. In the display area for performance monitoring, click **+**.
5. In the **Add Counters** dialog, under **Available Counters**, select **One Identity Manager Web Portal** and add to the entry.

   This displays performance indicators for the web application. The following indicators are available.

<table>
<thead>
<tr>
<th>Performance indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AJAX calls</td>
<td>Number of HTTP queries processed asynchronously.</td>
</tr>
<tr>
<td>Objects</td>
<td>Number of active database objects.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Number of exception errors that have occurred.</td>
</tr>
<tr>
<td>Forms</td>
<td>Number of active forms.</td>
</tr>
<tr>
<td>HTML requests</td>
<td>Number of HTML page requests.</td>
</tr>
<tr>
<td>PID</td>
<td>Number of process IDs.</td>
</tr>
<tr>
<td>Contexts</td>
<td>Number of active module objects.</td>
</tr>
<tr>
<td>Sessions</td>
<td>Number of active sessions.</td>
</tr>
<tr>
<td>Sessions total</td>
<td>Total number of sessions since the application started.</td>
</tr>
</tbody>
</table>

6. Enter any new performance indicators you wish and select the web application under **Instances of selected object**.

   **TIP:** Only the web applications that have started are displayed for selection. If you install a new web application, it may take a few minutes before the list of available web applications including the new one is available.
Installing and updating the Manager web application

Manager functionality can be provided by web applications. Before installation ensure that the minimal hardware and software prerequisites are fulfilled on the server.

Detailed information about this topic

- Minimum system requirements for the web server on page 39
- Installing the Manager web application on page 144
- Updating the Manager web application on page 147
- Uninstalling the Manager web application on page 148
- Appendix: Extended configuration of the Manager web application on page 171

Installing the Manager web application

One Identity Manager requires each web application to be defined in one language. If you wish to publish an application in two languages, you must install two separate applications. Web Installer installs one application per language by default.

You can define a language pool for these applications if several application are running at once. If a user calls up a web application from the language pool, he is automatically diverted to the web application which matches his language. It is, therefore, not important to declare all the web application URLs in the language pool.

This mechanism also allows you to achieve simple load balancing.

⚠️ IMPORTANT: Start the Manager web application installation on the server.

To install the Manager web application

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. Go to the Installation tab and select the entry Web based components and click
**Install.** Starts the Web Installer.

3. On the start page of the Web Installer, select **ManagerInstall web application** and click **Next.**

4. On the **Database connection** page, enter the connection credentials for the One Identity Manager database.

5. Configure the following settings on the **Select setup target** page.

**Table 48: Settings for the Installation Target**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Name used as application name, as in the title bar of the browser, for example.</td>
</tr>
<tr>
<td>Target in IIS</td>
<td>Internet Information Services web page on which to install the application.</td>
</tr>
<tr>
<td>Enforce SSL</td>
<td>Specifies whether insecure websites are available for installation. If the option is set, only sites secured by SSL can be used for installing. This setting is the default value. If this option is not set, insecure websites can be used for installing.</td>
</tr>
<tr>
<td>URL</td>
<td>The application's Uniform Resource Locator (URL).</td>
</tr>
<tr>
<td>Install dedicated application pool</td>
<td>Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.</td>
</tr>
<tr>
<td>Application pool</td>
<td>The application pool to use. This can only be entered if the option <strong>Install dedicated application pool</strong> is not set.</td>
</tr>
<tr>
<td></td>
<td>If you use the default value <strong>DefaultAppPool</strong>, the application pool has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>&lt;application name&gt;Pool</td>
</tr>
<tr>
<td>Identity</td>
<td>Permissions for executing an application pool. You can use a default identity or a custom user account.</td>
</tr>
<tr>
<td></td>
<td>If you use the default value <strong>ApplicationPoolIdentity</strong>, the user account has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>IIS APPPOOL&lt;application name&gt;Pool</td>
</tr>
<tr>
<td></td>
<td>You can authorize another user by clicking ... next to the box, enabling the option <strong>Custom account</strong> and entering the user and password.</td>
</tr>
<tr>
<td>Web authentication</td>
<td>Specifies the type for authentication against the web application. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows authentication (Single Sign-On)</strong></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method is Windows authentication is installed.</td>
<td></td>
</tr>
</tbody>
</table>

- **Anonymous**
  
  Login is possible without Windows authentication. The user is authenticated against the Internet Information Services and the web application anonymously and the web application is directed to a login page.

<table>
<thead>
<tr>
<th>Database authentication</th>
<th><strong>NOTE:</strong> You can only see this section if you have selected an SQL database connection on the Database connection page.</th>
</tr>
</thead>
</table>

Specifies the type for authentication against the One Identity Manager database. You have the following options:

- **Windows authentication**
  
  The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible with a user defined user account or a default identity for the application pool.

- **SQL authentication**
  
  Login is only possible through a user defined user account. Authentication is completed with a user name and password. This access data is saved in the web application configuration as computer specific encrypted.

6. Specify other application specific settings on the **Configuration** page.
   
   a. Select the language of the application from the **Language** menu. The language influences how dates and numbers displayed amongst other things.
   
   b. The web application requires access permissions to itself. If you selected the authentication type **Windows authentication (single sign-on)** for the Web authentication, enter the domain, user account, and password for the user. For anonymous web authentication, no further entries are required.

7. Specify the user account for automatic updating on the **Set update credentials** page. The user account is used to add or replace files in the application directory.
8. Installation progress is displayed on the **Setup is running** page. Once installation is complete, click **Next**.

9. Click **Finish** on the last page to end the program.

**NOTE:** The Web Installer generates the web application and the corresponding configuration files (web.config) for each directory. The Web Installer uses default values for the configuration settings. You can keep these values. It is recommended you check the settings with the help of the Manager Web Configuration Editor.

### Displaying the Manager web application

The Manager web application is accessed via a browser front end. Use the appropriate URL for this:

- `http://<server name>/<application name>`
- `https://<server>/<application name>`

### Updating the Manager web application

**NOTE:**

- We recommend that you perform the automatic update only in specific maintenance windows, in which the application cannot be accessed by users and the application can be manually restarted with no risk.

- The following permissions are required for automatic updating:
  - The user account for updating requires write permissions for the application directory.
  - The user account for updating requires the local security policy **Log on as a batch job**.
  - The user account running the application pool requires the local security policies **Replace a process level token** and **Adjust memory quotas for a process**.
The application update happens automatically if the plugin "Auto update" is enabled for the web application.

To run an update, first load the files to be updated into the One Identity Manager database. The necessary files are loaded into the One Identity Manager database and updated when a hotfix, a service pack or a full version update is run.

The **Automatic update** plug-in performs a check when the application is started, and every approx. 5 minutes thereafter. New files are loaded from the database as they are identified. The plug-in cannot update the files while the application is running. The update waits until the application is restarted.

The application is restarted automatically by the web server when it has been idle for a defined length of time. This may take some time or be hindered by continuous user requests.

**Related topics**

- Automatic updating of One Identity Manager on page 85
- Appendix: Extended configuration of the Manager web application on page 171

## Uninstalling the Manager web application

**To uninstall a web application**

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. On the start page of the installation wizard:
   a. Select the **Installation** tab.
   b. Select **Web-based components** and click **Install**.
      Starts the Web Installer.
3. On the Web Installer start page, click **Uninstall a One Identity Manager web application** and click **Next**.
4. The **Uninstall a One Identity Manager web application** page displays all installed web applications.
   a. Select the web application you want to remove by double-clicking it.
      The ✔ icon is displayed in front of the application.
   b. In the **Authentication method** area, select an authentication method and enter the corresponding login data.
   c. To start uninstalling the web application(s), click **Next**.
   d. Confirm the security prompt with **Yes**.
5. The uninstall progress is displayed on the **Setup is running** page.
6. Once installation is complete, click **Next**.
7. On the **Wizard complete** page, click **Finish**.
8. Close the autorun program.
Logging in to One Identity Manager tools

When you start one of the One Identity Manager tools, a default connection dialog opens.

**Figure 5: Default connection dialog**

![Default connection dialog](image)

When you log in, you need to be aware of the difference between a database user and a user of individual One Identity Manager tools (system user). Several system users can work with one database user.

Login takes place in two steps:
Selecting the database connection to log in to the database

Selecting the authentication method and finding the system user for logging in

Permitted system user IDs are determined by the authentication module you select. One Identity Manager provides various authentication modules for this purpose.

The One Identity Manager tools can only be started if the user has the relevant program function permissions. Some administration tools expect a specific access level for the selected SQL Server login.

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

NOTE: When you start the program, it tries to restore the last used connection. This might lead to a delay resulting in an error if you frequently swap between connections to other database servers.

To prevent the previous connection restoring, create the following registry key:

HKEY_CURRENT_USER\Software\One Identity\One Identity Manager\Global\Settings\[RestoreLastConnection]="false"

**Detailed information about this topic**

- Logging in to the One Identity Manager database on page 151
- Logging in to the One Identity Manager tools using a system ID on page 153
- Enabling other authentication modules on page 154
- Enabling other login languages on page 156
- Checking authentication on page 156
- Password expiry on page 156

**Logging in to the One Identity Manager database**

*To select an existing connection*

- Select the connection under **Select a database connection** in the connection dialog.

**NOTE:**

- Newly created connections are not shown in the connection dialog until the program has been restarted.
- Connections that do not use the expected access level for SQL Server logins are not shown in the connection dialog.
- The access level for an existing connection is shown in the menu item’s tooltip.
To create a new connection to the One Identity Manager database

1. Under Select a database connection, click Add new connection and select the SQL Server system type.
2. Click Next.
3. Enter the connection data for the database server.

Table 49: SQL Server database connection data

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Database server.</td>
</tr>
<tr>
<td>Windows authentication</td>
<td>Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td>
</tr>
<tr>
<td>User</td>
<td>SQL Server Login name.</td>
</tr>
<tr>
<td>Password</td>
<td>SQL Server login password.</td>
</tr>
<tr>
<td>Database</td>
<td>Database.</td>
</tr>
</tbody>
</table>

4. Select Test connection in the Options menu.
   This attempts to connect the database with the given connection data. You are prompted to confirm a message about the test.

   NOTE: Using Options | Advanced option item, you can make further changes to the connection configuration.

5. Click Finished.

To set up a new connection to the application server

1. Under Select a database connection, click Add new connection and select Application server.
2. Click Next.
3. Enter the address (URL) for the application server.
4. If you access an application server secured through SSL/TLS, configure additional settings for the certificate:
   - If the certificate's server name matches the application server's URL and, if the server certificate can be successfully validated, the server name displayed in green next the URL. By clicking on the server name next to the URL, you can get information about the certificate. You can select a certificate required for logging in, under Pin server certificate.
   - If the certificate's server name does not match the application server's URL or, if the server certificate cannot be successfully verified, the server name displayed in red next the URL. You decide whether to trust the certificate.
If a client certificate is expected according to the SSL settings, select the certificate under Select client certificate and specify how the certificate is to be verified. You have the following options: Find by subject name, Find by issuer name and Find by thumbprint.

If you want to use a self-signed certificate, enable Accept self-signed certificate.

5. Select Test connection in the Options menu.

This attempts to connect the database with the given connection data. You are prompted to confirm a message about the test.

| NOTE: Using Options | Advanced option item, you can make further changes to the connection configuration. |

6. Click Finished.

To delete a connection

1. Select the connection under Select a database connection.
2. Press DEL.
3. Confirm the security prompt with Yes.

The database connection is no longer displayed in the connection dialog.

Related topics

- Logging in to the One Identity Manager tools using a system ID on page 153

Logging in to the One Identity Manager tools using a system ID

Following the database login, the user must log in as a system user to the started program. Permitted system user IDs are determined by the authentication module you select.

| NOTE: |
| After the initial schema installation, only the System user and ComponentAuthenticator authentication modules and the role-based authentication modules are enabled in One Identity Manager. |
| The One Identity Manager tools can only be started if the user has the relevant program function permissions. |

To log in to One Identity Manager tools with a system user identifier

1. Select the authentication module under Authentication method in the connection dialog.
This displays a list of all available authentication modules.

2. Enter the login data for the system user ID.
   Which login data you require depends on the authentication module selected.

3. Click **Connect**.
   The connection data is saved and made available for the next login.

**Figure 6: Login window**

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

**Related topics**

- Logging in to the One Identity Manager database on page 151
- Enabling other authentication modules on page 154
- Error messages when logging into One Identity Manager tools on page 159

**Enabling other authentication modules**

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

1. In Designer, select Base data | Security settings | Authentication modules.
2. In List Editor, select the authentication module.
3. In the Properties view, set the Activated property to True.
4. Save the changes.

Language settings in One Identity Manager

The default One Identity Manager installation is supplied in the languages English - United States [en-US] and German - Germany [de-DE]. You can add other languages to the user interface and display text if required. In this instance, you must translate the text before One Identity Manager goes live. There is a Designer in the Language Editor to help you do this. A special control is provided in the One Identity Manager tools that aids multi-language input.

One Identity Manager default language

Maintenance of default data takes place in the default language. The default language for an installation of One Identity Manager is English - United States [en-US]. The default language is valid across the system. It is not recommended to change the default language during working hours.

The ideal case is when the One Identity Manager language matches the user’s administration tool login language. If these two settings are different, then the default language is used if no captions are found in the requested login language for a set of language-dependent data.

User login language

The language used in the user interface is the same as the language used when logging into the administration tools. When you log in for the first time, the system language is used for displaying the user interface. Users can change their login language in the program settings in all administration tools. This sets the language globally for all the tools that the user uses. Therefore the user does not have to set the login language in every tool separately. Changes to the login language take effect after the tool has been restarted.

Any language for which the Select in front-end option is activated can be used as a login language.

Related topics

- Enabling other login languages on page 156
Enabling other login languages

To enable an additional login language

1. In Designer, select Base data | Localization | Languages.
2. In the List Editor, select the language.
3. In the Properties view, set the Select in front-end property to True.
4. Save the changes.

Related topics
- Language settings in One Identity Manager on page 155

Password expiry

There are different ways to inform employees that their password is going to expire:

- Users are alerted about their password expiring when they log in to One Identity Manager and can change their password if necessary.
- For employee-based authentication modules, the system sends reminder notifications in relation to expiring passwords as of 7 days in advance of the password expiry date.
  - You can adjust the time in days in the Common | Authentication | DialogUserPasswordReminder configuration parameter. Edit the configuration parameter in the Designer.
  - The notifications are triggered in accordance with the Reminder system user password expires schedule and use the Employee - system user password expires mail template. You can adjust the schedule and mail template in Designer if required.

TIP: To prevent passwords expiring for service account, for example, you can set Password never expires (DialogUser.PasswordNeverExpires) in the Designer for the affected system users.

Checking authentication

When a user logs in, a validity check is run. Use the settings to configure additional options.
The system runs additional validity checks to prevent users from working with established connections, if they were deactivated after they logged in. The check takes place when the next permissions based action on the connection at a fixed interval of 20 minutes.

You can adjust the interval in the configuration parameter **Common | Authentication | CheckInterval**. Edit the configuration parameter in the Designer.

The number of session that a user can open within a short time is limited to 10 session a minute.

If this number is exceeded, the user is sent an error message.

You have logged in too often in the last minute. Please wait a moment before you log in again.

This check is done for each front-end if the login is local. If the login is on the application server, it is checked for each application server.

You can modify the number of sessions in the configuration parameter **Common | Authentication | SessionsPerUserAndMinute**. Edit the configuration parameter in the Designer.

Use the configuration parameter **QBM | AppServer | SessionTimeout** to add the timeout in hours, after which inactive application server sessions are closed. The default value is **24** hours. Edit the configuration parameter in the Designer.
Error handling

For more detailed information, see the One Identity Manager Process Monitoring and Troubleshooting Guide.

Displaying the transport history and checking the One Identity Manager version

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.

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.
Error messages when logging into One Identity Manager tools

Problem
When logging into a One Identity Manager tool, the following error message appears:

[810284] Failed to authenticate user.
[810015] Login for user {0} failed.
[810017] Wrong user name or password.

Possible Cause
- The specified user is not supported by the selected authentication module.
- The specified password is incorrect.
- The employee used for the login is deactivated.
- The user account used for the login is deactivated.

Solution
Check your login information.

Problem
When logging into a One Identity Manager tool, the following error message appears:

[810374] You are not allowed to run this application.

Cause
The One Identity Manager tools can only be started if the user has the relevant program function permissions. You are logging in with a system user ID that does not have the required permissions to start the program.

Possible solutions
- Use a system user ID that has permissions to use the required program function to start the program.
- Provide the system user with the required program function.
  - In Designer, check under **Permissions | Program functions** to see which permissions group contains the required program function.
  - For non-role-based logins: Add the system user to the permissions group in the Designer under **Permissions | System users**.
  - For role-based logins: Ensure that the user is assigned to the application role that contains the program function.

For detailed information about the One Identity Manager authentication modules, permissions groups and application roles, as well as program functions, see the *One Identity Manager Authorization and Authentication Guide*.

## Error messages when installing and updating the One Identity Manager database

Before the installation or update of the One Identity Manager database starts, the Configuration Wizard checks the settings of the database server and the database required for the installation and operation of the One Identity Manager database. For more information, see Database server settings and the One Identity Manager database on page 23.

Some of these settings are corrected by the Configuration Wizard. If the correction is not possible, a corresponding message is issued in Configuration Wizard. In this case, correct the errors manually.

### Table 50: Messages in Configuration Wizard before a database installation or update starts

<table>
<thead>
<tr>
<th>Message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SQL Server Agent did not start.</td>
<td>Start the SQL Server Agent in the SQL Server Service Management Portal. You can log in to an SQL Server Agent both with a domain user account (Domain users) with Windows authentication as well as with a local system account.</td>
</tr>
<tr>
<td>The database collation setting is not valid. ‘SQL_Latin1_General_CP1_CI_AS’ is required.</td>
<td>Set the <strong>Sort order</strong> (collation) database property to the value <strong>SQL_Latin1_General_CP1_CI_AS</strong>.</td>
</tr>
<tr>
<td>The migration cannot be executed because a replication is currently</td>
<td>For more information, see Database errors when migrating a database in SQL Server AlwaysOn availability groups or database mirroring on page 162.</td>
</tr>
<tr>
<td>Message</td>
<td>Solution</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>running.</td>
<td></td>
</tr>
<tr>
<td>The value in 'DialogDatabase.DataOrigin' is invalid. Start by running a database compilation.</td>
<td>Use the Database Compiler to regenerate a database ID and to compile the database. All parts of the database need to be recompiled. Make sure that all the code snippets and all processes are marked.</td>
</tr>
<tr>
<td>The Service Broker cannot be activated because other users are still active.</td>
<td>End the connections of other users to the database.</td>
</tr>
<tr>
<td>The database has no data-file group for in-memory OLTP.</td>
<td>Use the repair method to create a data-file group.</td>
</tr>
<tr>
<td>The database has not defined a file in the data-file group for in-memory OLTP.</td>
<td>Use the repair method to create a database file. The file is created in the directory of the data file (*.mdf).</td>
</tr>
<tr>
<td>The SQL Server has not activated in-memory OLTP.</td>
<td>Set the Is XTP Supported database server property to the True value.</td>
</tr>
<tr>
<td>The 'Arithmetic Abort enabled' database property is not enabled.</td>
<td>Set the Arithmetic Abort enabled database property to the True value.</td>
</tr>
<tr>
<td>The 'Quoted Identifiers Enabled' database property is not activated.</td>
<td>Set the Quoted Identifiers Enabled database property to the True value.</td>
</tr>
<tr>
<td>You cannot run a migration if the recovery model is not 'Simple'.</td>
<td>Set the Recovery model database property to the Simple value.</td>
</tr>
<tr>
<td>The transaction mode cannot be set because other users are active.</td>
<td>End the connections of other users to the database.</td>
</tr>
<tr>
<td>The job queue and/or the DBQueue is not empty. Refer to the documentation for additional information and suggested solutions for this test.</td>
<td>Ensure that the Job queue processes and task in the DBQueue have been processed before starting the update. Use the Job Queue Info program to monitor process handling. For more detailed information, see the One Identity Manager Process Monitoring and Troubleshooting Guide. The Configuration Wizard has the option to ignore this message. Only use this option in test or development environments. By updating the database, modifications may be made, which result in not being able to handle the processes anymore.</td>
</tr>
<tr>
<td>Message</td>
<td>Solution</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The ‘viadmin’ system user must have a valid password that is not empty.</td>
<td>Make sure that the system user has a valid password.</td>
</tr>
</tbody>
</table>

Database errors when migrating a database in SQL Server AlwaysOn availability groups or database mirroring

Possible problems

- The data does not start updating. The Configuration Wizard shows the message:
  The migration cannot be executed because a replication is currently running.
- The following error occurs during a One Identity Manager schema update:
  Database error 1468: The operation cannot be performed on database "<database name>" because it is involved in a database mirroring session or an availability group. Some operations are not allowed on a database that is participating in a database mirroring session or in an availability group. ALTER DATABASE statement failed.

Cause

The database is part of an AlwaysOn availability group or is participating in a database mirroring.

Solution

1. Remove the database from the AlwaysOn availability group or the database mirroring.
2. Update the One Identity Manager schema.
3. Re-admit the database to the AlwaysOn availability group or the database mirroring.
DBQueue Processor does not process tasks

Possible issues

- After restoring a One Identity Manager database from a database backup, no more DBQueue Processor tasks are handled.
- If the SQL Server in running on a virtual machine and the virtual machine is suspended, it is possible that no more DBQueue Processor tasks are handled after restarting the virtual machine.

Probable reason

The SQL Server Service Broker may not be reacting because of initializing the DBQueue Processor. The Service Broker is implemented for DBQueue Processor communications.

Solution

Execute the following steps using a suitable program for executing SQL queries in the database.

**IMPORTANT:** Select a user that you use for migrating the database to execute the SQL queries.

1. Stop all DBQueue Processor components.
   ```
   exec QBM_PWatchDogPrepare 1
   go
   exec QBM_PDBQueuePrepare 1
   go
   ```
2. Check whether other database sessions are active.
   ```
   select *
   from sys.sysprocesses p
   where dbid = DB_ID()
   and spid <> @@SPID
   ```
   If there are still sessions active, they must be closed first.
3. Create a new ServiceBroker ID and enable message delivery.
   ```
   alter database <database name> set NEW_BROKER
   go
   alter database <database name> set enable_broker
   go
   ```
4. Initializing the DBQueue Processor.

```plaintext
exec QBM_PDBQueuePrepare 0,1
```

```plaintext
exec QBM_PWatchDogPrepare
```

**NOTE:** If you restore a test or development database from a backup of another One Identity Manager database, these steps are executed by the Database Compiler. Manual execution of the steps is not necessary in this case. For more information, see Appendix: Creating a One Identity Manager database for a test or development environment from a database backup on page 169.

---

**Message: Enter email address in configuration parameter**

The parameter SenderAddress or Address contains the value `<Enter email address in configuration parameter "...">` in a process for sending emails. Check process parameters in Job Queue Info.

The message is also sent to the One Identity Manager Service log file if extended error reporting in debug mode is configured for the One Identity Manager Service.

**Probable Issue**

The One Identity Manager sends email notifications about various actions taken within the system. The One Identity Manager email notification system is not completely configured.

**Solution**

- Check the configuration parameters for the email notification system in the **Base data | General | Configuration parameters** category in Designer and customize the values.

**Detailed information about this topic**

- Setting up the email notification system on page 69
Operations Support Web Portal is not displayed

Problem
An empty page is displayed in the Internet Explorer if the Operations Support Web Portal is opened with the URL.

Possible Cause
The Operations Support Web Portal should be displayed on an Intranet page and the Display intranet sites in compatibility view setting enabled in the web server.

Solution
In the configuration file (web.config) of the Web Portal application, extend the <system.webServer> section. Enter an attribute or compatibility mode.

```xml
<system.webServer>
  ...
  <httpProtocol>
    <customHeaders>
      ...
      <add name="X-UA-Compatible" value="IE=11" />
      ...
    </customHeaders>
  </httpProtocol>
</system.webServer>
```

Removing superfluous modules

You can remove modules from the One Identity Manager database that you no longer require in your system.
IMPORTANT:

- By removing a module, you lose all the data that goes with it. So it is important to make a backup of the One Identity Manager database before removing any modules.
- In certain circumstances, dependencies to other modules may be deleted by removing a module, therefore, update the One Identity Manager schema after removing a module.
- Other tests may be necessary after removing a module. Remove the module in your test environment first and test the One Identity Manager functionality thoroughly. Make sure to also check any custom adaptations that may use functions in the modules that have been removed.

To remove a module

1. Terminate all web applications using the Internet Information Services (IIS) Manager.
2. Close all One Identity Manager tools except for Job Queue Info.
3. Wait until all processes have terminated. You can do this using the Job Queue Info.
4. Close all One Identity Manager Services via the services manager.
5. Terminate all application servers using the IIS Manager.
6. Wait until all DBQueue Processor tasks have completed. You can do this using the Job Queue Info.
7. Close Job Queue Info.
8. Start a suitable program for executing SQL queries.

IMPORTANT:

- Select a user that you use for migrating the database to execute the SQL queries.
- Execute the following steps separately using a suitable program for executing SQL queries.

Test the output of the query after each step. The output provides additional advice about removing a module.

a. Activate single-user mode for the One Identity Manager database.
   ```sql
   exec dbo.QBM_PSingUserRequest @spid
   ```

b. Stop the DBQueue Processor components.
   ```sql
   exec QBM_PWatchDogPrepare 1
   go
   exec QBM_PDBQueuePrepare 1
   go
   ```

c. Delete all triggers in the database.
exec QBM_PTriggerDrop '%', @force = 1
d. Delete all constraints in the database.
   exec QBM_PConstraintFKDrop '%','%','%'
e. Delete the module you no longer need.
   exec QBM_PModuleRemove '<3-character module abbreviation>'
Example:
declare @ModulesToRemove varchar(100) = 'SAP' + char(7) + 'SHR' + char(7) + 'SBW' + char(7) + 'SAC' + char(7)
exec QBM_PModuleRemove @ModulesToRemove
   go
f. If you delete the Business Roles Module (RMB), you must also delete the entries in the table OrgRoot.
   exec QBM_PDeleteDeep '<Key><T>OrgRoot</T><P>3031e9af-6a53-4876-bbfb-0f7fbe264131</P></Key>

9. End single-user mode for the One Identity Manager database.
   exec dbo.QBM_PSingleUserRelease @spid
10. Update the One Identity Manager schema with the Configuration Wizard. Select all remaining modules for updating.
11. If support sent you hotfixes for this version, then these hotfixes must also be reinstalled.
12. Start the application server, the One Identity Manager Services and the web applications.

Log message for search index creation

Indexing log messages are stored in the application server log (\App_Data\Logs\AppServer.log by default).
A new indexing run is usually started after the indexing interval period specified by the configuration parameter **Common | Indexing | Interval** has elapsed.
If a table being indexed contains more objects to be indexed than the maximum specified by configuration parameter **Common | Indexing | BatchSize**, then the indexing process for the table will stop.
A message is written to the application server log.

   INFO (Indexing ) : Index for Person partially updated, will continue at next run
If at least one table has not been fully indexed, then indexing will restart after 3 seconds. A message is written to the application server log.
INFO (Indexing ) : Index is incomplete (28.06%); indexing will continue in 3000 ms

If a signal to reuse (recycling) the application pool has already been received, the log message will read, e.g.,

INFO (Indexing ) : Index is incomplete (28.06%); indexing will continue when the application re-starts

As long as there is at least one incomplete table, then only the incomplete tables will be indexed during an indexing run.
Appendix: Creating a One Identity Manager database for a test or development environment from a database backup

To create a test or development database from a database backup from another system

1. Create a new database on the database server in the reference environment.
2. Create a database backup of the original database.
3. Restore the backup to the reference database.
4. Restore permissions for the database user on the database server.
5. Compile the database with the Database Compiler.

Use the Database Compiler to customize connection data for the database and compile all scripts and processes in the database.

a. Open Launchpad and select Compile the database. Starts the Database Compiler.

b. On the Database Compiler start page, click Next.

c. On the Connect to database page, enter the connection data for the One Identity Manager database.

d. The database ID is verified. If, during the verification, it transpires that the database ID is incorrect, you will be prompted to create a new ID. Confirm this prompt with OK. The database ID is changed.

e. On the Database connection information insufficient page, check the database connection data and change if necessary.

   • Test the connection parameters (ConnectionString)

     Change the entry using the [...] button beside the input field. Select your database connection data.

   • Test the full customer name.
f. This test the database connection. Confirm the prompt with **OK**.

g. Enter the valid connection data for the One Identity Manager database.

h. On the **Connect to database** page, enter the connection data for the One Identity Manager database.

i. The components to be compiled are displayed on the **Compilation settings** page. To start compiling, click **Next**.

   This starts the compilation process. The process may take some time.

j. The results of the compilation process are shown on **Compilation**. Click **Next** after compilation is complete.

k. Click **Finish** on the last page to end the program.

6. Adjust the database staging level of the database in the Designer.

   a. Select **Base Data | General | Databases** in Designer.

   b. Select the database and change the value of the **Staging level** property to **Test environment** or **Development system**.

   c. Select **Database | Save to database** and click **Save**.

7. Customize the synchronization project's connection data in the Synchronization Editor.

**Related topics**

* Configuring a One Identity Manager database for testing, development or production on page 60
Appendix: Extended configuration of the Manager web application

NOTE: The Web Installer uses default values for most configuration settings. You can use these values normally. It is recommended you check the settings with the help of the Manager Web Configuration Editor.

You configure the Manager web application configuration with the Manager Web Configuration Editor. The Manager Web Configuration Editor is part of the web application and can be found in the install directory in the subdirectory WebConfigEditor.

To run configuration

1. Start the file WebConfigEditor.exe and log in to the One Identity Manager database.
   The Manager Web Configuration Editor automatically opens the web.config file of the web application.
2. Modify the configuration settings.
3. Save the changes.

Detailed information about this topic

- General on page 172
- Database connection on page 172
- Security on page 173
- Debugging on page 174
- Performance on page 175
- File download on page 175
- ASP.net basic settings on page 176
- Application pool on page 177
- Plug-ins on page 178
- Load balancing on page 178
- Single Sign-On on page 179
General

In the **General** area, you configure the appearance of the Manager web application.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Language. The language influences how dates and numbers displayed amongst other things.</td>
</tr>
<tr>
<td>Session timeout</td>
<td>User's idle time in minutes after which the user is automatically logged out. This value depends on the timeout mode and directly effects memory requirements and therefore the application's performance.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This value should be set as long as required and as short as possible because orphaned sessions use memory and negatively effect the application's performance.</td>
</tr>
<tr>
<td>Timeout mode</td>
<td>Methods for determining timeouts. Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>TimeOut:</strong> A session is ended when the period of time defined under Session timeout has elapsed with no user activity.</td>
</tr>
<tr>
<td></td>
<td>- <strong>HeartBeat:</strong> A session is ended when the period of time defined under Session timeout has elapsed with no user activity. The user's open browser window prompts automatically. The timeout begins when the browser window is closed.</td>
</tr>
<tr>
<td>Visualization</td>
<td>Visualization of the application.</td>
</tr>
<tr>
<td>Dynamic design select</td>
<td>Not in use.</td>
</tr>
<tr>
<td>Enable portal mode</td>
<td>Permits the application in a frame to be linked to another application.</td>
</tr>
</tbody>
</table>

Database connection

In the **Database connection** area, you create all database parameters for the Manager web application.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Database connection. You can select between an SQL Server database</td>
</tr>
</tbody>
</table>
Setting | Description
--- | ---
Application | Application which specifies the contents of the web application. Usually, you should select Manager.
Display name | Name used as application name, as in the title bar of the browser, for example.
Authentication | Methods for authenticating the user when logging in to the application.
Single Sign-On | Specifies whether single sign-on is used. Set this option if you user single sign-on. The application does not display a login page to the user but tries to identity the user automatically.

Security

In the Security area, you define several important settings that influence the security of the Manager web application.

Table 53: Meaning of configuration settings for security

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staging</td>
<td>Default configuration of the staging environment. This setting also affects other configuration groups.</td>
</tr>
</tbody>
</table>

Table 54: Permitted values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>Recommended setting for all productive installation.</td>
</tr>
<tr>
<td>Test</td>
<td>Setting if the application was installed for test purposes.</td>
</tr>
<tr>
<td>Development</td>
<td>Setting if the application was installed in a development environment.</td>
</tr>
<tr>
<td>Custom</td>
<td>Setting if all settings are made manually.</td>
</tr>
</tbody>
</table>

Invalid session response delay

Time in seconds that a client sided request with false session data is blocked. This setting prevents possible "Brute force" access attempts.

Permit login without cookies

The application uses session cookies to secure client-server communication. Set this setting to allow user login without cookies. This would be the case, for example, if cookies were forbidden in a company network.
NOTE: It is not recommended to enable this setting.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close browser window after logout</td>
<td>Specifies whether the browser window is closed after logging out. If this setting is enabled, the application tries to close the user’s browser window after logging out. This function is not supported by every browser or only when the browser prompts.</td>
</tr>
</tbody>
</table>

## Debugging

The **Debugging** area contains useful settings for troubleshooting in the Manager web application. Normally, you cannot configure anything here.

### Table 55: Meaning of configuration settings for debugging

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log mode</td>
<td>The amount of data to be logged.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When the application is in productive operation, <strong>Normal</strong> should be set.</td>
</tr>
<tr>
<td>Enable documentation mode</td>
<td>Specifies whether additional data is displayed in the application interface, for example, the name of the active form. The effect depends on the visualization selected.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This setting should not be enabled in a live environment.</td>
</tr>
<tr>
<td>Enable SQL log</td>
<td>Specifies whether the all database instructions are logged. The log is written in the SQL log directory.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This setting should not be enabled in a live environment.</td>
</tr>
<tr>
<td>Show ASP.Net error messages</td>
<td>Specifies whether ASP.Net's own error messages are shown.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This setting should not be enabled in a live environment.</td>
</tr>
<tr>
<td>Enable test mode</td>
<td>Specifies whether automatic tests are supported.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This setting should not be enabled in a live environment.</td>
</tr>
</tbody>
</table>

### Related topics

- **Directories** on page 176
Performance

In the Performance area, you define several important settings that influence the performance of the Manager web application.

### Table 56: Meaning of configuration settings for performance

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancing</td>
<td>The mode of integrated load balancing. In most cases, DistributeEqually should be selected.</td>
</tr>
<tr>
<td>Maximum workload</td>
<td>Maximum number of user sessions an application accepts. The application can be installed multiple times if a large number of sessions is required because system resources for each application process are limited.</td>
</tr>
<tr>
<td>Force maximum workload</td>
<td>The value in Maximum workload is overridden if this setting is not set. However, it is used as a threshold value for the DistributeSuccessively load balancing method.</td>
</tr>
<tr>
<td>Compress HTTP transfer</td>
<td>Specifies whether usage of compression for HTTP communication is set.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Compression of HTTP communication must also be configured for Internet Information Services. For more information see the Web server documentation.</td>
</tr>
<tr>
<td>Host segmentation</td>
<td>Specifies host segmentation. This setting allows distribution of client sided requests to several server addresses representing aliases for the web front-end. This bypasses some of the browser limitation and can therefore shorten loading time if the network connection is bad.</td>
</tr>
</tbody>
</table>

Related topics
- Load balancing on page 178

File download

To enable the download of larger files, the Manager web application requires a directory in which the download can be made available to the user. This effects reports, for example, which are generated by the application and saved as PDF by the user.

### Table 57: Meaning of the configuration settings for the file download

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable file</td>
<td>Specifies whether file download is enabled. Enable this setting to allow larger files, such as reports, to be downloaded. If file download is not set, certain</td>
</tr>
</tbody>
</table>
### Setting Description

**Download functions are not available.**

**Download directory**  
Directory for the application to use to make download available. The application requires full access rights to this directory.

**Cleanup interval**  
Time in minutes search for and remove redundant files.

**Supply time**  
Time in minutes before download is available to the user. Once a download has been initiated, the application cannot verify when and if the download was executed by the user so that the download must be aborted after a set time interval.

### ASP.net basic settings

In the area **ASP.NET settings** you can see some settings of ASP.Net, which can be edited by the Manager Web Configuration Editor.

**Table 58: Meaning of configuration settings for ASP.Net**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max request length</td>
<td>Maximum length of the user request in kilobytes (KB). This limits, amongst others, the maximum size of file that can be loaded.</td>
</tr>
<tr>
<td>Execution timeout</td>
<td>Maximum time in seconds for processing a user request. The user request is aborted if timeout is exceeded.</td>
</tr>
</tbody>
</table>

**NOTE:** This time should not be too short because the user session can be lost if the timeout is exceeded.

### Directories

In the **Directories** area you configure all the directories required by the Manager web application.

**Table 59: Meaning of configuration settings for directories**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application directory</td>
<td>Full path to the application's installation directory. This is the directory where you will find the file web.config.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log directory</td>
<td>Directory to which the application log is written. This directory can be relative to the application directory.</td>
</tr>
<tr>
<td>Database cache</td>
<td>Full path to the directory to save frequently used database contents.</td>
</tr>
<tr>
<td>Script assembly cache</td>
<td>Full path to the directory for caching assembler files.</td>
</tr>
<tr>
<td>SQL log directory</td>
<td>Full path to the directory where database accesses are logged. The SQL log is only used for finding errors and must be enabled through the <strong>Enable SQL log</strong> option in the <strong>Debugging</strong> pane.</td>
</tr>
</tbody>
</table>

**NOTE:** Ensure correct case.

**Related topics**

- [Debugging](#) on page 174

### Application pool

In the **Application pool** view, you define all applications that work together to make the application available to the user in multiple languages.

- Click **Add application** to define another application.
- Click **Remove application** to select an application to remove.
- You can change the order by using the arrows on the right side.

**NOTE:** You must at least define the currently configured application. The order has immediately effect on login performance because the status of configured applications is queried in the defined order.

#### Table 60: Meaning of the configuration settings for the application pool

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect URL</td>
<td>Full address of the application. It must also be possible to resolve this address on the client side through the user's browser.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The applications communicate with each other over the defined URL. Permissions are required to do this if anonymous access is not permitted. The application required the same access rights as required when the URL is called by browser on the server.</td>
</tr>
</tbody>
</table>

**NOTE:** Ensure correct case.
Related topics

- Load balancing on page 178

Plug-ins

Plug-ins extend the functionality of the Manager web application. You can enable a plug-in by setting the option in front of the plug-in name. You may find plug-in specific settings under a plug-in.

Plug-in automatic update

This plug-in runs automatic update.

Table 61: Meaning of configuration settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic update</td>
<td>Automatic update is enabled.</td>
</tr>
<tr>
<td>Severity code</td>
<td>Severity of a change in order to start automatic update.</td>
</tr>
</tbody>
</table>

Related topics

- Updating the Manager web application on page 147
- Automatic updating of One Identity Manager on page 85

Load balancing

The Manager web application provides simple load balancing in order to distribute user sessions and the resulting load across multiple processes or even servers. To do this, the application is installed multiple times on the same or on other servers.

All collaborating applications that can be logged into, are declared in the applications’ Application pool. The selection algorithm for load distribution distributes user logins across the defined applications.

NOTE: Even if only one application is installed, it must be defined in your application pool, otherwise you cannot log in.
Table 62: Supported algorithms for load balancing

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DistributeEqually</td>
<td>This algorithm distributes user logins such that each application in one language has the same number of active users, if possible. This algorithm is the default and is required in 99% of cases.</td>
</tr>
<tr>
<td>DistributeSuccessively</td>
<td>This algorithm distributes user logins by order of application definition in the application pool. First of all, all user logins are forwarded to the first application in the desired language. When this has reached its maximum load, logins are forwarded to the next application.</td>
</tr>
</tbody>
</table>

Load balancing solves the following problems:

- **Multi-language**
  Language is fixed for per application so that an application can only provide user sessions in one language. If users can log in with multiple languages, at least one application must be installed for each language.

- **Bypassing resource limitations**
  If multiple web applications are installed and these are assigned to different Internet Information Services application pools, these are started in separate processes.

- **Increasing performance**
  Performance can be noticeably improved by installing on several servers.

- **Redundancy**
  Multiple installation does not necessarily complete outage if just one of the installed application fails.

**Related topics**

- [Application pool on page 177](#)

# Single Sign-On

The Manager web application supports a single sign-on mechanism that enables authentication of a user without the user having to repeatedly enter their user name and password.

**Prerequisites required:**

- Disabling anonymous access
- Configuration of an authentication module capable of single sign-on
For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

- Permissions in the application owns application pool

You can disable anonymous access on the web server. This means the user’s browser must provide the data required for authentication.

**To disable the anonymous access**

1. Open the configuration of the Manager web application in the Internet Information Services and activate the configuration for **Authentication**.
2. Change the value of the status to **disabled** in **Anonymous Authentication**.

**Related topics**

- Application pool on page 177
# Appendix: Machine roles and installation packages

Table 63: Machine role and installation package options

<table>
<thead>
<tr>
<th>Machine role</th>
<th>Description of the Installation Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation</td>
<td>Contains all basic components for installing tools on an administrative workstation.</td>
</tr>
<tr>
<td>Administration</td>
<td>Contains One Identity Manager administration tools required by default users for fulfilling their task with One Identity Manager, As well as the tools, which ensure basic functionality for working with One Identity Manager, this includes the Manager as the main administration tools.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Contains all One Identity Manager tools of the default user and additional programs for configuring the system. These include, for example, Configuration Wizard, Database Compiler, Database Transporter, Crypto Configuration, Designer, Web Designer, and configuration tools for the One Identity Manager Service.</td>
</tr>
<tr>
<td>Development &amp; Testing</td>
<td>Contains the One Identity Manager tools for developing and testing custom scripts and forms, for example, the System Debugger.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Contains One Identity Manager programs for monitoring the system status, for example Job Queue Info.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Contains One Identity Manager documentation in different languages.</td>
</tr>
<tr>
<td>Server</td>
<td>Contains all the basic components for setting up a server.</td>
</tr>
<tr>
<td>Machine role</td>
<td>Description of the Installation Package</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Job server</td>
<td>Contains the One Identity Manager Service and basic processing components. Additional machine roles contain connectors for synchronizing individual target systems.</td>
</tr>
</tbody>
</table>
About us

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
A
Analyzer 13
application server 11
  install 112-113
  One Identity Manager Service 18
  One Identity Manager tools 18
search index
  update 118
search indexing service 112-113
search service 113
status display 116
system requirements 40
uninstall 118
update 117
web.config 91, 113, 117
authentication
  test 156
authentication module 153
    enable 154
authorizations 26, 41, 43
autoupdate process 88

C
cluster resource
  log file 83
  One Identity Manager Service 83
Configuration Wizard 13, 50, 53, 101, 103, 105
Crypto Configuration 13, 61
custom configuration package 100
  import 108

D
database
  configure 50, 60
custom configuration package 100
development environment 60, 169
crypt 61-65
Hotfix package 100, 106
install 50
live environment 60
log in 151
migration log 105
migration package 100
module overview 158
reference database 169
SQL Server 53, 103
staging level 60, 169
system requirements 23, 31
test environment 60, 169
transport history 105-106, 158
transport package 100
update 100-101, 103, 105-106
version 105, 158
Database Compiler 13
database server
  system requirements 22-23, 31
Database Transporter 13, 107-108
database user
  authorizations 26
SQL Server 26
default connection dialog 150
default language 155
Designer 13
Docker image 20

E
email notification 69, 164
encryption 61-66
key
change 63
create 62
generate 61
key data 61
key file 61
private key 61

F
firewall configuration 44
full text search
application server 112-113, 139
search service 112-113, 139
Web Portal 139

H
HistoryDB Manager 13
Hotfix package 100
file
backup 110
import 110
import 108
install 106
show contents 107

I
installation prerequisites 21-23, 26, 31, 37-41, 43-44
InstallState.config 85

J
Job Queue Info 13
Job server
install 47, 75-77
set up 75-77
update 88
Job Service Configuration 13

L
language
enable 156
Select in GUI 156
language setting
default language 155
login language 155
Launchpad 13
License Meter 13
login 150-151, 153
default connection dialog 150
SQL Server 151
SQL Server login 151
system user ID 153
login language 155
enable 156

M
machine role 181
Manager 13
Manager web application 13
    application directory 176
    application pool 177
    ASP.Net base settings 176
    cache directory 176
    configure 171
    database connection 172
    debugging 174
    directory 176
    file download 175
    general settings 172
    install 144
    language 172
    load balancing 175, 178
    log directory 176
    logging 174
    open 147
    performance 175
    plugins 178
    security 173
    single sign-on 179
    timeout 172
    uninstall 148
    update 147
        automatic 178
    web.config 144, 171
Manager Web Configuration Editor 171
migration package 100
monitor.config
    Web Portal 133

O
OAuth 2.0/OpenID Connect
    Web application 134
One Identity Manager
    application server 11
    architecture overview 11
    authorizations 41
    database 11
    front-end 11
    hotfix 93
    install 45
    Server Service 11
    service pack 93
    system configurations
        email notification 69, 164
    update 93
    user 41
    version change 93
    web server 11
One Identity Manager components
    install 47, 49
    update 87, 97
One Identity Manager Docker image 20
One Identity Manager schema
    install 50
One Identity Manager Service 11
    cluster resource 81, 83
    database key 66
    install 75-77
    installation prerequisites 38, 43
    key file 66
    log file 80
    private.key 66
    start 81

N
NLog.config
    Web Portal 133
notification system 69, 164
One Identity Manager tools 13
    Analyzer 13
    Configuration Wizard 13
    Crypto Configuration 13
    Database Compiler 13
    Database Transporter 13
    Designer 13
    HistoryDB Manager 13
    install 47, 49
    installation prerequisites 37
    Job Queue Info 13
    Job Service Configuration 13
    Launchpad 13
    License Meter 13
    log in 150, 153
    Manager 13
    One Identity Manager Web 13
    Operations Support Web Portal 13
    Password Reset Portal 13
    Report Editor 13
    Schema Extension 13
    Server Installer 13
    Software Loader 13
    Synchronization Editor 13
    System Debugger 13
    update 87
    Web Designer 13
    Web Installer 13
    Web Portal 13
    Operations Support Web Portal 13
    compatibility mode 165
    display 165

P
    password
        reminder notification 156
        sequence 156
    Password Reset Portal 13
    ports 44

R
    Report Editor 13

S
    Schema Extension 13
    server
        install 47, 75-77
        update 88
    Server Installer 13
    service server
        system requirements 38
    Software Loader 13, 110
    software revision 85
    software update
        automatic 85
        disable 90-91
        enable 90, 105
        file
            backup 110
            import 110
            version 110
    InstallState.config 85
    One Identity Manager Service 88
    One Identity Manager tools 87
    put into operation 90
    compatibility mode 165
server 88
softwarerevision.viv 85, 87-88
Update.exe 85, 87, 89
update.lock 85
update.log 85
Update.zip 85, 87-89
Web application 89
Web Portal 89
softwarerevision.viv 85, 87-88
SQL processing server 45
supplier notification 67
disable 68
enable 67
verify 68
Synchronization Editor 13
System Debugger 13
system requirements
application server 40
authorizations 41
database 23, 31
database server 22-23, 31
database user
SQL Server 26
One Identity Manager Service 38
One Identity Manager tools 37
service server 38
user 41
web server 39
workstation 37
system user ID
log in 153

T
transport history 158
transport package 100
import 108
show contents 107
troubleshooting 158

U
update
automatic 85
update server 45, 90
Update.exe 85, 87, 89
update.lock 85, 87
update.log 85
Update.zip 85, 87-89

W
Web application
update 89
Web Designer 13
Web Installer 13, 113, 118, 126, 132,
144, 148
Web Portal 13
application log 136
cache 139
configure 133
database connection 134
database log 136
debugger service 139
event log 136
exceptions 141
install 126
log 136
log file 141
monitor 89
monitor.config 133
NLog.config 133
OAuth 2.0/OpenID Connect 134
performance indicator 142
runtime monitoring 140
search service 139
security 141
uninstall 132
update 89, 131
  automatic 137
wait 140
web project 134
web settings 138
web.config 133
web server 11
  system requirements 39
web.config
  application server 91, 113, 117
  Manager web application 144, 171
  Web Portal 133
WebConfigEditor.exe 171
WebDesigner.ConfigFileEditor.exe 133
workstation
  install 47
  system requirements 37