

One Identity Manager 9.3

Installation Guide

Copyright 2025 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 website (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/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Installation Guide
Updated - 06 January 2025, 10:59

For the most recent documents and product information, see Online product documentation.

Contents

About this guide ... **8**

One Identity Manager overview ... **9**

One Identity Manager editions ... 9

One Identity Manager architecture ... 10

One Identity Manager tools ... 13

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

Installation prerequisites ... **20**

Supported database systems ... 21

Minimum system requirements for implementing SQL Servers as database servers ... 21

Settings for the database server and the One Identity Manager database on a SQL Server ... 23

Users and permissions 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

Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database ... 33

Requirements for Azure SQL Database as database system ... 37

Settings for the database server and the One Identity Manager database in Azure SQL Database ... 38

Users and permissions for the One Identity Manager database in Azure SQL Database ... 40

Requirements for Amazon RDS for SQL Server as database system ... 43

Minimum system requirements for administrative workstations ... 43

Minimum system requirements for Job servers ... 44

Minimum system requirements for API Servers ... 45

Minimum system requirements for application servers ... 47

Minimum system requirements for web servers ... 48

Users for One Identity Manager ... 49

Setting up permissions for creating an HTTP server ... 52

Communications ports and firewall configuration ... 52

Installing One Identity Manager ... **54**

One Identity Manager Docker images ... 55
Before you start installing One Identity Manager ... 56
Installing One Identity Manager components ... 57
Installing One Identity Manager components on a Windows terminal server ... 60
Installing and configuring a One Identity Manager database ... 61
Tips for setting up a One Identity Manager database ... 63
Installing and configuring a One Identity Manager database ... 64
Editing a One Identity Manager database during setup using the Configuration Wizard ... 70
Configuring a One Identity Manager database for testing, development, or production ... 72
Encrypting database information ... 73
Creating new database keys and encrypting database information ... 74
Changing database keys and encrypting database information ... 75
Reencrypting database information ... 76
Decrypting database information ... 77
Tips for working with an encrypted One Identity Manager database ... 78
One Identity Manager vendor notification ... 80
Enabling vendor notification ... 80
Checking vendor notification ... 81
Disabling vendor notification ... 81
Setting up the email notification system ... 82
Sending email notifications via Microsoft 365 ... 87

Installing and configuring the One Identity Manager Service ... 90
Setting up Job servers ... 91
Installing the One Identity Manager Service with the Server Installer ... 92
Displaying the One Identity Manager Service log file ... 95
Changing the user account or start type of the One Identity Manager Service ... 96
The One Identity Manager Service in a cluster ... 97
Registering the One Identity Manager Service in a cluster ... 98
Installing and configuring the One Identity Manager Service in a cluster ... 99

Automatic updating of One Identity Manager ... 101
Basics for automatic software update ... 101
Automatic updating of the One Identity Manager tools ... 103
User intervention in automatic updating of One Identity Manager tools ... 104

Automatic updating of the One Identity Manager Service ... 104
Automatic updating of web applications ... 105
Implementing the automatic software update ... 106
Disabling automatic software update ... 107

Updating One Identity Manager ... 108
The update process for releasing a new One Identity Manager version ... 109
Updating One Identity Manager components with the installation wizard ... 112
Updating the One Identity Manager database ... 114
Advice on updating the One Identity Manager database ... 115
Updating the One Identity Manager database with the Configuration Wizard ... 117
Editing the One Identity Manager database while updating with the Configuration Wizard ... 120
Installing a hotfix in the One Identity Manager database ... 122
Displaying the contents of a transport package with the Database Transporter ... 123
Importing transport packages with the Database Transporter ... 124
Importing files with the Software Loader ... 126

Installing additional modules for a existing One Identity Manager installation ... 129

Installing and updating an application server ... 131
Tips for installing an application server ... 131
Installing application servers ... 132
Displaying application servers' status ... 136
Installing or uninstalling a search service for full-text search ... 137
Updating the search index on application servers ... 138
Updating application servers ... 139
Uninstalling application servers ... 140

Installing and updating an API Server ... 142
Installing the API Server ... 143
Displaying an overview of HTML web applications ... 149
API Servers for configuring load balancing ... 149
Installing or uninstalling the SCIM plugin ... 150
Modifying authentication data for API Server projects ... 151
Adjusting IIS request limits for the API Server ... 153
Updating API Servers ... 154

Uninstalling API Server ... 156

Installing and updating the Manager web application ... 157

Installing the Manager web application ... 157

Displaying the Manager web application ... 161

Manager web application update ... 161

Uninstalling Manager web applications ... 162

Logging in to One Identity Manager tools ... 163

Setting up new logins via the application server ... 164

Setting up new logins via direct connection to the database ... 166

Selecting and editing existing login connections ... 167

Enabling additional authentication modules ... 168

Language settings in One Identity Manager ... 169

Enabling other login languages ... 169

Password expiry ... 170

Checking authentication ... 170

Connection pool for separate sessions for reading and writing on different database servers ... 171

Troubleshooting ... 172

Displaying the transport history and testing the One Identity Manager version ... 172

Error messages logging in to One Identity Manager tools ... 173

Error messages when installing and updating the One Identity Manager database ... 174

Database errors migrating a database to SQL Server AlwaysOn availability groups ... 176

Error messages when generating email notifications ... 177

Removing unnecessary modules from the One Identity Manager database ... 178

Deleting One Identity Manager databases ... 179

Log message for search index creation ... 180

Appendix: Advanced configuration of the Manager web application ... 181

Customizing the Manager web application configuration ... 181

Configuration settings for the Manager web application ... 182

Load balancing of the Manager web application ... 186

Manager web application single sign-on ... 187

Appendix: Machine roles and installation packages ... 188

Appendix: Configuration parameters for the email notification system ... 190

Appendix: How to configure the One Identity Manager database using SQL Server AlwaysOn availability groups **196**

About us **199**

Contacting us 199

Technical support resources 199

Index **200**

1

About this guide

The *One Identity Manager Installation Guide* describes the installation and initial going live of One Identity Manager. This shows you 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 One Identity Manager documentation in the Manager and in the Designer by selecting the **Help** > **Search** menu item. The online version of One Identity Manager documentation is available in the Support portal under Technical Documentation. You will find videos with additional information at 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 while the IT team focuses on their core competencies.

With this product, you can:

- 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 Starling

Initiate your subscription within your One Identity on-prem product and join your on-prem solutions to our One Identity Starling cloud platform. Giving your organization immediate access to a number of cloud-delivered microservices, which expand the capabilities of your One Identity on-prem solutions. We will continuously make available new products and features to One Identity Starling. For a free trial of our One Identity Starling offerings and to get the latest product feature updates, visit cloud.oneidentity.com.

One Identity Manager editions

One Identity Manager is available in the following editions.

One Identity Manager

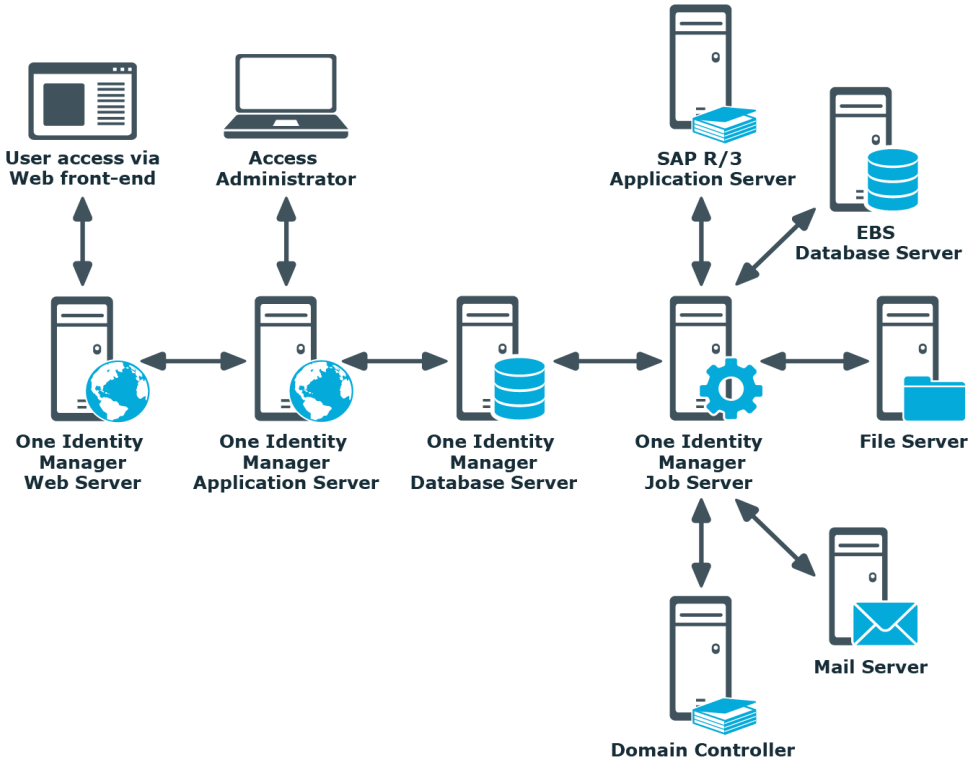
This edition contains all management modules (IT Shop & workflow, delegation, management of system roles and business roles, role mining, risk assessment, attestation, compliance, company policies, report subscriptions), as well as Unified Namespace and connectors for Active Directory.

One Identity Manager Data Governance Edition

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.

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 core of One Identity Manager. 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. For data management, the database maps managed target systems and ERP structures as well as 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 identities, user accounts, groups, memberships, operating data, approval workflows, attestation, recertification, and compliance rules.

The metadata 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 run by the object layer.

An SQL Server, a managed instance in Azure SQL Database, Azure SQL Database, or Amazon RDS for SQL Server can be used as the database system.

Server service

One Identity Manager uses 'processes' for mapping business processes. A process consists of process steps that represent processing tasks and are joined by predecessor/successor relations. This functionality allows flexibility when linking actions and sequences to 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 throughout the network of information that is administrated in the One Identity Manager database. The One Identity Manager Service performs data synchronization between the database and any connected target systems and runs actions at the database and file level. The service must be installed on the One Identity Manager network server to run the processes. A server running the One Identity Manager Service is called the Job server. The Job server must be declared in the One Identity Manager database.

The One Identity Manager Service retrieves process steps from the Job queue. Process steps are run 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 performance of the process steps and determines how processing should continue depending on the results of the run 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 retaining the object layer themselves and accessing the database layer directly. In this case, only the part of the object layer that is required for the acquisition process is mapped in the clients.

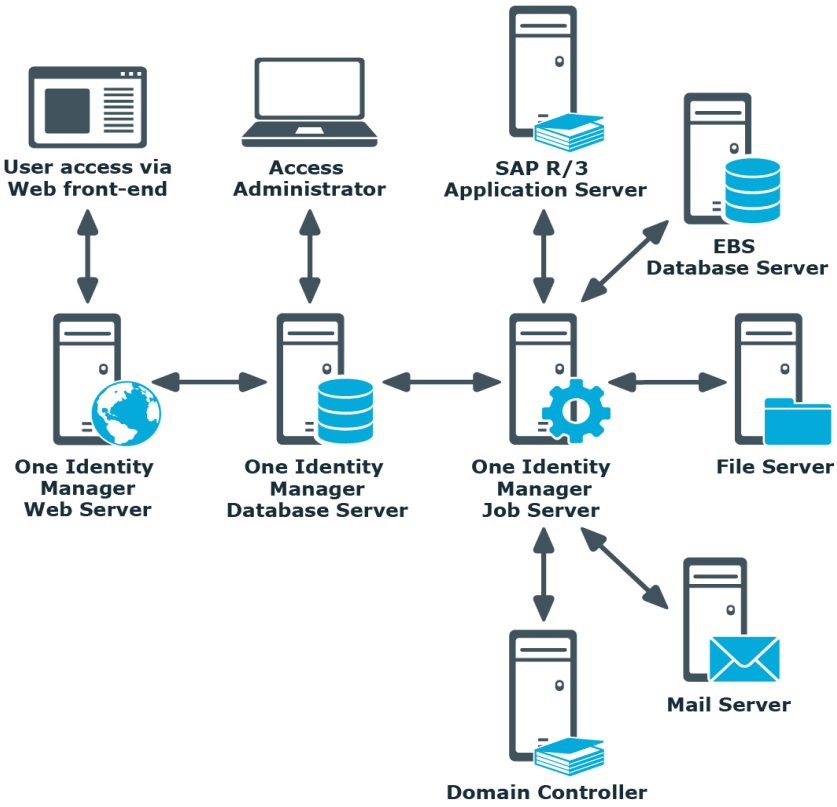
Web server

To implement browser-based user interfaces, there is an application running on a web server that is based on a website render engine. Users use a web browser to access the website that has been dynamically set up and customized for them. Data exchange between database and web server can take place either directly or through the application server.

Front-ends

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

Figure 2: Overview of One Identity Manager components 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 manage identities differs from the configuration tool. The content displayed and its editability are dependent on the permissions of the logged in user.

Table 1: Overview of One Identity Manager tools

Tool	Short description
Launchpad	The Launchpad is the central tool for starting One Identity Manager administration tools and configuration tools. You can use the Launchpad to check the existing One Identity Manager installation and start One Identity Manager tools to run individual tasks. The Launchpad can be customized. In the Designer, you can define your own menu items and actions for the Launchpad.
Web Portal	The Web Portal is a web-based application for all One Identity Manager users. The Web Portal provides stringent workflows for the following actions: • Changing your own main data and password. • Editing or entering identity main data of direct reports. • Searching, requesting, canceling, or renewing products in the IT Shop. • Delegating own roles. • Editing assigned approvals, attestation cases, and rule violations. In the information system, you may see several evaluations, for example, about your own requests and attestation cases, employee numbers, approvals, rule violations, or the Unified Namespace. The Web Portal is made available over the API Server. Through a web browser, users can access the website that has been dynamically set up and customized for

Tool	Short description
	them.
Password Reset Portal	The Password Reset Portal allows users to securely reset passwords of the user accounts they manage. The Password Reset Portal is made available over the API Server. The necessary security is guaranteed by multi-factor authentication.
Operations Support Web Portal	The Operations Support Web Portal helps you to manage and use your web applications. You can use the Operations Support Web Portal to monitor the handling of processes and DBQueue tasks. You can also create passcodes for your colleagues. The Operations Support Web Portal is made available over the API Server.
Manager	The Manager is the main administration tool for setting up all identity data. It displays and maintains all the data required for the administration of identities, their user accounts, permissions, and company-specific roles in a One Identity Manager network. Company resources required to carry out tasks can be configured and assigned to identities. You can also use the 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 identities or roles and their assignments. By implementing One Identity Manager application roles, every One Identity Manager user obtains only those permissions they require to fulfill necessary administrative duties. Manager functionality can be provided by web applications.
Synchronization Editor	You use the Synchronization Editor to connect different target systems to One Identity Manager. Use this tool to configure data synchronization for any target system and specify which target system data is

Tool	Short description
	mapped to the One Identity Manager database. You also define the object properties mapping and the synchronization sequence as a workflow.
Analyzer	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.
Job Queue Info	The Job Queue Info helps you 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.
Configuration Wizard	The Configuration Wizard is used to set up the database for use in a One Identity Manager network. All the Configuration Wizard schema tables, data types, and database procedures are loaded into the database with the One Identity Manager. SQL logins and database users are created with permissions for the One Identity Manager schema. Automatic version control is integrated into One Identity Manager, ensuring that One Identity Manager components are always consistent with each other and with the database. If program updates are implemented that change the structure (for example, table extensions), database migration is then necessary. The Configuration Wizard runs this schema installation depending on the current status of the schema.
Designer	The Designer is the main tool for configuring 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. You use the Designer to specify permissions for the different administrative tasks of individual users and user groups. Another important task is the definition of workflows for technically illustrating the administration procedures in a company. The Designer provides various editors for

Tool	Short description
	the One Identity Manager system configuration. The range of functions and the operating methods of the editors are tailored to the differing configuration requirements.
Data Import	With the Data Import program, One Identity Manager offers a simple way to import 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.
Crypto Configuration	In certain circumstances it is necessary store encrypted information in the database. Use the Crypto Configuration program to carry out encryption. This program creates a code file and converts the contents of the affected database column. The coded information is stored in the database.
Database Compiler	You must compile the One Identity Manager database after making changes to configuration data. After a migration package or full custom configuration package is imported, database compiling begins immediately from the Configuration Wizard or Database Transporter. The Database Compiler compiles the One Identity Manager database after you import hotfixes or when changes have been made to processes, scripts, formatting rules, object definitions, task definitions, or preprocessor-relevant configuration parameters.
Report Editor	With the Report Editor, you can group One Identity Manager object data together into reports. You can group, accumulate, and graphically represent this data. Predefined reports are supplied though migration but you can also create your own reports with the Report Editor.
Schema Extension	The Schema Extension is implemented to extend the One Identity Manager schema by custom tables and columns. Using the object technology in

Tool	Short description
	One Identity Manager, you can customize the application data model at database level so that the extensions are available with full functionality at object level.
System Debugger	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.
Database Transporter	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).
Job Service Configuration	Use the Job Service Configuration to create and customize the configuration file for the One Identity Manager Service. The One Identity Manager Service and its plug-ins 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.
License Meter	Using the License Meter, you can track and maintain the licenses in your One Identity Manager database. The wizard creates a report with license-relevant information.
Software Loader	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.
Server Installer	Use the Server Installer to install and configure the One Identity Manager Service. Use the Server Installer to install the One Identity Manager Service locally or remotely.
API Server	The API Server deploys the Web Portal, the Password Reset Portal, the Administration Portal as well as the Operations Support Web Portal and your HTML5 web applications. It also provides an API.

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 shows you which One Identity Manager components work against an application server. Some front-ends have only limited functionality to work with an application server.

Table 2: One Identity Manager components and application servers

Component	Connection through application server?	Restrictions
Launchpad	Yes	Certain application, which you can start from the Launchpad, require a direct connection to the database.
Web Portal	Yes	
Password Reset Portal	Yes	
Operations Support Web Portal	Yes	
Manager	Yes	The consistency check is not supported. Some forms are not supported.
Manager web application	Yes	Some forms are not supported.
Synchronization Editor	Yes	
Analyzer	Yes	
Job Queue Info	No	
Configuration Wizard	No	
Designer	Yes	The consistency check is not supported. Process simulation is not supported. Database compilation is not supported.

Component	Connection through application server?	Restrictions
Data Import	Yes	
Crypto Configuration	No	
Database Compiler	No	
Report Editor	Yes	SQL query testing is not supported.
Schema Extension	No	
System Debugger	No	
Database Transporter	No	
License Meter	Yes	
Software Loader	Yes	
One Identity Manager Service	Yes	
Server Installer	Yes	
API Server	Yes	
Database Agent Service	No	

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 strong 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

- Supported database systems on page 21
- Minimum system requirements for implementing SQL Servers as database servers on page 21
- Requirements for a managed instance in Azure SQL Database on page 30
- Requirements for Azure SQL Database as database system on page 37
- Requirements for Amazon RDS for SQL Server as database system on page 43
- Minimum system requirements for administrative workstations on page 43
- Minimum system requirements for Job servers on page 44
- Minimum system requirements for API Servers on page 45
- Minimum system requirements for application servers on page 47
- Minimum system requirements for web servers on page 48
- Users for One Identity Manager on page 49

- Users and permissions for the One Identity Manager database on an SQL Server on page 26
- Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33
- Users and permissions for the One Identity Manager database in Azure SQL Database on page 40
- Setting up permissions for creating an HTTP server on page 52
- Communications ports and firewall configuration on page 52

Supported database systems

One Identity Manager supports the following database systems:

- SQL Server
- Managed instances in the Azure SQL Database
- Azure SQL Database
- Amazon RDS for SQL Server

Detailed information about this topic

- Minimum system requirements for implementing SQL Servers as database servers on page 21
- Requirements for a managed instance in Azure SQL Database on page 30
- Requirements for Azure SQL Database as database system on page 37
- Requirements for Amazon RDS for SQL Server as database system on page 43

Minimum system requirements for implementing SQL Servers as database servers

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 3: Minimum system requirements for SQL Servers

Requirement	Detail
Processor	8 physical cores with 2.5 GHz+ frequency (non-production) 16 physical cores with 2.5 GHz+ frequency (production) NOTE: 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM (non-production) 64 GB+ RAM (production)
Hard drive storage	100 GB
Operating system	Windows operating systems • Note the requirements of Microsoft for the version of SQL Server you are using. UNIX and Linux operating systems • Note the operating system manufacturer's minimum requirements for SQL Server databases.
Software	Following versions are supported: • SQL Server 2022 Standard Edition (64-bit) with the current cumulative update NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems. NOTE: Ledger is not supported. For more information, see the Knowledge Base. • SQL Server Management Studio (recommended)

NOTE: The minimum requirements listed above are considered to be for general use. With each custom One Identity Manager deployment these values may need to be increased to provide ideal performance. To determine production hardware requirements, it is strongly recommended to consult a qualified One Identity Partner or the One Identity Professional Services team. Failure to do so may result in poor database performance.

For additional hardware recommendations, read the KB article https://support.oneidentity.com/identity-manager/kb/290330/how-to-configure-settings-as-per-the-system-information-overview, which describes the overview of the system information available in One Identity Manager.

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

- Settings for the database server and the One Identity Manager database on a SQL Server on page 23
- Users and permissions for the One Identity Manager database on an SQL Server on page 26

Settings for the database server and the One Identity Manager database on a SQL Server

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

Table 4: Database server settings

Property	Value	Comment
Language	English	Select **English** as the default language for database users.
Server Collation	Case insensitive SQL_Latin1_General_CP1_CI_AS (recommended)	
Extreme transaction processing supported (Is XTP supported)	True	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 default 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 does not start.

Table 5: Database settings

Property	Value	Comment
Collation	SQL_Latin1_General_	The setting is checked by the

Property	Value	Comment
	CP1_CI_AS	Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Recovery model	Simple	The setting is tested by the Configuration Wizard before installing or updating One Identity Manager database. If the recovery model is not set to the value **`Simple`**, a warning is issued before installing or updating starts. You can ignore this warning. For performance reasons, however, it is recommended you set the database to the **`Simple`** recovery model for the duration of the schema installation or update.
Compatibility level	SQL Server 2022 (160)	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Create Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics Asynchronously	False	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Arithmetic Abort enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Quoted Identifiers	True	The setting is checked by the

Property	Value	Comment
Enabled		Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Is Read Committed Snapshot On	True	The default setting for transactions is **AutoCommit**. 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.
Parameterization	Forced	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
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 **Filestream data** file type 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 the 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

Property	Value	Comment
		directory of the data file (`*.mdf`).
Table variable deferred compilation (DEFERRED_ COMPILATION_ TV)	ON	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Interleaved execution (INTERLEAVED_ EXECUTION_TVF)	ON	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.

For more information about the named database server properties, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/view-or-change-server-properties-sql-server.

For more information about the database properties, see https://docs.microsoft.com/en-us/sql/relational-databases/databases/view-or-change-the-properties-of-a-database and https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-databases-transact-sql.

Related topics

- Minimum system requirements for implementing SQL Servers as database servers on page 21
- Users and permissions for the One Identity Manager database on an SQL Server on page 26
- Error messages when installing and updating the One Identity Manager database on page 174

Users and permissions 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 required for the initial setup 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 8.0.x to 9.3, you will also require an installation user.

- Administrative user

  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.

- Configuration user

  The configuration user can run 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 users

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

For more information about minimum access levels for One Identity Manager tools, see the *One Identity Manager Authorization and Authentication Guide*.

Permissions for installation users

An SQL 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 the **sysadmin** server role

  This server role is only required if the database is created by the Configuration Wizard and the directories for the file must be selected in the file browser. If the files are stored in the default database server directories, permissions are not necessary.

- Member of **securityadmin** server role

  This server role is required to create SQL logins.

- **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.

  The permissions are required to check connections and close these if necessary.

- **alter any server role** permissions

  The permissions are required to create the server role for the administrative user.

msdb database:

- **alter any user** permissions

  The permissions are required to create the necessary database users for the administrative user.

- **alter any role** permissions

  This permission is required to create the necessary database role for the administrative user.

master database:

- **alter any user** permissions

  The permissions are required to create the necessary database users for the administrative user.

- **alter any role** permissions

  This permission is required to create the necessary database role for the administrative user.

- **Run** permissions with the **with grant option** option for the `xp_readerrorlog` procedure

  The permissions are 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 required for installing the schema with the Configuration Wizard in an existing database or for updating the schema.

Permissions for administrative users

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

SQL Server:

- **OneIMAdminRole_<DatabaseName>** server role
  - **alter any server role** permissions

    The permissions are required to create the server role for the configuration user.

  - **view any definition** permissions

    The permissions are required to link the SQL logins for the configuration user and the end user with the corresponding database users.
- **<DatabaseName>_Admin** SQL login

        - Member of the **OneIMAdminRole_<DatabaseName>** server role
        - **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.

          The permissions are required to check connections and close these if necessary.

master database:

- **OneIMRole_<DatabaseName>** database role
    - **Run** permissions for the `xp_readerrorlog` procedure

      The permissions are 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 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 login.

Permissions for configuration users

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

SQL Server:

- **OneIMConfigRole_<DatabaseName>** server role
    - **view server state** and **alter any connection** permissions

      The 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**, **Run**, and **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 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**, and **Delete** permissions for selected tables in the database
  - **View Definition** permissions for the database
  - **Run** and **References** permissions for individual functions, procedures, and types
- **User** database user
  - Member of the **OneIMUserRoleDB** database role
  - The database user is connected with the **<DatabaseName>_User** 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 login.

To implement Windows authentication

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

Requirements for a managed instance in Azure SQL Database

For more information about Azure SQL Database, refer to the Microsoft website under https://azure.microsoft.com/en-us/products/azure-sql/database/.

The following requirements and limitations apply to the use of a managed instance in Azure SQL Database as a database system.

- The **Business Critical** tier is required.
- Ledger is not supported. For more information, see the Knowledge Base.

Related topics

- Database server settings and the One Identity Manager database in a managed instance in an Azure SQL Database on page 31
- Users and permissions for the One Identity Manager database in a manage instance in 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 6: Database server settings

Property	Value	Comment
Language	English	Select `English` as the default language for database users.
Server Collation	Case insensitive SQL_Latin1_General_CP1_CI_AS (recommended)	
Extreme transaction processing supported (Is XTP supported)	True	Default setting.

Table 7: Database settings

Property	Value	Comment
Collation	SQL_Latin1_General_CP1_CI_AS	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.

Property	Value	Comment
Recovery model	Full	Default setting.
Compatibility level	SQL Server 2022 (160)	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Create Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics Asynchronously	False	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Arithmetic Abort enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Quoted Identifiers Enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Is Read Committed Snapshot On	True	The default setting for transactions is **`AutoCommit`**. 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

Property	Value	Comment
		Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Parameterization	Forced	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Database file and date file group for memory-optimized tables	Required	Default setting.
Table variable deferred compilation (DEFERRED_COMPILATION_TV)	ON	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Interleaved execution (INTERLEAVED_EXECUTION_TVF)	ON	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.

Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database

The following users are identified for using a One Identity Manager database in a managed instance in 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 required for the initial setup of a One Identity Manager database using the Configuration Wizard.

- Administrative user

  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.

- Configuration user

  The configuration user can run 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 users

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

For more information about minimum access levels for One Identity Manager tools, see the *One Identity Manager Authorization and Authentication Guide*.

Permissions for installation users

The server administrator set up when Azure SQL was deployed has the administrative permissions to directly install and use a One Identity Manager database. Likewise, the granulated permissions concept can be enabled by this user.

If this user cannot be used, an SQL login and database user must be provided with the following permissions.

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 SQL logins.

- **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.

  The permissions are required to check connections and close these if necessary.

- **alter any server role** permissions

  The permissions are required to create the server role for the administrative user.

msdb database:

- **alter any user** permissions

  The permissions are required to create the necessary database users for the administrative user.

- **alter any role** permissions

  This permission is required to create the necessary database role for the administrative user.

master database:

- **alter any user** permissions

  The permissions are required to create the necessary database users for the administrative user.

- **alter any role** permissions

  This permission is required to create the necessary database role for the administrative user.

- **Run** permissions with the **with grant option** option for the `xp_readerrorlog` procedure

  The permissions are 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 required for installing the schema with the Configuration Wizard in an existing database or for updating the schema.

Permissions for administrative users

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

SQL Server:

- **OneIMAdminRole_<DatabaseName>** server role
  - **alter any server role** permissions

    The permissions are required to create the server role for the configuration user.
  - **view any definition** permissions

    The permissions are required to link the SQL logins for the configuration user and the end user with the corresponding database users.
- **<DatabaseName>_Admin** SQL login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.

    The permissions are required to check connections and close these if necessary.

master database:

- **OneIMRole_<DatabaseName>** database role
  - **Run** permissions for the `xp_readerrorlog` procedure

    The permissions are 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 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 login.

Permissions for configuration users

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

SQL Server:

- **OneIMConfigRole_<DatabaseName>** server role
  - **view server state** and **alter any connection** permissions

    The 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**, **Run**, and **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 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**, and **Delete** permissions for selected tables in the database
  - **View Definition** permissions for the database
  - **Run** and **References** permissions for individual functions, procedures, and types
- **User** database user
  - Member of the **OneIMUserRoleDB** database role
  - The database user is connected with the **<DatabaseName>_User** login.

Requirements for Azure SQL Database as database system

For more information about Azure SQL Database, refer to the Microsoft website under https://azure.microsoft.com/en-us/products/azure-sql/database/.

The following requirements and limitations apply to the use of Azure SQL Database as a database system.

- If you use Azure SQL Database as the database system, you must supply a database. There is no support for creating a new database in Azure SQL Database with the Configuration Wizard.
- `use` statements are not supported.
- Strong passwords must be used for the SQL login.

  For more information, see under Strong Passwords in the Microsoft documentation.
- Ledger is not supported. For more information, see the Knowledge Base.

Related topics

- Settings for the database server and the One Identity Manager database in Azure SQL Database on page 38
- Users and permissions for the One Identity Manager database in Azure SQL Database on page 40

Settings for the database server and the One Identity Manager database in 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

Property	Value	Comment
Language	English	Select **English** as the default language for database users.
Server Collation	Case insensitive SQL_Latin1_General_CP1_CI_AS (recommended)	
Extreme transaction processing supported (Is XTP supported)	True	Default setting.

Table 9: Database settings

Property	Value	Comment
Collation	SQL_Latin1_General_CP1_CI_AS	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Recovery model	Full	Default setting.
Compatibility level	SQL Server 2022 (160)	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Create Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics	True	The setting is checked by the Configuration Wizard before installing or

Property	Value	Comment
		updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics Asynchronously	False	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Arithmetic Abort enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Quoted Identifiers Enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Is Read Committed Snapshot On	True	The default setting for transactions is **`AutoCommit`**. 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.
Parameterization	Forced	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Database file and date file group for memory-optimized tables	Required	Default setting.

Property	Value	Comment
Table variable deferred compilation (DEFERRED_ COMPILATION_ TV)	ON	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Interleaved execution (INTERLEAVED_ EXECUTION_TVF)	ON	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.

Users and permissions for the One Identity Manager database in Azure SQL Database

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

- Installation user

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

- Administrative user

  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.

- Configuration user

  The configuration user can run 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 users

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

For more information about minimum access levels for One Identity Manager tools, see the *One Identity Manager Authorization and Authentication Guide*.

Permissions for installation users

The server administrator set up when Azure SQL was deployed has the administrative permissions to directly install and use a One Identity Manager database. Likewise, the granulated permissions concept can be enabled by this user.

If this user cannot be used, an SQL login and database user must be provided with the following permissions.

master database:

- Member of the **loginmanager** database role

  The permissions are required to create the necessary database users for the administrative user.

One Identity Manager database:

- Member of the **db_owner** database role

  This database role is required for installing the schema with the Configuration Wizard in an existing database or for updating the schema.

Permissions for administrative users

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

SQL Server:

- **OneIMAdminRole_<DatabaseName>** server role
  - **alter any server role** permissions

    The permissions are required to create the server role for the configuration user.
  - **view any definition** permissions

    The permissions are required to link the SQL logins for the configuration user and the end user with the corresponding database users.
- **<DatabaseName>_Admin** SQL login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.

    The permissions are required to check connections and close these if necessary.

master database:

- **OneIMRole_<DatabaseName>** database role
  - **Run** permissions for the `xp_readerrorlog` procedure

    The permissions are 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 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 login.

Permissions for configuration users

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

SQL Server:

- **OneIMConfigRole_<DatabaseName>** server role
  - **view server state** and **alter any connection** permissions

    The 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**, **Run**, and **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 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**, and **Delete** permissions for selected tables in the database
  - **View Definition** permissions for the database
  - **Run** and **References** permissions for individual functions, procedures, and types
- **User** database user
  - Member of the **OneIMUserRoleDB** database role
  - The database user is connected with the **<DatabaseName>_User** login.

Requirements for Amazon RDS for SQL Server as database system

The following requirements and limitations apply to the use of Amazon RDS for SQL Server as a database system.

- If you use Amazon RDS for SQL Server as the database system, you must supply a database. There is no support for creating a new database in Amazon RDS for SQL Server with the Configuration Wizard.
- The granular permissions concept is not supported.

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.

A minimum of the following system prerequisites must be fulfilled before installing the One Identity Manager components on an administrative workstation.

Table 10: Minimum system requirements for administrative workstations

Requirement	Detail
Processor	4 physical cores 2 GHz+
Memory	4 GB+ RAM
Hard drive storage	5 GB
Operating system	Windows operating systems Following versions are supported: • Windows 11 (x64) • Windows 10 (32-bit or 64-bit) at least version 1511
Additional software	• .NET 8.0 SDK with the current service pack • Microsoft Edge WebView2
Supported browsers	• Firefox (release channel) • Chrome (release channel) • Microsoft Edge (release channel)

Minimum system requirements for Job servers

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

You install the One Identity Manager Service on a server. A server running the One Identity Manager Service is subsequently called the Job server.

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

Table 11: Minimum system requirements for Job servers

Requirement	Detail
Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating	Windows operating systems

Requirement	Detail
system	The following versions are supported: • Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems • .NET 8 Desktop Runtime NOTE: When connecting the target system, refer to the target system manufacturer's recommendations. Linux operating systems • .NET 8 Runtime NOTE: It is recommended to use .Net container images.

Related topics

- Users for One Identity Manager on page 49

Minimum system requirements for API Servers

The API Server deploys the Web Portal, the Password Reset Portal, the Administration Portal as well as the Operations Support Web Portal and your HTML5 web applications. It also provides an API.

A minimum of the following system prerequisites must be fulfilled to install an API Server server.

Table 12: Minimum system requirements for API Servers

Requirement	Detail
Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems The following versions are supported: • Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Docker images for Linux distributions supported by the .NET project

Additional software	Windows operating systems
	• ASP.NET Core Windows Hosting Bundle
	• Microsoft Internet Information Services 10 or 8.5, or 8 with the role services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • 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

Requirement	Detail
	• ASP.NET Core Runtime NOTE: It is recommended to use .Net container images. • ASP.NET Core Hosting process manager, deployed via Docker container

Minimum system requirements for application servers

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

Table 13: Minimum system requirements for application servers

Requirement	Detail
Processor	8 physical cores 2.5 GHz+
Memory	8 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems The following versions are supported: • Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Docker images for Linux distributions supported by the .NET project
Additional software	Windows operating systems • ASP.NET Core Windows Hosting Bundle • Microsoft Internet Information Services 10 or 8.5, or 8 with the role services:

Requirement	Detail
	• Web Server > Common HTTP Features > Static Content • Web Server > Common HTTP Features > Default Document • 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 • ASP.NET Core Runtime NOTE: It is recommended to use .Net container images. • ASP.NET Core Hosting process manager, deployed via Docker container

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.

Minimum system requirements for web servers

Manager functionality can be provided by web applications. A minimum of the following system prerequisites must be fulfilled to install a web server.

Table 14: Minimum system requirements for web servers

Requirement	Detail
Processor	4 physical cores 1.65 GHz+
Memory	4 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems The following versions are supported:

Requirement	Detail
	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Linux operating systems • Docker images for Linux distributions supported by the .NET project

Additional software	Windows operating systems
	• ASP.NET Core Windows Hosting Bundle
	• Microsoft Internet Information Services 10 or 8.5, or 8 with the role services:
	  • Web Server > Common HTTP Features > Static Content
	  • Web Server > Common HTTP Features > Default Document
	  • 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
	• ASP.NET Core Runtime
	  NOTE: It is recommended to use .Net container images.
	• ASP.NET Core Hosting process manager, deployed via Docker container

Users for One Identity Manager

The following users are required for start-up and normal operations of One Identity Manager. You can provide additional users whose permissions are tailored to their tasks and functions.

Table 15: Users for One Identity Manager

User	Permissions
User for installing One Identity Manager	The installation user is needed for the initial installation of a One Identity Manager database using the Configuration Wizard. For more information, see Users and permissions for the One Identity Manager database on an SQL Server on page 26, Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33, and Users and permissions for the One Identity Manager database in Azure SQL Database on page 40.
User for administrative tasks in One Identity Manager	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 more information, see Users and permissions for the One Identity Manager database on an SQL Server on page 26, Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33, and Users and permissions for the One Identity Manager database in Azure SQL Database on page 40.
User for configuration tasks in One Identity Manager	The configuration user can run 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 more information, see Users and permissions for the One Identity Manager database on an SQL Server on page 26, Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33, and Users and permissions for the One Identity Manager database in Azure SQL Database on page 40.
End user for One Identity Manager	End users are only assigned permissions at database level in order, for example, to complete tasks with the Manager or the Web Portal. For more information, see Users and permissions for the One Identity Manager database on an SQL Server on page 26, Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33, and Users and permissions for the One Identity Manager database in Azure SQL Database on page 40.

User	Permissions
User for Logging into One Identity Manager	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 permissions groups. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
User account for the One Identity Manager Service	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding 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 permissions. The user account requires permissions for the internal web service. NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions 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 One Identity Manager. In the default installation, 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 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 52.

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 run 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's user account (**NT Authority\NetworkService**), explicit permissions for the internal web service must be granted. This can be run 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 run 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 16: Communications port

Default port	Description
1433	Port for communicating with the One Identity Manager database.
80	Port for accessing web applications.
88	Kerberos authentication system (if Kerberos authentication is implemented).
135	Microsoft End Point Mapper (EPMAP) (also, DCE/RPC Locator Service).
137	NetBIOS Name Service.
139	NetBIOS Session Service.

Default port	Description
443	Default port for HTTPS connections.
1880	Port for the HTTP protocol of One Identity Manager Service.
2880	Port for access tests with the Synchronization Editor, such as in the target system browser or for simulating synchronization. Default port for the `RemoteConnectPlugin`.

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

Installing One Identity Manager

The following steps are required to install One Identity Manager:

1. Install One Identity Manager tools on the administrative workstation on which the One Identity Manager database schema installation will be started.
2. Install and configure the One Identity Manager database with the Configuration Wizard.
3. Set up the server, which handles the SQL processes.
    - The server must be entered in the database as a Job server with the **SQL processing server** server function.
    - 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. Set up an update server for automatic software updating of other servers.
    - 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 One Identity Manager database must be installed and configured on the server.
5. Setting up and configuring the Database Agent Service

    The Database Agent Service controls processing of DBQueue Processor tasks. The Database Agent Service is deployed through the One Identity Manager Service plugin. Alternatively, the Database Agent Service can be run from the `DatabaseAgentServiceCmd.exe` command line program.

NOTE: You can proceed with setting up an SQL processing server and the update server using the Configuration Wizard. You can also set up the Database Agent Service with the Configuration Wizard.

You can also install the following:

- Additional workstations.
- Additional servers with the One Identity Manager Service.
- An application server.

- An API Server with HTML web applications.
- The Password Reset Portal on a web server.

  For more information about installing and configuring the Password Reset Portal, see the *One Identity Manager Web Application Configuration Guide*.
- The Manager web application on a web server

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

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

NOTE: One Identity provides various Docker images for simple and standardized installation and running of individual Docker components in One Identity Manager containers.

Detailed information about this topic

- One Identity Manager Docker images on page 55
- Before you start installing One Identity Manager on page 56
- Installing One Identity Manager components on page 57
- Installing and configuring a One Identity Manager database on page 61
- Installing and configuring the One Identity Manager Service on page 90
- Installing application servers on page 132
- Installing and updating the Manager web application on page 157
- Updating One Identity Manager on page 108

One Identity Manager Docker images

One Identity provides various Docker images for simple and standardized installation and running of individual One Identity Manager components in Docker containers. You can find One Identity Manager Docker images, together with detailed information about the usage and configuration of the individual images under https://hub.docker.com/u/oneidentity/. For videos with additional information, see the One Identity Manager Containerization video series at www.YouTube.com/OneIdentity. For more information about Docker, see https://www.docker.com/.

Table 17: Available One Identity Manager Docker images

Docker image	Description
oneidentity/oneim-job	This image runs 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 secret values and environment variables.
oneidentity/oneim-appserver	This image runs 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 secret values and environment variables.
oneidentity/oneim-installer	This image contains a simple installation program that can be used in derived images to create the file structure for One Identity Manager applications.
oneidentity/oneim-api	This image runs an instance of the API Server. When started, it downloads the necessary files from the configured One Identity Manager database. This behavior can be controlled using secret values and environment variables.
oneidentity/oneim-dbagent	This image runs an instance of the Database Agent Service. The necessary files are download when it starts. This behavior can be controlled using secret values and environment variables.

There are additional examples of Docker files under https://github.com/OneIdentity in the Docker Files Repository. You can use the examples to create your own Docker container images based on One Identity Manager Docker images.

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 program and service components otherwise installation cannot begin.

Detailed information about this topic

- Installation prerequisites on page 20
- Installing One Identity Manager on page 54
- Updating One Identity Manager on page 108

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.

NOTE: On Linux operating systems, use of oneidentity/oneim-installer docker images is recommended.

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 and select an edition.
3. Click **Install**.

   This starts the installation wizard.
4. Select the language for the installation wizard on the start page and click **Next**.
5. Confirm the conditions of the license.
6. 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.
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.
   - Select the connection in **Select a database connection**.

     - OR -

- Click **Add new connection**, select the **SQL Server** system type, and enter the connection data.
  - **Server**: Database server.
  - **Windows authentication**: (Optional) Specifies whether the 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**: User's SQL login name.
  - **Password**: Password for the SQL user's login.
  - **Database**: List of possible databases on the database server. Select the database.
  - **Encrypt communication**: Specifies whether encryption is required for exchanging data between the client and server. Select the minimum encryption level. The encryption level that is actually used depends on the database server configuration. For more information, see the documentation from Microsoft.

    Permitted values are:
    - `Optional`: Communication is not encrypted.
    - `Mandatory`: Data exchange is encrypted. The **Trust server certificate** option, allows you to also specify whether to verify the server certificate.
    - `Strict (SQL Server 2022 and Azure SQL)`: The data exchange is encrypted. The server certificate is always verified.
  - **Trust server certificate**: If this option is enabled, the data exchange between the client and server is encrypted. However, the server certificate is not verified.

8. 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**.

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

   NOTE: When you select the machine role, all machine subroles are selected as well. You can deselect individual packages.

   You can select the following machine roles.
   - **Workstation**: Contains all basic components for installing tools on an administrative workstation.
   - **Workstation | Administration**: Contains administration tools required by default users for fulfilling their tasks with One Identity Manager. In addition to the tools that ensure basic functionality for working with One Identity Manager, the administration machine role includes the Manager as a main administration tool.

- **Workstation | Configuration**: Contains all tools for the default user and additional programs required to configure the system. These include, for example, the Configuration Wizard, Database Compiler, Database Transporter, Designer, and configuration tools for the One Identity Manager Service.
- **Workstation | Command line administration tools**: Contains various command line programs.
- **Workstation | Development and Testing**: Contains the tools to develop and test custom scripts, such as the System Debugger.
- **Workstation | Monitoring**: Contains programs for monitoring the system status, such as the Job Queue Info.
- **Server**: Contains all the basic components for setting up a server.
- **Server | Job Server**: Contains the One Identity Manager Service and basic processing components. Additional machine roles contain connectors for synchronizing individual target systems.
- **Server | Job Server | Configuration tool**: Contain configuration tool for the One Identity Manager Service.
- **Database Agent**: Contains the `DatabaseAgentServiceCmd.exe` program for running the Database Agent Service from the command line.
- **Documentation**: Contains One Identity Manager documentation in different languages.

10. On the **Install WebView2** page you are prompted to install Microsoft Edge WebView2. The user interface of some One Identity Manager components requires Microsoft Edge WebView2 to display certain content.

    NOTE: This page is only shown if you want to install One Identity Manager components that are expecting WebView2 and WebView2 is not yet installed.

11. 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 **Server | Job Server** machine role.

12. You can start different programs for further installation on the last page of the install wizard.
    - To install the One Identity Manager schema, start the Configuration Wizard and follow the Configuration Wizard instructions.

      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 Job Service Configuration program.

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

13. Click **Finish** to close the installation wizard.
14. Close the autorun program.

One Identity Manager is installed for all user accounts on the workstation or server. In the default installation, 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 56
- Installation prerequisites on page 20
- One Identity Manager tools on page 13
- Installing One Identity Manager components on a Windows terminal server on page 60
- Installing and configuring a One Identity Manager database on page 61
- Installing and configuring the One Identity Manager Service on page 90
- Machine roles and installation packages on page 188

Installing 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, the users themselves also have the relevant permissions to use the Windows terminal server.

To install One Identity Manager components on a Windows terminal server:

1. Log in with a user account that has administrator permissions on the Windows terminal server.

   Logging in using a console connection is recommended. You can use the following calling syntax:

   `Start/Run: mstsc /Console /v:<server name>`

   with:

   <server name>: Terminal server name (without leading "\")
2. Open the command line console (`CMD.exe`) and switch the Windows terminal server into software installation mode. You can do this with the following command line call:

   `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. You can do this with the following command line call:

   ```
   CHANGE USER /EXECUTE
   ```

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 57

Installing and configuring a One Identity Manager database

To set up the One Identity Manager database, use the Configuration Wizard. The Configuration Wizard runs 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. Creates the required SQL logins and database users permissions for the administrative user, configuration user, and end user.
3. Creates administrative system users and permissions groups.
4. Encrypts the database.
5. Installs and configures a One Identity Manager Service with direct access to the database for handling SQL processes and automatic server software updates.
6. Installs and configures the Database Agent Service.

   The Database Agent Service controls processing of DBQueue Processor tasks. The Database Agent Service is deployed through the One Identity Manager Service plugin. Alternatively, the Database Agent Service can be run from the `DatabaseAgentServiceCmd.exe` command line program.

NOTE: Additional steps are run in the One Identity Manager depending on the selected Configuration Wizard modules.

Additional steps are required to configure the One Identity Manager database following the schema installation:

- Configure the database for testing, development, or production.
- 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 various 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. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.
- In certain circumstances, it is necessary to store encrypted information in the One Identity Manager database. If you did not encrypt the database when you installed with the Configuration Wizard, use the Crypto Configuration program to encrypt.
- 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 percent. 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

- Tips for setting up a One Identity Manager database on page 63
- Installing and configuring a One Identity Manager database on page 64
- Configuring a One Identity Manager database for testing, development, or production on page 72
- Encrypting database information on page 73
- One Identity Manager vendor notification on page 80
- Setting up the email notification system on page 82

Related topics

- Installing One Identity Manager components on page 57
- Minimum system requirements for implementing SQL Servers as database servers on page 21
- Requirements for a managed instance in Azure SQL Database on page 30
- Requirements for Azure SQL Database as database system on page 37
- Requirements for Amazon RDS for SQL Server as database system on page 43

- Users and permissions for the One Identity Manager database on an SQL Server on page 26
- Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33
- Users and permissions for the One Identity Manager database in Azure SQL Database on page 40

Tips for setting up a One Identity Manager database

Note the following information when setting up the 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:
  - Installation of the Configuration Wizard

    Use the installation 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.
- An installation user with permissions for installing a One Identity Manager database must exist. If you want to use an administrative user to install a One Identity Manager database, ensure that this user has the required permissions.

  For more information, see Users and permissions for the One Identity Manager database on an SQL Server on page 26, Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33, and Users and permissions for the One Identity Manager database in Azure SQL Database on page 40.
- 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 Settings for the database server and the One Identity Manager database on a SQL Server 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.
- If you install the One Identity Manager schema in Azure SQL Database, you must supply a database. There is no support for creating a new database in Azure SQL Database with the Configuration Wizard.

For more information, see Settings for the database server and the One Identity Manager database in Azure SQL Database on page 38.

- If you install the One Identity Manager schema in Amazon RDS for SQL Server, you must supply a database. There is no support for creating a new database in Amazon RDS for SQL Server with the Configuration Wizard.

  For more information, see Requirements for Amazon RDS for SQL Server as database system on page 43.
- For One Identity Manager databases on SQL Servers, it is recommended, on performance grounds that you set the database to the **`Simple`** recovery model for the duration of the schema installation.
- Always start Configuration Wizard on an administrative workstation.
- The program performs a remote installation of One Identity Manager Service.
- 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 90.
- If you are working with an encrypted One Identity Manager database, see Tips for working with an encrypted One Identity Manager database on page 78.

Installing and configuring a 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. On the Configuration Wizard's home page, select the **Create and install database** option and click **Next**.
3. To install a new database, enter the following database connection data on the **Create administrative connection** page.
   - **Server**: Database server.
   - **Windows authentication**: (Optional) Specifies whether the 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 login name of the installation user.

- **Password**: Password for the installation user.
- **Encrypt communication**: Specifies whether encryption is required for exchanging data between the client and server. Select the minimum encryption level. The encryption level that is actually used depends on the database server configuration. For more information, see the documentation from Microsoft.

  Permitted values are:

  - `Optional`: Communication is not encrypted.
  - `Mandatory`: Data exchange is encrypted. The **Trust server certificate** option, allows you to also specify whether to verify the server certificate.
  - `Strict (SQL Server 2022 and Azure SQL)`: The data exchange is encrypted. The server certificate is always verified.
- **Trust server certificate**: If this option is enabled, the data exchange between the client and server is encrypted. However, the server certificate is not verified.

- OR -

To use an existing empty database, on the **Create administrative connection**page, select the **Use an existing, empty database for installation** option and enter the database connection information.

NOTE: To install the One Identity Manager schema in an existing database in Azure SQL Database, enable the option and enter the database connection credentials.

NOTE: To install the One Identity Manager schema in an existing database in Amazon RDS for SQL Server, enable the option and enter the database connection credentials.

- **Server**: Database server.
- (Optional) **Windows Authentication**: Specifies whether the 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 login name of the installation user.
- **Password**: Password for the installation user.
- **Database**: Name of the database.
- **Encrypt communication**: Specifies whether encryption is required for exchanging data between the client and server. Select the minimum encryption level. The encryption level that is actually used depends on the database server configuration. For more information, see the documentation from Microsoft.

  Permitted values are:

- **`Optional`**: Communication is not encrypted.
- **`Mandatory`**: Data exchange is encrypted. The **Trust server certificate** option, allows you to also specify whether to verify the server certificate.
- **`Strict (SQL Server 2022 and Azure SQL)`**: The data exchange is encrypted. The server certificate is always verified.

- **Trust server certificate**: If this option is enabled, the data exchange between the client and server is encrypted. However, the server certificate is not verified.

TIP: To configure additional connection settings, enable the **Advanced** option.

4. 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 18: Database properties

Data	Description
Database name	Name of the database.
Data directory	Directory in which the data file is created. You have the following options: • **`<default>`**: The database server's default directory. • **`<browse>`**: Select a directory using the file browser. • **`<directory name>`**: Directory in which data files are already installed.
Log directory	Directory in which the transaction log file is created. You have the following options: • **`<default>`**: The database server's default directory. • **`<browse>`**: Select a directory using the file browser. • **`<directory name>`**: Directory in which transaction log files are already installed.
Memory tables directory	Directory for the data file group and the database file for memory-optimized tables. You have the following options: • **`<default>`**: The database server's default directory. • **`<browse>`**: Select a directory using the file browser. • **No memory-optimized file group (only History Database)**: No directory is created for the data file group and the database file for memory-optimized

Data	Description
	tables. This setting is only allowed for installing a History Database. • `<Directory name>`: Directory in which data files for memory-optimized tables are already installed.
Initial size	Initial size of the database files. You have the following options: • `<Default>`: Default entry for the database server. • `<custom>`: User-defined entry. • Different recommended sizes: Depending on the number of identities being administrated.

b. In the **Installation source** pane, select the directory with the installation files.

- OR -

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

5. On the **Select configuration module** page, select the configuration module .
   - If you started the Configuration Wizard from the install wizard, the configuration modules for the selected edition are already activated. In this case, check over the module selection.
   - Select the configuration module at this point if you started the Configuration Wizard directly. Dependent configuration modules are selected automatically.
6. Error that prevent processing the database are displayed on the **Database check** page. Correct the errors before you continue with the installation.
7. On the **Create a new login for administrators** page, decide which SQL login to use for administrative users. You have the following options:
   - **Create new logins for the database**: Select this option if you want to work with granular permissions.

     This creates a new administrative SQL login for the database.
     - Enter the login name, password, and password confirmation for the new SQL login.

     Later on in the process, the Configuration Wizard sets up additional SQL logins for the configuration user and the end user.
   - **Use an existing SQL login**: Select this option if you have already created an administrative SQL login and want to use it. Later on in the process, the Configuration Wizard sets up additional SQL logins for the configuration user and the end user.

a. Enter the login name, password, and password confirmation for the SQL login.

b. Set the **Permissions** option so that the SQL login obtains permissions for the database. If this option is not set, only the permissions are tested.

- **Use the current SQL login for the database**: When you select this option, no additional SQL 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: To install the One Identity Manager schema in an existing database in Amazon RDS for SQL Server, select this option. The granular permissions concept is not supported.

  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/.

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

   Installation and configuration of the database are 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 logins for configuration and end users** page, enter the login name, the password, and password confirmation for the SQL logins of 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, 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 additional 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 **CCCViewPermissions** and **CCCEditPermissions** are created permission groups. Administrative system users are automatically added to these permissions groups.
- For role-based login, the **CCCViewRole** and **CCCEditRole** permission groups are created.

To create more permissions groups

i. Enable the **Advanced** option and in the **Permissions groups** view, click the ✚ button.

ii. Enter the name of 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 **Enable database encryption** page, select one of the following options:
    - **Skip database encryption**: The database is not encrypted. You can encrypt the database at later date using the Crypto Configuration program.
    - **Enable database encryption**: The database is encrypted in the next step.
        1. In the **Private key** field, enter the name of the key file (default: `private.key`).
        2. Click **New** and, using the file browser, select the where you want to store the key file.
        3. Click **Save**.

           This generates the key file (`*.key`). This closes the file browser and displays the path and file name under **Private key**.
        4. Confirm that you have saved the key file.

           Take the Tips for working with an encrypted One Identity Manager database on page 78 into account.
12. 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 Job server with the One Identity Manager Service at this stage, select the **Skip service installation** option.

    a. In the **Installation data** pane, enter the following data for installing the One Identity Manager Service.
        - **Computer**: Select the server, on which you want to install and start the service, from the drop-down or enter the server's name or IP address.

          To run the installation locally, select `Local installation` from the drop-down.
        - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

You can also change other One Identity Manager Service details in the advanced options, such as the installation directory, name, display name, and the One Identity Manager Service description.

b. In the **Machine roles** pane, select the machine role for the service. By default, the **Server | Job Server** machine role is set. You can add more machine roles.

c. (Optional) Enable the **Advanced** option and, in the **Configuration** pane, check the configuration of the One Identity Manager Service.

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

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

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

> NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

13. The **Processing database tasks** page only appears if there are still tasks for the DBQueue Processor queued in the DBQueue that are required for installing the database. Once processing is complete, click **Next**.
14. On the last page of the Configuration Wizard, click **Finish**.

Related topics

- Tips for setting up a One Identity Manager database on page 63
- Error messages when installing and updating the One Identity Manager database on page 174
- Editing a One Identity Manager database during setup using the Configuration Wizard on page 70
- Encrypting database information on page 73
- Tips for working with an encrypted One Identity Manager database on page 78

Editing a 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 logins and database users with permissions for the administrative user, configuration user and end user. For more information, see Users and permissions for the One Identity Manager database on an SQL Server on page 26.
- Installs 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, or 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.
- Compiles 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.
- Uploads 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 more information about system users, permissions groups, 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 production 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**.
- Installs and configures 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 run 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 carries out the following steps.

- Installs the One Identity Manager Service components.
- Configuring the One Identity Manager Service
- Starts the One Identity Manager Service.

- Installs and configures the Database Agent Service.

  The Database Agent Service controls processing of DBQueue Processor tasks. The Database Agent Service is deployed through the One Identity Manager Service plugin. Alternatively, the Database Agent Service can be run from the `DatabaseAgentServiceCmd.exe` command line program.

  NOTE: If the Database Agent Service is not working, a message is displayed in the status bar in all the administration tools. To see this message, users must have at least the configuration user access level.

Related topics

- Automatic updating of One Identity Manager on page 101
- Displaying the transport history and testing the One Identity Manager version on page 172

Configuring a One Identity Manager database for testing, development, or production

Use the staging level of the One Identity Manager database to specify whether the database is a test database, development database, or a production database. A number of database settings are controlled by the staging level.

If you change the database's staging level, the following settings are configured.

- Color of the One Identity Manager tools status bar
  - Development: none
  - Test: green
  - Production: yellow
- Maximum runtime for the central dispatcher to process DBQueue Processor tasks
  - Development: 20 minutes
  - Test: 40 minutes
  - Production: 120 minutes
- Maximum number of slots for processing DBQueue Processor tasks
  - Development: 5
  - Test: 7
  - Production: maximum number of slots according to hardware configuration

The default configuration settings for processing DBQueue Processor tasks are configured for normal operation and usually do not need to be modified. If required, you can control processing using different configuration settings. For more information, see the *One Identity Manager Configuration Guide*.

To modify a database staging level

1. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Database staging level** entry and click **Run**.

   This starts the Designer.
3. In the Designer, select the **Base Data > General > Databases** category.
4. In the List Editor, select the database.
5. In the edit view, select the **General** tab.
6. Change the value of the **Staging level** property to `Test environment`, `Development system`, or `Production system`.
7. Confirm the security prompt with **Yes**.
8. Select the **Database > Save to database** and click **Save**.

Encrypting 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.

In certain circumstances, it is necessary to store encrypted information in the One Identity Manager database: If you did not encrypt the database when you installed

with the Configuration Wizard, use the Crypto Configuration program to encrypt. With this program an encryption file is created and the contents of the database columns that are affected are converted.

To change the encryption method

- In the Designer, set the **Common | EncryptionScheme** configuration parameter and select one of the options:
  - **`RSA`**: RSA encryption with AES for large data (default).
  - **`FIPSCompliantRSA`**: FIPS certified RSA with AES for large data. This method is used if encryption must match the FIPS 104-2 standard. The local security policy **Use FIPS compliant algorithms for encryption, hashing, and signing** must be enabled.

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

Detailed information about this topic

- Creating new database keys and encrypting database information on page 74
- Changing database keys and encrypting database information on page 75
- Reencrypting database information on page 76
- Decrypting database information on page 77
- Tips for working with an encrypted One Identity Manager database on page 78

Creating new database keys and encrypting 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. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Encrypt the database** entry and click **Run**.

   This starts the Crypto Configuration program.
3. Click **Next** on the home page.
4. On the **New database connection** page, enter the valid connection credentials for the One Identity Manager database.
5. On the **Select action** page, select **Create or change database key**.
6. On the **Private key** page, select **There was no encryption yet**.
7. On the **New private key** page, create a new 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. This closes the file browser and displays the path and file name under **Private key**.

d. Click **Next**.

This establishes which data to encrypt.

8. The date to be encrypted is displayed on the **Convert database** page.

a. Click **Convert**.

b. Confirm the following two security questions with **Yes**.

This starts data encryption and displays the conversion progress.

c. Click **Next**.

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

Related topics

- Changing database keys and encrypting database information on page 75
- Reencrypting database information on page 76
- Decrypting database information on page 77
- Tips for working with an encrypted One Identity Manager database on page 78

Changing database keys and encrypting 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.
- 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. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Encrypt the database** entry and click **Run**.

   This starts the Crypto Configuration program.
3. Click **Next** on the home page.

4. On the **New database connection** page, enter the valid connection credentials for the One Identity Manager database.
5. On the **Select action** page, select **Create or change database key**.
6. 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**.

       This closes the file browser and displays the path and file name.
    e. Click **Next**.
7. On the **New private key** page, create a new 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. This closes the file browser and displays the path and file name under **Private key**.
    d. Click **Next**.

       This establishes which data to encrypt.
8. The date to be encrypted is displayed on the **Convert database** page.
    a. Click **Convert**.
    b. Confirm the following two security questions with **Yes**.

       This starts data encryption and displays the conversion progress.
    c. Click **Next**.
9. Click **Finish** on the last page to end the program.

Related topics

- Creating new database keys and encrypting database information on page 74
- Reencrypting database information on page 76
- Decrypting database information on page 77
- Tips for working with an encrypted One Identity Manager database on page 78

Reencrypting database information

Use this method if the database already has encryption but you want to encrypt more columns.

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. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Encrypt the database** entry and click **Run**.

   This starts the Crypto Configuration program.
3. Click **Next** on the home page.
4. On the **New database connection** page, enter the valid connection credentials for the One Identity Manager database.
5. On the **Select action** page, select **Encrypt using existing key**.

   This establishes which data to encrypt.
6. The date to be encrypted is displayed on the **Convert database** page.
   a. Click **Convert**.
   b. Confirm the following two security questions with **Yes**.

      This starts data encryption and displays the conversion progress.
   c. Click **Next**.
7. Click **Finish** on the last page to end the program.

Related topics

- Creating new database keys and encrypting database information on page 74
- Changing database keys and encrypting database information on page 75
- Decrypting database information on page 77
- Tips for working with an encrypted One Identity Manager database on page 78

Decrypting database information

NOTE:

- You need the file with the database key for this.
- 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 decrypt the One Identity Manager database

1. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Encrypt the database** entry and click **Run**.

   This starts the Crypto Configuration program.
3. Click **Next** on the home page.
4. On the **New database connection** page, enter the valid connection credentials for the One Identity Manager database.
5. On the **Select action** page, select **Decrypt data**.

   The establishes which data to decrypt.
6. The **Convert database** page displays the data to decrypt.
   a. Click **Convert**.
   b. Confirm the following two security questions with **Yes**.
   c. Using the file browser, select the (`*.key`) file with the database key.
   d. Click **Open**.

      This closes the file browser. Data decryption starts and displays the conversion progress.
   e. Click **Next**.
7. Click **Finish** on the last page to end the program.

Related topics

- Creating new database keys and encrypting database information on page 74
- Changing database keys and encrypting database information on page 75
- Reencrypting database information on page 76
- Tips for working with an encrypted One Identity Manager database on page 78

Tips for 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.

IMPORTANT:

- The file with the private key must exist in the server's installation directory on all servers with an active One Identity Manager Service.
- If you change the One Identity Manager Service user account, you must save the key file in the service's install directory again.

To declare the database key

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

Table 19: Configuring the One Identity Manager Service for encryption

Configuration module	Parameters	Meaning
JobServiceDestination	Encryption method (`EncryptionScheme`)	Encryption method used
JobServiceDestination	File with private key (`PrivateKey`)	Enter the file with the encryption information. The default file is `private.key`.
JobServiceDestination	Private key identifier (`PrivateKeyId`)	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.
File with the private key.		Private key identifier and path to private key file. The ID is expected in the JobServiceDestination in the **Private key identifier** parameter (`PrivateKeyId`) The default key has the ID **`Default`**.

2. Save the key file created in the service's install directory.
3. Open the service management and restart the One Identity Manager Service.

Detailed information about this topic

- Encrypting database information on page 73

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 80
- Checking vendor notification on page 81
- Disabling vendor notification on page 81

Enabling vendor notification

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

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 to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Configure vendor notification** entry and click **Run**.

   This starts the Designer and opens the Configuration Parameter Editor.
3. Enable the **Common | MailNotification | VendorNotification** configuration parameter and enter the email address of your business contact.

The email address is used as the return address for notifying vendors.

4. Select the **Database > Save to database** and click **Save**.

Detailed information about this topic

- Checking vendor notification on page 81
- Disabling vendor notification on page 81
- Setting up the email notification system on page 82

Checking vendor notification

NOTE: You can only configure vendor notification in the Launchpad on a One Identity Manager database with the `Production system` staging level.

To check whether vendor notification is enabled

- Start the Launchpad and log in to the One Identity Manager database.

  In the **Installation overview > Installation Check list** section, in the **Configure vendor notification** entry, you can see whether the function is enabled.

Detailed information about this topic

- Enabling vendor notification on page 80
- Disabling vendor notification on page 81

Disabling vendor notification

NOTE: You can only configure vendor notification in the Launchpad on a One Identity Manager database with the `Production system` staging level.

To disable a vendor notification

1. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Installation overview > Installation Checklist** section, select the **Configure email delivery** entry and click **Run**.

   This starts the Designer and opens the Configuration Parameter Editor.
3. Disable the **Common | MailNotification | VendorNotification** configuration parameter.
4. Select the **Database > Save to database** and click **Save**.

Related topics

- Enabling vendor notification on page 80
- Checking vendor notification on page 81

Setting up the email notification system

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 run during process handling. You can implement custom notifications in addition to predefined notification processes.

To change the configuration settings for email notifications, use the email configuration wizard or edit the configuration parameters in the Designer.

NOTE: Some configuration settings are only available if the One Identity Manager modules are installed.

To set up the email notification system

1. In the Launchpad, in the **Installation overview > Installation Checklist** section, select the **Configure email delivery** entry and click **Run**.
2. On the home page of the Mail Configuration Wizard, click **Next**.
3. On the **Create connection to the SMTP server** page, configure the SMTP server connection to use for sending emails.

    - **SMTP server**: SMTP server for sending email notifications. If a server is not given, `localhost` is used.
    - **User name**: User account name for authentication on an SMTP server.
    - **Domain**: User account domain for authentication on the SMTP server.
    - **Password** and **Password repeat**: User account password for authentication on the SMTP server.

      To test the user account data, click **Test connection**.
    - **Microsoft 365 client ID**: Application client ID used to send the emails. You can find your application ID in the Microsoft Entra ID Admin Center under **Applications > App registrations < <your application> > Overview > Application (client) ID**.
    - **Port**: Port of the SMTP service on the SMTP server. Default: **25**
    - **Transport encryption**: Encryption method for sending email notifications. If none of the following options are given, the port is used to define the behavior (port 25: no encryption, port 465: with SSL/TLS encryption).

      Permitted values are:

- **Auto**: Identifies the encryption method automatically.
- **SSL**: Encrypts the entire session with SSL/TLS.
- **STARTTLS**: Uses the STARTTLS mail server extension. Switches TLS encryption after the greeting and loading the server capabilities. The connection fails if the server does not support the STARTTLS extension.
- **STARTTLSWhenAvailable**: Uses the STARTTLS mail server extension if available. Switches on TLS encryption after the greeting and loading the server capabilities, however, only if it supports the STARTTLS extension.
- **None**: No security for the transport layer. All data is sent as plain text.

- **Accept self-signed certificates**: Specifies whether self-signed certificates for TLS connections are accepted.
- **Allow server name mismatch in certificates**: Specifies whether server names that do not match are permitted by certificates for TLS connections.

4. On the **Define SMTP Job servers** page, select at least one Job server to take on the **SMTP server** functionality.
5. On the **Email settings** page, you can define the default email address of a sender and a recipient as well as the layout of the email.

   - **Recipient address**: Default email address of the recipient of the notifications.
   - **Sender address**: Sender's default email address for sending automatically generated notifications.

     Syntax:

     ```
     sender@company.com
     ```

     Example:

     ```
     noreply@company.com
     ```

     You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>).

     Example:

     ```
     One Identity <noreply@company.com>
     ```
   - **Language code**: Default language used to send email notifications if a language cannot be determined for a recipient.
   - **Language**: Default language for sending email notifications.
   - **Font**: Default font for email notifications.
   - **Font size**: Default font size for email notifications.
   - **Signature**: Signature under the salutation.
   - **Company**: Company name.
   - **Link**: Link to the company's website.
   - **Link display**: Display text for the link to the company's website.

6. On the **Data security** page, you can configure the data security settings.

    - **Certificate thumbprint**: SHA1 thumbprint of the certificate to use for the signature. This can be in the computer's or the user's certificate store.

      NOTE: Ensure that the private key in the certificate is marked as exportable.

      If you want to use a digital signature, enable **Certificate thumbprint** and specify the thumbprint.
    - **Encryption**: Specifies whether emails are encrypted. If you enable this function, additional settings are shown.
    - **Domain controller**: Domain controller of the requested domain to use.
    - **Domain**: Distinguished name of the domain to request.
    - **User account**:User account for querying Active Directory.
    - **Password** and **Confirm password**: Password of the user account.
    - **Port**: Communication port for secure access. Default: `389`
    - **Use Secure Sockets Layer Protokoll (SSL)**: Specifies whether to use an SSL/TLS encrypted connection.
    - **Certificate encryption script**: Script that supplies a list of encryption certificates. Default: `QBM_GetCertificates`
    - **Authentication type**: Authentication type for logging in to LDAP. Default: `Basic`

      Permitted values are:

        - `Basic`: Uses default authentication.
        - `Negotiate`: Uses Negotiate authentication from Microsoft.
        - `Kerberos`: Uses Kerberos authentication.
        - `NTLM`: Uses Windows NT Challenge/Response (NTLM) authentication.
7. On the **Email notifications about requests** page, make any changes to the general settings for email notifications about requests. In addition, define whether the **Approval by mail** feature can be used for requests. If you enable this feature, the settings you need are shown.

    - **Sender address**: Sender's default email address for sending automatically generated notifications.

      Syntax:

      `sender@company.com`

      Example:

      `noreply@company.com`

      You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>).

      Example:

```
One Identity <noreply@company.com>
```

- **Daily notifications about pending approvals**: Specifies whether approvers only receive emails once a day if there are requests awaiting their approval decisions.

  If this option is not set, approvers immediately receive an email once a request is available for approval. Set this option to reduce the number of email notifications. This will mean that you cannot use the **Approval by mail** feature.

  > TIP: To use a template other than the default one for this, change the value in the **QER | ITShop | MailTemplateIdents | RequestApproverByCollection** configuration parameter in the Designer.

- **IT Shop approval by mail**: Specifies whether the **Approval by mail** feature can also be used for approving requests. If you enable the feature, adjust the required settings. Then you cannot use the **Daily notifications about pending approvals** feature.
- **User name**: Name of the user account for authenticating the mailbox used for approval by mail.
- **Domain**: Domain of the user account for authenticating the mailbox used for approval by mail.
- **Password** and **Password repeat**: Password of the user account for authenticating the mailbox used for approval by mail.
- **Web service URL**: Specifies whether the URL of the Microsoft Exchange web service for accessing the mailbox is used. If you enable this functionality, enter the URL.
- **Mailbox**: Microsoft Exchange mailbox to which approvals by mail are sent.
- **Delete behavior**: Specifies the way emails are deleted from the inbox.
- **Application ID**: Exchange Online application ID for authentication with OAuth 2.0. If the value is not set, the **Basic** or the **NTML** authentication method is used.

8. On the **Email notifications about attestation** page, make any changes to the general settings for email notifications about attestations. In addition, define whether the **Approval by mail** feature can be used for attestations. If you enable this feature, the settings you need are shown.

   - **Sender address**: Sender's default email address for sending automatically generated notifications.

     Syntax:

     ```
     sender@company.com
     ```

     Example:

     ```
     noreply@company.com
     ```

     You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>).

Example:

```
One Identity <noreply@company.com>
```

- **Daily notifications about pending approvals**: Specifies whether attestors only receive emails once a day if there are attestation cases awaiting their approval decisions.

  If this option is not set, attestors immediately receive an email once an attestation case is available for approval. Set this option to reduce the number of email notifications. Then you cannot use the **Approval by mail** feature.

  TIP: To use a template other than the default one for this, change the value in the **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter in the Designer.

- **Attestation by mail**: Specifies whether the **Approval by mail** feature can be used. If you enable the feature, adjust the required settings. Then you cannot use the **Daily notifications about pending approvals** feature.
- **User name**: Name of the user account for authenticating the mailbox used for approval by mail.
- **Domain**: Domain of the user account for authenticating the mailbox used for approval by mail.
- **Password** and **Password repeat**: Password of the user account for authenticating the mailbox used for approval by mail.
- **Web service URL**: Specifies whether the URL of the Microsoft Exchange web service for accessing the mailbox is used. If you enable this functionality, enter the URL.
- **Mailbox**: Microsoft Exchange mailbox to which approvals by mail are sent.
- **Delete behavior**: Specifies the way emails are deleted from the inbox.
- **Application ID**: Exchange Online application ID for authentication with OAuth 2.0. If the value is not set, the **Basic** or the **NTML** authentication method is used.

9. On the **Report subscriptions** page, you can change the default settings for report subscriptions.

   - **Sender address**: Sender's default email address for sending automatically generated notifications about report subscriptions. Replace the default address with a valid email address.

     Syntax:

     ```
     sender@company.com
     ```

     Example:

     ```
     noreply@company.com
     ```

     You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>).

     Example:

`One Identity <noreply@company.com>`

- **Default report template**: Default report that is used as a template for creating simple list reports.
- **Store subscription**: Specifies whether subscribed reports are saved in a repository. If you enable the feature, adjust the required settings.
- **Report storage share**: Path to the repository for subscribed reports.

  Syntax: `\\<server>\<share>`
- **Storage life time (days)** Maximum retention period in days that a report is available in the storage share. After this period, reports are deleted.

10. On the **Email notifications about actions in the target system** page, you can enter an email address for notifying about actions in the target system. This might be error or success messages about changes in the target system.

    - **<Target system type>**: Specifies whether email notifications are sent with error or success messages about changes in target systems of this type. If you enable the feature, enter the email address to send notifications to.
11. On the last page of the Mail Configuration Wizard, click **Finish**.

There may be other configuration settings required for different notification processes. You can edit these in the configuration parameters in the Designer if required.

Related topics

- Sending email notifications via Microsoft 365 on page 87
- Configuration parameters for the email notification system on page 190
- Setting up Job servers on page 91
- Error messages when generating email notifications on page 177

Sending email notifications via Microsoft 365

To send email notifications via Microsoft 365, perform the following steps.

- Register an application in the Microsoft Entra ID Admin Center (https://admin.microsoft.com/). For more information about registering an application, see https://docs.microsoft.com/azure/active-directory/develop/quickstart-register-app.
- Modify the configuration settings for email notifications in the One Identity Manager. These settings are used in the default processes for sending emails.

Registering the application in Microsoft Entra ID

NOTE: When you add an application to Microsoft Entra ID, it creates an application ID. You need the application ID for configuring sending mail notifications.

To register an application in Microsoft Entra ID

1. Log in to the Microsoft Entra ID Admin Center (https://admin.microsoft.com/).
2. Register a new application under **Applications > App registrations**.
    a. Under **Name**, enter a name for your application.
    b. Under **Redirect URI (optional)**, select `Public client/native (mobile & desktop)`.
    c. Click **Register**.
3. Under **Manage > Authentication**, in the **Advanced settings** section under **Allow public client flows**, set the **Enable the following mobile and desktop flows** to **Yes**. Click **Save**.
4. Under **Manage > API permissions** in the **Configured permissions** section, configure the following settings.
    a. Remove the `User.Read` Microsoft Graph permission.
    b. Click **Add a permission** and under **Request API permissions > Microsoft APIs**, select the **Microsoft Graph** tile.
    c. Select **Delegated permissions** and select the `SMTP.Send` permission.
    d. Click **Add permissions**.
    e. To grant administration consent for these permissions, click **Grant Admin consent** and confirm the prompt with **Yes**.

Modifying configuration settings in One Identity Manager

To change the configuration settings, use the email configuration wizard or edit the configuration parameters in the Designer.

Table 20: Configuration settings for email notifications via Microsoft 365

Setting	Value	Configuration parameter
SMTP server	smtp.office365.com	Common | MailNotification | SMTPRelay
Port	587	Common | MailNotification | SMTPPort
Microsoft 365 client ID	Application client ID used to send the emails. You can find your application ID in the Microsoft Entra ID	Common | MailNotification |

Setting	Value	Configuration parameter
	Admin Center under **Applications > App registrations < <your application> > Overview > Application (client) ID**.	O365ClientId
User name	Microsoft 365 user email address.	Common | MailNotification | SMTPAccount
Password	User password.	Common | MailNotification | SMTPPassword

Related topics

- Setting up the email notification system on page 82
- Configuration parameters for the email notification system on page 190

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 run 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 with respect to the server function.
- Install the One Identity Manager Service.
- Configure the One Identity Manager Service.
- Start the One Identity Manager Service.

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

NOTE: On Linux operating systems, use of oneidentity/oneim-job docker images is recommended.

Related topics

- One Identity Manager Docker images on page 55
- Setting up Job servers on page 91
- Installing the One Identity Manager Service with the Server Installer on page 92
- Displaying the One Identity Manager Service log file on page 95
- Changing the user account or start type of the One Identity Manager Service on page 96
- The One Identity Manager Service in a cluster on page 97

- Updating One Identity Manager on page 108
- Machine roles and installation packages on page 188

Setting up Job servers

Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using exactly this queue name:

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

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 **SQL processing server** and **Update server** server functions. Use the Configuration Wizard to configure the service and install it 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 it on a server.
- You can create Job servers in the Designer.

  Use the Designer, to create a Job server with the machine roles and server functions, configure the service on the server and install the service remotely. For more information, see the *One Identity Manager Configuration Guide*.
- Alternatively, you can use the installation wizard to install the service components on the server and then configure the service using the Job Service Configuration program. For detailed information about configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.
- If the **Common | Jobservice | AutoCreateServerFromQueues** configuration parameter 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 a One Identity Manager database on page 64
- Installing the One Identity Manager Service with the Server Installer on page 92
- Installing One Identity Manager components on page 57
- Implementing the automatic software update on page 106

Installing the One Identity Manager Service with the Server Installer

IMPORTANT: If you are working with an encrypted One Identity Manager database, see Tips for working with an encrypted One Identity Manager database on page 78.

To set up a Job server, perform the following steps.

1. Create a Job server and install and configure the One Identity Manager Service.

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

   - Sets up a Job server.
   - Specifies machine roles and server function for the Job server.
   - Installs One Identity Manager Service components corresponding to the machine roles.
   - Configures the One Identity Manager Service.
   - Starts the One Identity Manager Service.

   Use the Server Installer to install the One Identity Manager Service locally or remotely.

   To remotely install the One Identity Manager Service, provide an administrative workstation on which the One Identity Manager components are installed. Ensure that the One Identity Manager components are installed on the server before installing locally. For more information about installing One Identity Manager components, see the *One Identity Manager Installation Guide*.
2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.
3. To generate processes for the Job server, you need the provider, connection parameters and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For more information about connection data, see the *One Identity Manager Configuration Guide*.

To install and configure the One Identity Manager Service on a server

1. Start the Server Installer program.

   NOTE: To install remotely, start the Server Installer program on your administrative workstation. To install locally, start the program on the server.

2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

   You can connect via the application server or directly to connect to the database.

3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.

   a. Select a Job server from the **Server** drop-down.

      - OR -

      To create a new Job server, click **Add**.

   b. Enter the following data for the Job server.

      - **Server**: Name of the Job server.
      - **Queue**: Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
      - **Full server name**: Full server name in accordance with DNS syntax.

        Syntax:

        ```
        <Name of servers>.<Fully qualified domain name>
        ```

   > 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 the Designer.

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

5. On the **Server functions** page, specify the function of the server in the One Identity Manager environment. One Identity Manager processes are handled with respect to 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. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

   For a direct connection to the database:

   a. In the module list, select **Process collection > sqlprovider**.

   b. Click the **Connection parameter** entry, then click the **Edit** button.

c. Enter the connection data for the One Identity Manager database.

d. Click **OK**.

For a connection to the application server:

a. In the module list, select the **Process collection** entry and click the **Insert** button.

b. Select **AppServerJobProvider** and click **OK**.

c. In the module list, select **Process collection > AppServerJobProvider**.

d. Click the **Connection parameter** entry, then click the **Edit** button.

e. Enter the address (URL) for the application server and click **OK**.

f. Click the **Authentication data** entry and click the **Edit** button.

g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

h. Click **OK**.

7. To configure the installation, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. On the **Service access** page, enter the service's installation data.

    - **Computer**: Select the server, on which you want to install and start the service, from the drop-down or enter the server's name or IP address.

      To run the installation locally, select `Local installation` from the drop-down.

    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

    You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

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

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

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

    NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Related topics

- Minimum system requirements for Job servers on page 44
- Users for One Identity Manager on page 49
- Changing the user account or start type of the One Identity Manager Service on page 96
- Machine roles and installation packages on page 188

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**.

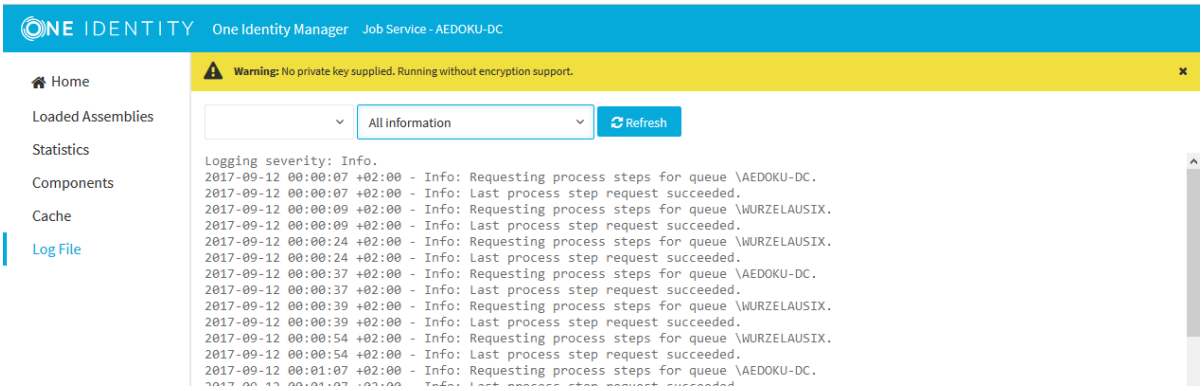
Different credentials are expected depending on how the authentication method is configured for displaying the log file.

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

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

   The One Identity Manager Service HTTP server for the Job server is queried and the various One Identity Manager Service services are displayed.
3. To display the contents of the log file, select **Log File** in the navigation view.

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 drop-down on the website for this. Only text contained in the log file can be displayed in

this case. For example, if the message type is `Warning`, 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 21: Log file color code

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

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

For more information about configuring how the One Identity Manager Service log file is displayed, see the *One Identity Manager User Guide for One Identity Manager Tools User Interface*.

Changing the user account or start type of the One Identity Manager Service

NOTE:

- In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.
- If you change the One Identity Manager Service's user account, you must save the service's configuration file in the service's install directory again.
- If you are working with an encrypted One Identity Manager database, see Tips for working with an encrypted One Identity Manager database on page 78.

To customize login data and the way the service is started

1. Open the service management of the server and select the **One Identity Manager Service** in the list of services.
2. Open service properties with the **Properties** context menu item.
3. On the **General** tab, change the start type if necessary.

   The `Automatic` start type 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.

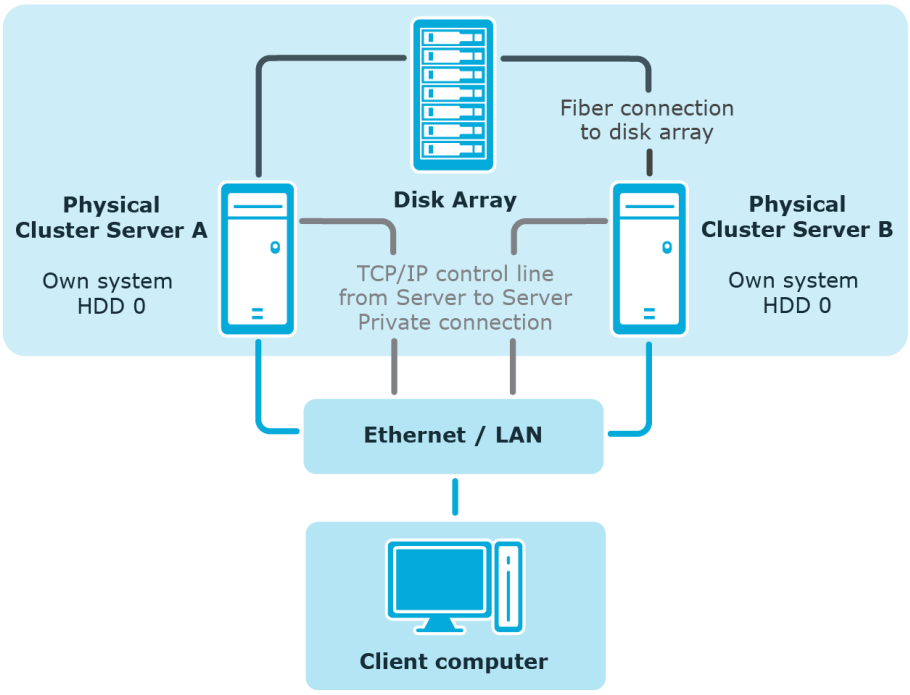
Related topics

- Minimum system requirements for Job servers on page 44
- Users for One Identity Manager on page 49

The One Identity Manager Service in a cluster

The idea of a cluster solution is to make the system highly available. The goal 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.

Figure 4: Example of a cluster solution



This cluster is made up of two 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 98
- Installing and configuring the One Identity Manager Service in a cluster on page 99

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 that 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), or 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. Therefore, the service always has the same configuration irrelevant 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 into the required state (**`Manual`** or **`Stopped`**) before they are registered by the program.

Related topics

- The One Identity Manager Service in a cluster on page 97
- Installing and configuring the One Identity Manager Service in a cluster on page 99

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 **Queue** parameter 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. 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, you must 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 **`Generic Service`** resource type.
- Select the following One Identity Manager Service dependencies.
  - Cluster IP address
  - Cluster name
  - Quorum; for example, disc: D
- Do not enter additional 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 Identity One 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 97
- Registering the One Identity Manager Service in a cluster on page 98

6

Automatic updating of One Identity Manager

Local installation and updating of software in particular can prove to be problematic due to the distributed structure of servers and workstations. To help guarantee an acceptable workload for network administrators, a One Identity Manager automatic update method 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 101
- Implementing the automatic software update on page 106
- Disabling automatic software update on page 107

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.

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 `Softwarerevision.viv` file. This file is assigned the **Read only** and **Not visible** permissions 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

The `Update.zip` file plays a central role in automatic updating. The zip archive contains the `Update.exe` and all the files that are required on the clients or servers 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 `Update.zip` file is stored in the `QBMFileRevision` table.

The zip archive is extended with all files from the installation data that correspond to the `*.Update.zip` name filter. 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 `InstallState.config` file. This file contains information about the installed machine roles, installation packages and files.

Whether or not a software update is required, depends on the comparison of semaphore values from the database and the `softwarerevision.viv` file. 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 database, perform the following checks:

- Has the file size changed?

  In this case, the file is added to the list of files to be updated.

- Has the hash value changed?

  In this 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. Any files that no longer exist are deleted.

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 103
- Automatic updating of the One Identity Manager Service on page 104
- Automatic updating of web applications on page 105
- Implementing the automatic software update on page 106
- Disabling automatic software update on page 107

Automatic updating of the One Identity Manager tools

When a program starts up, it establishes a connection to the database and carries out the semaphore test. If the `softwarerevision.viv` file 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`) requires an administrator to log in if user account control is active, assuming that the current 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 begins.

The application then loads the `Update.zip` file 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 (`Update.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 may interfere with the update process. At the same time, administrator permissions requirements are authorized by user account control, if they are necessary.

In this update procedure, not only are the files exchanged but other migration steps from the `*.Update.dlls` are also run. 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 run 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 104

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 or not the users of One Identity Manager tools can decide when their own workstations are updated, is controlled by the **Common | AutoUpdate | AllowOutOfTimeApps** configuration parameter. This means:

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

  NOTE: If users do not want to update immediately, they can continue working. The update begins 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 necessary 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 **`software revision`** semaphore. If this value differs from the value in the database, the Job server is labeled as "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 **Common | Autoupdate | ServiceUpdateType** configuration parameter.

First, the start time of the last change is determined from the `SoftwareRevision.viv` file. 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 obtains an `AutoUpdate` process from the server. which loads the `Update.zip` file 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 run.

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 updates. 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 **Replace a process level token** and **Adjust memory quotas for a process** local security policies.

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.

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 `Update.zip` file 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 application servers on page 139
- Manager web application update on page 161

Implementing the automatic software update

The following permissions are required for automatic software updating:

- It is recommended that you apply full access permissions 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. In the Designer, check the **Common | Autoupdate** configuration parameter.
    - If the configuration parameter is set (default), One Identity Manager files that do not have the current revision status, are updated automatically.
    - If this configuration parameter is not set, no automatic update is performed.
3. Use the **Common | AutoUpdate | AllowOutOfTimeApps** configuration parameter 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 **Common | Autoupdate | ServiceUpdateType** configuration parameter, determine which procedure is used to update the One Identity Manager Service.

Table 22: Methods under to the configuration parameter Common | Autoupdate | ServiceUpdateType

Method	Meaning
Queue	A process is queued in the Job queue that distributes the files.
DB	The files are reloaded directly from the database. Implement this procedure if all Job servers have a direct connection to the database.

Method	Meaning
Auto	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.

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

Related topics

- Basics for automatic software update on page 101
- Disabling automatic software update on page 107

Disabling automatic software update

NOTE: If the **Common | Autoupdate** configuration parameter 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 workstation automatic update

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

This disables automatic updating completely on this workstation.

Disabling a Job server automatic update

Configure the Job server automatic update in the Job server entry.

To exclude individual Job servers from updating automatically

1. In the Designer, select the **Base Data > Installation > Job server** category.
2. Select the Job server to be edited in the Job server overview.
3. On the **Properties** tab, enable the **No automatic software update** option.
4. Select the **Database > Save to database** and click **Save**.

Disabling automatic application server update

Configure automatic updating in the application server's Manager web application file. For more information, see Updating application servers on page 139.

Updating 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 109
- Automatic updating of One Identity Manager on page 101
- Updating One Identity Manager components with the installation wizard on page 112
- Updating the One Identity Manager database on page 114

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 the Designer, carry out all consistency checks in the **Database** section.
    a. In the Designer, start the Consistency Editor with the **Database > Check data consistency** menu item.
    b. In the **Test options** dialog, click the icon .
    c. Enable all tests in the **Database** view and click **OK**.
    d. Start testing with the **Consistency check > Run** menu item.

    All the 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 will start.
    a. Run the `autorun.exe` program 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. 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 **160** and change it if necessary.
6. Run a schema update of the One Identity Manager database.
    - 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.

- Use the same user that you used to initially install 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.

- If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to 9.3, use an installation user in accordance with Users and permissions for the One Identity Manager database on an SQL Server on page 26.

  After updating One Identity Manager, change the connection parameters. This affect the connection credentials for the database (`DialogDatabase`), for example, the One Identity Manager Service, the application server, administration tools and configuration tools, web applications and web services, and the connection credentials in synchronization projects.
- If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

7. Update the One Identity Manager Service on the update server.
   a. Run 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 credentials of the One Identity Manager Service. 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 additional workstations and Job servers manually. This may be required, for example, if there are a significant number of new changes with a One Identity Manager version update that 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 available for this.

NOTE: Some patches are applied automatically. A process that migrates all existing synchronization projects is queued in the Job queue to do this. To run the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

- Check whether the `DPR_Migrate_Shell` process 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 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 **Update immediately** in the logged in user's menu.

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 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 permissions 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 101
- Updating One Identity Manager components with the installation wizard on page 112
- Updating the One Identity Manager database on page 114
- Installing and updating an application server on page 131
- Installing and updating an API Server on page 142
- Installing and updating the Manager web application on page 157

Updating One Identity Manager components with the installation wizard

NOTE: You can use the automatic software update method for updating workstations and servers. For more information, see Automatic updating of One Identity Manager on page 101.

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

NOTE: If you change versions or add more modules to an existing One Identity Manager installation, use the installation wizard to update the workstation that the One Identity Manager database schema installation starts on.

To update a workstation using the installation wizard

1. Run the program `autorun.exe` from the root directory on the One Identity Manager installation medium.
2. Change to the **Installation** tab. Select the edition that you installed.
3. Click **Install**.

   This starts the installation wizard.
4. Select the language for the installation wizard on the start page and click **Next**.
5. Confirm the conditions of the license.
6. On the **Installation settings** page, enter the following information.
   - **Installation source**: Select the directory containing the installation files.
   - **Installation directory**: Select your current installation directory. Otherwise, the components are not updated and a new installation is created in the second directory instead.

     NOTE: To make additional changes to the 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 default 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.
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.

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

  - OR -

- Click **Add new connection**, select the **SQL Server** system type, and enter the connection data.
  - **Server**: Database server.
  - **Windows authentication**: (Optional) Specifies whether the 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**: User's SQL login name.
  - **Password**: Password for the SQL user's login.
  - **Database**: List of possible databases on the database server. Select the database.
  - **Encrypt communication**: Specifies whether encryption is required for exchanging data between the client and server. Select the minimum encryption level. The encryption level that is actually used depends on the database server configuration. For more information, see the documentation from Microsoft.

    Permitted values are:

    - `Optional`: Communication is not encrypted.
    - `Mandatory`: Data exchange is encrypted. The **Trust server certificate** option, allows you to also specify whether to verify the server certificate.
    - `Strict (SQL Server 2022 and Azure SQL)`: The data exchange is encrypted. The server certificate is always verified.
  - **Trust server certificate**: If this option is enabled, the data exchange between the client and server is encrypted. However, the server certificate is not verified.

8. 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**.

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

   NOTE: Machine roles matching the existing installation are already enabled.

10. On the **Install WebView2** page you are prompted to install Microsoft Edge WebView2. The user interface of some One Identity Manager components requires Microsoft Edge WebView2 to display certain content.

    NOTE: This page is only shown if you want to install One Identity Manager components that are expecting WebView2 and WebView2 is not yet installed.

11. You can start different programs for further installation on the last page of the install wizard.
    - To install the One Identity Manager schema, start the Configuration Wizard and follow the Configuration Wizard instructions.

      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 Job Service Configuration program.

      NOTE: Run this step only on servers on which you have installed the One Identity Manager Service.
12. Click **Finish** to close the installation wizard.
13. 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.

   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. Check the login credentials of the One Identity Manager Service. Specify the service account to use.
4. Start the One Identity Manager Service in service management.

Updating the One Identity Manager database

Automatic version control is integrated into 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 are available for the version of One Identity Manager you are currently running or for 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 the changes in a test system before you load a transport package into a live system.

You can customize the One Identity Manager schema 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 23: Transport package

Transport package type	Description	Tool used
Migration package	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.	Configuration Wizard
Hotfix package	Hotfix packages are provided to load individual corrections to the default configuration such as templates, scripts, processes, or files into the database. Multiple hotfix packages are combined into one cumulative hotfix package. NOTE: If a hotfix package only contains changed files, load these files into the database using the Software Loader file.	Database Transporter Software Loader
Custom configuration package	A custom configuration package is used to exchange customer specific changes between the development, test, and production system database. This transport package is created by the customer and loaded into the database.	Database Transporter

NOTE: If other configuration customizations are to be transferred to a One Identity Manager database in addition to a hotfix package, you can create a cumulative transport package to do this and, by using the Database Transporter, import the transport package into the target database.

Related topics

- Updating the One Identity Manager database with the Configuration Wizard on page 117
- Installing a hotfix in the One Identity Manager database on page 122

Advice on updating the One Identity Manager database

Note the following information when updating up 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 One Identity Manager databases on SQL Servers, it is recommended, on performance grounds, that you set the database to the **Simple** recovery model for the duration of 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 that you used to initially install 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.
- If you want to switch to the granular permissions concept when you upgrade from version 8.0.x to 9.3, use an installation user in accordance with Users and permissions for the One Identity Manager database on an SQL Server on page 26.

  After updating One Identity Manager, change the connection parameters. This affect the connection credentials for the database (`DialogDatabase`), for example, the One Identity Manager Service, the application server, administration tools and configuration tools, web applications and web services, and the connection credentials in synchronization projects.
- If you want to switch to granular permissions when you update from 8.1.x, contact support. To access the Support Portal, go to 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 switches automatically to multi-user mode. If this is not possible, you receive a message in which you can manually switch to multi-user 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*.

- Use the `Modules\QBM\dvd\AddOn\SDK\SQLSamples\MSSQL2K\SDK_Remove_Rights_on_msdb.sql` SDK script to remove permissions that are not longer required for the msdb database.
- It is not recommended to perform an upgrade of the existing modules to a new One Identity Manager version and install additional modules at the same time. This may cause dependencies between modules to be constructed incorrectly. First update the existing modules to the new One Identity Manager version. Then restart the Configuration Wizard and install the additional modules.

Detailed information about this topic

- Updating the One Identity Manager database with the Configuration Wizard on page 117
- Editing the One Identity Manager database while updating with the Configuration Wizard on page 120
- Users and permissions for the One Identity Manager database on an SQL Server on page 26

Updating the One Identity Manager database with the Configuration Wizard

IMPORTANT: Test your changes in a test system before you load a migration package in a live 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. On the Configuration Wizard home page, select the **Update database** option and click **Next**.
3. On the **Select database** page, select the database and installation directory.
    a. Select the database connection in the **Select a database connection** pane. Select a user who at least has administrative permissions for the One Identity Manager database.
    b. In the **Installation source** pane, select the directory with the installation files.
4. Configuration modules and version information are shown on 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 run.

d. (Optional) If it is necessary to select more modules, enable the **Add more modules** option.

e. (Optional) Specify whether to fully repair and verify the supplied default data.

5. On the **Select configuration modules** page, select the additional modules and confirm the security prompt.

   NOTE: This page is only shown if you set **Add more modules**.

   If you add more modules, your custom administrative users obtain the permissions for this module.

6. On the **Database check** page, errors are displayed that prevent the database from being processed. Correct the errors before you continue updating.

7. On the **Initiating the update** page, you will go through the different phases in preparation for database update.

   NOTE: This page is only displayed when updating a database that has at least One Identity Manager version 8.2.

   This step-by-step preparation is intended to ensure that users are informed about the upcoming update and that processes can be shut down in a targeted manner.

   Alternatively, you can start the database update immediately. This skips the preparation phases.

   - Running through preparation phases (default)

     a. Wait until the Configuration Wizard has completed each phase of the database update preparations. The information about the phases is displayed.

     b. Click **Next**.

   - Starting the database update immediately

     a. Click the **Click <here> to start the update immediately** link.

     b. Click **Next**.

8. Other users with existing connections to the database are displayed on the **Active sessions** page.

   - Disconnect the connections on order to start database processing.

9. On the **Create a new login for administrators** page, decide which SQL login to use for administrative users.

   NOTE: This page is only shown when updating a One Identity Manager database from version 8.0.x to version 9.3.

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

You have the following options:

- **Create new logins for the database**: Select this option if you want to work with granular permissions.

  This creates a new administrative SQL login for the database.

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

  Later on in the process, the Configuration Wizard sets up additional SQL logins for the configuration user and the end user.

- **Use the current SQL login for the database**: When you select this option, no additional SQL 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.

10. On the **System administrator connection** page, enter the login credentials for the database login with system administrator permissions.

    NOTE: This page is only shown if you are working with granular permissions and you have to make changes to the administration user's permissions.

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

    TIP: Set **Advanced** to obtain detailed information about processing steps and the migration log. You can copy messages to the clipboard with **CTRL + C**.

    a. During the update process, you must log in as an administrative user.

       i. Enter a user name and password for the administrative system user.

       ii. Click **Connect**.

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

12. On the **Create logins for configuration and end users** page, enter the login name, the password, and password confirmation for the SQL logins of configuration users and end users.

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

    NOTE: This page is only shown when upgrading a One Identity Manager database from version 8.0 to version 9.3 if you have opted for granular permissions on the **Create a new login for administrators** page.

13. On the **System Information** page, configure administrative system users for the One Identity Manager. Enter a password and password confirmation.

    NOTE: This page is only shown if the upgrade creates new administrative system users.

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

    NOTE: 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.

15. The **Processing database tasks** page is only shown if there are still DBQueue Processor tasks queued in the DBQueue that are prerequisite for installing the database. Once processing is complete, click **Next**.
16. On the last page of the Configuration Wizard, click **Finish**.

Related topics

- Advice on updating the One Identity Manager database on page 115
- Editing the One Identity Manager database while updating with the Configuration Wizard on page 120
- One Identity Manager vendor notification on page 80
- Users and permissions for the One Identity Manager database on an SQL Server on page 26
- Users and permissions for the One Identity Manager database in a manage instance in Azure SQL Database on page 33
- Users and permissions for the One Identity Manager database in Azure SQL Database on page 40
- Error messages when installing and updating the One Identity Manager database on page 174

Editing the One Identity Manager database while updating 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:

1. Prepare the update.

   NOTE: This step is performed only when updating a database that has at least One Identity Manager version 8.2.

   This runs through the various phases for preparing the database update. This step-by-step preparation is intended to ensure that users are informed about the upcoming update and that processes can be terminated in a targeted manner. Alternatively, you can start the database update immediately. This skips the preparation phases.

   These are the phases:

   - Normal operation mode: The database is in normal operating mode. The update process has not yet been initiated.
   - Updating information: All database users are informed about the upcoming update. The system does accept anymore processes. The preparation phase is displayed in the program's status bar.
   - Preparing update: New users cannot log in to the database anymore. All running processes will still be completed. If this is taking a long time, check the Job queue and the DB queue for processes. The preparation phase is displayed in the program's status bar.
   - Running update: The database is ready for updating. The update can start. The preparation phase is displayed in the program's status bar.

2. Updating the One Identity Manager schema.

   Before the schema update, 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. The schema uses the delta method to update. A comparison with the previous version is used to identify and import new, changed and deleted content. If the option to fully repair and verify the supplied default data is enabled, the default data is migrated in full. This procedure usually takes some time.

   When a migration package is imported into a One Identity Manager database, the following operations are carried out:

   - Insert: If the object is not found in the target database, a new object is created with the key values.
   - Update: If the object is found in the target database, the object is updated.
   - Delete: Objects that are no longer needed are deleted from the target database.

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

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

3. 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.

4. 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.

5. Migrating 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.

   NOTE: Synchronization and provisioning processes are deferred until migration is complete. You can adjust the deferral time using the **Common | Jobservice | RedoDelayMinutes** configuration parameter.

6. Finalizing the update.

   Processes queued by the schema update are in the final stage of processing. Finally, the database is switched back to normal operating mode.

Related topics

- Automatic updating of One Identity Manager on page 101
- Displaying the transport history and testing the One Identity Manager version on page 172
- Error messages when installing and updating the One Identity Manager database on page 174

Installing a hotfix in the One Identity Manager database

IMPORTANT: Test changes in a test system before you install a hotfix in a live system.

Hotfix packages contain:

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

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

  NOTE: If other configuration customizations are to be transferred to a One Identity Manager database in addition to a hotfix package, you can create a cumulative transport package to do this and, by using the Database Transporter, import the transport package into the target database.

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

Hotfix packages that contain modified files are deployed as a Zip file. Unpack the Zip file and use the Software Loader to import the modified files into the database. The files are distributed to the workstations and servers by automatic software update. If you do not use automatic software update, update the workstations and servers manually.

Detailed information about this topic

- Displaying the contents of a transport package with the Database Transporter on page 123
- Importing transport packages with the Database Transporter on page 124
- Importing files with the Software Loader on page 126
- Displaying the transport history and testing the One Identity Manager version on page 172
- Automatic updating of One Identity Manager on page 101

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 to the One Identity Manager database.
2. In the **Change & Extend > Change, extend and prepare the data model** section, select the **Transport custom modifications** entry and click **Run**.

   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
     1. Click **+** to select an entry in the transport file and select **Sort in import order** from the context menu.
     2. 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.

3. 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 transport packages with the Database Transporter on page 124

Importing transport packages with the Database Transporter

IMPORTANT: Test changes in a test system before you install a hotfix in a live system.

NOTE:

- Use a copy of the production database for testing.
- You can display the contents of a transport package with the Database Transporter before you import.
- To import transport packages with the Database Transporter, users require the **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 as many existing connections to the database as possible before starting the import. It is not mandatory to close the One Identity Manager Service connections. However, ensure that there are no processes running when the import is going to start.
- 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 to the One Identity Manager database.
2. In the **Change & Extend > Change, extend and prepare the data model** section, select the **Transport custom modifications** entry and click **Run**.

   This starts the Database Transporter program.
3. Select **Import transport file** on the home 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**.
   - **Create an import log file**: Enable this option to create a log file for the data import. The log file is saved in the output directory of the transport file.
   - **Import objects singly and ignore errors**: Enable this option to import objects 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.
   - **Ignore default data differences**: Enable this option to ignore changes to default data. If you do not enable this option, the import procedure is canceled if changes to default data are included.
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.

   NOTE: During import, if the expected value does not match with the actual value in the database, the **Merge conflict** dialog opens. For each conflict, you must decide which value is committed to the database.
   - If you want to keep database value, enable **Current database value**.
   - If you want the value from the transport package to overwrite the database value, enable **Transport value**.
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 123
- Displaying the transport history and testing the One Identity Manager version on page 172

Importing files with the Software Loader

IMPORTANT: Test changes in a test system before you install a hotfix in a live system.

To deploy files

1. Hotfix packages that contain modified files are deployed as a Zip file. Unpack the Zip file in a temporary directory on the administrative workstation.
2. Copy the files to the installation directory on your administrative workstation.

   Make sure that the directory structure is preserved. For example, copy `*.exe` files or `*.dll` files to the `%ProgramFiles%\One Identity\One Identity Manager` directory. Copy the Zip files for Angular projects (`Html_<MMM>.zip`) to the `%ProgramFiles%\One Identity\One Identity Manager\imxweb` directory.
3. Start the Software Loader on the administrative workstation and import the file into the One Identity Manager database.

   NOTE: When you select the root directory in the Software Loader, ensure this does not create any unintended directory trees or delete directories that are still required.

To import files into a One Identity Manager database

1. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Change & Extend > Change, extend and prepare the data model** section, select the **Import files for software update** entry and click **Run**.

   This starts the Software Loader program.
3. Select **Import into database** on the home 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 24: Meaning of the status

State	Meaning
Version unknown	The file belongs to the known files but has not yet been loaded into the database. There is no version information in the database.
Unknown file	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.

State	Meaning
Version OK	The file version matches the version in the database.
Version modified	The file version has changed with respect to the version in the database.

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, development, and production databases.
   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 the files to the machine role.
   b. (Optional) For more file settings, click **...** next to the file names.

Table 25: Other file settings

Setting	Description
Source directory	Path to the installation source directory.
Create backup	A copy must be made of the file during the automatic software update.
No update	The file is not updated by the automatic software update.

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

For more information about the Software Loader, see the *One Identity Manager Operational Guide*.

Related topics

- Automatic updating of One Identity Manager on page 101
- Machine roles and installation packages on page 188

8

Installing additional modules for a existing One Identity Manager installation

To add more One Identity Manager modules to an existing One Identity Manager installation, perform the following steps:

1. Install the One Identity Manager components included in the module on workstations and servers.

   Update the workstation to be used to start the One Identity Manager database schema installation with the installation wizard. All other workstations and servers obtain the new components through automatic software updates. Use the installation wizard to manually update individual workstations and servers.

2. Install the module in the One Identity Manager database.

   IMPORTANT: When a module is post-installed, all other modules in the database are also processed. If support sent you hotfixes for this version, then these hotfixes must also be reinstalled.

   NOTE: It is not recommended to perform an upgrade of the existing modules to a new One Identity Manager version and install additional modules at the same time. This may cause dependencies between modules to be constructed incorrectly. First update the existing modules to the new One Identity Manager version. Then restart the Configuration Wizard and install the additional modules.

   NOTE: If you add more modules, your custom administrative users obtain the permissions for this module.

To install components of a module on the workstation

1. Run the program `autorun.exe` from the root directory on the One Identity Manager installation medium.
2. Switch to the **Installation** section. Select the edition that you installed.
3. Click **Install**.

   This starts the installation wizard.

4. Follow the installation instructions. In the process, note the following:

a. On the **Installation settings** page, enter the following information:
    - **Installation source**: Select the directory containing the installation files.
    - **Installation directory**: Select your current installation directory. Otherwise, the components are not updated and a new installation is created in the second directory instead.
    - **Add further modules to the selected edition**: Enable the option.

b. On the **Module selection** page, select the additional module to install.

c. If you update the workstation that is going to start the One Identity Manager database schema, you can start the Configuration Wizard on the last page of the installation wizard.

To install the module extensions in the One Identity Manager database

1. Start the Configuration Wizard on the administrative workstation.
2. On the Configuration Wizard home page, select the **Update database** option and click **Next**.
3. Follow the installation instructions. In the process, note the following:
    - Configuration modules and version information are shown on the **Product description** page.
        a. Confirm that you have an up-to-date backup of database.
        b. Confirm that the database consistency checks were run.
        c. Set the **Add more modules** option.
    - On the **Select configuration module** page, select the additional module.

Related topics

- Updating One Identity Manager components with the installation wizard on page 112
- Advice on updating the One Identity Manager database on page 115
- Updating the One Identity Manager database with the Configuration Wizard on page 117

9

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.

NOTE: On Linux operating systems, use of oneidentity/oneim-appserver docker images is recommended.

Detailed information about this topic

- Minimum system requirements for application servers on page 47
- Tips for installing an application server on page 131
- Installing application servers on page 132
- Displaying application servers' status on page 136
- Installing or uninstalling a search service for full-text search on page 137
- Updating the search index on application servers on page 138
- Updating application servers on page 139
- Uninstalling application servers on page 140

Tips for installing an application server

Note the following 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 sufficient permissions for a configuration user. Use the SQL login for the configuration user to connect to the

One Identity Manager database and to authenticate 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 that use the SQL 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 **QBM | AppServer | SessionTimeout** configuration parameter to add the timeout in hours, after which inactive application server sessions are closed. The default value is **24** hours. In the Designer, edit the configuration parameter.

Installing application servers

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

NOTE: On Linux operating systems, use of oneidentity/oneim-appserver docker images is recommended.

To install an application server

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:
   a. Change to the **Installation** tab.
   b. In the **Web-based components** section, click **Install**.

   This starts the Web Installer.
3. Select **Install application server** on the Web Installer and click **Next**.
4. On the **Database connection** page, perform the following actions.
   a. To use an existing connection to the One Identity Manager database, select it in the **Select a database connection** drop-down.

      - OR -

      To create a new connection to the One Identity Manager database, click **Add new connection** and enter a new connection.
   b. Under **Authentication method**, specify the method and login data you would like to use.
5. On the **Installation source** page in the **Installation source** section, specify where to find the installation data.
   - To retrieve the installation data from the database, enable the **Database** option.

- To retrieve the installation data from the installation media (for example, from the hard drive), enable the **File system** option and enter the path.

6. Configure the following settings on the **Select setup target** page.

Table 26: Settings for the installation target

Setting	Description
Application name	Enter the name to use in the browser as the application name.
Target in IIS	Select the website on the Internet Information Services where the application is installed.
Enforce SSL	Specifies whether secure or insecure websites are available to install. 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.
URL	Enter the application's URL.
Install dedicated application pool	Enable this option if you want to install a separate application pool 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.
Application pool	Select the application pool to use. This can only be entered if the **Install dedicated application pool** option is not set. If you use the **DefaultAppPool** default value, the application pool has the following syntax: `<application name>_POOL`
Identity	Specify the permissions for implementing the application pool. You can use a default identity or a custom user account. If you use the **ApplicationPoolIdentity** default value, the user account has the following syntax: `IIS APPPOOL\<application name>_POOL` You can authorize another user by clicking **...** next to the box, enabling the option **Custom account** and entering the user and password.
Assign file permissions for application pool identity	Specify whether the identity that the application pool was running with obtains the file permissions.

Setting	Description
Web authentication	Specify which type of authentication to use against the web application. You have the following options: • Windows authentication (single sign-on) The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the identity 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. • 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	NOTE: You can only see this section if you have selected an SQL database connection on the **Database connection** page. Specify which type of authentication to use 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 Authentication is completed using an SQL login and password. The SQL login used is from the database connection. Use the [**...**] button to enter a different SQL login, for example, if the application is run with a access level for end users. This access data is saved in the web application configuration as computer specific encrypted.

7. 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.

8. On the **Set session token certificate** page, select the certificate for creating and checking session tokens.

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

   - To use an existing certificate, set the following:
     1. **Session token certificate**: Select the `Use existing certificate` entry.
     2. **Select certificate**: Select the certificate.

        NOTE: It is strongly recommended to use the certificate already in use in other application servers and API Servers.

     3. **Show invalid certificates too**: (Optional) Enable this option to show other certificates.
   - To create a new certificate, set the following:
     1. **Session token certificate**: Select the `Create new certificate` entry.
     2. **Certificate issuer**: Enter the issuer of the certificate.
     3. **Key length**: Specify the key length for the certificate.

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

     NOTE: It is strongly recommended to export this newly created certificate and use it in other application servers and API Servers as well, so that all these server components have and use the identical session certificate.
   - To create a new certificate file, set the following:
     1. **Session token certificate**: Select the `Generate new certificate file` entry.
     2. **Certificate issuer**: Enter the issuer of the certificate.
     3. **Key length**: Specify the key length for the certificate.
     4. **Certificate file**: Enter the directory path and name of the certificate file.

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

     NOTE: It is strongly recommended to use this newly created certificate in other application servers and API Servers as well, so that all these server components have and use the identical session certificate.
9. 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 run 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.
10. (Optional) The One Identity Manager History Database is used to provide archived data for analyzing in reports and the TimeTrace. If you access the One Identity Manager History Database is through an application server, on the **Edit History Database connections** page, enter the One Identity Manager

History Database ID and the connection parameters.

NOTE: You can enter the One Identity Manager History Database's connection parameters at a later date. Use the `appsettings.json` configuration file to do this.

For more information about connecting to the One Identity Manager History Database through an application server and the required configuration, see the *One Identity Manager Data Archiving Administration Guide*.

11. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
12. Click **Finish** on the last page to end the program.
13. Close the autorun program.

NOTE: The Web Installer generates both the web application and the `appsettings.json` configuration file. The Web Installer uses default values for the configuration settings. You can keep these values but it is recommended you check the settings. You will find the `appsettings.json` configuration file in the web application installation directory in the Internet Information Services.

Related topics

- Minimum system requirements for application servers on page 47
- Tips for installing an application server on page 131
- Displaying application servers' status on page 136
- Installing or uninstalling a search service for full-text search on page 137
- Updating application servers on page 139
- Users and permissions for the One Identity Manager database on an SQL Server on page 26
- Machine roles and installation packages on page 188

Displaying application servers' 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>

TIP: You can open the web server's status display in the Job Queue Info. In the 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 **AppServer_Logs** program function see the log.

In addition, API documentation is available here. To access the REST API in the application server, users require the **AppServer_API** program function. For more information about the REST API, see the *One Identity Manager REST API Reference Guide*

Installing or uninstalling a search service for full-text search

To use the Web Portal or full-text search in the Manager, you need an application server with a search service installed on it. You usually set up the machine roles for search indexing for full-text search when you install an application server.

If necessary, you can install the machine roles at a later date. If necessary you can uninstall the machine roles again. Customize the application server installation.

To install the search server on an application server at a later date

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:
   a. Click **Installation**.
   b. In the **Web-based components** pane, click **Install**.

   Starts the Web Installer.
3. On the Web Installer home page, click **Modify application server installation** and click **Next**.
4. On the **Installation source** page, select the application server instance that you want to customize.
5. On the **Database connection** page, select the database connection and authentication method.
6. On the **Assign machine roles** page, enable the **Search Service** and **Search Indexing Service** machine roles.
7. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
8. Click **Finish** on the last page to end the program.
9. Close the autorun program.

To uninstall the search server on an application server

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:

a. Click **Installation**.

b. In the **Web-based components** pane, click **Install**.

Starts the Web Installer.

3. On the Web Installer home page, click **Modify application server installation** and click **Next**.
4. On the **Installation source** page, select the application server instance that you want to customize.
5. On the **Database connection** page, select the database connection and authentication method.
6. On the **Assign machine roles** page, disable the **Search Service** and **Search Indexing Service** machine roles.
7. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
8. Click **Finish** on the last page to end the program.
9. Close the autorun program.

Related topics

- Installing application servers on page 132
- Updating the search index on application servers on page 138

Updating the search index on application servers

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

The **Common | Indexing | Interval** configuration parameter 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-in user, click **Update Index**.
3. Select one of the following options:
   - **All values**: Updates all indexes.
   - **Only changed values**: Only updates changed indexes.
   - **Optimize index**: Optimizes the search index.

Related topics

- Displaying application servers' status on page 136
- Log message for search index creation on page 180

Updating application servers

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 **Replace a process level token** and **Adjust memory quotas for a process** local security policies.

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 depends on the selected mode for automatic update. 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.

Configure the automatic update in the application server's `appsettings.json` configuration file. You can use the `AutoUpdate` configuration settings to control the update behavior.

Table 27: Configuration settings for automatic update

Setting	Description
Off	Specifies whether automatic update is disabled (**`true`**) or enabled (**`false`**).
Mode	Mode for automatic update. Permitted values are: • **`timer`**: Scheduled checking. At application start up, a check for updated files in the database is carried out and afterward, at scheduled intervals (`checkinterval` setting). • **`manual`**: Manual checking. You start the check from the application server's status page. Regular checking if updated files

Setting	Description
	in the database does not take place. Default value: **timer**
CheckInterval	Time period for search for update in **timer** mode. Default value: **5** minutes
InactivityTime	Time period without user activity so that the update can be started. Default value: **10** seconds

Example: Entry for automatic updating of an application server in the appsettings.json configuration file

```
"AutoUpdate": {
      // "Off": true,
      "Mode": "timer", // Valid options: timer, manual
      "CheckInterval": "00:05:00",
      "InactivityTime": "00:00:10"
}
```

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 application servers' status on page 136
- Automatic updating of One Identity Manager on page 101

Uninstalling application servers

Perform the following steps to uninstall the 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. Change to the **Installation** tab.

b. In the **Web-based components** pane, click **Install**.

This starts the Web Installer.

3. On the Web Installer start page, click **Uninstall a web application** and click **Next**.
4. On the **Uninstall a web application** page, double-click the application that you want to remove.

   The  icon is displayed in front of the application.
5. Click **Next**.
6. On the **Database connection** page, select the database connection and authentication method and enter the corresponding login data.
7. Click **Next**.
8. Confirm the security prompt with **Yes**.
9. The uninstall progress is displayed on the **Setup is running** page.
10. Once installation is complete, click **Next**.
11. On the **Wizard complete** page, click **Finish**.
12. Close the autorun program.

10

Installing and updating an API Server

The API Server deploys the Web Portal, the Password Reset Portal, the Administration Portal as well as the Operations Support Web Portal and your HTML5 web applications. It also provides an API.

You can install the API Server with help from the Web Installer or the ImxClient command line program (the **install-apiserver** command). Read through the following sections for instructions on how to install the API Server on a Web Installer using the Windows Server and set it up with the default configuration. For more information about installing with the ImxClient command line program, see the *One Identity Manager API Development Guide*.

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

NOTE: On Linux operating systems, use of oneidentity/oneim-api docker images is recommended.

Detailed information about this topic

- Minimum system requirements for API Servers on page 45
- Installing the API Server on page 143
- Displaying an overview of HTML web applications on page 149
- API Servers for configuring load balancing on page 149
- Installing or uninstalling the SCIM plugin on page 150
- Modifying authentication data for API Server projects on page 151
- Adjusting IIS request limits for the API Server on page 153
- Updating API Servers on page 154
- Uninstalling API Server on page 156

Installing the API Server

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

NOTE: On Linux operating systems, use of oneidentity/oneim-api docker images is recommended.

To install the API Server

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:
   a. Click **Installation**.
   b. In the **Web-based components** pane, click **Install**.

   This starts the Web Installer.
3. On the start page of the Web Installer, click **Install API Server** and click **Next**.
4. On the **Database connection** page, do the following.

   TIP: One Identity recommend establishing a connection via an application server.

   a. To use an existing connection to the One Identity Manager database, select it in the **Select a database connection** drop-down.

      - OR -

      To create a new connection to the One Identity Manager database, click **Add new connection** and enter a new connection.

   b. Under **Authentication method**, specify the method and login data you would like to use.
5. On the **Installation source** page in the **Installation source** pane, specify where to find the installation data.
   - To retrieve the installation data from the database, activate the **Database** option.
   - to retrieve the installation data from the installation media (for example, from the hard drive), activate the **File system** option and enter the path.
6. On the **Installation source** page, in the **Additional connections** section, enter any additional information for authentication. This displays the number of connections that can be configured.
   a. To configure additional authentication data, click .
   b. In the **Authentication data** dialog, select the project you want to authenticate and enter the authentication data.

      NOTE: You can also configure the authentication data for optional projects at a later date. You must enter authentication data if the project is marked in red.

- **Multi-factor authentication with OneLogin (OneLogin)**: Multi-factor authentication with OneLogin can be used for specific security-critical actions in One Identity Manager. For more information, see the *One Identity Manager Web Application Configuration Guide*.

  Enter the authentication data for logging in to the OneLogin domain.

  - **Connection string**: Connection string for logging in to the OneLogin domain.

    Syntax:
    `Domain=<domain>;ClientId=<clientid>;ClientSecret=<clientSecret>`

    - OR -

  - **Domain**: Enter the DNS name of the synchronized OneLogin domain.

    Example: `<your domain>.onelogin.com`

  - **Client ID**: Enter the client ID with which the application is registered in OneLogin. You obtain the client ID when you register your application with OneLogin.
  - **Client secret**: Enter the security token for the OneLogin application. You obtain the client secret when you register your application with OneLogin.

- **Authentication for self-registration of new users (sub:register)**: For self-registration of new users in the Password Reset Portal, a user is required with which the new user accounts are created.

  NOTE: It is recommended to use the **IdentityRegistration** system user. This system user has the specified permissions required for self-registration of new users in the Password Reset Portal.

  If you have your own system user, ensure that it has the necessary permissions. For more information about system users and permissions, see the *One Identity Manager Authorization and Authentication Guide*.

  - If you use the **IdentityRegistration** system user, enter a password for the system user.
  - If you want to use your own system user, under **Authentication method**, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

c. To test the data, click **Test connection**.

d. To accept the data, click **OK**.

7. Configure the following settings on the **Select setup target** page.

Table 28: Settings for the installation target

Setting	Description
Application name	Enter the name to use in the browser as the application name.
Target in IIS	Select the website on the Internet Information Services where the application is installed.
Enforce SSL	Specifies whether secure or insecure websites are available to install. 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.
URL	Enter the application's URL.
Install dedicated application pool	Enable this option if you want to install a separate application pool 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.
Application pool	Select the application pool to use. This can only be entered if the **Install dedicated application pool** option is not set. If you use the **DefaultAppPool** default value, the application pool has the following syntax: `<application name>_POOL`
Identity	Specify the permissions for implementing the application pool. You can use a default identity or a custom user account. If you use the **ApplicationPoolIdentity** default value, the user account has the following syntax: `IIS APPPOOL\<application name>_POOL` You can authorize another user by clicking **...** next to the box, enabling the option **Custom account** and entering the user and password.
Assign file permissions for application pool identity	Specify whether the identity that the application pool was running with obtains the file permissions.
Overwrite default IIS request limits	Specify whether the default IIS values for the URL length, query string length, and content length are overwritten. If the values are not adequate, IIS returns an HTTP 404 error. For more information, see HTTP 404 Error Substatus Codes.

Setting	Description
	Adjust the values to suit your requests if necessary. • **Max. URL length [B]**: Maximum length if a URL in bytes. The default value is **4096** bytes. • **Max. query string length [B]**: Maximum length of a query string in bytes. The default value is **32768 bytes**. • **Max. content length [B]**: Maximum length of content in bytes. The efault value is **30000000 bytes**. NOTE: You can configure these values at a later date.
Web authentication	Specify which type of authentication to use against the web application. You have the following options: • Windows authentication (single sign-on) The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the identity 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. • 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	NOTE: You can only see this section if you have selected an SQL database connection on the **Database connection** page. Specify which type of authentication to use 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 Authentication is completed using an SQL login and password. The SQL login used is from the database connection. Use the [**...**] button to enter a different SQL login, for example, if the application is run with a access

Setting	Description
	level for end users. This access data is saved in the web application configuration as computer specific encrypted.

8. On the **Select application server** page, perform the following actions.

   NOTE: This page only shown if you have selected a direct database connection.

   NOTE: If you would like to use the full-text search, then you must specify an application server.

   a. Click **Select application server**.

   b. In the dialog, in the **URL** field, enter the web address of the application server that is running the search service for full-text search.

   c. Click **OK**.

9. On the **Set session token certificate** page, select the certificate for creating and checking session tokens.

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

   - To use an existing certificate, set the following:
     1. **Session token certificate**: Select the **`Use existing certificate`** entry.
     2. **Select certificate**: Select the certificate.

        NOTE: It is strongly recommended to use the certificate already in use in other application servers and API Servers.

     3. **Show invalid certificates too**: (Optional) Enable this option to show other certificates.
   - To create a new certificate, set the following:
     1. **Session token certificate**: Select the **`Create new certificate`** entry.
     2. **Certificate issuer**: Enter the issuer of the certificate.
     3. **Key length**: Specify the key length for the certificate.

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

     NOTE: It is strongly recommended to export this newly created certificate and use it in other application servers and API Servers as well, so that all these server components have and use the identical session certificate.
   - To create a new certificate file, set the following:
     1. **Session token certificate**: Select the **`Generate new certificate file`** entry.
     2. **Certificate issuer**: Enter the issuer of the certificate.
     3. **Key length**: Specify the key length for the certificate.
     4. **Certificate file**: Enter the directory path and name of the certificate file.

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

NOTE: It is strongly recommended to use this newly created certificate in other application servers and API Servers as well, so that all these server components have and use the identical session certificate.

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

    The **SCIM Provider** machine role is required for the SCIM plug-in in the API Server. For more information about the SCIM plug-in, see the *One Identity Manager Configuration Guide*.

    NOTE: You can configure the SCIM plug-in at a later date.

11. 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.

12. On the **Application token** page, enter the application token for the API Server into the input field. The application token is required by the Password Reset Portal.

    NOTE: Handle the application token like a password. Once the application is saved in the database, it cannot be displayed in text form again. Make a note of the application token if necessary.

    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, note that the current token will become invalid and every location that uses it must be updated with the new token.

13. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
14. On the **Wizard complete** page, click **Finish**.
15. Close the autorun program.

Related topics

- Minimum system requirements for API Servers on page 45
- Installing or uninstalling the SCIM plugin on page 150
- Modifying authentication data for API Server projects on page 151
- Adjusting IIS request limits for the API Server on page 153
- Uninstalling API Server on page 156

Displaying an overview of HTML web applications

The API Server deploys the Web Portal, the Password Reset Portal, as well as the Operations Support Web Portal and an Administration Portal.

To access all installed HTML applications

- In a web browser, open the web address (URL) of your API Server.

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

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

  All HTML applications are displayed in the web application overview. You can launch several web applications from here.

In the Administration Portal, you obtain an overview of the status of the API Server, the configuration, and can view the logs. You can configure the API server and its API projects in the Administration Portal and display the information. For more information, see the *One Identity Manager Web Application Configuration Guide*.

Related topics

- Installing the API Server on page 143

API Servers for configuring load balancing

An API Server can be configured as part of an application pool and participate in load balancing.

Prerequisites for load balancing

- All API Servers that participate in load balancing must be configured with the same certificate when they are installed.

  With this certificate, all API Servers from the application pool can encrypt and decrypt their data securely. When changing API Servers, another API Server can restore the session so that web application users can work seamlessly. You set the certificate in the **Set session token certificate** step when you install the API server.

  NOTE: This certificate is independent of the certificate used for SSL.

- For the best possible performance, the load balancing must support session bindings (sticky sessions). All HTTP requests in a session should be routed to the same API Server, because rebuilding a session leads to performance issues.

Related topics

- Installing the API Server on page 143

Installing or uninstalling the SCIM plugin

For more information about SCIM plugin, see the *One Identity Manager Configuration Guide*.

The SCIM 2.0 service provider for One Identity Manager is provided as a plugin for the API Server. You usually set up the machine role for the SCIM plugin when installing a API Server.

If necessary, you can install the machine role at a later date. Uninstall the machine roles again as required. Customize the API Server installation.

To install the SCIM plugin on an API Server at a later date

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:
   a. Click **Installation**.
   b. In the **Web-based components** pane, click **Install**.

   This starts the Web Installer.
3. On the Web Installer start page, click **Modify API Server installation** and click **Next**.
4. On the **Installation source** page, select the API Server instance that you want to customize.
5. On the **Database connection** page, select the database connection and authentication method.
6. On the **Assign machine roles** page, enable the **SCIM Provider** machine role.
7. (Optional) In the **Installation source** page, change the connection settings.
8. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
9. Click **Finish** on the last page to end the program.
10. Close the autorun program.

To uninstall the SCIM plugin on an API Server at a later date

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.

2. On the installation wizard's home page, perform the following actions:
    a. Click **Installation**.
    b. In the **Web-based components** pane, click **Install**.

    Starts the Web Installer.
3. On the Web Installer start page, click **Modify API Server installation** and click **Next**.
4. On the **Installation source** page, select the API Server instance that you want to customize.
5. On the **Database connection** page, select the database connection and authentication method.
6. On the **Assign machine roles** page, disable the **SCIM provider** machine role.
7. (Optional) In the **Installation source** page, change the connection settings.
8. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
9. Click **Finish** on the last page to end the program.
10. Close the autorun program.

Related topics

- Installing the API Server on page 143
- Modifying authentication data for API Server projects on page 151
- Adjusting IIS request limits for the API Server on page 153

Modifying authentication data for API Server projects

Normally, you enter the authentication data for projects when you install an API Server. But it possible to configure the authentication data for optional projects at a later date.

To add authentication data at a later date

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:
    a. Click **Installation**.
    b. In the **Web-based components** pane, click **Install**.

    Starts the Web Installer.

3. On the Web Installer start page, click **Modify API Server installation** and click **Next**.
4. On the **Installation source** page, select the API Server instance that you want to modify.
5. On the **Database connection** page, select the database connection and authentication method.
6. (Optional) On the **Assign machine roles** page, alter the usage of the **SCIM Provider** machine role.
7. On the **Installation source** page, in the **Additional connections** section, enter any additional information for authentication. This displays the number of connections that can be configured.
    a. To configure additional authentication data, click .
    b. In the **Authentication data** dialog, select the project you want to authenticate and enter the authentication data.
        - **Multi-factor authentication with OneLogin (OneLogin)**: Multi-factor authentication with OneLogin can be used for specific security-critical actions in One Identity Manager. For more information, see the *One Identity Manager Web Application Configuration Guide*.

          Enter the authentication data for logging in to the OneLogin domain.
            - **Connection string**: Connection string for logging in to the OneLogin domain.

              Syntax:
              `Domain=<domain>;ClientId=<clientid>;ClientSecret=<clientSecret>`

              - OR -
            - **Domain**: Enter the DNS name of the synchronized OneLogin domain.

              Example: `<your domain>.onelogin.com`
            - **Client ID**: Enter the client ID with which the application is registered in OneLogin. You obtain the client ID when you register your application with OneLogin.
            - **Client secret**: Enter the security token for the OneLogin application. You obtain the client secret when you register your application with OneLogin.
        - **Authentication for self-registration of new users (sub:register)**: For self-registration of new users in the Password Reset Portal, a user is required with which the new user accounts are created.

          NOTE: It is recommended to use the **IdentityRegistration** system user. This system user has the specified permissions required for self-registration of new users in the Password Reset Portal.

If you have your own system user, ensure that it has the necessary permissions. For more information about system users and permissions, see the *One Identity Manager Authorization and Authentication Guide*.

- If you use the **IdentityRegistration** system user, enter a password for the system user.
- If you want to use your own system user, under **Authentication method**, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

c. To test the data, click **Test connection**.

d. To accept the data, click **OK**.

8. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
9. Click **Finish** on the last page to end the program.
10. Close the autorun program.

Related topics

- Installing and updating an API Server on page 142
- Installing or uninstalling the SCIM plugin on page 150
- Adjusting IIS request limits for the API Server on page 153

Adjusting IIS request limits for the API Server

Normally, you specify whether the default IIS values for the URL length, query string length, and content length are overwritten during the API Server installation.

But it is also possible to configure the settings at a later date.

If the values are not adequate, IIS returns an HTTP 404 error. For more information, see HTTP 404 Error Substatus Codes.

To adjust the IIS request limits later

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. On the installation wizard's home page, perform the following actions:

a. Click **Installation**.

b. In the **Web-based components** pane, click **Install**.

Starts the Web Installer.

3. On the Web Installer start page, click **Modify API Server installation** and click **Next**.
4. On the **Installation source** page, select the API Server instance that you want to customize.
5. On the **Database connection** page, select the database connection and authentication method.
6. (Optional) On the **Assign machine roles** page, alter the usage of the **SCIM Provider** machine role.
7. On the **Installation source** page, enable the **Overwrite default IIS request limits** option and change the values as required.
   - **Max. URL length [B]**: Maximum length if a URL in bytes. The default value is `4096` bytes.
   - **Max. query string length [B]**: Maximum length of a query string in bytes. The default value is `32768 bytes`.
   - **Max. content length [B]**: Maximum length of content in bytes. The efault value is **30000000 bytes**.
8. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.
9. Click **Finish** on the last page to end the program.
10. Close the autorun program.

Related topics

- Installing and updating an API Server on page 142
- Installing or uninstalling the SCIM plugin on page 150
- Modifying authentication data for API Server projects on page 151

Updating API Servers

NOTE: Best practice is to perform automatic updates within special maintenance windows in which the application is not accessible by users and the application can be restarted manually without risk.

The following permissions are required to automatically update an IIS installation of the API Server:

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

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 update process differs depending on how the API Server is run:

- Running on the IIS: The API Server automatically checks for updates on a regular basis. If updates are available, the API Server starts the update process. The API Server then restarts itself.
- Running as a Docker container: As soon as the Docker container starts, the update starts. If updates become available during operation, the Docker container shuts down. You must then restart the Docker container either manually or using a container orchestration program.
- Running from the ImxClient command line program: The API Server does not load updates independently. To install updates, you must restart the command line program manually.

To enable or disable automatic updates for a web application

1. Start the Designer program.
2. Connect to the relevant database.
3. Navigate to **Base data** > **Security settings** > **Web server configurations**.
4. In the List Editor, select the corresponding web application.
5. Perform one of the following actions:
    - To enable automatic updates, set the **Auto update level** to `active`.
    - To disable automatic updates, set the **Auto update level** to `inactive`.
6. Commit the changes.

Related topics

- Automatic updating of One Identity Manager on page 101

Uninstalling API Server

Perform the following steps to uninstall the 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. Change to the **Installation** tab.
   b. In the **Web-based components** pane, click **Install**.

   This starts the Web Installer.
3. On the Web Installer start page, click **Uninstall a web application** and click **Next**.
4. On the **Uninstall a web application** page, double-click the application that you want to remove.

   The  icon is displayed in front of the application.
5. Click **Next**.
6. On the **Database connection** page, select the database connection and authentication method and enter the corresponding login data.
7. Click **Next**.
8. Confirm the security prompt with **Yes**.
9. The uninstall progress is displayed on the **Setup is running** page.
10. Once installation is complete, click **Next**.
11. On the **Wizard complete** page, click **Finish**.
12. Close the autorun program.

Related topics

- Installing the API Server on page 143

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 web servers on page 48
- Installing the Manager web application on page 157
- Manager web application update on page 161
- Uninstalling Manager web applications on page 162
- Advanced configuration of the Manager web application on page 181

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, they are automatically diverted to the web application that matches their 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. On the installation wizard's home page, perform the following actions:

a. Change to the **Installation** tab.

b. In the **Web-based components** section, click **Install**.

Starts the Web Installer.

3. On the start page of the Web Installer, select **Install Manager web application** and click **Next**.
4. On the **Database connection** page, do the following:

   TIP: It is recommended to establish a connection through the application server.

   a. To use an existing connection to the One Identity Manager database, select it in the **Select a database connection** drop-down.

      - OR -

      To create a new connection to the One Identity Manager database, click **Add new connection** and enter a new connection.

   b. Under **Authentication method**, specify the method and login data you would like to use.
5. On the **Installation source** page in the **Installation source** section, specify where to find the installation data.
   - To retrieve the installation data from the database, activate the **Database** option.
   - to retrieve the installation data from the installation media (for example, from the hard drive), activate the **File system** option and enter the path.
6. Configure the following settings on the **Select setup target** page.

Table 29: Settings for the installation target

Setting	Description
Application name	Enter the name to use in the browser as the application name.
Target in IIS	Select the website on the Internet Information Services where the application is installed.
Enforce SSL	Specifies whether secure or insecure websites are available to install. 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.
URL	Enter the application's URL.
Install dedicated applic-	Enable this option if you want to install a separate application pool for each application. This allows applications to be set up

Setting	Description
ation pool	independently of one another. If this option is set, each application is installed in its own application pool.
Application pool	Select the application pool to use. This can only be entered if the **Install dedicated application pool** option is not set. If you use the **DefaultAppPool** default value, the application pool has the following syntax: `<application name>_POOL`
Identity	Specify the permissions for implementing the application pool. You can use a default identity or a custom user account. If you use the **ApplicationPoolIdentity** default value, the user account has the following syntax: `IIS APPPOOL\<application name>_POOL` You can authorize another user by clicking **...** next to the box, enabling the option **Custom account** and entering the user and password.
Assign file permissions for application pool identity	Specify whether the identity that the application pool was running with obtains the file permissions.
Web authentication	Specify which type of authentication to use against the web application. You have the following options: • Windows authentication (single sign-on) The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the identity 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. • 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	NOTE: You can only see this section if you have selected an SQL database connection on the **Database connection** page. Specify which type of authentication to use against the One Identity Manager database. You have the following options:

Setting	Description
	• 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 Authentication is completed using an SQL login and password. The SQL login used is from the database connection. Use the [**...**] button to enter a different SQL login, for example, if the application is run with a access level for end users. This access data is saved in the web application configuration as computer specific encrypted.

7. Specify other application specific settings on the **Configuration** page.
   a. Select the language of the application from the **Language** drop-down. The language influences how dates and numbers displayed amongst other things.
   b. The web application requires access permissions to itself. If you selected the **Windows authentication (single sign-on)** authentication type as web authentication, enter the domain, user account, and password for the user. For anonymous web authentication, no further entries are required.
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 run 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. Once installation is complete, click **Next**.
10. Click **Finish** on the last page to end the program.

NOTE: The Web Installer generates both the web application and the `appsettings.json` configuration file. 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 App Configuration Editor. You will find the `appsettings.json` configuration file in the web application installation directory in the Internet Information Services.

Related topics

- Manager web application update on page 161
- Advanced configuration of the Manager web application on page 181

Displaying the Manager web application

The Manager web application is accessed over a browser.

Use the appropriate URL for this:

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

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

Manager web application update

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

The application update happens automatically if the **Auto update** plug-in 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 101
- Advanced configuration of the Manager web application on page 181

Uninstalling Manager web applications

Perform the following steps to uninstall the 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. Change to the **Installation** tab.
   b. In the **Web-based components** pane, click **Install**.

   This starts the Web Installer.
3. On the Web Installer start page, click **Uninstall a web application** and click **Next**.
4. On the **Uninstall a web application** page, double-click the application that you want to remove.

   The  icon is displayed in front of the application.
5. Click **Next**.
6. On the **Database connection** page, select the database connection and authentication method and enter the corresponding login data.
7. Click **Next**.
8. Confirm the security prompt with **Yes**.
9. The uninstall progress is displayed on the **Setup is running** page.
10. Once installation is complete, click **Next**.
11. On the **Wizard complete** page, click **Finish**.
12. Close the autorun program.

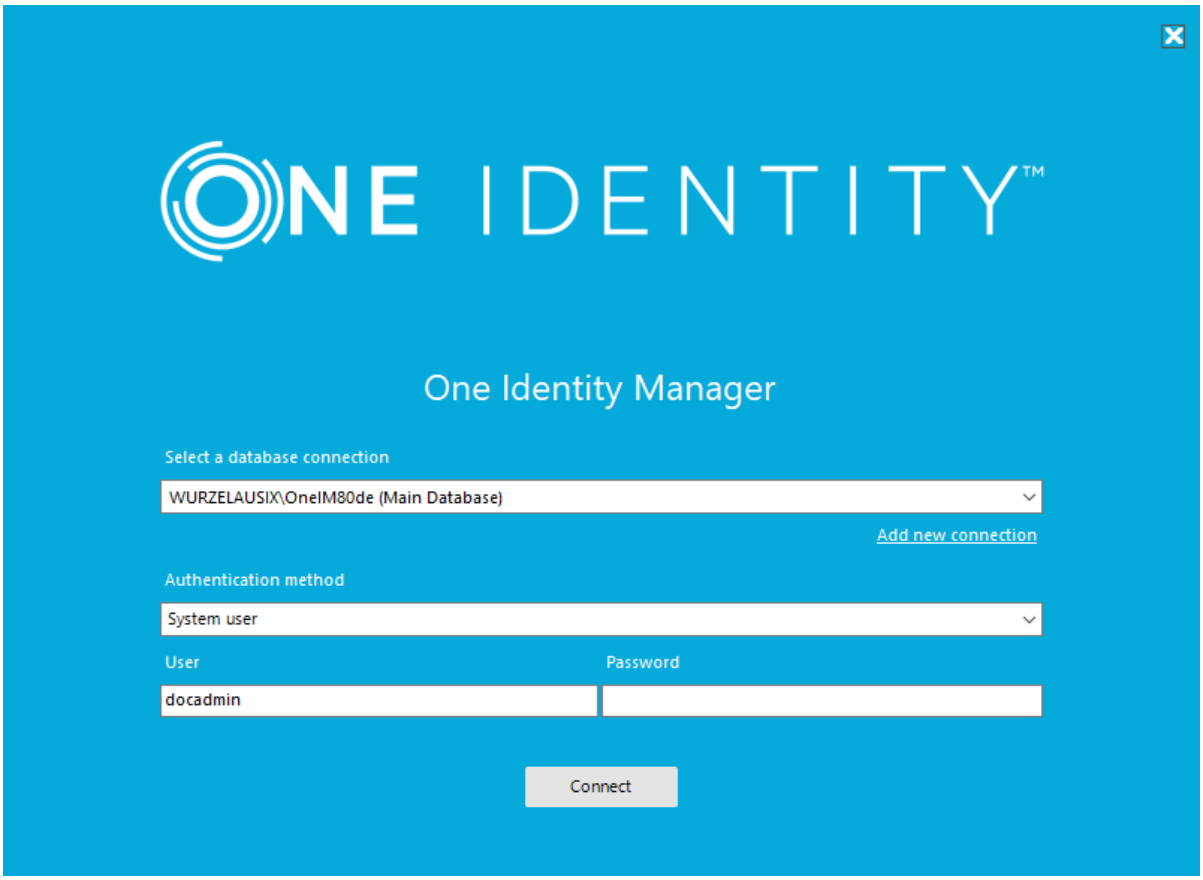
12

Logging in to One Identity Manager tools

NOTE: One Identity Manager tools can only be started if the user has the relevant program functions. For more information about program functions, see the *One Identity Manager Authorization and Authentication Guide*.

When you start one of the One Identity Manager tools, a default connection dialog opens. This tries to restore the last used connection.

Figure 5: Default connection dialog



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:

1. Selecting the database connection to log in to the database

   You can login to the database via an application server or a direct connection to the database.

2. 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.

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

   NOTE: Use non role-based authentication modules to log in to the Designer. Role-based authentication modules for logging in to the Designer are not supported.

Detailed information about this topic

- Setting up new logins via the application server on page 164
- Setting up new logins via direct connection to the database on page 166
- Selecting and editing existing login connections on page 167
- Enabling additional authentication modules on page 168
- Enabling other login languages on page 169
- Checking authentication on page 170
- Password expiry on page 170

Setting up new logins via the application server

Perform the following steps if you want to log in via an application server.

To establish a new connection to the database via an application server

1. Start a One Identity Manager tool, such as the Manager, from the install directory.

   This opens the connection dialog.

2. In the connection dialog, under **Select a database connection**, click **Add new connection** and select the **Application server** system type.

3. Click **Next**.
4. Enter the address (URL) for the application server.
5. 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 the server name next to the URL, you can get information about the 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 is 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 the **Accept self-signed certificate** option.
6. 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 options** item, you can make additional changes to the connection configuration.
7. Click **Finished**.
8. In the connection dialog, under **Authentication method**, select the authentication module.

    This displays a list of all available authentication modules.
9. Enter the login data for the system user ID.

    The login data required depends on which authentication module you select.
10. Click **Connect**.

NOTE: The connection is saved and made available for the next login.

Related topics

- Setting up new logins via direct connection to the database on page 166
- Selecting and editing existing login connections on page 167

Setting up new logins via direct connection to the database

Perform the following steps if you want to set up a log in via a direct connection to the database.

To create a new connection to the database

1. Start a One Identity Manager tool, such as the Database Compiler, from the install directory.

   This opens the connection dialog.
2. In the connection dialog, under **Select a database connection**, click **Add new connection** and select the **SQL Server** system type.
3. Click **Next**.
4. Enter the connection data for the database server.
   - **Server**: Database server.
   - **Windows authentication**: (Optional) Specifies whether the 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**: User's SQL login name.
   - **Password**: Password for the SQL user's login.
   - **Database**: List of possible databases on the database server. Select the database.
   - **Encrypt communication**: Specifies whether encryption is required for exchanging data between the client and server. Select the minimum encryption level. The encryption level that is actually used depends on the database server configuration. For more information, see the documentation from Microsoft.

     Permitted values are:
     - `Optional`: Communication is not encrypted.
     - `Mandatory`: Data exchange is encrypted. The **Trust server certificate** option, allows you to also specify whether to verify the server certificate.
     - `Strict (SQL Server 2022 and Azure SQL)`: The data exchange is encrypted. The server certificate is always verified.
   - **Trust server certificate**: If this option is enabled, the data exchange between the client and server is encrypted. However, the server certificate is not verified.
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 options** item, you can make additional changes to the connection configuration.

6. Click **Finished**.
7. In the connection dialog, under **Authentication method**, select the authentication module.

   This displays a list of all available authentication modules.
8. Enter the login data for the system user ID.

   The login data required depends on which authentication module you select.
9. Click **Connect**.

NOTE: The connection is saved and made available for the next login.

Related topics

- Selecting and editing existing login connections on page 167
- Setting up new logins via the application server on page 164

Selecting and editing existing login connections

NOTE: Newly created connections are not shown in the connection dialog until the program has been restarted.

NOTE: Connections that do not use the expected access level for SQL logins are not shown in the connection dialog. The access level for an existing connection is shown in the menu item's tooltip. For more information about the minimum access levels of One Identity Manager tools, see the *One Identity Manager Authorization and Authentication Guide*.

NOTE: When you start the program, it tries to restore the last used connection. This may 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"
```

To select an existing login connection

1. Start a One Identity Manager tool, such as the Manager, from the install directory.

   This opens the connection dialog.
2. In the connection dialog, select the connection under **Select a database connection**.

3. In the connection dialog, under **Authentication method**, select the authentication module.

   This displays a list of all available authentication modules.
4. Enter the login data for the system user ID.

   The login data required depends on which authentication module you select.
5. Click **Connect**.

To delete a connection in the connection dialog

1. In the connection dialog, select the connection under **Select database connection**.
2. Press **DEL**.
3. Confirm the security prompt with **Yes**.

   The connection is no longer shown in the connection dialog.

To delete an SQL Server from the server list in the connection dialog

1. In the connection dialog, under **Select a database connection**, click **Add new connection** and select the **SQL Server** system type.
2. Click **Next**.
3. Open the **Server** drop-down and mark the server you want to delete.
4. Press the **Del** key.
5. Confirm the security prompt with **Yes**.

   This removes the SQL Server from the list.

Enabling additional authentication modules

To use an authentication module for logging in, you must enable the authentication module. Perform the following steps to enable an authentication module.

To enable an authentication module

1. In the Designer, select the **Base data > Security settings > Authentication modules** category.
2. In the List Editor, select the authentication module.
3. In the **Properties** view, set the **Activated** property to `True`.
4. Select the **Database > Save to database** and click **Save**.

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

Language settings in One Identity Manager

The default One Identity Manager installation is supplied in the **English - United States [en-US]** and **German - Germany [de-DE]** language. 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 Language Editor in the Designer 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.

In the ideal case, 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 in to 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 user's tools. 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 is 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 169

Enabling other login languages

Any language for which the **Select in front-end** option is activated can be used as a login language. Perform the following steps to enable a login language.

To enable an additional login language

1. In the Designer, select the **Base data > Localization > Languages** category.
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.
5. Select the **Database > Save to database** and click **Save**.

Related topics

- Language settings in One Identity Manager on page 169

Password expiry

There are different ways to inform users 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 identity-based authentication modules, the system sends reminder notifications in relation to expiring passwords as of seven 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 **Identity - system user password expires** mail template. You can adjust the schedule and mail template in the 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 with next action on the connection after a fixed interval of 20 minutes.

You can adjust the interval in the **Common | Authentication | CheckInterval** configuration parameter. In the Designer, edit the configuration parameter.

- 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 **Common | Authentication | SessionsPerUserAndMinute** configuration parameter. In the Designer, edit the configuration parameter.

- Use the **QBM | AppServer | SessionTimeout** configuration parameter to add the timeout in hours, after which inactive application server sessions are closed. The default value is **24** hours. In the Designer, edit the configuration parameter.

Connection pool for separate sessions for reading and writing on different database servers

To be able to use separate session for reading and writing to different databases servers, you need to adjust the connection data of the **Data Source** property.

The **Data Source** property can contain a pipe (|) delimited server list. The first server specified is the primary server used for write access. All other servers are read-only copies with read access only. The prerequisite for this is that the database name and the credentials on the secondary servers are identical to the primary server.

NOTE: In the connection dialog you can reach the property through the **Options > Advanced options** setting.

The internal physical read sessions are distributed randomly over the read-only copies and the primary server. With one primary server and two secondary servers, the primary server receives approximately 1/3 of the connections for read operations.

NOTE: The connection pool does not open a new connection for each operation. If no new parallel requests come, all requests run over the same connection and therefore on the same server.

The procedure relies on replication taking place between the servers and the data always being up to date in the copies as well.

Related topics

- Setting up new logins via direct connection to the database on page 166

13

Troubleshooting

For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.

Displaying the transport history and testing 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 the Designer and select the **Help > Transport history** menu item.

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

To obtain an overview of the system configuration

- Start the Designer or the Manager and select the **Help > Info** menu item.

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

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

Related topics

- One Identity Manager vendor notification on page 80

Error messages logging in to One Identity Manager tools

Problem

When logging in to 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 user account used for the login is locked.
- The identity used to log in is temporarily or permanently deactivated.
- The identity used for log in is classified as a security threat.

Possible solutions

- Check your login credentials.
- Check if the identity used to log in is locked. In the Manager, use the following menu items in the **Identities** category.
    - **Inactive identities**: This displays temporarily and permanently deactivated identities.
    - **Security incidents**: This displays the identities that are classified as security threats.
    - **Locked identities**: This displays identities that have exceeded the maximum number of failed logins and have been locked out.
- Check if the system user used to log in is locked. Locked system users are displayed in the Designer in the **Permissions > System users > Locked system users** category.

For more information about deactivated identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

You can reset the passwords of identities and system users who have been locked in Password Reset Portal. This unlocks the identities and system users again. For more information, see the *One Identity Manager Web Portal User Guide* and the *One Identity Manager Web Application Configuration Guide*.

Problem

When logging in to 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 the Designer, search in the **Permissions > Program functions** category for the permissions group that has the required program functionality.
    - For non role-based login: 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 more 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 Settings for the database server and the One Identity Manager database on a SQL Server 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 30: Messages in the Configuration Wizard before starting the installation or update of a database

Message	Solution
The database collation setting	Set the **Sort order** (collation) database property to the

Message	Solution
is not valid. SQL_Latin1_General_CP1_CI_AS is required.	value **SQL_Latin1_General_CP1_CI_AS**.
The migration cannot be carried out because a replication is currently running.	For more information, see Database errors migrating a database to SQL Server AlwaysOn availability groups on page 176.
The value in DialogDatabase.DataOrigin is invalid. Start by running a database compilation.	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.
The database has no data-file group for in-memory OLTP.	Use the repair method to create a data-file group.
The database has not defined a file in the data-file group for in-memory OLTP.	Use the repair method to create a database file. The file is created in the directory of the data file (`*.mdf`).
The SQL Server has not activated in-memory OLTP.	Set the **Is XTP Supported** database server property value to **True**.
The Arithmetic Abort enabled database property is not enabled.	Set the **Arithmetic Abort enabled** database property value to **True**.
The Quoted Identifiers Enabled database property is not activated.	Set the **Quoted Identifiers Enabled** database property value to **True**.
You cannot run a migration if the recovery model is not Simple.	Set the **Recovery model** database property value to **Simple**.
The transaction mode cannot be set because other users are active.	End the connections of other users to the database.
The Job queue and/or the DBQueue is not empty. Refer to the documentation for additional information and suggested solutions for this test.	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 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 for testing or development. By updating the database, modifications may be made

Message	Solution
	that result in not being able to handle the processes anymore.
The viadmin system user must have a valid password that is not empty.	Make sure that the system user has a valid password.
The database has the status 'Initialmigration'. Therefore the Configuration Wizard cannot be run.	The initial schema installation of the database was not completely finished. This may have different reason. For example, the database or failover cluster could not be reached during the schema installation. Create a new database and rerun the initial schema installation. For more information, see Installing and configuring a One Identity Manager database on page 61.
The SQL login specified in QBMDBPrincipal.LoginName does not exist.	Use the repair method to create the SQL login.

Database errors migrating a database to SQL Server AlwaysOn availability groups

Possible problems

- The data does not start updating. The Configuration Wizard shows the message:

  ```
  The migration cannot be carried out 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.

Solution

1. Remove the database from the AlwaysOn availability group.
2. Update the One Identity Manager schema.
3. Put the database back into the AlwaysOn availability group.

Error messages when generating email notifications

Problem

When email notifications are generated in processes, any error messages are logged.

```
The configuration parameter '{0}' still contains the default value '{1}'. Adjust this value to suit your system environment.
```

```
The configuration parameter '{0}' does not exist or is not set. It is a mandatory value and must be configured in your system.
```

```
Use the Designer to configure the parameter '{0}' or contact your administrator.
```

Cause

One Identity Manager sends email notifications about various actions taken within the system. One Identity Manager email notification system is not completely configured.

Solution

Check the configuration parameters for the email notification system. To do this, use the email configuration wizard.

To start the email configuration wizard in the Launchpad.

1. In the Launchpad, in the **Configuration** section, select **Configure email connection**.
2. Click **Run**.

To start the email configuration wizard in the Designer.

1. In the Designer, in the **Base data > General > Configuration parameters** category, select the **Common | MailNotification** configuration parameter.
2. In theConfiguration Parameter Editor, click **...** next to the **Value** field.

Detailed information about this topic

- Setting up the email notification system on page 82
- Configuration parameters for the email notification system on page 190

Removing unnecessary modules from the One Identity Manager database

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 stopped. You can do this using the Job Queue Info.
4. Stop all One Identity Manager Services through the services manager.
5. Stop 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 running SQL queries.

   IMPORTANT:

   - Select a user that you use for migrating the database to run the SQL queries.
   - Run the following steps separately using a suitable program for running SQL queries.

     Test the output of the query after each step. The output provides additional tips for removing a module.

   a. Activate single-user mode for the One Identity Manager database.

      ```
      exec dbo.QBM_PSingleUserRequest @@spid
      ```

   b. Delete all triggers in the database.

      ```
      exec QBM_PTriggerDrop '%', @force = 1
      ```

c. Delete all constraints in the database.

```
exec QBM_PConstraintFKDrop '%','%','%'
```

d. Delete the module you no longer need.

```
exec QBM_PModuleRemove '<3-char module abbreviation>'
```

Example:

```
declare @ModulesToRemove varchar(100) = 'SAP' + char(7)
      + 'SHR' + char(7)
      + 'SBW' + char(7)
      + 'SAC' + char(7)
exec QBM_PModuleRemove @ModulesToRemove
go
```

e. If you delete the Business Roles Module (RMB), you must also delete the entries in the `OrgRoot` table.

```
exec QBM_PDeleteDeep '<Key><T>OrgRoot</T><P>3031e9af-6a53-4876-bbfb-0f7fbf264131</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.

Deleting One Identity Manager databases

The Configuration Wizard provides support for deleting a One Identity Manager database. Deleting a database also removes the database users, database roles, and server roles, as well as SQL logins.

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

To delete a database

1. Start the Configuration Wizard.
2. On the Configuration Wizard home page, select the **Delete One Identity Manager database** option and click **Next**.
3. On the **Select database** page, select the database and installation directory.

a. Select the database connection in the **Select a database connection** pane. Select a user who at least has administrative permissions for the One Identity Manager database.

b. In the **Installation source** pane, select the directory with the installation files.

4. On the **Database check** page, errors are displayed that prevent the database from being processed. Correct the errors before you continue updating.
5. To start the deletion process, click **Next**.
6. On the **Processing database** page, each step of the deletion process is displayed.
   a. Read and check each step.
   b. To run the step, click **Confirm delete**.
   c. After the deletion process is complete, click **Next**.
7. On the last page of the Configuration Wizard, click **Finish**.

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 usually starts after the indexing interval period specified by the **Common | Indexing | Interval** configuration parameter has elapsed.

If a table being indexed contains more objects to be indexed than the maximum specified by the **Common | Indexing | BatchSize** configuration parameter, 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 three 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, for example:

```
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 A

Advanced configuration of the Manager web application

The configuration settings for the Manager web application are saved in the `appsettings.json` configuration file. You will find the `appsettings.json` configuration file in the web application installation directory in the Internet Information Services.

The Web Installer uses default values for the configuration settings when installing the Manager web application. You can keep these values. It is recommended you check the settings with the help of the App Configuration Editor.

Related topics

- Installing and updating the Manager web application on page 157
- Customizing the Manager web application configuration on page 181
- Configuration settings for the Manager web application on page 182
- Load balancing of the Manager web application on page 186
- Manager web application single sign-on on page 187

Customizing the Manager web application configuration

Use the App Configuration Editor to configure the Manager web application configuration. The App Configuration Editor is part of the web application and can be found in the Manager install directory in the `WebConfigEditor` subdirectory.

To run configuration

1. Start the `AppConfigurationEditor.exe` file from the `WebConfigEditor` subdirectory of the Manager web application installation directory.
2. In the **Configuration files** section, double-click the `appsettings.json` configuration file to open it.

3. (Optional) To display all the configuration settings, click **Show all**.
4. Modify the configuration settings.
5. Save the changes.

Related topics

- Configuration settings for the Manager web application on page 182

Configuration settings for the Manager web application

Use the App Configuration Editor to change the following configuration settings for the Manager web application. The settings are saved in the `appsettings.json` configuration file. You will find the `appsettings.json` configuration file in the web application installation directory in the Internet Information Services.

Table 31: Configuration settings for the Manager web application

Setting	Description
General	General settings of the Manager web application
Language	The Manager web application language. The language influences how dates and numbers displayed amongst other things. Default value: **`en-US`**
Session timeout	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. Default value: **`2`** NOTE: 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.
Timeout mode	Methods for determining timeouts. Permitted values are: • **`TimeOut`**: A session is ended when the period of time defined under **Session timeout** elapsed with no user activity. • **`HeartBeat`**: A session is ended when the period of time defined under **Session timeout** elapsed with no user activity. The user's open browser window prompts automatically and the timeout starts once the browser window closes. Default value: **`HeartBeat`**

Setting	Description
Database connection	Settings for connecting to the database.
Database	Database connection. Select either a direct database connection or an application server.
Program	Application which specifies the contents of the web application. Default value: **Manager**
Authentication	Methods for authenticating the user when logging in to the application. For more information about authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
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	Security settings of the Manager web application
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. Default value: **10** seconds
Close browser window after logout	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. Default value: **Disabled**
Debugging	Settings for debugging the Manager web application.
Enable documentation mode	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. Default value: **Disabled** NOTE: This setting should not be enabled in a production environment.
Performance	Settings that affect the performance of the Manager web application.
Load balancing	The mode of integrated load balancing. Permitted values: • **DistributeEqually**: This algorithm distributes user logins such that each application in one language has the same number of active users, if possible. • **DistributeSuccessively**: 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

Setting	Description
	desired language. When this has reached it maximum load, logins are forwarded to the next application. In most cases, **DistributeEqually** should be selected. Default value: **DistributeEqually**
Maximum workload	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. Default value: **20** sessions
Force maximum workload	The value in **Maximum workload** is overridden is this setting is not set. However, it is used as a threshold value for the **DistributeSuccessively** load balancing method. Default value: **Disabled**
Compress HTTP transfer	Specifies whether use of compression for HTTP communication is set. Default value: **Disabled** NOTE: Compression of HTTP communication must also be configured for Internet Information Services. For more information see the Web server documentation.
File download	Settings for downloading the Manager web application.
Enable file download	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 functions are not available. Default value: **Enabled**
Download directory	Directory for the application to use to make downloads available, such as reports generated by the application and saved by users as PDF. The application requires full permissions to this directory. Default value: **.\App_Data\Download**
Cleanup interval	Time in minutes search for and remove redundant files. Default value: **2** minutes
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 run by the user so that the download must be stopped after a set time interval. Default value: **4** minutes
Application pool	Define all applications that work together to make the application available to users in multiple languages.

Setting	Description
	• 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.
Redirect URL	Full address of the application. It must also be possible to resolve this address on the client side through the user's browser. NOTE: Ensure correct case.
Authentication	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 permissions as required when the URL is called by browser on the server. Enter the domain, user account, and password for logging in the user account.
Plug-ins	Plug-ins extend the functionality of the Manager web application.
Auto update	Automatic update is enabled. Default value: **`Enabled`**
Severity	Severity of a change in order to start automatic update. Permitted values: • Use the **Common | Autoupdate** configuration parameter setting • Noncritical change • Non-functional change • Functional change • Critical update Default value: Use the **Common | Autoupdate** configuration parameter setting

Related topics

- Customizing the Manager web application configuration on page 181
- Load balancing of the Manager web application on page 186
- Manager web application single sign-on on page 187

Load balancing of the Manager web application

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 in to, 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 32: Supported algorithms for load balancing

Algorithm	Description
DistributeEqually	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 most cases.
DistributeSuccessively	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 it maximum load, logins are forwarded to the next application.

Load balancing solves the following problems:

- Multilingual

  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 necessary complete outage if just one of the installed application fails.

Related topics

- Configuration settings for the Manager web application on page 182

Manager web application 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:

- Anonymous access disabled.
- Configuration of an authentication module capable of single sign-on.

  For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
- Permissions in the application's own 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

- Configuration settings for the Manager web application on page 182

Appendix B

Machine roles and installation packages

The following table contains possible machine roles and installation package descriptions. The machine role selected determines which installation packages are installed on a workstation or on a Job server.

For more information about machine roles, see the *One Identity Manager Configuration Guide*.

NOTE: Other machine roles and installation packages may be available depending on which One Identity Manager modules are installed.

Table 33: Machine role and installation package options

Machine role	Description of the installation package
Database Agent	Contains the `DatabaseAgentServiceCmd.exe` program for running the Database Agent Service from the command line.
Documentation	Contains One Identity Manager documentation in different languages.
Server	Contains all the basic components for setting up a server.
Server | Job Server	Contains the One Identity Manager Service and basic processing components. Additional machine roles contain connectors for synchronizing individual target systems.
Server | Job Server | Config-uration tool	Contain configuration tool for the One Identity Manager Service.
Server | Web	Contains all the basic components for setting up a web server.
Server | Web | Application Server	Contains the components for setting up an 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.
Server | Web | Business	Contains the components for setting up an API Server.

Machine role	Description of the installation package
API Server	
Server | Web | Business API Server | Application Insights Integration	Contains the plugin for integration with Microsoft Application Insights.
Server | Web | Business API Server | SCIM Provider	Contains the SCIM Plugin for the API Server
Server | Web | Manager Web Application	Contains the tools for installing and configuring the Manager on a web server.
Workstation	Contains all basic components for installing tools on an administrative workstation.
Workstation | Administration	Contains administration tools required by default users for fulfilling their tasks with One Identity Manager. In addition to the tools that ensure basic functionality for working with One Identity Manager, the administration machine role includes the Manager as a main administration tool.
Workstation | Command line administration tools	Contains various command line programs.
Workstation | Configuration	Contains all tools for the default user and additional programs required to configure the system. For example, these include the Configuration Wizard, Database Compiler, Database Transporter, Crypto Configuration, Designer as well as configuration tools for the One Identity Manager Service.
Workstation | Development and Testing	Contains the tools to develop and test custom scripts, such as the System Debugger.
Workstation | Monitoring	Contains programs for monitoring the system status, for example the Job Queue Info program.

Appendix C

Configuration parameters for the email notification system

Use the following configuration parameters to configure the email notification system.

NOTE: Some configuration parameters are only available if the One Identity Manager modules are installed.

Table 34: General configuration parameters for mail notification

Configuration parameter	Meaning
Common | InternationalEMail	Specifies whether international domain names and unicode characters are supported in email addresses. IMPORTANT: The mail server must also support this function. If necessary, you must override the script `VID_IsSMTPAddress`
Common | MailNotification	Specifies whether the configuration subparameters that deal with notifications take effect.
Common | MailNotification | AcceptSelfSignedCert	Specifies whether self-signed certificates for TLS connections are accepted.
Common | MailNotification | AllowServerNameMismatchInCert	Specifies whether server names that do not match are permitted by certificates for TLS connections.
Common | MailNotification | DefaultAddress	Default email address of the recipient of the notifications.
Common | MailNotification | DefaultCulture	Default language used to send email notifications if a language cannot be determined for a recipient.
Common | MailNotification | DefaultLanguage	Default language for sending email notifications.
Common | MailNotification | DefaultSender	Sender's default email address for sending automatically generated notifications. Syntax:

Configuration parameter	Meaning

	`sender@company.com`
	Example:
	`noreply@company.com`
	You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>).
	Example:
	`One Identity <noreply@company.com>`

Common | MailNotification | Encrypt	Specifies whether emails are encrypted.
Common | MailNotification | Encrypt | AuthenticationType	Authentication method for logging in to LDAP. Permitted values are: • **`Basic`**: Uses default authentication. • **`Negotiate`**: Uses Negotiate authentication from Microsoft. • **`Kerberos`**: Uses Kerberos authentication. • **`NTLM`**: Uses Windows NT Challenge/Response (NTLM) authentication. Default: **`Basic`** For more information about authentication types, see the MSDN Library.
Common | MailNotification | Encrypt | ConnectDC	Domain controller of the requested domain to use.
Common | MailNotification | Encrypt | ConnectPassword	Password of the user account. 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 request.
Common | MailNotification | Encrypt | EncryptionCertificateScript	Script that supplies a list of encryption certificates. Default: **`QBM_GetCertificates`** This parametrizes the script code using the other parameters and creates an Active Directory request with user and password in the form `LDAP://<connect domain controller:389/<domain to query>`.

Configuration parameter	Meaning
Common | MailNotification | Encrypt | Port	Server port for secure access to LDAP. Default: **389**
Common | MailNotification | Encrypt | UseSSL	Specifies whether to use an SSL/TLS encrypted connection.
Common | MailNotification | NotifyAboutWaitingJobs	Specifies whether a message should be sent if the process steps have a particular status in the Job queue.
Common | MailNotification| O365ClientId	Application client ID used to send the emails. You can find your application ID in the Microsoft Entra ID Admin Center under **Applications > App registrations < <your application> > Overview > Application (client) ID**.
Common | MailNotification | SignCertificateThumbprint	SHA1 thumbprint of the certificate to use for the signature. This can be in the computer's or the user's certificate store. NOTE: Ensure that the private key in the certificate is marked as exportable.
Common | MailNotification | SMTPAccount	User account name for authentication on an SMTP server.
Common | MailNotification | SMTPDomain	User account domain for authentication on the SMTP server.
Common | MailNotification | SMTPPassword	User account password for authentication on the SMTP server.
Common | MailNotification | SMTPPort	Port of the SMTP service on the SMTP server. Default: **25**
Common | MailNotification | SMTPRelay	SMTP server for sending email notifications. If a server is not given, **localhost** is used.
Common | MailNotification | SMTPUseDefaultCredentials	Specifies which credentials are used for authentication on the SMTP server. If this parameter is set, the One Identity Manager Service login credentials are used for authentication on the SMTP server. If the configuration parameter is not set, the login data defined in the **Common | MailNotification | SMTPDomain** and **Common | MailNotification | SMTPAccount** or **Common | MailNotification | SMTPPassword** configuration parameters is used. (Default)

Configuration parameter	Meaning
Common | MailNotification | TransportSecurity	Encryption method for sending email notifications. If none of the following options are given, the port is used to define the behavior (port 25: no encryption, port 465: with SSL/TLS encryption). Permitted values are: • **`Auto`**: Identifies the encryption method automatically. • **`SSL`**: Encrypts the entire session with SSL/TLS. • **`STARTTLS`**: Uses the STARTTLS mail server extension. Switches TLS encryption after the greeting and loading the server capabilities. The connection fails if the server does not support the STARTTLS extension. • **`STARTTLSWhenAvailable`**: Uses the STARTTLS mail server extension if available. Switches on TLS encryption after the greeting and loading the server capabilities, however, only if it supports the STARTTLS extension. • **`None`**: No security for the transport layer. All data is sent as plain text.
Common | MailNotification | VendorNotification	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 35: Additional parameters for email notifications

Configuration parameters	Description
QER | Attestation | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications about attestation cases. Replace the default address with a valid email address.
QER | ComplianceCheck | EmailNotification | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications about rule checking. Replace the default address with a valid email address.
QER | ITShop | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications about requests. Replace the default address with a valid email address.
QER | Policy | EmailNotification | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications when company policies are checked. Replace the default address with a valid email address.
QER | RPS | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications about report subscriptions. Replace the default address with a valid email address.
TargetSystem | ADS | DefaultAddress	Default email address of the recipient for notifications about actions in the Active Directory target system.
TargetSystem | ADS | Exchange2000 | DefaultAddress	Default email address of the recipient for notifications about actions in the Microsoft Exchange target system.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Default email address for sending warning emails.
TargetSystem | AzureAD | DefaultAddress	Default email address of the recipient for notifications about actions in the Microsoft Entra ID target system.
TargetSystem | AzureAD | ExchangeOnline | DefaultAddress	Default email address of the recipient for notifications about actions in the Exchange Online target system.
TargetSystem | CSM | DefaultAddress	Default email address of the recipient for notifications about actions in the cloud target system.
TargetSystem | EBS | DefaultAddress	Default email address of the recipient for notifications about actions in the Oracle E-Business Suite target system.
TargetSystem | LDAP | DefaultAddress	Default email address of the recipient for notifications about actions in the LDAP target system.
TargetSystem | NDO | DefaultAddress	Default email address of the recipient for notifications about actions in the HCL Domino target system.

Configuration parameters	Description
TargetSystem | OneLogin | DefaultAddress	Default email address of the recipient for notifications about actions in the OneLogin target system.
TargetSystem | PAG| DefaultAddress	Default email address of the recipient for notifications about actions in the Privileged Account Management system.
TargetSystem | SAPR3 | DefaultAddress	Default email address of the recipient for notifications about actions in the SAP R/3 target system.
TargetSystem | SharePoint | DefaultAddress	Default email address of the recipient for notifications about actions in the SharePoint target system.
TargetSystem | Unix | DefaultAddress	Default email address of the recipient for notifications about actions in the Unix-based target system.
TargetSystem | UNS | DefaultAddress	Default email address of the recipient for notifications about actions in the custom target system.

Detailed information about this topic

- Setting up the email notification system on page 82
- Sending email notifications via Microsoft 365 on page 87
- Error messages when generating email notifications on page 177

Appendix D

How to configure the One Identity Manager database using SQL Server AlwaysOn availability groups

Only the settings for working with One Identity Manager are described below. For more information about SQL Server AlwaysOn availability groups, see Always On availability groups: a high-availability and disaster-recovery solution.

NOTE: If you want to include a One Identity Manager database in a SQL Server AlwaysOn availability group, note that one availability group is required per availability database.

Example:

You want two databases (for example, UAC and QA) to be part of an SQL Server AlwaysOn availability group as availability databases. Each database requires its own availability group (for example, AGUAC and AGQA).

NOTE: Custom SQL logins for the One Identity Manager database must be available on all nodes.

If you are working with granular permissions, you must also provide SQL logins on all nodes. Ensure that an SQL login with the connected server roles is created on all nodes with the same security ID (SID), otherwise failover problems may occur.

Prerequisite

A failover cluster manager has been configured. Therefore, run the Server Manager on the database server and install the **Failover Clustering** feature.

Installing One Identity Manager

1. Run the program Configuration Wizard against a cluster node and follow the installation instructions.
2. Install and launch the One Identity Manager Service. After all processes in the Job queue have been processed, stop the One Identity Manager Service.
3. Run the Designer and set up the staging layer for the database.

4. In SQL Server Management Studio, change the recovery model for the One Identity Manager database from **Simple** to **Full**.
5. Create a full backup of the database.
6. Make sure that the firewall is configured to support cluster communication.
7. Run the SQL Server Configuration Manager and locate the SQL Server service. Open the properties and enable **Always-On Availability Groups**. Restart the SQL Server service on all nodes.

   For more information, see Enable or Disable Always On availability group feature.

Configuring the SQL Server AlwaysOn availability groups

1. In SQL Server Management Studio, connect the server instance that hosts the primary node. To configure the availability groups, navigate to **AlwaysOn High Availability**, right-click and select **New Availability Group Wizard**.

   For more information about the New Availability Group Wizard, see Use the Availability Group Wizard (SQL Server Management Studio).
2. In the New Availability Group Wizard, enter the name of the new availability group and select the One Identity Manager database to be included in the new availability group.
3. In the New Availability Group Wizard, you create and configure a replica for the new availability group.
   a. Add the secondary SQL Server cluster node.
   b. Enable automatic failover and synchronous handover for both nodes.
   c. Make all nodes a readable secondary node; select the **Yes** value.
   d. Specify an availability group listener.

      For example, for the DNS name, use the same name as the availability group but with the suffix "L", and use port 1433. Assign an IP address on the same subnet as the SQL Server.

      For more information, see Specify Replicas Page (New Availability Group Wizard: Add Replica Wizard).
4. In the New Availability Group Wizard, you define the settings for data synchronization. The settings for data synchronization depend on your infrastructure.

   If you are using a network share to synchronize data between replicas, select the **Full** option and specify the network location. Server instances hosting a replica require read and write access to the share.

One Identity Manager configuration

1. Run the program Database Compiler. Connect to the primary node and compile the database. Do not change the database connection data at this time.

   For more information, see the *One Identity Manager Operational Guide*.
2. Then update the database connection data in Designer.

a. Start the Designer and connect to the primary node.
b. In the Designer, select the **Base Data > General > Databases** category.
c. Select the database in the List Editor.
d. Select the **Define connection string for database** task.
e. Enter the connection data for the database. Use the DNS name of the listener instead of the server name.

For more information, see the *One Identity Manager Configuration Guide*.

3. Run the program Database Compiler and compile the database. Use the listener.
4. Run the Job Service Configuration and change the connection details for the One Identity Manager Service. Use the listener.

   It is recommended to change the queue name to better reflect the cluster. Note that you also update the queue name in Designer.

   For more information, see the *One Identity Manager Configuration Guide*.
5. Ensure that Job servers, application servers, front-ends, web applications, and synchronization projects use the listener to log in to the database.

Related topics

- Installing and configuring a One Identity Manager database on page 61
- Installing and configuring the One Identity Manager Service on page 90
- Logging in to One Identity Manager tools on page 163
- Database errors migrating a database to SQL Server AlwaysOn availability groups on page 176

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

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

Index

A

Analyzer 13
API Server
  customize 150-151, 153
  install 143
  install SCIM Plugin 150
  load balancing 149
  system requirements 45
  uninstall 156
  uninstall SCIM Plugin 150
  update 154
App Configuration Editor 181
AppConfigurationEditor.exe 181
application server 10
  appsettings.json 107, 132, 139
  install 131-132, 137
  One Identity Manager Service 18
  One Identity Manager tools 18
  search index
    update 138
  Search Indexing Service 131-132, 137
  Search Service 132, 137
  search service
    install 132, 137
    uninstall 137
  status display 136
  system requirements 47
  uninstall 137, 140
  update 139
appsettings.json
  application server 107, 132, 139
  Manager web application 157, 181
authentication
  test 170
authentication module
  enable 168
authorizations 26, 49, 52
autoupdate process 104

C

cluster resource
  log file 99
  One Identity Manager Service 99
Configuration Wizard 13, 61, 64, 115, 117, 120, 179
Crypto Configuration 13, 73
custom configuration package 114
  import 124
  show contents 123

D

database
  configure 61, 72
  custom configuration package 114
  delete 179
  development environment 72
  encrypt 73-77
  hotfix package 114, 122
  install 61
  live environment 72
  migration log 120

migration package 114
module overview 172
SQL Server 64, 117, 179
staging level 72
system requirements 23, 31, 38
test environment 72
transport history 120, 122, 172
transport package 114
update 114-115, 117, 120, 122
version 120, 172
Database Compiler 13
database server
system requirements 21, 23, 31, 38
Database Transporter 13, 123-124
database user
authorizations 26
SQL Server 26
default connection dialog 163
default language 169
Designer 13
Docker image 55

E

email configuration wizard 82
email notification 82, 177
encryption 73-78
Key
change 75
create 74
generate 73
key data 73
key file 73
private key 73

F

firewall configuration 52
full text search
application server 131-132
search service 131-132, 137

H

hotfix package 114
file
backup 126
import 126
import 124
install 122
show contents 123

I

installation prerequisites 20-21, 23, 26, 31, 38, 43-45, 47-49, 52
firewall 52
ports 52
InstallState.config 101

J

Job Queue Info 13
Job server
install 57, 90-92
set up 90-92
update 104
Job Service Configuration 13

L

language
default language 169
enable 169
login language 169
Select in GUI 169
Launchpad 13
License Meter 13
login 163
default connection dialog 163
login language 169
enable 169

M

Machine role 188
Manager 13
Manager web application 13
appsettings.json 157, 181-182
configure 181
install 157
load balancing 186
open 161
settings 182
single sign-on 187
uninstall 162
update 161
migration package 114

N

notification system 82, 177

O

One Identity Manager
application server 10
architecture overview 10
authorizations 49
database 10
front-end 10
hotfix 108
install 54
Server Service 10
service pack 108
system configurations
email notification 82, 177
update 108
user 49
version change 108
Web server 10
One Identity Manager components
install 57, 60
update 103, 112
One Identity Manager Docker image 55
One Identity Manager schema
install 61
One Identity Manager Service 10
cluster resource 97, 99
database key 78
install 90-92
installation prerequisites 44, 52
key file 78
log file 95
private.key 78
start 96
start type 96
update 104

user account 96
authorizations 49
One Identity Manager tools 13
Analyzer 13
Configuration Wizard 13
Crypto Configuration 13
Database Compiler 13
Database Transporter 13
Designer 13
install 57, 60
installation prerequisites 43
Job Queue Info 13
Job Service Configuration 13
Launchpad 13
License Meter 13
log in 163
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 103
Web Installer 13
Web Portal 13
Operations Support Web Portal 13

P

password
reminder notification 170
sequence 170
Password Reset Portal 13
ports 52

R

Report Editor 13

S

Schema Extension 13
server
install 57, 90-92
update 104
Server Installer 13
service server
system requirements 44
show web applications 149
Software Loader 13, 126
software revision 101
software update
automatic 101
deactivate 106-107
enable 106, 120
file
backup 126
import 126
version 126
InstallState.config 101
One Identity Manager Service 104
One Identity Manager tools 103
put into operation 106
server 104
softwarerevision.viv 101, 103-104
Update.exe 101, 103, 105
update.lock 101
update.log 101

Update.zip 101, 103-105
Web application 105
softwarerevision.viv 101, 103-104
SQL processing server 54
supplier notification 80
deactivate 81
enable 80
verify 81
Synchronization Editor 13
system configurations
overview 172
System Debugger 13
system requirements
API Server 45
application server 47
authorizations 49
database 23, 31, 38
database server 21, 23, 31, 38
database user
SQL Server 26
One Identity Manager Service 44
One Identity Manager tools 43
service server 44
user 49
Web server 48
workstation 43

T

transport history 172
transport package 114
import 124
show contents 123
troubleshooting 172

U

update
automatic 101
update server 54, 106
Update.exe 101, 103, 105
update.lock 101, 103
update.log 101
Update.zip 101, 103-105

W

Web application
update 105
Web Installer 13, 132, 140, 157, 162
Web Portal 13
Web server 10
system requirements 48
workstation
install 57
system requirements 43