ONE IDENTITY™

One Identity Manager 8.1.4

Installation Guide

Contents

About this guide

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

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

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

Available documentation

You can access 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:

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

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

Starling Cloud Join

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 our Starling Cloud platform. 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.

Table 1: One Identity Manager editions

Edition	Description
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 Active Directory Edition	This edition contains all the functionality required for Active Directory support including connectors for Active Directory, attestation, IT Shop and workflows, and report functions.
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
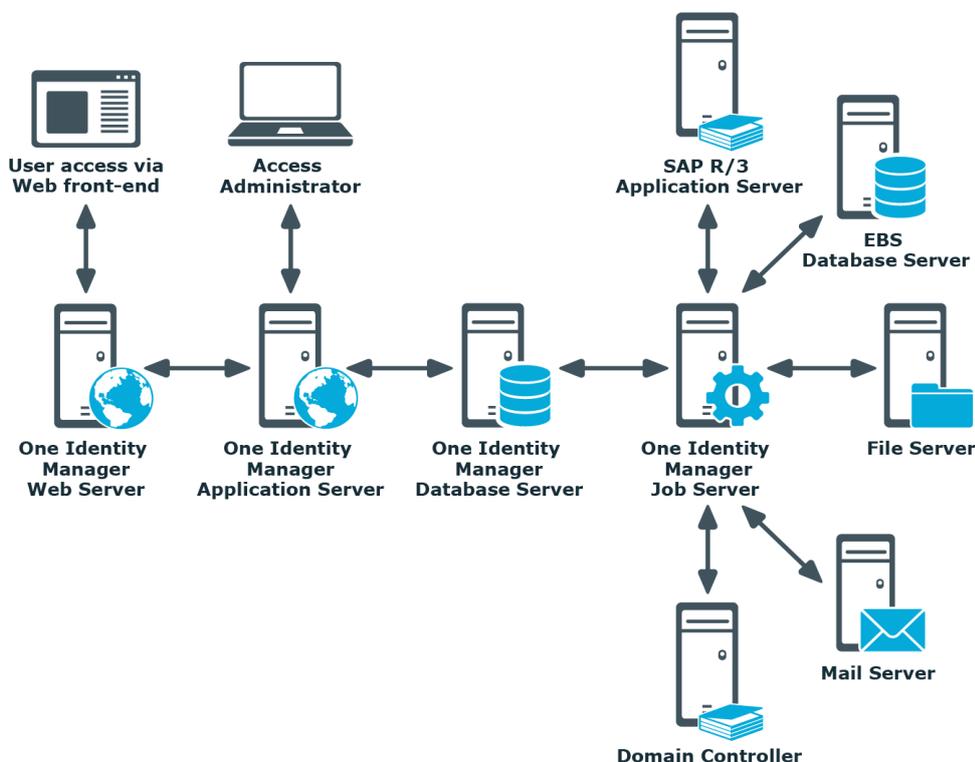
One Identity Manager consists of the following components:

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 employees, 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 executed by the object layer.

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

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

Application server

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

Clients can alternatively work without external application servers by 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, a different front-end is used to configure One Identity Manager than that for managing employee data. The contents to be displayed and the extent to which it can be altered is determined in conjunction with the access rights of the respective user through the object layer. Available front-end solutions are both client and browser-based.

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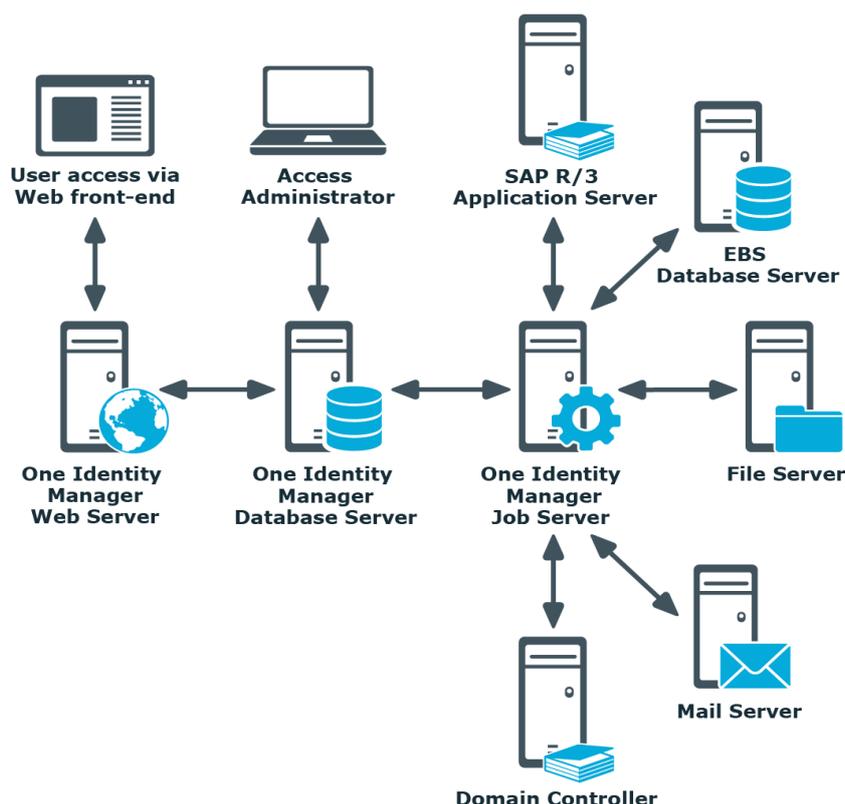
Related topics

- 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 configure One Identity Manager differs from the tool used to manage employee data. The content to be displayed and the extent to which it can be altered is determined in conjunction with the access rights of the respective user through the object layer.

Table 2: Overview of One Identity Manager tools

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 execute 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 in the following areas:
	• Changing employee master data and own password.
	• Editing or entering employee master data for subordinate staff.
	• 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 requires a web server. Through a web browser, users can access the website that has been dynamically set up and customized for them. Once the web server has been configured and a web project in has been published in the Web Designer, you can start the Web Portal in your own web browser.
Password Reset Portal	The Password Reset Portal allows users to securely reset passwords of the user accounts they manage.
	To utilize the Password Reset Portal, it must be installed as a dedicated web application. The necessary security is guaranteed by multi-factor authentication.
Operations Support Web Portal	The Operations Support Web Portal was created with help desk staff in mind, who need support when executing tasks and process steps. You can use the Operations Support Web Portal to monitor the handling of processes and DBQueue tasks. You can also create access codes for your colleagues.
	Before you can use the Operations Support Web Portal, you must install an API Server.
Manager	The Manager is the main administration tool for setting up information about employees and their identities. It displays and maintains all the

Tool	Short description
	data required for the administration of employees, their user accounts, permissions, and company-specific roles in a One Identity Manager network. Company resources employees require can be entered and assigned to them.
	You can also use 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 employees or roles and their assignments.
	By implementing One Identity Manager application roles, every One Identity Manager user obtains only those access permissions they require to fulfill necessary administrative duties.
	Manager functionality can be provided by web applications.
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 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 on a SQL Server for use in a One Identity Manager network. All the One Identity Manager schema tables, data types, and database procedures are loaded into the database with the Configuration Wizard. SQL Server 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

Tool	Short description
	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 executes 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 also use the Designer to set up the permissions structure for 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 the One Identity Manager system configuration. The range of functions and the operating methods of the editors are tailored to the differing configuration requirements.
Web Designer	Use the Web Designer to configure and extend the Web Portal. It includes functions for adapting Web Portal workflows and developing new workflows.
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

Tool	Short description
	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	Use the Schema Extension to extend the existing application data model of the One Identity Manager database with customized tables and columns. Using the object technology in 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).
HistoryDB Manager	One Identity Manager historical data is transferred at regular intervals into a One Identity Manager History Database thus, the One Identity Manager History Database provides an archive of change information. The HistoryDB Manager tool displays the data in the One Identity Manager History Database. Use the HistoryDB Manager to set up access to the source databases.
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 plugins are configured with this file. The configuration file is necessary both for One Identity Manager Service on a Windows based operating system and also for the Linux daemon.
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. The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

Tool	Short description
API Designer	The API Designer allows you to create, record, compile, and publish a Representational State Transfer Application Programming Interface (REST-API) in the quickest way possible. This API is based on the OpenAPI Specification and the One Identity Manager database model. To use the API, you must install an API Server.
API Server	The API Server provides the API that you create in the API Designer. It also provides the Operations Support Web Portal and your HTML5 web applications.

Related topics

-

Which components and front ends work with an application server?

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

Table 3: 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. Compliance rule simulation is not supported. Some forms are not supported.
Manager web	Yes	Some forms are not supported.

Component	Connection through application server?	Restrictions
application		
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.
Web Designer	Yes	
Data Import	Yes	
Crypto Configuration	No	
Database Compiler	No	
Report Editor	Yes	SQL query testing is not supported.
Schema Extension	No	
System Debugger	Yes	
Database Transporter	No	
HistoryDB Manager	Yes	
License Meter	Yes	
Software Loader	Yes	
SPML web application	No	
SOAP Web Service	No	

Component	Connection through application server?	Restrictions
One Identity Manager Service	Yes	
Server Installer	Yes	
API Designer	Yes	
API Server	Yes	

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

- Minimum system requirements for implementing SQL Servers as database servers on page 22
- Requirements for a managed instance in Azure SQL Database on page 31
- Minimum system requirements for administrative workstations on page 37
- Minimum system requirements for the service server on page 38
- Minimum system requirements for the web server on page 39
- Minimum system requirements for the application server on page 41
- Users for One Identity Manager on page 42
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26
- Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33

Minimum system requirements for 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 4: Minimum system requirements - database server

Processor	8 physical cores 2.5 GHz+ NOTE: 16 physical cores are recommended on the grounds of performance.
Memory	16 GB+ RAM
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	The following versions are supported: • SQL Server 2016 Standard Edition (64-bit), Service Pack 2 with the current cumulative update • SQL Server 2017 Standard Edition (64-bit) with the current cumulative update • SQL Server 2019 Standard Edition (64-bit) with the current cumulative update NOTE: The cumulative update 2 for SQL Server 2019 is not supported. NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended. • SQL Server Management Studio (recommended)

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 with granular permission 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 5: Database server settings

Property	Value	Comment
Language	English	
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 standard installation. The setting is tested by the Configuration Wizard before installing or updating One Identity Manager database. If XTP is not activated, the installation or update does not start.
SQL Server Agent	Started	Start the SQL Server Agent in the SQL Server Service Management Portal. You can log in on a SQL Server Agent as a domain user with Windows authentication or with a local system account. The setting is tested by the Configuration Wizard

Property	Value	Comment
		before installing or updating One Identity Manager database. If the SQL Server Agent is not started, the installation or update is not started.

Table 6: 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	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 2016 (130)	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	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.
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 Identi-	True	The setting is checked by the Configuration

Property	Value	Comment
fiers Enabled		Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Broker 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	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

Property	Value	Comment
		is created by the repair method in the directory of the data file (`*.mdf`).

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 detailed 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

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

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

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

- Installation user

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

    NOTE: If you want to change to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x, or 8.0.x to 8.1.4, you will also require an installation user.

- Administrative user

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

- Configuration user

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

- End user

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

Permissions for installation users

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

SQL Server:

- Member of **dbcreator** server role

    The server role is only required if the database is created using the Configuration Wizard.

- Member of 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 Server 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:

- **Select** permissions with the **with grant option** option for the `dbo.sysjobs`, `sysjobstepsdbo.sysjobschedules`, `dbo.sysjobactivity`, `dbo.sysschedules`, and `dbo.sysjobhistory` tables

    The permissions are required to execute and monitor database schedules.

- **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.

- Member of the **SQLAgentUserRole** database role

This database role is required for managing database schedules during an update from version 7.0.x, 7.1.x, or 8.0.x to version 8.1.4.

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.

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

Permissions for administrative users

During the installation of the One Identity Manager database using 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 Server logins for the configuration user and the end user with the corresponding database users.

- **<DatabaseName>_Admin** SQL server login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - **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.

msdb database:

- **OneIMRole_<DatabaseName>** database role

    - Member of the **SQLAgentUserRole** database role

        The database role is required to execute database schedules.

    - **Select** permissions for the dbo.sysjobs, dbo.sysjobschedules, dbo.sysjobactivity, dbo.sysschedules and dbo.sysjobhistory tables

        The permissions are required to execute and monitor database schedules.

- **OneIM_<DatabaseName>** database user

    - Member of the **OneIMRole_<DatabaseName>** database role

    - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

master database:

- **OneIMRole_<DatabaseName>** database role

    - **Execute** 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 server login.

One Identity Manager database:

- **Admin** database user

    - Member in **db_owner** database role

        The database role is required to update a database with the Configuration Wizard.

    - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

Permissions for configuration users

During the installation of the One Identity Manager database using 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**, **Execute**, 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 Server login.

Permissions for end users

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

SQL Server:

- **<DatabaseName>_User** SQL login

One Identity Manager database:

- **OneIMUserRoleDB** database role

    - **Insert**, **Update**, **Select**, and **Delete** permissions for selected tables in the database

    - **View Definition** permissions for the database

    - **Execute** 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** SQL Server login.

Tips for using integrated Windows authentication

Integrated Windows authentication can be used without restriction for the One Identity Manager Service and the web applications. Integrated Windows authentication can be used

for FAT clients. Use of Windows groups for logging in is supported. To ensure functionality it is strongly recommended you use SQL Server login.

To implement Windows authentication

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

Requirements for a managed instance in Azure SQL Database

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

Related topics

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

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

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

Table 7: Database server settings

Property	Value	Comment
Language	English	
Server Collation	Case insensitive	
	SQL_Latin1_General_CP1_CI_AS (recommended)	
Extreme transaction processing supported (Is	True	Default

Property	Value	Comment
XTP supported)		setting.
SQL Server Agent	Started	Default setting.

Table 8: 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 2016 (130)	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	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.
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 Identi- fiers 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.
Broker 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.

Property	Value	Comment
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.

Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database

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

- Installation user

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

- Administrative user

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

- Configuration user

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

- End user

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

Permissions for installation users

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

SQL Server:

- Member of **dbcreator** server role

  The server role is only required if the database is created using the Configuration Wizard.

- Member of **securityadmin** server role

  This server role is required to create SQL Server 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:

- **Select** permissions with the **with grant option** option for the dbo.sysjobs, sysjobsteps, dbo.sysjobschedules, dbo.sysjobactivity, dbo.sysschedules, and dbo.sysjobhistory tables

  The permissions are required to execute and monitor database schedules.

- **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.

- **Execute** 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.

- **Execute** permissions with the **with grant option** option for the `xp_sqlagent_is_starting, xp_sqlagent_notify,` and `xp_sqlagent_enum_jobs` procedures

  The permissions are required to execute and monitor database schedules.

One Identity Manager database:

- Member of the **db_owner** database role

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

Permissions for administrative users

During the installation of the One Identity Manager database using 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 Server logins for the configuration user and the end user with the corresponding database users.

- **<DatabaseName>_Admin** SQL server login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - **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.

msdb database:

- **OneIMRole_<DatabaseName>** database role
  - Member of the **SQLAgentUserRole** database role

    The database role is required to execute database schedules.

  - **Select** permissions for the `dbo.sysjobs,sysjobsteps,` `dbo.sysjobschedules,`

`dbo.sysjobactivity`, `dbo.sysschedules` and `dbo.sysjobhistory` tables

The permissions are required to execute and monitor database schedules.

- **OneIM_<DatabaseName>** database user

  - Member of the **OneIMRole_<DatabaseName>** database role

  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

master database:

- **OneIMRole_<DatabaseName>** database role

  - **Execute** permissions for the `xp_readerrorlog` procedure

    The permissions are required to find out information about the database server's system status.

  - **Execute** permissions for the `xp_sqlagent_is_starting`, `xp_sqlagent_notify`, and `xp_sqlagent_enum_jobs` procedures

    The permissions are required to execute and monitor database schedules.

- **OneIM_<DatabaseName>** database user

  - Member of the **OneIMRole_<DatabaseName>** database role

  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

One Identity Manager database:

- **Admin** database user

  - Member in **db_owner** database role

    The database role is required to update a database with the Configuration Wizard.

  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

Permissions for configuration users

During the installation of the One Identity Manager database using 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**, **Execute**, 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 Server login.

Permissions for end users

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

SQL Server:

- **<DatabaseName>_User** SQL login

One Identity Manager database:

- **OneIMUserRoleDB** database role
    - **Insert**, **Update**, **Select**, and **Delete** permissions for selected tables in the database
    - **View Definition** permissions for the database
    - **Execute** 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** SQL Server login.

Minimum system requirements for administrative workstations

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

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

Table 9: Minimum system requirements - administrative workstations

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

Minimum system requirements for the service server

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

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

Table 10: Minimum system requirements - services server

Processor	8 physical cores 2.5 GHz+
Memory	16 GB RAM
Hard drive storage	40 GB
Operating system	Windows operating systems The following versions are supported: • Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1

- or later

  - Windows Server 2012

  - Windows Server 2012 R2

  - Windows Server 2016

  - Windows Server 2019

Linux operating systems

  - Linux operating system (64-bit), supported by the Mono project, or Docker images provided by the Mono project.

Additional software	Windows operating systems
	• Microsoft .NET Framework Version 4.7.2 or later
	NOTE: Take the target system manufacturer's recommendations for connecting the target system into account.
	Linux operating systems
	• Mono 5.14 or higher

Related topics

Minimum system requirements for the web server

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

Table 11: System requirements - web server

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 2008 R2 (non-Itanium based 64-bit) service pack 1 or later

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Linux operating systems

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

Additional software	Windows operating systems

Windows operating systems

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

Linux operating systems

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

Minimum system requirements for the application server

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

Table 12: System requirements - application server

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 2008 R2 (non-Itanium based 64-bit) service pack 1 or later - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2019 Linux operating systems - Linux operating system (64-bit), supported by the Mono project, or Docker images provided by the Mono project. Note the operating system manufacturer's minimum requirements for Apache HTTP Server.
Additional software	Windows operating systems - Microsoft .NET Framework Version 4.7.2 or later - Microsoft Internet Information Services 10, 8.5, 8, 7.5, or 7 with ASP.NET 4.7.2, and the Role Services: - Web Server | Common HTTP Features | Static Content - Web Server | Common HTTP Features | Default Document - Web Server | Application Development | ASP.NET - Web Server | Application Development | .NET Extensibility - Web Server | Application Development | ISAPI Extensions - Web Server | Application Development | ISAPI Filters

- Web Server | Security | Basic Authentication
- Web Server | Security | Windows Authentication
- Web Server | Performance | Static Content Compression
- Web Server | Performance | Dynamic Content Compression

Linux operating systems

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

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

Users for One Identity Manager

Table 13: 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 detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.
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 detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.
User for configuration tasks in One Identity Manager	The configuration user can execute configuration tasks within the One Identity Manager, for example, creating customer-specific schema extensions or working with the Designer. Configuration users need permissions at the server and database levels. For detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity

User	Permissions
	Manager database in a managed instance in an Azure SQL Database on page 33.
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 detailed information, see Users with granular permission for the One Identity Manager database on an SQL Server on page 26 and Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33.
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 permission group memberships. For detailed information about the 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 One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires access permissions to the internal web service. NOTE: If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access 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 44.

Setting up permissions for creating an HTTP server

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

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

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

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

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

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

`netsh http show urlacl`

Communications ports and firewall configuration

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

The following ports are required:

Table 14: Communications port

Default port	Description
1433	Port for communicating with the One Identity Manager database.
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.
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).

Default port	Description
137	NetBIOS Name Service.
139	NetBIOS Session Service.

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.

3. Set up the server, which handles the SQL processes.

   a. The server must be entered in the database as a Job server with the **SQL processing server** server function.

   b. A One Identity Manager Service with direct access to the One Identity Manager database must be installed and configured on the server.

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

4. Set up an update server for automatic software updating of other servers.

   a. The server must be entered in the database as a Job server with the server function **Update server**.

   b. A One Identity Manager Service with direct access to the One Identity Manager database must be installed and configured on the server.

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

You can also install the following:

- Additional workstations.
- Additional servers with the One Identity Manager Service.
- An application server.
- The Web Portal on a web server.
- The Password Reset Portal on a web server.

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

- The Manager web application on a web server
- Additional web services like SPML Web service or SOAP Web Service.

For detailed information about installing the web services, see the *One Identity Manager Configuration Guide*.

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

- Use the installation wizard to install the One Identity Manager components on workstations for the first time.
- Use the installation wizards to install the One Identity Manager Service on servers for the first time or remote with the Server Installer.
- 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 install-ation and execution of individual Docker components in One Identity Manager containers.

Detailed information about this topic

One Identity Manager Docker images

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

Table 15: Available One Identity Manager Docker images

Docker image	Description
oneidentity/oneim-job	This image executes an instance of a One Identity Manager Service. When started, it downloads the necessary files for a specific Job

Docker image	Description
	server. This behavior can be controlled using encrypted values and environment variables.
oneidentity/oneim-appserver	This image executes an instance of the One Identity Manager application server. When started, it downloads the necessary files from the configured One Identity Manager database. This behavior can be controlled using encrypted values and environment variables.
oneidentity/oneim-web	This image executes an instance of the Web Portal. When started, it downloads the necessary files from the configured One Identity Manager database. This behavior can be controlled using encrypted values and environment variables.
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 executes 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 encrypted values and environment variables.

Before you start installing One Identity Manager

Before you start installing One Identity Manager:

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

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

Detailed information about this topic

Installing One Identity Manager components

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

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

To install the One Identity Manager components

1. Launch autorun.exe from the root directory of the One Identity Manager installation medium.
2. Switch to the **Installation** tab, select the edition, and click **Install**.
3. This starts the installation wizard. On the start page, select the language for the installation wizard.
4. Confirm the conditions of the license.
5. On the **Installation settings** page, enter the following information.
    - **Installation source**: Select the directory containing the installation files.
    - **Installation directory**: Select the directory in which you want to install the files for One Identity Manager.

      NOTE: To make 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 standard installation, no further configuration settings are necessary.
    - **Select installation modules using the database**: Set this option to load the installation data using the existing One Identity Manager database.

      NOTE: Leave this option empty to install the workstation on which you start the One Identity Manager schema installation.
    - **Add further modules to the selected edition**: Set this option to add additional One Identity Manager modules to the selected edition.
6. On the **Module selection** page, also select the modules to be installed.

    NOTE: This page is only shown if you set the **Add more modules to the selected Edition** option.
7. Enter the database connection data on the **Connect to database** page.

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

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

        - OR -

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

Table 16: SQL Server database connection data

Data	Description
Server	Database server.
Windows authentication	Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
User	SQL Server login name.
Password	SQL Server login password.
Database	Database.

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

  The login data required depends on which authentication module you select.

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

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

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

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

10. 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 work station on which you start the installation of the One Identity Manager schema.

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

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

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

12. Close the autorun program.

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

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

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

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

   Logging in using a console connection is recommended. Call this up with

   `Start/Execute: mstsc /Console /v:<servername>`

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

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

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

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

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

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

Related topics

- Installing One Identity Manager components on page 49

Installing and configuring a One Identity Manager database

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

1. Installs the One Identity Manager schema in a database.

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

2. Creates the required SQL Server 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.

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

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

- Configure the database for a test, development, or live system.

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

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

  Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. 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

- Advice on setting up a One Identity Manager database on page 53
- Installing and configuring a One Identity Manager database on page 54
- Configuring a One Identity Manager database for testing, development, or production on page 61
- Encrypting database information on page 62
- One Identity Manager vendor notification on page 68
- Setting up the email notification system on page 70

Related topics

- Minimum system requirements for implementing SQL Servers as database servers on page 22
- Requirements for a managed instance in Azure SQL Database on page 31
- Installing One Identity Manager components on page 49
- Users with granular permission for the One Identity Manager database on an SQL Server on page 26
- Permissions for the One Identity Manager database in a managed instance in an Azure SQL Database on page 33

Advice on setting up a One Identity Manager database

- The following prerequisites must be fulfilled on the workstation from which you want to start the One Identity Manager database setup:
  - 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.

- To ensure that HTML applications are successfully compiled, you must download packages from the NPM repository. Ensure that the workstation you are compiling on, can establish a connection to the registry.n-pmjs.org:443 website.

  Alternatively, you can download packages from a proxy server and install them manually.

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

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

- If you want to install the One Identity Manager schema in an existing database, ensure that the database has the required settings. For more information, see 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.

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

- If you start the Configuration Wizard on a server on which you also want to configure a One Identity Manager Service, simply skip the section for installing the service on the local server in the Configuration Wizard. Install the One Identity Manager Service with the installation wizard in this case. For more information, see Installing and configuring the One Identity Manager Service on page 76.

- If you are working with an encrypted One Identity Manager database, see Advice on working with an encrypted One Identity Manager database on page 67.

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 home page, select the **Create and install a database** option and click **Next**.

3. On the **Create administrative connection** page, execute the following steps to use an existing database.

   a. Enable the **Advanced** option.

   b. In the **Advanced options** pane, set the **Use an existing, empty database for installation** option.

   c. Enter the following connection data for the database.

      - **Server**: Database server.

      - (Optional) **Windows Authentication**: Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

      - **User**: SQL Server Login name of the installation user.

      - **Password**: Password for the installation user.

      - **Database**: Select the database.

   - OR -

   To install a new database, enter the following database connection data on the **Create administrative connection** page.

      - **Server**: Database server.

      - (Optional) **Windows Authentication**: Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

      - **User**: SQL Server Login name of the installation user.

      - **Password**: Password for the installation user.

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

   - OR -

   If you are creating a new database, perform the following tasks on the **Create database** page.

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

Table 17: Database properties

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 data file group and 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. • **<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 employees being administrated.

    b. In the **Installation source** pane, select the directory with 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. Check the module selection in this case.

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

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

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

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

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

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

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

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

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

   Installation and configuration of the database 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 SQL server logins** page, enter the login name, the password, and password confirmation for the SQL Server logins for configuration users and end users.

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

10. On the **System information** page, enter the customer information and create administrative system users for One Identity Manager.

    a. In the **Customer information** view, enter the full name of the company.

    b. In the **System user** view, 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 additional permissions groups

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

ii. Enter the name for the permissions group. Label custom permission groups with the prefix **CCC**.

iii. For role-based permissions groups, enable the **Role-based** option.

11. On the **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.

a. In the **Private key** field, enter the name of the key file.

b. Click **New** and, using the file browser, select the where you want to store the key file.

Click **Save**.

c. Confirm that you have saved the key file.

Take the Advice on working with an encrypted One Identity Manager database on page 67 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**: Name or IP address of the server that the service is installed and started on.
- **Service account**: User account data for the One Identity Manager Service.

  - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.
  - To start the service under another account, disable the **Local**

system account option and enter the user account, password and password confirmation.

- To change the install directory, names, display names or description of the One Identity Manager Service, use the other options.

b. (Optional): Enable the **Advanced** option and enter the **Installation account** data.

- To use the current user's account, set the option **Current user**.

- To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.

c. In the **Machine roles** pane, select the machine role for the service. The **Job server** machine role is defined by default. You can add more machine roles.

d. (Optional) In the **Configuration** pane, check the One Identity Manager Service configuration. Enable the **Advanced** option.

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

e. 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. On the last page of the Configuration Wizard, click **Finish**.

Related topics

- Advice on setting up a One Identity Manager database on page 53
- Error messages when installing and updating the One Identity Manager database on page 161
- Editing a One Identity Manager database during setup using the Configuration Wizard on page 59
- Encrypting database information on page 62

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

- 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 detailed information about system users, access rights and granting permissions, see the *One Identity Manager Authorization and Authentication Guide*.

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

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

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

- 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 execute the processes. The server must be declared as a Job server in the One Identity Manager database.

  During the initial schema installation with the Configuration Wizard, in the One Identity Manager database a Job server is already created for the server on which

the One Identity Manager database is installed. This Job server receives the server functions **SQL processing server** and **Update server**:

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

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

The Configuration Wizard executes the following steps.

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

Related topics

- Automatic updating of One Identity Manager on page 86
-

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

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

Table 18: Database settings for development, test, and live environments

Setting	Database staging level		
	Development environment	Test environment	Live environment
Color of the One Identity Manager tools status bar	None	Green	Yellow
Maximum DBQueue Processor runtime	20 minutes	40 minutes	120 minutes
Maximum number of slots for the DBQueue Processor	5	7	Maximum number of slots according to the hardware configuration

To modify a database staging level

1. Open the Launchpad and select **Database staging level**. Starts the Designer.

2. Select the database and change the value of the **Staging level** property to **Test environment**, **Development environment**, or **Live environment**.

3. Select **Database | Save to database** and click **Save**.

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

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

Table 19: Configuration parameters for the DBQueue Processor

Configuration parameter	Meaning
QBM | DBQueue | CountSlotsMax	This configuration parameter specifies the maximum number of slots to be used. Use this configuration parameter to reduce the number of slots if required. Values lower than **5** are not permitted.
	Exception: Enter a value of **0** for using the maximum number of slots available based on the hardware configuration.
QBM | DBQueue | KeepAlive	This configuration parameter regulates the maximum runtime of the central dispatcher. Tasks on slots currently in use are still processed when the timeout expires. Then the slot database schedules are stopped and the central dispatches exits.
	The lowest permitted value for runtime is **5 minutes**; the maximum permitted value is **720 minutes**.

Related topics

- Creating a One Identity Manager database for a test or development environment from a database backup on page 170

Encrypting database information

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

- In the Designer, choose the **Common | EncryptionScheme** configuration parameter to define which encryption method to use. Permitted values are:

- **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 is used as the method.

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

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.

Detailed information about this topic

Creating a new database key and encrypting the database information

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

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

1. Open the Launchpad and select the **Encrypt database** entry. This starts the Crypto Configuration program.
2. Click **Next** on the start page.
3. On the **New database connection** page, enter the valid connection data for the One Identity Manager database and click **Next**.
4. Select **Create or change database key** on the **Select action** page and click **Next**.
5. Select **There was no encryption yet** on the **Private key** page and click **Next**.

6. Create a new key on the **New private key** page.

   a. Click **Create key**.

   b. Select the directory path for saving the file using the file browser and enter a name for the key file.

   c. Click **Save**.

      The (*.key) key file is generated. The file browser is closed. The path and filename are displayed under **Private key**.

   d. Click **Next**.

      This establishes which data is encrypted.

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

   a. Click **Convert**.

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

      The data encryption is started. Conversion progress is displayed.

   c. Click **Next**.

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

Related topics

- Changing a database key and encrypting the database information on page 64
- Re-encrypting the database information on page 65
- Decrypting the database information on page 66
- Advice on working with an encrypted One Identity Manager database on page 67

Changing a database key and encrypting the database information

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

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

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

1. Open the Launchpad and select the **Encrypt database** entry. This starts the Crypto Configuration program.

2. Click **Next** on the start page.

3. On the **New database connection** page, enter the valid connection data for the One Identity Manager database and click **Next**.

4. Select **Create or change database key** on the **Select action** page and click **Next**.

5. Load the existing key on **Private key**.

   a. Select **Encryption was enabled**.

   b. Click **Load key**.

   c. Using the file browser, select the (*.key) file with the old database key.

   d. Click **Open**.

      The file browser is closed. The path and file name are shown.

   e. Click **Next**.

6. Create a new key on **New private key**.

   a. Click **Create key**.

   b. Select the directory path for saving the file using the file browser and enter a name for the key file.

   c. Click **Save**.

      The (*.key) key file is generated. The file browser is closed. The path and filename are displayed under **Private key**.

   d. Click **Next**.

      This establishes which data is encrypted.

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

   a. Click **Convert**.

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

      The data encryption is started. Conversion progress is displayed.

   c. Click **Next**.

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

Related topics

Re-encrypting the database information

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

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

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

1. Open the Launchpad and select the **Encrypt database** entry. This starts the Crypto Configuration program.

2. Click **Next** on the start page.

3. On the **New database connection** page, enter the valid connection data for the One Identity Manager database and click **Next**.

4. Select **Encrypt using existing key** on the **Select action** page and click **Next**.

   This establishes which data is encrypted.

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

   a. Click **Convert**.

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

      The data encryption is started. Conversion progress is displayed.

   c. Click **Next**.

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

Related topics

- Creating a new database key and encrypting the database information on page 63
- Changing a database key and encrypting the database information on page 64
- Decrypting the database information on page 66
- Advice on working with an encrypted One Identity Manager database on page 67

Decrypting the database information

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

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

To decrypt the One Identity Manager database

1. Open the Launchpad and select the **Encrypt database** entry. This starts the Crypto Configuration program.

2. Click **Next** on the start page.

3. On the **New database connection** page, enter the valid connection data for the One Identity Manager database and click **Next**.

4. Select **Decrypt data** on the **Select action** page and click **Next**.

   This establishes which data is encrypted.

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

    a. Click **Convert**.

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

    c. The data encryption is started. Conversion progress is displayed.

    d. Using the file browser, select the (*.key) file with the database key.

    e. Click **Open**.

       The file browser is closed. The data decryption is started. Conversion progress is displayed.

    f. Click **Next**.

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

Related topics

- Creating a new database key and encrypting the database information on page 63
- Changing a database key and encrypting the database information on page 64
- Re-encrypting the database information on page 65
- Advice on working with an encrypted One Identity Manager database on page 67

Advice on working with an encrypted One Identity Manager database

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

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

To declare the database key

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

Table 20: 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**.

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

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

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

Detailed information about this topic

- Encrypting database information on page 62

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

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.

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

2. Select the **Configure vendor notification** item and click **Start**.

   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 **Database | Save to database** and click **Save**.

Detailed information about this topic

Checking the vendor notification

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

To check whether vendor notification is enabled

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

  Look at the **Configure vendor notification** In the installation view to see is the functionality is enabled.

Detailed information about this topic

- Enabling vendor notification on page 69
- Disabling vendor notification on page 70

Disabling vendor notification

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

To disable a vendor notification

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select **Configure vendor notification** and click **Start**.

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

Related topics

- Enabling vendor notification on page 69
- Checking the vendor notification on page 70

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 executed during process handling.

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

To use the notification system

1. Use the Job Server Editor to set up a Job server as a SMTP host for mail distribution.

2. In the Designer, check the configuration parameters of the email notification system in the **Base data | General | Configuration parameters** category and customize the values.

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

Table 21: General configuration parameters for mail notification

Configuration parameter	Meaning
Common | InternationalEMail	This parameter 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	Notification data.
Common | MailNotification | AcceptSelfSignedCert	If this configuration parameter is set, self-signed TLS connection certificates are accepted.
Common | MailNotification | AllowServerNameMismatchInCert	If this configuration parameter is set, server names that do not match are permitted by TLS connection certificates.
Common | MailNotification | DefaultAddress	Default email address (recipient) for sending notifications.
Common | MailNotification | DefaultCulture	Default language that emails are sent in if no language can be determined for a recipient.
Common | MailNotification | DefaultLanguage	Default language for sending messages.
Common | MailNotification | DefaultSender	Default email address (sender) for sending notifications.
Common | MailNotification | Encrypt	Specifies whether emails are encrypted.
Common | MailNotification | Encrypt | ConnectDC	Domain controller to use.
Common | MailNotification | Encrypt | ConnectPassword	User password. This is optional.
Common | MailNotification | Encrypt | ConnectUser	User account for querying Active Directory. This is optional.

Configuration parameter	Meaning
Common	MailNotification	Encrypt	DomainDN	Distinguished name of the domain to search through.
Common	MailNotification	Encrypt	Encryp- tionCertificateScript	Script that supplies a list of encrypted certificates (default: QBM_GetCertificates).
Common	MailNotification	NotifyAboutWaitingJobs	Specifies whether a message should be sent if the process steps have a particular status in the job queue.
Common	MailNotification	SignCertificateThumbprint	SHA1 thumbprint of the certificate to use for the signature. This can be in the computer's or the user's My Store.
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 for SMTP services on the SMTP server (default: 25).
Common	MailNotification	SMTPRelay	SMTP server for sending notifications.
Common	MailNotification	SMTPUseDefaultCredentials	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.
Common	MailNotification	TransportSecurity	This configuration parameter defined the encryption method for sending notification by email. 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.

Configuration parameter	Meaning
	- **STARTTLS**: Uses the STARTLS 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	Enables the email address of your company's contact person. The email address is used as the return address for notifying vendors.

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

Table 22: Additional parameters for email notifications

Configuration parameter	Description
QER | Attestation | DefaultSenderAddress	This configuration parameter contains the sender email address for messages automatically generated for attestation.
QER | ComplianceCheck | EmailNotification | DefaultSenderAddress	This configuration parameter contains the sender email address for automatically generated messages during rule checking.
QER | ITShop | DefaultSenderAddress	This configuration parameter contains the sender email address for automatically generated messages within the IT Shop.

Configuration parameter	Description
QER | Policy | EmailNotification | DefaultSenderAddress	This configuration parameter contains the sender email address for automatically generated messages within company policy checking.
QER | RPS | DefaultSenderAddress	This configuration parameter contains the sender email address for automatically generated notifications.
TargetSystem | ADS | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the Active Directory target system.
TargetSystem | ADS | Exchange2000 | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the Microsoft Exchange target system.
TargetSystem | ADS | MemberShipRestriction | MailNotification	This configuration parameter contain the default email address for sending warnings by email.
TargetSystem | AzureAD | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the Azure Active Directory target system.
TargetSystem | AzureAD | ExchangeOnline | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the Exchange Online target system.
TargetSystem | CSM | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the cloud target system.
TargetSystem | EBS | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem | LDAP | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the LDAP target system.
TargetSystem | NDO | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the IBM Notes target system.
TargetSystem | SAPR3 | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the SAP R/3 target system.
TargetSystem | SharePoint | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the SharePoint target system.

Configuration parameter	Description
TargetSystem | Unix | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the Unix target system.
TargetSystem | UNS | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the custom target system.
TargetSystem | PAG| DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the Privileged Account Management system.

Related topics

- Setting up Job servers on page 77
- Message: Enter email address in configuration parameter on page 165

Installing and configuring the One Identity Manager Service

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

Setting up a Job server requires the following steps:

- Create an entry for the Job server in the One Identity Manager database.
- Specify the machine roles and server functions for the Job server.

  Installation packages to be installed on the Job server are found, depending on the selected machine roles. The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

- Install the One Identity Manager Service.
- Configure the One Identity Manager Service.
- Start the One Identity Manager Service.

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

Related topics

- Setting up Job servers on page 77
- Remote installation of the One Identity Manager Service with the Server Installer on page 78
- Displaying the One Identity Manager Service log file on page 81
- Changing the user account or One Identity Manager Service start type on page 82
- The One Identity Manager Service in a cluster on page 82
- Updating One Identity Manager on page 94
- Machine roles and installation packages on page 182

Setting up Job servers

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

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

There are several methods for setting up a Job server:

- For the initial schema installation with the Configuration Wizard, you already set up a Job server with the **SQL processing server** and **Update server** server functions. Use the Configuration Wizard to configure the service and install the service remotely on a server.
- To configure further Job servers, use the Server Installer program.

  Using the Server Installer, you create the Job server with its machine roles and server functions in the database. Use the Server Installer to configure the service and install the service remotely on a server.

- You can create Job servers in the Designer.

  In the Designer, you can create a Job server with the machine roles and server functions, configure the service on the server and install the service remotely. For detailed information, see *One Identity Manager Configuration Guide*.

- If a remote installation is not possible, you can install and configure the service locally on a server.

  - Install the service components on the server using the installation wizard.
  - Configure the service using the Job Service Configuration program. For more detailed information about configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.
  - If the **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 54
- Remote installation of the One Identity Manager Service with the Server Installer on page 78

Remote installation of the One Identity Manager Service with the Server Installer

IMPORTANT: If you are working with an encrypted One Identity Manager database, see Advice on working with an encrypted One Identity Manager database on page 67.

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

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

NOTE: 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 detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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

To remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed.

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager 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** menu.

       - 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 One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this unique queue identifier. 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 detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.

- For a direct connection to the database:
    a. 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.

- For a connection to the application server:
    a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
    b. Click the **Connection parameter** entry, then click the **Edit** button.
    c. Enter the connection data for the application server.
    d. Click the **Authentication data** entry and click the **Edit** button.
    e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication

modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.

8. Confirm the security prompt with **Yes**.

9. On the **Select installation source** page, select the directory with the install files.

10. On the **Select private key file** page, select the file with the private key.

    NOTE: This page is only displayed when the database is encrypted.

11. On the **Service access** page, enter the service's installation data.

    - **Computer**: Name or IP address of the server that the service is installed and started on.

    - **Service account**: User account data for the One Identity Manager Service.

        - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.

        - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.

    - **Installation account**: Data for the administrative user account to install the service.

        - To use the current user's account, set the **Current user** option.

        - To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.

    - To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.

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

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

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

Displaying the One Identity Manager Service log file

The One Identity Manager Service log file can be displayed in a browser.

You call up the log file with the appropriate URL:

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

The default value is port 1880.

To open the One Identity Manager Service log file in 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.

Figure 3: The One Identity Manager Service log file
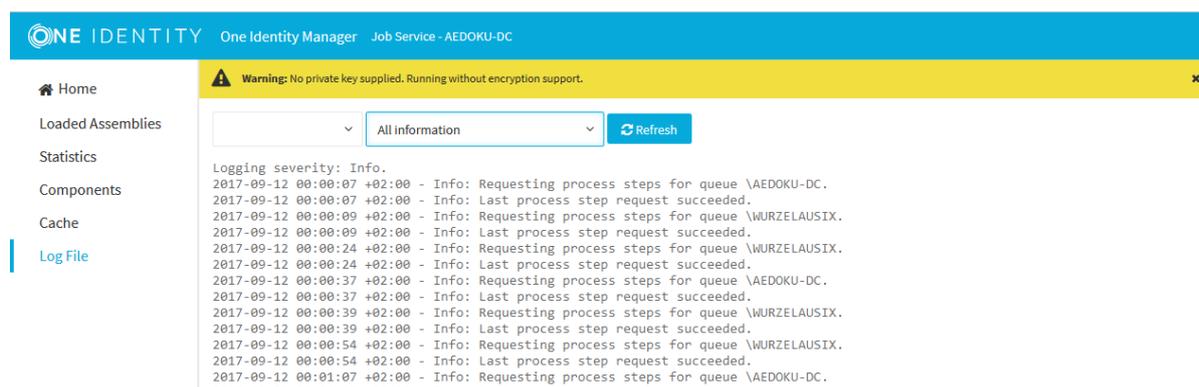
The messages to be displayed on the web page can be filtered interactively. There is a menu on the website for this. Only text contained in the log file can be displayed in this case. For example, if the message type is **Warning**, messages with the **Info** message type cannot also be displayed if the relevant filter is selected.

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

Table 23: 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.

Changing the user account or One Identity Manager Service start type

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

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.

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

NOTE: If you are working with an encrypted One Identity Manager database, see Advice on working with an encrypted One Identity Manager database on page 67.

Related topics

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
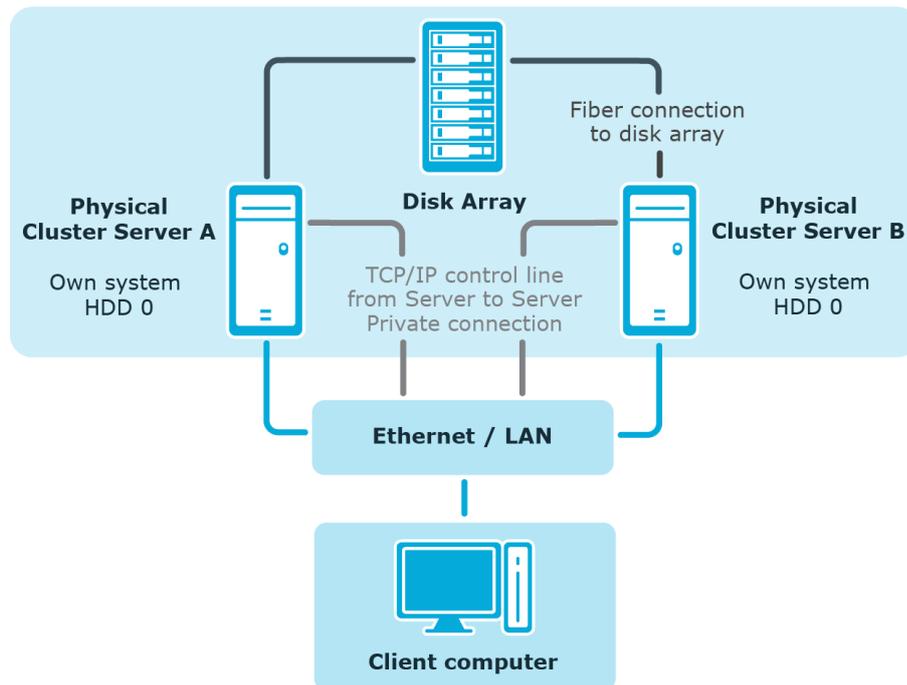
This cluster is made up of two physical computers Server A and Server B that use the same disk array and have their own individual system hard drive. Every server has a Windows operating system. Both servers are installed identically so that in the case of failure one server can take over from the other.

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

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 in the required state (manual or stopped) before registration by the program.

Related topics

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 IdentityOne Identity Manager Service
- In the configuration file of the One Identity Manager Service, adapt the directory information in the **Log file** (OutPutFile) parameter of the log writer.
- Copy the configuration file to all the physical cluster nodes in the One Identity Manager Service install directory after you have changed it.

Related topics

- The One Identity Manager Service in a cluster on page 82
- Registering the One Identity Manager Service in a cluster on page 83

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

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

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

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

The zip archive contains the following files:

- `Update.exe`

- `VI.Base.dll`

- `NLog.dll`

- `Newtonsoft.Json.dll`

- `InstallManager.Msi.dll`

- `InstallManager.Core.dll`

The zip archive is extended with all files from the installation data that correspond to the `*.Update.dll` 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 data, make 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.

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

When a program starts up, VI.DB.dll creates 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 necessary.

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

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

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

Related topics

- User intervention in automatic updating of One Identity Manager tools on page 89

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 executed 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 receives 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 executed.

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

Automatic updating of web applications

In principle, web applications support automatic software 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 **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.

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

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

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

The application then loads the `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

Implementing the automatic software update

The following permissions are required for automatic software updating:

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

To implement automatic software updating

1. Ensure that an update server is set up. This server ensures that the other servers are updated automatically.

    - The server must be entered in the database as a Job server with the **Update server** server function.
    - 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 deactivated, 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 24: Procedure according to the Common | Autoupdate | ServiceUpdateType configuration parameter

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

Disabling automatic 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 automatic update on workstations

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

This disables automatic updating completely on this workstation.

Disabling Job server automatic updating

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

Disabling automatic update of the Web Portal

You can disable Web Portal updates in the database. If the property QBMWebApplication.AutoUpdateLevel is set to the value **1** (inactive), this web application can

no longer be updated by the automatic software update.

Configuring automatic update of an application server

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

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

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

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 by selecting the **Database | Check data consistency** menu item.

   b. In the **Test options** dialog click the icon ⥯.

   c. Activate all tests in the **Database** view and click **OK**.

   d. To start the check, select 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. Execute 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. (From version 7.0.x or version 7.1.x) End the One Identity Manager Service on the server that processes direct database queries.

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

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

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

6. Run a schema update of the One Identity Manager database.

   - 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.

NOTE: If you want to switch to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.4, you will also require an installation user in accordance with Users with granular permission 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, 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. (From version 7.0.x or version 7.1.x) Update the One Identity Manager Service on the server that processes direct database queries.

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

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

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

   c. Click **Install**.

      This starts the installation wizard.

   d. Follow the installation instructions.

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

8. Check the One Identity Manager Service's login information. Revert to the original settings if the One Identity Manager Service did not initially use the local system account for logging in. Specify the service account to 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 project is queued in the Job queue to do this. To execute the process, the One Identity Manager Service must be started on the database server and on all the synchronization servers.

- Check whether the 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 detailed information about applying patches, see the *One Identity Manager Target System Synchronization Reference Guide*.

To update an application server to a new version

- The application server starts updating automatically after the One Identity Manager database schema update.

- To start the update manually, open the status page for the application in the browser and click **Update immediately** in the logged in user's menu.

To update the Web Portal to a new version

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

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

- To manually update the Web Portal, uninstall the existing Web Portal and install the Web Portal again.

To update an API Server to a new version

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

To update the Operations Support Web Portal to a new version

- (As from version 8.1.x) After updating the API Server, compile the HTML application **Operations Support Portal**.

- (As from version 8.0.x)

  1. Uninstall the Operations Support Web Portal.

  2. Install an API Server and compile the HTML application **Operations Support Portal**.

To update the Manager web application to a new version

  1. Uninstall the Manager web application.

  2. Reinstall the Manager web application.

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

Detailed information about this topic

Updating One Identity Manager components

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

In some cases it may be necessary to update the workstations and servers manually using the installation wizard. This 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: When changing versions, use the installation wizard to update the workstation on which the schema installation of the One Identity Manager database is started.

To update a workstation using the installation wizard

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

Table 25: Settings for the installation

Setting	Description
Installation source	Select the directory containing the installation files.
Installation directory	Select the directory of your previous One Identity Manager installation. Otherwise, the components are not updated and a new installation is created in the second directory instead. 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 standard installation, no further configuration settings are necessary.
Select installation modules using the database	Set this option to load the installation information using the existing One Identity Manager database. NOTE: Leave this option empty to install the workstation on which you start the One Identity Manager schema installation.
Add further modules to the selected edition	Set this option to add additional One Identity Manager modules to the selected edition

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

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

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

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

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

      - OR -

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

   Table 26: SQL Server database connection data

Data	Description
Server	Database server.
Windows authentication	Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment

Data	Description
	supports Windows authentication.
User	SQL Server login name.
Password	SQL Server login password.
Database	Database.

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

    The login data required depends on which authentication module you select.

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

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

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

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

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

11. Close the autorun program.

To update the One Identity Manager Service using the installation wizard

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

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

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

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

Related topics

- Automatic updating of One Identity Manager on page 86

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 changes in a test system before you load a transport package in a productive 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 27: 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. 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 productive system database. This transport package is created by the customer and loaded into the database.	Database Transporter

NOTE: If, in additional to a hotfix package, there are additional customized configuration settings to be installed in a One Identity Manager database, create a custom configuration package and use the Database Transporter to import it into the target database. There is no support for merging a hotfix package with a custom configuration package into one transport package.

Related topics

-
-
-

Advice on updating the One Identity Manager database

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

- Before you update the One Identity Manager schema, ensure that the administrative system user, who is going to compile the database, has a password. Otherwise the schema update cannot be completed successfully.

- Use the Configuration Wizard to update the One Identity Manager database if you have received a service pack or complete version update. The Configuration Wizard carries out the update of the schema and transfers the current status to the version history.

- For 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.

NOTE: If you want to switch to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.4, you will also require an installation user in accordance with Users with granular permission 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, 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*.

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

  Alternatively, you can download packages from a proxy server and install them manually.

Detailed information about this topic

Updating the One Identity Manager database with the Configuration Wizard

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

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

To update a database

1. Start the Configuration Wizard.

2. 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 executed.

    d. Set **Add other modules** to select other modules.

5. Select the additional module on the **Select configuration modules** page.

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

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

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

    -   Disconnect the connections on order to start database processing.

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

    NOTE: This page is only shown when updating a One Identity Manager database with version 7.0.x, 7.1.x or 8.0.x to version 8.1.4.

    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/.

    You have the following options:

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

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

    -   **Use the current SQL Server login for the database**: If you select this option, no other SQL server logins are created for the database. In this case,

you cannot work with granular permissions concepts at SQL level. The user you specified is used to connect to the database.

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

9. 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.

   a. You must log in as an administrative user to compile the system.

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

      ii. Click **Log in**.

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

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

    NOTE: This page is only shown when updating a One Identity Manager database with version 7.0, 7.1 or 8.0 to version 8.1.4.

11. 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.

12. On the last page of the Configuration Wizard, click **Finish**.

Related topics

- Advice on updating the One Identity Manager database on page 102
- Editing the One Identity Manager database during update with the Configuration Wizard on page 106
- One Identity Manager vendor notification on page 68

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

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

The Configuration Wizard performs the following steps:

- Updating the One Identity Manager schema.

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

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

Table 28: Operations when importing a migration package

Operations	Description
Insert	If the object is not found in the target database, a new object is generated with the key values.
Refresh	If the object is found in the target database, the object is updated.
Delete	Objects that are no longer needed are deleted.

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

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

- Compiling the system.

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

- Uploading files for automatic software update.

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

- Migration of synchronization projects.

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

Related topics

Installing a hotfix in the One Identity Manager database

IMPORTANT: Test changes in a test system before you install a hotfix in a productive 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
- Modified files, such as *.exe, *.dll or *.vif

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

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

NOTE: If, in additional to a hotfix package, there are additional customized configuration settings to be installed in a One Identity Manager database, create a custom configuration package and use the Database Transporter to import it into the target database. There is no support for merging a hotfix package with a custom configuration package into one transport package.

Detailed information about this topic

Displaying the contents of a transport package with the Database Transporter

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** view, select the **Transport custom modifications** entry. This starts the Database Transporter program.

3. Select **Show transport file**.

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

5. Click **Next** on the **Select transport file** page.

6. The contents of the transport file are displayed on the **Show transport file** page.

   - To display the sequence in which the objects are imported:

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

     b. Click **OK** and enter the connection credentials for the database. This step is only required when you established the first in the order.

        The order in which the entry's objects are imported into the database is found.

     c. Repeat this step for all other entries for which you want to determine the import order.

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

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

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

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

Related topics

Importing a transport package with the Database Transporter

NOTE:

- Test the changes in a test environment before you load a transport package in a production system. Use a copy of the production database for testing.
- To import transport packages with Database Transporter, the user requires the **Allows transport packages to be imported into the database** (`Transport_Import`) program function.
- Start Database Transporter on an administrative workstation.
- The database is set to single-user mode for the duration of the import. Close all existing connections to the database before starting the import.
- When you import a transport package with schema extensions, the database is set to maintenance mode. Objects cannot be processed in the database during this time.
- When you import a transport package with the Database Transporter, the import date and description, the database version, and the transport package name are recorded in the transport history of the target database.

To import a transport package

1. Start the Launchpad and log in to the One Identity Manager database.
2. In the **Change & Extend** view, select the **Transport custom modifications** entry. This starts the Database Transporter program.
3. Select **Import transport file** on the start page.
4. On the **Select the database connection** page, check the One Identity Manager database connection data and change it if necessary.
5. Select the transport package file browser and click **Open**.
6. Specify your import options on **Select transport file**.

Table 29: Import options

Setting	Description
Create a log file for the data import	Enable this option to create a log file for the import. The log file is saved in the output directory of the transport file.
Import objects singly and ignore	Enable this option to import options individually. Errors, which might occur during importing are ignored and displayed when importing is complete. If you do not enable this option, the import procedure is canceled when errors occur.

Setting	Description
errors	
Ignore default data differ- ences	Enable this option to ignore changes to default data during the import. If you do not enable this option, the import procedure is canceled if changes to default data are included.

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

Importing files with the Software Loader

NOTE:

- Start Software Loader on an administrative workstation.

- When selecting the base directory, ensure that a directory hierarchy is not created unintentionally.

- For web applications, select the installation directory of the web application to ensure that the required subdirectories, for example the `bin` directory, are detected correctly.

- For detailed information about how to import customer-defined files using the Software Loader, see the *One Identity Manager Operational Guide*.

To import files into a One Identity Manager database

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

2. In the **Change & Extend** view, select the **Import files for software update** entry. This starts the Software Loader program.

3. Select **Import into database** on the start page.

4. On the **Connect to database** page, check the One Identity Manager database connection data and change if necessary.

5. Specify the file to be imported on **Select files**.

   a. Select the base directory where the files can be found.

   The status and file size of all the files in the selected directory are displayed in the file list.

   Table 30: Meaning of status

Status	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.
Version OK	The file version matches the version in the database.
Version modified	The file version has been modified compared with 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 database, development database and productive database.

a. Select **Assign files to following change label**.

b. Use the button next to the option to select the change label.

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

8. Specify other file settings on **Assign machine roles**.

a. Assign a computer role to the files.

b. (Optional) For more file settings, click **...** next to the file names.

Table 31: More file settings

Setting	Description
Directory source	Directory path in installation source.
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. Click **Finish** on the last page to end the program.

Related topics

- Automatic updating of One Identity Manager on page 86
- Machine roles and installation packages on page 182

Installing and updating an application server

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

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

Detailed information about this topic

Advice for installing an application server

- If you want to run the One Identity Manager Service or the Designer through an application server, the application server requires sufficient permissions for a configuration user. Use the SQL Server login 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 Server login for end users.

- To use the Web Portal or full text search in the Manager, you need an application server with a search service installed on it.

- Start the application server installation locally on the server.

- Use the **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 an application server

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

To install an application server

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

2. Go to the **Installation** tab and select the **Web based components** item and 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, enter the connection credentials for the One Identity Managerdatabase.

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

Table 32: Settings for the installation target

Setting	Description
Application name	Name used as application name, as in the title bar of the browser, for example.
Target in IIS	Internet Information Services web page on which to install the application.
Enforce SSL	Specifies whether insecure websites are available for install-ation. 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	The application's Uniform Resource Locator (URL).
Install dedicated application pool	Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.

Setting	Description
Application pool	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	Permissions for executing an 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 **Custom account** option and entering the user and password.
Web authentication	Specifies the type for authentication 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 employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method if Windows authentication is installed.
	- **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 a SQL database connection on the **Database connection** page.
	Specifies the type for authentication against the One Identity Manager database. You have the following options:
	- **Windows authentication**
	The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible with a user-defined user account or a default identity for

Setting	Description
	the application pool.

- **SQL authentication**

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

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

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

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

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

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

   a. To create a new certificate, enter the following information.

      i. **Session token certificate**: Select **Create new certificate**.

      ii. **Certificate issuer**: Enter the issuer of the certificate.

      iii. **Key length**: Specify the key length for the certificate.

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

   b. To use an existing certificate, enter the following information.

      i. **Session token certificate**: Select the entry **Use existing certificate**.

      ii. **Select certificate**: Select the certificate.

   c. To generate a new certificate file, enter the following information.

      i. **Session token certificate**: Select **Generate new certificate file**.

      ii. **Certificate issuer**: Enter the issuer of the certificate.

      iii. **Key length**: Specify the key length for the certificate.

      iv. **Certificate file**: Enter the directory path and name of the certificate file.

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

8. Specify the user account for automatic updating on the **Set update credentials**

page. The user account is used to add or replace files in the application directory.

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

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

9. (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 configuration file (`web.config`) to do this.

  For detailed information about connecting to the One Identity Manager History Database through an application server and the required configuration, see the *One Identity Manager Operational Guide*.

10. Installation progress is displayed on the **Setup is running** page. After installation is complete, click **Next**.

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

12. Close the autorun program.

> NOTE: The Web Installer generates both the web application and the configuration file (`web.config`). 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 configuration file (`web.config`) in the web application directory in the Internet Information Services.

Related topics

Displaying the application server status

You can access the application server from a browser.

Use the appropriate URL for this:

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

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

> 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 **Enables log display in the application server** program function (AppServer_Logs) can see the log. In addition, API documentation is available here.

Updating an application server

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

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

<autoupdate>

    <!-- <add key="off" value="true" /> -->

    <add key="checkinterval" value="00:05:00"/>

    <add key="inactivitytime" value="00:00:10"/>

</autoupdate>

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

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

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

To start the update manually

1. Open the status page for the application server in the browser.

2. In the menu for the currently logged on user, click **Update immediately**.

Related topics

- Displaying the application server status on page 117
- Automatic updating of One Identity Manager on page 86

Updating the search index on the application server

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

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

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. Choose whether you want to update all indexes, or only some indexes.

Related topics

- Displaying the application server status on page 117
- Log message for search index creation on page 168

Uninstalling an application server

To uninstall a web application

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

2. On the start page 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 One Identity Manager web application** and click **Next**.

4. On the **Uninstall a One Identity Manager web application**, 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.

Installing the API Server

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

To make full use of the API Designer, you must first install the API Server. 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 Windows server using the Web Installer and set it up with the default configuration. For more information about installing using the ImxClient command line program, see *One Identity Manager API Designer User and Development Guide*.

Detailed information about this topic

- Installing the API Server on page 121

Installing the API Server

The following describes how to the install the API Server.

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

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

TIP: You can install the API Server using the ImxClient command line program (**install-apiserver** command). For more information, see the *One Identity Manager API Designer User and Development Guide*.

To install the API Server

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

2. On the start page of the installation wizard, switch to the **Installation** tab in the navigation on the left.

3. Click **Install** next to **Web-based components**.

This starts the Web Installer.

4. On the Web Installer start page, click **Install API Server**.

5. Click **Next**.

6. On the **Database connection** page, do the following:

   | TIP: One Identity recommends using an AppServer connection.

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

     - OR -

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

7. Select the authentication method and enter the login data for the database under **Authentication method**.

8. Click **Next**.

9. On the **Installation source** page, do the following:

   - To retrieve the installation data from the database, activate the **Database** option.

     - OR -

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

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

Table 33: Settings for the installation target

Setting	Description
Application name	Name used as application name, as in the title bar of the browser, for example.
Target in IIS	Internet Information Services web page on which to install the application.
Enforce SSL	Specifies whether the API Server web page can only be opened over an encrypted connection.
URL	The application's Uniform Resource Locator (URL).
Install dedicated application pool	Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.
Application pool	The application pool to use. This can only be entered if the option **Install dedicated application pool** is not set. If you use the default value **DefaultAppPool**, the application

Setting	Description
	pool has the following syntax:
	`<application name>_POOL`
Identity	Permissions for executing an 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.
Web authentication	Specifies the type for authentication 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. The web application logs in the employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method is Windows authentication is installed. • **Anonymous** Login is possible without Windows authentication. The user is authenticated against the Internet Information Services and the web application anonymously. The web application is rerouted to a login page.
Database authentication	NOTE: You can only see this pane if you have selected a SQL database connection on the **Database connection** page. Specifies the type for authentication against the One Identity Manager database. You have the following options: • **Windows authentication** The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible with a user-defined user account or a default identity for the application pool. • **SQL authentication** Login is only possible through a user-defined user

Setting	Description
	account. Authentication is done using user name and password. This access data is saved in the web application configuration as computer specific encrypted.

11. Click **Next**.

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

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

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

    a. Click **Select application server**.

    b. Enter the application server's web address in the **URL** field.

    c. Click **OK**.

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

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

    - To use an existing certificate:

        a. In the **Session token certificate** list, select **Use existing certificate**.

        b. Select an existing certificate from the **Select certificate** list.

    - To create a new certificate:

        a. In the **Session token certificate** list, select **Create new certificate**.

        b. In the **Certificate issuer** field, the name of the certificate issuer.

        c. Select the key length of the certificate from the **Key length** list.

    - To create a new certificate file:

        a. In the **Session token certificate** list, select **Create new certificate file**.

        b. In the **Certificate issuer** field, the name of the certificate issuer.

        c. Select the key length of the certificate from the **Key length** list.

        d. In the **Certificate file** field, enter the path and file name for the new certificate.

15. Click **Next**.

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

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

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

17. Click **Next**.

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

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

19. Click **Next**.

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

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

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

22. Close the autorun program.

Related topics

- Uninstalling the API Server on page 126

Installing and accessing HTML5 applications

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

To install and compile HTML applications

1. Start the Designer.

2. Connect to the relevant database.

3. In the navigation, select **Getting Started | Edit configuration parameters**.

4. On the **Configuration parameters** tab, enable the **QBM | HtmlDevelopment | Compiler** configuration parameter.

5. Recompile the database.

NOTE: Ensure that the workstation you are compiling on, can establish a connection to the `registry.npmjs.org:443` website.

To access all installed HTML5 applications

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

  All installed HTML5 applications are displayed.

Related topics

-

Uninstalling the API Server

To uninstall a web application

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

2. On the start page 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 One Identity Manager web application** and click **Next**.

4. On the **Uninstall a One Identity Manager web application**, 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, configuring, and maintaining the Web Portal

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

Detailed information about this topic

Installing the Web Portal

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

NOTES:

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

- Prepare an application server on which the search service for the Web Portal is installed.

- Start the Web Portal installation locally on the server.

- If you install the Web Portal with HTTPS, the transfer method for cookies is configured to use HTTPS in the Web Installer.

- If you change the SSL settings for the Web Portal at a later time, you must

manually update the value in the Web Portal's `web.config` configuration file.

- Default values are used for the configuration settings during installation. You can keep these values. Check the settings using the Web Designer Configuration Editor.

  ### *To make a modification*

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

To install the Web Portal

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

2. On the start page of the installation wizard, switch to the **installation** tab in the navigation on the left.

3. Click **Install** next to **Web-based components**.

   This starts the Web Installer.

4. On the Web Installer start page, click **Install Web Portal**.

5. Click **Continue**.

6. On the **Database connection** page, do the following:

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

      - OR -

    - to create a new connection to the One Identity Manager database, click **Add new connection** and enter a new connection. For more information, see Configuring the database connection on page 134.

7. Select the authentication method and enter the login data for the database under **Authentication method**.

8. Click **Continue**.

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

   Table 34: Settings for the installation target

Setting	Description
Application name	Name used as application name, as in the title bar of the browser, for example.
Target in IIS	Internet Information Services web page on which to install the application.
Enforce SSL	Specifies whether insecure websites are available for installation. If the option is set, only sites secured by SSL can be used for installing. This setting is the default value. If this option is not set, insecure websites can be used for installing.

Setting	Description
URL	The application's Uniform Resource Locator (URL).
Install dedicated application pool	Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.
Application pool	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	Permissions for executing an 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 **Custom account** option and entering the user and password.
Web authentication	Specifies the type for authentication 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 employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method if Windows authentication is installed. • **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 a SQL database connection on the **Database connection** page. Specifies the type for authentication against the One Identity

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

10. Click **Continue**.

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

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

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

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

    a. Click **Select application server**.

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

    c. Click **OK**.

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

13. On the **Installation source** page, perform one of the following actions in the **Installation source** area:

    • to retrieve the installation data from the database, activate the **Load from database** option.

      - OR -

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

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

   NOTE: If no further authentication settings are required, the message **No authentication data required** is displayed.

   a. Click .

   b. In the **Authentication data** dialog, click a red project.

   c. Under **Authentication method**, specify the method and login data you would like to use.

   d. Repeat these steps for all other red projects.

   e. Click **OK**.

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

   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.

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

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

   - **Use IIS credentials for update**: Set this option to use the user account used by the application pool to run updates.

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

17. Click **Continue**.

18. On the **Application token** page, enter the application token for the Web project.

   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.

   NOTE: Handle the application token like as 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.

19. Click **Continue**.

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

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

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

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

23. Click **Continue**.

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

25. Close the autorun program.

Related topics

Updating the Web Portal

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

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

To update the web application automatically

1. Open the Runtime Monitor in the browser.

2. On the **Status** tab, select either the **Update now** or the **Update when all user sessions are closed** options.

To update a web application manually

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

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

Related topics

- Configuring the automatic update for the Web Portal on page 138
- Automatic updating of web applications on page 90
- Installing the Web Portal on page 127
- Displaying the runtime monitor on page 141
- Maintenance mode on page 142

Uninstalling the Web Portal

To uninstall a web application

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

2. On the start page 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 One Identity Manager web application** and click **Next**.

4. On the **Uninstall a One Identity Manager web application**, 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.

Configuring the Web Portal

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

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

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

To configure a web application

1. Start the WebDesigner.ConfigFileEditor.exe program from the installation directory of the web application.

2. Select the **web.config** configuration file in the Open configuration file view and click **Open**.

3. Select the required authentication procedure and log on.

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

Detailed information about this topic

- Configuring the database connection on page 134
- Authentication data for the web application on page 135
- Logging for the web application on page 137
- Configuring the automatic update for the Web Portal on page 138
- Advanced web settings on page 139
- Storing the cache directories on page 139
- Configuring the debugger service on page 140
- Configuring the search service on page 140

Configuring the database connection

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

To select a new database connection

1. Open the Web Designer Configuration Editor.

2. In the **Database connection** view, click the **Enter new connection** link.

3. Select the system type and enter the connection data:

   - For the **SQL Server** system type, enter the following information.

   Table 35: SQL Server database connection data

Data	Description
Server	Database server.
Windows authentication	Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
User	SQL Server login name.
Password	SQL Server login password.
Database	Database.

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

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

Related topics

- Logging in to the One Identity Manager database on page 152

Authentication data for the web application

The authentication data for the web project and subprojects is configured in the Web Designer Configuration Editor in the **Web project** area. For detailed information about the authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

Table 36: Authentication data for the web project

Setting	Description
Web project	Name of the web project.
Authentication module	Authentication module for logging on to the web project. NOTE: Some authentication modules support single sign-on. In such cases, a corresponding message is shown beneath selection.

Setting	Description
Perform single sign-on, if an error occurs, using the following module.	If the module selected under **Authentication module** supports single sign-on, you have the option to specify an alternative authentication method here. This authentication method is used as a fallback if single sign-on fails for any reason.
Debugging	Activate this option if you want to use a debugging environment.
OAuth	If you use the **OAuth 2.0 / OpenID Connect** or **OAuth 2.0 / OpenID Connect (role-based)** authentication modules, make your configuration settings here.
OAuth 2.0 / OpenID Connect configuration	Select the OAuth 2.0 / OpenID Connect configuration that you want to adjust.
Client ID for OAuth authentication	ID of the application on the identity provider. Example: urn:OneIdentityManager/Web
Issuer information for the OAuth certificate	This is used to find the certificate in the certificate store. Either the thumb nail or the issuer of the certificate is required. For example: `O=[company name], OU=[organizational unit], CN=[server IP]`
OAuth Resource	Uniform Resource Name (URN) of the resource to be queried. Only required if the identity provider requires this value.
Thumbprint for the OAuth certificate	Thumbprint of the certificate used to verify the security token. Either the thumb nail or the issuer of the certificate is required.
Endpoint	Uniform Resource Locator (URL) of the certificate end point on the authorization server. For example: https://certificateServer/certificate.crt
Authentication data for subprojects	Authentication data for subprojects.

To enter or change authentication data for a sub project

1. Open the Web Designer Configuration Editor.

2. In the **Web project** pane, next to the **Authentication for sub projects is missing** message, click 🗐.

3. In the edit view, click on the project marked in red.

4. In the **Authentication method** pane, select the required authentication procedure and enter the required login information.

5. Click **OK**.

Logging for the web application

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

- General
- Application log
- Event log
- Database log

Table 37: General settings for logging

Setting	Description
Application	Name of the web application.
Company name	Name of the company that uses the web application.
Product title	Software manufacturer's product name
Log directory	Directory in which the log files of the web application are saved. The web server process must have write access to this folder.

Table 38: Application log settings

Setting	logging
Severity code	Severity level of the log.
Archive every	Maximum runtime of a log file before it is renamed. When a log file has reached its maximum age, the file is renamed and a new log file is started.
Archive numbering	Specifies whether the archive files of the application log are numbered in ascending or descending order.

Table 39: Event log settings

Setting	Description
Severity code	Severity level of the log.

Table 40: Database log settings

Setting	Description
Severity code	Severity level of the log.

Setting	Description
Archive every	Maximum runtime of a log file before it is renamed. When a log file has reached its maximum age, the file is renamed and a new log file is started.
Archive numbering	Specifies whether the archive files of the database log are numbered in ascending or descending order.

Table 41: Permitted severities

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

Configuring the automatic update for the Web Portal

NOTE: The following permissions are required for automatic updating:

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

The automatic update is configured in the Web Designer Configuration Editor in the **Automatic update** pane.

To configure the automatic update of the web application

1. Open the Web Designer Configuration Editor.

2. In the **Automatic updates** pane, set the **Enable automatic updates** option.

3. Define the user account for the automatic update. The user account is used to add or replace files in the application directory.

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

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

Related topics

- Automatic updating of One Identity Manager on page 86
- Automatic updating of web applications on page 90
- Updating the Web Portal on page 132

Advanced web settings

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

Table 42: Web setting

Setting	Description
HTML headers	HTTP header lines that the server outputs for every HTTP query.
After logging off	Page that is displayed after the user has logged off.
Close session after idle time (minutes)	Period of inactivity after which the session is closed. NOTE: Enter the value 0 if you want the session to remain open despite being idle.
Compress HTTP transfer	Specifies whether the HTTP transfer takes place in compressed form.
Create Windows performance indicators	When you install a web application, performance counters are registered, which provide information about the state of the application. For detailed information, see the Using the performance indicators for monitoring on page 143.

Storing the cache directories

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

Table 43: Settings for cache directories

Setting	Description
Cache directory	Full path to the directory used for temporary saving of frequently used application contents.
Assembly cache	Full path to the directory for caching assembler files.

Configuring the debugger service

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

To restrict the port range of the WCF connection

1. Open the Web Designer Configuration Editor.

2. In the **Debugger service** pane, enable the **Limit port range** option and define the limits for the port using the connection.

Configuring the search service

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

- If you run the Web Portal directly over an application server installed with the search service, you can use the full text search immediately.

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

  The application server is usually entered during the Web Portal installation. For subsequent changes, use the Web Designer Configuration Editor.

To enter an application server at a later date

1. Open the Web Designer Configuration Editor.

2. In the **Search service** pane, click **Select application server**.

3. Enter the application server's web address in the **URL**.

4. Test the connection by selecting **Test connection** from the **Options** menu.

5. Edit other optional settings by selecting **Advanced settings** from the **Options** menu.

6. To accept the settings, click **OK**.

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

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

Related topics

Maintenance of the Web Portal

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

Detailed information about this topic

Displaying the runtime monitor

The Web Portal includes a runtime monitor for monitoring. The runtime monitor is accessed over a browser front end.

Use the appropriate URL for this:

    http://<servername>/<application>/monitor

Related topics

Access permissions for the runtime monitor

Access to the runtime monitor is configured in the configuration file (`monitor.config`) of the web application. The default settings enables only members of the **BUILTIN\Administrators** group to access the runtime monitor.

```
<?xml version="1.0"?>
```

```
<!-- Permission to use WebDesigner runtime monitor -->
```

```
<authorization>
```

```
      <allow roles="BUILTIN\Administrators" />
```

```
      <deny users="*" />
```

```
</authorization>
```

For more information about changing this setting, see the ASP.NET documentation.

Log files and exceptions

The log files are displayed in the Runtime Monitor.

- All log files generated by the web application are displayed on the **Log files** tab.

  You can filter these file and search by strings. The log files exist in physical form in the log directory defined by the configuration in the configuration file of the web application, usually `./Logs`).

- The **Exceptions** tab display log messages that contain exception errors. These messages are sorted by exception error and in descending order of frequency. The top exception error in the list is the error that occurs most frequently.

NOTE: The Web Installer writes important events to the log file of the application. You can view this log file in the Windows event display.

Related topics

Maintenance mode

To carry out maintenance work, switch the web application to maintenance mode. You use maintenance mode, for example, to enable an update at a particular time.

No new sessions are permitted in maintenance mode. Current sessions are not affected. While maintenance work is being performed, users who view the web application are displayed the contents of the `Maintenance.html` file, which is located in the installation

directory of the web application. You can edit this file to display details of the maintenance work for the user.

To switch the web application to maintenance mode

1. Open the Runtime Monitor in the browser.

2. On the **Status** tab, click **Start maintenance mode**.

To end maintenance mode

1. Open the Runtime Monitor in the browser.

2. On the **Status** tab, click **End maintenance mode**.

Maintenance mode can also be activated by creating the file `App_Data\Maintenance.mode` in the installation directory of the web application, and terminated by deleting this file.

Related topics

Using the performance indicators for monitoring

When you install a web application, performance counters are registered, which provide information about the state of the application.

Performance indicators can be installed later.

NOTE: Prerequisites for this are that the web application is installed on a Windows Server and has sufficient permissions to offer performance indicators. It may be necessary to add the application pool user account to the local group **Performance monitoring user** for this. Apart from this, the web application must be running in order to select the performance indicators.

To post-install performance indicators

1. Open the Web Designer Configuration Editor.

2. Click **Web settings** and **Create Windows performance counters**.

    After this is successfully completed, an installation prompt is displayed.

3. Confirm the prompt with **OK**.

To view performance counters

1. Log in to the server on which the web application is installed.

2. Start performance monitoring of Windows.

3. In the dialog on the left-hand side, select **Performance monitoring**.

4. In the performance monitoring view, click ✚.

5. In the **Add Counters** dialog, under **Available Counters**, select **One Identity ManagerWeb Portal** and add to the entry.

This displays performance indicators for the web application. The following indicators are available.

Table 44: Performance indicators

Performance indicator	Description
AJAX calls	Number of HTTP queries processed asynchronously.
Objects	Number of active database objects.
Exceptions	Number of exception errors that have occurred.
Forms	Number of active forms.
HTML requests	Number of HTML page requests.
PID	Number of process IDs.
Contexts	Number of active module objects.
Sessions	Number of active sessions.
Sessions total	Total number of sessions since the application started.

6. Enter any new performance indicators you wish and select the web application under **Instances of selected object:**.

TIP: Only running web applications are displayed for selection. If you install a new web application, it may take a few minutes before the list of available web applications including the new one is available.

Installing and updating the Manager web application

Manager functionality can be provided by web applications. Before installation ensure that the minimal hardware and software prerequisites are fulfilled on the server.

Detailed information about this topic

Installing the Manager web application

One Identity Manager requires each web application to be defined in one language. If you wish to publish an application in two languages, you must install two separate applications. Web Installer installs one application per language by default.

You can define a language pool for these applications if several application are running at once. If a user calls up a web application from the language pool, he is automatically diverted to the web application which matches his language. It is, therefore, not important to declare all the web application URLs in the language pool.

This mechanism also allows you to achieve simple load balancing.

IMPORTANT: Start the Manager web application installation on the server.

To install the Manager web application

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

2. Go to the **Installation** tab and select the **Web based components** item and 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, enter the connection credentials for the One Identity Manager database.

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

Table 45: Settings for the installation target

Setting	Description
Application name	Name used as application name, as in the title bar of the browser, for example.
Target in IIS	Internet Information Services web page on which to install the application.
Enforce SSL	Specifies whether insecure websites are available for install-ation. 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	The application's Uniform Resource Locator (URL).
Install dedicated application pool	Specifies whether an application pool is installed for each application. This allows applications to be set up independently of one another. If this option is set, each application is installed in its own application pool.
Application pool	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	Permissions for executing an 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 **Custom account** option and entering the user and password.
Web authen-tication	Specifies the type for authentication against the web application. You have the following options:
	• **Windows authentication (single sign-on)**

Setting	Description
	The user is authenticated against the Internet Information Services using their Windows user account and the web application logs in the employee assigned to the user account as role-based. If single sign-on is not possible, the user is diverted to a login page. You can only select this authentication method if Windows authentication is installed.
	• **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 a SQL database connection on the **Database connection** page.
	Specifies the type for authentication against the One Identity Manager database. You have the following options:
	• **Windows authentication**
	The web application is authenticated against the One Identity Manager database with the same Windows user account that your application pool uses. Login is possible with a user-defined user account or a default identity for the application pool.
	• **SQL authentication**
	Authentication is completed with a SQL Server login and password. The SQL Server login from the database connection is used. Use the [**...**] button to enter a different SQL login, for example, if the application is executed with a access level for end users. This access data is saved in the web application configuration as computer specific encrypted.

6. Specify other application specific settings on the **Configuration** page.

   a. Select the language of the application from the **Language** menu. The language influences how dates and numbers displayed amongst other things.

   b. The web application requires access permissions to itself. If you selected the **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.

7. Specify the user account for automatic updating on the **Set update credentials**

page. The user account is used to add or replace files in the application directory.

- **Use IIS credentials for update**: Set this option to use the user account under which the application pool is executed for the updates.
- **Use other credentials for updates**: To use a different user account, set this option. Specify the domain, the user name, and the user password.

8. Installation progress is displayed on the **Setup is running** page. Once installation is complete, click **Next**.

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

NOTE: The Web Installer generates both the web application and the configuration file (`web.config`). The Web Installer uses default values for the configuration settings. You can keep these values. It is recommended you check the settings with the help of the Manager Web Configuration Editor. You will find the configuration file (`web.config`) in the web application directory in the Internet Information Services.

Related topics

- Updating the Manager web application on page 148
- Advanced configuration of the Manager web application on page 172

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>

Updating the Manager web application

NOTE:

- We recommend that you perform the automatic update only in specific maintenance windows, in which the application cannot be accessed by users and the application can be manually restarted with no risk.
- The following permissions are required for automatic updating:
    - The user account for updating requires write permissions for the application directory.
    - The user account for updating requires the **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** plugin 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

Uninstalling the Manager web application

To uninstall a web application

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

2. On the start page of the installation wizard:

   a. 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 One Identity Manager web application** and click **Next**.

4. On the **Uninstall a One Identity Manager web application**, 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.

Logging in to One Identity Manager tools

When you start one of the One Identity Manager tools, a default connection dialog opens.

Figure 5: Default connection dialog
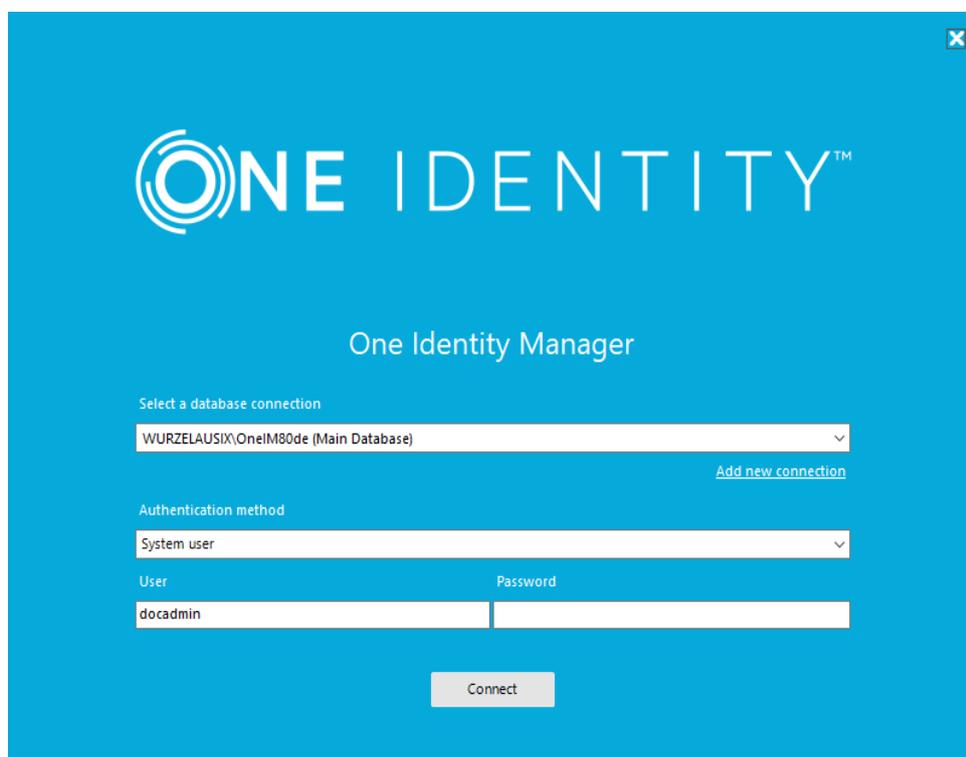
When you log in, you need to be aware of the difference between a database user and a user of individual One Identity Manager tools (system user). Several system users can work with one database user.

Login takes place in two steps:

- Selecting the database connection to log in to the database
- Selecting the authentication method and finding the system user for logging in

  Permitted system user IDs are determined by the authentication module you select. One Identity Manager provides various authentication modules for this purpose.

The One Identity Manager tools can only be started if the user has the relevant program function permissions. Some administration tools expect a specific access level for the selected SQL Server login.

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

NOTE: When you start the program, it tries to restore the last used connection. This 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"

Detailed information about this topic

- Logging in to the One Identity Manager database on page 152
- Logging in to the One Identity Manager tools using a system ID on page 154
- Enabling additional authentication modules on page 156
- Enabling additional login languages on page 157
- Checking authentication on page 158
- Password expiry on page 157

Logging in to the One Identity Manager database

To select an existing connection

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

NOTE:

- Newly created connections are not shown in the connection dialog until the program has been restarted.
- Connections that do not use the expected access level for SQL Server logins are not shown in the connection dialog.
- The access level for an existing connection is shown in the menu item's tooltip.

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

To create a new connection to the One Identity Manager database

1. Under **Select a database connection**, click **Add new connection** and select the **SQL Server** system type.

2. Click **Next**.

3. Enter the connection data for the database server.

   Table 46: SQL Server database connection data

Data	Description
Server	Database server.
Windows authentication	Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
User	SQL Server login name.
Password	SQL Server login password.
Database	Database.

4. Select **Test connection** in the **Options** menu.

   This attempts to connect the database with the given connection data. You are prompted to confirm a message about the test.

   NOTE: Using **Options | Advanced option** item, you can make additional changes to the connection configuration.

5. Click **Finished**.

To set up a new connection to the application server

1. Under **Select a database connection**, click **Add new connection** and select the **Application server** system type.

2. Click **Next**.

3. Enter the address (URL) for the application server.

4. If you access an application server secured through SSL/TLS, configure additional settings for the certificate:

   - If the certificate's server name matches the application server's URL and, if the server certificate can be successfully validated, the server name displayed in green next the URL. By clicking the server name next to the URL, you can get information about the certificate. You can select a certificate required for logging in, under **Pin server certificate**.

- If the certificate's server name does not match the application server's URL or, if the server certificate cannot be successfully verified, the server name 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.

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 the **Options | Advanced options** menu item, you can make additional changes to the connection configuration.

6. Click **Finished**.

To delete a connection

1. Select the connection under **Select a database connection**.

2. Press **DEL**.

3. Confirm the security prompt with **Yes**.

   The database connection is no longer displayed in the connection dialog.

Related topics

- Logging in to the One Identity Manager tools using a system ID on page 154

Logging in to the One Identity Manager tools using a system ID

Following the database login, the user must log in to the program as a system user. Permitted system user IDs are determined by the authentication module you select.

NOTE:

- After the initial schema installation, only the **System user** and **ComponentAuthenticator** authentication modules and the role-based authentication modules are enabled in One Identity Manager.

- The One Identity Manager tools can only be started if the user has the relevant program function permissions.

- 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.

To log in to One Identity Manager tools with a system user identifier

1. Select the authentication module under **Authentication method** in the connection dialog.

   This displays a list of all available authentication modules.

2. Enter the login data for the system user ID.

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

3. Click **Connect**.

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

Figure 6: Login window
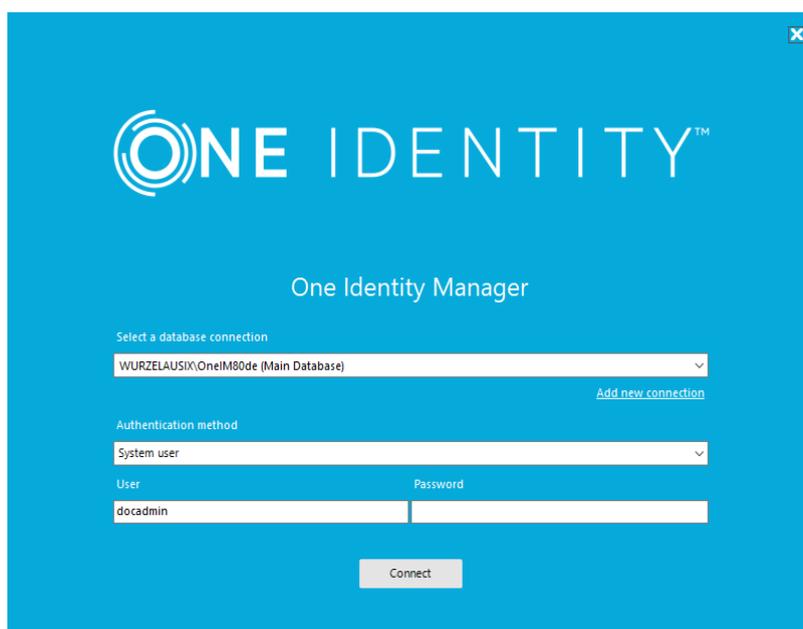
For detailed information about the One Identity Manager authentication modules and program functions, see the *One Identity Manager Authorization and Authentication Guide*.

Related topics

- Logging in to the One Identity Manager database on page 152
- Enabling additional authentication modules on page 156
- Error messages logging in to One Identity Manager tools on page 160

Enabling additional authentication modules

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

To enable an authentication module

1. In 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. Save the changes.

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 additional login languages on page 157

Enabling additional login languages

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.

Related topics

- Language settings in One Identity Manager on page 156

Password expiry

There are different ways to inform employees that their password is going to expire:

- Users are alerted about their password expiring when they log in to One Identity Manager and can change their password if necessary.

- For employee-based authentication modules, the system sends reminder notifications in relation to expiring passwords as of 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 **Employee - 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 when the next permissions based action on the connection at 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.

Troubleshooting

For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.

Displaying the transport history and checking the One Identity Manager version

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

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

To display transport history

- Start the Designer and select the **Help | Transport history** menu item.

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.

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

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

Related topics

- One Identity Manager vendor notification on page 68

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 employee used for the login is deactivated.
- The user account used for the login is deactivated.

Solution

Check your login information.

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, check under **Permissions | Program functions** to see which permissions group contains the required program function.
    - For non role-based logins, add the system user to the permissions group in the Designer under **Permissions | System users**.

- For role-based logins, ensure that the user is assigned to the application role that contains the program function.

For detailed information about the One Identity Manager authentication modules, permissions groups and application roles, as well as program functions, see the *One Identity Manager Authorization and Authentication Guide*.

Error messages when installing and updating the One Identity Manager database

Before the installation or update of the One Identity Manager database starts, the Configuration Wizard checks the settings of the database server and the database required for the installation and operation of the One Identity Manager database. For more information, see 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 47: Messages in Configuration Wizard before a database installation or update starts

Message	Solution
The SQL Server Agent did not start.	Start the SQL Server Agent in the SQL Server Service Management Portal. You can log in to a SQL Server Agent both with a domain user account (**Domain users**) with Windows authentication as well as with a local system account.
The database collation setting is not valid. SQL_Latin1_General_CP1_CI_AS is required.	Set the **Sort order** (collation) database property to the value **SQL_Latin1_General_CP1_CI_AS**.
The migration cannot be executed because a replication is currently running.	For more information, see Database errors when migrating a database in SQL Server AlwaysOn availability groups or database mirroring on page 163.
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.

Message	Solution
The Service Broker cannot be activated because other users are still active.	End other user's connections to the database.
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 detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
	The Configuration Wizard has the option to ignore this message. Only use this option in test or development environments. By updating the database, modifications may be made 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.
At least one Agent job has a different owner to that of	Select a user who has at least administrative permissions for the One Identity Manager database to update the One

Message	Solution
the current user. This can lead to errors if the DBQueue Processor is stopped.	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.

Database errors when migrating a database in SQL Server AlwaysOn availability groups or database mirroring

Possible problems

- The data does not start updating. The Configuration Wizard shows the message:

  `The migration cannot be executed because a replication is currently running.`

- The following error occurs during a One Identity Manager schema update:

  `Database error 1468: The operation cannot be performed on database "<database name>" because it is involved in a database mirroring session or an availability group. Some operations are not allowed on a database that is participating in a database mirroring session or in an availability group. ALTER DATABASE statement failed.`

Cause

The database is part of an AlwaysOn availability group or is participating in a database mirroring.

Solution

1. Remove the database from the AlwaysOn availability group or the database mirroring.

2. Update the One Identity Manager schema.

3. Re-admit the database to the AlwaysOn availability group or the database mirroring.

DBQueue Processor does not process tasks

Possible issues

- After restoring a One Identity Manager database from a database backup, no DBQueue Processor tasks are handled.

- If the SQL Server in running on a virtual machine and the virtual machine is suspended, it is possible that no DBQueue Processor tasks are handled after restarting the virtual machine.

Probable reason

The SQL Server Service Broker cannot be reactivated during initialization of the DBQueue Processor. The Service Broker is implemented for DBQueue Processor communications.

Solution

Execute the following steps using a suitable program for executing SQL queries in the database:

IMPORTANT: Select a user that you use for migrating the database to execute the SQL queries.

1. Stop all DBQueue Processor components.

   exec QBM_PWatchDogPrepare 1

   go

   exec QBM_PDBQueuePrepare 1

   go

2. Check whether other database sessions are active.

   select *

   from sys.sysprocesses p

   where dbid = DB_ID()

   and spid <> @@SPID

   If there are still sessions active, they must be closed first.

3. Create a new ServiceBroker ID and enable message delivery.

   alter database <database name> set NEW_BROKER

   go

   alter database <database name> set enable_broker

   go

4. Initializing the DBQueue Processor.

```
exec QBM_PDBQueuePrepare 0,1

go

exec QBM_PWatchDogPrepare

go
```

NOTE: If you restore a test or development database from a backup of another One Identity Manager database, these steps are executed by the Database Compiler. Manual execution of the steps is not necessary in this case. For more information, see Creating a One Identity Manager database for a test or development environment from a database backup on page 170.

Message: Enter email address in configuration parameter

In a process for sending emails, the value of the `SenderAddress` or `Address` parameter is `<Enter email address in configuration parameter "...">`. Check process parameters in Job Queue Info.

The message is also sent to the One Identity Manager Service log file if extended error reporting in debug mode is configured for the One Identity Manager Service.

Probable issue

One Identity Manager sends email notifications about various actions taken within the system. One Identity Manager email notification system is not completely configured.

Solution

- In the Designer, check the configuration parameters of the email notification system in the **Base data | General | Configuration parameters** category and customize the values.

Detailed information about this topic

- Setting up the email notification system on page 70

Operations Support Web Portal is not displayed

Problem

An empty page is displayed in the Internet Explorer if the Operations Support Web Portal is opened with the URL.

Possible cause

The Operations Support Web Portal should be displayed on an intranet page and the **Display intranet sites in compatibility view** setting enabled in the web server.

Solution

In the configuration file (`web.config`) of the Web Portal application, extend the `<system.webServer>` section. Enter an attribute or compatibility mode:

```
<system.webServer>

    ...

    <httpProtocol>

        <customHeaders>

        ...

        <add name="X-UA-Compatible" value="IE=11" />

        ...

        </customHeaders>

    </httpProtocol>

</system.webServer>
```

Removing superfluous modules

You can remove modules from the One Identity Manager database that you no longer require in your system.

IMPORTANT:

- By removing a module, you lose all the data that goes with it. So it is important to make a backup of the One Identity Manager database before removing any modules.

- In certain circumstances, dependencies to other modules may be deleted by removing a module. Therefore, update the One Identity Manager schema after

removing a module.

- Other tests may be necessary after removing a module. Remove the module in your test environment first and test the One Identity Manager functionality thoroughly. Make sure to also check any custom adaptations that may use functions in the modules that have been removed.

To remove a module

1. Terminate all web applications using the Internet Information Services (IIS) Manager.
2. Close all One Identity Manager tools except for Job Queue Info.
3. Wait until all processes have terminated. You can do this using the Job Queue Info.
4. Close all One Identity Manager Services through the services manager.
5. Terminate all application servers using the IIS Manager.
6. Wait until all DBQueue Processor tasks have completed. You can do this using the Job Queue Info.
7. Close Job Queue Info.
8. Start a suitable program for executing SQL queries.

   IMPORTANT:

   - Select a user that you use for migrating the database to execute the SQL queries.
   - Execute the following steps separately using a suitable program for executing SQL queries.

     Test the output of the query after each step. The output provides additional advice about removing a module.

   a. Activate single-user mode for the One Identity Manager database.

      ```
      exec dbo.QBM_PSingleUserRequest @@spid
      ```

   b. Stop the DBQueue Processor components.

      ```
      exec QBM_PWatchDogPrepare 1

      go

      exec QBM_PDBQueuePrepare 1

      go
      ```

   c. Delete all triggers in the database.

      ```
      exec QBM_PTriggerDrop '%', @force = 1
      ```

   d. Delete all constraints in the database.

      ```
      exec QBM_PConstraintFKDrop '%','%','%'
      ```

   e. Delete the module you no longer need.

      ```
      exec QBM_PModuleRemove '<3-character module abbreviation>'
      ```

      Example:

```
            declare @ModulesToRemove varchar(100) = 'SAP' + char(7)

                  + 'SHR' + char(7)

                  + 'SBW' + char(7)

                  + 'SAC' + char(7)

            exec QBM_PModuleRemove @ModulesToRemove

            go
```

     f. If you delete the Business Roles Module (RMB), you must also delete the entries in the `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.

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.

Creating a One Identity Manager database for a test or development environment from a database backup

NOTE: Additional steps are required if you work with granular permissions concepts at SQL level. In this case, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

To create a test or development database from a database backup from another system

1. Create a new database on the database server in the reference environment.

2. Create a database backup of the original database.

3. Restore the backup to the reference database.

4. Restore permissions for the database user on the database server.

5. Compile the database with the Database Compiler.

   Use the Database Compiler to customize connection data for the database and compile all scripts and processes in the database.

   a. Open Launchpad and select **Compile the database**. This starts the Database Compiler.

   b. On the Database Compiler start page, click **Next**.

   c. On the **Connect to database** page, enter the connection data for the One Identity Manager database.

   d. The database ID is verified. If, during the verification, it transpires that the database ID is incorrect, you will be prompted to create a new ID. Confirm this prompt with **OK**. The database ID is changed.

   e. On the **Database connection information insufficient** page, check the database connection data and change if necessary.

- Test the connection parameters (ConnectionString).

   Change the entry using the [**...**] button beside the input field. Select your database connection data.

   - Test the full customer name.

   f. This test the database connection. Confirm the prompt with **OK**.

   g. Enter the valid connection data for the One Identity Manager database.

   h. On the **Connect to database** page, enter the connection data for the One Identity Manager database.

   i. The components to be compiled are displayed on the **Compilation settings** page. To start compiling, click **Next**.

   This starts the compilation process. The process may take some time.

   j. The results of the compilation process are shown on **Compilation**. Click **Next** after compilation is complete.

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

6. In the Designer, adjust the database staging level of the database.

   a. In the Designer, select the **Base Data | General | Databases** category.

   b. Select the database and change the value of the **Staging level** property to **Test environment** or **Development system**.

   c. Select **Database | Save to database** and click **Save**.

7. Customize the synchronization project's connection data in the Synchronization Editor.

Related topics

- Configuring a One Identity Manager database for testing, development, or production on page 61

Advanced configuration of the Manager web application

NOTE: The Web Installer uses default values for most configuration settings. You can use these values normally. It is recommended you check the settings with the help of the Manager Web Configuration Editor.

You configure the Manager web application configuration with the Manager Web Configuration Editor. The Manager Web Configuration Editor is part of the web application and can be found in the install directory in the subdirectory `WebConfigEditor`.

To run configuration

1. Start the file `WebConfigEditor.exe` and log in to the One Identity Manager database.

   The Manager Web Configuration Editor automatically opens the `web.config` file of the web application.

2. Modify the configuration settings.

3. Save the changes.

Detailed information about this topic

General

In the **General** pane, you configure the appearance of the Manager web application.

Table 48: Meaning of general configuration settings

Setting	Description
Language	Language. The language influences how dates and numbers displayed amongst other things.
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. 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 the session timeout has elapsed with no user activity. • **HeartBeat**: A session is ended when the period of time defined under the session timeout has elapsed with no user activity. The user's open browser window prompts automatically. The timeout begins when the browser window is closed.
Visualization	Visualization of the application.
Dynamic design select	Not in use.
Enable portal mode	Permits the application in a frame to be linked to another application.

Database connection

In the **Database connection** pane, you create all database parameters for the Manager web application.

Table 49: Meaning of database connection configuration settings

Setting	Description
Database	Database connection. You can select between a SQL Server database connection and an application server.

Setting	Description
Application	Application which specifies the contents of the web application. Usually, you should select **Manager**.
Display name	Name used as application name, as in the title bar of the browser, for example.
Authentication	Methods for authenticating the user when logging in to the application.
Single sign-on	Specifies whether single sign-on is used. Set this option if you user single sign-on. The application does not display a login page to the user but tries to identity the user automatically.

Security

In the **Security** pane, you define several important settings that influence the security of the Manager web application.

Table 50: Meaning of configuration settings for security

Setting	Description
Staging	Default configuration of the staging environment. This setting also affects other configuration groups. **Table 51: Permitted values** <table><tr><th>Value</th><th>Description</th></tr><tr><td>Production</td><td>Recommended setting for all productive installation.</td></tr><tr><td>Test</td><td>Setting if the application was installed for test purposes.</td></tr><tr><td>Development</td><td>Setting if the application was installed in a development environment.</td></tr><tr><td>Custom</td><td>Setting if all settings are made manually.</td></tr></table>
Invalid session response delay	Time in seconds that a client sided request with false session data is blocked. This setting prevents possible "Brute force" access attempts.
Permit login without cookies	The application uses session cookies to secure client-server communication. Set this setting to allow user login without cookies. This would be the case, for example, if cookies were forbidden in a company network. │ NOTE: It is not recommended to enable this setting.
Close	Specifies whether the browser window is closed after logging out. If this

Setting	Description
browser window after logout	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.

Debugging

The **Debugging** area contains useful settings for troubleshooting in the Manager web application. Normally, you cannot configure anything here.

Table 52: Meaning of configuration settings for debugging

Setting	Description
Log mode	The amount of data to be logged.
	NOTE: When the application is in productive operation, **Normal** should be set.
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.
	NOTE: This setting should not be enabled in a live environment.
Enable SQL log	Specifies whether the all database instructions are logged. The log is written in the SQL log directory.
	NOTE: This setting should not be enabled in a live environment.
Show ASP.Net error messages	Specifies whether ASP.Net's own error messages are shown.
	NOTE: This setting should not be enabled in a live environment.
Enable test mode	Specifies whether automatic tests are supported.
	NOTE: This setting should not be enabled in a live environment.

Related topics

- Directories on page 177

Performance

In the **Performance** pane, you define several important settings that influence the performance of the Manager web application.

Table 53: Meaning of configuration settings for performance

Setting	Description
Load balancing	The mode of integrated load balancing. In most cases, **DistributeEqually** should be selected.
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.
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.
Compress HTTP transfer	Specifies whether usage of compression for HTTP communication is set. NOTE: Compression of HTTP communication must also be configured for Internet Information Services. For more information see the Web server documentation.
Host segmentation	Specifies host segmentation. This setting allows distribution of client sided requests to several server addresses representing aliases for the web front-end. This bypasses some of the browser limitation and can therefore shorten loading time if the network connection is bad.

Related topics

- Load balancing on page 179

File download

To enable the download of larger files, the Manager web application requires a directory in which the download can be made available to the user. This effects reports, for example, which are generated by the application and saved as PDF by the user.

Table 54: Meaning of the configuration settings for the file download

Setting	Description
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.
Download directory	Directory for the application to use to make download available. The application requires full access rights to this directory.
Cleanup interval	Time in minutes search for and remove redundant files.

Setting	Description
Supply time	Time in minutes before download is available to the user. Once a download has been initiated, the application cannot verify when and if the download was executed by the user so that the download must be aborted after a set time interval.

ASP.Net basic settings

In the area **ASP.NET settings** you can see some settings of ASP.Net, which can be edited by the Manager Web Configuration Editor.

Table 55: Meaning of configuration settings for ASP.Net

Setting	Description
Max request length	Maximum length of the user request in kilobytes (KB). This limits, amongst others, the maximum size of file that can be loaded.
Execution timeout	Maximum time in seconds for processing a user request. The user request is aborted if timeout is exceeded. NOTE: This time should not be too short because the user session can be lost if the timeout is exceeded.

Directories

In the **Directories** area you configure all the directories required by the Manager web application.

Table 56: Meaning of configuration settings for directories

Setting	Description
Application directory	Full path to the application's installation directory. This is the directory where you will find the file `web.config`. NOTE: Ensure correct case.
Log directory	Directory to which the application log is written. This directory can be relative to the application directory.
Database cache	Full path to the directory to save frequently used database contents.

Setting	Description
Script assembly cache	Full path to the directory for caching assembler files.
SQL log directory	Full path to the directory where database accesses are logged. The SQL log is only used for finding errors and must be enabled through the **Enable SQL log** option in the **Debugging** pane.

Related topics

- Debugging on page 175

Application pool

In the **Application pool** view, you define all applications that work together to make the application available to the user in multiple languages.

- Click **Add application** to define another application.
- Click **Remove application** to select an application to remove.
- You can change the order by using the arrows on the right side.

NOTE: You must at least define the currently configured application. The order has immediately effect on login performance because the status of configured applications is queried in the defined order.

Table 57: Meaning of the configuration settings for the application pool

Setting	Description
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 access rights as required when the URL is called by browser on the server.

Related topics

- Load balancing on page 179

Plug-ins

Plug-ins extend the functionality of the Manager web application. You can enable a plug-in by setting the option in front of the plug-in name. You may find plug-in specific settings under a plug-in.

Plug-in automatic update

This plug-in runs automatic update.

Table 58: Meaning of configuration settings

Setting	Meaning
Auto update	Automatic update is enabled.
Severity code	Severity of a change in order to start automatic update.

Related topics

- Updating the Manager web application on page 148
- Automatic updating of One Identity Manager on page 86

Load balancing

The Manager web application provides simple load balancing in order to distribute user sessions and the resulting load across multiple processes or even servers. To do this, the application is installed multiple times on the same or on other servers.

All collaborating applications that can be logged into, are declared in the applications' Application pool. The selection algorithm for load distribution distributes user logins across the defined applications.

NOTE: Even if only one application is installed, it must be defined in your application pool, otherwise you cannot log in.

Table 59: 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 99% of cases.
DistributeSuccessively	This algorithm distributes user logins by order of application

Algorithm	Description
	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:

- Multi-language

  Language is fixed for per application so that an application can only provide user sessions in one language. If users can log in with multiple languages, at least one application must be installed for each language.

- Bypassing resource limitations

  If multiple web applications are installed and these are assigned to different Internet Information Services application pools, these are started in separate processes.

- Increasing performance

  Performance can be noticeably improved by installing on several servers.

- Redundancy

  Multiple installation does not necessary complete outage if just one of the installed application fails.

Related topics

- Application pool on page 178

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 detailed information about the 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

- Application pool on page 178

Machine roles and installation packages

Table 60: Machine role and installation package options

Machine role		Description of the installation package
Workstation		Contains all basic components for installing tools on an administrative workstation.
	Administration	Contains One Identity Manager administration tools required by default users to fulfill 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.
	Configuration	Contains all One Identity Manager tools for the default user and additional programs for configuring the system. These include, for example, the Configuration Wizard, Database Compiler, Database Transporter, Crypto Configuration, Designer, Web Designer, and configuration tools for the One Identity Manager Service.
	Development & Testing	Contains the One Identity Manager tools for developing and testing custom scripts and forms, for example, the System Debugger.
	Monitoring	Contains One Identity Manager programs for monitoring the system status, for example, the Job Queue Info program.
Documentation		Contains One Identity Manager documentation in different languages.
Server		Contains all the basic components for setting up a server.

Machine role	Description of the installation package
Job server	Contains the One Identity Manager Service and basic processing components. Additional machine roles contain connectors for synchronizing individual target systems.

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