One Identity Manager On Demand (Starling Edition)

Quick Start Guide

Legend

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

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

One Identity Manager On Demand (Starling Edition) Quick Start Guide
Updated - 23 August 2024, 06:43

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

Contents

1

About this guide

The *One Identity Manager On Demand (Starling Edition) Quick Start Guide* provides an overview of the architecture of our One Identity Manager On Demand offering and its core capabilities. It also provides information about the customization limitations and prerequisites you will need before installing the One Identity Manager On Demand on-premises components, and how to set up, install, and update One Identity Manager On Demand on-premises components.

This guide is intended for, system administrators, consultants and any other IAM professionals using the product.

Available documentation

You can access One Identity Manager On Demand documentation in the Manager and in the Designer by selecting the **Help** > **Search** menu item. The online version of One Identity Manager On Demand documentation is available on the Support Portal under Technical Documentation. You will find videos with additional information at www.YouTube.com/OneIdentity.

One Identity Manager On Demand overview

One Identity Manager On Demand is a cloud service offering from One Identity that provides a fully-functional implementation of the One Identity Manager application, deployed to customers over the cloud (https://cloud.oneidentity.com) and supported by the One Identity operations team.

One Identity Manager On Demand 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 tackle all Identity Governance and Administration core functions:

- **Identity life cycle**: Maintaining digital identities, their relationships with the organization and their attributes during the entire process from creation to eventual archiving, using one or more identity life cycle patterns.
- **Entitlement management**: Maintaining the link between identities and access rights to be able to tell who has access to what and who is responsible for maintaining an account or access right. This includes maintaining and curating the entitlements catalog to describe the types of accounts, roles, group memberships and other entitlements.
- **Access requests**: Enabling users, or others acting on behalf of a user, to request access rights through a business-friendly user interface.
- **Workflow**: Orchestrating tasks to enable functions such as access approvals, notifications, escalations, manual fulfillment requests and integration with other business processes. For example, this allows managers or resource owners to approve or deny requests.
- **Policy and role management**: Maintaining rules that govern automatic assignment (and removal) of access rights; providing visibility of access rights for selection in access requests, approval processes, dependencies and incompatibilities between access rights; and so on. Roles are a common vehicle for policy management.
- **Access certification**: Requiring people like managers and resource owners to review and certify the access rights that users have on a periodic basis to ensure

access continues to comply with policies.

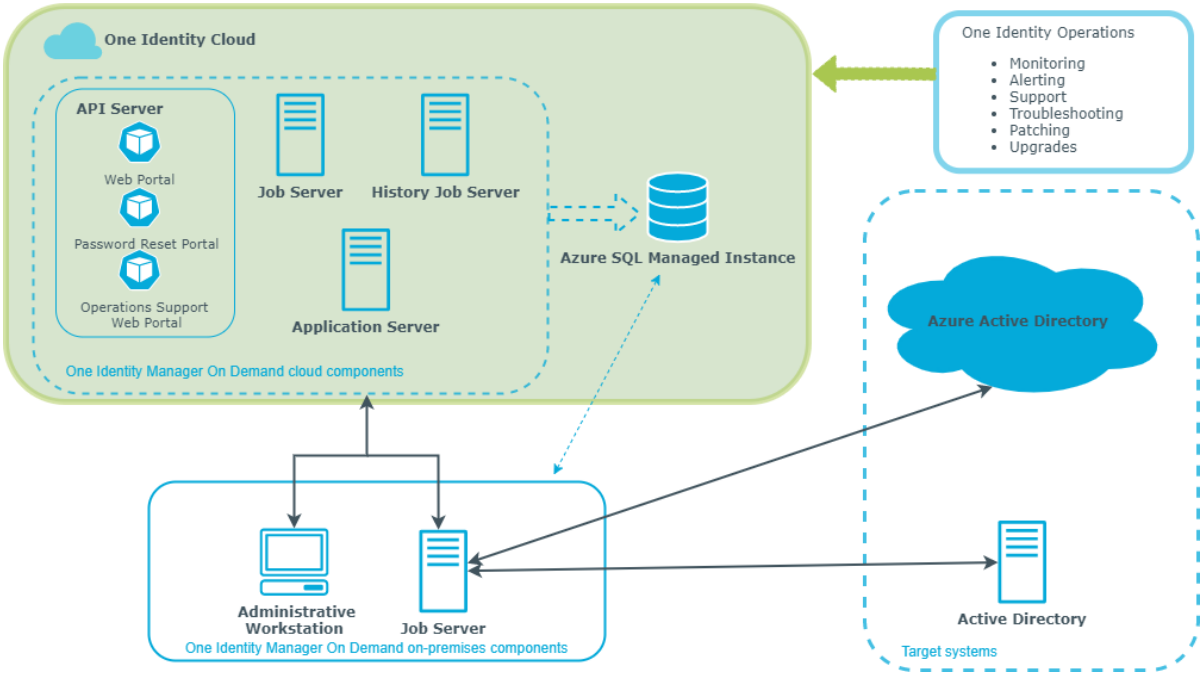
- **Fulfillment:** Propagating changes initiated by One Identity Manager On Demand to target systems. Automatic fulfillment (often called "provisioning") connects with user account target systems, while manual fulfillment utilizes a workflow or external process to complete actions.
- **Auditing**: Evaluating business rules and controls against the current state of identities and access rights, providing a means for alerting control owners of exceptions (such as changes made directly on target systems) and allowing for orderly remediation.
- **Identity analytics and reporting**: Providing means to: (a) evaluate risk based on identity information insights; (b) apply techniques to cleanup excessive, outlier or wrongful entitlements; and (c) enhance the continuous process of identity governance, including risk reporting.

Every one of these core functions is based on an automation-optimized architecture that addresses major Identity Governance and Administration challenges at a fraction of the complexity and time of "traditional" solutions.

Architecture overview

The architecture overview shows the different components of One Identity Manager On Demand. One Identity Manager On Demand cloud components are managed and monitored by the One Identity operations team. One Identity Manager On Demand on-premises components must be installed and configured locally to connect and synchronize on-premises target systems with One Identity Manager On Demand cloud components.

Figure 1: Overview of One Identity Manager On Demand components



4

Using One Identity Manager On Demand as a Starling service

One Identity Manager On Demand is integrated as a Starling service in One Identity Starling (https://cloud.oneidentity.com). One Identity Manager On Demand is available as a time-limited trial version and as a paid subscription.

- To use One Identity Manager On Demand for a limited time period, contact One Identity. One Identity can enable proof of concept for your product trial. You will be notified once proof of concept has been added to your organization's account. The product performs exactly how it would with a test instance with no restrictions. A proof of concept trial is limited to 30 days but if you need more time, you can ask for an extension before the trial subscription ends.
- To use a paid subscription, contact One Identity to set up the subscription. You will receive a subscription confirmation email from One Identity.

  A paid subscription offers you full access to the product for the length of your contract and with a fixed number of user licenses. With a paid subscription, you get a test instance and a production instance.

To use One Identity Manager On Demand as a Starling service, you require a Starling organization. You can add the Starling service to an existing organization or set up a new one. For more information about organizations, see the *One Identity Starling User Guide* under Organization creation and management.

To start a subscription

1. Log in to the One Identity Starling portal.
2. Configure your subscription.
   - To configure a product trial, on the home page, select the **View On Demand Services** section.
     a. Select **One Identity Manager On Demand (Starling Edition)** and click **Trial**.

        This creates a trial subscription. **One Identity Manager On Demand (Starling Edition)** is shown as a new tile in the **My Services** section and can be used until trial period ends.

b. On the home page, in the **My Services** section, click the **One Identity Manager On Demand (Starling Edition)** tile.

- To configure a paid product, click on the **One Identity Manager On Demand (Starling Edition)** tile in the **My Services** section on the home page.

3. Select the type of deployment.
   - To start a proof of concept trial, click **Proof of concept trial**.
   - To start a paid subscription, click **Production**.
4. Select the region where you want your One Identity Manager On Demand instance to be deployed.
5. Enter a domain name for your One Identity Manager On Demand instance.

   The domain name may not be longer than 40 characters and must be unique within Starling.
6. Click **Set Up Deployment**.

   This starts up a One Identity Manager On Demand instance. It can take a while to complete. Once your instance is ready to use, you will receive an email containing a link to it.

Information provided for accessing One Identity Manager On Demand

After successful deployment, information about your subscription is displayed in the One Identity Manager On Demand portal along with the connection details of your One Identity Starling deployment. You need this information for accessing One Identity Manager On Demand.

To display the information

1. Log in to the One Identity Starling portal.
2. On the home page, in the **My Services** section, click the **One Identity Manager On Demand (Starling Edition)** tile.

Administrative system user

The **cccAdmin** system user is an administrative system user. You can use this system user to log on to the tools for the first time and to configure One Identity Manager On Demand. Provided are:

- **User name**: cccAdmin
- **Password**: Password for the **cccAdmin** system user.

Synchronization user

The **Synchronization** system user has the necessary permissions to set up and run target system synchronizations using an application server. Provided are:

- **User name**: Synchronization
- **Password**: Password for the **Synchronization** system user.

Database connection data

It is generally recommended that on-premises components use the application server to connect to the database. However, some components require a direct database connection. For more information, see Which components and front-ends work with an application server? in the Online documentation on the Support Portal.

The following information is provided for the direct database connection:

- **Database address**: Public endpoint of the Azure SQL Managed Instance.
- **Database name**: Name of the database.
- **User name**: SQL Server Login name of the **<database name>_cccConfig** user.
- **Password**: Password for the user's SQL Server login.

  NOTE: The database login password expires after 42 days after which, you must change the password.

IMPORTANT: Access to the database is limited solely to the IP addresses and IP ranges that have been granted access.

To share IP addresses and IP ranges

- On the **Database Access** tile, click **Manage Database Access** and enter one or more public IP addresses or IP ranges (separated by commas) or specify the CIDR notation.

Encryption key for database encryption

To synchronize a target system you must declare the database key in the One Identity Manager On Demand Service. The file with the private key must exist in the server's installation directory on all servers with an active One Identity Manager On Demand Service.

For more information, see Tips for working with an encrypted One Identity Manager database in the Online documentation on the Support Portal.

Endpoint URLs

- Web Portal / API Server

  This endpoint is used deploy the Web Portal, the Password Reset Portal and the Operations Support Web Portal. In addition, you gain access to the API Server's administration portal and the API Server's API documentation.

- App Server

  This endpoint is used to deploy the application server. You need the URL to connect to the application server in the on-premises components. Furthermore, administrative system users can see the application server's status as well as the application server's REST API documentation through this endpoint.

- Job server

  This endpoint is used to deploy the cloud Job server's status information and log file.

One Identity Manager On Demand cloud components

The following One Identity Manager On Demand components are deployed as part of the cloud infrastructure. These components are managed by One Identity and monitored by the operations team.

Table 1: Overview of One Identity Manager On Demand cloud components

Component	Description
Azure SQL Managed Instance	The Azure SQL Managed Instance is an intelligent, scalable, cloud database service.
API Server	The API Server deploys the Web Portal, the Password Reset Portal, and the Operations Support Web Portal. NOTE: Any customizations of the base Angular code are supported solely by the customer.
Web Portal	The Web Portal is a web-based application for all One Identity Manager On Demand users. The Web Portal provides stringent workflows for the following actions: • Changing your own main data and password. • Editing or entering identity main data of direct reports. • Searching, requesting, canceling, or renewing products in the IT Shop. • Delegating own roles. • Editing assigned approvals, attestation cases, and rule violations. In the information system, you may see several evaluations, for example, about your own requests and attestation cases, employee numbers, approvals, rule violations, or the Unified Namespace.

Component	Description
	The Web Portal is made available over the API Server. Through a web browser, users can access the website that has been dynamically set up and customized for them.
Password Reset Portal	The Password Reset Portal allows users to securely reset passwords of the user accounts they manage. The Password Reset Portal is made available over the API Server.
Operations Support Web Portal	The Operations Support Web Portal helps you to manage and use your web applications. You can use the Operations Support Web Portal to monitor the handling of processes and DBQueue tasks. You can also create passcodes for your colleagues. The Operations Support Web Portal is made available over the API Server.
Application server	The application server deploys a connection pool for accessing the database from outside the One Identity Cloud.
Job server	This One Identity Manager On Demand Service handles defined processes and should not be used to perform data synchronization between the database and any connected target systems.

Related topics

- Supported browsers on page 13
- Requirements for connecting One Identity Starling on page 14
- Database backup policies on page 14
- Architecture overview on page 7
- Information provided for accessing One Identity Manager On Demand on page 10
- One Identity Manager On Demand on-premises components on page 15

Supported browsers

You can use any browser to access One Identity Manager On Demand cloud components if it is supported by One Identity Starling. For more information, see under System requirements in the *One Identity Starling Release Notes*.

Enable JavaScript in your browser for the One Identity Manager On Demand Web Portal to work. For optimal displaying of the graphical user interface, use a device with a minimum

screen resolution of 1280 x 1024 pixels and at least 16-bit color depth. For mobile viewing, for example when using a tablet, use a device with a display size of at least 9.7 inches.

Requirements for connecting One Identity Starling

To integrate One Identity Starling, you require different DNS addresses. For more information, see under System requirements in the *One Identity Starling Release Notes*.

Database backup policies

The following database backup policies are implemented.

- Geo-redundant backup storage
- Storage of Point-In-Time Restore (PITR) backups for 35 days
- Storage of weekly Long-Term Retention (LTR) backups for 3 months

One Identity Manager On Demand on-premises components

One Identity Manager On Demand on-premises components must be installed and configured locally to connect and synchronize on-premises target systems with One Identity Manager On Demand cloud components. To get started, the One Identity Manager On Demand Client installation package is available on the Support portal under Downloads.

Different tools are provided for different tasks. For example, the tool used to configure One Identity Manager On Demand differs from the tool used to manage identities. The content displayed and its editability are dependent on the permissions of the logged in user.

The following table contains the most important tools for getting started. For more information about the tools, see One Identity Manager tools in the Online documentation on the Support Portal.

Table 2: One Identity Manager On Demand on-premises components

Components	Description
Synchronization Editor	You use the Synchronization Editor to connect different target systems to One Identity Manager On Demand. Use this tool to configure data synchronization for any target system and specify which target system data is mapped to the One Identity Manager On Demand database. You also define the object properties mapping and the synchronization sequence as a workflow.
Manager	The Manager is the main administration tool for setting up all identity data. It displays and maintains all the data required for the administration of identities, their user accounts, permissions, and company-specific roles in a One Identity Manager On Demand network. Company resources required to carry out tasks can be configured and assigned to identities.
Job server	The One Identity Manager On Demand Service performs data synchronization between the database and any connected target systems and runs actions at the database and file level. The service must be installed on the One Identity Manager On

Components	Description
	Demand network server to run the processes. A server running the One Identity Manager On Demand Service is called the Job server. The Job server must be declared in the One Identity Manager On Demand database. NOTE: For process collection, the One Identity Manager On Demand Service should connect through the application server.
Server Installer	Use the Server Installer to install and configure the One Identity Manager On Demand Service. Use the Server Installer to install the One Identity Manager On Demand Service locally or remotely.
Designer	The Designer is the main tool for configuring One Identity Manager On Demand. The program offers an overview of the entire One Identity Manager On Demand data model. It enables the configuration of global system settings. You use the Designer to specify permissions for the different administrative tasks of individual users and user groups.

It is generally recommended that on-premises components use the application server to connect to the database. However, some components require a direct database connection. For more information, see Which components and front-ends work with an application server? in the Online documentation on the Support Portal.

Related topics

- Minimum system requirements for administrative workstations on page 16
- Minimum system requirements for Job servers on page 17
- Installing One Identity Manager On Demand on-premises components on page 19
- Architecture overview on page 7
- Information provided for accessing One Identity Manager On Demand on page 10
- One Identity Manager On Demand cloud components on page 12

Minimum system requirements for administrative workstations

The following system prerequisites must be fulfilled before installing the One Identity Manager On Demand components on an administrative workstation.

Table 3: 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 11 (x64) • Windows 10 (32-bit or 64-bit) at least version 1511
Additional software	• Microsoft .NET Framework version 4.8 or later • Microsoft Edge WebView2
Supported browsers	• Firefox (release channel) • Chrome (release channel) • Microsoft Edge (release channel)

Minimum system requirements for Job servers

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

Table 4: Minimum system requirements - Job 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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012

Additional software	• Microsoft .NET Framework version 4.8 or later NOTE: When connecting the target system, refer to the target system manufacturer's recommendations.

Working with One Identity Manager On Demand

The following sections provide you with information on the first steps for putting One Identity Manager On Demand into operation. For more information, see One Identity Manager On Demand (Starling Edition) documentation and One Identity Manager documentation on the Support Portal.

Detailed information about this topic

- Installing One Identity Manager On Demand on-premises components on page 19
- Logging in to One Identity Manager On Demand components on page 22
- Setting up a One Identity Manager On Demand on-premises Job server on page 26
- How to transfer script modifications from the test instance to the production instance on page 30

Installing One Identity Manager On Demand on-premises components

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

- Use the installation wizard to install the One Identity Manager On Demand components on workstations for the first time.
- Use the installation wizard or the Server Installer to install the One Identity Manager On Demand Service on the servers for the first time.

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

To install the One Identity Manager On Demand components

1. Launch `autorun.exe` from the root directory of the One Identity Manager On Demand installation medium.
2. Switch to the **Installation** tab and select an edition.
3. Click **Install**.

   This starts the installation wizard.
4. Select the language for the installation wizard on the start page and click **Next**.
5. Confirm the conditions of the license.
6. On the **Installation settings** page, enter the following information.
   - **Installation source**: Select the directory containing the installation files.
   - **Installation directory**: Select the directory in which you want to install the files for One Identity Manager On Demand.

     NOTE: To make further configuration settings, click on the arrow button next to the input field. Here, you can specify whether you are installing on a 64-bit or a 32-bit operating system.

     For a standard installation, no further configuration settings are necessary.
7. On the **Assign machine roles** page, define the machine roles.

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

   You can select the following machine roles.
   - **Workstation**: Contains all basic components for installing tools on an administrative workstation.
   - **Workstation |Administration**: Contains administration tools required by default users for fulfilling their tasks with One Identity Manager On Demand. In addition to the tools that ensure basic functionality for working with One Identity Manager On Demand, the administration machine role includes the Manager as a main administration tool.
   - **Workstation | Configuration**: Contains all tools for the default user and additional programs required to configure the system. These include, for example, the Database Compiler, Database Transporter, Designer, and configuration tools for the One Identity Manager On Demand Service.
   - **Workstation | Development and Testing**: Contains the tools to develop and test custom scripts, such as the System Debugger.
   - **Workstation | Monitoring**: Contains programs for monitoring the system status, such as the Job Queue Info.
   - **Server**: Contains all the basic components for setting up a server.
   - **Server | Job Server**: Contains the One Identity Manager On Demand Service and basic processing components. Additional machine roles contain connectors for synchronizing individual target systems.

- **Server | Job Server | Configuration tool**: Contain configuration tool for the One Identity Manager On Demand Service.

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

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

9. On the **Change service properties** page, you can change the name, display name and the description for installing the One Identity Manager On Demand 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 create the configuration of the One Identity Manager On Demand Service, start the Job Service Configuration program.

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

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

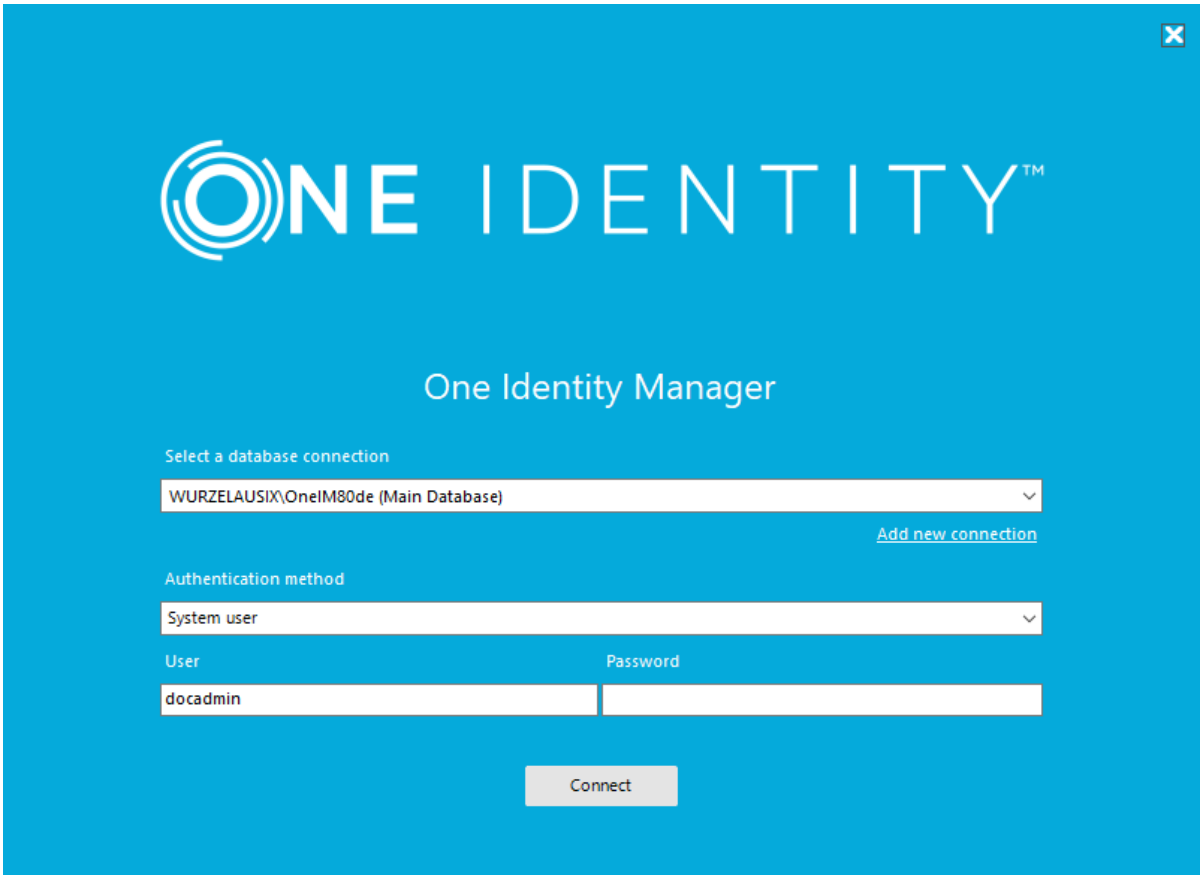
One Identity Manager On Demand is installed for all user accounts on the workstation or server. In the default installation, One Identity Manager On Demand is installed under:

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

Logging in to One Identity Manager On Demand components

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

Figure 2: Default connection dialog



Login takes place in two steps:

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

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

2. Selecting the authentication method and finding the system user for logging in

For more information, see Logging in to One Identity Manager tools in the Online documentation on the Support Portal.

It is generally recommended that One Identity Manager On Demand on-premises components use the application server to connect to the database. However, some components require a direct database connection. For more information, see Which

components and front-ends work with an application server? in the Online documentation on the Support Portal.

Related topics

- One Identity Manager On Demand system users on page 23
- Logging in via application server on page 24
- Logging in via direct connection to the database on page 25

One Identity Manager On Demand system users

One Identity Manager On Demand provides various system users whose permissions are matched to the various tasks.

- System user **cccAdmin**

  The **cccAdmin** system user is an administrative system user. For example, you use this system user to log on to One Identity Manager On Demand components, such as the Launchpad or Jobserver, via the application server.

- System user **Synchronization**

  The **Synchronization** system user has the necessary permissions to set up and run target system synchronizations using an application server. Use this system user to log in to the Synchronization Editor via the application server.

- System user **viadmin**

  The **viadmin** system user is an administrative system user. This system user is used by the One Identity operations team to access One Identity Manager On Demand components.

  > IMPORTANT: The **viadmin** system user is required by the One Identity operations team for upgrading and installing hotfixes. Ensure that this system user can be used to log in to One Identity Manager On Demand components. This system user's settings and password must not be changed.

Related topics

- Information provided for accessing One Identity Manager On Demand on page 10
- Logging in via application server on page 24

Logging in via application server

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

Prerequisites

For the One Identity Manager On Demand components connection you need the application server's URL as well as the user name and password of the system user. This information is provided in the One Identity Starling Portal. For more information, see Information provided for accessing One Identity Manager On Demand on page 10.

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

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

   This opens the connection dialog.
2. In the connection dialog, under **Select a database connection**, click **Add new connection** and select the **Application server** system type.
3. Click **Next**.
4. Enter the address (URL) for the application server.
5. (Optional) You have the option to select a certificate under **Pin server certificate** that is then required for logging in. In this case, select a root certificate (Root CA) because this generally subject to less change.
6. Select **Test connection** in the **Options** menu.

   This attempts to connect the database with the given connection data. You are prompted to confirm a message about the test.

   NOTE: Using **Options > Advanced options** item, you can make additional changes to the connection configuration.
7. Click **Finished**.
8. In the connection dialog, under **Authentication method**, select the **System user** authentication module.
9. Enter the login data for the system user ID. Enter the user name and the password.
10. Click **Connect**.

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

Logging in via direct connection to the database

Perform the following steps to use a direct connection to log in to the database.

Prerequisites

IMPORTANT: Access to the database is limited solely to the IP addresses and IP ranges that have been granted access.

The database connection credentials are provided in the One Identity Starling portal. For more information, see Information provided for accessing One Identity Manager On Demand on page 10.

To create a new connection to the database

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

   This opens the connection dialog.
2. In the connection dialog, under **Select a database connection**, click **Add new connection** and select the **SQL Server** system type.
3. Click **Next**.
4. Enter the connection data for the database server.
   - **Server**: Database server. Enter the **Database address**.
   - (Optional) **Windows Authentication**: Specifies whether the integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
   - **User**: The user's SQL Server login name.
   - **Password**: Password for the user's SQL Server login.
   - **Database**: Select the database.
5. Select **Test connection** in the **Options** menu.

   This attempts to connect the database with the given connection data. You are prompted to confirm a message about the test.

   NOTE: Using **Options > Advanced options** item, you can make additional changes to the connection configuration.
6. Click **Finished**.
7. In the connection dialog, under **Authentication method**, select the **System user** authentication module.
8. Enter the login data for the system user ID. Enter the user name and the password.
9. Click **Connect**.

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

Setting up a One Identity Manager On Demand on-premises Job server

For more information about installing and configuring the One Identity Manager On Demand Service, see Installing and configuring the One Identity Manager Service and The One Identity Manager Service functionality in the online documentation on the Support Portal.

To set up a One Identity Manager On Demand on-premises Job server, perform the following steps.

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

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

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

   Use the Server Installer to install the One Identity Manager On Demand Service locally or remotely.
2. Declare the database key in the One Identity Manager On Demand Service.
3. The One Identity Manager On Demand Service should connect via an application for process collection. Configure addition connection data in the Designer.

Related topics

- Minimum system requirements for Job servers on page 17
- Installing and configuring the One Identity Manager On Demand Service on a Job server on page 26
- Declaring database keys on a Job server on page 29
- Configuring connection data for the application server on page 29

Installing and configuring the One Identity Manager On Demand Service on a Job server

Perform these steps to install the One Identity Manager On Demand Service on a Job server and establish a connection through an application server.

Prerequisites

To remotely install the One Identity Manager On Demand Service, provide an administrative workstation on which the One Identity Manager On Demand components are installed. Ensure that the One Identity Manager On Demand components are installed on the server before installing locally.

For the One Identity Manager On Demand Service connection you need the application server's URL as well as the user name and password of the system user. This information is provided in the One Identity Starling Portal. For more information, see Information provided for accessing One Identity Manager On Demand on page 10.

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

1. Start the Server Installer program.

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

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

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

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

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

   b. Enter the following data for the Job server.

      - **Server**: Name of the Job server.
      - **Queue**: Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager On Demand 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.

4. On the **Machine roles** page specify which roles the Job server is to have in One Identity Manager On Demand. 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 On Demand environment. One Identity Manager On Demand 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 On Demand Service configuration.

   For a connection to the application server:

   a. In the module list, select the **Process collection** entry and click the **Insert** button.
   b. Select **AppServerJobProvider** and click **OK**.
   c. In the module list, select **Process collection > AppServerJobProvider**.
   d. Click the **Connection parameter** entry, then click the **Edit** button.
   e. Enter the address (URL) for the application server and click **OK**.
   f. Click the **Authentication data** entry and click the **Edit** button.
   g. In the **Authentication method** dialog, select the **System user** authentication method and enter the user name and password of the system user.
   h. Click **OK**.
   i. In the module list, select the **Process collection** entry.
   j. Select the **sqlprovider** and click the **Remove** button.
   k. (Optional) Check the rest of the service configuration. The initial service configuration is predefined. If further changes need to be made to the configuration, you can do this later with the Designer.

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

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

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

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

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

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

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

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

Related topics

- Installing One Identity Manager On Demand on-premises components on page 19
- Logging in via application server on page 24
- Logging in via direct connection to the database on page 25
- Declaring database keys on a Job server on page 29
- Configuring connection data for the application server on page 29

Declaring database keys on a Job server

Perform the following steps to deploy the database key for the One Identity Manager On Demand Service.

Prerequisite

The key for the database encryption is available in the One Identity Starling portal. For more information, see Information provided for accessing One Identity Manager On Demand on page 10.

To declare the database key on a Job server

1. Create a `private.key` file.
2. Add the key for the database encryption in the `private.key` file and save the file.
3. Copy the file with the private key in the service's install directory.
4. Open the service management and restart the One Identity Manager On Demand Service.

Configuring connection data for the application server

Perform these steps to configure the Job server to connect via the application server.

Prerequisites

For the One Identity Manager On Demand Service connection you need the application server's URL as well as the user name and password of the system user. This information is provided in the One Identity Starling Portal. For more information, see Information provided for accessing One Identity Manager On Demand on page 10.

To declare the connection data on the Job server

1. Start the Designer.
2. In the Designer, select the **Base Data > Installation > Job server** category.
3. In the Job Server Editor, select the Job server to edit in the Job servers overview.
4. On the **Properties** tab, enable the **No direct database connection** option.
5. On the **Properties** tab, click the icon next to the **Connection data** menu and enter the following connection data for the application server.
    - **Display name**: Enter a display name for the connection.
    - **Provider**: Select **Application server**.
    - **Connection parameter**: Enter the address (URL) for the application server.
    - **Authentication data**: Enter the authentication data.
        a. Click the **...** button.
        b. In the **Authentication method** dialog, select the **System user** authentication method and enter the user name and password of the system user.
        c. Click **OK**.
6. To save the connection data, click **OK**.
7. Select the **Database > Commit to database** and click **Save**.

How to transfer script modifications from the test instance to the production instance

With a paid subscription, you get a test instance and a production instance. Test your script in the test instance first before adding the changes to the production instance.

To transfer changes the between test and product instances, use the Database Transporter. With this you can create transport packages from the test instance and then use the Database Transporter again to import the transport packages into the production instance.

For detailed information about working with the Database Transporter, see Transporting custom changes in the online documentation on the Support Portal.

9

One Identity Manager On Demand configuration, customization and product limitations

A configuration is where you use the provided original tools in the system to change its behavior or features without adding additional code or customization.

A customization is a feature or extension or modification of available feature(s) that requires custom coding and or some form of implementation.

To ensure our One Identity operations team can manage, monitor, and perform upgrades to the One Identity Manager On Demand cloud components, all customizations to the offering are strictly prohibited.

Ignoring these limitations may cause the One Identity Manager On Demand cloud components to become in an unupgradable state. If this happens, additional professional services may be required at the customers expenses to revert the One Identity Manager On Demand cloud components to the original state or to install upgrades to the One Identity Manager On Demand cloud components.

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