One Identity Manager On Demand

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 Quick Start Guide
Updated - 20 October 2022, 13:22

Contents

1

About this guide

The *One Identity Manager On Demand 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 on-premises component, and how to set up, install, and update One Identity Manager On Demand on-premises components.One Identity Manager On Demand

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 in 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 approvals 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 permissions to be able to tell who has access to what and who is responsible for maintaining an account or access permissions. 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 permissions 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 permissions; providing visibility of access permissions for selection in access requests, approval processes, dependencies, and incompatibilities between access permissions; 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 permissions that users have on a periodic basis to

ensure access continues to comply with policies.

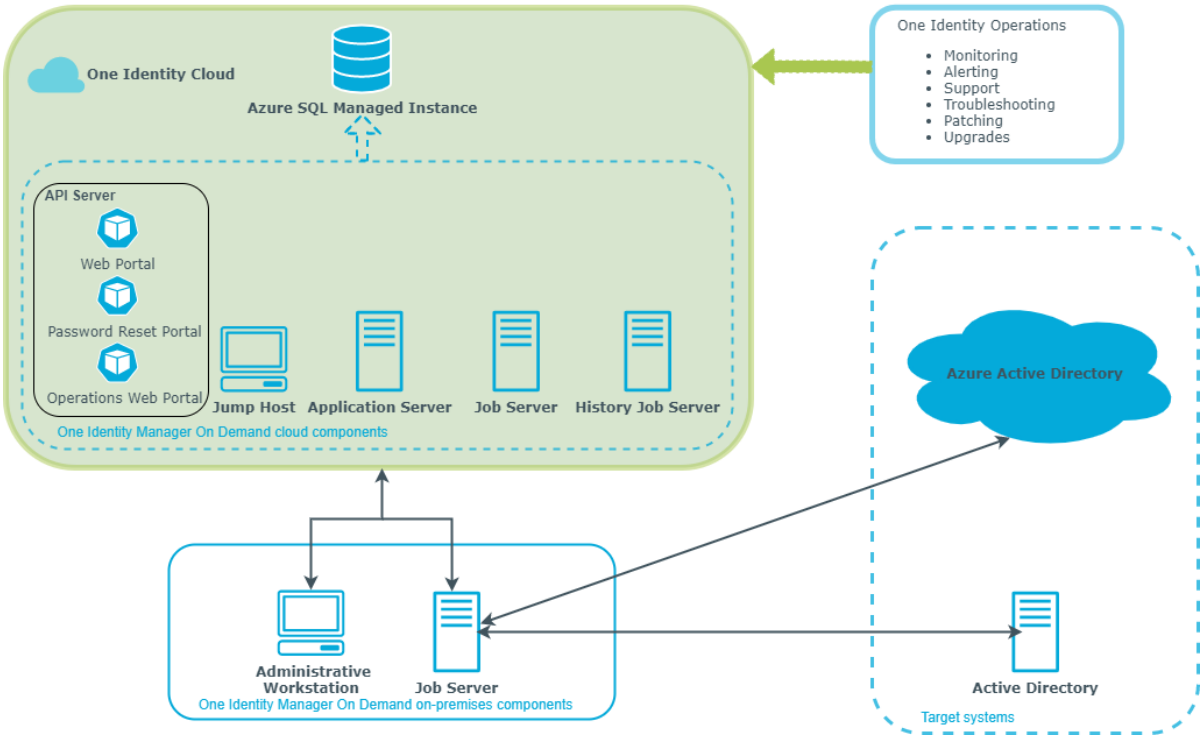
- **Fulfillment:** Propagating changes initiated by One Identity Manager On Demand to target systems. Automatic fulfillment (often called "provisioning") connects with user account target systems, while manual fulfillment utilizes a workflow or external process to complete actions.
- **Auditing**: Evaluating business rules and controls against the identities' current state and access permissions, 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



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.

For the One Identity operations team to deploy One Identity Manager On Demand, you must first provide One Identity with your configuration data. To do this, use the One Identity Starling portal.

Prerequisites

- 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*.
- To use One Identity Manager On Demand for limited period of time, contact One Identity. They can activate a product trial for your organization. One Identity notifies you once the product trial has been added to your organization's account.
- To configure a subscribed product, you will receive confirmation of your subscription by email from One Identity.

To submit the configuration information to the One Identity operations team

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** and click **Trial**.

        This creates a trial subscription. **One Identity Manager On Demand** 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** tile.

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

3. In the **Contact Information** step, you enter details of a technical contact that the One Identity operations team can get in touch with.
   - If you are the technical contact, select **I am the technical contact**.
   - If you want to specify another contact, select **Someone else is the technical contact** and invite the contact using the **Invite Collaborator**.

     TIP: You can also invite collaborators on the **Collaborators** tab.
4. Click **Next: Technical Information**.
5. In the **Technical Information** step, enter the information required for your One Identity Manager On Demand configuration.
6. To submit the configuration to the One Identity operations team, click **Submit Details** and confirm the prompt.
7. After configuration is complete, the **Setting up** step provides information about deployment status. You will be notified by mail when the status changes.

   NOTE: If the custom configuration is rejected by the One Identity operations team, you can update the configuration data with **Update Details** and resubmit.

After successful deployment, the **Application** tab displays the connection details of your One Identity Manager On Demand deployment. You need this information for accessing the One Identity Manager On Demand cloud components.

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.
Web Portal	The Web Portal is a web-based application for all One Identity Manager On Demand users. The Web Portal provides stringent workflows in the following areas: • Changing employee main data and own password. • Editing or entering employee main data of 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 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. The Web Designer Web Portal is deployed for compatibility reasons. The

Component	Description
	Web Designer Web Portal requires a web server.
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.
History Job Server	The One Identity Manager On Demand History Service ensures data transfer from the One Identity Manager On Demand database to the One Identity Manager History Database.
Jump host	The jump host is used to access the One Identity Manager On Demand administration and configuration tools.

Related topics

- Supported browsers on page 11
- Architecture overview on page 7
- One Identity Manager On Demand on-premises components on page 12

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 the *One Identity Starling User Guide*.

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.

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 in 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' data. 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 information about employees and their identities. It displays and maintains all the data required for the administration of employees, their user accounts, permissions, and company-specific roles in a One Identity Manager On Demand network. Company resources employees require can be entered and assigned to them.
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.

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 13
- Minimum system requirements for Job servers on page 14
- Installing One Identity Manager On Demand on-premises components on page 14
- Architecture overview on page 7
- One Identity Manager On Demand cloud components on page 10

Minimum system requirements for administrative workstations

To install on an administrative workstation, the following system requirements must be met.

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 • Windows 8.1 (32-bit or 64-bit) with the current service pack
Additional software	• Microsoft .NET Framework Version 4.7.2 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 4.7.2 or later NOTE: When connecting the target system, refer to the target system manufacturer's recommendations.

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 wizards to install the One Identity Manager On Demand Service on servers for the first time or remote with the Server Installer.

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. Select the language for the installation wizard on the start page and click **Next**.
3. Confirm the conditions of the license.
4. 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.
5. On the **Assign machine roles** page, define the machine roles.

   NOTE: The machine roles appropriate for the One Identity Manager On Demand modules are enabled. All machine subroles are selected when you select the machine role. You can deselect individual packages.
6. 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.
7. 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.
8. Click **Finish** to close the installation wizard.
9. 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)

Notes on live operations

The consistency check provides different tests for analyzing data objects and to ascertain the current state of their data. It is recommended to run consistency checks at regular intervals and after extensive changes to the system configuration. You can run consistency checks in the Manager and the Designer. For more information, see under Checking data consistency in the Support Portal online documentation.

Not all consistency checks are available for end users and configuration users. If you want to run a database consistency check with administrative permissions, you must submit a service request through support. You can find the Support Portal under Product Support - Identity Manager On Demand.

8

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. These customizations include, object-dependent references, column-dependent references, modules, Web Designer components, importing compiled DLLs, and extending the base schema.

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 enter an non-upgradable 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