



Password Manager On Demand

Quick Start Guide

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon 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.

Contents

Overview: What is Password Manager On Demand?	4
Architectural Overview	5
Operational Guidelines	6
Sending required information to One Identity	7
What you receive from One Identity	10
Logging in to the Password Manager Administration Site	12
Configuring reporting in Password Manager	13
VPN Notes	17
General Notes	18
About us	19
Contacting us	20
Technical support resources	21

Overview: What is Password Manager On Demand?

This product is a complete Password Manager installation, provisioned in the One Identity cloud and connected to your network through a virtual private network (VPN) to manage the passwords of your on-premises Active Directory user accounts. One Identity will operate and monitor the runtime environment for you.

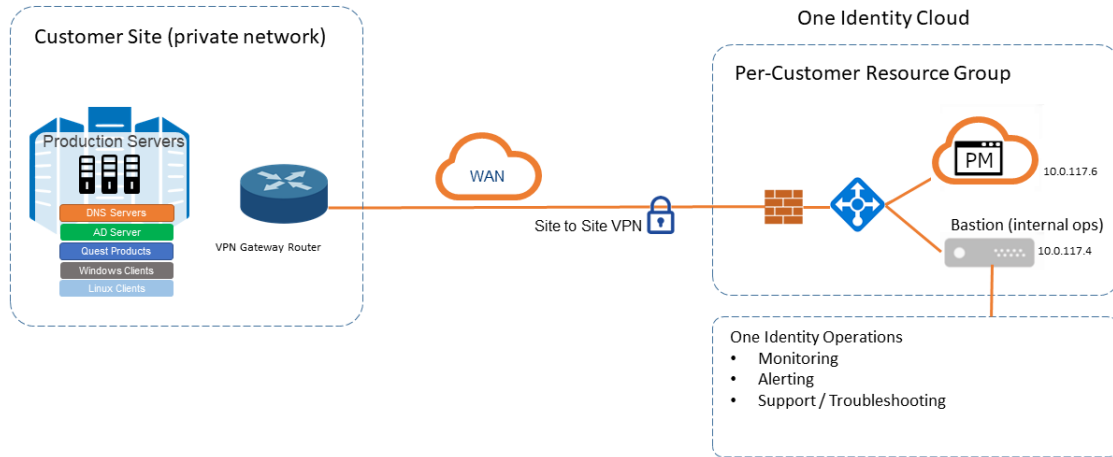
Password Manager On Demand is available both in a limited-time trial mode and in a subscription-based licensing model. Once One Identity enables Password Manager On Demand for your organization, you must send a set of required configuration information to the One Identity Cloud Operations Team via the [One Identity Starling](#) portal. For more information on providing the requested information, see [Sending required information to One Identity](#).

One Identity will provision your environment after providing the requested information. This provisioning can take up to 24 hours to complete, and some additional VPN configuration may be required to adjust your VPN gateway device to connect to the VPN gateway hosted on your behalf.

Because One Identity is provisioning this deployment in an address that is private to your VPN, One Identity will provide the IP address for Password Manager On Demand, and the administrator account credentials.

Architectural Overview

The following describes the components and architectural overview of your deployment.



Password Manager is a web-based application that provides an easy-to-implement and use, yet highly secure password management solution. Users can connect to Password Manager by using their favorite browser and perform password self-management tasks, therefore eliminating the need for assistance from high-level administrators and reducing helpdesk workload.

The solution offers a powerful and flexible password policy control mechanism that allows Password Manager administrators to ensure that all passwords in the organization comply with the established policies.

Operational Guidelines

The following list describes the operational guidelines for your deployment.

- The One Identity Cloud Operations Team pre-configures the administrator password. Use the administrator account and password to configure Password Manager On Demand for your environment.
- The One Identity Cloud Operations Team will proactively monitor your installation.
- The One Identity Cloud Operations Team will back up the system periodically and retain the backup for a period of 7 days in case an emergency restoration is required. Contact One Identity Support if an explicit restore is required.

Sending required information to One Identity

Before the One Identity Cloud Operations Team can configure and provision your Password Manager On Demand environment, you must send a set of configuration information via the One Identity Starling portal (<https://www.cloud.oneidentity.com>).

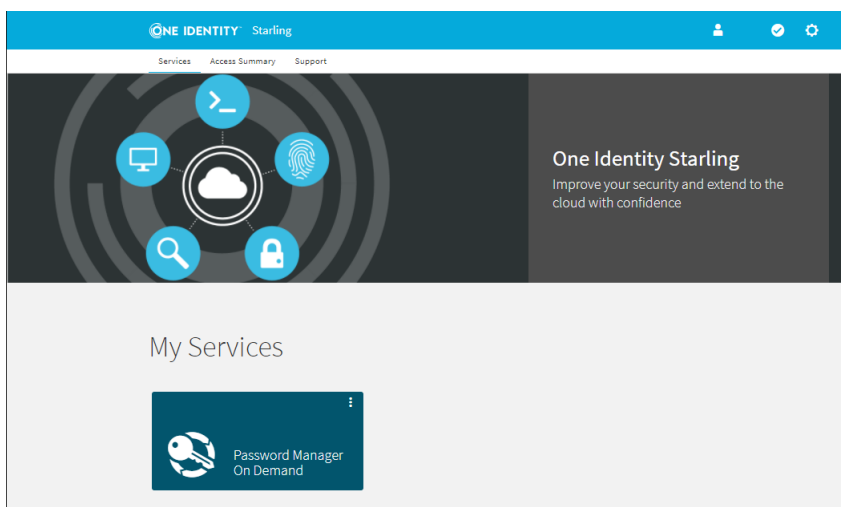
Prerequisites

Before collecting and sending the required information, make sure that the following conditions are met:

- Your organization is already registered on the [One Identity Starling](#) portal.
- If you configure a product trial, your One Identity representative notified your organization that the product trial has been added to your organization account.
- If you configure a subscribed product, your organization received a subscription confirmation email from One Identity.

To send product configuration information to the One Identity Cloud Operations Team

1. To open the list of product services available for your organization, in the [One Identity Starling](#) portal, click **Services**.



2. To start configuring the product, open the **Application** page of Password Manager On Demand.
 - To configure a product trial, open the **View On Demand services** ribbon at the bottom of the page and click **Password Manager On Demand > Trial**. This will create the trial subscription for you. Continue configuring the trial

subscription as described in the next bullet point.

- To configure a subscribed product (or an active product trial), click **My Services > Password Manager On Demand**.
3. In the **Contact Information** step, specify whether you are the technical contact for the One Identity Cloud Operations Team in your organization.

- If you are the technical contact (that is you have all the technical information required by One Identity to configure and provision Password Manager On Demand), select **I am the technical contact** and click **Next: Technical information**.
- If you are not the technical contact, then invite the contact who can provide the required configuration information. This is typically required if the initial On Demand invitation email was sent to you due to organizational policies, even if you are not the technical contact of the On Demand product. To invite the actual technical collaborator:
 - a. Select **Someone else is the technical contact**, then click **Invite Collaborator**.
 - b. In the **Invite Collaborator** dialog, provide the name and email address of the technical contact.
 - c. To send an invitation to the specified contact, click **Invite**.

TIP: You can also invite a technical contact by clicking **Collaborators** on the top left corner of the One Identity Starling web interface.

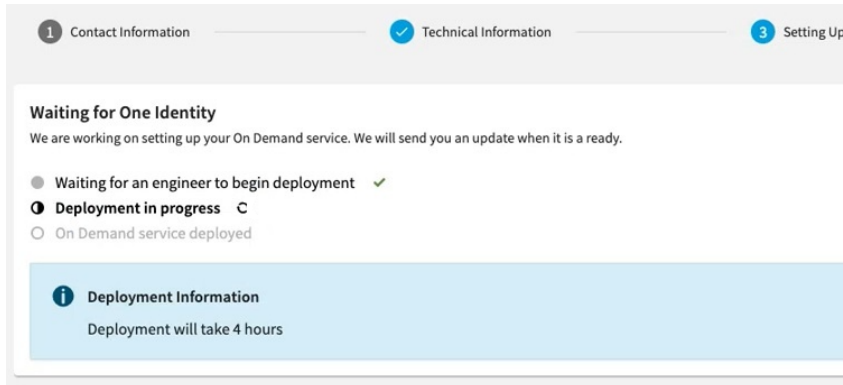
Once you sent the invitation to the technical contact, make sure that they perform the remaining steps.

4. In the **Technical Information** step, provide the required configuration information as instructed on-screen.
5. To confirm the information you entered, click **Submit Details**. This opens the **Confirm Details** dialog, where you can either send the information to the One Identity Cloud Operations Team (**Submit Details**), or return to the **Technical Information** step and make any final changes (**Edit Details**).

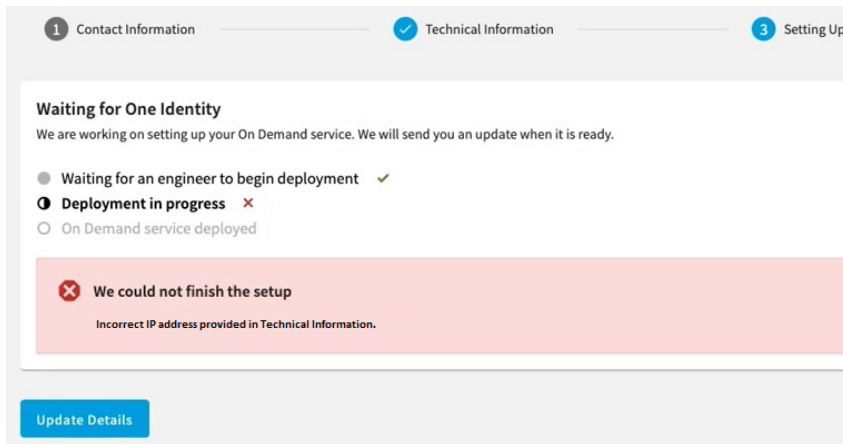
NOTE: Once you submit the specified information, you cannot make any further changes, unless One Identity rejects the provided configuration information for

some reason.

6. Once you sent the configuration information, the **Setting Up** step will indicate the status of provisioning and configuring Password Manager On Demand. One Identity will also send you an email notification each time the status of deployment changes.



The **Setting Up** step will also indicate if configuration fails for any reason (for example, because of incorrect data provided in the **Technical Information** step).



To open the **Technical Information** step and fix the provided information as requested by the One Identity Cloud Team, click **Update Details**. Once you updated the configuration details, resend them to the One Identity Cloud Operations Team by clicking **Submit Details** again in the **Technical Information** step.

Once Password Manager On Demand is configured for your organization, the **Application** page of Password Manager On Demand will display the connection and configuration data of your On Demand deployment.

What you receive from One Identity

Once your Password Manager On Demand installation is provisioned in the One Identity Cloud by the One Identity Cloud Operations Team, you will receive the following information and resources from One Identity:

- **Public IP address of the Password Manager On Demand instance**

You will need to setup a DNS reference for this public IP.

- **Administrator account (padmin) and password**

The account name and password will be sent to your Password Manager On Demand contact email address that you have provided during the registration process.

After receiving the Administrator account credentials, configure Password Manager On Demand. For more information, see [Password Manager Administration Guide](#).

- **User-specific technical details provided by One Identity**

One Identity will also provide you with technical details specific to each user as shown in the following example table. You can use that information, for example, to log in to the Password Manager Administration Site, and so on.

Table 1: Example of technical details provided by One Identity

Name	User-specific detail
Admin account name	CUSTOMER\padmin
Admin account password	*****
Admin URL	https://<public DNS name>/PMAdmin
Helpdesk Site URL	https://<public DNS name>/PMHelpdesk
Private IP Address	192.168.7.5
Public IP Address	13.64.230.0
Self-Service Site URL	https://<public DNS name>/PMSelfService
Public DNS Name	<CustomerName>.cloud.oneidentity.com
Reporting Services Report Server URL	https://<public DNS name>/ReportServer
Reporting Services Reports URL	https://<public DNS name>/Reports
SQL Reporting Services reports account	CUSTOMER\srs_reports
SQL Reporting Services reports account password	*****

TIP: Once Password Manager On Demand is provisioned, you can also download and install the following optional components in your on-premises environment:

- The Offline Password Reset (OPR) component (32-bit and 64-bit installers are available).
- The Password Policy Manager (PPM) component (64-bit installer only).
- The Secure Password Extension (SPE) component (32-bit and 64-bit installers are available).
- The administrative template required by OPR and SPE.
- The Password Manager Administrative Template Configuration tool, required to install administrative template.

Download the archive containing these resources from the Password Manager On Demand section of the *One Identity Support Portal*:

<https://support.oneidentity.com/password-manager-on-demand/hosted/download-new-releases>

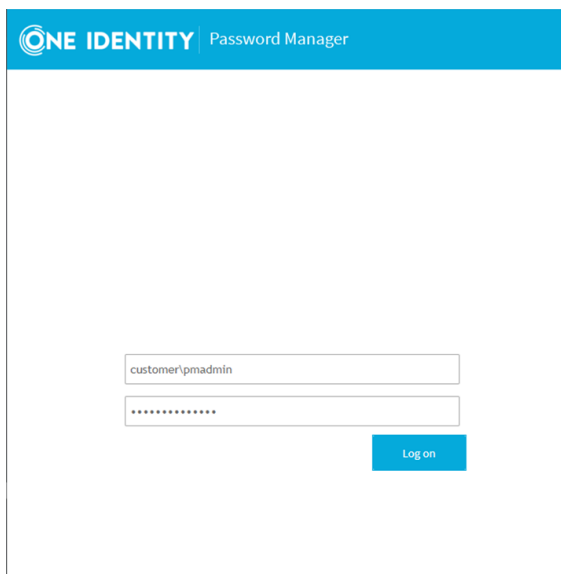
For the system requirements of these components, see the [Password Manager On Demand Release Notes](#).

Logging in to the Password Manager Administration Site

You can access the Password Manager Administration Site using the account details provided by One Identity.

To log in to the Password Manager Administration Site

1. Navigate to <https://<public DNS name>/PMAAdmin>.



The screenshot shows the login interface for the Password Manager Administration Site. At the top, there is a blue header with the One Identity logo and the text 'Password Manager'. Below the header, the main content area is white and contains a login form. The form consists of two input fields: the first field contains the text 'customer\padmin' and the second field contains a series of dots representing a password. To the right of the password field is a blue button labeled 'Log on'.

2. Log in using the **customer\padmin** account details provided by One Identity.
For more information on the provided information, see [User-specific technical details provided by One Identity](#).

Configuring reporting in Password Manager

To enable the reporting functionality in Password Manager, set up the reporting environment as described below.

Prerequisites

You have logged in to the the Password Manager Administration site. For more information, see [Logging in to the Password Manager Administration Site](#).

To configure reporting in Password Manager

1. From the main menu, select **Reporting**.



The screenshot shows the Password Manager Reporting interface. The left navigation menu includes Home, Licensing, General Settings, Password Policies, One Identity Starling, and Reporting (selected). The main content area is titled 'Reporting' and 'Statistics'. It features a bar chart icon and the text 'Reporting and User Action History'. Below this, there are links for 'Statistics', 'Reports', 'History', 'Edit Connections', and 'Disconnect Servers'. The page displays 'User Statistics on Thursday, May 06, 2021 04:00:00' with the following data:

Category	Count
Users (total)	0
Registered with Password Manager	0 users (0% of total)
Not registered with Password Manager	0 users (0% of total)
Scheduled to create profile	0 users (0% of total)
Scheduled to update profile	0 users (0% of total)

2. Click **Edit Connections**.
3. In **SQL Server Connection Settings**, configure the following:
 - In the **SQL Server** field , enter localhost\SQLEXPRESS.
 - In the **Database name** field, enter PasswordManager.
You can enter any valid name for the database.

SQL Server Connection Settings

Specify settings for connecting to the SQL Server.

SQL Server:

Database name:

Select an account for connecting to the SQL Server:

Password Manager Service account (CUSTOMER\SVC_oipm)

Specific SQL Server account

User name:

Password:

4. Click **Next**.
5. In **Create Database**, leave the Password Manager service account selected and click **OK**.

Create Database

Select the account that will be used to create the database.

Password Manager Service account (CUSTOMER\SVC_oipm)

Specific SQL Server account

User name:

Password:

6. In **Report Server Connection Settings**, configure the following:
 - In the **Report Server URL** field, enter `https://<public DNS name>/ReportServer`.
 - In the **Report Manager URL (optional)** field, enter `https://<public DNS name>/Reports`.
 - For both the deploying SSRS reports and connect to the data source fields, enter the `CUSTOMER\ssrs_reports` account details.

- Check the **Use as Windows credentials when connecting to the data source** option and click **OK**.

Report Server Connection Settings

Specify settings for connecting to the Report Server.

Report Server URL:

Report Manager URL (optional):

Specify the account for deploying SSRS reports:

User name:

Password:

Specify the account that the Report Server will use to connect to the data source:

User name:

Password:

Use as Windows credentials when connecting to the data source

7. To be able to run History reports, navigate to **General Settings > Scheduled Tasks** and under **User Status Statistics**, click **Run now**.

The screenshot shows the 'Scheduled Tasks' configuration page in the Password Manager web interface. The left sidebar contains navigation options like Home, Licensing, General Settings, Password Policies, One Identity Starling, and Reporting. The main content area shows a list of tasks with details for each:

- Reminder to Change Password**: Schedule: daily at 01:00, Instance: PASSWORDMGR01.customerfastsaas.corp, Last run time: 2022-05-06 01:00:00, Status: ran for 0 h 0 m.
- User Status Statistics**: Schedule: daily at 04:00, Instance: PASSWORDMGR01.customerfastsaas.corp, Last run time: 2022-05-06 04:00:00, Status: ran for 0 h 0 m. This task has a checkmark and a 'Run now' button.
- Clear Old Records from Reporting Database**: Schedule: once at 1/1/0001 12:00:00 AM, Instance: PASSWORDMGR01.customerfastsaas.corp, Record Types: never, Last run time: never, Status: never. This task is disabled and has a red message: 'Please configure the task settings'.

Result

You have enabled the reporting functionality in Password Manager as shown in the following example figure.

- Home
- Licensing
- General Settings
- Password Policies
- One Identity Starling
- Reporting

Reporting > Reports

Reports



Reporting and User Action History

[Statistics](#) | [Reports](#) | [History](#) | [Edit Connections](#) | [Disconnect Servers](#)

Reports list:

Report Name	Description	
Actions by month (bar chart)	Monthly number of user actions performed in Password Manager.	
Actions by Type	List of user actions sorted by type.	
Actions by user (pie chart)	Pie chart representing the percentages of actions performed by users in Password Manager.	
Actions by User	Summary of actions performed by each user.	
Email notifications by type (table)	List of email notifications sent to users sorted by type.	
Email notifications by user (table)	Summary of email notifications sent to each user.	
Help desk usage by actions (table)	Summary of actions performed on the Helpdesk site.	
Help desk usage by operators (table)	Summary of actions performed by each helpdesk operator.	
Help desk usage by users (table)	Summary of actions performed by helpdesk operators for each user.	
Registrations by month (bar chart)	Monthly number of users registered with Password Manager.	
User status (pie chart)	Pie chart representing the percentages of user statuses in Password Manager.	
User status (table)	List of users and their statuses in Password Manager.	

VPN Notes

The following describes details regarding your VPN connection and configuration. Make sure that you read and understand these guidelines.

- The parameters collected to set up your VPN initially are used to provision explicit network routes in Azure to connect your Password Manager On Demand instance to your own network.

⚠ CAUTION: If you are planning to change your VPN settings or other aspects of network configuration (for example, firewall rules), contact One Identity Support in advance to ensure that the One Identity Cloud Operations Team can make suitable changes to keep your network connected.

- As part of the provisioning process, you should receive a "VPN Configuration Bundle" which is created by the One Identity Cloud Operations Team to connect to your VPN device. Apply this script to your VPN configuration to set up the connection between your on-premises network and the VPN Gateway the One Identity Cloud operations provisions for you.
- One Identity monitors the VPN connection and raises an alarm condition if the VPN appears to be disconnected for approximately 15 minutes.
- One Identity uses the Azure Gateway product, which supports several common on-premises VPN devices.

For more information, see [About VPN devices and IPsec/IKE parameters for Site-to-Site VPN Gateway connections](#) in the *Microsoft VPN Gateway documentation*.

For additional troubleshooting and configuration information, see the Microsoft [VPN Gateway documentation](#).

General Notes

- The delivery of your system will be based on the data provided to One Identity at setup time.

For example, your Password Manager On Demand instance will reside in the One Identity Cloud at a distinct IP address. This is the system you will connect to configure and use the system. This IP address will be inside the pre-selected subnet of your network address space because of the VPN connection.

- Email notifications will be sent using your internal email solution. Therefore, make sure to configure your organizational email policies to allow the Password Manager On Demand service to send emails.

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