# Password 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.**

Password Manager On Demand Quick Start Guide
Updated - 07 May 2021, 02:48

# Contents

# Overview: What is Password Manager On Demand?

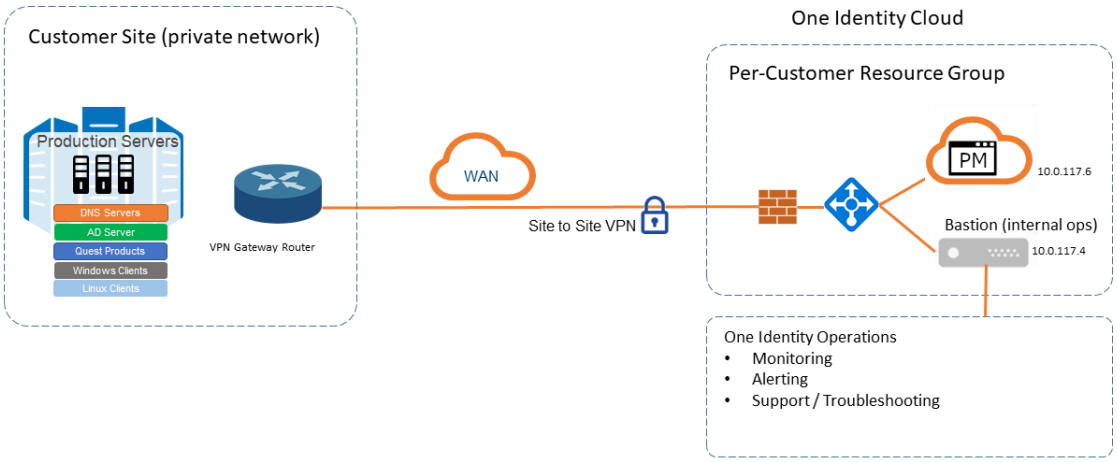
This product is a complete Password Manager installation, provisioned in One Identity's cloud and connected to your network through a virtual private network (VPN) to manage the passwords of your on-premises Active Directory user accounts.

One Identity will operate and monitor the runtime environment for you. When you purchase Password Manager On Demand, our team will provision your environment after collecting your specific network and VPN connection 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 in an address that is private to your VPN, One Identity will provide the IP address for Password Manager On Demand, and an 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 help desk workload.

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

# Operational Guidelines

The following describe operational guidelines on how your deployment will be operated.

- 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.

# What you receive from One Identity

You will receive the following 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 (`pmadmin`) 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.

- **Secure Password Extension (SPE) installer `.msi` file**

  After installing this component, end-users will be able to access Password Manager On Demand functionality from their client desktops.

- **GPO Administrative Templates**

  This template contains the group policy settings for Password Manager On Demand. You will have to configure the url for the self-service site so that you can use the Secure Password Extension.

- **Password Policy Manager (PPM) installer `.msi` file**

  (Optional): To ensure that passwords meet granular complexity requirements, install Password Policy Manager on all Domain Controllers (DC).

- **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 example table below. 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\pmadmin |
| Admin account password | ********** |
| Admin URL | https://<public DNS name>/PMAdmin |
| Helpdesk URL | https://<public DNS name>/PMHelpdesk |
| Private IP Address | 192.168.7.5 |
| Public IP Address | 13.64.230.0 |
| SelfService URL | https://<public DNS name>/PMSelfService |

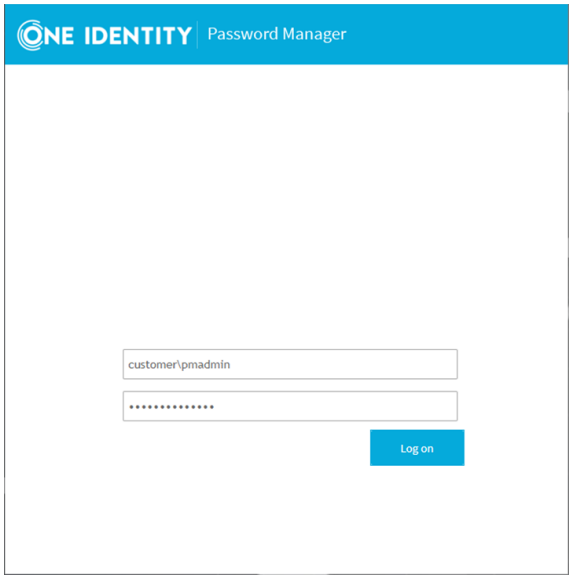
| Name | User-specific detail |
| --- | --- |
| Public DNS Name | <CustomerName>.cloud.oneidentity.com |
| Reporting Services Report Server URL | https://<public DNS name>/ReportServer |
| Reporting Services Reports URL | https://<public DNS name>/Reports |
| SQL Reporting Services reports account | CUSTOMER\ssrs_reports |
| SQL Reporting Services reports account password | ********** |

# 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>/PMAdmin.




2. Log in using the **customer\pmadmin** 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

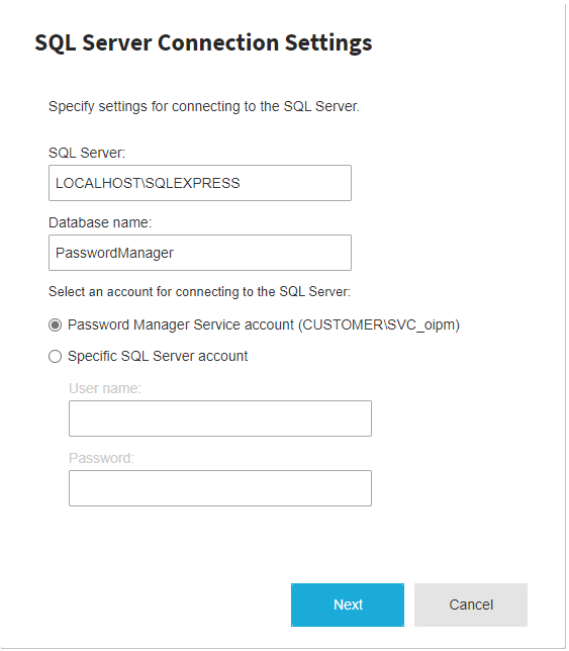
You have logged in to the the Password Manager Administration site. For more information, see Logging in to the Password Manager Administration site.

***To configure reporting in Password Manager***

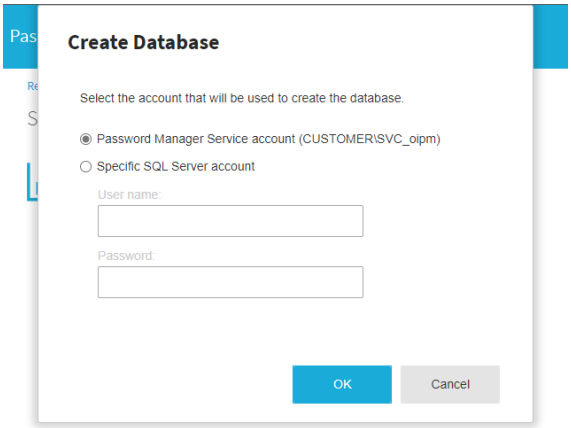
1. From the main menu, select **Reporting**.


2. Click **Edit Connections**.
3. In **SQL Server Connection Settings**, enter:
   - In the **SQL Server** field , enter `localhost\SQLEXPRESS`.
   - In the **Database name** field, enter `PasswordManager`.

     You can enter any valid name for the database.

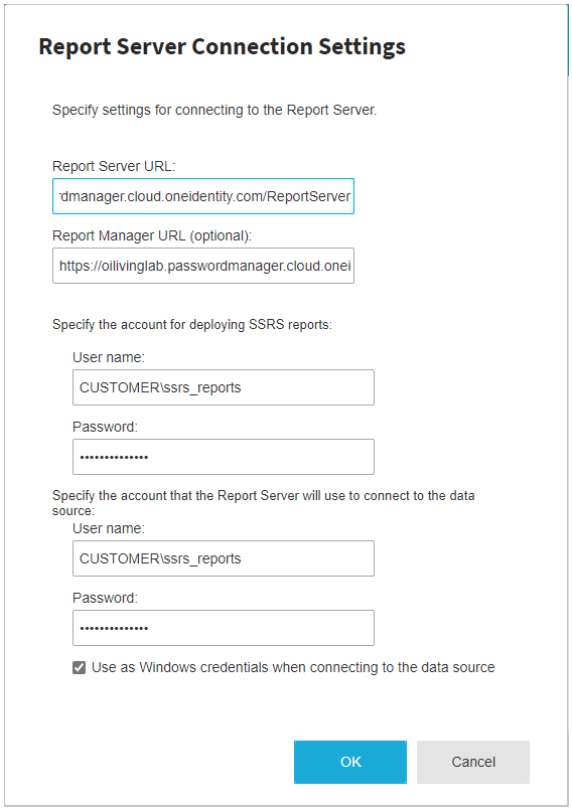



4. Click **Next**.
5. In **Create Database**, leave the Password Manager service account selected and click **OK**.

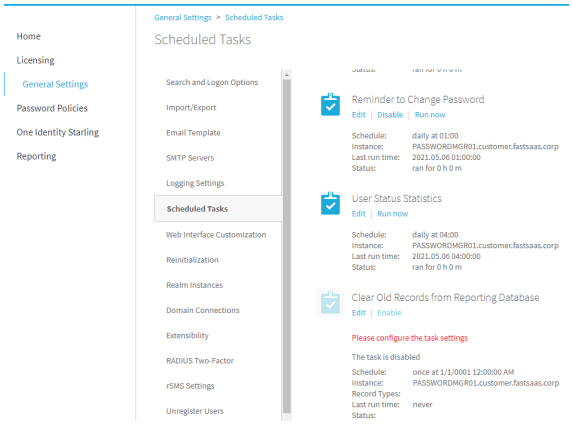



6. In **Report Server Connection Settings**, enter:
   - In the **Report Server URL** field, enter `https://<public DNS name>/ReportServer`.
   - In the **Report Manager URL (optional)** field, enter `https://<public DNS name>/Reports`.
   - For both the deploying SSRS reports and connect to the data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

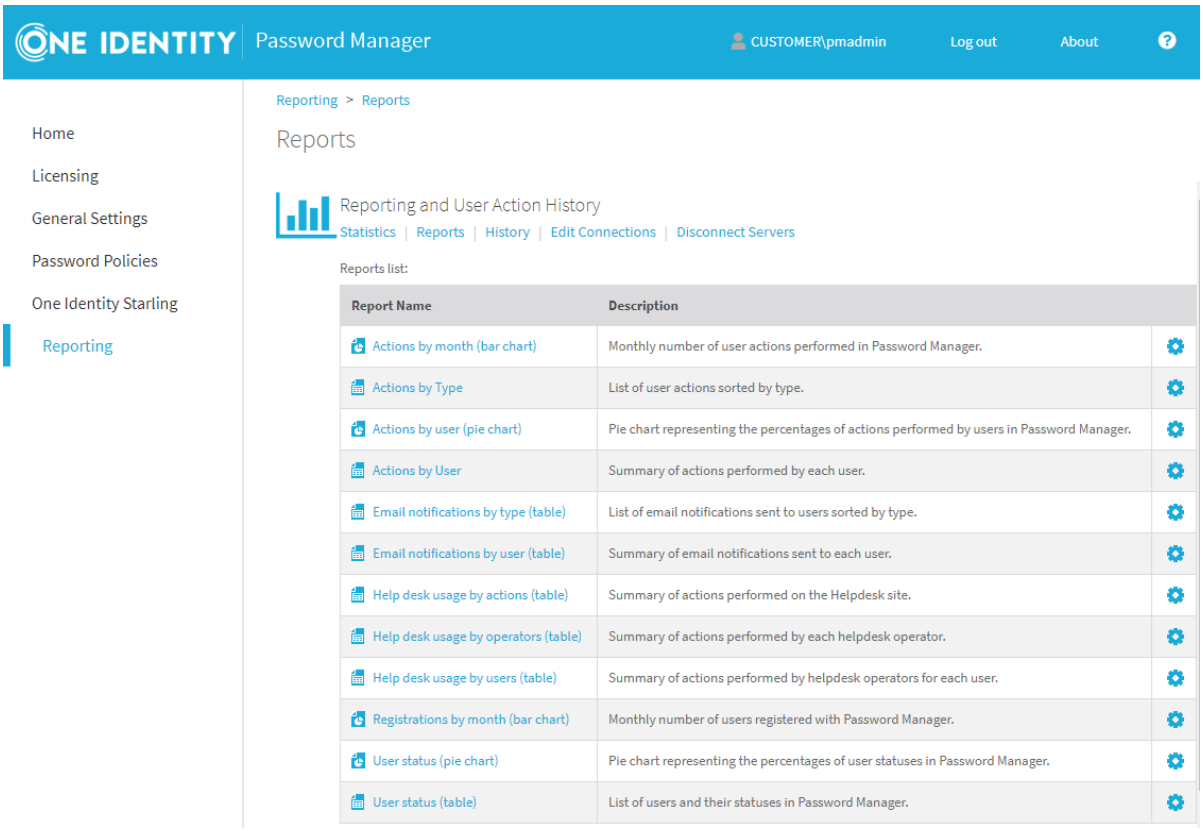



7. To be able to run History reports, navigate to **General Settings > Scheduled Tasks** and under **User Status Statistics**, click **Run now**.




## Result

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


ONE IDENTITY
Password Manager
CUSTOMER\pmadmin
Log out
About
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 *Microsoft's VPN Gateway documentation*.

  For additional troubleshooting and configuration information, see VPN Gateway documentation in *Microsoft's VPN Gateway documentation*.

# General Notes

- Delivery of your system will be a direct result of 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.
- Email notifications will be sent using your internal email solution. Please be sure to configure this 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