Password Manager On Demand

Release Notes

20 April 2022

These release notes provide information about the 20 April 2022 release of Password Manager On Demand. For the most recent documents and product information, see the Password Manager On Demand documentation on the *One Identity Support Portal*.

About this release

Password Manager On Demand is a complete Password Manager installation, provisioned in the One Identity cloud and connected to your network through a virtual private network (VPN). You can use Password Manager to manage the passwords of your on-premises Active Directory (AD) user accounts.

This Password Manager On Demand release is a full maintenance release with new features and functionality based on Password Manager 5.9.7.

New features

NOTE: This document lists only the On Demand-specific changes of Password Manager On Demand. For more information on the new features of Password Manager 5.9.7, see New features in the *Password Manager 5.9.7 Release Notes*.

The 20 April 2022 release of Password Manager On Demand has the following new features:

- Support for the Password Manager On Demand 5.9.7 release.
- One Identity now offers a customized archive for Password Manager On Demand, containing the following on-premises resources and optional software components:

- 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 System requirements.

See also:

- Enhancements on page 2.
- Resolved issues on page 2.

Enhancements

NOTE: This document lists only the On Demand-specific changes of Password Manager On Demand. For more information on the enhancements of Password Manager 5.9.7, see Enhancements in the *Password Manager 5.9.7 Release Notes*.

The 20 April 2022 release of Password Manager On Demand has no enhancements compared to the previous release.

Resolved issues

NOTE: This document lists only the On Demand-specific changes of Password Manager On Demand. For more information on the resolved issues of Password Manager 5.9.7, see Resolved Issues in the *Password Manager 5.9.7 Release Notes*.

The 20 April 2022 release of Password Manager On Demand has no resolved issues compared to the previous release.

Known issues

NOTE: This document lists only the On Demand-specific changes of Password Manager On Demand. For more information on the known issues of Password Manager 5.9.7, see Known Issues in the *Password Manager 5.9.7 Release Notes*.

The 20 April 2022 release of Password Manager On Demand has no known issues compared to the previous release.

System requirements

One Identity Password Manager On Demand provides its core features in a SaaS-delivered model. Therefore, you do not need to install the Password Manager Service or deploy the Administration, Self-Service and Helpdesk Sites on-premises.

However, to ensure that all Password Manager functionality is available in your organization, One Identity recommends installing the optional Offline Password Reset, Password Policy Manager and Secure Password Extension components on-premises with the indicated system requirements.

Download the archive containing these components, their administrative template and the Administrative Template Configuration Tool 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

Offline Password Reset

To allow users resetting their forgotten passwords when the company domain is unavailable (for example, because they are not connected to the corporate network), deploy the Offline Password Reset component on all target computers of the managed domain.

The target computers must meet the following minimum software requirements.

Table 1: Offline Password Reset Requirements

Requirement	Details
Operating system	Offline Password Reset supports the following operating systems: • Microsoft Windows 8.1 (32-bit and 64-bit editions) • Microsoft Windows 10 (32-bit and 64-bit editions)

For more information on how to install and configure Offline Password Reset, see To enable the Offline Password Reset functionality in the *Password Manager How-to Guide*.

Password Policy Manager requirements

To implement password policies in an Active Directory (AD) domain managed by Password Manager On Demand, deploy the Password Policy Manager (PPM) component on all domain controllers of the managed domain.

The domain controllers where you plan to install PPM must meet the following requirements:

Table 2: Password Policy Manager Requirements

Requirement	Details
Hard disk space	30 MB of free hard disk space.
Operating system	Password Policy Manager supports the following 64-bit operating systems: • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 NOTE: Password Policy Manager does not support Windows Server Core mode setup.

For more information on how to install and configure Password Policy Manager, see Installing Password Policy Manager in the *Password Manager How-to Guide*.

Secure Password Extension requirements

To support password resets from the Windows login screen, you must deploy Secure Password Extension on all target computers in the managed domain. The target computers must meet the following minimum software requirements:

Table 3: Secure Password Extension requirements

Requirement	Details
Operating system	Secure Password Extension supports the following operating systems: • Microsoft Windows 8.1 (32-bit and 64-bit editions) • Microsoft Windows 10 (32-bit and 64-bit editions)
Web browser	Microsoft Internet Explorer 11 NOTE: Due to potential security threats, One Identity does not recommend using any Internet Explorer plug-ins on computers with Secure Password Extension installed.

For more information on how to install and configure Secure Password Extension, see To deploy and configure Secure Password Extension in the *Password Manager How-to Guide*.

Password Manager Administrative Template Configuration tool

To add the administrative template provided by One Identity to the Group Policy Management Editor, use the Password Manager Administrative Template Configuration tool.

Table 4: Password Manager Administrative Template Configuration tool requirements

Requirement	Details
Operating system	The Password Manager Administrative Template Configuration tool supports the following operating systems: • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 NOTE: You must run this tool on the Active Directory Domain Controller of your organization.

New organization instructions

One Identity Password Manager On Demand provides its core features in a SaaS-delivered model. Therefore, you do not need to install the Password Manager Service or deploy the Administration, Self-Service and Helpdesk Sites on-premises.

However, to ensure that all Password Manager functionality is available in your organization, One Identity recommends installing the optional Offline Password Reset, Password Policy Manager and Secure Password Extension components on-premises with the indicated system requirements.

Download the archive containing these components, their administrative template and the Administrative Template Configuration Tool 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

When deploying Password Manager On Demand in your organization the first time, the deployment procedure has the following steps:

1. You must provide a set of technical and contact information via the One Identity Starling portal (https://www.cloud.oneidentity.com/) to the One Identity Cloud Operations Team. This is required so that you can connect to Password Manager On Demand later, and configure and use the product from within your company network.
2. The One Identity Cloud Operations Team pre-configures your cloud Password Manager environment and its administrator password, and will maintain the environment for you.

3. The One Identity Cloud Operations Team will notify you once they provisioned and configured your Password Manager On Demand environment, and will send you detailed information and resources to complete setting up your connection in your organization to Password Manager On Demand.
4. (Optional) To install the available on-premises Password Manager components (Offline Password Reset, Password Policy Manager, Secure Password Extension), and the Group Policy administrative template for the Offline Password Reset and Secure Password Extension components, download and extract the Password Manager On Demand installation package, available on the One Identity Support Portal.

For detailed instructions on how to deploy Password Manager On Demand in your organization, see *Password Manager On Demand Quick Start Guide* in the Password Manager On Demand documentation of the *One Identity Support Portal*.

More resources

Additional information is available from the following resources:

- For the most recent documents and product information, see the Password Manager On Demand documentation in the *One Identity Support Portal*.
- Join the Password Manager On Demand community at https://www.oneidentity.com/community/password-manager to get the latest product information, find helpful resources, test the product betas, and participate in discussions with the Password Manager On Demand team and other community members.

Product licensing

Use of this software is governed by the Software Transaction Agreement found at http://www.oneidentity.com/legal/sta.aspx and the SaaS Addendum at http://www.oneidentity.com/legal/saas-addendum.aspx. This software does not require an activation or license key to operate.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the

following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

The release is localized to the following languages: Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Swedish.

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

Patents

Trademarks

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.