Password Manager 5.13.2

Release Notes

27 February 2024, 17:20

These release notes provide information about the Password Manager 5.13.2 release. For the most recent documents and product information, see Password Manager Technical Documents on the One Identity Support Portal.

About this release

Password Manager 5.13.2 is a patch release with resolved issues.

- For the list of resolved issues, see Resolved issues.
- For the list of known issues, see Known issues.

Resolved issues

The following is a list of issues addressed in this release.

Table 1: Resolved issues – General Password Manager Issues

Resolved issue	Issue ID
Users can now register with the **Personal Email** method.	432389
The **Required unique characters** rule now evaluates the password correctly.	432728
The Chromium component of SPE has been updated to `117.2.4`.	434516
Fixed a potential security vulnerability in Secure Password Extension.	438569

Table 2: Resolved issues – Password Manager Self-Service Site

Resolved issue	Issue ID
The Password Manager Self-Service Site now uses the word **server** in the routes instead of **api**.	427249
The Password Manager Self-Service Site now authenticates the user correctly in the **Authentication with external provider** when the **Popup** login style is in use.	432719
The Password Manager Self-Service Site now presents HTML coded UI text labels in custom activities. The HTML code is sanitized by default, but this can be turned off in the `config.json` file at `<Password Manger installation folder>/Password Manager/Web/SelfService/Scripts/libs/assets/config/config.json`.	417153
The Password Manager Self-Service Site can load activities of the same type after one another correctly.	434544

Table 3: Resolved issues – Password Manager Administration Site

Resolved issue	Issue ID
The Password Manager Administration Site now displays the **Not configured** state of the **Authentication Methods** activity based on its settings.	426384
On the Password Manager Administration Site, the STS config page now sets the properties for External Federation providers correctly. Any previously configured but not working External Federation authentication provider must be saved again for it to work correctly.	432659
The Password Manager Administration Site now navigates to the correct Secure Token Server configuration page when stating that there are some configuration issues with a link pointing to the configuration page.	432924
Allow user search from external network now stores the state of **Allow user search from external network** option when **Do not allow users to search for their accounts** is selected. NOTE: You must reconfigure the **Allow user search from external network** option for the Administration Site to store the state of **Allow user search from external network**.	395034
ECDSA certificates are now supported.	404015

Table 4: Resolved issues – Password Manager Helpdesk Site

Resolved issue	Issue ID
The Password Manager Helpdesk Site now displays the **User cannot change password** information correctly.	426861

Resolved issue	Issue ID
Password Manager Helpdesk Site operators can now search for accounts across multiple domains based on the settings of the Helpdesk page even if domain selection is not available.	433314
Error pages now reflect the previously configured Web Interface customizations.	409587

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 5: Known issues

Known issue	Issue ID
When User Principal Name (UPN) is used as service account, installing a Password Manager hotfix can lock the service account. **Workaround** To solve the problem: 1. Change the service account to the `domainname\username` format. 2. Provide a password for the same service account user. 3. Install the Password Manager hotfix.	255614
Following a Password Manager upgrade, the **General** > **Settings** > **Scheduled Tasks** > **Active Directory Sites** task is disabled. **Workaround** After upgrading Password Manager to a newer version, enable the **Active Directory Sites** task manually.	246147
When scheduled from the secondary instance of the Password Manager server, the **General Settings** > **Unregister Users** task does not run. **Workaround** Schedule the **Unregister Users** task on the primary instance of Password Manager.	233679
If the application pool identity is a domain user with minimal permissions, then **Web interface customization** changes are not applied to the Self-Service and Helpdesk Sites.	233658
In the **General Settings** > **Instance Reinitalization** page, the **Corporate phone** attribute is not imported from the primary instance to	229200

Known issue	Issue ID
the secondary instance. **Workaround** Update the **Corporate phone** attribute manually on the secondary instance to have the same value as on the primary Password Manager instance.	
If the Password Manager Self-Service Site contains an IPv6 address, the location-sensitive authentication (LSA) feature does not work. **Workaround** LSA currently supports IPv4 addresses only. Therefore, do not access the Password Manager Self-Service Site from an external network where the request contains an IPV6 address.	221571
When configuring a dictionary rule in the Password Manager Administration Site, the **Policy Rules** > **Dictionary Rule** > **Enable dictionary lookup to reject passwords that contain** > **Beginning characters of a dictionary word** setting does not work correctly if you specify only 2 beginning characters. **Workaround** One Identity recommends using the **A complete word from the dictionary (QPMDictionary.txt)** setting when configuring a dictionary rule.	221468
If no appropriate authentication methods are configured for it, the **Forgot My Password** screen may appear blank in the Password Manager Self-Service Site or Helpdesk Site. **Workaround** In the Password Manager Administration Site, One Identity recommends configuring the **Register** workflow with **Security Questions** as one of its registration modes.	221389
When a symmetry rule is configured with the **Policy Rules** > **Symmetry Rule** setting of the Password Manager Administration Site, it may fail to validate passwords containing non-consecutive characters. **Workaround** Do not use the **Policy Rules** > **Symmetry Rule** > **Maximum number of consecutive characters within a password, that read the same in both directions (pass4554word)** setting.	220177
In a Password Manager for AD LDS environment, if the User Scope is configured with an AD LDS account, the **Forgot My Password** and **Manage My Passwords** workflows will fail. **Workaround**	220171

Known issue	Issue ID
When configuring a User Scope, do not use **The following AD LDS account** setting of the **Access account** > **Edit AD LDS Instance Connection** dialog.	
When a Questions and Answers Policy is updated with any language other than English, users may receive both the default and the custom email notifications on the Password Manager Self-Service Site. **Workaround** For the **Email user if workflow succeeds** workflow, change the value of the **Select email template to use** setting to **Customize**.	219401
Upgrading Password Manager from version 5.6.3 to 5.9.x keeps the previous **My Questions and Answers** profile workflow. **Workaround** To solve the problem: 1. In the Password Manager Administration Site, navigate to the **My Questions and Answers** profile workflow. 2. Open **Workflow Settings** > **Availability**. 3. Set **Enable the workflow** to **Never**. 4. Select **Show the workflow on the Self-Service Site**. 5. To apply your changes, click **OK**.	215892
The **User Status Statistics** scheduled task may fail intermittently.	171590
After upgrading to Password Manager 5.9.x, the **My Notifications** custom workflow cannot be edited in the Password Manager Self-Service Site. **Workaround** One Identity recommends to use the legacy Self-Service Site to edit the **My Notifications** workflow.	171589
When using Password Manager for AD LDS, the **Password Policies** page of the Administration Site is not updated when a password policy is created. **Workaround** After a new Password Policy is created, click **Save**, and immediately cancel the **Add New Policy** wizard. The page will refresh and list the new policy.	170587
After upgrading to Password Manager for AD LDS 5.9.x, the **General Settings** > **Search and Logon Options** menu may display an error when its settings are modified. **Workaround** To solve this problem:	170560

Known issue	Issue ID
1. In the Password Manager for AD LDS Helpdesk Site, navigate to **General Settings** > **Search and Logon Options**. 2. In the **Users must enter the following user account attribute for identification** setting, change the value from `sAMAccountName` to `cn`.	
In Password Manager for AD LDS, certain column data required for custom activities are not available in generated reports.	170355
After upgrading Password Manager from an earlier version to 5.9.x, the upgrade process may create duplicate URL references for the Password Manager User Site. **Workaround** Manually delete URL shortcuts that are not required.	169921
When a Password Manager for AD LDS instance and the Password Manager for AD LDS server instance are not configured on the same machine, Password Policy Rules are not displayed in the new and legacy Password Manager for AD LDS Self-Service Sites. **Workaround** Configure the Password Manager for AD LDS instance and the Password Manager for AD LDS server instance on the same machine.	169763
The user search settings of the Password Manager for AD LDS Helpdesk Site may work incorrectly. **Workaround** To solve the problem: 1. In the Password Manager for AD LDS Helpdesk Site, navigate to **General Settings** > **Search and Logon Options**. 2. Use the `cn` attribute instead of `mail` to search for users.	169384
The Password Manager Self-Service Site may not launch on Secure Password Extension (SPE) through a 32-bit operating system. **Workaround** If you have a 32-bit operating system, One Identity recommends to use the legacy Self-Service Site.	167871
When a password is changed from the target Active Directory (AD) system to that of the source AD, One Identity Quick Connect may be unable to synchronize passwords. **Workaround** Restart the Quick Connect Capture Agent Service on all the source and target systems.	167573

Known issue	Issue ID
In Password Manager versions 5.8.2 and 5.9.x, you can only reconnect to a domain on the second attempt. **Workaround** To solve the problem: 1. In the Password Manager Administration Site, select the User Scope, Helpdesk Scope or Password Policy you want to configure. 2. Click **Add domain connection** twice to add a new domain connection.	166950
In email notifications, the `#OPERATOR_ACCOUNT_NAME#`, `#OPERATOR_IP#`, `#WORKFLOW_RESULT#`, and `#WORKFLOW_SUMMARY#` parameters are not populated.	141728
On Windows Server 2019, the Password Manager Service and One Identity rSMS Service may stop. **Workaround** To solve the problem, make sure that the domain controller machine and the clients are at two separate entities.	127587
When editing a dictionary file between the size of 10–20 MB from a Password Policy, the web browser session may crash, and an error may appear in the Windows Event Viewer. **Workaround** If you must modify a dictionary file larger than 10 MB, edit it from the domain machine where Password Policy Manager (PPM) is installed.	115957
When performing a password reset with the Password Manager Helpdesk Site, the site also accepts the previous/old password. **Workaround** Manually enter a different password during the short duration of the password reset.	114822

System requirements

Before installing Password Manager 5.13.2, ensure that your system meets the following minimum hardware and software requirements.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. For more information about environment virtualization, see One Identity's Product Support Policies.

Password Manager Service and Administration Site requirements

Before installing Password Manager, ensure your system meets the following minimum hardware and software requirements. These requirements are applicable both to Full Installation and Distributed Installation (when the Self-Service Site and the Helpdesk Site are installed on separate systems).

Table 6: Password Manager Service and Administration Site requirements

Requirement	Details
Platform	1.6 GHz or higher.
Memory	At least 4 GB RAM.
Hard disk space	2.7 GB of free disk space. NOTE: If .NET Framework is already installed, then installation may require less disk space.
Operating system	Password Manager can be run on any of the following operating systems: • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 NOTE: Consider the following operating system and machine restrictions: • Password Manager is not supported on Windows Server Core mode setup. • One Identity does not recommend installing Password Manager on the machine where the Domain Controller (DC) server is installed. • Password Manager supports Windows Server 2016 and later versions in domain and forest functional levels, including domains operating in a mixed mode. • Password Manager does not support Windows Server 2012 R2 and earlier versions.
Internet Information Services	Password Manager requires any of the following Microsoft Internet Information Services (IIS) versions on the web server of your environment: • IIS 8.0 • IIS 10.0

Requirement	Details
	NOTE: PMSelfService site requires IIS 10. TIP: To ensure best practice security, configure Password Manager to use HTTPS. For more information, see *Password Manager 5.13.2 Administrator Guide* or *Password Manager 5.13.2 Administrator Guide (AD LDS Edition)*.
Web browser	Password Manager supports the following web browsers: • Microsoft Edge • Mozilla Firefox 10 or later • Apple Safari 5 or later • Google Chrome 15 or later
Microsoft .NET Framework	Microsoft .NET Framework 4.7.2 NOTE: Install .NET Framework before you install Password Manager.
Visual C++ Runtime Libraries	Password Manager supports the following Visual C++ Runtime Libraries: • Visual C++ Runtime Libraries 2017 • Visual C++ Runtime Libraries 2010 Visual C++ Runtime Libraries x86 and x64 are included in the Password Manager distribution package. NOTE: Install Visual C++ Runtime Libraries 2010 and Visual C++ Runtime Libraries 2017 before you install Password Manager.
Minimum screen resolution	1280x1024 pixels

Password Manager Self-Service Site requirements

Make sure that every client computer meets the following minimum software requirements:

Table 7: Password Manager Self-Service Site requirements

Requirement	Details
Web browser	The Password Manager Self-Service Site supports the following browsers: • Microsoft Edge

Requirement	Details
	• Mozilla Firefox 10 or later • Apple Safari 5 or later • Google Chrome 15 or later
Mobile web browser	The Password Manager Self-Service Site supports the following mobile browsers: • Microsoft Edge • Mozilla Firefox • Apple Safari • Google Chrome • DuckDuckGo • Samsung Internet
Minimum screen resolution	1280x1024 pixels

Password Manager Helpdesk requirements

Make sure that every client computer meets the following minimum software requirements:

Table 8: Password Manager Helpdesk Site requirements

Requirement	Details
Web browser	The Password Manager Helpdesk Site supports the following browsers: • Microsoft Edge • Mozilla Firefox 10 or later • Apple Safari 5 or later • Google Chrome 15 or later
Minimum screen resolution	1280x1024 pixels

Password Policy Manager requirements

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

The domain controllers where you plan to install the Password Policy Manager component must meet the following requirements:

Table 9: Password Policy Manager Requirements

Requirement	Details
Hard disk space	30 MB of free hard disk space.
Operating system	Password Policy Manager supports the following operating systems: • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 NOTE: Password Manager does not support Windows Server Core mode setup.

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 10: Secure Password Extension requirements

Requirement	Details
Operating system	Secure Password Extension supports the following operating systems: • Microsoft Windows 8.1 • Microsoft Windows 10 • Microsoft Windows 11
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.

Offline Password Reset requirements

To allow users to reset their forgotten passwords when they are not connected to the corporate network (making their domain unavailable), deploy the Offline Password Reset component on all target computers in the managed domain.

NOTE: Users can reset their passwords offline only if the Offline Password Reset component has been already installed prior to their scheduled password reset time.

The target computers must meet the following minimum software requirements:

Table 11: Offline Password Reset requirements

Requirement	Details
Operating system	The Offline Password Reset component supports the following operating systems: • Microsoft Windows 8.1 • Microsoft Windows 10 • Microsoft Windows 11 NOTE: Password Manager does not support Windows Server Core mode setup.

Password Manager Reports requirements

To configure and use Password Manager reports, you must:

1. Install an SQL server in your environment.
2. Configure reporting settings on the Password Manager Administration Site. For more information, see *Reporting* in *Password Manager 5.13.2 Administration Guide* or *Password Manager 5.13.2 Administration Guide (AD LDS Edition)*.

The report definitions included with Password Manager support all features of the SQL server versions listed in this section. All supported Microsoft SQL Server Reporting Services in Password Manager support SSL connection.

Table 12: Password Manager Reports requirements

Requirement	Details
SQL Server	The following SQL Server versions are supported: • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 • Microsoft SQL Server 2017 • Microsoft SQL Server 2019 • Microsoft SQL Server 2022

Accessing External URLs

To enable Password Manager to download images:

- The machine where Password Manager is installed must have an active Internet access.

Product licensing

Password Manager requires a license key for operation. For more information on license management, see *Licensing* in the *Password Manager 5.13.2 Administration Guide* or the *Password Manager 5.13.2 Administration Guide (AD LDS Edition)* documents.

[Placeholder for text]

Upgrade and installation instructions

For more information on how to install or upgrade Password Manager, see the following resources:

- When you upgrade Password Manager from versions prior 5.11.0 or 5.11.1 and Secure Token Server features are used, create a backup of **`Rsts.exe.config`** in `<password-manager-install-folder>\Service\SecureTokenServer`. When the upgrade is finished, restore these files.

  This procedure is not required for upgrades starting from version 5.12.0.
- If in any of the workflows in the **Authentication Methods** activity is used with the **Personal Email: Authenticate with Passcode** method, administrators must reconfigure this activity.
- For more information on the upgrade procedure, see *Upgrading Password Manager* in the *Password Manager 5.13.2 Administration Guide* or the *Password Manager 5.13.2 Administration Guide (AD LDS Edition)* documents.

  You can upgrade to Password Manager 5.13.2 from version 5.9.x or later.
- For more information on how to install and configure Password Manager, see *Installing Password Manager* in the *Password Manager 5.13.2 Administration Guide*, *Password Manager 5.13.2 Administration Guide (AD LDS Edition)*, or the *Password Manager 5.13.2 Quick Start Guide* documents.

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.

The Password Manager Self-Service Site is not localized in any language other than English.

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

Third-party contributions

This product contains some third-party components (listed below). Copies of their licenses may be found at referencing https://www.oneidentity.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 13: List of Third-Party Contributions

Component	License or Acknowledgement

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.