

One Identity Password Manager 5.8.2

Release Notes

Friday, December 21, 2018

These release notes provide information about the One Identity Password Manager release.

- [About One Identity Password Manager 5.8.2](#)
- [New features](#)
- [Enhancements](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [Product licensing](#)
- [Getting started with Password Manager 5.8.2](#)
- [Globalization](#)

About One Identity Password Manager 5.8.2

One Identity 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, thus 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 established policies.

New features

The following is a list of new features in Password Manager 5.8.2:

- Migration Wizard for ADLDS.
- FailSafe Support in Password Manager.

See also:

[Enhancements](#)

[Resolved issues](#)

Enhancements

The following is a list of enhancements implemented in Password Manager 5.8.2.

Table 1: Enhancements

Enhancement	Issue ID
Make the phone number attribute configurable from admin site for S2FA.	771907
Add custom attributes to user properties rule.	770718
Upgrade JQuery to the latest version.	767705
Provide meaningful numbers for EventID.	593514
More space between lines of password rules.	771686

Resolved issues

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

Table 2:

Resolved issue	Issue ID
Security Issue – improvements and remediation	663568
Security Issue – improvements and remediation	762917

Resolved issue	Issue ID
Security Issue – improvements and remediation	762918
Security Issue – improvements and remediation	762920
Security Issue – improvements and remediation	762921
Security Issue – improvements and remediation	762931
Security Issue – improvements and remediation	762932
Security Issue – improvements and remediation	768579
Inaccessible PMAAdmin site of PM 5.8.0, if local Administrator is used as PMSERVICE account.	776994
Inaccessible PMAAdmin site after upgrading to Password Manager 5.8.0 because of items absent in groups.	776930
Incorrect layout of PMUser site in Chrome when max-device-width is around 1024px.	773133
All dictionary operations must go through PMSERVICE.	767867
Password expiration notifications are not being sent by scheduled task.	778973
Password length indicator turns green after 7 characters, when 10 character is min pwd length.	775773
Offline Password Reset - Identification dialog - Spanish text does not fit its textbox area.	776608
Dictionary rule indicator on PMUser site displays incorrect results when user quickly types dictionary word.	777958
Performance issue in Password Manager	783464
Duplicate entries in search results when parent and child domain are added in user scope	784086
The character length of the answers in the Q&A profile do not adhere to the minimum character rule.	786226
Password Manager replication task throws a NullReference exception.	782810
After an upgrade to Password Manager 5.8.0, searching for an user requires a long time and timeout exception is displayed.	787723
User authentication on Password Manager Administrator, helpdesk, or user site is not functional.	787958
Setting an answer to a question is allowed even when the Q&A policy is configured to disallow this operation.	748048
Same answer can be provided to different questions in the Q&A profile.	750086

Resolved issue	Issue ID
User can be searched using any AD attribute in helpdesk site	786240
Using Password Manager when connected to the internet, Google fonts are downloaded and used in the application.	758639
Integrating help desk with Active Roles does not work as expected	760804
Password reset operation is applied to all Quick Connect systems though specific systems are selected from the user interface.	772977
Unable to setup SQL/SSRS connection after installing SOL257656	790606
Password Manager service crashes intermittently	783977
Unable to change the password with script or html tags such as <>	90415
User Status Statistics scheduled task throws SQLException with message "Incorrect syntax near ' '".	93268
Reset or Change password workflow throws exception "The server is not operational".	85546
Addressed translation issues in French files.	97907
My Notifications workflow contains Register and Manage My Profile workflow text.	99647
UK country code added in the phone number section during user registration.	99489

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 3:

Known issue	Issue ID
Users may fail to log in on the Self-Service site using their user principal names (UPNs). Workaround: Remove the corresponding managed domain from user scopes of configured Management Policies and add it again.	203516
On the Self-Service site, users may fail to authenticate themselves with	217751

Known issue	Issue ID
<p>passwords, if passwords contain only blank characters.</p> <p>Workaround: Users must change passwords so that passwords do not contain only blank characters.</p>	
<p>If you add a domain group to a user scope on the Administration site and then rename the group using standard Active Directory management tools (for instance, the "Active Directory Users and Groups" console), Password Manager may not rename the group on the User Scope page of the Administration site.</p> <p>Workaround: Remove the group from the user scope and add it again.</p>	220304
<p>If a user belongs to user scopes of two Management Policies, the user may receive two email notifications instead of one when enforcement rules and reminders are applied.</p> <p>Workaround: Either remove the user from the user scope of one Management Policy or from user scopes of enforcement rules and reminders belonging to a single Management Policy.</p>	220778
<p>If a domain management account is disabled or its password is changed, Password Manager continues to access managed domains and no errors occur.</p>	221124
<p>After importing the configuration to a Password Manager instance, there may be no notification on the Administration site that the account used to connect to the domain is invalid if the Password Manager Service account is used for connection.</p> <p>Do either of the following to work around this issue:</p> <ul style="list-style-type: none"> • After importing the configuration to a Password Manager instance residing in a different domain or installed on a standalone server, verify each domain connection and accounts used to access domains. • Do not use the "Password Manager Service account" setting for connecting to managed domains if Password Manager instances are installed in different domains or on standalone servers. 	259528
<p>Search for users may fail on the Self-Service and Helpdesk sites and a list of domain controllers for a managed domain may fail to be displayed on the Administration site, when a new domain controller is being promoted in the environment.</p> <p>Workaround: Stop all Password Manager application pools in the IIS and start them after the domain controller has been promoted and corresponding changes have been replicated.</p>	315876
<p>When two Management Policies have mutually exclusive user scopes, search for users on the Self-Service or Helpdesk site may fail.</p>	324517

Known issue	Issue ID
<p>Workaround: Do not create Management Policies with mutually exclusive user scopes, i.e. do not add the same groups to the scope of users allowed to access the Self-Service site in one Management Policy and to the scope of users denied access to the Self-Service site in the other Management Policy.</p>	
<p>Search for users may fail on the Self-Service and Helpdesk sites and a list of domain controllers for a managed domain may fail to be displayed on the Administration site, when a new domain controller is being promoted in the environment.</p>	335554
<p>Workaround: Stop all Password Manager application pools in the IIS and start them after the domain controller has been promoted and corresponding changes have been replicated.</p>	
<p>When installing Password Manager on a computer running Windows Server 2012 or Windows Server 2012 R2, installation may fail with the following error logged if the installation log is enabled: Error 0x80090016: Failed to Commit IIS Config Changes</p>	350492
<p>Workaround: To resolve this issue, follow instructions in Microsoft's article at http://support.microsoft.com/kb/977754.</p>	
<p>When several domains sharing the same UPN suffix are added to the user scope, Password Manager may fail to find users on the Self-Service site when search for users belonging to a domain other than the first one is performed by a user principal name.</p>	353295
<p>To work around this issue, perform the following steps on the "Search and Logon Options" page of the Administration site:</p>	
<ol style="list-style-type: none"> 1. Select the "Users must enter the following user account attribute for identification" option. 2. Enter the userPrincipalName value in the text box below that option. 3. Click Save. 	
<p>Information on how to clean up the Password Manager database is missing from the Password Manager Administrator Guide.</p>	437796
<p>Firefox may stop responding when you try to configure a UI-control in a custom activity.</p>	468748
<p>Workaround: Use a different browser, such as Chrome.</p>	
<p>After upgrade, the Password Manager service may not start as expected.</p>	468736
<p>Workaround: Use the Services console (Services.msc) to start the Password Manager service: Right-click that service in the console, and then click Start.</p>	
<p>After upgrade, you may view old QPM* application(s) in the IIS Manager console.</p>	468735

Known issue	Issue ID
Workaround: You may safely delete the old QPM* application(s) in the IIS Manager console.	
Form authentication fails for admin site if the domain name is not specified. Workaround: Provide the Domain name or Username to log into the Admin site.	98052


System requirements

This section provides system requirements for installing and running Password Manager and its components.

Password Manager Service and Administration Site requirements

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

Table 4:

Requirement	Details
Platform	1.6 GHz or higher Intel Pentium-compatible CPU
Memory	At least 1.5 GB RAM
Hard Disk Space	2.7 GB of free disk space  NOTE: If .Net Framework is already installed, then installation may take less space.
Operating System	Password Manager can be run on any of the following operating systems: <ul style="list-style-type: none"> • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016

Requirement	Details
Internet Information Services	<p data-bbox="592 271 1369 338">NOTE: Password Manager is not supported on Windows Server Core mode setup.</p> <p data-bbox="571 371 1342 434">On the Web server, Password Manager requires any of the following IIS versions:</p> <ul data-bbox="624 461 1246 636" style="list-style-type: none"> <li data-bbox="624 461 1230 488">• Microsoft Internet Information Services 7.0 <li data-bbox="624 506 1230 533">• Microsoft Internet Information Services 7.5 <li data-bbox="624 551 1230 577">• Microsoft Internet Information Services 8.0 <li data-bbox="624 595 1246 622">• Microsoft Internet Information Services 10.0 <p data-bbox="571 658 1358 752">To ensure best practice security, Password Manager should be configured to use HTTPS. For more information, see Administrator Guide.</p>
Web Browser	<p data-bbox="571 779 970 806">Microsoft Internet Explorer 11</p> <p data-bbox="571 824 767 851">Microsoft Edge</p> <p data-bbox="571 869 911 896">Mozilla Firefox 10 or later</p> <p data-bbox="571 913 759 940">Apple Safari 5</p> <p data-bbox="571 958 922 985">Google Chrome 15 or later</p>
Microsoft .NET Framework	<p data-bbox="571 1025 1002 1052">Microsoft .NET Framework 4.6.1</p> <p data-bbox="571 1070 975 1097">Microsoft .NET Framework 4.7</p> <p data-bbox="571 1115 1002 1142">Microsoft .NET Framework 4.7.1</p> <p data-bbox="571 1169 1321 1232">(This is not included with Password Manager distribution package.)</p> <p data-bbox="592 1258 1326 1321">NOTE: You must install .NET Framework before you install Password Manager.</p>
Visual C++ Runtime Libraries	<p data-bbox="571 1357 1038 1384">Visual C++ Runtime Libraries 2015</p> <p data-bbox="571 1402 1374 1536">Visual C++ Runtime Libraries x86 and x64 are included with the Password Manager distribution package. You must install Visual C++ Runtime Libraries 2015 before you install Password Manager.</p>
Acrobat Reader	<p data-bbox="571 1563 823 1590">Acrobat Reader DC</p> <p data-bbox="571 1608 1305 1671">Acrobat Reader DC 2018.011.20038 is included with the Password Manager distribution package.</p>
Minimum screen resolution	1280*1024 pixels

Password Manager supports Windows 2008 R2 and later versions in domain and forest functional levels, including domains operating in a mixed mode. Note that Password Manager installation is not supported on Windows 2008 and earlier versions.

Self-Service site and Helpdesk site requirements

Ensure that each of the client computers meets the following minimum software requirements:

Table 5:

Requirement	Details
Web Browser	Password Manager Self-Service and Helpdesk sites require any of the following Web browsers: <ul style="list-style-type: none">• Microsoft Internet Explorer 11• Microsoft Edge• Mozilla Firefox 10 or later• Apple Safari 5• Google Chrome 15 or later
Minimum screen resolution	1280*1024 pixels

Password Policy Manager requirements

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

The domain controllers where you plan to install a 32-bit or 64-bit version of Password Policy Manager component must meet the following requirements:

Table 6:

Requirement	Details
Hard Disk Space	30 MB of free hard disk space

Requirement	Details
Operating System	<p>Password Policy Manager can be run on any of the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 <p>i NOTE: Password Manager is not supported on Windows Server Core mode setup.</p>
Visual C++ Runtime Libraries	<p>Visual C++ Runtime Libraries 2015</p> <p>Visual C++ Runtime Libraries x86 and x64 are included with the Password Manager distribution package. You must install Visual C++ Runtime Libraries 2015 before you install the Password Policy Manager component.</p>

Secure Password Extension requirements

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

Table 7:

Requirement	Details
Operating System	<p>Secure Password Extension can be run on any of the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10
Web Browser	<p>Microsoft Internet Explorer 11</p> <p>We do not recommend use of any plug-ins for Microsoft Internet Explorer on computers where you plan to deploy Secure Password Extension, since the plug-ins extend Internet Explorer functionality and could pose security threats.</p>

Offline Password Reset requirements

To allow users to reset their forgotten passwords when users are not connected to the corporate network and domain is not available, you must deploy the Offline Password Reset component on all target computers in a managed domain. The target computers must meet the following minimum software requirements:

Table 8:

Requirement	Details
Operating System	<p>The Offline Password Reset component can be run on any of the following operating systems:</p> <ul style="list-style-type: none">• Microsoft Windows 7 Service Pack 1• Microsoft Windows 8• Microsoft Windows 8.1• Microsoft Windows 10 <p>NOTE: Password Manager is not supported on Windows Server Core mode setup.</p>

Password Manager Reports requirements

To be able to use Password Manager reports, you must install SQL Server and then configure reporting settings on the Password Manager Administration site.

Report definitions included with Password Manager are designed to support the functionality of all the supported Microsoft SQL Server Reporting Services listed in the following table. All the supported Microsoft SQL Server Reporting Services in Password Manager support SSL connection.

Table 9:

Requirement	Details
SQL Server	<p>Any of the following SQL Server versions is required:</p> <ul style="list-style-type: none">• Microsoft SQL Server 2008• Microsoft SQL Server 2008 R2

Requirement	Details
	<ul style="list-style-type: none"> • Microsoft SQL Server 2008 R2 Service Pack 2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2012 Service Pack 3 • Microsoft SQL Server 2012 Service Pack 4 • Microsoft SQL Server 2012 R2 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016

Accessing External URLs

To be able to download images, the following Password Manager websites need access to external URLs. The system where Password Manager is installed, must have access to internet to download images from the following URLs in the table.

Table 10: External URLs accessed by Password Manager

Site	External URL
User site	https://www.google.com/recaptcha/api.js https://www.gstatic.com/recaptcha/api2/v1520836262157/recaptcha__en.js https://www.google.com/recaptcha/api2/anchor?k=6LcG2DsUAAAAAKEKCWADyjQe2Zek5DqQUw-WgNZT&co=aHR0cDovL2dpdC50ZXN0LnBtLmNvcmsubGFiLmxvY2FsOjgw&hl=en-US&v=v1520836262157&theme=dark&size=normal&cb=mpq6141fwe4g https://www.google.com/recaptcha/api2/bframe?hl=en&v=v1520836262157&k=6LcG2DsUAAAAAKEKCWADyjQe2Zek5DqQUw-WgNZT&cb=xxe585r8wtzi https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=v1520836262157
Admin Site	api.2fa.cloud.oneidentity.com
Self-Service	api.2fa.cloud.oneidentity.com
Helpdesk	api.2fa.cloud.oneidentity.com

Upgrade and compatibility

Password Manager 5.8.2 is upgradable from Password Manager version 5.6.3 or later. For more information on how to upgrade, see the Administrator Guide.

Product licensing

For the license management instructions, see the Licensing section in the Password Manager Administrator Guide.

Getting started with Password Manager 5.8.2

Installation instructions

You can use the following steps to install Password Manager:

1. Run **autorun.exe**, located in the root folder of the Password Manager distribution CD.
2. Ensure that Adobe Acrobat Reader is installed on your computer. If not, go to the **Redistributables** page in the **Autorun** window and click **Adobe Acrobat Reader** to install the viewer.
3. Go to the **Documentation** page in the **Autorun** window.
4. In the **Password Manager** section, click **Administrator Guide** to display the document.
5. Follow the instructions in the Administrator Guide to install Password Manager components.

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 or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

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

Copyright 2018 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 indicates a potential for property damage, personal injury, or death.**
-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.**

Password Manager Release Notes
Updated - December 2018
Version - 5.8.2