One Identity Password Manager 5.8.0

Release Notes

Wednesday, May 23, 2018

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

About One Identity Password Manager 5.8.0

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 5.8.0:

- Integration of One Identity Starling 2FA with Password Manager.
- Integration of One Identity Starling 2FA in Password Manager to protect Administration site.
- Integration of One Identity Starling 2FA in Password Manager to protect Helpdesk site.
- Added option for the users to register with either Q&A or mobile or email address.
- Clear old hives from AD user objects.
- Clean up records in the reporting database older than a specified date.
- Support from LDAP to LDAP over SSL.
- Incorporated Password Manager with new Starling nugget package.
- Support for AZURE MFA 2FA.
- Custom script activity are shown in reports.
- QR code Enhancement in Offline Password Reset.

One Identity Hybrid Subscription

The newest versions of One Identity's on-premises products offer a mandatory One Identity Hybrid Subscription, which helps you transition to a hybrid environment on your way to the cloud. The subscription enables you to join Password Manager with the One Identity Starling software-as-a-service platform. This gives your organization immediate access to a number of cloud-delivered features and services, which expand the capabilities of Password Manager. When new products and features become available to One Identity Starling, the One Identity Hybrid Subscription allows you to use these immediately for Password Manager to add value to your subscription.

See also:

Enhancements

Resolved issues

Enhancements

The following is a list of enhancements implemented in Password Manager 5.8.0.

Table 1: Enhancements

Enhancement	Issue ID
Set 'Product_Name_Short' Parameter in the email notifications.	604546
Implement ability to change FROM field for notification email.	482152
Add First Name, Last Name, Windows login, hostname, UPN as separate parameters to email template.	670050
Auto-Generate Temporary Password for the Helpdesk users	746270
Connect PM to Azure MFA RADIUS	716033
Support for SQL 2012 SP 4	761286
Support for Dot Net Framework 4.7	761287
Support for Adobe Acrobat DC	764053

Resolved issues

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

Table 2:

Resolved issue	Issue ID
Sysvol folder is not present in default location.	756087
Password rule checker on web page does not correspond to Password Policy Manager.	727820
DsQuerySitesByCost sometimes produce errors which break execution of the whole workflow. Displays error of 1722: The RPC server is unavailable.	753274
Password is not masked in service host verbose log during offline password reset.	728087
Password is not masked on Admin site for domain management account (PM 5.6.3).	753761
Color customization is not applied to PMUser and PMHelpdesk site (ADLDS 5.7).	724137
Migration Wizard fails with error 1722: The RPC server is unavailable.	726230
Connection to reset password is empty when the change password run in user site.	724792

Resolved issue	Issue ID
Proxy settings are not applied by Secure Password Extension. All http traffic redirects to user site.	714515
Authenticate user by email (search) or logon names does not work if there are two or more Management Policies for the same domain.	744486
Repair of PM 5.7.1, clears SoftLicense key and makes it impossible to install any new license.	760828
Security vulnerability issue in Admin web application.	762913
Security vulnerability issue in Admin web application.	762905
Security vulnerability issue in Admin web application.	762908
Security vulnerability issue in Admin web application.	764060
Integration of Help Desk with Active Roles does not function as expected.	760804

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 passwords, if passwords contain only blank characters. Workaround: Users must change passwords so that passwords do not contain only blank characters.	217751
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.	220304

Known issue	Issue ID
Workaround: Remove the group from the user scope and add it again.	
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. 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.	220778
If a domain management account is disabled or its password is changed, Password Manager continues to access managed domains and no errors occur.	221124
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. Do either of the following to work around this issue: • 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
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. 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.	315876
When two Management Policies have mutually exclusive user scopes, search for users on the Self-Service or Helpdesk site may fail. 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.	324517
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.	335554

Known issue	Issue ID
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.	
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 Workaround: To resolve this issue, follow instructions in Microsoft's article at http://support.microsoft.com/kb/977754.	350492
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. To work around this issue, perform the following steps on the "Search and Logon Options" page of the Administration site: 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.	353295
Information on how to clean up the Password Manager database is missing from the Password Manager Administrator Guide.	437796
Firefox may stop responding when you try to configure a UI-control in a custom activity. Workaround: Use a different browser, such as Chrome.	468748
After upgrade, the Password Manager service may not start as expected. Workaround: Use the Services console (Services.msc) to start the Password Manager service: Right-click that service in the console, and then click Start.	468736
After upgrade, you may view old QPM* application(s) in the IIS Manager console. Workaround: You may safely delete the old QPM* application(s) in the IIS Manager console.	468735

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: • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 (Supports only Password Manager 5.7) NOTE: Password Manager is not supported on Windows Server Core mode setup.
Internet Information Services	On the Web server, Password Manager requires any of the following IIS versions: • Microsoft Internet Information Services 7.0 • Microsoft Internet Information Services 7.5 • Microsoft Internet Information Services 8.0 • Microsoft Internet Information Services 10.0 It is strongly recommended that you use HTTPS with Password Manager. For more information, see Administrator Guide.
Web Browser	Microsoft Internet Explorer 11 Microsoft Edge

Requirement	Details
	Mozilla Firefox 10 or later Apple Safari 5 Google Chrome 15 or later
Microsoft .NET Framework	Microsoft .NET Framework 4.6.1 Microsoft .NET Framework 4.7 Microsoft .NET Framework 4.7.1 (This is not included with Password Manager distribution package.) NOTE: You must install .NET Framework before you install Password Manager.
Visual C++ Runtime Libraries	Visual C++ Runtime Libraries 2015 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.
Acrobat Reader	Acrobat Reader DC Acrobat Reader DC 2018.011.20038 is included with the Password Manager distribution package.
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:

Requirement	Details
	• 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
Operating System	Password Policy Manager can be run on any of the following operating systems: • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 (Supports only Password Manager 5.7) NOTE: Password Manager is not supported on Windows Server Core mode setup.
Visual C++ Runtime Libraries	Visual C++ Runtime Libraries 2015 Visual C++ Runtime Libraries x86 and x64 are included with the Password Managerdistribution package. You must install Visual C++ Runtime Libraries 2015 before you install the Password Policy Manager component.

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	Secure Password Extension can be run on any of the following operating systems: • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10 Password Manager is not supported on Windows Server Core mode setup.
Web Browser	Microsoft Internet Explorer 11 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.

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	The Offline Password Reset component can be run on any of the following operating systems:

Requirement	Details
	• Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10 NOTE: Password Manager is not supported on Windows Server Core mode setup.

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	Any of the following SQL Server versions is required: • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • 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 fonts and images below Password Manager websites needs access to certain external URLs. The system where Password Manager is installed, must have access to internet to download images and fonts from below mentioned URLs.

Table 10:

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 https://fonts.gstatic.com https://fonts.googleapis.com
Admin Site	https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,300i,400,400i,600,600i,700,700i api.2fa.cloud.oneidentity.com
Self-Service	api.2fa.cloud.oneidentity.com
Help-desk	api.2fa.cloud.oneidentity.com

Upgrade and compatibility

Password Manager 5.8.0 is upgradable from Password Manager version 5.5.3 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 5.8.0

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

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

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 - May 2018
Version - 5.8.0