

One Identity Password Manager 5.9.5

Release Notes

Wednesday, May 19, 2021

These release notes provide information about the One Identity Password Manager release. For the most recent documents and product information, see [Password Manager online product documentation](#).

- [About One Identity Password Manager 5.9.5](#)
- [New features](#)
- [Enhancements](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [Upgrade and compatibility](#)
- [Product licensing](#)
- [Getting started with Password Manager 5.9.5](#)
- [Globalization](#)

About One Identity Password Manager 5.9.5

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 the supported 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 this release.

- Password Manager Self-Service site is fully functional
- Support for **Redistributable Secret Management Service** (rSMS) is fully functional
- Password Manager Group Policy ADM templates are migrated to ADMX format

See also:

[Enhancements](#)

[Resolved issues](#)

Enhancements

The following is a list of enhancements implemented in this release.

Table 1: Enhancements

Enhancement	Issue ID
<p>Password Manager Self-Service site is fully functional.</p> <p>The Password Manager Self-Service site provides functionality similar to the Legacy Self-Service site. The Password Manager Self-Service site includes enhancements to the user interface to improve the usability of the site.</p> <ul style="list-style-type: none">• Web interface customization is fully implemented in Password Manager Self Service site, which was a limitation in 5.9.3.• Change Language configured from the Q&A profile is now supported in the Password Manager Self Service site, which was a limitation in 5.9.3.• It is possible to revert to the Legacy Self-Service site at any time.• The URL for the PasswordManager_AD LDS has now been changed to https://<domain name>/PMSelfServiceAD LDS.	

Enhancement	Issue ID
<ul style="list-style-type: none"> The Password Manager Self Service site is now localized in other supported languages too. <p>Alternative options</p> <p>As an alternative to using Password Manager Self-Service site, use the Legacy Self-Service site.</p>	
<p>Support for Redistributable Secret Management Service (rSMS) is fully functional.</p> <p>Redistributable Secret Management Service (rSMS) can be used to manage user passwords across multiple connected systems. Using the rSMS service it is possible to quickly synchronize the passwords across connected systems. By default, the rSMS service is installed with the Password Manager software.</p> <p>Alternative options</p> <p>The Redistributable Secret Management Service (rSMS) feature can be used as an alternative to Quick Connect.</p>	
<p>Permission checker PowerShell tool</p> <ul style="list-style-type: none"> Readme is improvised with details Configuration.XML is clear and contains description Domain management account permissions and Local system permissions are separated. 	
<p>The UI of Web interface customization is changed to support the two types of Self Service site:</p> <ul style="list-style-type: none"> Self-Service UI 5.9.5 onwards Self-Service site (pre-5.9.5). 	
<p>Licensing enhancements:</p> <ul style="list-style-type: none"> Status of the license whether compliant/ Non-compliant is displayed in the Admin site. A column indicator to display the total purchased licenses and total number of users using it. If a telephone license is expired and it is past the grace period of 30 days , users will not be able to authenticate via phone if you do not decrease the number of user accounts set in the scope or do not update the license. 	
<p>Feedback form of the Password Manager Self service site is now documented.</p>	

Enhancement	Issue ID
Password Manager now supports the latest JQuery version 3.5.1.	
Introduction of new window in the Offline Reset Password (OPR) to support the QR code image in any resolution. It also provides the Self-Service site URL for the user if it is already present in the registry of that client machine.	
<p>Password Manager upgrade process has slight changes:</p> <ul style="list-style-type: none"> • Inplace upgrade has been improvised and with reduced steps during the installation process. • In-place upgrade will now install the following sites: Administration Site, Helpdesk Site, Password Manager Self-Service Site, and Legacy Self Service site • Manual upgrade now does not support Legacy self service site, by default. It has to be exclusively installed 	
Clean installation of 5.9.5 now installs the following sites: Administration site, Helpdesk site, Password Manager Self Service site. If the user intends to have Legacy Self service site then, it needs to be installed exclusively.	
The option Disable user search on Self-Service site for external network. Defining Corporate IP Address Range from General settings is required has now been changed to Allow user search from external network and is now part of Allow users to search for their accounts section in the Search and Logon Options.	224128

Resolved issues

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

Table 2: Resolved issues

Resolved issue	Issue ID
reCAPTCHA images are not displayed in Secure Password Extension (SPE).	100051
reCAPTCHA image is not validated on user search page if more than one user is found.	100266
reCAPTCHA is not validated if proxy is configured.	109946
Helpdesk site search limited to the specified attribute when Do not allow users to search for their accounts option is selected.	101164
Starling does not use the complete proxy settings.	106778

Resolved issue	Issue ID
Error occurred while running password expiration task.	790395
Scheduled tasks fail in multi-processor systems.	108986
Server error in Password Manager user application.	108086
Failed to update user profile when all the options are selected as registration mode and None is selected in mandatory registration mode.	110869
Duplicate entries observed in user search reports.	111445
Removal of OneIdentity phone number from the Help file of PMUser site.	125287
InstallDir registry value being reset to default.	85542
SPE Popup notification not working as expected	125586
User search in the Self Service site returns objects based on the AD attribute "Office"	127654
High transaction response time observed for beyond 100Vu concurrency load in user registration scenario.	139474
Manage My Password accepts old password during 5 minutes after the change	85601
In-place upgrade to latest builds does not load the images without page refresh	99351
No option to unjoin starling if it fails from PMAdmin site	108356
Starling join and subsequent SMS/Phone authentication are not working as expected, during/after upgrades.	125349
Server side request forgery (SSRF) Vulnerability in Password Manager user site.	127765
Registration workflow for end user require corporate mobile phone as optional, when starling is joined.	126565
TLS 1.0 has to be enabled for Starling authentication to work.	125661
Password Manager service becomes unresponsive under user load.	114913
Page scrolling does not work on iPad devices.	90421
Error when trying to send passcode.	117146
Dictionary rule being validated after all other policy rules are satisfied.	108328
#USER_UPN_NAME# for Password Expiration is not working as	110913

Resolved issue	Issue ID
expected.	
Reset Password workflow restricts helpdesk user to reset the password if Password Age rule is configured.	112471
Lot of errors "Input string was not in a correct format" are captured in the PM service logs.	114241
Unable to save the web service handler Power shell code in custom web services.	114414
Ability to remove the 0 (zero) through the script from the comment attribute.	110228
Configure persistent country code when post configuration of user's phone number registration.	110040
Simplify customization/localization method for country code's country name.	110039
Users With Apostrophes in their Name Do Not Meet Password Complexity Rules.	121280
Missing "Hide my answers for security purposes" checkbox in Forgot my password.	785014
#USER_FIRST_NAME# and #USER_LAST_NAME# are not populated in User Enforcement Rules email notifications.	85530
Password field does not support certain special characters leading to incorrect behavior of password strength meter.	218978
Password Manager license key grows indefinitely and gets corrupted in the registry.	218133
<p>i NOTE: If you are upgrading to 5.9.x, it is recommended to reinstall the license file once the upgrade is complete. Before installing the license, delete the existing SoftLicense binary value from [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Quest Software] registry key.</p>	
User is not able to change/ reset password in self service and helpdesk workflows, when Force user to change password at next logon activity is enabled, with LDAP over SSL.	218760
When Authentication Methods activity is configured for any workflow, user can identify the wrongly answered question from the HTTP Response object even after unchecking the Allow users to see what questions were answered correctly option.	220312

Resolved issue	Issue ID
User search with Domain\UserName does not show any results when Users must enter their logon names for identification on the Self-Service site option is selected.	229152
When Security questions are selected as the registration mode and if both E-mail and Mobile values are configured in the Active Directory before the user registration, Access is Denied error occurs while saving Q&A profile from the PMUser site.	227358
In the self-service site, partial username search from an external network displays the self-service tasks even if Allow user search from external network option is selected.	224128
ARS integration section has now been removed from the Admin guide.	228591
Content related to configuring read/write permissions to the E-Mail and Mobile attribute for Corporate Authentication is not available in the Password Manager Admin Guide.	228049
One Identity rSMS service runs successfully with the PM service account when installed, but fails to run when the account credentials are changed.	228856
Admin guide is now updated for occurrences of Vericloud with Vericlouds.	226427
Password Manager Self Service site does not allow to reset the password without the challenge code if Allow users to reset passwords offline option is enabled in the Reset Password in Active directory activity of the workflow.	221679
PM Self service site does not appear appropriately when accessed on the default browser of Android Tablet.	233336
Maximum Password Age configured as part of PM Password Policy, does not allow user to change password when user's password expires or when user's last password change duration is greater than Maximum Password Age.	230900
Permission Checker script unable to report the missing permissions required when the Password Manager Administrator is configured as a domain user with minimal permissions.	234824
Though Recaptcha is enabled, error message does not appear in UI when the internet connection is disabled.	216728
Password Manager authentication gets impacted when Microsoft updates settings for LDAP channel binding and LDAP signing.	201031
User is not able to reset the password in the AD environment even after enabling the Force user to change password at next logon	218760

Resolved issue	Issue ID
activity with LDAP over SSL.	
Password Manager server reaches 100% CPU utilization intermittently.	215747
When Authentication Methods activity is configured for any workflow, user can identify the wrongly answered question from the HTTP Response object even after unchecking the Allow users to see what questions were answered correctly option.	220312
User Status Statistics schedule task fails with LINQ exception when processing big groups.	220083
Few fields of the PMUser Site does not appear, when accessed on an Android Tablet Browser.	167521
Disabled users are not able to register with Password Manager successfully.	221967
Improper error messages appear when Google recaptcha service is not available.	220045
Support for reCAPTCHA v3 in PM application along-with configurable reCAPTCHA score (applicable to Legacy Self service only)	226568
When a PM service account is different than that of the logged in user account, installation of hotfix resets and locks the service account credentials.	228256
In the self-service site, partial username search displays the self-service tasks even if Allow user search from external network option is selected.	224128
When security questions are selected as the registration mode, Access is Denied error occurs while saving Q&A profile from the PMUser site.	227358
Reminder to Change Password and User Status Statistics schedule task fails with timeout exception.	227730
Service connection endpoint and replication container objects are not getting created for secondary replication instance.	227941
Reminder to Change Password and other scheduled tasks are failing on both the replication instances.	231398
Complexity Rule is not working as expected when the user account name has less than 3 characters.	231562
Complexity Rule password policy validation does not consider "." and "_" as special characters.	233386
Some of the special characters supported by windows were not	235732

Resolved issue	Issue ID
supported by Password Manager while checking for complexity rule.	
PM policy Complexity Rule validation fails when the characters of the user name are separated by space and are also part of the password entered.	235469
User cannot complete registration from Self-Service site if "Personal contact method" is selected during registration.	237830
Service connection endpoint and replication container objects are not getting created for secondary replication instance.	227941
jQuery has to be upgraded to version 3.4 to avoid new security vulnerability, which enabled attackers to overwrite a JavaScript application object prototype.	217557
reCAPTCHA icon does not appear in iPhone Safari/Chrome browsers.	237080
Scheduled Task execution fails on an environment configured with SSL.	235453
Leaf node created has permissions set to only the Computer account and the Domain Admin group, but not the Domain Users group.	113376
Starling Unjoin fails from Password Manager due to SSL/TLS version changes in Starling.	241191
User cannot validate password in PMADLDSUser page.	243161
PMUser site displays "You cannot use this account to log on to the Self-Service Site" error message when user named "SAVE" is accessed.	242412
Leaf node created has permissions set only to the Computer account and to the Domain Admin group, but not to the Domain Users group.	248783
Support for reCAPTCHA v3 authentication(applicable to Legacy Self service site only)	241594
Reminder to Change Password and User Status Statistics schedule task fails with timeout exception.	249374
Starling authentication fails when spaces are present as a separator in the mobile attribute of a user.	250379/250669
QR Code of OPR breaks when the Windows screen resolution is more than 100%.	239501
In Quick Connect, choosing Change password in this system independently from Active Directory option does not work as expected.	169315

Workaround: It is recommended to use Legacy Self-Service Site.

Resolved issue	Issue ID
<p>Please complete the reCAPTCHA message is shown in the search page when a non-existing user is searched in the Password Manager Self Service site.</p> <p>Workaround: Search user with valid username and correct reCAPTCHA in the Password Manager self Service site.</p>	170886
<p>Installation of Password Manager 5.9.x on a non-supported OS does not show a user-friendly message.</p> <p>Workaround: Password Manager installation has to always happen on a supported version of OS.</p>	215686
<p>Post upgrade of Password Manager from 5.9.x onwards, Digital signatures tab is missing for few DLL files.</p>	215928
<p>UI Hangs when S2FA is enabled for Admin, and when Starling is not reachable/account is disabled.</p>	252250
<p>Password Manager application to use the latest available jQuery version [3.5.1] in its application.</p>	245028

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 issues

Known issue	Issue ID
<p>On the Helpdesk Site, if the AutoGenerated password is enabled, the AutoGenerated password is not accepted, and the button is displayed by default. This issue occurs, if the company does not have a password policy set in Active Directory.</p> <p>Workaround: Set the password policy in Active Directory.</p>	264489
<p>The Q&A Policy can be saved without filling the mandatory questions fields. By leaving these fields empty, certain self-service workflows will not work.</p> <p>Workaround: Always provide mandatory questions when you are configuring the Q&A Policy.</p>	261495
<p>When scheduling tasks, the administrator can select a date which has already passed, and schedule a task for that day. For example, the administrator can select 2020-12-31 when, in fact, the current date is 2021-01-01. A status message is displayed of the un-register scheduled task.</p>	261496

Known issue	Issue ID
<p>Workaround: Currently, there is no workaround for this issue.</p>	
<p>Installing the hotfix locks the service account when UPN is used as service account.</p>	255614
<p>Workaround: Change the service account to "domainname\username" format and provide a password for the same service account user, and then, install the hotfix.</p>	
<p>Users may fail to log in on the Self-Service site using their user principal names (UPNs).</p>	203516
<p>Workaround: Remove the corresponding managed domain from user scopes of configured Management Policies and add it again.</p>	
<p>On the Self-Service site, users may fail to authenticate themselves with passwords, if passwords contain only blank characters.</p>	217751
<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>	220304
<p>Workaround: Remove the group from the user scope and add it again.</p>	
<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>	220778
<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>	
<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>	259528
<p>Workaround:</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 connect- 	

Known issue	Issue ID
ing to managed domains if Password Manager instances are installed in different domains or on standalone servers.	
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.	315876
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 two Management Policies have mutually exclusive user scopes, search for users on the Self-Service or Helpdesk site may fail.	324517
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.	
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.	353295
Workaround: Perform the following steps on the "Search and Logon Options" page of the Administration site:	
<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. 	
After upgrade, the Password Manager service may not start as expected.	468736
Workaround: Use the Services console (Services.msc) to start the Password Manager service: Right-click that service in the console, and then click Start.	
After upgrade, you may view old QPM* application(s) in the IIS Manager console.	468735
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.	98052
Workaround: Provide the Domain name or Username to log into the Admin site.	
Browser session crashes and an error is displayed in the windows event log, when the dictionary file between the size of 10 MB to 20 MB is edited from the	115957

Known issue	Issue ID
Password Policy.	
Workaround: If any modifications have to be made to the Dictionary file exceeding size greater than 10 MB, it has to be edited from the domain machine where the Password Policy Manager (PPM) is installed.	
On Windows Server 2019, services for Password Manager and rSMS is stopped.	127587
Workaround: Ensure that the DC machine and clients are at two separate entities.	
rSMS service restart is required for custom log path and custom certificate changes.	113794
A warning is displayed by the One Identity rSMS Service when you try to uninstall/ upgrade existing Password Manager version while the rSMS service is still running.	116469
Workaround: Accept the Warning and proceed with the uninstallation.	
In Quick Connect, unable to synchronize passwords when password is changed from the target to the source Active Directory system.	167573
Workaround: Restart the Quick Connect Capture Agent Service on all the source and target systems.	
On the Password Manager Administrator site, the page keeps loading after removing a custom workflow that was added.	169056
Workaround: Refresh the page to completely delete the custom workflow.	
Password Manager self-service site is not launched on SPE through a 32-bit system.	167871
Workaround: Recommend to use the Legacy self-service site on a 32-bit system.	
The user interface does not function as expected, when a large organizational unit (OU) is unregistered and the unregister task is stopped.	168143
Workaround: Refresh the unregister user page.	
Unable to edit or delete the translated questions in the Q&A profile.	168957
Workaround: Add another translated language to edit the previous translated question.	
The Password Policy Rules are not displayed in the Legacy self service site or the Password Manager self service site for Password Manager ADLDS.	169763
Workaround: Password Policy rules are displayed when the configured ADLDS instance and the Password Manager server instance is configured on the same machine	

Known issue	Issue ID
<p>Not able to access the Password Manager Administrator site when the domain user is the member of the local PMAAdmin group.</p> <p>Workaround: For PM versions 5.8.x or later, users must be a part of the local PMAAdmin group and either of IIS_IUSRS or Administrators group to access the PMAAdmin site.</p>	170441
<p>#OPERATOR_ACCOUNT_NAME#, #OPERATOR_IP#, #WORKFLOW_RESULT#, and #WORKFLOW_SUMMARY# parameters are not populated in the email notification.</p>	141728
<p>After upgrading Password Manager to 5.9.x, duplicate URL references are created for user site.</p> <p>Workaround: Open the location where the shortcuts of the URL are present and delete, if not required.</p>	169921
<p>Allow users to specify different password for this system option is not working as expected.</p> <p>Workaround: Restart the Quick Connect Capture Agent Service on all the source and target systems.</p>	169325
<p>After upgrading to Password Manager 5.9.x ADLDS version, search and logon page under General Settings menu displays an error when modified.</p> <p>Workaround: Replace the sAMAccountName attribute with cn in the Helpdesk site page under search and logon options for the option Users must enter the following user account attribute for identification.</p>	170560
<p>Issues in user search setting for Helpesk in ADLDS.</p> <p>Workaround: Search the user by the cn attribute though mail is the specified attribute in the helpdesk site of search and logon options.</p>	169384
<p>In Password Manager ADLDS, the UI is not updated when a password policy is created.</p> <p>Workaround: After a new policy is created, Click Save and immediately cancel the wizard of Create policy. Page refreshes to display the already created policy</p>	170587
<p>After upgrading to 5.9.x, My notification for a custom workflow cannot be edited in the Password Manager Self Service site.</p> <p>Workaround: It is recommended to use Legacy Self Service Site to edit My Notification.</p>	171589
<p>User Status Statistics, scheduled task fails intermittently.</p>	171590
<p>Symmetry rule fails to validate the password containing non-consecutive characters.</p> <p>Workaround: Administrators must avoid configuring the symmetry criteria</p>	220177

Known issue	Issue ID
<p>Maximum number of consecutive characters within a password, that read the same in both directions (pass4554word) under the Symmetry Rule.</p>	
<p>In the Password Manager Self-Service site of the ADLDS version of Password Manager, Change Language link of Q & A profile is not available in the Register page.</p>	221453
<p>Workaround: It is recommended to use the Legacy self-service site.</p>	
<p>When appropriate Authentication methods are not selected, Forgot My Password workflow screen is blank.</p>	221389
<p>Workaround: It is recommended to configure the Register workflow settings making Security Questions as one of the registration modes.</p>	
<p>Dictionary rule is not working as expected when 2 beginning characters of a dictionary word option is selected.</p>	221468
<p>Workaround: Configure the complete word from the dictionary (QPMDictionary.txt) as part of the Dictionary rule.</p>	
<p>During Password reset, helpdesk site accepts both previous/old passwords.</p>	114822
<p>Workaround: user has to manually enter a different password during a short duration of password reset.</p>	
<p>Post upgrade of Password Manager from 5.6.3 to 5.9.x, My questions and answers profile workflow still exists.</p>	215892
<p>Workaround: Navigate to My questions and answers profile workflow. Open the Workflow Settings page and navigate to the Availability tab. Click Never under Enable the workflow and Show the workflow on the Self-Service site options, and then click OK.</p>	
<p>In the Password Manager version 5.8.2 and 5.9.x, reconnecting to a domain is successful only after the two attempts.</p>	166950
<p>Workaround: Clicking on Add Domain Connection for two times will add a new domain connection.</p>	
<p>Inappropriate error message appears when recaptcha not entered for the second time.</p>	217064
<p>Workaround: Search users with correct username and recaptcha.</p>	
<p>In the Password Manager self-service site of the Password Manager version 5.9.x, password history does not appear.</p>	221152
<p>Workaround: It is recommended to use the Legacy self-service site.</p>	
<p>In the Password Manager self-service site, select language option does not change the language in the Display user agreement action.</p>	217068
<p>Workaround: It is recommended to use the Legacy version of self-service</p>	

Known issue	Issue ID
site.	
Few column data required for custom activities are not available on the reports generated on ADLDS.	170355
Location sensitive Authentication (LSA) feature does not work if self-service site request contain IPV6 address.	221571
Workaround: Do not access the self service site from an external network, where the request contains an IPV6 address. LSA currently works only for IPv4 addresses.	
Forgot My Password, Manage My Passwords fails in ADLDS environment, when the userscope is configured with ADLDS account.	220171
Workaround: Do not configure the userscope of Password Manager for ADLDS using "The following AD LDS account:"	
Corporate phone attribute does not get imported from primary instance onto the secondary replication instance in the Re-initialization page.	229200
Workaround: The Corporate phone attribute could be manually changed on the secondary instance to have the same value for Corporate Phone on both the PM Instances.	
Users receive both default and custom email notifications, when Q&A profile is updated with any other language(other than English) in the Self service site.	219401
Workaround : Change the settings in Email user if workflow succeeds workflow to Customize for the Select email template to use: option.	
Password Manager for ADLDS does not support Dictionary rule in OI Password policies.	97249
Workaround: Do not configure dictionary rule in Password Manager for ADLDS.	
When the Select default Language for email in the Email Template is configured as English(United States), users will receive emails only in English irrespective of the language chosen during registration, in the Self service site.	85543
Web interface customization does not get applied on Password Manager(AD and ADLDS), when the App pool account is a domain user with minimal permission.	233658
Unregister user task does not run when scheduled from the secondary instance of the Password Manager server.	233679
Workaround: It is recommended to schedule an Unregister Users task on the Primary instance of Password Manager.	

Known issue	Issue ID
reCAPTCHA v3 does not work in Password Manager self-service site. Workaround: It is recommended to use reCAPTCHA v2 instead of reCAPTCHA v3 for reCAPTCHA activity.	251284
Post upgrade, Active Directory sites (Scheduled Task) are in disabled state. Workaround: Post upgrade, manually enable the Active Directory sites.	246147

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 for Full Installation and Distributed Installation, if you have the Self-Service site and Helpdesk site installed on separate systems.

Table 4: 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 <div style="border-left: 1px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p>i NOTE: If .Net Framework is already installed, then installation may take less space.</p> </div>
Operating System	<p>Password Manager can be run on any of the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019

Requirement	Details
Internet Information Services	<p data-bbox="592 271 724 297">NOTE:</p> <ul data-bbox="691 331 1362 506" style="list-style-type: none"> <li data-bbox="691 331 1362 394">• Password Manager is not supported on Windows Server Core mode setup. <li data-bbox="691 412 1362 506">• It is recommended not to install Password Manager on the machine where Domain Controller (DC) server is installed.
Web Browser	<p data-bbox="571 539 1362 602">On the Web server, Password Manager requires any of the following IIS versions:</p> <ul data-bbox="624 629 1251 801" style="list-style-type: none"> <li data-bbox="624 629 1251 656">• Microsoft Internet Information Services 7.0 <li data-bbox="624 678 1251 705">• Microsoft Internet Information Services 7.5 <li data-bbox="624 728 1251 754">• Microsoft Internet Information Services 8.0 <li data-bbox="624 777 1251 804">• Microsoft Internet Information Services 10.0 <p data-bbox="571 831 1362 920">To ensure best practice security, Password Manager should be configured to use HTTPS. For more information, see Administrator Guide.</p>
Microsoft .NET Framework	<p data-bbox="571 1196 1007 1223">Microsoft .NET Framework 4.7.2</p> <p data-bbox="592 1249 1331 1317">NOTE: You must install .NET Framework before you install Password Manager.</p>
Visual C++ Runtime Libraries	<p data-bbox="571 1352 1038 1379">Visual C++ Runtime Libraries 2017</p> <p data-bbox="571 1402 1038 1429">Visual C++ Runtime Libraries 2010</p> <p data-bbox="571 1451 1374 1514">Visual C++ Runtime Libraries x86 and x64 are included with the Password Manager distribution package.</p> <p data-bbox="571 1536 1315 1626">You must install Visual C++ Runtime Libraries 2010 and Visual C++ Runtime Libraries 2017 before you install Password Manager.</p>
Acrobat Reader	<p data-bbox="571 1653 826 1680">Acrobat Reader DC</p> <p data-bbox="571 1702 1278 1760">Acrobat Reader DC 17.009.20044 is included with the Password Manager distribution package.</p>
Minimum screen resolution	1280*1024 pixels

Password Manager supports Windows Server 2012 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: Self-Service site and Helpdesk site requirements

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 or later• 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 64-bit version of Password Policy Manager component must meet the following requirements:

Table 6: Password Policy Manager Requirements

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: <ul style="list-style-type: none">• Microsoft Windows Server 2012 R2

Requirement	Details
	<ul style="list-style-type: none"> • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 <p>NOTE:</p> <ul style="list-style-type: none"> • Password Manager is not supported on Windows Server Core mode setup.

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: Secure Password Extension requirements

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 8.1 • Microsoft Windows 10 <p>NOTE:</p> <ul style="list-style-type: none"> • Operating systems that are not listed above are not supported.
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:

The Offline Password Reset component needs to be installed prior for this to work during the Password reset time.

Table 8: Offline Password Reset requirements

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 8.1• Microsoft Windows 10 <p>NOTE:</p> <ul style="list-style-type: none">• Password Manager is not supported on Windows Server Core mode setup.• Operating systems that are not listed above are not supported.

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: Password Manager Reports requirements

Requirement	Details
SQL Server	<p>Any of the following SQL Server versions is required:</p> <ul style="list-style-type: none">• Microsoft SQL Server 2012 R2• Microsoft SQL Server 2014• Microsoft SQL Server 2016• Microsoft SQL Server 2017• Microsoft SQL Server 2019

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	Google api.js
If you are using Starling, make sure that you have access to the following URLs.	
Admin Site	2faclient.cloud.oneidentity.com
Self-Service Site	2faclient.cloud.oneidentity.com
Helpdesk Site	2faclient.cloud.oneidentity.com

Upgrade and compatibility

Password Manager 5.9.5 is upgradable over version 5.8.2 or later.

For more information on the upgrade, please refer to the **Upgrading Password Manager** section in the Administration guide.

Product licensing

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

Getting started with Password Manager 5.9.5

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** tab in the **Autorun** window.
4. 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.

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 or other inquiries, 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

Copyright 2021 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 - May 2021
Version - 5.9.5