



One Identity Password Manager 5.9.7

How to Guide

Copyright 2022 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 How to Guide
Updated - April 2022
Version - 5.9.7

Contents

Overview	6
What's new in Password Manager 5.9.7	6
System requirements	6
Minimum permissions	9
Licensing	10
Using a license from a previous version	10
Telephone verification license	11
Starling 2FA license	11
RADIUS Two-Factor Authentication	11
How to obtain a new license key	11
Upgrading	12
Upgrade considerations	12
Is it possible to upgrade the Password Manager servers first and then the SPE (Secure Password Extension) at a later time?	12
Is it possible to roll back after the upgrade?	13
Does Password Policy Manager have to be upgraded on the Domain Controllers?	13
Upgrading from Password Manager 5.7.1 or later versions	14
Upgrading the Secure Password Extension	14
To remove the existing and assign a latest-version package	15
To remove an assigned MSI package	15
To deploy and configure Secure Password Extension	15
Upgrading Offline Password Reset	16
To remove the existing and assign a latest-version package	16
To remove an assigned MSI package	17
To deploy and configure Secure Password Extension	17
Additional information regarding upgrading	18
Secure Password Extension	19
Secure Password Extension communication	19
Requirements	20
Common Issues	20

GPO options for Proxy Settings	20
Workarounds	20
Offline Password Reset	22
Requirements	22
To enable the offline password reset functionality	23
Password Policy Manager	27
Overview	27
How it Works	27
Installing Password Policy Manager	28
Settings Controlled by the Password Policy	28
Configuring rules for a Password Policy	29
Configuration	30
Common Sample Questions	32
Helpdesk scope and options	33
Reinitialization	37
Reports	38
How to configure reports	39
Can you use a report database from a previous version of Password Manager?	39
Starling 2FA	40
Customizations	41
Customization tool	41
Troubleshooting	42
How to enable logging	42
To enable logging for Password Manager service	43
To enable logging for a stand-alone server	44
To enable logging for the Secure Password Extension (SPE)	44
To enable Password Policy Manager (PPM) logging:	45
Common solutions	46
How to move the Password Manager database	46
Changing the Password Manager service account	47
Workflow design considerations	48
When to use one Workflow	48
Benefit:	48

Drawback:	48
When to use separate workflows	48
Benefit:	49
Drawback:	49
Summary	49
Notes	50
About us	51
Contacting us	51
Technical support resources	51

Overview

This guide is intended for Password Manager 5.9.7. For versions 5.8.2 or previous releases, please refer to the respective versions of the How-to Guide. Unless otherwise stated, any reference to Password Manager in this guide is only applicable to versions 5.9.7.

For information on the Product Life Cycle, please visit the Password Manager product page at <https://support.oneidentity.com/password-manager/>.

What's new in Password Manager 5.9.7

Hiding personally identifiable information

Added a new option under **General Settings > Search and Logon Options > Security Settings** to show or truncate personally identifiable information (PII) on the user interface. For more information on configuring this setting and its effects, see *Hiding personally identifiable information for logged-in users* in the *Password Manager Administration Guide* or *Password Manager Administration Guide (AD LDS edition)* document (depending on the type of directory service you use).

NOTE: This section lists only the major new features of this release. For more information on the enhancements and known or resolved issues of Password Manager 5.9.7, see the *Password Manager 5.9.7 Release Notes* document.

System requirements

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

Table 1:
Password Manager and supported operating systems

Password Manager versions	Microsoft Windows versions
5.9.x	• Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 NOTE: Password Manager is not supported on Windows Server Core mode setup.

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.

Table 2:
Password Policy Manager and supported operating systems

Password Policy Manager versions	Microsoft Windows versions
5.9.x	• Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 NOTE: Password Manager is not supported on Windows Server Core mode setup.

Table 3:
Secure Password Extension and supported operating systems

Secure Password Extension versions	Microsoft Windows versions
5.9.x	• 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.

Table 4:
Offline Password Reset and supported operating systems

Offline Password Reset versions	Microsoft Windows versions
5.9.x	• Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows 10
	i NOTE: Password Manager is not supported on Windows Server Core mode setup.

Microsoft SQL Server versions supported for Password Manager service installation:

Table 5:
Password Manager and supported Microsoft SQL server

Password Manager versions	Microsoft SQL Versions
5.9.x	• Microsoft SQL Server 2012 R2 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 • Microsoft SQL Server 2017

Table 6:
Password Manager and supported Web browsers

Password Manager versions	Web browsers
5.9.x	• Microsoft Internet Explorer 11 • Microsoft Edge • Mozilla Firefox 10 or later • Apple Safari 5 • Google Chrome 15 or later

Table 7:
Microsoft .Net Framework

Password Manager versions	.Net Version
5.9.x	Microsoft .NET Framework 4.7.2

For additional detailed requirements, see the *One Identity Password Manager 5.9.7 Release Notes*.

Minimum permissions

As Password Manager sets passwords and other information on User objects in Active Directory, One Identity recommends that the best method to grant sufficient permissions is to make the Password Manager Service account a member of Domain Admins.

However, if the Password Manager Service account cannot be added to Domain Admins due to security and internal company restrictions, follow the comprehensive step-by-step instructions mentioned in <https://support.oneidentity.com/password-manager/kb/27946>.

In addition, the accounts you specify when installing Password Manager must meet the following requirements:

- Password Manager service account must be a member of the local **Administrators** group on the server where Password Manager is installed
- The Application pool identity account must be a member of the **IIS_IUSRS** local group when using IIS 7.0 or later. The account must also have permissions to create files in the **<Password Manager installation folder>\App_Data** folder.
- The Application pool identity account must have the Full Control permission set for the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager**

Licensing

The Password Manager license specifies the maximum number of user accounts enabled for management by Password Manager in all managed domains. When launching the Administration site, Password Manager counts the actual number of user accounts defined in all of the User scopes, and compares it with the maximum number specified by the license. If the number exceeds the maximum licensed number, a license violation occurs. A warning message is displayed on every connection to the Administration site of Password Manager. In the event of a license violation, you have the following options:

- Exclude a number of user accounts from the user accounts managed by Password Manager to bring your license count in line with the licensed value and reconnect to the Administration site to recalculate the license number
- Remove one or more managed domains to decrease the number of managed user accounts
- Purchase a new license with a greater number of user accounts. Click **Licensing** on the left menu and then select **Install License**

Note that the following items are not limited by the license:

- The number of computers connected to the Administration, Self-Service, and Helpdesk sites of Password Manager
- The number of Password Manager instances in a large enterprise. Password Manager can be installed on multiple servers for enhanced performance and fault tolerance with no impact to the license count

Using a license from a previous version

The License keys are set for major versions, such as 4.x or 5.x. As such, when the product changes to a major version number, a new key must be used.

For example, if you are currently running 4.7, then you must obtain a new License Key in order to upgrade and install any version of 5.x.

Telephone verification license

Password Manager previously provided the option for a separate Telephone Verification license using Telesign. If you already own a Telephone Verification license, you may continue to use it. New licenses can no longer be purchased as this feature has been replaced with Starling Two-Factor Authentication.

Starling 2FA license

Password Manager has the option to use Starling Two factor (2FA) Authentication.

Starling Two-Factor Authentication is a SaaS application that enables two-factor authentication on Password Manager. Starling Two-Factor Authentication uses the token generated by SMS, phone call or Defender Cloud application for authentication. Users can use this token to authenticate themselves on the Self-Service site and Helpdesk site.

For more information regarding Starling Two-Factor Authentication, see Starling 2FA later in this Guide.

RADIUS Two-Factor Authentication

RADIUS Two-Factor Authentication enables two-factor authentication on Password Manager. RADIUS Two-Factor Authentication uses one-time passwords to authenticate users on the Self-Service site and Helpdesk site.

To configure RADIUS Two-Factor Authentication in Password Manager, you have to configure the RADIUS server details in Password Manager.

RADIUS Two-Factor Authentication supports RADIUS servers such as AZURE MFA.

For more information, see Authenticate with RADIUS Two-Factor Authentication in the Password Manager Administration Guide.

How to obtain a new license key

To obtain a new License Key, please contact either your Account Manager or One Identity Licensing here:

<https://support.oneidentity.com/>

Upgrading

[Upgrade considerations](#)

[Upgrading from Password Manager 5.7.1 or later versions](#)

[Upgrading the Secure Password Extension](#)

[Upgrading Offline Password Reset](#)

Upgrade considerations

Password Manager 5.9.7 only supports upgrading from 5.7.1 or later.

If you have customized Password Manager in any manner, it is recommended to backup any of the modified files prior to upgrading as the upgrade process will remove the folder structure of the previous version of Password Manager, thus removing any custom settings.

It is not recommended to replace these files after upgrading, however you can refer to them for any custom settings. For instance, if you have changed the OU in which the _QPMStorageContainer account is stored in, then change the new file settings accordingly as the rest of the file will contain version-specific information. Failure to retain the new file could result in the product not functioning.

Is it possible to upgrade the Password Manager servers first and then the SPE (Secure Password Extension) at a later time?

Yes, it is possible for older SPE versions to communicate with Password Manager but in a very limited capacity.

The only option available for older SPE clients is the "Forgot My Password" link on the Windows logon screen. Options such as Registration are not supported.

To be able to accommodate this scenario, you can perform any of the following options:

1. Leave one old Password Manager server live so that the old SPE clients can still reach it.
2. Create a GPO using the Password Manager ADM template to force the Self Service URL to the new server

NOTE: Older SPE clients will work with the new Self Service site, but only if URL redirection is enabled.

3. Update DNS to have the old Password Manager server IP updated to the new server IP.

It is recommended to upgrade the SPE clients as soon as possible to avoid having the overlap.

Is it possible to roll back after the upgrade?

Once you upgrade to 5.9.7, it is not possible to roll back due to the security enhancements implemented. The configuration is encrypted in a new manner, along with all of the user profiles.

The only possible roll back option is to use a product such as Quest Recovery Manager for Active Directory (RMAD) to backup prior to upgrading, and then restore the "comment" attribute for all users after you have restored the Password Manager configuration to the pre-upgrade version.

Does Password Policy Manager have to be upgraded on the Domain Controllers?

Password Policy Manager must also be upgraded on all Domain Controllers. Note that the Domain Controllers must be rebooted.

NOTE: Although an older version of the components such as the SPE and Password Policy Manager may work with later Password Manager server versions, it has not been fully tested and is not officially supported.

Upgrading from Password Manager 5.7.1 or later versions

1. Navigate to the old Password Manager version 5.7.1 or later. Admin site and Export the Configuration from the 5.7.1 or later instance. Navigate to **General Settings > Import/Export**. Click on **Export Configuration Settings** from the dropdown option. Enter a password, and click **Export**.
2. Uninstall the exiting installation of Password Manager from **Programs and Features** in **Control Panel**.
3. Install Password Manager 5.9.7 on the server by launching **Autorun** within the installation media and walking through the installation wizard.
4. In the Password Manager Admin site, navigate to **General Settings | Import/Export**.
5. Click on the **Export Configuration Settings** option and choose **Import Configuration Settings**.
6. Click **Upload** and select the Export settings from Step 1.
7. Verify that the settings have been successfully imported to the new installation.
8. A reboot of the server is recommended.
9. If **Reporting** was configured in previous versions (5.7.1 or later), navigate to **Reporting** in the Admin site.
10. Click **Disconnect Servers** and click **Ok**.
11. Click **Edit Connections**.
12. Follow the wizard to create a new database and enter the SQL Reporting information.
13. After the configuration is confirmed, run the included Migration Wizard located in the installation source under \Password Manager\Setup\Migration Wizard. The file is **QPM.MigrationWizard.exe**.

NOTE: The Migration Wizard must be run as the account running Password Manager service as only that account will have the ability to update and re-encrypt the user profiles.

Upgrading the Secure Password Extension

You can centrally upgrade workstations to the latest version of Secure Password Extension by assigning the software for deployment using Windows Group Policy. It is recommended to remove the existing MSI package from the Software installation list, and then assign the latest-version package.

To remove the existing and assign a latest-version package

Remove the assigned package from the list of software to be installed.

For Password Manager 5.7.x or later:

SecurePasswordExtension_x86.msi or **SecurePasswordExtension_x64.msi**

You uninstall Secure Password Extension from end-user computers by removing the appropriate installation packages assigned through Group Policy. Uninstalling Secure Password Extension makes the Self-Service site no longer available from the Windows logon screen.

To remove an assigned MSI package

1. Start the Group Policy Management snap-in. To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Group Policy Management**.
2. In the console tree, click the group policy object with which you deployed the package, and then click **Edit**.
3. Expand the **Software Settings** container that contains the Software installation item with which you deployed the package.
4. Click the **Software installation** container that contains the package.
5. In the right pane of the Group Policy window, right-click the package name, point to **All Tasks**, and then click **Remove**.
6. Click **Immediately uninstall the software from users and computers**, and then click **OK**.
7. Quit the Group Policy Object Editor snap-in, and then quit the Group Policy Management snap-in.

Then, add the latest-version MSI packages to the list of software to be installed to a new GPO for the new version.

To deploy and configure Secure Password Extension

To configure and deploy the Secure Password Extension on end-user computers, do the following:

1. Copy the required installation package (**SecurePasswordExtension_x86.msi** or **SecurePasswordExtension_x64.msi**) from the installation CD to a network share accessible from all domain controllers where you want to install Secure Password

Extension. The MSI packages are located in the **\Password Manager\Setup** folder of the installation CD.

2. Create a GPO and link it to all computers, sites, domains, or organizational units where you want to use Secure Password Extension. You may also choose an existing GPO to use with Secure Password Extension.
3. Open the GPO in the Group Policy Object Editor, and then do the following:
 - Expand Computer Configuration/Software Settings, right-click Software installation, and then select New | Package.
 - Browse for the MSI package you have copied in step 1, and then click Open.
 - In the Deploy Software window, select a deployment method and click OK.
 - Verify and configure the properties of the installation, if needed.

When upgrading Secure Password Extension, do not forget to upgrade the **prm_gina.admx** administrative template with the one located in the **\Password Manager\Setup\Administrative Template** folder of the installation CD.

The **prm_gina.admx** administrative template file is located in the **\Password Manager\Setup\Administrative Template** folder of the installation CD. This administrative template is designed to be used with Windows Server 2008 R2 and later operating systems. Before using this administrative template, copy the **prm_gina.admx** and **prm_gina.adml** files from the installation CD to the following locations:
%systemroot%\policyDefinitions (for the **prm_gina.admx** file) and
%systemroot%\policyDefinitions\En-US (for the **prm_gina.adml** file).

Upgrading Offline Password Reset

You can centrally upgrade workstations to the latest version of Offline Password Reset by assigning the software for deployment using Windows Group Policy. It is recommended to remove the existing MSI package from the Software installation list, and then assign the latest-version package.

To remove the existing and assign a latest-version package

Remove the assigned package from the list of software to be installed.

For Password Manager 5.7.1 or later:

OfflinePasswordReset_x86.msi or **OfflinePasswordReset_x64.msi**

You uninstall Secure Password Extension from end-user computers by removing the appropriate installation packages assigned through Group Policy. Uninstalling Secure Password Extension makes the Self-Service site no longer available from the Windows login screen.

To remove an assigned MSI package

1. Start the Group Policy Management snap-in. To do this, click **Start**, point to Programs, point to Administrative Tools, and click **Group Policy Management**.
2. In the console tree, click the group policy object with which you deployed the package, and click **Edit**.
3. Expand the **Software Settings** container that contains the Software installation item with which you deployed the package.
4. Click the **Software installation** container that contains the package.
5. In the right pane of the Group Policy window, right-click the package name, point to **All Tasks**, and click **Remove**.
6. Click **Immediately uninstall the software from users and computers**, and click **OK**.
7. Quit the Group Policy Object Editor snap-in, and then quit the Group Policy Management snap-in.

Add the latest-version MSI packages to the list of software to be installed to a new GPO for the new version.

To deploy and configure Secure Password Extension

To configure and deploy the Secure Password Extension on end-user computers, do the following:

1. Copy the required installation package (**Offline Password Reset x86.msi** or **Offline Password Reset x64.msi**) from the installation CD to a network share accessible from all domain controllers where you want to install Secure Password Extension. The MSI packages are located in the **\Password Manager\Setup** folder of the installation CD.
2. Create a GPO and link it to all computers, sites, domains, or organizational units where you want to use Secure Password Extension. You may also choose an existing GPO to use with Secure Password Extension.
3. Open the GPO in the Group Policy Object Editor, and then do the following:
 - Expand Computer Configuration/Software Settings, right-click Software installation, and then select **New | Package**.
 - Browse for the MSI package you have copied in step 1, and then click **Open**.
 - In the **Deploy Software** window, select a deployment method and click **OK**.
 - Verify and configure the properties of the installation, if needed.

When upgrading Offline Password Reset, do not forget to upgrade the **prm_gina.admx** administrative template with the one located in the **\Password Manager\Setup\Administrative Template** folder of the installation CD.

The **prm_gina.admx** administrative template file is located in the **\Password Manager\Setup\Administrative Template** folder of the installation CD. This administrative template is designed to be used with Windows Server 2008 R2 and later operating systems. Before using this administrative template, copy the **prm_gina.admx** and **prm_gina.adml** files from the installation CD to the following locations:
%systemroot%\policyDefinitions (for the **prm_gina.admx** file) and
%systemroot%\policyDefinitions\En-US (for the **prm_gina.adml** file).

Additional information regarding upgrading

- **Upgrading Password Manager** section in the Password Manager Admin Guide
- Solution 105240: <https://support.oneidentity.com/kb/105240>
- Solution 104599: <https://support.oneidentity.com/kb/104599>

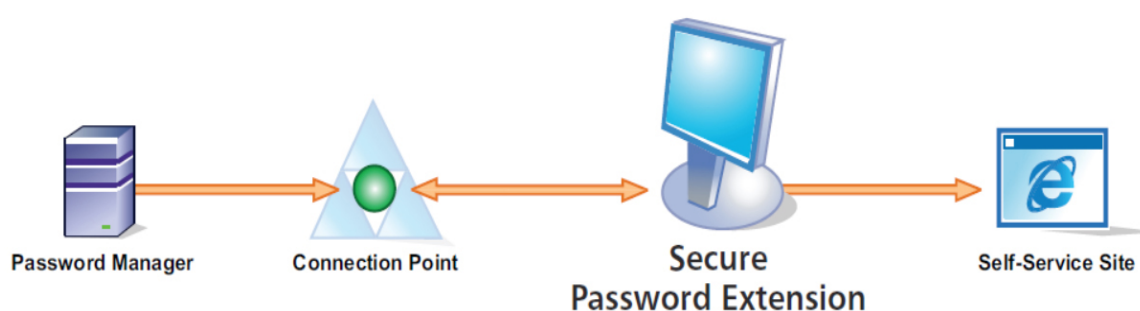
Secure Password Extension

Secure Password Extension is an application that provides one-click access to the complete functionality of the Self-Service site from the Windows logon screen. Secure Password Extension also provides dialog boxes displayed on end-user computers. These dialog boxes notify users who must create or update their Questions and Answers profiles with Password Manager.

Secure Password Extension communication

Secure Password Extension uses a URL from a service connection point to locate the Self-Service site. You can also override the default URL published in the service connection point by specifying a different URL in the General Settings of the Administration site or by specifying a different URL in the supplied administrative template and applying the template (via GPO) to selected users.

Figure 1:



Requirements

Password Manager must have sufficient permissions to create and write Service Connection Point objects in Active Directory under the System\One Identity for 5.7.1 and later. The URL is written in the Service Connection Point object.

Alternatively, you can take advantage of the included Password Manager GPO Administrative template to set the URL and push it down to clients so that the machines do not have to query Active Directory. This also ensures that the setting remains when users are not connected to the domain.

Common Issues

Common issues for the SPE client include network restrictions such as load balancers, proxy servers and Certificate Authorities. If the SPE is restricted by any of these then the Password Manager server cannot be contacted and the user will receive an error.

GPO options for Proxy Settings

The following Proxy options can be set using the included ADM template found in the installation media under Password Manager\Setup\Administrative Template:

Table 8:
Proxy settings

Proxy Options	Description
Enable proxy server access	This policy setting determines whether connections to the Self-Service from the Windows logon screen are established through the specified proxy server.
Enable proxy server access	Specifies the settings required to enable proxy server access to the Self-Service site from the Windows logon screen.
Configure optional proxy settings	Specifies optional settings for the proxy server access.

Workarounds

As previously noted, common issues include conflicts with proxy servers, load balancers and firewalls.

If the SPE cannot communicate with the Self-Service site, try the following:

1. Logon to the workstation and confirm that the Self-Service URL that is published on the desktop (shortcut) works
2. Make note of the URL that is set in the browser address bar
3. Logon to the Password Manager Admin site and under **General Settings | Realm Instances** ensure the URL is the same.

If the URL is incorrect in the Admin site:

- Update the setting on the Realm Instances page to the correct desired URL

If the URL is correct in the Admin site:

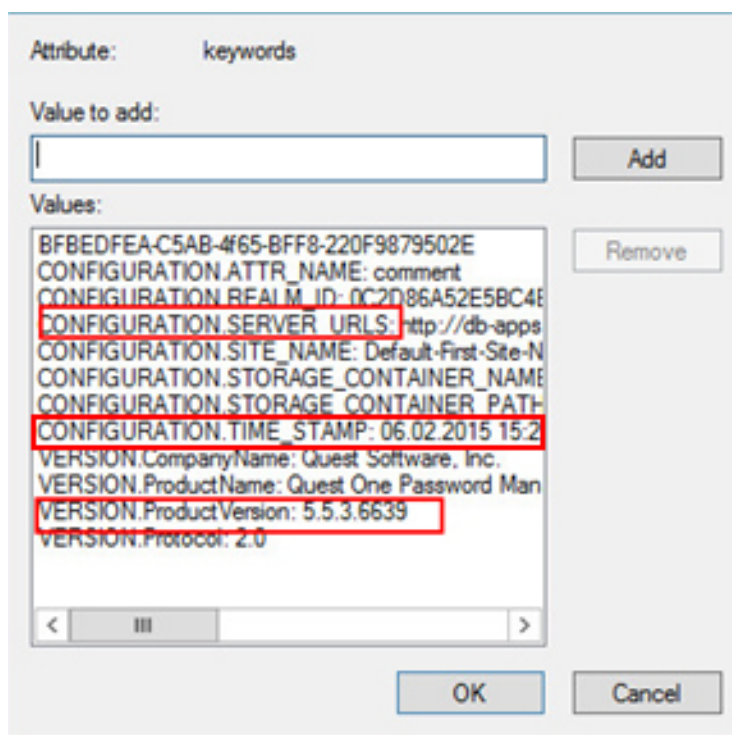
- Check in Active Directory under **System\One Identity** for any Service Connection Points. You can either use **ADSIEdit** or **Active Directory Users and Computers** MMC Snap-Ins.

Any stale or invalid Service Connections Points available, must be deleted.

In order to determine whether or not the Service Connection Points are valid, you will have to right-click and select **Properties** on the object and click **Attribute Editor**. Look for **keywords** and then click Edit. Look for the entries called **CONFIGURATION.SERVER_URLS**, **CONFIGURATION.TIME_STAMP** and also **VERSION.ProductVersion**.

Example:

Figure 2:



4. If the URLs and Service Connection Point objects are correct, check proxy settings.
Check with your internal team that is responsible for the proxy server configuration to confirm whether or not anonymous access is allowed.
If it is not allowed, try setting the following options in a GPO using the Password Manager Administrative template:
Proxy server: i.e. `http://proxy.dc.domain.com:8080`
Or
Proxy server configuration script: **`http://proxy.dc.domain.com/proxy.pac`**
5. Confirm the Network Load Balancer has the correct server IP addresses configured.
Check with your internal team that is responsible for the Network Load Balancer to ensure it has the correct IP addresses for all Password Manager servers using the Self-Service URL.

Offline Password Reset

The Offline Password Reset utility allows resetting passwords when users have forgotten their current passwords and their computers are not connected to the Intranet (Active Directory is not available).

Requirements

- The client machine must have the Offline Password Reset utility installed along with the SPE (Secure Password Extension).
- The user must have Internet access from another machine or Internet-capable Smartphone to access the public-facing corporate Password Manager Self Service site
- The Forgot My Password workflow (or similar) must have the Allow Users to reset passwords offline option enabled on the Change Password In Active Directory action.
- Cached logon attempts must be configured
- The Password Manager administrative template must be configured to turn on Offline Reset functionality

To enable the offline password reset functionality

1. Install the offline password reset component on target users' computers via group policy. Use the Password Manager files (OfflinePasswordReset_64.msi and OfflinePasswordReset_x86.msi) located in the \Password Manager\Setup folder on the installation CD.

Secure Password Extension (SPE) must be installed on target users' computers as well.

2. Set the required number of cached user logon attempts. This is necessary because the offline password reset functionality will be available only for users who have previously logged in on their computers. You can use Microsoft knowledge base article <http://support.microsoft.com/kb/172931> to change the number of cached logon attempts. It is recommended to use the default value (10).

Figure 3: Setting Logon Count via GPO

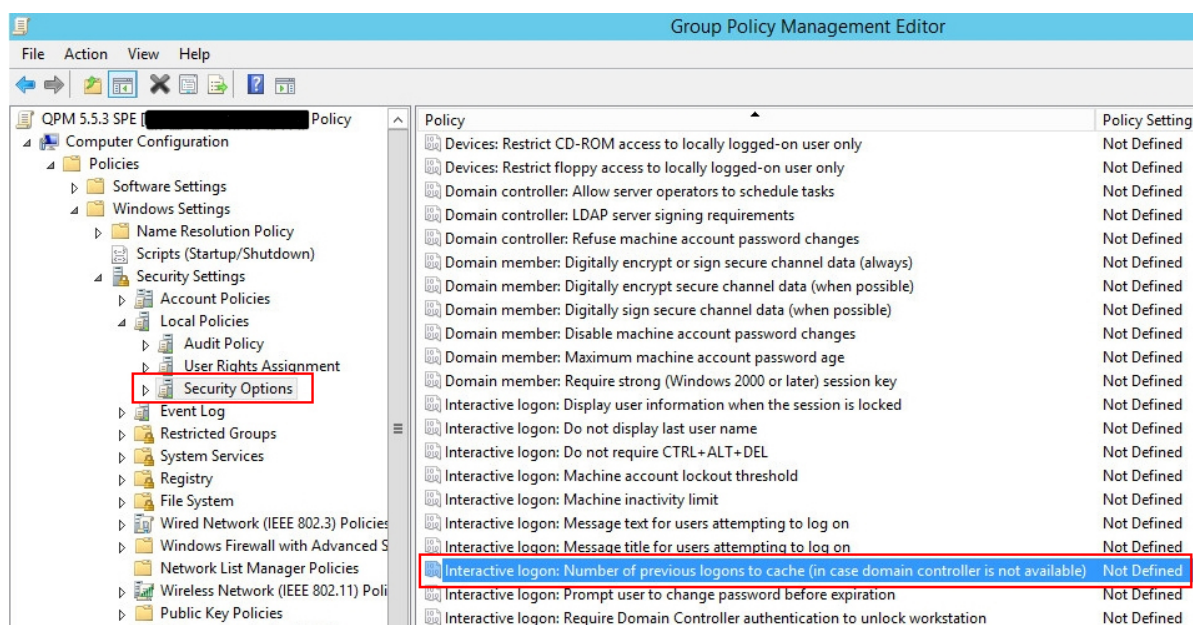
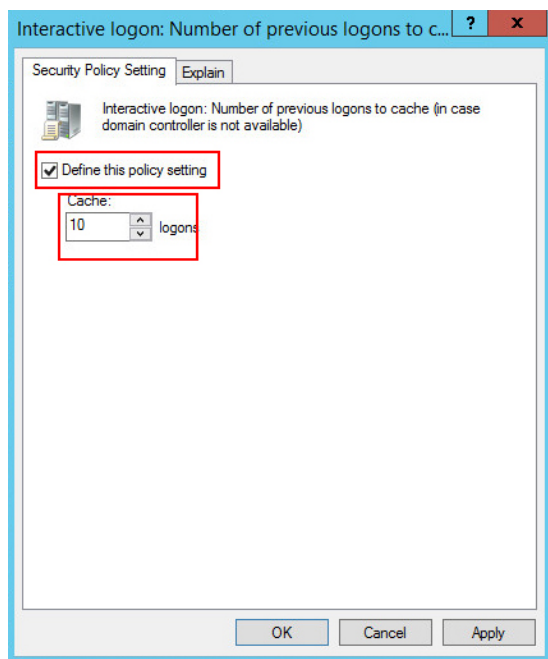


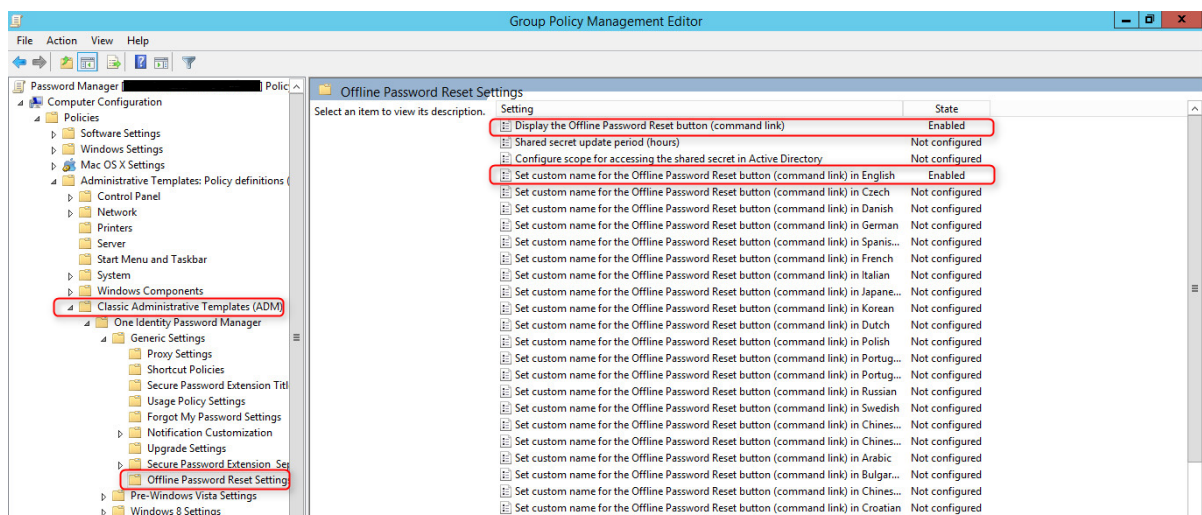
Figure 4:



3. Use the administrative template **prm_gina.admx** to turn on the offline password reset functionality. The administrative template file is located in the **\Password Manager\Setup\Administrative Template** folder of the installation CD. In the template, enable the following settings:

- Display the Offline Password Reset button (command link)
- Set custom name for the Offline Password Reset button (command link) in <Language>”

Figure 5:



4. Use the **Reset password in Active Directory** activity in a required workflow and select the **Allow users to reset passwords offline** option.

Figure 6:

Home > Default Management Policy > Forgot My Password

Forgot My Password Workflow

Drag activities from the left pane to the right to include activities in the workflow.

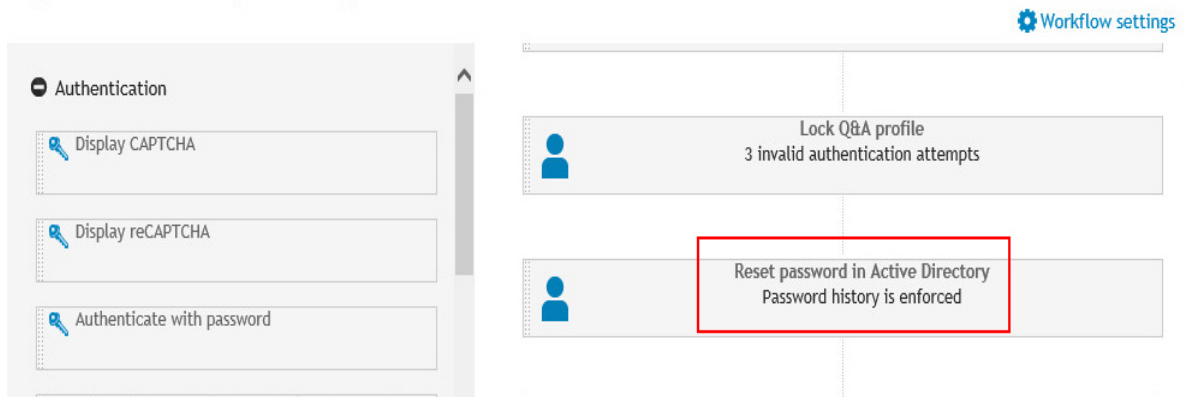
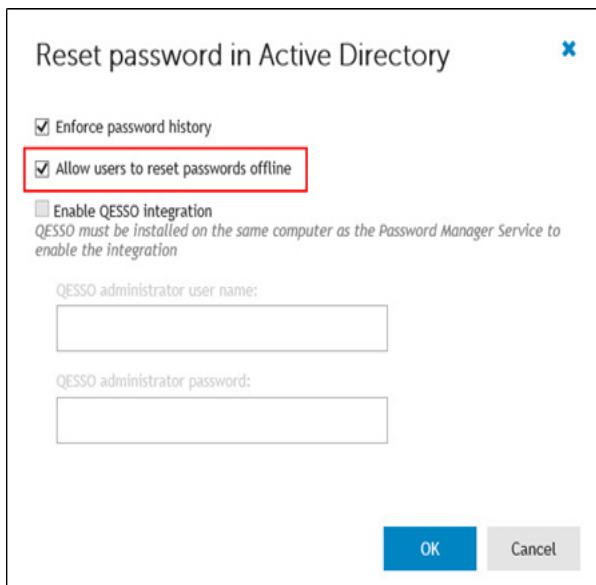


Figure 7:



5. Save the workflow.

To provide authentication during the offline password reset procedure, a shared secret is used. The shared secret is stored locally on the user's computer and its copy is published in Active Directory in the computer's account during the first logon if the computer is connected to the domain. By default, only domain administrators and the

computer account have access to the shared secret. You can specify other users and groups who will have the permission to read the shared secret from the domain. To do this, use the **Configure scope for accessing the shared secret in Active Directory** setting in the administrative template.

Password Policy Manager

Overview

In addition to providing the ability to manage user passwords, Password Manager also provides the ability to configure Password Policies similar to native Password Policies and Windows Fine-Grained Password Policies found in Active Directory. Password Manager Password policies can provide restrictions such as password length, dictionary lookup and history.

The Password Policies are stored in Group Policy Objects (GPOs) and are applied by linking the GPO to a target container defined in Active Directory, such as an Organizational Unit or group.

Password Policy Manager (PPM) is an optional and independently deployed component of Password Manager. The Password Policy Manager component is necessary to enforce password policies configured in Password Manager in instances when users change their passwords using tools other than Password Manager. To enforce password policies which you define with Password Manager, you must deploy Password Policy Manager on all Domain Controllers (DCs) in a managed domain.

How it Works

When a user changes a password in Password Manager, the new password is checked right away, and if it complies with password policies configured in Password Manager, the new password is accepted.

When a user changes a password outside of Password Manager, such as pressing CTRL+ALT+DELETE, the new password will not be checked immediately by Password Manager. The password's compliance with password policy rules will be checked on a Domain Controller. This is why Password Policy Manager must be installed on all Domain Controllers in a managed domain. If Password Policy Manager is not installed, in this case when the user changes password not in Password Manager, password policies configured in Password Manager will be ignored.

Password Policy Manager extends the default password policy settings and allows configuring policy scopes for each policy, so that only specified Organizational Units and groups are affected by the policy.

Password policy settings are stored as Group Policy Objects. Password Policy Manager creates new GPOs, and it does not change any existing GPOs.

Depending on whether a Domain Controller is running an x86 or x64 version of Microsoft Windows Server operating system, the appropriate version of Password Policy Manager must be installed.

NOTE: Password Policy Manager does not override the native Windows security policy rules, rather the more restrictive of the two rules will be enforced. So if both Password Manager and the Windows Password policy have minimum length requirements and they are not the same, then the more restrictive of the two will be enforced. Password Manager does not overwrite or exclude the native default Windows policies. If you don't want those in place, you will need to disable them.

Installing Password Policy Manager

Password Policy Manager is deployed on all Domain Controllers (DC) via the Group Policy. You can create a new Group Policy Object (GPO) or use an existing one to assign the Password Policy Manager installation package to the destination computers. Password Policy Manager is then installed on computers on which the GPO applies.

The installation package is located in the `\Password Manager\Setup` folder of the ISO image or the extracted installation archive, and has the following file name:

`PasswordPolicyManager_x64.msi`

Settings Controlled by the Password Policy

- **Password Age Rule:** Ensures that users cannot use expired passwords or change their passwords too frequently.
- **Length Rule:** Ensures that passwords contain the required number of characters.
- **Complexity Rule:** Ensures that passwords meet minimum complexity requirements.
- **Required Characters Rule:** Ensures that passwords contain certain character categories.
- **Disallowed Characters Rule:** Rejects passwords that contain certain character categories.
- **Sequence Rule:** Rejects passwords that contain more repeated characters than it is allowed.

- **User Properties Rule:** Rejects passwords that contain part of a user account property value.
- **Dictionary Rule:** Rejects passwords that match dictionary words or their parts.
- **Symmetry Rule:** Ensures that password or its part does not read the same in both directions.
- **Custom Rule:** Use this rule to display the custom policy rule message for users when other policy rules cannot be read or to hide the configured policy rules.

Configuring rules for a Password Policy

To configure rules for a password policy:

1. On the home page of the Administration site, click the **Password Policies** tab
2. Under the **Password Policies for Managed Domains** tab, click **Add domain connection**
3. If you already have a Domain Connection configured (such as for User and Helpdesk scopes), click **Use this connection**
4. Click **One Identity password policies are not configured**
5. Click **Add new password policy**
6. Enter an appropriate policy name when prompted
7. Click **Edit** and configure the required settings under the **Policy Rules** tab
8. Click **Policy Scope** tab
9. Click **Add** in both the **Organizational Units** and **Groups** options to link the Policy to the appropriate Organizational Unit and corresponding Group.

NOTE: You must select both or the policy will not be applied to users. The options set here are exactly as you would see the Link option in the native **Microsoft Group Policy Management Console** (GPMC.msc) MMC Snap-In.
10. Once the Policy Rules are configured and the Policy is linked, click the **Policy Settings** tab and un-check the **Disable this policy** feature to enable the policy
11. Click **Save**

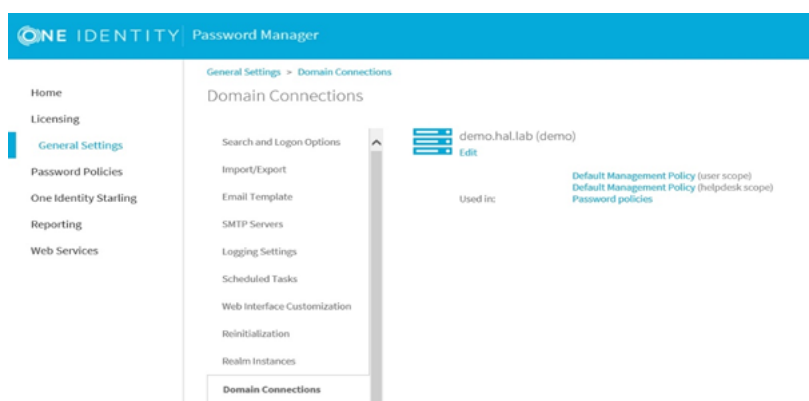
Configuration

The following are the common configuration recommendations:

- Use the same Domain Connection for User Scope, Helpdesk Scope and Password Policy settings.

Example:

Figure 8:



- When adding in a User Scope, choose **Use this connection** if you already have a connection to that Domain.

Example:

Figure 9:

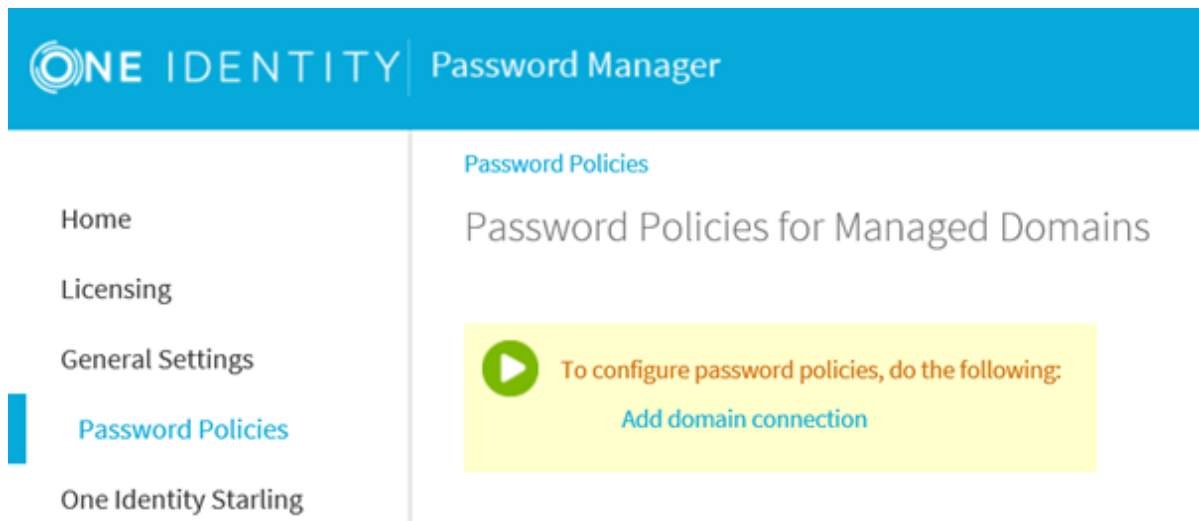
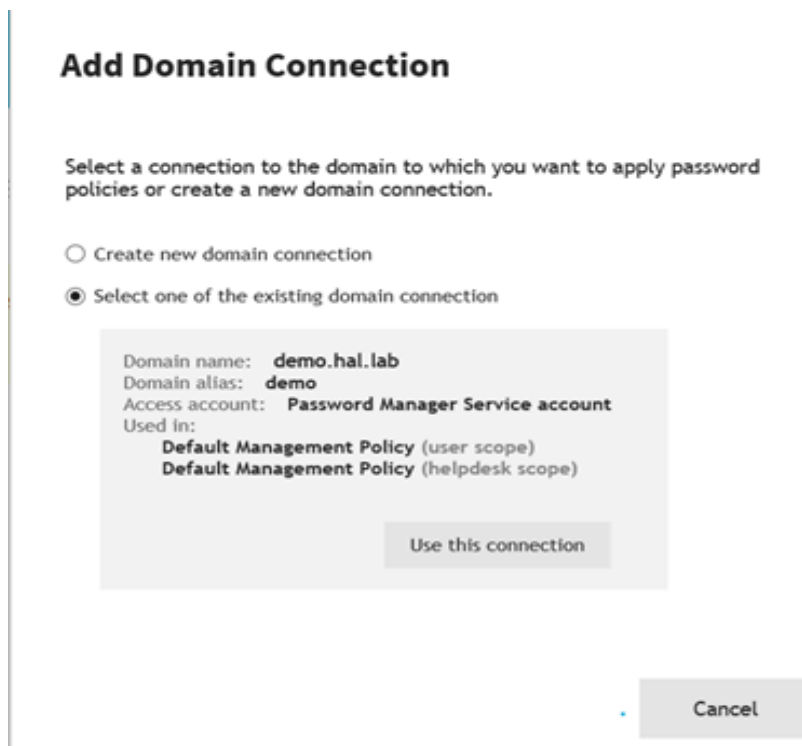


Figure 10:



Why?

The duplicate entries increase the size of the Shared.storage file, which in turn gets replicated to Active Directory, which will increase network traffic with a larger replicated data size. The duplicate entries also cause numerous duplicate connections with the Scheduled Tasks and thus increases the time it takes to complete each Scheduled Task.

For example, if you have a total of 20 Management Scopes, you should only have 20 Domain Connections. If you were to select Add domain connection for every User Scope, Helpdesk Scope and Password Policy setting you would have 60 total Domain Connections.

- It is not possible to use Optional questions to authenticate for the Helpdesk site. Only Mandatory and Helpdesk questions can be used
- It is recommended to use a Helpdesk question as the Helpdesk staff can see the answers which allows the Helpdesk staff to authenticate the user
- To pre-populate and pre-register users, use the Bulk Import Wizard. Please follow solution 128944:

<https://support.oneidentity.com/password-manager/kb/128944>

Common Sample Questions

- What is the name of the street where you first lived?
- What is your favorite movie?
- What is your Mother's maiden name?
- What year (YYYY) was your Mother born?
- What is your Father's middle name?
- What year (YYYY) was your Father born?
- What is the year (YYYY) of your first car?
- What is the make of your first car?
- What is the model of your first car?
- What was your first hire date with XXXXX (company name)?
- What is your employee number with XXXXX (company name)?
- Where is your favorite vacation location?
- What is the name of your first child?
- What is the name of your oldest niece?
- What is the name of your first employer?
- What is your favorite hobby?
- What is your paternal grandfather's first name?
- What is your paternal grandmother's first name?
- In what city was your mother born? (Enter full name of city only)
- In what city was your father born? (Enter full name of city only)
- In what city was your high school? (Enter only "Charlotte" for Charlotte High School)
- Where did you meet your spouse for the first time? (Enter full name of city only)
- What was the name of your first pet?

- In what year (YYYY) did you graduate from high school?
- Who is your favorite childhood superhero?

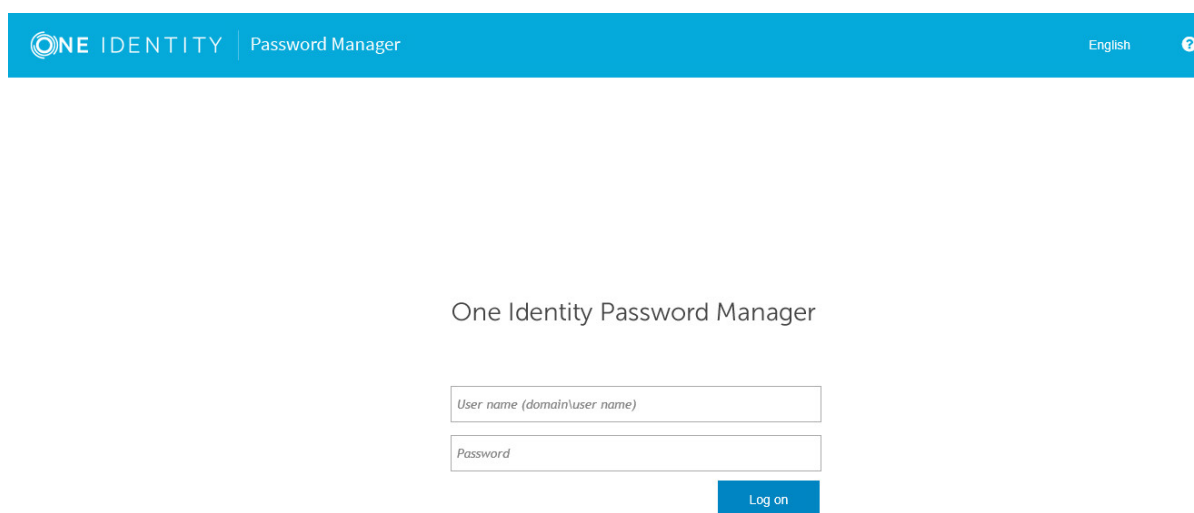
Helpdesk scope and options

The Helpdesk site handles typical tasks performed by Helpdesk operators, such as resetting passwords, unlocking user accounts, assigning temporary passcodes, and managing users' Questions and Answers profiles.

The Helpdesk site can be installed either on the same server as the Administration Site and Password Manager service, or on a stand-alone server.

The Helpdesk site uses a form-based authentication which prompts users to logon:

Figure 11:



ONE IDENTITY | Password Manager English ?

One Identity Password Manager

User name (domain\user name)

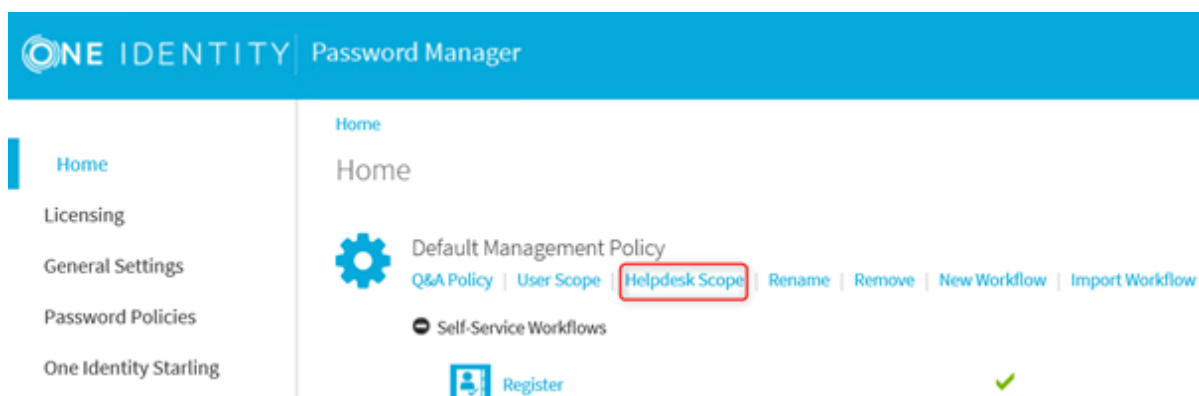
Password

Log on

Password Manager allows a Helpdesk group to be added for each Management Scope. If you require different Helpdesk groups to be able to administer different scopes of users, additional Management Scopes will have to be created to accommodate the restrictions for the Helpdesk groups.

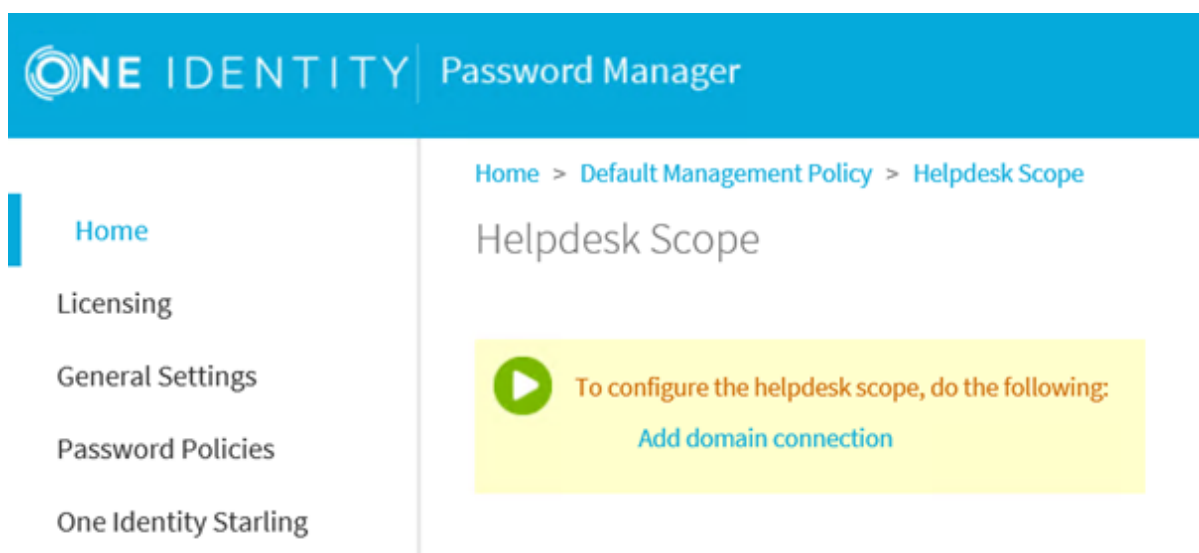
The Scope of who can logon to the Helpdesk site can be configured in the Admin site for each Management Policy:

Figure 12:



To select the Groups who can access the Helpdesk site, first click Helpdesk Scope, then click Add domain connection.

Figure 13:



If you already have a Domain connection, select **Use this connection:**

Figure 14:

Add Domain Connection

Select a connection to the domain to which you want to apply password policies or create a new domain connection.

☐ Create new domain connection

☒ Select one of the existing domain connection

Domain name: **demo.hal.lab**

Domain alias: **demo**

Access account: **Password Manager Service account**

Used in:

- Default Management Policy (user scope)**
- Default Management Policy (helpdesk scope)**

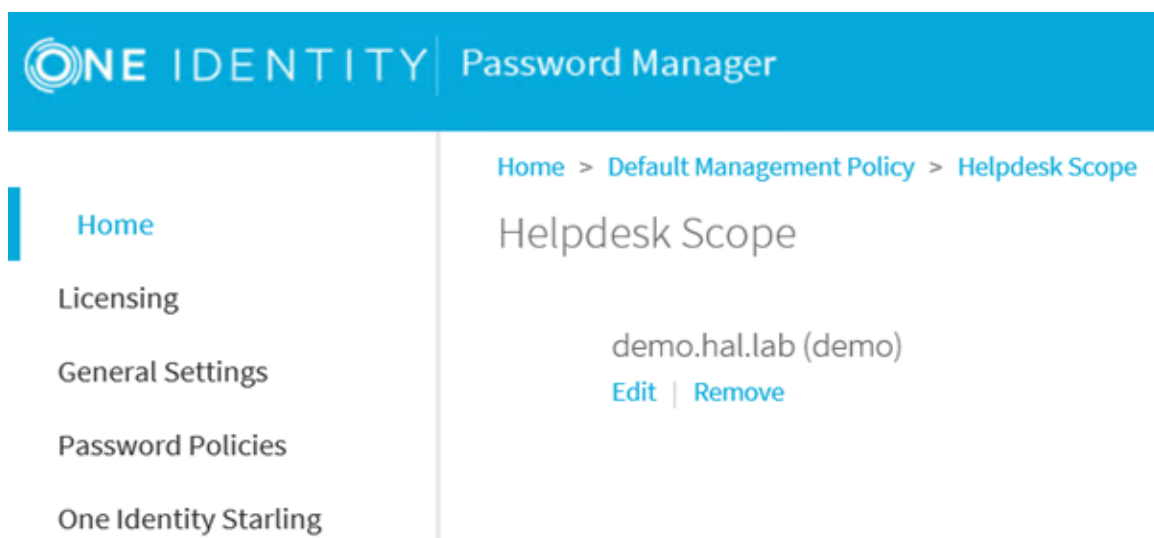
Use this connection

Cancel

If you do not see the desired Domain Connection, click **Add domain connection** and enter the required information.

Once the Domain has been added, select **Edit**:

Figure 15:



Add in the Groups to be allowed access to the Helpdesk site and perform Helpdesk actions.

Reinitialization

Password Manager has the ability to change the configuration options, such as the encryption level and the attribute used to store Users' Q&A Profile settings without the need to reinstall or modify configuration files.

If you choose to perform a Reinitialization, please keep the following in mind:

When changing the Encryption algorithm within the **PMAAdmin site | General settings | Reinitialization section** the following message occurs:

 **WARNING:** You are changing configuration and security settings. To prevent users from losing their Q&A profiles use the Migration Wizard to update the profiles.

What are the next steps?

1. Once the setting has been changed select **Save**
2. Provide a password to the new configuration file
3. Select **Export** (do not click Save yet)
4. Click **Save** after the Export is complete or it will not work
5. Launch the **Migration Wizard** found in the Password Manager Autorun and select: **Update users' Q&A profiles with new instance settings** and follow the wizard

Reports

Reporting is an optional component. The Reports section of the Admin site includes a number of pre-defined reports that help you perform the following tasks:

- Track user registration activity
- Analyze information about what actions are performed by users in Password Manager
- Check users' registration status
- View a list of users whose Questions and Answers profiles must be updated to comply with the current administrator-defined settings
- Track helpdesk operators' activity

To use Password Manager Reports, you need to connect to a Microsoft SQL Server and a Microsoft Reporting Service Server (SSRS).

To use the **User Action History** functionality, you need to connect to an SQL Server only.

NOTE: When a user registers with Password Manager, the Q&A profile information is stored within the user object in Active Directory. Reporting only allows the ability to query user statistic information and does not store the profile data in the database.

If you choose to take advantage of the Password Manager reports, the following is required:

- Microsoft SQL Reporting Services (SSRS) must be installed and configured
 - Please note that if the SQL Server service and SSRS are on different hosts, you may encounter a "Double-Hop" authentication issue. Please see this article for more information:

<https://support.oneidentity.com/password-manager/kb/69693>

- The Password Manager service account must have sufficient permissions to create and write to a database on the SQL server

NOTE: You cannot pre-create the database. Password Manager must create it.

- The Password Manager service account must have sufficient permission to publish reports on the SSRS server.

How to configure reports

To configure Reports, complete the following:

1. Navigate to the Password Manager Admin site
2. Click the **Reports** tab
3. Select **Edit Connections**
4. Enter the name of the SQL Server
5. Provide the name of the database the Password Manager will create
6. Provide the name of the account that will create the database server.

NOTE: This account must have the DB Creator role.

7. Click **Next**
8. Enter the Report Server URL which can be obtained from the SQL Reporting Service Configuration Manager (on the SQL Reporting Services server)
9. Enter the Report Manager URL.
10. Click **OK**.
11. The Reports are now configured. However, in order to populate the data the Scheduled Tasks found under the General Settings tab must be run.

Please also refer to Video Solution 106401 which demonstrates how to configure Reports in Password Manager:

<https://support.oneidentity.com/password-manager/kb/106401>

Can you use a report database from a previous version of Password Manager?

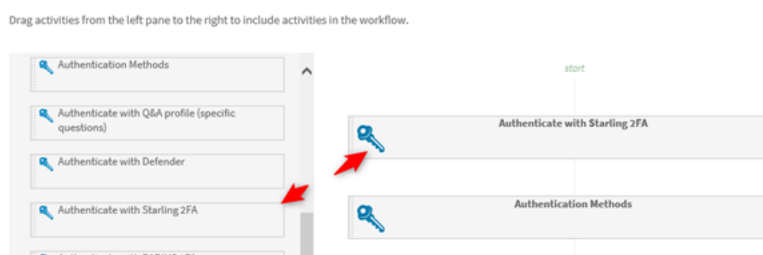
A database created in Password Manager version 5.7.1 or later can be used when upgrading to 5.9.7.

Starling 2FA

To add Starling 2FA in Password Manager, perform the following:

1. In the PMAdmin site, navigate to **Settings | One Identity Starling**
2. Click **Join to Starling** button
3. Follow the prompts to authenticate your Starling account or alternatively sign up for Starling 2FA if you do not have an account.
4. Once you have joined to Starling you will see confirmation and the option to Unjoin Starling
5. Now that Starling 2FA is configured you can add the option to authenticate with Starling 2FA in any workflow such as this:

Figure 16:



For full configuration details please refer to the following video demonstration:

<https://support.oneidentity.com/kb/255662>.

Customizations

You can now create custom activities and workflows in Password Manager. An embedded user interface designer allows you to easily create user interface for your custom activities. You can also convert any built-in activity to custom and modify its behavior by PowerShell scripts. The import/export functionality enables you to share custom activities and workflows with Password Manager instances outside of the replication group. This feature requires PSO assistance and is not covered by the technical support.

For PSO assistance, please contact your Account Manager or Sales Representative.

Customization tool

The Customization Tool available for 5.7.1, 5.8.x, and 5.9.x can be downloaded here:

<https://support.oneidentity.com/password-manager/kb/254176>.

Troubleshooting

After you upgrade, there is a possibility that the **Local.storage** file changes the value of "role" from "Primary" to "Secondary" if it detects any existing Service Connection Points in Active Directory.

This issue can happen in these scenarios: One Identity Password Manager

1. If you have an old Service Connection Point from a previous version (such as 4.7 or 5.0.3) and it was not cleaned up/removed from Active Directory
2. If you have more than one Password Manager server instance in the same domain and you upgraded both. They may both default to "Secondary" as a precaution

Please keep in mind that if you have multiple Password Manager servers, one of these must be "Primary" and all others "Secondary" for the same domain (realm) instances.

If you fall into either of the aforementioned scenarios, please check the settings in the following file after you finish the overall upgrade process:

C:\ProgramData\One Identity\Password Manager\Local.storage

The setting is located near the top of the file:

```
<setting name="role" value="Secondary" />
```

Ensure only one Password Manager server has this setting:

```
<setting name="role" value="Primary" />
```

NOTE: If no servers are set to "Primary", designate one of your choosing and update it. After the file is updated and saved, restart the Password Manager service on that server only.

How to enable logging

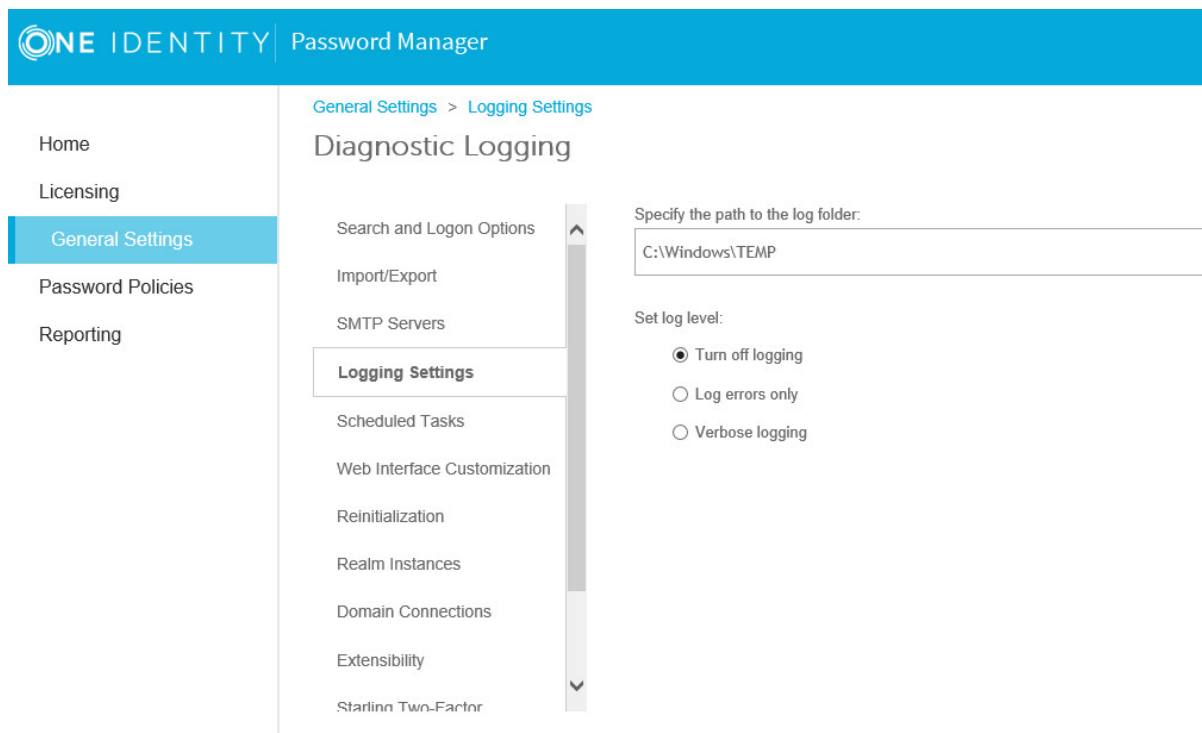
Logging is a valuable resource in troubleshooting issues with Password Manager. When working with One Identity Support, Verbose logging is required as it provides more details for troubleshooting issues.

CAUTION: One Identity does not provide support for problems that arise from improper modification of the registry. The Windows registry contains information critical to your computer and applications. Make sure you back up the registry before modifying it. For more information on the Windows Registry Editor and how to back up and restore it, refer to Microsoft Article ID 256986 "Description of the Microsoft Windows registry" at Microsoft Support: <http://support.microsoft.com/default.aspx?kbid=256986>.

To enable logging for Password Manager service

Navigate to the PMAAdmin site | General Settings | Logging Settings:

Figure 17:



The log files created on the Password Manager server are called:

- QPM.Service.Host_****-**-**.log
- QPM.UI.Admin.MVC_****-**-**.log
- QPM.UI.User.MVC_****-**-**.log

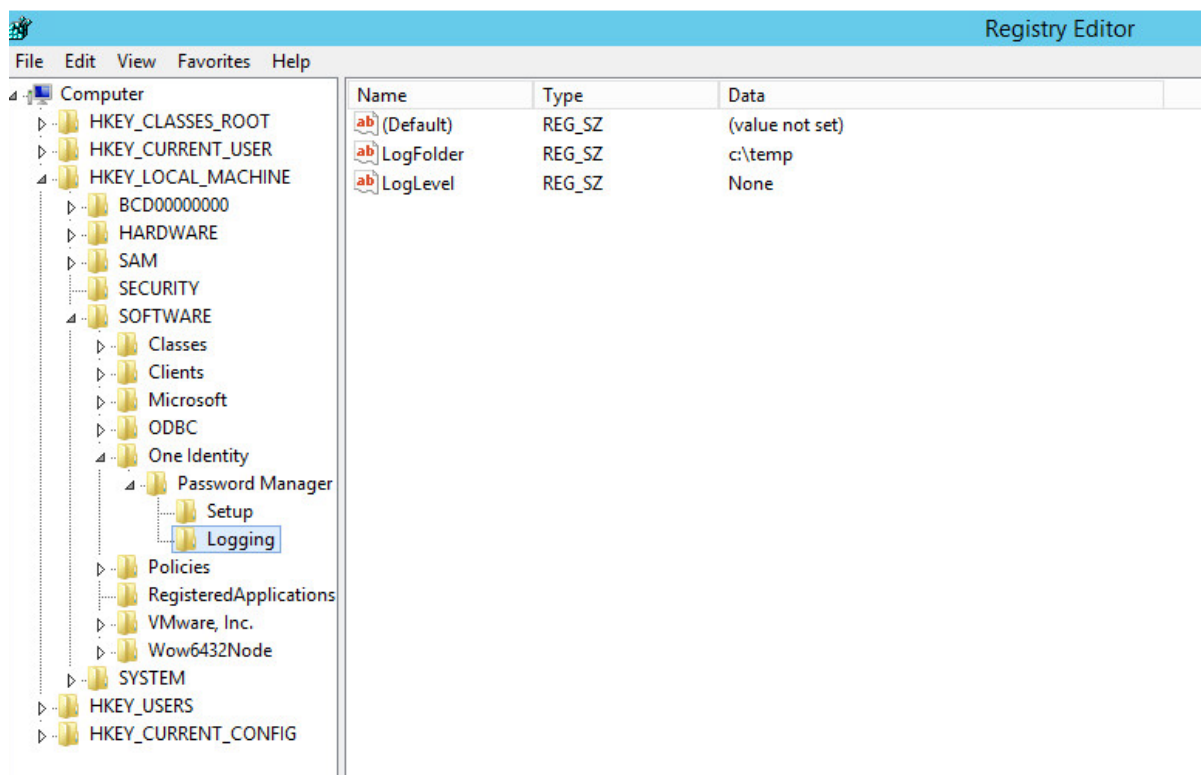
To enable logging for a stand-alone server

To enable logging for stand-alone (aka DMZ) instances hosting only the Self Service site, follow these steps:

Under HKEY_LOCAL_MACHINE\Software\One Identity\Password Manager, create the following string and DWORD (32-bit) values respectively:

- LogFolder** and set the "Value data" to **C:** (You can specify any location/folder, but the folder needs to be created beforehand)
- LogLevel** and set the "Value data" to **All**

Figure 18:



To enable logging for the Secure Password Extension (SPE)

The following registry key will enable/disable logging for the SPE:

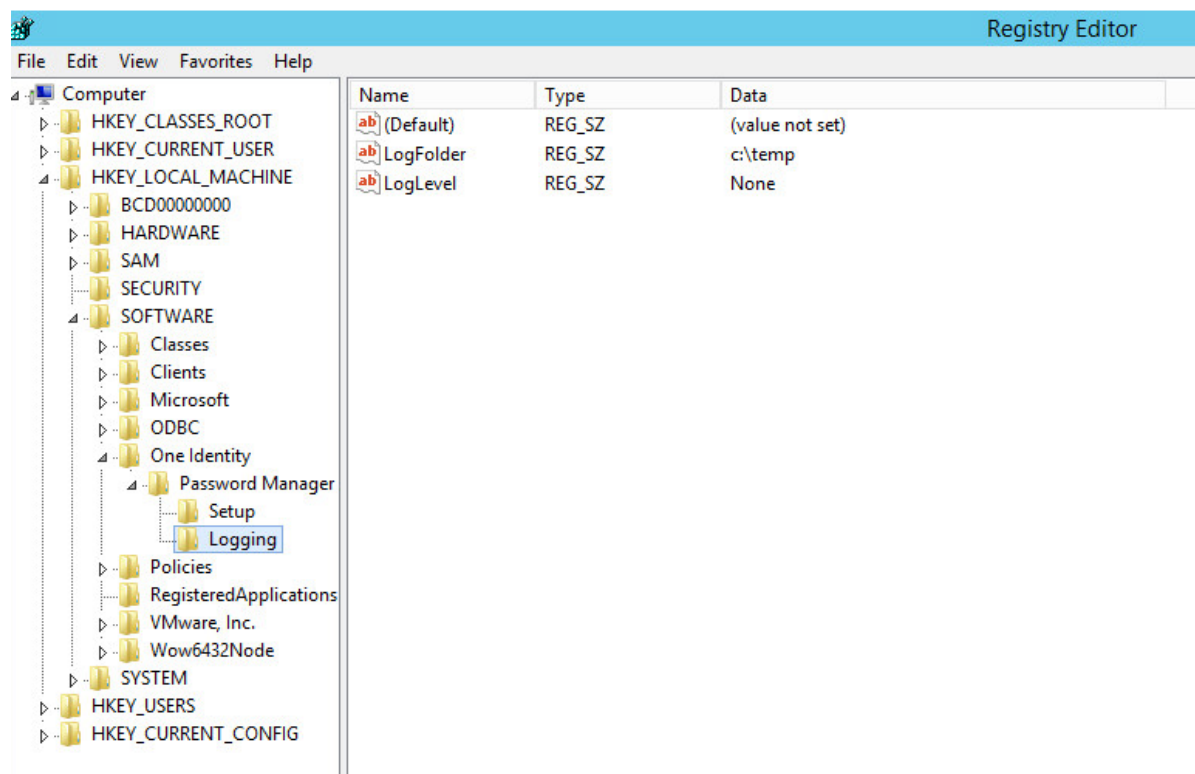
HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging

NOTE: If the keys Password Manager\Logging do not exist please create them.

Under **Password Manager\Logging** create the following strings:

- **LogFolder** with a value of **C:**
- **LogLevel** with a value of **All**

Figure 19:



Once you are done gathering the logs, either delete the two new string values or change **LogLevel** to a value of **None**. Failure to disable logging afterwards can result in the server's hard drive becoming full and disrupting all services for the server.

The logfiles generated will be **QPM_SPE.log** and **QPM_SPEenroll.log** (for all versions).

To enable Password Policy Manager (PPM) logging:

If it does not already exist, create the following key in the local registry of one of the affected Domain Controllers (DCs):

HKEY_LOCAL_MACHINE\Software\One Identity\Password Manager\Logging

Under HKEY_LOCAL_MACHINE\Software\One Identity\Password Manager, create the following string and DWORD (32-bit) values respectively:

1. **LogFolder** and set the "Value data" to **C:** (You can specify any location/folder, but the folder needs to be created beforehand)
2. **LogLevel** and set the "Value data" to **ffffffff** (8 **F**'s in Hexadecimal)

3. Restart the Domain Controller
4. Reproduce the experienced issue
5. Once you are done gathering the logs, either delete the two new string values or change LogLevel to a value of None. Failure to disable logging afterwards can result in the server's hard drive becoming full and disrupting all services for the server.

The logfile generated will be **QPM.PPMgr_XXXX-XX-XX.log**

Common solutions

- SSL Certificate is Invalid:
<https://support.oneidentity.com/password-manager/kb/85083>
- User Status Statistics errors:
<https://support.oneidentity.com/password-manager/kb/129522>
<https://support.oneidentity.com/password-manager/kb/135020>
- SSL options:
<https://support.oneidentity.com/password-manager/kb/88265>
- Expired certificate:
<https://support.oneidentity.com/password-manager/kb/134732>

How to move the Password Manager database

Password Manager uses the database to store user information for statistics and reporting. This is assuming that the database will move to another SQL Server with a new instance of SQL Reporting Services.

How to move the Password Manager Database:

1. Open **SQL Management Studio** on the existing SQL Server and detach the database
2. Move the Database files to the new SQL Server (both the MDF and LDF files are required)
3. Attach to the database on the new SQL Server
4. Open the Password Manager Admin site and browse to the **Reports** tab
5. Select **Edit Connection** and follow the Wizard inputting the new server name and credentials to re-attach the database and to redeploy the SQL Reporting Services Reports to the new SQL Reporting Services Server.

Also see Solution 87872:

<https://support.oneidentity.com/password-manager/kb/87872>

Changing the Password Manager service account

Password Manager has two main sections where a password must be changed. The Password Manager service and the Application Pool identity.

- 1 **NOTE:** If you want to modify the service account after installing Password Manager 5.9.7, you cannot modify it by changing the account on Password Manager service because the new account will not be able to read the current configuration.

To modify the service account after installing Password Manager 5.9.7:

1. On the menu bar, click **General Settings**, then click the **Import/Export** tab and export the configuration file of the primary instance of Password Manager.
 - 1 **NOTE:** Due to security enhancements, a complex password is generated while exporting the configuration. You must remember the password or store it in a secure place, to use while importing the configuration.
2. Stop the Password Manager Service.
3. At the command prompt, type **services.msc** and select **Password Manager Service** in the console and change the log on details.
4. Start the Password Manager Service.
 - 1 **NOTE:** Before you continue, it is recommended to back up the **One Identity** folder at **C:\ProgramData**.
5. Delete the One Identity folder at C:\ProgramData.
6. Restart the computer.
7. Open the Administration site.
8. On the **Instance Initialization** page, select **Unique instance** and click **Save**. On the menu bar, click **General Settings**, then click the **Import/Export** tab and import the configuration file, which was exported before changing the service account.

To change the Password Manager Application Pool account:

1. Launch IIS (Internet Information Server)
2. Select **Application Pools**
3. Right-click **PMAdmin**
4. Select **Advanced settings**
5. Select **Identity**
6. Within the Application Pool identity select **"Set..."**
7. Then set the new credentials

8. Restart the application pool to make sure it starts
9. Repeat Steps 4-8 for the Helpdesk and Self-Service Application pools

Workflow design considerations

A Workflow is the set of options available to Users and Helpdesk staff on the Self Service and Helpdesk sites. Each of these options are also comprised of various actions that will be performed. For instance, if a user chooses **Forgot My Password**, you can add in options to authenticate the user using the Question and Answer profiles and send an email upon completion.

Each Workflow contains specific user scopes to which the Workflow will be applied. As such, it is recommended to keep the number of Workflows to a minimum. For instance, if you have two domains but the rules are the same for each, you can simply add in both domains for the Workflow.

When to use one Workflow

- Same Question & Answer profiles for all users in all Domains
- Same email notification requirements (languages, logos, same text)

Benefit:

- Reduced administrative overhead (less items to update – i.e. email templates)
- Reduced size of the Shared.storage file which contains all Q&A profile settings, including all associated Questions, Email templates and additional language additions

Drawback:

- Cannot provide different requirements for exception users/groups (i.e. separate requirements for service accounts)

When to use separate workflows

- Different Q & A profile requirements for different groups of users (i.e. one for Users, one for Admins)
- Different email notification requirements (languages, logos, different text)

- Different Helpdesk Scope requirements
 - i.e. Helpdesk "Group A" can only reset passwords for normal users while Helpdesk "Group B" can reset passwords for administrators

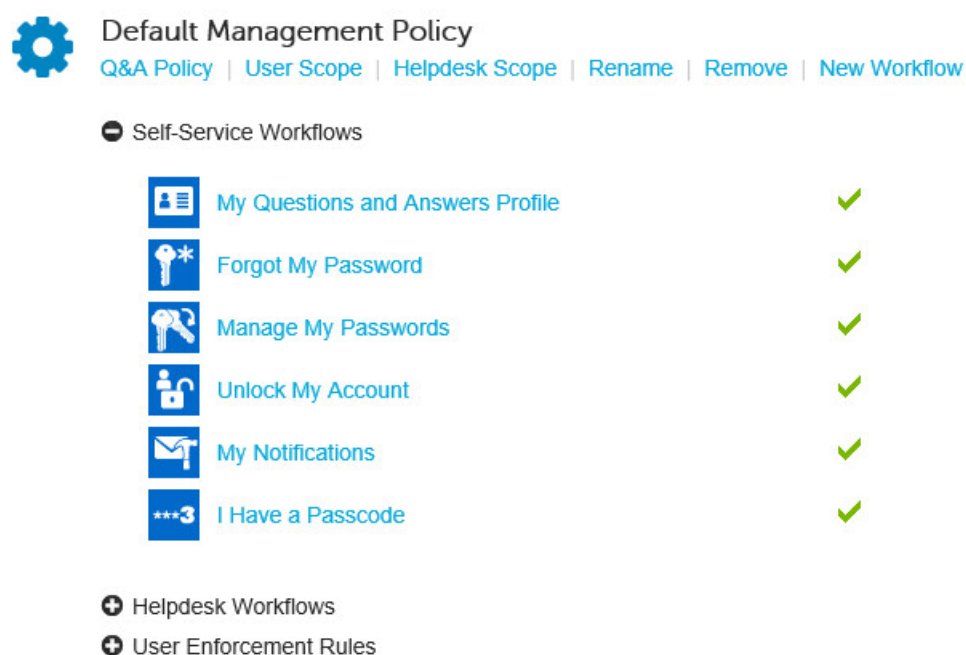
Benefit:

- Ability to provide different requirements for different subsets of users

Drawback:

Increased **Shared.storage** file leading to increased memory usage of the Password Manager Service process and increased size of the corresponding **QPMStorageContainer** AD account which in turn will increase replication traffic due to the size of the user account

Figure 20:



Summary

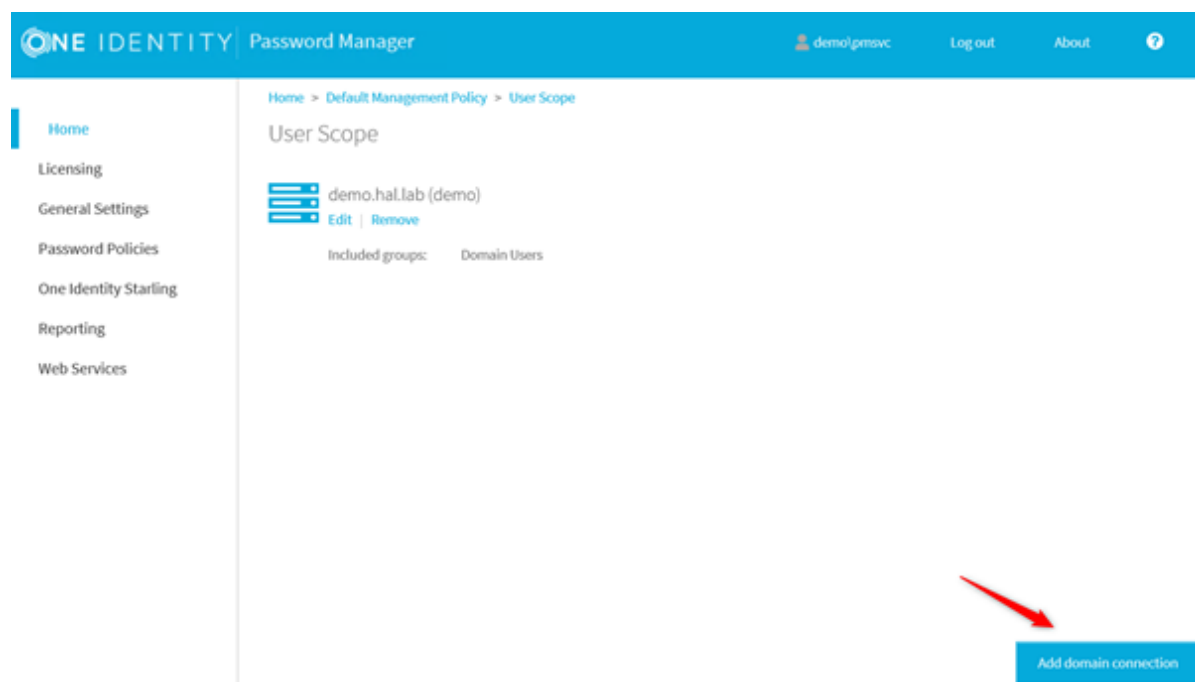
If possible, keep the number of Workflows and associated customizations within each to an absolute minimum. The more you add, the larger the **Shared.storage** file grows and in

turn causes more memory usage for the Password Manager Service process and increased replication traffic in Active Directory.

Notes

If you are going to use the same Workflow for all domains, you can easily add in the required domain in the User Scope section:

Figure 21:



This will apply the Workflow settings to users within all Domains listed and the corresponding groups that you select in each respective Domain.

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