



Password Manager 5.16

Administration Guide (AD LDS
Edition)

Copyright 2026 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 website (<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/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Password Manager Administration Guide (AD LDS Edition)
Updated - 02 March 2026, 10:27

For the most recent documents and product information, see [Online product documentation](#).

Contents

About Password Manager	1
About Password Manager for AD LDS	1
Getting Started	3
Different sites for Different roles	3
Password Manager for AD LDS components	3
Licensing	4
Installing the license for Password Manager for AD LDS	6
Updating the license	10
Telephone verification feature license	11
Installing Password Manager: Checklist	11
Installing Password Manager for AD LDS	12
Configuring Password Manager Service Account and Application Pool Identity	13
Enabling HTTPS	13
Installing Password Manager for AD LDS	14
Extending AD LDS Schema	15
Initializing a Password Manager for AD LDS instance	16
Installing the Password Manager for AD LDS Self-Service Site and Helpdesk Site on a standalone server	18
FailSafe support in Password Manager	20
Installing multiple instances of Password Manager for AD LDS	21
Specifying custom certificates for authentication and traffic encryption	22
Step 1: Obtain and install custom certificates from a trusted Windows-based certification authority	23
Step 2: Providing certificate issued for the server computer of the Password Manager Workflow Service	24
Step 3: Providing the certificate issued for the client computers of the Self-Service and Helpdesk Sites	25
Password Manager Architecture	26
Password Manager Components and Third-Party Solutions	26
Password Manager Service, Workflow Service and Administration Site	27
Self-Service Site	28
Helpdesk Site	28

TeleSign	29
SQL Server Database and SQL Server Reporting Services	29
Defender	29
Password Manager Secure Token Server	30
RADIUS Two-Factor Authentication	33
Redistributable Secret Management Service	34
Location sensitive authentication	34
Working with Power BI templates	35
Password Manager Credential Checker	36
Typical Deployment Scenarios	37
Simple deployment	37
Deployment of the Password Manager for AD LDS Self-Service and Helpdesk Sites on standalone servers	38
Realm deployment	39
Multiple Realm Deployment	40
Password Manager for AD LDS in a perimeter network	40
Installing Password Manager for AD LDS in a perimeter network with reverse proxy	41
Management Policy Overview	42
Management Policy components	42
Management Policy and other Password Manager settings	43
Password Policy Overview	43
reCAPTCHA Overview	44
How it works	44
How to Use reCAPTCHA on Password Manager Sites	45
System Requirements for Using reCAPTCHA	46
References	46
User Enrollment Process Overview	46
Questions and Answers Policy Overview	47
Q&A Policy and Authentication	47
Q&A Policy and User Enforcement	48
Data Replication	49
Storing Data	49
Replicating data	49
Changing replication settings	50
Phone-based authentication service overview	51

About phone-based authentication in Password Manager for AD LDS	52
Using phone-based authentication in Password Manager for AD LDS	53
Configuring phone-based authentication for Password Manager for AD LDS	54
Configuring Management Policy	55
Configuring Permissions for Access Account	55
Connecting to AD LDS Instance	56
Changing Access Account	58
Removing Connection to AD LDS Instance	59
Adding Secret Questions	59
Editing and Deleting secret questions	60
Management Policies	62
Checklist: Configuring Password Manager	62
Understanding Management Policies	63
Adding or cloning a new Management Policy	64
Configuring Access to the Administration Site	65
Configuring Access to the Password Manager Self-Service Site	65
Configuring Access to the Helpdesk Site	65
Changing Access Account	67
Removing Connection to AD LDS Instance	68
Configuring Questions and Answers Policy	68
Creating Secret Questions	68
Editing and Deleting secret questions	71
Configuring Q&A Profile Settings	72
Workflow overview	74
Workflow structure	74
Workflow states	75
Workflow settings	76
Custom workflows	80
Importing and exporting workflows	80
Custom Activities	82
Custom activity settings in Password Manager for AD LDS	82
Creating custom activities	83
Importing and exporting custom activities	84
Removing Custom Activities	85
Password Manager Self-Service Site workflows	85

Register	86
Configuring country code drop-down menu	87
Manage My Profile	87
Forgot My Password	87
Manage My Passwords	88
Unlock My Account	88
My Notifications	89
I Have a Passcode	89
Overview of built-in Password Manager Self-Service Site activities	89
Authentication activities	90
Action activities	101
Notification activities	106
Helpdesk Workflows	110
Verify User Identity	110
Assign Passcode	111
Reset Password	111
Unlock Account	111
Unlock Profile	112
Enforce Update of Profile	112
Overview of Built-in Helpdesk Activities	112
Authentication Activities	113
Action Activities	118
Notification Activities	121
User Enforcement Rules	123
Invite Users to Create/Update Profiles	123
Remind Users to Create/Update Profiles	126
Remind Users to Change Password	128
General Settings	131
General Settings Overview	131
Search and Logon Options	132
Configuring Search Options for the Self-Service Site	132
Partial user search on external network	134
Configuring CAPTCHA or reCAPTCHA for the Find Your Account page	135
Configuring Search Options for the Helpdesk Site	136
Configuring Security Settings	137

Hiding the domain user name on the Self-Service Site	137
Hiding personally identifiable information for logged-in users	138
Creating a custom pattern from AD attributes to show on the Self-Service Site	139
Applying regular expression on UPN or username	140
Configuring anti-bot security settings	140
Import/Export Configuration Settings	145
Exporting Configuration Settings	145
Importing Configuration Settings	146
Outgoing Mail Servers	147
Diagnostic Logging	148
Scheduled Tasks	149
Invitation to Create/Update Profile Task	149
Reminder to Create/Update Profile Task	150
Reminder to Change Password Task	151
Retry Failed Auditing Messages task	152
Maximum Password Age Policy Task	153
Update RADIUS server status	154
User Status Statistics Task	155
Clear Old Records from Reporting Database	156
Web Interface Customization	156
Instance Reinitialization	159
Modifying service connection settings	159
Modifying the advanced settings of instance reinitialization	161
Realm Instances	163
AD LDS Instance Connections	163
Using Connections to AD LDS Instances	163
Specifying Access Account for AD LDS Instance Connections	164
Changing Access Account for AD LDS Instance Connections	166
Removing Connection to AD LDS Instance	166
Enabling Password Manager for AD LDS extensibility features and troubleshooting mode	167
About Password Manager for AD LDS extensibility features	168
RADIUS Two-Factor Authentication	169
Internal Feedback	170
Customizing help link URL	170

Password Manager components and third-party applications	171
Password Manager Secure Token Server	171
Configuring Password Manager Secure Token Server	174
Unregistering users from Password Manager	175
Bulk Force Password Reset	176
Fido2 key management	177
Working with Redistributable Secret Management account	178
Redistributable Secret Management Service supported platforms	179
Customizing Redistributable Secret Management log path	181
Email templates	181
Upgrading Password Manager for AD LDS	183
Performing an in-place upgrade from an older Password Manager for AD LDS version to Password Manager for AD LDS 5.16	184
Upgrading Password Manager for AD LDS manually from an older version	185
Password Policies	187
About Password Policies	187
Creating a Password Policy	188
Managing Password Policy Scope	189
Applying Password Policies	190
Changing Policy Priority	192
Configuring Password Policy Rules	192
Password Compliance	193
Password Age Rule	194
Length Rule	195
Complexity Rule	195
Required Characters Rule	196
Disallowed Characters Rule	197
Sequence Rule	198
User Properties Rule	198
Symmetry Rule	200
Custom Rule	201
Deleting a Password Policy	201
Enable 2FA for Administrators and Enable 2FA for HelpDesk Users	203
Reporting	204

Reporting and User Action History Overview	204
Setting Up Reporting Environment	205
Using Password Manager for AD LDS reports	205
Browsing the User Action History	212
Managing Connections to SQL Server and Report Server	215
Best Practices for Configuring Reporting Services	215
Reporting Services Default Configuration	216
Reporting Services Firewall Issues	218
Accounts Used in Password Manager for AD LDS	219
The Password Manager Service Account	219
Application Pool Identity	219
Access Account for Application Directory Partition Connection	220
Appendix B: Open Communication Ports for Password Manager for AD LDS	222
Customization Options Overview	224
Customization of Steps in Password Manager Self-Service Site, and Helpdesk Tasks	224
Email Notification Customization	225
User Agreement Customization	225
Account Search Options Customization	226
Web Interface Customization	226
Customization of Password Policies List	226
Customization of Password Strength Meter	227
About us	229
Contacting us	229
Technical support resources	229

About Password Manager

About Password Manager for AD LDS

About Password Manager for AD LDS

Password Manager for AD LDS is a web-based application that provides an easy-to-implement and use, yet highly-secure password management solution.

- Administrators can use the Password Manager for AD LDS Administration Site to access a powerful and flexible password policy control mechanism to ensure that all passwords in the organization comply with the established policies.
- Helpdesk agents can use the Password Manager for AD LDS Helpdesk Site to support end-users in solving potential password management and access issues.
- End-users can use the Password Manager for AD LDS Self-Service Site to perform password self-management tasks, reducing the need for assistance from high-level administrators and helpdesk agents.

Password Manager for AD LDS also allows managing users that do not have AD LDS accounts. For example, using Password Manager for AD LDS, you can manage passwords for contractors and other external users as well.

The key features and benefits of Password Manager for AD LDS include:

- **Global access:** Password Manager for AD LDS provides constant access to the Self-Service Site from intranet computers as well as via Internet from any most common browser. The solution supports flexible access modes and login options.
- **Strong data encryption and secure communication:** The solution relies on industry-leading technologies for enhanced communication security and data encryption.
- **Web interface for helpdesk service:** Password Manager for AD LDS features a Helpdesk Site that allows administrators to delegate helpdesk tasks to dedicated operators. These tasks include resetting user passwords, managing the users' Questions and Answers Profiles and assigning temporary passcodes to users.

- **Password Policy Manager:** Password Policy Manager is an independent component of Password Manager for AD LDS that is used to enforce the password policies configured via Password Manager for AD LDS. This module must be installed on domain controllers (DCs) running a 64-bit Microsoft Windows Server operating system.
- **Email event notifications:** Administrators can configure event notifications that are sent by email to designated recipients when specified events occur.
- **Advanced domain management:** Password Manager for AD LDS is capable of managing domains across trust boundaries (no trust relationship required).
- **Powerful password policies:** Password Manager for AD LDS ensures that only passwords that meet administrator-defined policies are accepted. Unsuccessful authentication attempts are logged and the corresponding accounts are locked, if necessary.
- **Granular policy enforcement:** Password policies are applied on a per-group or per-Organizational Unit (OU) basis.
- **Questions and Answers authentication mechanism:** To reset passwords or unlock accounts, users are prompted to answer a series of questions for which they must provide their secret answers when registering with Password Manager for AD LDS.
- **Enhanced user name search options:** Users can view their account attributes, such as login name, first name, display name, or SMTP address when searching for their forgotten user names. More specific search queries return the most relevant search results.
- **Fault tolerance and scalability:** Password Manager for AD LDS is designed to work with network load balancing clusters and in web farm environments.

Getting Started

Different sites for Different roles

Password Manager for AD LDS components

Licensing

Installing Password Manager: Checklist

Installing Password Manager for AD LDS

Specifying custom certificates for authentication and traffic encryption

Different sites for Different roles

The Web Interface allows multiple websites to be installed with individual, customizable configurations. The following is a list of configuration templates that are available out-of-the box:

- **Administration Site:** is for individuals who are responsible for implementing password self-management through performing administrative tasks, such as configuring site-specific settings and enforcing password policies, to suit the specific needs of their organization.
- **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.
- **Self-Service Site:** In Password Manager version 5.16, you have the option to access the Password Manager Self-Service Site. The Password Manager Self-Service Site includes enhancements to the user interface to improve the usability of the site.

Password Manager for AD LDS components

Password Manager for AD LDS includes the following components.

NOTE: You can install these components on 64-bit operating systems only.

Table 1: Password Manager for AD LDS components

Component	Description	Importance
Password Manager for AD LDS	The suite of role-based sites that exposes the functionality of Password Manager for AD LDS to end users.	Required

IMPORTANT: One Identity strongly recommends not to install Password Manager for AD LDS on Domain Controllers (DCs).

Licensing

The Password Manager for AD LDS license specifies the maximum number of user accounts that Password Manager for AD LDS manages across all domains. Administrators can run the User Status Statistics (USS) task to identify if the installation is legally compliant: the scheduler counts the number of user accounts and compares it with the maximum number the license specifies.

Password Manager for AD LDS indicates with header warnings if:

- No license could be found.
- The number of managed user accounts exceeds the licensed number.
- Any errors occurred when running the task.
- The license is installed but its scope is not configured for managed persons or managed external persons.

To view the compliance status of the Password Manager for AD LDS license

1. Log in to the Password Manager for AD LDS Administration Site.
2. To open the licensing table, on the left pane, click **Licensing**.
3. In the license table, check the **Compliant** column. Compliant licenses are indicated with a green tick, while non-compliant licenses are shown with a red X.

Figure 1: Password Manager Administration Site – License table

Licensing > Licenses

Licenses

License	Type	Status	Expires	Total purchased licenses	Total required licenses	Compliant
License for One Identity Password Manager	Term	Ok	2025. 05. 07.	Managed: 999999, External managed: 999999	Managed: 2, External managed: 0	✓

Managed Persons

Managed External Persons

Telephone Verification

The total number of purchased and used licenses are indicated for both managed and external managed persons, in support of users who have multiple user accounts in the environment that Password Manager for AD LDS manages:

- "Managed persons" are persons with one or more user accounts within the environment that Password Manager manages.
- "Managed external persons" are persons with a part-time, contract, contractor or temporary employee status with one or more user accounts within the environment that Password Manager manages.

NOTE: Consider the following regarding managed accounts:

- Password Manager for AD LDS does not count disabled user accounts and user accounts not configured in the user scope in the list of managed users and managed external users.
- If the number of **Total purchased licenses** is lower than the number of **Total required licenses**, then the **Managed Persons** and **Managed External Persons** tabs of the **Licensing** page will not be visible.

Your license becomes non-compliant if:

- The Password Manager for AD LDS license is not installed.
- The maximum number of users has been exceeded.
- The term license has expired.

If this happens, then to solve the problem:

- In case of an exceeded user count:
 - Reduce the number of user accounts in the user scope. To recalculate and display the new user counts, in the Administration Site, run the User Status Statistics (USS) scheduled task.
 - Remove one or more managed domains to decrease the number of managed user accounts.

- Contact One Identity Sales to purchase additional licenses, then update your license as described in [Updating the license](#).
- In case of an expired license, contact One Identity Sales for renewal.

NOTE: Consider the following regarding licenses:

- Password Manager for AD LDS will continue to operate without business interruption in a non-compliant configuration.
- The following resources are not limited by the Password Manager for AD LDS license:
 - The number of computers connected to the Password Manager Administration Site, Helpdesk Site and Self-Service Site.
 - The number of Password Manager for AD LDS instances installed in your environment. This is to ensure that Password Manager for AD LDS can be deployed in enterprise environments for enhanced performance and fault tolerance.

To view the license number of the Password Manager for AD LDS license

1. In the Password Manager Administration Site, navigate to the **About** section.
2. To display the license number, click the **Licenses** tab.

Installing the license for Password Manager for AD LDS

The Password Manager license is installed the first time when you install Password Manager.

Prerequisites

IMPORTANT: Password Manager for AD LDS version 5.15.1 requires a new license key. If you are upgrading to 5.16 from 5.14.x or earlier, make sure to obtain the new key before installing the release. To obtain a new key, see the [Licensing Key Upgrade](#) page.

For assistance with your license upgrade, submit a request using the licensing assistance from the [One Identity Support Portal](#).

To install the license during Password Manager for AD LDS installation

1. From the new license, copy the .DLV file to the Password Manager host.
2. Start the installation of Password Manager.

3. During the installation when prompted, provide the .DLV license file. To open the **License status** dialog, in the Installation Wizard, click **Licenses** .
4. To locate and open your license key file, click **Browse license** and navigate to select the .DLV license file you copied over previously.
5. In the **Select License File** dialog, open your license key file and click **Close**.

Some license types might include counters for "managed persons" and "managed external persons" along with a counter for user accounts. In Password Manager terminology:

- "Managed persons" are persons with one or more user accounts within the environment that Password Manager manages.
- "Managed external persons" are persons with a part-time, contract, contractor or temporary employee status with one or more user accounts within the environment that Password Manager manages.

Password Manager applies the same license violation policies to managed persons and managed external persons as to user accounts. To specify these user groups, use the corresponding license scopes after you install Password Manager.

NOTE: Consider the following when installing or configuring licenses:

- License scopes are available only if your license includes managed persons and managed external persons.
- If the number of **Total purchased licenses** is lower than the number of **Total required licenses**, then the **Managed Persons** and **Managed External Persons** tabs of the **Licensing** page will not be visible.

To add an AD LDS instance to the managed persons scope

1. In the menu bar of the Administration Site, click **Licensing**.
2. In the **Licenses** page, click the **Managed Persons** tab.
3. On the **Scope of Managed Persons** page, click **Connect to AD LDS instance**.
4. If connections already exist, select a connection from the list. If you want to create a new connection, click **Add new connection**.
5. If you selected to create the new connection, in the **Connect to AD LDS Instance** dialog, configure the following options:
 - In the **Server name on which AD LDS instance is installed** text box, enter the name of the server to which you want to connect.
 - In **Port number (LDAP or SSL)**, enter the port number that you specified when installing the AD LDS instance. If you select **Use SSL**, enter the SSL port number; otherwise, LDAP port number. One Identity recommends using SSL in your production environment.
 - In **Application directory partition**, enter the name of the application directory partition from the AD LDS instance to which you want to connect.

- In **Application directory partition alias**, enter the alias for the application directory partition which will be used to address the partition on the Self-Service Site.
- In the **Access account** section, select **Password Manager Service account** to have Password Manager access the AD LDS instance using the Password Manager Service account, otherwise, select **The following Active Directory account or the following AD LDS account** and enter the required user name and password.

For information on how to prepare the access account, see [Configuring Permissions for Access Account](#).

6. To apply your changes, click **Save**.

To specify groups or Organizational Units included in the scope of managed persons

1. In the menu bar of the Administration Site, click **Licensing**.
2. In the **Licenses** page, click the **Managed Persons** tab.
3. On the **Scope of Managed Persons** page, select the domain connection for which you want to specify groups or OUs and click **Edit**.
4. Do the following:
 - To specify the groups, click **Add** under **Groups included into the scope of managed persons**.
 - To specify the OUs, click **Add** under **Organizational Units included into the scope of managed persons**.
5. To apply your changes, click **Save**.

To specify groups or OUs excluded from the scope of managed persons

1. In the menu bar of the Administration Site, click **Licensing**.
2. In the **Licenses** page, click the **Managed Persons** tab.
3. On the **Scope of Managed Persons** page, select the connection for which you want to specify groups or OUs and click **Edit**.
4. Do the following:
 - To specify the groups, click **Add** under **Groups excluded from the scope of managed persons**.
 - To specify the OUs, click **Add** under **Organizational Units excluded from the scope of managed persons**.
5. To apply your changes, click **Save**.

You can use the procedures below to specify the scope of managed external persons.

To add AD LDS instance to the managed external persons scope

1. In the menu bar of the Administration Site, click **Licensing**.
2. In the **Licenses** page, click the **Managed Persons** tab.
3. On the **Scope of Managed External Persons** page, click **Connect to AD LDS Instance**.
4. If connections already exist, select a connection from the list. If you want to create a new connection, click **Add new connection**.
5. If you selected to create the new connection, in the **Connect to AD LDS Instance** dialog, configure the following options:
 - In the **Server name on which AD LDS instance is installed** text box, enter the name of the server to which you want to connect.
 - In the **Port number (LDAP or SSL)** text box, enter the port number that you specified when installing the AD LDS instance. If you select the **Use SSL** check box, enter the SSL port number; otherwise, LDAP port number. It is recommended to use SSL in your production environment.
 - a. In the **Application directory partition** text box, enter the name of the application directory partition from the AD LDS instance to which you want to connect.
 - b. In the **Application directory partition alias** text box, enter the alias for the application directory partition which will be used to address the partition on the Self-Service Site.
 - c. In the **Access account** section, select **Password Manager Service account** to have Password Manager access the AD LDS instance using the Password Manager Service account, otherwise, select **The following Active Directory account** or **The following AD LDS account** radio button and enter the required user name and password.

For information on how to prepare the access account, see [Configuring Permissions for Access Account](#).

6. To apply your changes, click **Save**.

To specify groups or organization units included in the scope of managed persons

1. On the menu bar of the Administration Site, click **Licensing**.
2. On the **Licenses** page, click the **Managed Persons** tab.
3. On the **Scope of Managed Persons** page, select the domain connection for which you want to specify groups or OUs and click **Edit**.
4. Do the following:
 - To specify the groups, click **Add** under **Groups included into the scope of managed persons**.

- To specify the OUs, click **Add** under **Organizational Units included into the scope of managed persons**.
5. To apply your changes, click **Save**.

To specify groups or OUs excluded from the scope of managed persons

1. On the menu bar of the Administration Site, click **Licensing**.
2. On the **Licenses** page, click the **Managed External Persons** tab.
3. On the **Scope of Managed External Persons** page, select the domain connection for which you want to specify groups or OUs and click **Edit**.
4. Do the following:
 - To specify the groups, click **Add** under **Groups excluded from the scope of managed external persons**.
 - To specify the OUs, click **Add** under **Organizational Units excluded from the scope of managed external persons**.
5. To apply your changes, click **Save**.

Updating the license

If you have purchased a new license, you must update the license by installing the new license key file. You can use the **About** section of the Administration Site to check the license number of the installed license.

Prerequisites

IMPORTANT: Password Manager for AD LDS version 5.15.1 requires a new license key. If you are upgrading to 5.16 from 5.14.x or earlier, make sure to obtain the new key before installing the release. To obtain a new key, see the [Licensing Key Upgrade](#) page.

For assistance with your license upgrade, submit a request using the licensing assistance from the [One Identity Support Portal](#).

To update the license

1. In the menu bar of the Administration Site, click **Licensing**.
2. In the **Licenses** page, click **Install License**.
3. Select the license key file.
4. To apply the new license, click **Save**.

NOTE: If the license installation fails for any reason, Password Manager for AD LDS will indicate it with an error. In such cases:

- Verify that the license key file is correct.
- Contact One Identity Support.

Telephone verification feature license

Starting from version 5.15.0, Password Manager for AD LDS features are no longer tied to licenses, so the **Licensing** > **Telephone Verification** tab is always visible, regardless of whether you use the feature or not.

However, to use telephone verification features (allowing users to authenticate themselves via automated voice calls or one-time PINs received in text messages), you must configure your own phone authentication settings under the **General Settings** > **Phone Authentication** tab of the Password Manager for AD LDS Administration Site. For more information, see [Configuring phone-based authentication for Password Manager for AD LDS](#).

After configuring telephone verification, you must specify a separate scope for users for telephone verification service. Only users included in the scope will have access to the service.

Installing Password Manager: Checklist

This checklist provides tasks that an administrator should perform before installing Password Manager.

- Before installing Password Manager, obtain a new license key. For more information on the license requirement, see [Knowledge Base Article 4380378 New License requirement for Password Manager 5.15](#) on the One Identity support portal.
- If you are performing an upgrade, make sure to export the Password Manager configuration settings. For more information, see [Exporting Configuration Settings](#) on page 145.
- Make sure that the required firewall ports are open.
- Make sure to have a service account and application pool account with the required permissions.
- Obtain a certificate that contains all names used for accessing Password Manager.

NOTE: Certificates must contain all names used to access the Password Manager sites. If there are multiple servers in the Realm, include all servers.

For example, if you have two Password Manager servers, the Subject Alternative Name (SAN) should contain the following values:

Value	Example
Host name of Password Manager server 1	PMServer1
Host name of Password Manager server 2	PMServer2
Wildcard for the domain	*.mydomain.local
(Optional) Fully Qualified Domain Name (FQDN) of the servers	PMServer1.mydomain.local PMServer2.mydomain.local

IMPORTANT: One Identity cannot assist with obtaining certificates. To obtain the required certificate, contact your internal network team or Certificate Authority.

- Configure the following ports in IIS with the proper certificate:
 - 443 (Default HTTPS)
 - 20000 (Secure Token Server)
- Make sure to extend the AD LDS schema. For more information, see [Extending AD LDS Schema](#).

For additional information, see [Knowledge Base Article 4381287 HSTS Certificate requirement for Password Manager 5.15](#) on the One Identity support portal.

Installing Password Manager for AD LDS

This section describes how to install Password Manager. You will learn how to configure Password Manager Service account and application pool identity. A separate section will guide you through the steps required to install Password Manager. For more information see [Typical Deployment Scenarios](#).

NOTE: Password Manager for Active Directory (AD) and Password Manager for Active Directory Lightweight Directory Services (AD LDS) must not be installed on the same server.

Configuring Password Manager Service Account and Application Pool Identity

When installing Password Manager, you are prompted to specify two accounts: Password Manager Service account and application pool identity. Password Manager Service account is an account under which Password Manager Service runs. You can also use Password Manager Service account as a domain management account (the account that is necessary to add managed domains when configuring the user and Helpdesk scopes). To do this, ensure that Password Manager Service account has the minimum permissions required to successfully perform password management tasks in the domain. For more information, see [Configuring Permissions for Domain Management Account](#).

Application pool identity is an account under which the application pool's worker process runs. The account you specify as the application pool identity will be used to run Password Manager Web sites.

For Password Manager to run successfully, the accounts you specify when installing Password Manager must meet the following requirements:

- Password Manager Service account must be a member of the Administrators group on the web server where Password Manager is installed.
- Application pool identity account must be a member of the **IIS_IUSRS** local group on the web server in IIS 7.0 and must have permissions to create files in the **<Password Manager installation folder>\App_Data** folder.
- Application pool identity account must the full control permission set for the following registry keys: **HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager**.
- If the App pool account is a domain user with minimal permission, make sure that **<PM installation folder>\Web** folder must be provided with full control permission set for Application pool identity account.

Before you install Password Manager, make sure that the Password Manager Service account and application pool identity have the rights listed above.

Enabling HTTPS

One Identity strongly recommends that you use HTTPS with Password Manager. The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web.

For instructions on how to configure SSL in order to support HTTPS connections from client applications, see [Enable SSL for all customers who interact with your Web site in IIS](#) in the *Microsoft Windows documentation*.

NOTE: The HSTS functionality is a web security policy mechanism. It is enabled by default, which enables the Password Manager installation to be redirected from HTTP to use HTTPS.

However, HSTS can be disabled for testing purposes to access the Password Manager sites without using HTTPS. To disable HSTS, perform the following steps:

To disable HSTS

1. Open **regedit**.
2. Navigate to HKEY_LOCAL_MACHINE\Software\One Identity\Password Manager.
3. Change the value of **HSTSEnabled** to false.
4. Restart the Password Manager Service.

Installing Password Manager for AD LDS

You can install Password Manager by completing the following steps.

For an overview of the various installation scenarios, see [Typical Deployment Scenarios](#).

To install Password Manager for AD LDS

1. Run the **Password Manager for AD LDS** installer from the installation media.
2. Read the license agreement, select **I accept the terms in the license agreement**, then click **Next**.
3. On the **User Information** page, specify the following options, then click **Next**:
 - a. **Full name**: Enter your name.
 - b. **Organization**: Enter the name of your organization.
 - c. **Licenses**: Specify the path to the license file that you have obtained from your One Identity representative.
4. On the **Custom Setup** page, select the components to install, then click **Next**:
 - a. **Full Installation**: Select this option to install the Password Manager Service and Workflow Service, along with all sites (Administration, Self-Service and Helpdesk) on the current computer.
 - b. **Password Manager Self-Service Site**: Select this option to install only the Password Manager Self-Service Site.
 - c. **Helpdesk Site**: Select this option to install only the Helpdesk Site.

You can install all Password Manager for AD LDS components together on a single server or you can deploy the Password Manager Self-Service Site and Helpdesk Site on a standalone server. To learn more about installing the Self-Service Site and Helpdesk Site on a standalone server, see [Installing the Password Manager for AD LDS Self-Service Site and Helpdesk Site on a standalone server](#).

NOTE: By default, Secure Password Extension uses the Self-Service Site that is installed on the same server with the Password Manager Service and the

Password Manager Workflow Service. However, you can configure Secure Password Extension to use another Self-Service Site. For more information, see *Locating Self-Service Site* in the *Password Manager Administration Guide*.

5. On the **Password Manager Service Account Information** page, specify the name and password for the Password Manager Service account, then click **Next**. Use the following user name format:

DOMAIN\Username

For more information on the requirements for the Password Manager Service account, see [Configuring Password Manager Service Account and Application Pool Identity](#).

6. On the **Specify Web Site and Application Pool Identity** page, select the website name, specify the name and password for the account to be used as application pool identity, then click **Next**. For more information on the requirements for the application pool identity, see [Configuring Password Manager Service Account and Application Pool Identity](#).
7. Click **Install**.

When the installation is complete, click **Finish**.

NOTE: By default, Password Manager for AD LDS uses built-in certificates to encrypt traffic between the Password Manager websites (Self-Service Site and Helpdesk Site) and the Password Manager Workflow Service. After installing Password Manager, if the websites and the Password Manager Workflow Service are installed on different computers, One Identity recommends that you replace these certificates with new ones. For more information, see [Specifying custom certificates for authentication and traffic encryption](#).

Extending AD LDS Schema

To use Password Manager with an AD LDS instance, you need to extend the AD LDS schema to include required object class definitions.

When installing a unique AD LDS instance, you must specify the LDAP and SSL port numbers and the application directory partition name. Make sure, you remember the values you enter because you will need to use them when extending the AD LDS schema.

IMPORTANT: When you install an AD LDS instance, in the AD LDS setup wizard select the option to create a new application directory partition and, on the **Importing LDIF Files** page, select all shown files.

To extend AD LDS schema

1. On a computer where an AD LDS instance is installed, create a temporary folder.
2. Copy all files from the Password Manager\Setup\ADLDS Extension folder on the Password Manager installation media to the folder you created in step 1.
3. In the temporary folder, modify the `prepare_ad_lds.cmd` file using any text editor. Replace the port number in the line `SET PORT=50000` with the LDAP port number you specified in the AD LDS setup wizard.
4. In the temporary folder, modify the `data.ldf` file using any text editor. Replace all occurrences of the `O=Quest,C=US` with the application directory partition name you specified in the AD LDS setup wizard.
5. Run the `prepare_ad_lds.cmd` file.

Initializing a Password Manager for AD LDS instance

After installing Password Manager for AD LDS, you must initialize an instance before you can begin the configuration of a new Management Policy, including the configuration of the:

- User and Helpdesk scopes.
- Questions and Answers policy.
- Workflow management.

You can initialize a Password Manager for AD LDS instance by two means:

- Creating a unique instance.
- Setting up a replica of an existing instance.

If you create a replica of an existing instance, the new instance will share its entire configuration with the original instance. Password Manager for AD LDS instances sharing the same configuration are referred to as a "Password Manager realm". For more information about Password Manager realms, see [Installing multiple instances of Password Manager for AD LDS](#).

Prerequisites

To access the Administration Site, your user account must be part of the local groups:

- PMAAdmin
- IIS_IUSRS
- Administrators

To initialize Password Manager for AD LDS instance

1. Open the Administration Site by entering the following address in a web browser:

http(s)://<computer-name>/PMAAdmin

In the above URL, <computer-name> is the name of the computer on which Password Manager is installed.

You can obtain the URL path to the Administration Site from your system administrator.

2. On the login page, enter your user name and password and click **Log on**. The **Instance Initialization** page will appear automatically.

NOTE: For Password Manager 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 Administration Site.

3. On the **Instance Initialization** page, select one of the following options, depending on what type of instance you want to create:
 - **Unique instance:** Creates a new instance.
 - **Replica of existing instance:** Joins a new instance to a Password Manager for AD LDS realm.
4. If you selected the option **Replica of an existing instance**, follow the instructions of [Installing multiple instances of Password Manager for AD LDS](#).
5. If you selected the option **Unique instance**, under **Service connection settings**, specify the following:
 - **Certificate name:** Select the certificate that was issued for the computer running the Password Manager Service. If you decide to install the Password Manager Self-Service, and Helpdesk sites separately from the Password Manager Workflow Service, then One Identity recommends to replace the built-in certificate that is used encrypt traffic between the Workflow Service and the sites. For more information, see [Specifying custom certificates for authentication and traffic encryption](#).
 - **Port number:** Specify the port that the Self-Service and Helpdesk Sites will use to connect to the Password Manager Workflow Service. By default, port **20002** is used, which is inbound to the Password Manager Server.

NOTE: Port **20002** is the only default value that can be modified to another value, depending on the environmental requirements.

6. Under **Advanced settings**, specifying the following:
 - a. **Encryption algorithm:** Specify the encryption algorithm that will be used to encrypt the users' answers to secret questions and other security-sensitive information. You can select from two options: **Triple DES** and **AES**. By default, Password Manager uses Triple DES algorithm to encrypt data.

NOTE: If the **Store answers using reversible encryption** option is selected in the Q&A Profile settings, the users' answers will be encrypted. Otherwise, the answers will be hashed.

- b. **Encryption key length:** Specify whether a 192-bit or 256-bit encryption key will be used.
- c. **Hashing algorithm:** Specify the hashing algorithm that will be used to hash users' answers to secret questions. The following algorithms are available: **MD5** and **SHA-256**. By default, Password Manager uses SHA-256 hashing algorithm.

NOTE: If the **Store answers using reversible encryption** option is not selected in the Q&A profile settings, Password Manager will hash the users' answers.

- d. **Store user's Questions and Answers profile in the following attribute of user's account in Active Directory:** Enter the attribute name that will be used for storing Q&A profile data. By default, Password Manager stores:
 - Q&A profile data in the comment attribute of each user's account.
 - Configuration data in the comment attribute of a configuration storage account that is automatically created when installing Password Manager.

7. To complete instance initialization, click **Save**.

Installing the Password Manager for AD LDS Self-Service Site and Helpdesk Site on a standalone server

Password Manager for AD LDS allows you to install the Password Manager Self-Service Site and Helpdesk Site on a standalone server. For example, you can use this installation scenario to deploy Password Manager in a perimeter network.

If you deploy Password Manager in a perimeter network, One Identity recommends that you install the Password Manager Service, the Password Manager Workflow Service and the sites in a corporate network at first (that is, use the **Full Installation** option in the Password Manager setup), then install only the Password Manager Self-Service Site in the perimeter network.

NOTE: If you perform this installation scenario, then make sure that the server running the Password Manager Workflow Service and the server(s) running the Helpdesk Site and the Self-Service Site can communicate with each other through the port configured for the Password Manager Workflow Service.

For more information on how to configure the Password Manager Workflow Service port, see [Modifying service connection settings](#).

To install the Password Manager for AD LDS Self-Service Site and Helpdesk Site on a standalone server

1. Run the Password Manager for AD LDS installer from the installation media.
2. Read the license agreement, select **I accept the terms in the license agreement**, then click **Next**.
3. On the **User Information** page, specify the following options, then click **Next**:
 - a. **Full name**: Enter your name.
 - b. **Organization**: Enter the name of your organization.
 - c. **Licenses**: Specify the path to the license file that you have obtained from your One Identity representative.
4. On the **Custom Setup** page, select the **Password Manager Self-Service Site**, and/or **Helpdesk Site** features, then click **Next**.
5. On the **Specify Web Site and Application Pool Identity** page, select the website name and specify the name, and password for the account to be used as application pool identity, then click **Next**. For more information on the requirements for the application pool identity, see [Configuring Password Manager Service Account and Application Pool Identity](#).
6. Click **Install**.
7. When the installation is complete, click **Finish**.

After you installed the Self-Service Site and the Helpdesk Site on a standalone server, initialize the sites to start using them.

NOTE: Perform the following initialization procedures on the server(s) where the Self-Service Site and the Helpdesk Site are installed.

To initialize the Password Manager for AD LDS Self-Service Site

1. Log in to the server where the Self-Service Site is installed.
2. Open the Self-Service Site by entering the following address:
http(s)://<computer-name>/PMSelfService
In this URL, <computer-name> is the name of the computer on which the Password Manager Self-Service Site is installed.
The **Self-Service Site Initialization** page will appear automatically.
3. In **Computer name or IP address**, specify the Password Manager Workflow Service host name or IP address.

4. In **Port number**, specify the port number that the Self-Service Site will use to connect to the Password Manager Workflow Service.
5. To apply your changes, click **Save**.

To initialize the Password Manager for AD LDS Helpdesk Site

1. Log in to the server where the Helpdesk Site is installed.
2. Open the Helpdesk Site by entering the following address:
http(s)://<computer-name>/PMHelpdesk
In the above URL, <computer-name> is the name of the computer on which Helpdesk Site is installed.
The **Helpdesk Site Initialization** page will be displayed automatically.
3. In **Computer name or IP address**, specify the Password Manager Workflow Service host name or IP address.
4. In **Port number**, specify the port number that the Helpdesk Site will use to connect to the Password Manager Workflow Service.
5. To apply your changes, click **Save**.

NOTE: After the initialization of the Helpdesk Site and the Self-Service Site, the `wcfServiceRealms.xml` file is created. The `wcfServiceRealms.xml` file has records of all the installed Password Manager Service instances. The `wcfServiceRealms.xml` file is used to help the user to use one of the realm instances from the list, if the primary instance of the Password Manager Service is unavailable. For more information, see [FailSafe support in Password Manager](#)

IMPORTANT: If the Self-Service Site and/or the Helpdesk Site cannot reach the Password Manager Workflow Service, Password Manager will open the **Initialization** page of the affected site again when attempting to open the site. To solve the connection problem to the Password Manager Workflow Service, specify the **Computer name or IP address** and **Port number** settings again.

FailSafe support in Password Manager

This feature allows a user to login to the Helpdesk or Self-Service Site when the Password Manager Service is unavailable.

The Helpdesk and Self-Service Site use the Password Manager Service to communicate with Active Directory. If the Password Manager Service is unavailable, authentication and other such services do not function. For such scenario, Password Manager has a FailSafe feature integrated to connect to other available Password Manager service automatically.

After the initialization of Helpdesk and Self-Service Site, the `wcfServiceRealms.xml` file is created. This file has records of all the instances of Password Manager Services installed.

The user can use one of the realm instances listed in `WcfServiceRealms.xml` file, in case of unavailability of services in the primary instance of Password Manager Service.

For example, Helpdesk Site is connected to **Password Manager service 1**. If the **Password Manager service 1** is non-functional, with the integrated FailSafe feature, the Helpdesk Site automatically connects to **Password Manager service 2** to continue with the tasks uninterrupted. After the **Password Manager service 1** is restored, the Helpdesk Site is connected back to the initially connected Password Manager service, that is **Password Manager service 1**.

NOTE: Failsafe works in distributed environment. If all the Password Manager components are installed on the same server, the FailSafe operation might not work as expected.

NOTE: The Self-Service and Helpdesk Site's URLs must be accessible from Password Manager Service.

Installing multiple instances of Password Manager for AD LDS

Multiple Password Manager for AD LDS instances that share a common configuration are called a "Password Manager for AD LDS realm". In a realm, Password Manager Service instances share all settings and have the same set of management policies (that is, the same user scopes, Helpdesk scopes, Q&A policies and workflow settings).

If your organization uses multiple Password Manager for AD LDS instances, then One Identity recommends configuring a Password Manager for AD LDS realm to increase availability and fault tolerance.

CAUTION: If you configure a Password Manager for AD LDS realm, then do not edit Password Manager for AD LDS settings simultaneously on multiple instances of the same realm. Doing so might result in a loss of Password Manager configuration data.

To create a Password Manager for AD LDS realm

1. Export a configuration file from the Password Manager for AD LDS instance belonging to the target realm:
 - a. Connect to the Administration Site of the instance belonging to the target realm.
 - b. In the menu bar, click **General Settings > Import/Export**.
 - c. In the **Import/Export Configuration Settings** page, select **Export configuration settings**. To save the configuration file, click **Export**.

IMPORTANT: Remember the password that is generated when exporting the configuration file. You will need to enter this password when importing the configuration file for a new Password Manager for AD LDS instance that you want to add to the target realm.

2. Install a new Password Manager for AD LDS instance by running the Password Manager for AD LDS installer from the installation media. For more information on the installation procedure, see [Installing Password Manager for AD LDS](#) on page 12.
3. Open the Administration Site of the Password Manager for AD LDS instance that that you want to add to the realm.
4. On the **Instance Initialization** page, select **Replica of existing instance**.
5. To select and upload the configuration file that you exported from the instance belonging to the target realm, click **Upload**.
6. Enter the password to the configuration file, then click **Save**.

Specifying custom certificates for authentication and traffic encryption

If the Password Manager Workflow Service is installed on one computer and the Self-Service Site or Helpdesk Sites are installed on other computers, you must use certificate-based authentication and traffic encryption between the Workflow Service and the Password Manager websites.

By default, Password Manager uses built-in certificates issued by One Identity. However, you might want to install and use custom certificates issued by a trusted Windows-based certification authority.

This section provides instructions on how to start using custom certificates for authentication and traffic encryption between Password Manager for AD LDS components.

For more information, see the following sections:

1. [Step 1: Obtain and install custom certificates from a trusted Windows-based certification authority](#)
2. [Step 2: Providing certificate issued for the server computer of the Password Manager Workflow Service](#)
3. [Step 3: Providing the certificate issued for the client computers of the Self-Service and Helpdesk Sites](#)

Step 1: Obtain and install custom certificates from a trusted Windows-based certification authority

To install custom certificates for your Password Manager deployment if the Self-Service Site and the Helpdesk Site are installed on different machines than the Password Manager Service and the Password Manager Workflow Service, you must obtain two certificates from a trusted Windows-based certification authority:

- One for the computer running the Password Manager Service and Password Manager Workflow Service (this machine is called the "server computer").
- One for the computers running the Self-Service Site and the Helpdesk Site (called the "client computers").

When obtaining certificates, make sure that:

- The server computer can be accessed from the client computers by using the server certificate CN.
- **Both** is selected as a key usage in a certificate request.
- **Enable strong private key protection** is not selected in a certificate request.

IMPORTANT: When obtaining a certificate for the server computer, perform the following procedure on a computer where the Password Manager Service and the Password Manager Workflow Service are running. Use the Password Manager Service account to run a supported web browser.

When obtaining a certificate for the client computers, perform the following procedure on a computer running the Self-Service Site or Helpdesk Site and use the Application Pool Identity account to run a supported web browser.

To request a certificate from a trusted Windows-based certification authority for Password Manager for AD LDS

1. Use a browser to open `https://<server-name>/certsrv`. In this URL, <server-name> refers to the host name of the computer that runs the CA Web Enrollment role service.
2. On the **Welcome** page, click **Request a certificate**.
3. On the **Request a Certificate** page, click **Advanced Certificate Request**.
4. On the **Advanced Certificate Request** page, click **Create and submit a certificate request to this CA**.
5. Provide identification information as required. In the **Name** text box, enter the name of the server for which you are requesting a certificate.
6. In **Type of Certificate Needed**, select **Server Authentication Certificate**.
7. In **Key Options**, select **Create new key set**, and specify the following options:

- In **CSP** (Cryptographic service provider), select **Microsoft Enhanced RSA and AES Cryptographic Provider**.
 - In **Key Usage**, click **Both**.
 - In **Key Size**, set **1024** or more.
 - Select **Automatic key container name**.
 - Select the **Mark keys as exportable** check box.
 - Clear the **Enable strong private key protection** check box.
8. In **Additional Options**, specify the following:
 - In **Request Format**, select **CMC**.
 - In **Hash Algorithm**, select **sha256**.
 - Do not select the **Save request** check box.
 - Specify attributes if necessary and a friendly name for your request.
 9. Click **Submit**.
 10. If you see the **Certificate Issued** web page, click **Install this certificate**. If your request must be approved by your administrator first, wait for the approval then open the following URL:
 https://servername/certsrv
 11. Click **View the status of a pending certificate request**, then install the issued certificate.

Step 2: Providing certificate issued for the server computer of the Password Manager Workflow Service

In this step, you provide the certificate issued for the server computer to the Password Manager Workflow Service by using the Administration Site.

To provide the certificate to the Password Manager Workflow Service

1. Open the Administration Site by entering the following address in a web browser:
 http(s)://<computer-name>/PAdmin
 In the above URL, <computer-name> is the name of the computer on which Password Manager is installed.
2. Navigate to **Configuration > Reinitialization**.
3. Under the **Service connection settings**, select the custom certificate issued for the server computer from the **Certificate name** drop-down.
4. To apply your changes, click **Save**.

Step 3: Providing the certificate issued for the client computers of the Self-Service and Helpdesk Sites

In this step, you provide the certificate issued for the client computers to the Self-Service and Helpdesk sites installed separately from the Password Manager Service and Password Manager Workflow Service.

To provide the certificate to the Password Manager Self-Service Site

1. Open the Self-Service Site by entering the following address:

`http(s)://<computer-name>/PMSelfService`

In this URL, <computer-name> is the name of the computer on which the Password Manager Self-Service Site is installed.

The **Self-Service Site Initialization** page will appear automatically if the Self-Service Site is opened for the first time.

2. From the **Certificate name** drop-down list, select the custom certificate issued for the client computer.
3. To apply your changes, click **Save**.

To provide the certificate to the Helpdesk Site

1. Open the Helpdesk Site by entering the following address:

`http(s)://<computer-name>/PMHelpdesk`

In the above URL, <computer-name> is the name of the computer on which Helpdesk Site is installed.

The **Helpdesk Site Initialization** page will appear automatically if the Helpdesk Site is opened for the first time.

2. From the **Certificate name** drop-down list, select the custom certificate issued for the client computer.
3. To apply your changes, click **Save**.

Password Manager Architecture

[Password Manager Components and Third-Party Solutions](#)

[Typical Deployment Scenarios](#)

[Password Manager for AD LDS in a perimeter network](#)

[Management Policy Overview](#)

[Password Policy Overview](#)

[reCAPTCHA Overview](#)

[User Enrollment Process Overview](#)

[Questions and Answers Policy Overview](#)

[Data Replication](#)

[Phone-based authentication service overview](#)

[Configuring Management Policy](#)

Password Manager Components and Third-Party Solutions

This section provides information Password Manager components and third-party applications that can be used by Password Manager.

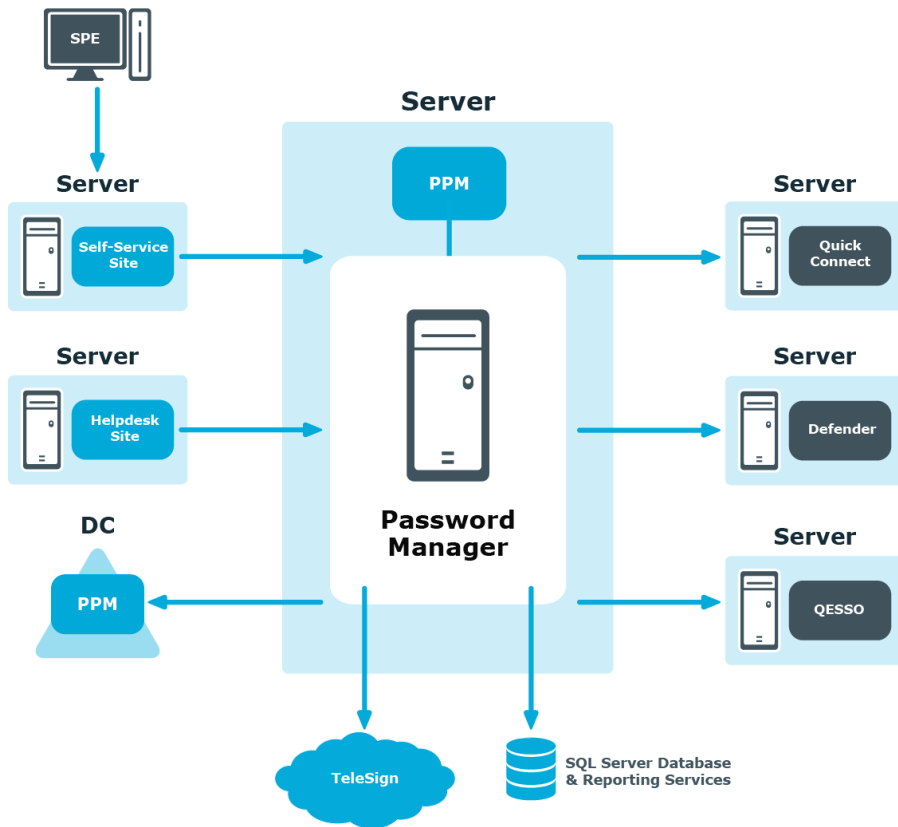
The following is a list of Password Manager components:

- [Password Manager Service, Workflow Service and Administration Site](#)
- [Self-Service Site](#)
- [Helpdesk Site](#)

The following is a list of third-party applications that can be used by Password Manager:

- [TeleSign](#)
- [SQL Server Database and SQL Server Reporting Services](#)

- Defender
- Password Manager Secure Token Server
- RADIUS Two-Factor Authentication



Password Manager = Password Manager Service + Administration site + Self-Service site + Helpdesk site

Password Manager Service, Workflow Service and Administration Site

The Password Manager Service, the Password Manager Workflow Service and the Administration Site are core components of Password Manager for AD LDS.

- The **Password Manager Service** is a Windows service that provides core functionality and runs under the Password Manager Service account. This account is specified during Password Manager for AD LDS installation.
- The **Password Manager Workflow Service** is also a Windows service that:

- Runs and handles Password Manager workflows.
- Communicates with the Password Manager Self-Service Site and Helpdesk Site.
- Uses port 20002 inbound to the Password Manager Server. If needed, you can set it to the desired value as described in [Initializing a Password Manager for AD LDS instance](#).

The Administration Site provides all the necessary settings for Password Manager administrators to configure and use Password Manager for AD LDS, including configuring:

- User and helpdesk scopes.
- Management policies.
- Password policy rules.

NOTE: Consider the following when deploying the Password Manager services and sites:

- You cannot install the Password Manager Administration Site separately from the Password Manager Service and the Password Manager Workflow Service. These services and the Administration Site must be installed on the same machine.
- If you install the Password Manager Service, the Password Manager Workflow Service and the Administration Site, you must also install the Self-Service Site and Helpdesk Site. However, you can install the Self-Service and Helpdesk Sites to different machines.

Self-Service Site

The Password Manager for AD LDS Self-Service Site allows users to easily and securely manage their passwords, eliminating the need for assistance from high-level administrators and reducing helpdesk workload.

You can install the Self-Service Site in two ways:

- On the same server where the Administration Site, the Password Manager Service and the Password Manager Workflow Service are installed.
- On a standalone server.

One Identity recommends deploying the Self-Service Site on a standalone server if, for example, you want to install the Self-Service Site in a perimeter network.

Helpdesk Site

The Helpdesk Site handles typical tasks performed by helpdesk operators, such as resetting passwords, unlocking user accounts, assigning temporary passcodes, and managing user

Questions and Answers profiles.

You can install the Helpdesk Site in two ways:

- On the same server where the Administration Site, the Password Manager Service and the Password Manager Workflow Service are installed.
- On a standalone server.

TeleSign

TeleSign is a third-party service that provides phone-based authentication for Password Manager for AD LDS users. To use the TeleSign service, you must:

- Have a valid license with TeleSign.
- Configure TeleSign phone-based authentication using your TeleSign API key and customer ID.
- Include the Authenticate with Phone activity in the corresponding workflows.

If TeleSign is configured, when users perform tasks on the Self-Service Site or Helpdesk Site, they will be prompted to select their phone number, then enter a one-time code on the site for verification.

The TeleSign service is available anywhere where users can receive calls or text messages. To receive verification codes, users do not need to install any applications on their phones.

To communicate with TeleSign, Password Manager for AD LDS uses REST API.

For more information, see [Phone-based authentication service overview](#).

SQL Server Database and SQL Server Reporting Services

Using a SQL database and SQL Server Reporting Services you can manage reports that allow you to analyze how the application is used.

The available out-of-the-box reports help you track user registration activity, Helpdesk tasks, user statuses, and so on.

For more information, see [Reporting and User Action History Overview](#).

Defender

IMPORTANT: Authenticating with Defender is an activity not supported with the current release of Password Manager AD LDS.

Defender is a One Identity product that provides two-factor authentication. Defender uses one-time passwords generated by special hardware or software tokens. If Password Manager is integrated with Defender, users can use one-time passwords to authenticate themselves on the Self-Service Site.

To use Defender with Password Manager, install the Defender Client SDK on the server on which Password Manager Service is installed.

For more information, see [Authenticate with Defender](#).

Password Manager Secure Token Server

Password Manager Secure Token Server (STS) is installed with Password Manager. You can configure STS to use internal or external providers with optional Multi-Factor Authentication (MFA).

You can use this feature on the new Password Manager Self-Service Site to authenticate users in a workflow, or to authenticate admin and helpdesk users. This feature is installed as a service called Password Manager Secure Token Service (STS). It has a configuration and user login interface.

How to use Password Manager STS features

To use the Password Manager STS feature, drag the **Authenticate with Secure Token Server** activity into any workflow.

- If you did not set up any Secure Token Server connection or did not have any valid providers configured in authentication providers, you cannot use this activity.
- If you set up one provider, you can start using it by dragging the activity in the workflow.
- If you set up more than one provider, you can select a specific provider for each activity that is used in workflows.

Authenticate with external provider in the Self-Service Site

If **Authenticate with Secure Token Server** is the current activity in a workflow, users will receive a login form where they must specify the credentials for the configured authentication provider. If the configured provider is using multi-factor authentication, the user is prompted for the next step. For more information, see [Authenticate with Secure Token Server](#).

This login interface uses the browser language, and supports the following languages:

- Argentinean (ar)
- Chinese (zh)
- Dutch (nl)
- English (en)

- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Russian (ru)
- Spanish (es)

Password Manger STS account restrictions

By default, the Password Manager STS account is set to be the same account as the Password Manager Service Account by the Password Manager installer. The account requires read rights on domain.

Using STS features in a Password Manager realm

The Password Manager STS settings are stored separately from other Password Manager settings in a file on each server. That file will be encrypted using the service user's DPAPI key by default, or a specified certificate and can be replicated to other servers in a realm. For the replication to work the Password Manager STS instances should use the same ports.

Using Certificate to protect STS configuration

A trusted X.509 certificate with a private key needs to be installed on each server in the LocalMachine's certificate store. The provided `Rsts.exe.config` XML configuration file (`\One Identity\Password Manager\Service\SecureTokenServer\`) will need to be modified on each machine running a PasswordManager STS instance. An example of the XML configuration file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="rstsConfigSource" type="Rsts.Config.RstsConfigSource, Rsts"/>
  </configSections>
  <rstsConfigSource xmlns="urn:Rsts.Config">
    <source type="FileConfigProvider">
      <fileConfigProvider fileName="rstsConfig.bin">
        <protection type="RsaDataProtection">
          <rsaDataProtection certificateStore="LocalMachine"
certificateLookupType="FindByThumbprint"
certificateLookupValue="b23655f8ac0b81c5b00bac0bc0a15e7e1d2b78be"/>
        </protection>
      </fileConfigProvider>
    </source>
  </rstsConfigSource>
</configuration>
```

The thumbprint of the certificate used to encrypt the Password Manager STS settings file is set in the `rsaDataProtection` element's `certificateLookupValue` attribute. Change the value of the `certificateLookupValue` attribute to match the used certificate's thumbprint. In case of swapping to certificate encryption, copy the protection element and its child nodes and replace the existing protection element in the `masterConfigProvider` and `slaveConfigProvider` node.

NOTE: This configuration will be used after the restart of Password Manager Secure Token Server service.

NOTE: The specified certificate must be valid, trusted and it must exist in the Local Computer's certificate store. It must have a private key. Access to the private key must be granted to the service account that is running the Password Manager Secure Token Server Windows Service. The private key must be an RSA key, of any length. A certificate with an ECC key is not supported.

CAUTION: The current `rstsConfig.bin` will be unusable. For master (or single) instances of STS, reconfiguration has to take place from start. In case of slave instances, if the replication process works correctly, no reconfiguration is needed.

Pre-configuration steps after swapping between encryption methods on master (or single) instance

Pre-configuration takes place on the Administration Site **General Settings > Secure Token Server** page. Password Manager will check if a reset happened, then try to configure the basic options needed for STS to work properly. If the configuration is successful, no modal should show up. After a page refresh, STS is useable again.

If Password Manager STS settings are not replicated automatically

To replicate the Password Manager STS settings manually, copy the `rstsConfig.bin` file from the server where you configured Password Manager STS to all other servers. After you copy the file, you must restart the Password Manager STS Windows Service.

NOTE: You can find `rstsConfig.bin` in `<installdir>/One Identity/Password Manager/Service/SecureTokenServer/`.

NOTE: This process needs to be repeated every time Password Manager STS settings are modified.

NOTE: : For this copy-paste process, the encryption method of the Password Manager STS has to be set to **certification based encryption** before configuration. See: [Using Certificate to protect STS configuration](#).

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.

To configure RADIUS Two-Factor Authentication

1. On the home page of the Administration Site, click **General Settings > RADIUS Two-Factor**.

The **RADIUS Two-Factor Authentication** page is displayed.

2. To add a new RADIUS server for authentication, click **Add RADIUS server**.
RADIUS Two-Factor Authentication page is displayed.

NOTE: You can add only two servers, one is used as a primary server and the other as a secondary server. The server that is created first is considered as the primary server and used for RADIUS authentication.

3. In the **RADIUS Server (IP address or hostname)** field, enter the RADIUS server IP address.
4. In the **Port number** field, enter the port number assigned during configuration of RADIUS.
5. In the **RADIUS Shared Secret** field, enter the password set during RADIUS configuration.
6. Specify the Active Directory attribute to authenticate the user from the drop-down menu.
7. From the **Additional RADIUS Attribute** section, select the required RADIUS attribute from the drop-down menu. Specify the value for the selected attribute and click **+**.

The RADIUS attributes and the corresponding values that you add is displayed.

NOTE: The RADIUS attributes supported are **NAS-IP-Address**, **NAS-Port**, **NAS-Port-Type**, and **NAS-Identifier**.

8. Click **Save**.

For more information, see [Authenticate with RADIUS Two-Factor Authentication](#).

Redistributable Secret Management Service

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.

NOTE: The Target platform IP address or the Hostname should not be same server where the One Identity rSMS service is installed.

Location sensitive authentication

The location sensitive authentication feature allow you to skip certain authentication methods for users trying to execute a workflow on Self-Service Site from a defined corporate network. Using this feature, you can also restrict the capability of searching for the users on Self-Service Site from IP addresses that is not specified in the defined corporate IP address range. For more information on restricting the user search, see [Account Search Options Customization](#).

IMPORTANT: It is mandatory to have at least one authentication method for users accessing the application from the defined corporate network.

You can use the location sensitive authentication feature for any of the authentication activities listed here.

- Q&A profile (random questions)
- Q&A profile (specific questions)
- Q&A profile (user-selected questions)
- Defender
- RADIUS Two-Factor Authentication
- Phone

Configuring corporate IP address range

You must specify a defined corporate IP address range that help in determining if the users are trying to execute the workflow from an internal or external network.

1. On the home page of the Administration Site, click **General Settings > Corporate IP Address Ranges**.
2. On the **Corporate IP Address Ranges** page, click **Add Corporate IP Address Range**.
3. Provide the **Network Address** and **Subnet Mask**.

4. Click **Save**.

The corporate IP address range is successfully added.

To edit the defined corporate IP address, click **Edit**. To delete the defined corporate IP address, click **Remove**.

Working with Power BI templates

Microsoft Power BI is an analytics service that is used to visualize large data with business intelligence. You can generate multiple interactive reports and customize dashboards with data insights and plot them on graphs to simplify data visualization.

IMPORTANT: The existing reporting in Password Manager is retained for the current release, after which it will be deprecated and replaced by Power BI reporting service.

The predefined Password Manager PowerBI template is available in Password Manager\Setup\Template\PowerBI Template of the installation media. You can extend the functionality by exporting the predefined template using the PowerBI Desktop software. The template provides the following reports by default:

- User Status
- Actions by Users
- Actions by Number of Users
- Users actions by Month
- Email Notification by Type and User
- Helpdesk usage by Actions
- Helpdesk usage by Operators
- Helpdesk usage by Users
- Registration by Month

To import the predefined PowerBI template

1. Download and install the Power BI Desktop software from the Microsoft Download Center.
2. Provide the credentials to login to the Power BI Desktop software.
3. Navigate to **File > Import > Power BI template**.
4. Select the predefined Power BI template and click **Open**.
The **SQL Server database** window is displayed.
5. The PowerBI Desktop initiates the process to connect to the database from which the template is created. Click **Cancel**.
6. The **Refresh** window is displayed. Click **Cancel**.

7. Navigate to the **Data Source settings** in the Power BI Desktop.
The **Data source settings** window is displayed.
8. Click **Change Source**.
9. Provide the SQL Server name in the **Server** field and the Database name in the **Database** field.
10. Click **OK**.
11. Click **Apply changes** in the warning message to apply the latest changes.
The Power BI Desktop is connected to the database and all the updates are displayed.

Alternative option

As an alternative to generating reports using predefined Power BI templates, you can use the **Reporting** feature. For more information, see [Reporting and User Action History Overview](#).

Password Manager Credential Checker

The Password Manager Credential Checker is based on PowerShell scripts used to check if the user's password is compromised. Credential Checker deals with actions related to change in password in Active Directory, reset password in Active Directory, change password in Active Directory and connected systems, or reset password in Active Directory and connected systems. By default, the Credential Checker PowerShell script implements Vericlouds CredVerify functionality for leaked password with hash segment.

IMPORTANT: If you prefer to use other credential checker service, modify the Credential Checker PowerShell script appropriately.

To configure the Password Manager credential checker

1. To enable the Password Manager credential checker, after the Password Manager is installed, on the Password Manager Administrator portal, navigate to **General settings > Extensibility** and select **Turn the credential checker mode on or off**.
2. On the Password Manager installation path, open the `compromised_password_checker` script. It is available in the `<installation location>\One Identity\Password Manager\Service\Resources\CredentialChecker` location.
3. Edit the script to provide the Vericlouds credentials:

```
$url=<valid URL>  
$api_key=<valid Key>  
$api_secret=<valid api secret>
```

4. Save the file.

When you enter a new password on the Self-Service Site using any of the workflows, such as, **Forgot Password** or **Manage My Passwords**, the Credential Checker validates the new password and check if it matches with the passwords listed in the VeriClouds. If the password matches, **Provided password is compromised, type another password. If you've ever used it anywhere before, change it!** is displayed.

This feature is not applicable if the user changes the password using **Ctrl + Alt + Delete** on the Windows logon screen.

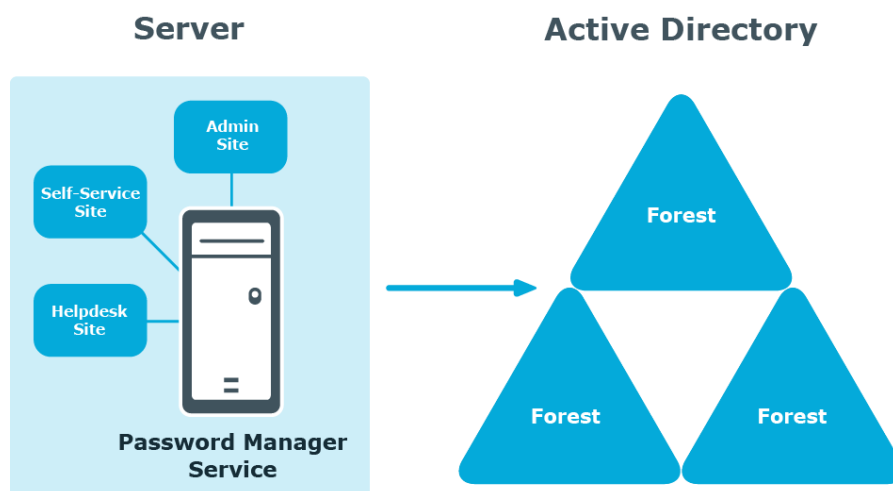
Typical Deployment Scenarios

This section describes typical deployment scenarios for Password Manager, including scenarios with installation of the Self-Service and Helpdesk sites on standalone servers, using realms, and so on.

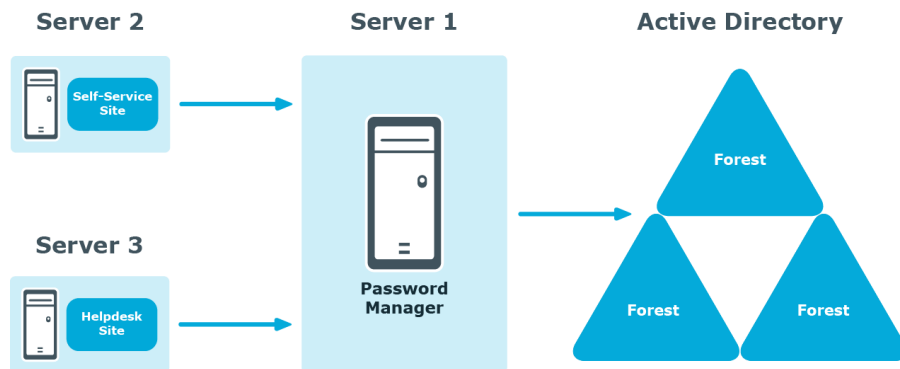
Simple deployment

In this scenario, you install all main Password Manager for AD LDS components (the Password Manager Service, the Password Manager Workflow Service, and all Password Manager sites) on a single server. This is the simplest deployment scenario, and One Identity recommends that you use it in small environments or for demonstration purposes.

Figure 2: Simple deployment of Password Manager on a single server



Deployment of the Password Manager for AD LDS Self-Service and Helpdesk Sites on standalone servers



You can install the Password Manager Self-Service Site, Helpdesk Site, or both on a standalone server.

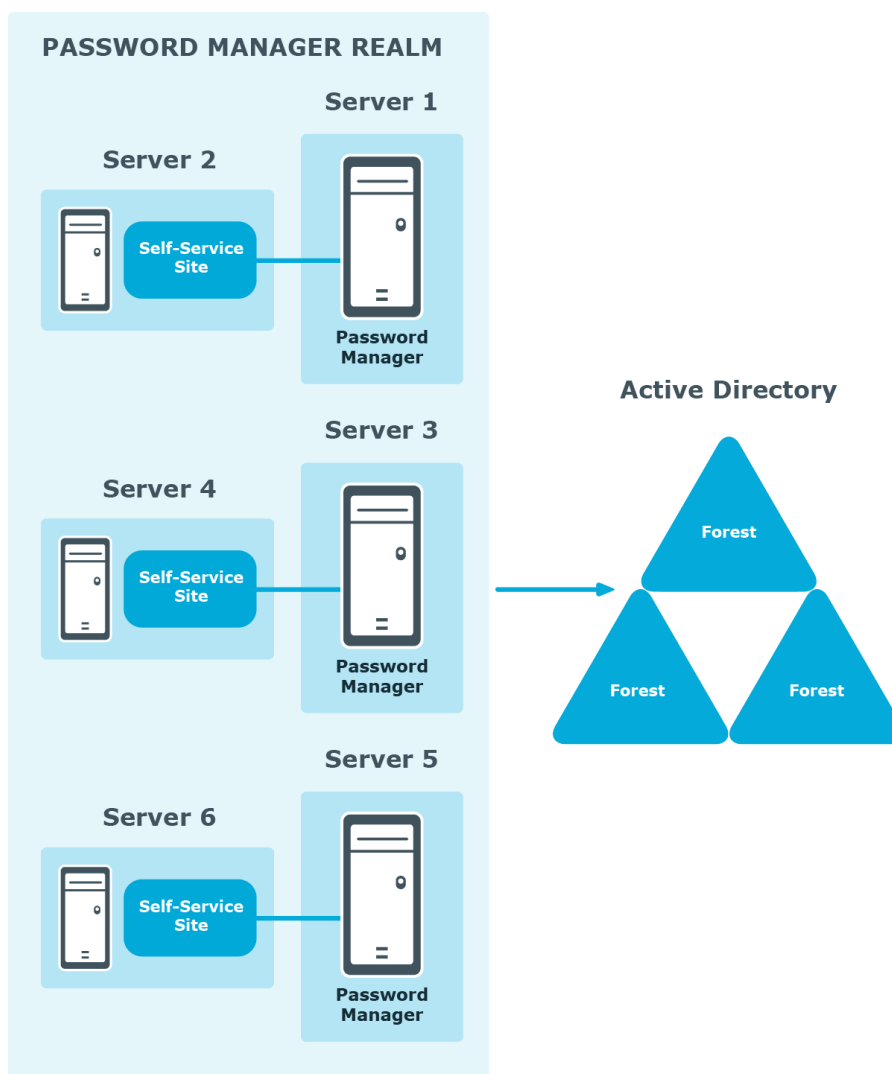
NOTE: While you can install the Password Manager Self-Service Site and Helpdesk Site to different machines than the one running the Password Manager Service and Password Manager Workflow Service, you must install the Administration Site on the machine running the Password Manager Service.

Use this infrastructure approach to deploy Password Manager in an environment with a perimeter network. Installing the Password Manager Self-Service Site and/or Helpdesk Site in the perimeter network enhances the security of your environment while preventing access to your internal network.

When deploying Password Manager in an environment with the perimeter network, One Identity recommends to perform a full installation of Password Manager in the internal corporate network, then install the Self-Service Site and/or the Helpdesk Site in the perimeter network.

If you deploy the available Password Manager components in this approach, open only the ports that you specified in the **Service connection settings** screen of the Administration Site, as described in [Modifying service connection settings](#).

Realm deployment



In this scenario, you install several Password Manager Services on separate servers. If all the instances of Password Manager share the same configuration (management policies, general settings, password policies, encryption algorithm, encryption key length, hashing algorithm, attribute for storing configuration data, and realm affinity ID), they are referred to as a realm.

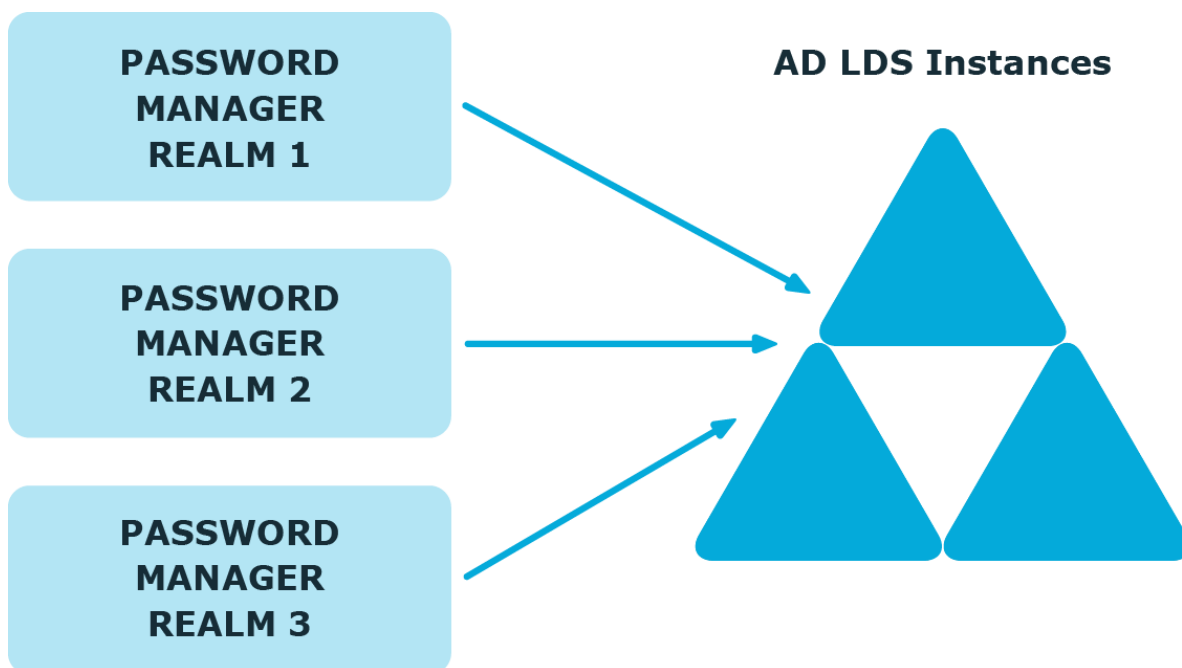
The realm provides for high availability of the service, load balancing, and fault tolerance.

For Password Manager Service instances installed on separate servers, you can use a load balancer to enhance service availability.

To create the Password Manager realm, you need to create replicas of an existing instance by exporting settings from this instance and importing the settings to a new instance.

For more information on how to create realms, see [Import/Export Configuration Settings](#).

Multiple Realm Deployment



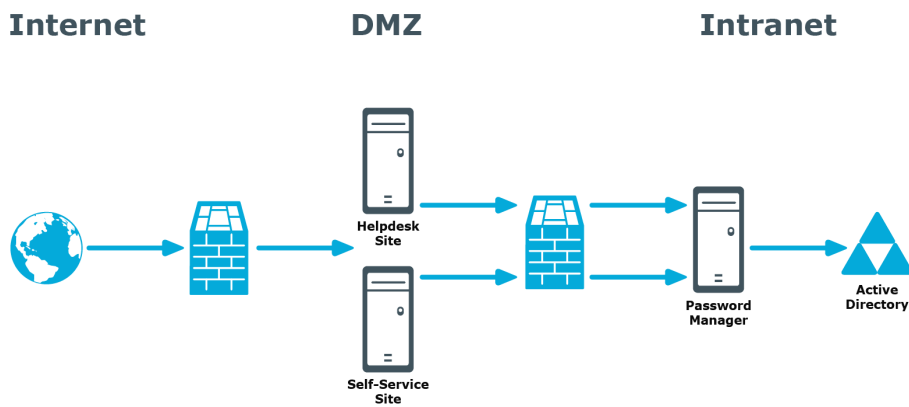
In this scenario, you deploy several Password Manager realms in your environment. You can use this scenario in complex environment, when several Password Manager configurations are required.

For example, a service provider can deploy two Password Manager realms, one realm to service company A, and the other - company B.

You can also use this scenario for a test deployment of Password Manager. In this case, the first realm is a production deployment of Password Manager, and the second realm can be used for testing purposes.

Password Manager for AD LDS in a perimeter network

When deploying Password Manager for AD LDS in a perimeter network, One Identity recommends to install the Password Manager Service, the Password Manager Workflow Service and the sites in a corporate network at first (that is, use the **Full installation** option in the Password Manager setup), then install only the Self-Service Site and the Helpdesk Site in the perimeter network.



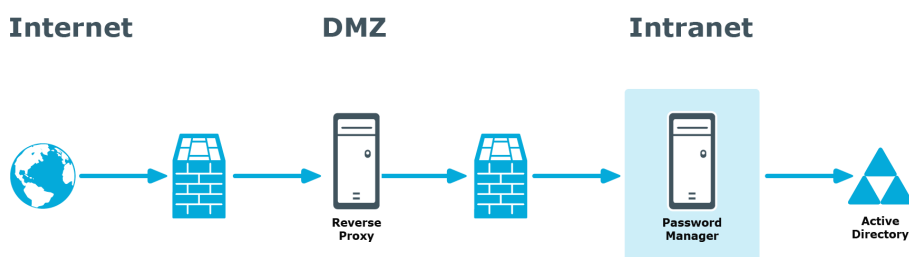
If you use this installation scenario, open only the ports in the firewall between the corporate network and the perimeter network that you configured in [Modifying service connection settings](#).

For more information on installing the Self-Service Site and the Helpdesk Site separately from the Password Manager Service and the Password Manager Workflow Service, see [Installing the Password Manager for AD LDS Self-Service Site and Helpdesk Site on a standalone server](#).

Installing Password Manager for AD LDS in a perimeter network with reverse proxy

A reverse proxy is a proxy server that is typically deployed in a perimeter network to enhance the security of the corporate network. By providing a single point of access to the servers installed in the intranet, the reverse proxy server protects the intranet from external attacks.

Figure 3: Password Manager installation in a perimeter network with reverse proxy



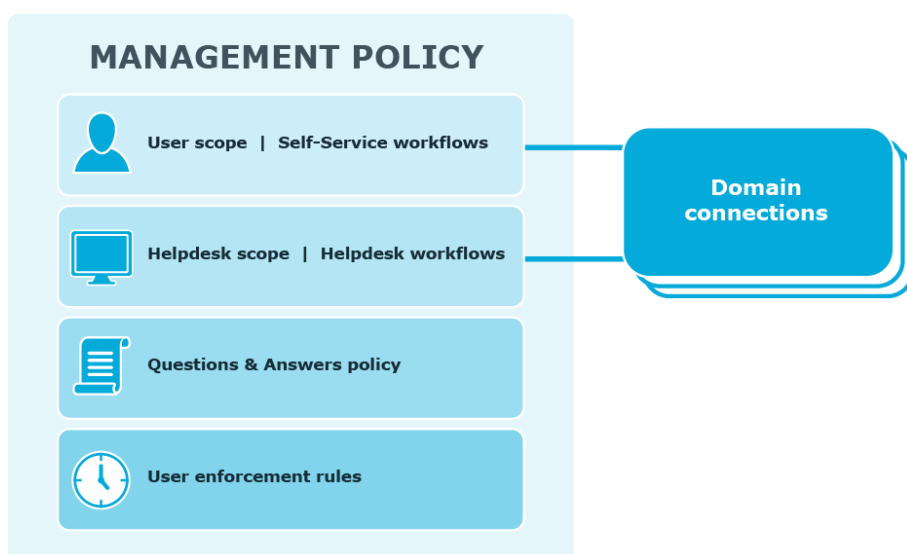
If you have the reverse proxy deployed in the perimeter network in your environment, One Identity recommends that you install the Password Manager Service, the Password Manager Workflow Service and Password Manager sites (the Self-Service and Helpdesk Sites) in the intranet, then configure the reverse proxy to redirect requests from external users to the correct intranet URLs of the Password Manager for AD LDS sites.

Management Policy Overview

A Management Policy is a core concept in Password Manager. Management Policies allow you to organize and group settings for dedicated users and helpdesk operators.

Management Policy components

The following diagram illustrates the Management Policy components.



User scope defines user groups from specified domains that can access the Self-Service Site and use the corresponding workflows. You can add multiple domains to a single user scope. You can also use the same domain connection in the user and Helpdesk scopes.

Helpdesk scope defines groups of Helpdesk operators from specified domains that can access the Helpdesk Site and manage users from the user scope using the Helpdesk workflows. You can add multiple domain connections to a single Helpdesk scope. You can also use the same domain connection in the user and Helpdesk scopes.

Self-Service and helpdesk workflows define the tasks that are available to users and Helpdesk operators on the Self-Service and Helpdesk sites: for example, **Forgot My Password**, **Assign Passcode**, **Unlock Account**, and so on.

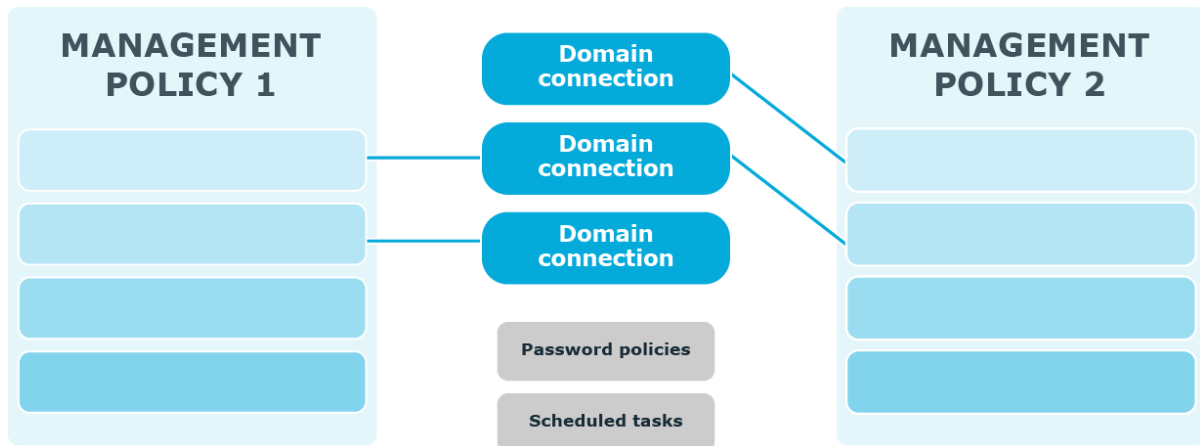
Questions and Answers policy comprises a list of secret questions (in the default and additional languages) that users must answer to authenticate themselves, and Q&A profile settings that specify various settings for questions and answers, such as a minimum length of an answer or a question, a number of required user-defined questions, and so on.

User enforcement rules define how users should be enforced to register with Password Manager and reminded to change their password. For each enforcement rule, a corresponding scheduled task exists. For example, the **Invitation to Create/Update Profile** scheduled task corresponds to the **Invite Users to Create/Update Q&A Profiles** enforcement rule. By default, the enforcement rules are not configured. To start

notifying users to create/update their Q&A profiles and change password, you need to configure the rules after Password Manager installation.

Management Policy and other Password Manager settings

The following diagram illustrates how several Management Policies interact with other Password Manager settings.



In a single Password Manager instance, you can create multiple Management Policies. Different Management Policies may use the same domain connections (specified in the user and Helpdesk scopes). If a user is included in the user scopes of both Management Policies, the settings from the first Management Policy in which scope the user is found will be applied to the user.

Settings from each Management Policy use the same scheduled tasks and password policies.

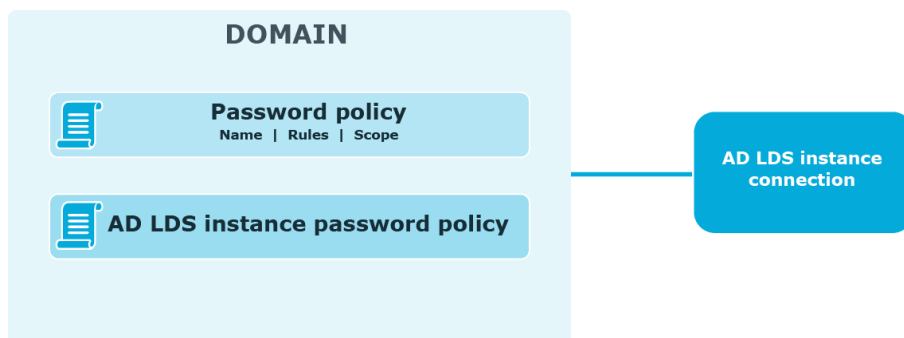
The **Invitation to Create/Update Profile, Reminder to Create/Update Profiles, Reminder to Change Password** scheduled tasks allow notifying users from scopes of user enforcement rules configured in Management Policies. For more information, see [Scheduled Tasks](#) and [User Enforcement Rules](#).

To set password policies for users from user scopes of Management Policies, you need to configure password policies and include corresponding users to the password policy scope. For more information about password policies, see [Creating a Password Policy](#).

Password Policy Overview

Password Manager provides the opportunity to granularly apply and manage password policies.

The following diagram shows available password policies and their structure:



By default, AD LDS enforces the local or domain policy applied to the computer on which an AD LDS instance runs. You can also configure password policies. Note that the password policy applied to the computer on which the AD LDS instance runs cannot be automatically displayed on the Self-Service Site when users change or reset passwords. To display such policy, use the **Custom rule** available in password policies. In this rule, enter the settings of the password policy applied to the computer running the AD LDS instance. For more information, see [Custom Rule](#).

To create and manage password policies, you need to add a connection to the AD LDS instance on the **Password Policies** tab of the Administration Site. When adding the connection, you specify the application directory partition to which password policies will be applied and the credentials that will be used to access the partition.

After you have added the connection, you can create password policies for this application directory partition. For each password policy, you can specify a name, a set of policy rules, and a scope.

Note that password policy rules are applied and displayed on the Self-Service Site when users change or reset passwords, only after you have added the connection and created policies for the corresponding application directory partition.

If a user is found in the scopes of several password policies, then the policy with the highest priority is applied to the user. Note that priority can be changed for policies with the same scope.

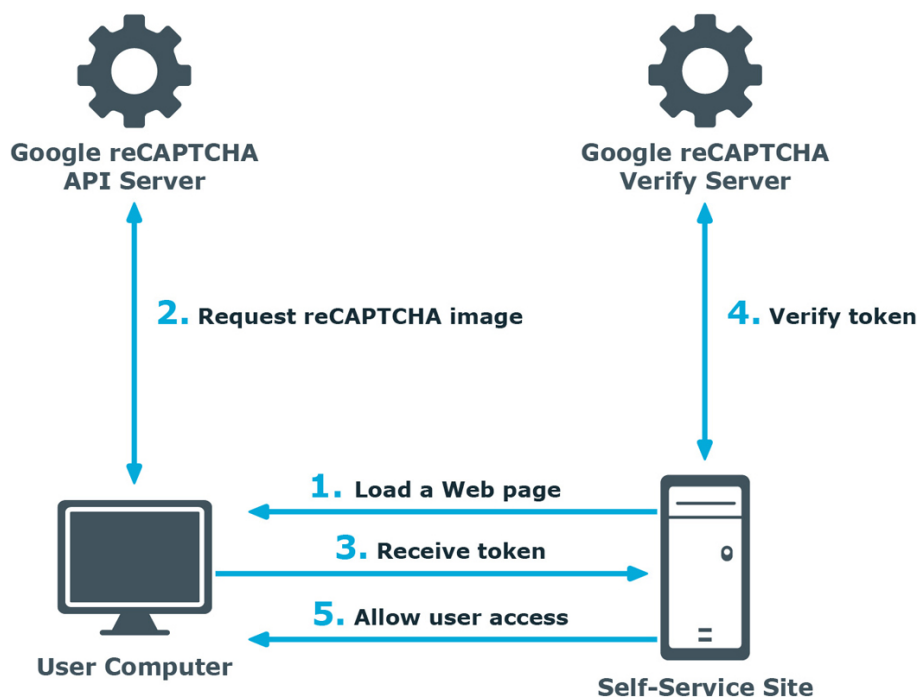
reCAPTCHA Overview

This section provides an overview of the reCAPTCHA service, system requirements for using it and references.

How it works

reCAPTCHA V2 is a free CAPTCHA service provided by Google. You can use it to protect the Self-Service from bots attempting to access restricted areas.

As reCAPTCHA uses images that optical character recognition software has been unable to read, it provides a secure protection for websites.



1. A user opens the Self-Service Site.
2. The user's browser sends the site key obtained during registration on the reCAPTCHA V2 site to the Google reCAPTCHA V2 API server and requires the user to select the check box indicating the user is not a robot.
3. Use this activity to verify reCAPTCHA on the Self-Service Site. User must select the **I'm not a robot** check box before beginning a workflow. This will either pass the user immediately (with No CAPTCHA) or challenge them to validate whether or not they are human. This feature provides enhanced protection against automated attacks.
4. The token and the secret key (obtained during registration on the reCAPTCHA V2 site) are then transferred to the Google reCAPTCHA V2 Verify server to be checked. After checking the response, the reCAPTCHA V2 server sends a reply back to the Password Manager server.
5. If the response is correct, the user is granted access to further steps on the Password Manager site.

How to Use reCAPTCHA on Password Manager Sites

To display reCAPTCHA images on the Self-Service Site, include the Display reCAPTCHA activity in required workflows. To require users to reply to a reCAPTCHA challenge before authentication, place the Display reCAPTCHA activity before any authentication activity in a workflow designer.

For more information on using reCAPTCHA in workflows, see [Display reCAPTCHA](#) on page 92.

You can also use reCAPTCHA on the Find Your Account page of the Self-Service Site and require users to reply to the reCAPTCHA challenge before searching for their accounts. For more information, see [Configuring CAPTCHA or reCAPTCHA for the Find Your Account page](#) on page 135.

System Requirements for Using reCAPTCHA

To be able to use reCAPTCHA on the Password Manager sites, make sure the following requirements are met:

- The Self-Service Site have access to the following address:
<http://www.google.com/recaptcha/api/verify>
- Users' computers have access to the Internet and to the www.google.com address.

References

Use the following resource for additional information on the reCAPTCHA service:

- <http://www.google.com/recaptcha>
- <https://policies.google.com/privacy?hl=en>
- <https://policies.google.com/terms?hl=en>
- <https://developers.google.com/terms/>

User Enrollment Process Overview

To enforce users to register with Password Manager you can use two enforcement rules: **Invite users to create/update Q&A profiles** and **Remind users to create/update Q&A profiles**.

To start the enrollment process, you need to enable and configure the **Invite users to create/update Q&A profiles** rule. This rule sends email notifications to the users specified in the rule's scope, inviting them to create or update their Q&A profiles. When configuring email notifications for this rule, you can insert a hyperlink to the Self-Service Site. To add the hyperlink, enter the required URL in the email notification body. For example, <http://mydomain.com/user>. Note, that you cannot specify the hyperlink text.

To configure the **Invite users to create/update Q&A profiles** enforcement rule, you need to specify the conditions under which users should be notified. For example, users are not registered with Password Manager, users' answers are shorter than required or users have specified the same answers for several questions. These conditions correspond to the

Q&A profile settings that are part of the Q&A policy. For more information, see [Configuring Q&A Profile Settings](#) on page 72. For more information on configuring this enforcement rule, see [Invite Users to Create/Update Profiles](#) on page 123.

Note that only one email notification is sent to each user. If you want to remind users that they should register with Password Manager or update their Q&A profiles and send multiple emails, enable and configure the **Remind users to create/update Q&A profiles** enforcement rule.

The **Remind users to create/update Q&A profiles** enforcement rule can notify users via email. When configuring this rule, you can specify several notification scenarios. For each scenario, you should set the time period since the invitation date.

For more information on configuring this enforcement rule, see [Remind Users to Create/Update Profiles](#) on page 126.

If you want to configure different notification scenarios for different user groups, you can create several Management Policies, and within each Management Policy configure the **Remind users to create/update Q&A profiles** enforcement rule appropriately for different user groups.

Questions and Answers Policy Overview

Questions and Answers policy consists of secret questions and Q&A profile settings. Secret questions are questions that users must answer to create their profiles and then use the profiles for authentication. You can create question lists in multiple languages. Each question list contains mandatory, optional, and helpdesk questions. When creating profiles, users must answer all mandatory and helpdesk questions, and a specified number of optional and user-defined questions. You can specify the required number of question in the Q&A profile settings.

When authenticating on the Self-Service Site with Q&A profiles, users can use mandatory, optional and user-defined questions from their profiles. When a helpdesk operator authenticates users, the operator can use mandatory and helpdesk questions from users' profiles.

Q&A profile settings are a collection of settings that define the number of user-defined and optional questions required for registration, minimum length of answers, encryption setting for storing answers, and others.

Q&A Policy and Authentication

When you configure the Q&A policy, you should remember that the settings you specify may affect the authentication process. The following authentication activities use the Q&A policy settings:

- **Authenticate with Q&A profile (random questions):** This activity is used in self-service workflows. It relies on the number of secret questions you specify in the activity. If a user's profile contains fewer questions, you can select whether to authenticate the user or not. For more information, see [Authenticate with Q&A Profile \(Random Questions\)](#) on page 95.
- **Authenticate with Q&A profile (specific questions):** This activity is used in self-service workflows. It relies on the specific secret questions you specify in the activity. If the specified questions cannot be found in a user's profile, the user will not be authenticated. For more information, see [Authenticate with Q&A Profile \(Specific Questions\)](#) on page 96.
- **Authenticate with Q&A profile (user-selected questions):** This activity is used in self-service workflows. It relies on the number and type of secret questions you specify in the activity. Users will be able to choose questions to authenticate with from their profile's answered questions. If the user's profile contains fewer questions than the set minimum, you can select whether to authenticate the user or not. For more information, see [Authenticate with Q&A Profile \(User-selected questions\)](#)
- **Authenticate with Q&A profile:** This activity is used in helpdesk workflows. It relies on the specific secret questions you specify in the activity and on the **Store answers using reversible encryption** option that you specify in the Q&A profile settings. If the specified questions cannot be found in a user's profile, the user will not be authenticated.

This activity uses mandatory and helpdesk questions. Helpdesk questions are always stored using reversible encryption. Mandatory questions are hashed, unless you select the **Store answers using reversible encryption** option in the Q&A profile settings. Note, that if mandatory questions are hashed, you will not be able to use the activity option that specifies that helpdesk operators verify user identity by comparing the answers provided by users with the displayed answers (the **Answers to the specified questions (user's answer is shown)** option). For more information, see [Authenticate with Q&A Profile](#).

Q&A Policy and User Enforcement

The **Q&A profile settings** affects the **Invite users to create/update Q&A profiles** enforcement rule. This rule has conditions that state when users should be notified to create or update their profiles. These conditions correspond to the Q&A profile settings. For example, the **User's answers are shorter than required** condition corresponds to the **Minimum length of answers** setting. So, when you change any of the Q&A profile settings, you can then select the corresponding condition in the rule and enforce users to create or update their profiles in accordance with the new settings. For more information, see [Invite Users to Create/Update Profiles](#) on page 123.

Data Replication

This section provides information on how Password Manager stores and replicates data.

Storing Data

There are two types of data stored by Password Manager: Password Manager configuration data and users' Q&A profiles. Password Manager configuration data contains all settings you configure in Password Manager. Users' Questions and Answers profiles are stored apart from the configuration data.

Q&A profiles are stored in the attribute of a user account in AD LDS that you specify during instance initialization. By default, it is the comment attribute. You can also change it after initializing a Password Manager instance; for more information, see [Instance Reinitialization](#) on page 159.

Password Manager configuration data is stored in the C:\ProgramData\One Identity\Password Manager for AD LDS folder. This folder contains two files (Shared.storage and Local.storage) and the LocalizationStorage folder.

The Shared.storage file contains configuration data that is shared among all instances of a realm: **Management Policies, General Settings, AD LDS connections, Custom Activities and Workflows, instance settings**, and so on.

The Local.storage file contains the instance-specific settings, such as the instance name and statistics about scheduled tasks.

The LocalizationStorage folder contains the user interface texts localized in several languages.

Replicating data

If you install a realm (several Password Manager instances sharing the same configuration), changes in the configuration of one instance are automatically propagated to other instances. To propagate the data, Password Manager replicates the data from the shared.storage file and the LocalizationStorage folder to Active Directory.

Before being written to Active Directory, the data is split into several segments and archived.

To distribute the configuration data from one instance to another, Password Manager uses a scheduled task and the PMReplication container in a managed domain to which the data is copied. The PMReplication container is a container that is automatically created in the Users container of the managed domain. To this container, containers for each Password Manager realm are added.

Names of these containers correspond to the realm affinity ID. Each realm container has the containers for every instance belonging to this realm. Names of instance containers correspond to the instance ID.

In the instance container, several user accounts are created. The number of user accounts is one more than the number of data segments. For example, if there are 20 data segments, then the instance container has 21 user accounts. Note that the created user accounts are disabled.

The same attribute that you specify for storing users' Q&A profiles is used to store the configuration data segments. The first user account stores the data replica ID, all other accounts store the data segments.

Replication mechanism analyses all data segments from all instances, selects data with the latest changes, and propagates it.

CAUTION: It is not recommended to edit Password Manager settings simultaneously on multiple instances belonging to one realm. Simultaneous modification of settings on multiple Password Manager instances may cause data loss.

Note that the domain management account must have the permission to create user accounts and containers in the Users container for configuration data to be replicated. For more information on configuring the domain management account, see [Configuring Permissions for Access Account](#).

Changing replication settings

By default, the data to be replicated is divided into segments by segment size (100 KB). Data can also be divided into segments according to a specified segment number.

You can also change the name of the storage container (by default, PMReplication) and the location for storing this container (by default, the Users container of a managed domain), and the names of user accounts used to store data segments.

You can change replication settings by modifying the `QPM.Service.Host.exe.config` file located in the `<Password Manager installation folder>\Service folder`.

CAUTION: Editing the configuration file may cause serious problems. It is recommended to back up the file before modifying it. Edit the `QPM.Service.Host.exe.config` file at your own risk.

Changing replication settings

1. On the computer where Password Manager is installed, open the `QPM.Service.Host.exe.config` file located in the `<Password Manager installation folder>\Service folder` with a text editor.
2. In the **replication** node, specify the following:

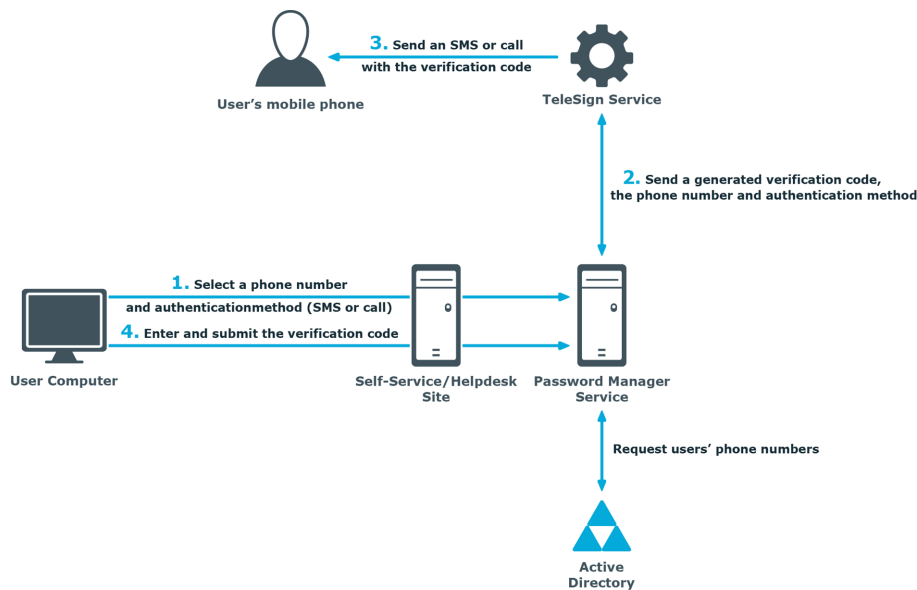
- To divide the configuration data into segments by a segment size, set the `packetLimitMode` to `LimitSize` (`packetLimitMode="LimitSize"`).
 - To divide the configuration data into segments by a number of segments, set the `packetLimitMode` to `LimitCount` (`packetLimitMode="LimitCount"`).
 - If you set the `packetLimitMode` to `LimitSize`, specify the maximum segment size in bytes in the `maxPacketSize` parameter. For example, `maxPacketSize="100000"`. Set the `maxPacketsCount` parameter to zero (`maxPacketsCount="0"`).
 - If you set the `packetLimitMode` to `LimitCount`, specify the maximum number of segments to be created in the `maxPacketsCount` parameter. For example, `maxPacketCount="10"`. Note, that this value must be greater than 1. Set the `maxPacketsSize` parameter to zero (`maxPacketsSize="0"`).
3. In the `storageManager` node, specify the following:
 - To change the name of the storage container, in the `storageContainerReplicationPath` element specify the required name. The default value is `CN=PMReplication`.
 - To change the container for storing replication data, in the `storageContainerPath` element specify the required container. The default value is `CN=Users`.
 - To change the names of user accounts used to store data segments, in the `storageContainerPartName` element specify the required name. The default value is `strg`.
 4. Save the `QPM.Service.Host.exe.config` file.
 5. Restart the Password Manager Service in the **Services** console. Type `services.msc` at a command prompt, select **Password Manager Service** in the console, and click **Restart**.
 6. Repeat steps 1-4 on each instance belonging to a Password Manager realm.

Phone-based authentication service overview

One of the authentication options Password Manager for AD LDS offers is phone-based authentication, allowing you to require users to enter a verification code on the Self-Service Site or Helpdesk Site. The verification code can be sent as an SMS or automated call.

This phone-based authentication service is provided by TeleSign.

About phone-based authentication in Password Manager for AD LDS



When starting a workflow containing phone-based authentication, Password Manager for AD LDS checks if the phone-based authentication service is configured. The workflow runs only if phone-based authentication is configured and working.

1. On the Self-Service Site or Helpdesk Site, a user selects their preferred phone number and verification method (SMS or automated call). This data is sent to Password Manager for AD LDS, which then gets the phone numbers from the Active Directory attributes specified in the workflow settings.
2. Password Manager for AD LDS then generates a verification code and transfers the code, selected phone number, and verification method to the TeleSign Service.

NOTE: The data is sent via HTTPS and the generated verification code is stored until the workflow ends. Only one code is stored at a time.

3. The TeleSign Service sends an automated call or SMS to the user's mobile phone with the verification code. The language of the automated call depends on the user interface language of the Self-Service Site or Helpdesk Site.
4. The user enters the verification code on the Self-Service Site, then the code is sent to Password Manager for AD LDS.
5. Password Manager for AD LDS checks the verification code. If it is correct, Password Manager for AD LDS gives access to the user to further steps on the Self-Service Site.

Using phone-based authentication in Password Manager for AD LDS

To use phone-based authentication on the Self-Service Site and Helpdesk Site, add the **Authenticate via Phone** activity to the self-service and helpdesk workflows. When configuring this activity, you can specify the AD LDS attributes from which the phone numbers will be retrieved, along with the available authentication methods (SMS or automated voice call).

Phone-based authentication also supports phone numbers that belong to Private Branch Exchange (PBX). PBX phones require either a live switchboard operator or an automated attendant to complete the call. By default, Password Manager supports the automated attendant scenario.

To configure the operator type for a PBX phone number

1. Open the `QPM.Service.Host.exe.config` file.
2. Set the `PhoneNumberExtensionType` parameter as follows:
 - For an automated attendant, set the parameter value to **1**.
 - For live operators, set the parameter value to **2**.
3. To dial DTMF digits, set the `PhoneNumberExtensionType` parameter to **1**.
4. (Optional) In the `PhoneNumberExtensionTemplate` parameter, include commas. Each comma represents a one-second pause in the dialing sequence. To increase the pause in the dialing sequence, include additional commas in the `PhoneNumberExtensionTemplate` parameter.

NOTE: You must configure the phone number extension with the extension separator in AD LDS. Phone numbers with an extension must have the words `Extension`, `Ext`, `Extn`, `x` or `X` in them to separate the extension number from the phone number, as shown in the following examples:

- +91-98881234567 Extension 1234
- +91-98881234567 Ext 1234
- +91-98881234567 Extn 1234
- +91-98861234567 x 1234
- +91-98861234567 Ex 1234

For more information on configuring this activity, see [Authenticate via phone in a self-service workflow](#) and [Authenticate via phone in a helpdesk workflow](#).

Configuring phone-based authentication for Password Manager for AD LDS

To use the phone-based authentication service in your workflows, you must configure it in the Password Manager for AD LDS Administration Site.

Prerequisites

To configure phone-based authentication for your workflows, the following conditions must be met:

- You must have a valid TeleSign license.
- You must have the required TeleSign API key and customer ID available for configuring the service.
- Outbound SSL connections must be allowed from the computer on which the Password Manager Service and Password Manager Workflow Service run to the following address:

`https://*.telesign.com`

Replace * with any valid subdomain name in the above URL, for example:

- `https://api.telesign.com`
- `https://www.telesign.com`

To configure phone-based authentication

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Phone Authentication**.
2. In **API key**, specify your TeleSign API key.
3. In **Customer ID**, specify your TeleSign customer ID.
4. To test your settings, in **Enter phone number**, specify a valid phone number, then select the authentication method (**SMS** or **Automated voice call**) that you want to use during testing.
5. To test your phone authentication settings, click **Test settings**.

TIP: If any errors occur during testing, then verify that:

- The specified **API key** and **Customer ID** are correct.
- The TeleSign services are up and running.
- Your internet connection is working.

6. To apply your changes, click **Save**.

Configuring Management Policy

After initializing the Administration Site, you need to configure the default Management Policy to enable users to use the Self-Service Site.

The required settings you need to configure for the Management Policy are a user scope and secret questions.

Configuring Permissions for Access Account

When you connect to an AD LDS instance, you can create a new connection or use existing connections, if any. When creating the connection, you must specify an access account - an account under which Password Manager will access the AD LDS instance and a specified application directory partition. You can use the Password Manager Service account, an Active Directory account or an AD LDS account. These accounts must have the following minimum set of permissions:

- Membership in the **Domain Users** group (for the Password Manager Service account and the Active Directory account)
- Membership in the **Readers** group in the application directory partition (for the AD LDS account)
- Membership in the **Administrators** group in the configuration directory partition
- The Read permission for all attributes of user objects
- The Write permission for the following attributes of user objects: **pwdLastSet**, **Comment**, **unicodePwd**, **lockoutTime**, **msDS-UserAccountDisabled**

NOTE: If the **Storage attribute** for **Security questions** under **Reinitialization** page is a custom value (say **userParameters**), then the Write permissions must be provided for that attribute instead of **Comment** attribute.

- The right to reset user passwords
- The permission to create user accounts and containers in the Users container
- The Read permission for attributes of the **organizationalUnit** object and container objects
- The Write permission for the **gpLink** attribute of the **organizationalUnit** objects and container objects
- The Read permission for the attributes of the container and **serviceConnectionPoint** objects in Group Policy containers
- The permission to create container objects in the **System** container
- The permission to create the **serviceConnectionPoint** objects in the **System** container

- The permission to delete the `serviceConnectionPoint` objects in the **System** container
- The Write permission for the keywords attribute of the `serviceConnectionPoint` objects in the **System** container

If you want to use the same connection in password policies as well, make sure the account has the following permissions:

- The Read permission for attributes of the `groupPolicyContainer` objects.
- The Write permission to create and delete the `groupPolicyContainer` objects in the System Policies container.
- The permission to create and delete container and the `serviceConnectionPoint` objects in Group Policy containers.
- The Read permission for the attributes of the container and `serviceConnectionPoint` objects in Group Policy containers.
- The Write permission for the `serviceBindingInformation` and `displayName` attributes of the `serviceConnectionPoint` objects in Group Policy containers.

Corporate Authentication

In the **Register** workflow, if the administrator selects **Corporate authentication** check box, the user can only review the corporate account details during registration. If **Allow user to edit corporate details** is selected, the user can update their respective corporate details, such as **Corporate email** or **Corporate phone number**, if the administrator did not previously populate the details in Active Directory (AD).

If **Corporate authentication** registration mode is selected in the **Register** activity, make sure that **Domain management account** has the following set of permissions.

1. The read permission for **Corporate email** attribute and **Corporate phone** attribute where, **Mobile** is the default attribute for the **Corporate phone**.
2. If **Allow user to edit corporate details** is selected under **Corporate authentication**, both Read and Write permission must be available for **Corporate email** attribute and **Corporate phone** attribute, where **Mobile** is the default attribute for the **Corporate phone**.

NOTE: If the **Corporate phone** attribute under **Reinitialization** page is a custom value (for example, `pager`), the Read/Write Permissions must be provided for that attribute instead of the `mobile` attribute.

Connecting to AD LDS Instance

After adding a connection to the user scope, you need to specify groups from the application directory partition that can access the Self-Service Site. By default, the group "Users" is included in the scope when you add the connection to the user scope. You can also restrict some groups from accessing the Self-Service Site.

To connect to AD LDS instance

1. Open the Administration Site by entering the Administration Site URL in the address bar of your browser. By default, the URL is `http(s)://<ComputerName>/PMAAdminADLDS`, where `<ComputerName>` is the name of the computer on which Password Manager is installed.
2. On the Password Manager Administration Site, select the Management Policy you want to configure and select **User Scope**.
3. On the **User Scope** page, click **Connect to AD LDS instance**.
4. If connections already exist, select a connection from the list.

If you want to create a new connection, click **Add new connection**.

5. To create a new connection, configure the following options in the **Connect to AD LDS Instance** dialog:
 - In the **Server name on which AD LDS instance is installed** text box, type the name of the server to which you want to connect.
 - In the **Port number (LDAP or SSL)** text box, enter the port number that you specified when installing the AD LDS instance. If you select the **Use SSL** check box, enter the SSL port number; otherwise, LDAP port number. It is recommended to use SSL in your production environment.

NOTE: These port settings are valid for the Self-Service Site and Helpdesk Site. To log in to the Password Manager Administration Site with LDAP over SSL, you have to create the registry key for LDAPS in the registry. For more information, see [Enabling LDAP over SSL](#).

- In the **Application directory partition** text box, enter the name of the application directory partition from the AD LDS instance to which you want to connect.
- In the **Application directory partition alias** text box, type the alias for the application directory partition which will be used to address the partition on the Self-Service Site.
- In the **Access account** section, select **Password Manager Service account** to have Password Manager access the AD LDS instance using the Password Manager Service account, otherwise, select **The following Active Directory account** or **The following AD LDS account** and enter the required user name and password.

For information on how to prepare the access account, see [Configuring Permissions for Access Account](#).

6. Click **Save**.

NOTE: When you add an AD LDS instance to the user scope, the group "Users" from the specified application directory partition is automatically included in the user scope.

To specify groups or OUs that are allowed to access the Self-Service Site

1. On the Administration Site, select the Management Policy you want to configure and click the **User Scope** link.
2. On the **User Scope** page, select the connection for which you want to specify groups or OUs and click **Edit**.
3. Do the following:
 - To specify the groups, under **Groups allowed access to the Self-Service Site** click **Add**.
 - To specify the OUs, under **Organizational Units allowed access to the Self-Service Site** click **Add**.
4. Click **Save**.

NOTE: If you have the **Domain Management account** configured with a user other than the Active Directory Administrator, then provide **Security** permissions to:

- All the groups
- All the OUs that are added as **Included groups**
- All **Included OUs** in the user scope

If the users/ groups/ OUs included in the user scope, are a member of Readers/ Administrators group in the ADLDS then, the Write Permissions are already inherited.

To specify groups or OUs that are denied access to the Self-Service Site

1. On the Administration Site, select the Management Policy you want to configure and click the **User Scope** link.
2. On the **User Scope** page, select the connection for which you want to specify groups or OUs and click **Edit**.
3. Do the following:
 - To specify the groups, click **Add** under **Groups denied access to the Self-Service Site**.
 - To specify the OUs, click **Add** under **Organizational Units denied access to the Self-Service Site**.
4. Click **Save**.

Changing Access Account

To access a managed AD LDS instance, you can use the Password Manager Service account, an Active Directory account or an AD LDS account. For more information on how to configure the access account, see [Configuring Permissions for Access Account](#) on page 55. Password Manager Service account is the account that was configured during Password

Manager installation. Password Manager Service account may be used as the access account only when the Service account has all required permissions.

To modify account used to access an AD LDS instance

1. On the Administration Site, select the Management Policy you want to configure and click the **User Scope** link.
2. On the **User Scope** page, select the connection for which you want to change access account and click **Edit**.
3. On the **User Scope Settings for #Application Directory Partition#** page, click **Edit**.
4. In the **Access account** section of the **Edit AD LDS Instance Connection** dialog, select **Password Manager Service account** to have Password Manager access the managed instance using the Password Manager Service account. Otherwise, select **The following Active Directory account** or **The following AD LDS account**, then enter the required user name and password.
5. Click **Save** and select how you want to apply the updated settings. You can either apply the new settings for this user scope only, or everywhere where this connection is used.

Removing Connection to AD LDS Instance

This section describes how to remove a connection to an AD LDS instance.

To remove a connection to AD LDS instance

1. On the Administration Site, select the Management Policy you want to configure and click the **User Scope** link.
2. On the **User Scope** page, select the connection you want to delete and click **Remove**. If you want to permanently remove the connection, remove it everywhere where it is used, then on the **General Settings > AD LDS Instance Connections** tab, click **Remove** under the required connection.

NOTE: The connection will be removed from the selected user scope only

Adding Secret Questions

Secret questions are the main part of the Questions and Answers policy that allows authenticating users on the Self-Service Site before users can perform any self-service tasks.

For more information on the Questions and Answers policy, see [Configuring Questions and Answers Policy](#) on page 68.

To create secret questions in the default language

1. Open the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http(s)://<ComputerName>/PAdminADLDS/`.
2. On the Administration Site home page, under the Management Policy that you want to configure, click **Add secret questions**.
3. On the **Configure Questions and Answers Policy** page, click **Add questions in the default language**.
4. In the **Edit Questions in the Default Language** dialog, specify mandatory, optional and helpdesk questions. To change the default language for secret questions click **Change language**.
5. To change the order of the questions, click the appropriate links.
6. To save the questions, click **Save**.

NOTE: Modifying a question list does not affect existing personal Questions or Answers profiles unless the users have to update their profiles as a result of the enforcement rules that require users to update Q&A profiles when the question list is modified. For more information on the enforcement rules, see [User Enforcement Rules](#) on page 123.

Editing and Deleting secret questions

Translation of questions can be made only to the questions that have been added in the default language.

To delete questions of a default language

1. To open the Administration Site, enter the Administration Site URL in the address bar of your web browser. By default, the URL is `http(s)://<ComputerName>/PAdminADLDS/`.
2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy.
3. On the **Configure Questions and Answers Policy** page, click **Edit questions** under **Question List**. The **Edit Questions in the Default Language** page appears.
4. Click **X** against the question that has to be deleted, then click **Save**.

To delete questions of a specific language

1. To open the Administration Site, enter the Administration Site URL in the address bar of your web browser. By default, the URL is `http(s)://<ComputerName>/PAdminADLDS/`.

2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy.
3. On the **Configure Questions and Answers Policy** page, click the language for which the questions have to be deleted. The **Translate Questions** page appears.
4. Click **Delete questions**, then click **OK**.

To Edit questions of a default language

1. On the home page of the Administration Site, click **Q&A Policy** link under the Management Policy.
2. On the **Configure Questions and Answers Policy** page, under **Questions List**, click the **Edit questions** link.
3. In the **Edit questions in the Default Language** page, edit the required question.
4. Click **Save**.

To Edit questions of a specific language

1. On the home page of the Administration Site, click **Q&A Policy** link under the Management Policy.
2. On the **Configure Questions and Answers Policy** page, navigate to the **Translations:** section and click the language for which the questions have to be edited.
3. In the translated text box against each of the questions, edit the required question.
4. Click **Save**.

IMPORTANT:

- **Q&A Policy** supports multiple languages. It requires the Password Manager Administrator to configure the required languages for the users to see the same in the Self service site.
- **Change language** link appears in the Self-Service Site only when the Password Manager administrator has translated the questions in the required languages.

Management Policies

- Checklist: Configuring Password Manager
- Understanding Management Policies
- Adding or cloning a new Management Policy
- Configuring Access to the Administration Site
- Configuring Access to the Password Manager Self-Service Site
- Configuring Access to the Helpdesk Site
- Configuring Questions and Answers Policy
- Workflow overview
- Custom workflows
- Custom Activities
- Password Manager Self-Service Site workflows
- Helpdesk Workflows
- User Enforcement Rules

Checklist: Configuring Password Manager

When you have installed Password Manager, follow this checklist to configure the solution to implement automated and secure password management in an AD LDS instance.

Table 2: Checklist to configure Password Manager

Step	Reference
Prepare an access account to AD LDS instance.	Configuring Permissions for Access Account on page 55

Step	Reference
Configure a user scope.	
Configure the Questions and Answers policy: create language-specific question lists, and configure Q&A profile settings if required.	Adding Secret Questions on page 59
Configure a helpdesk scope to grant access permissions for the Helpdesk Site to helpdesk operators and delegate administrative tasks.	Configuring Access to the Helpdesk Site on page 65
Configure self-service and helpdesk workflows to define what tasks will be available on the Self-Service and Helpdesk sites.	Password Manager Self-Service Site workflows Helpdesk Workflows on page 110
If required, configure rules for enforcing users to register with Password Manager.	User Enforcement Rules on page 123
Configure general settings that apply to all Management Policies (such as account search options, SMTP servers, scheduled tasks, and so on.)	General Settings Overview on page 131
Create password policies and configure password policy rules.	Creating a Password Policy on page 188
Ensure that all Password Manager users have JavaScript enabled in their browser settings.	
Ensure that the users know the Self-Service Site URL and can access the site to register and perform password self-management tasks.	

Understanding Management Policies

Management Policy is a core element of Password Manager. Using the Management Policy you can configure workflows for registering new users, resetting passwords, and others. For each Management Policy you can configure a user scope, and delegate helpdesk tasks by configuring a helpdesk scope. You can configure multiple Management Policies with different user and helpdesk scopes, workflows and secret questions. The default Management Policy with preconfigured workflows is available out of the box.

A Management Policy consists of the following components:

- Questions and Answers policy
- User scope
- Helpdesk scope

- Workflows
- User enforcement rules

User scope is a group or several groups of users managed by Password Manager. When configuring the user scope for a Management Policy, you can add connections to multiple AD LDS instances.

Helpdesk scope is a group of helpdesk operators who are allowed to manage users from the user scope of the same Management Policy. By configuring the helpdesk scope you can delegate administrative tasks to specified helpdesk operators. For more information about the helpdesk scope, see [Configuring Access to the Helpdesk Site](#) on page 65.

Questions and Answers policy (Q&A policy) is a policy within which secret questions and Q&A profile settings are defined. Secret questions are a set of mandatory, optional and helpdesk questions for users' Questions and Answers profiles. These questions are used to register users with Password Manager and later to authenticate users when they use the Self-Service Site. Q&A profile settings define how many questions a user must answer to create Q&A profile settings and set requirements for user's questions and answers. For more information about Q&A policy, see [Configuring Questions and Answers Policy](#) on page 68.

All **workflows** are divided into two categories: self-service and helpdesk workflows. The self-service workflows define the tasks available to users on the Self-Service Site, that is, every configured workflow is a task on the Self-Service Site. The helpdesk workflows define what tasks are available to helpdesk operators on the Helpdesk Site. A workflow consists of several activities that you can add to or remove from the workflow to customize it.

The **Default Management Policy** offers preconfigured workflows. You can also create your own workflows. For more information about workflows, see [Workflow overview](#) on page 74.

User enforcement rules allow you to set up the enforcement schedule to invite users to create or update their Q&A profiles and configure the reminder that will notify users to change passwords before password expiration. For more information, see [User Enforcement Rules](#) on page 123.

Adding or cloning a new Management Policy

In the Password Manager Administration Site, you can add or clone a new Management Policy.

To create a new Management Policy

- Enter the name of the new Management Policy in the **Name** text box.

To clone an existing Management Policy

1. In the Password Manager Administration Site, click **Add new Management policy**.
2. Check **Clone existing Management Policy**.
3. Select a Management Policy to clone from the list of already existing Management Policies.

Configuring Access to the Administration Site

By default, the access to the Administration Site is granted only to the domain user from the AD, who is a member of the local Administrators group and to the PMAAdminADLDS group which is created during Password Manager for AD LDS installation.

NOTE: The account that you specified as Application Pool Identity when installing Password Manager is automatically added to the PMAAdminADLDS group.

IMPORTANT: Make sure to grant access to the Administration Site only to the most trustworthy people, since managing the Password Manager configuration may require dealing with user-sensitive information.

Configuring Access to the Password Manager Self-Service Site

To configure access to the Self-Service Site, you need to configure a user scope for the Management Policy you want to use. The workflows and secret questions that you configure for the Management Policy will apply only to the user scope of this Management Policy. You can add connections to several AD LDS instances to a single user scope.

Configuring Access to the Helpdesk Site

In Password Manager you can easily delegate administrative tasks to dedicated helpdesk operators. By configuring the helpdesk scope you select groups of helpdesk operators who will have access to the Helpdesk Site. The Helpdesk Site handles typical tasks performed by helpdesk operators, such as resetting passwords, unlocking user accounts, assigning temporary passcodes, and others.

Members of the helpdesk scope are allowed to access the Helpdesk Site and manage users from the user scope of the same Management Policy only.

You can also restrict groups of helpdesk operators from accessing the Helpdesk Site.

To configure a helpdesk scope, you need to add a connection to an AD LDS instance to the scope at first, and then specify groups that will be allowed or denied access to the Helpdesk Site.

To manage all connections from a single place, click **General Settings > AD LDS Instance Connections** on the Administration Site. For more information, view [AD LDS Instance Connections](#) on page 163.

To connect to AD LDS instance

1. Open the Administration Site by entering the Administration Site URL in the address bar of your browser. By default, the URL is `http(s)://<ComputerName>/PMAdminADLDS`, where `<ComputerName>` is the name of the computer on which Password Manager is installed.
2. On the Administration Site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.
3. On the **Helpdesk Scope** page, click **Connect to AD LDS instance**.
4. If connections already exist, select a connection from the list. If you want to create a new connection, click **Add new connection**.
5. If you selected to create the new connection, in the **Connect to AD LDS Instance** dialog, configure the following options:
 - In **Server name on which AD LDS instance is installed**, type the name of the server to which you want to connect.
 - In **Port number (LDAP or SSL)**, enter the port number that you specified when installing the AD LDS instance. If you select **Use SSL**, enter the SSL port number; otherwise, LDAP port number. It is recommended to use SSL in your production environment.
 - In **Application directory partition**, enter the name of the application directory partition from the AD LDS instance to which you want to connect.
 - In **Application directory partition alias**, type the alias for the application directory partition which will be used to address the partition on the Self-Service Site.
 - In the **Access account** section, select **Password Manager Service account** to have Password Manager access the AD LDS instance using the Password Manager Service account, otherwise, select **The following Active Directory account** or **The following AD LDS account** and enter the required user name and password.

For information on how to prepare the access account, see [Configuring Permissions for Access Account](#) on page 55.

6. Click **Save**.

To specify groups or OUs that are allowed to access the Helpdesk Site

1. On the Administration Site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.
2. On the **Helpdesk Scope** page, select the connection for which you want to specify groups or OUs and click **Edit**.
3. Do the following:
 - To specify the groups, click **Add** under **Groups allowed access to the Helpdesk Site**.
 - To specify the OUs, click **Add** under **Organizational Units allowed access to the Helpdesk Site**.
4. Click **Save**.

To specify groups that are denied access to the Helpdesk Site

1. On the Administration Site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.
2. On the **Helpdesk Scope** page, select the connection for which you want to specify groups or OUs and click **Edit**.
3. Do the following:
 - To specify the groups, click **Add** under **Groups denied access to the Helpdesk Site**.
 - To specify the OUs, click **Add** under **Organizational Units denied access to the Helpdesk Site**.
4. Click **Save**.

Changing Access Account

To access a managed AD LDS instance, you can use the Password Manager Service account, an Active Directory account or an AD LDS account. For more information on how to configure the access account, see [Configuring Permissions for Access Account](#) on page 55. Password Manager Service account is the account that was configured during Password Manager installation. Password Manager Service account may be used as the access account only when the Service account has all required permissions.

To modify account used to access an AD LDS instance

1. On the Administration Site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.
2. On the **Helpdesk Scope** page, select the connection for which you want to change access account and click **Edit**.
3. On the **Helpdesk Scope Settings for #Application Directory Partition#** page, click **Edit**.

4. In the **Access account** section of the **Edit AD LDS Instance Connection** dialog, select **Password Manager Service account** to have Password Manager access the managed instance using the Password Manager Service account. Otherwise, select **The following Active Directory account** or **The following AD LDS account** and then enter the required user name and password.
5. Click **Save** and select how you want to apply the updated settings. You can either apply the new settings for this helpdesk scope only, or everywhere where this connection is used.

Removing Connection to AD LDS Instance

This section describes how to remove a connection to an AD LDS instance.

To remove a connection to AD LDS instance

1. On the Administration Site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.
2. On the **Helpdesk Scope** page, select the connection you want to delete and click **Remove**.

NOTE: The connection will be removed from this helpdesk scope only. If you want to permanently remove the connection, remove it everywhere where it is used, then on the **General Settings > AD LDS Instance Connections** tab, click **Remove** under the required connection.

Configuring Questions and Answers Policy

Questions and Answers policy allows you to create secret questions and specify Q&A profile settings. Secret questions are questions to which users provide answers when registering with Password Manager. Using the Q&A profile settings you can specify requirements for user's questions and answers. For example, you can prevent users from using the same answer for multiple questions.

Q&A policy settings affect user authentication and registration enforcement process. For more information, see [Questions and Answers Policy Overview](#) on page 47.

Creating Secret Questions

Secret questions are questions to which users provide their own answers, thus creating a personal Questions and Answers profile. Before users can register with Password Manager

by creating their personal Questions and Answers profiles, you must configure a question list containing the questions that will be presented to users.

You can create the question list in several languages, so that users can select a preferred language of questions and answers.

Password Manager uses personal Question and Answers profiles as an authentication method to allow users and helpdesk operators to manage user passwords in AD LDS instances and in multiple connected systems. A Q&A profile, or personal profile, is a set of questions specified by the Password Manager administrator, to which users must provide their secret answers that later can be used to authenticate the users. You can also require users to specify their own questions in their personal profiles. Then, users can securely reset their passwords or unlock their accounts by answering a series of questions from their personal profiles.

You can set requirements for answers that users specify in their Questions and Answers profiles. For example, you can prevent users from specifying the same answer for different questions, or set a minimum answer length. For more information, see [Configuring Q&A Profile Settings](#) on page 72.

Password Manager allows you to specify criteria for recognizing users' Questions and Answers profiles as not compliant with the current password management settings. This is essential if you want users to update their profiles each time when Q&A policy settings are changed. Helpdesk operators can force users to update their Q&A profiles if the profiles do not comply with current Q&A policy.

For information on how to enforce update of Q&A profiles, see [User Enforcement Rules](#) on page 123.

Secret questions can contain the following types of questions:

Table 3: Secret questions

Question type	Description
Mandatory questions	Questions of this type are an integral part of a user's Q&A profile. Users must provide an answer to each of these questions. These questions can be stored using reversible encryption or hashed.
Optional questions	Users can select what optional questions to answer. Administrator specifies only the number of questions that users must answer. These questions can be stored using reversible encryption or hashed.
Helpdesk questions	Security questions used by helpdesk to verify user's identity before performing password- and account management tasks. These questions are always stored using reversible encryption.
User-defined	Questions that must be created by the user.

For users to be able to create their personal Questions and Answers profiles, you must specify at least one secret question.

To create secret questions in the default language

1. Open the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http(s)://<ComputerName>/PAdminADLDS/`.
2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy you want to configure.
3. On the **Configure Questions and Answers Policy** page, select the default language for secret questions by clicking the language link in the **Default language** option.
4. Under **Question List**, click the **Edit questions** link to specify mandatory, optional and helpdesk questions in the default language.
5. In the **Edit Questions in the Default Language** dialog, specify mandatory, optional and helpdesk questions.
6. Change questions' order by clicking the appropriate links.
7. Click **Save** to save the questions and close the dialog.

IMPORTANT: If you add a questions to the question list in the default language, all translations of the question list will not be configured until you change them accordingly. This means that users will not be able to use the disabled languages for creating Q&A profiles. If you remove a question from the question list in the default language, this question will be automatically removed from translations of the question list.

IMPORTANT: Modifying a question list does not affect existing personal Questions or Answers profiles unless the users have to update their profiles as a result of the enforcement rules that require users to update Q&A profiles when the question list is modified. For more information on the enforcement rules, see [User Enforcement Rules](#) on page 123.

To translate secret questions

1. Open the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http(s)://<ComputerName>/PAdminADLDS/`.
2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy you want to configure.
3. On the **Configure Questions and Answers Policy** page, under **Question List**, click the **Translate questions** link.
4. In the **Select Additional Language** dialog, select an additional language for secret questions.
5. In the **Translate Questions** dialog, translate mandatory, optional and helpdesk questions from the default language into the additional language.

6. To change the language, click the **Change language** link.
7. To temporarily hide secret questions in the selected language, select the **Make questions in this language unavailable to users** check box. This setting will prevent users from creating or updating their Q&A profiles using the question list in this language.
8. Click **Save** to save changes and close the dialog.

IMPORTANT: If you deleted the translated question list, all users who have created their Questions and Answers profiles will be forced to update their Q&A profiles, if you have configured the enforcement rule. For more information, see [Invite Users to Create/Update Profiles](#) on page 123.

Editing and Deleting secret questions

Translation of questions can be made only to the questions that have been added in the default language.

To delete questions of a default language

1. To open the Administration Site, enter the Administration Site URL in the address bar of your web browser. By default, the URL is `http(s)://<ComputerName>/PMAAdminADLDS/`.
2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy.
3. On the **Configure Questions and Answers Policy** page, click **Edit questions** under **Question List**. The **Edit Questions in the Default Language** page appears.
4. Click **X** against the question that has to be deleted, then click **Save**.

To delete questions of a specific language

1. To open the Administration Site, enter the Administration Site URL in the address bar of your web browser. By default, the URL is `http(s)://<ComputerName>/PMAAdminADLDS/`.
2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy.
3. On the **Configure Questions and Answers Policy** page, click the language for which the questions have to be deleted. The **Translate Questions** page appears.
4. Click **Delete questions**, then click **OK**.

To Edit questions of a default language

1. On the home page of the Administration Site, click **Q&A Policy** link under the Management Policy.
2. On the **Configure Questions and Answers Policy** page, under **Questions List**, click the **Edit questions** link.
3. In the **Edit questions in the Default Language** page, edit the required question.
4. Click **Save**.

To Edit questions of a specific language

1. On the home page of the Administration Site, click **Q&A Policy** link under the Management Policy.
2. On the **Configure Questions and Answers Policy** page, navigate to the **Translations:** section and click the language for which the questions have to be edited.
3. In the translated text box against each of the questions, edit the required question.
4. Click **Save**.

IMPORTANT:

- **Q&A Policy** supports multiple languages. It requires the Password Manager Administrator to configure the required languages for the users to see the same in the Self service site.
- **Change language** link appears in the Self-Service Site only when the Password Manager administrator has translated the questions in the required languages.

Configuring Q&A Profile Settings

Q&A profile settings allow you to define settings and requirements for user's questions and answers. For example, you can prevent users from using the same answer for multiple questions. Questions and answers that do not comply with the policy will not be accepted.

To configure Questions and Answers policy

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the Administration Site home page, click the **Q&A Policy** link under the Management Policy you want to configure.

3. On the **Configure Questions and Answers Policy** page, click the **Q&A profile settings** link.
4. In the **Q&A Profile Settings** dialog, specify the following options:

Table 4: Questions and Answers profile settings

Option	Description
Question Settings	
Users must answer this number of optional questions to register	Set the required number of optional questions that a user must answer to create a Questions and Answers profile.
Users must answer this number of user-defined questions to register	Set the required number of user-defined questions that a user must specify to create a Questions and Answers profile.
Minimum length of user-defined questions	Set the minimum number of characters that user-defined questions can contain.
Answer Settings	
Minimum length of answers	Set the minimum number of characters that users' answers can contain.
Reject the same answers for different questions	Select to prevent users from specifying same answers for different questions.
Reject answers that contain corresponding questions	Select to prevent users from specifying answers that contain corresponding questions.
Store answers using reversible encryption	Select to store users' answers using reversible encryption. If you do not select this option, answers to mandatory, optional and user-defined questions are hashed. Note, that answers to helpdesk questions are always stored using reversible encryption, even if this option is not selected.
Security	

Option	Description
Settings	
Allow users to hide their answers	Select this check box to allow users to hide their answers on the screen, so that answer entry fields will look like a series of asterisks.
Hide users' answers by default	Select this check box to have Password Manager display users' answers as asterisks while they are typing in their answers.
Do not require users to confirm answers if answers are hidden	Select this check box to allow users to enter their answers only once, if answers are hidden.

5. Click **Save**.

Workflow overview

To customize the behavior of Password Manager for AD LDS, configure workflows in the Password Manager Administration Site. Workflows have 2 types:

- **Self-service workflows** customize the behavior of the Password Manager Self-Service Site. All configured and enabled self-service workflows are available as tasks on the Self-Service Site for Password Manager users.
- **Helpdesk workflows** customize the behavior of the Password Manager Helpdesk Site. All configured and enabled Helpdesk workflows are available on the Helpdesk Site as helpdesk operator actions.

To modify the behavior of an existing workflow task, in the **Home** page of the Password Manager Administration Site, click the management policy workflow you want to configure, and click **Workflow settings**.

Workflow structure

A workflow consists of activities. You can configure each activity independently.

Workflow activities have 3 types:

- **Authentication** provides authentication options, such as password-based authentication, Questions and Answers profiles, or phone-based authentication.

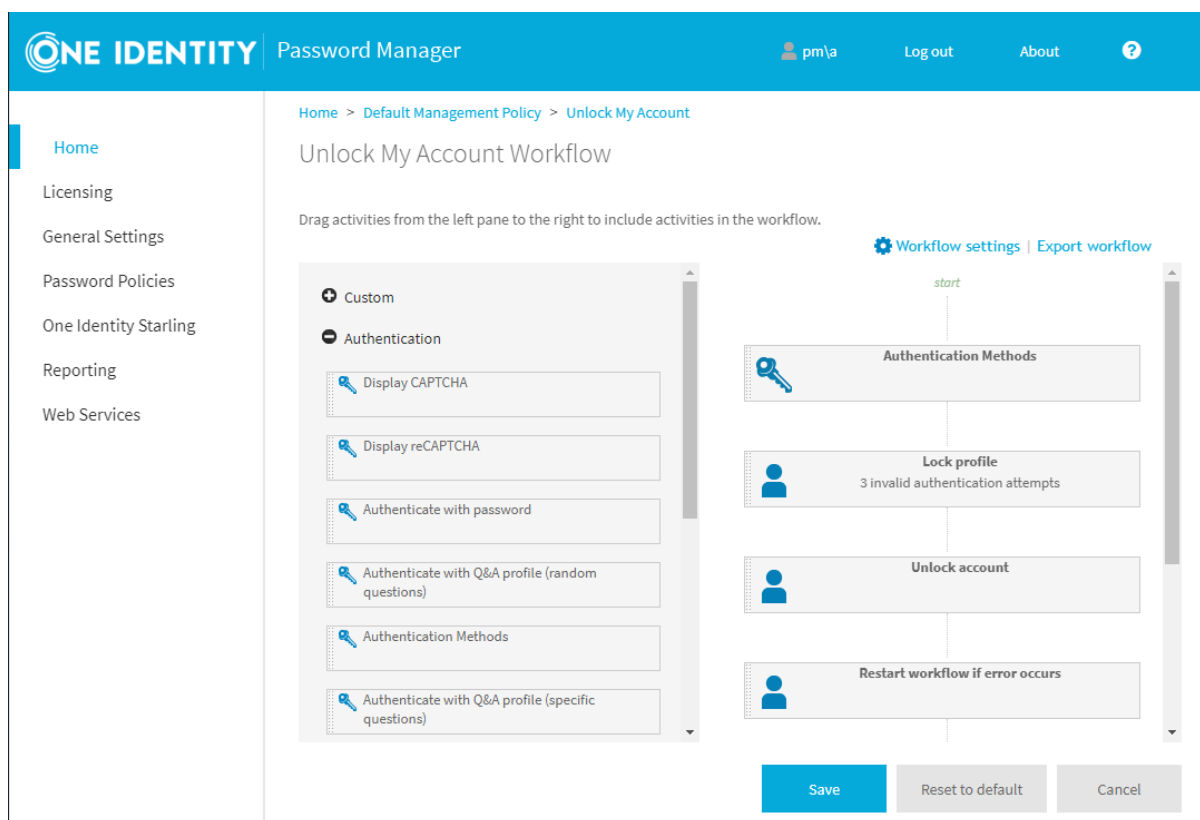
- **Actions** are core components in workflows, including activities like unlocking accounts, editing Q&A profiles, or resetting passwords.
- **Notifications** let you configure email notifications for users and administrators, and specify the conditions under which Password Manager for AD LDS will send these notifications.

You can also create custom activities. For more information, see [Custom Activities](#).

Password Manager for AD LDS lists the available activities in the left pane of the Workflow Designer. To add an activity to a workflow, drag and drop it into the right pane of the Workflow Designer. To remove an activity, click **Close** on the activity box.

Password Manager for AD LDS displays the workflow structure in the right pane of the Workflow Designer, indicating the type and order of activities to perform in the workflow. To change the order of the activities, simply move them up or down.

Figure 4: Home > <management-policy> > <workflow> > Workflow Settings



Workflow states

Workflow states determine how Password Manager for AD LDS ran a workflow and which activities of the workflow it initiated. Workflows have 3 states:

- **Success** is the state of the workflow if no errors occur when running a workflow. In this state, Password Manager for AD LDS performs all workflow activities, except the following:
 - **Email user if workflow fails**
 - **Email administrator if workflow fails**
 - **Lock Q&A profile**
 - **Restart workflow if error occurs**
 - **Failure** is the state of the workflow if an error occurs when running a workflow activity. If any errors occur during the workflow, Password Manager for AD LDS performs only the following activities:
 - **Email user if workflow fails**
 - **Email administrator if workflow fails**
 - **Lock Q&A profile**
 - **Restart workflow if error occurs**
- NOTE:** The **Restart workflow if error occurs** activity resets the workflow state to **Success** and runs the workflow from the beginning.
- **Critical Error** is the state of the workflow if a critical error occurs (for example, locking a user account or a Q&A profile). If any critical errors occur when running the workflow, Password Manager for AD LDS performs only the following activities:
 - **Email user if workflow fails**
 - **Email administrator if workflow fails**

Workflow settings

Workflow settings are grouped into 3 categories in the Password Manager for AD LDS Administration Site, under the **Home > <management-policy> > <workflow-name> > Workflow settings** window:

- **Language settings:** Settings in this category allow you to specify a custom name and description for the selected workflow on the Password Manager for AD LDS Self-Service Site or Helpdesk Site, either in the default language or in additional languages.
- NOTE:** You can specify custom names and descriptions only for the languages for which localization is available on the Password Manager for AD LDS Self-Service Site and Helpdesk Site.
- **Availability settings:** Settings in this category allow you to specify the conditions under which the workflow can appear in the Password Manager for AD LDS Self-Service Site or Helpdesk Site.

- **Customization settings:** Settings in this category allow you to specify a custom icon and a possible grouping key for the workflow.

To set the language settings of a workflow

1. On the Password Manager for AD LDS Administration Site, under **Home** > **<management-policy>**, click the workflow that you want to configure.
2. On the page of the configured workflow, click **Workflow settings**.
3. Under **Workflow Settings** > **Languages**, edit the workflow name and the workflow descriptions in the default language, then click **OK**.
4. (Optional) To edit the workflow name and the workflow description in other languages, click **Add new language**, select a language, then enter the workflow name and workflow descriptions in the selected language.
5. To apply your changes, click **OK**.

To set the availability settings of a workflow

1. On the Password Manager for AD LDS Administration Site, under **Home** > **<management-policy>**, click the workflow that you want to configure.
2. On the page of the configured workflow, click **Workflow settings**.
3. Under **Workflow Settings** > **Availability** > **Workflow availability**, specify when the workflow must be visible for your users:
 - **Always available:** The workflow is always visible for users in the Password Manager for AD LDS Self-Service Site or Helpdesk Site.
 - **Never available:** The workflow is always hidden in the Password Manager for AD LDS Self-Service Site or Helpdesk Site.
 - **Disable workflow if:** The workflow is visible or hidden in the Password Manager for AD LDS Self-Service Site or Helpdesk Site depending on whether the user meets or does not meet the configured conditions. You can configure the conditions to check with the following sub-settings:
 - **Account is locked:** Checks if the user's AD LDS account is locked by any local group policy (for example, because of specifying an incorrect password too many times).
 - **Account is disabled:** Checks if the user's AD LDS account has been disabled by an administrator.
 - **Account is expired:** Checks if the user's AD LDS account is expired.
 - **Profile is locked:** Checks if the user's Password Manager for AD LDS profile has been locked with the [Lock Q&A Profile](#) activity.
 - **User has passcode:** Checks if the user could generate and receive a passcode.
 - **User is registered:** Checks if the user is registered to the Password Manager for AD LDS Self-Service Site.

NOTE: Users are considered registered if they have manually registered earlier to the Password Manager Self-Service Site, or if the configured workflow contains an **Automatic register** activity.

- **User could not change password:** Checks if the user could not change their password.
- **Password is expired:** Checks if the user's password is expired.

All available sub-settings have 3 possible values:

- **Not used:** Password Manager for AD LDS will ignore the sub-setting when checking the state of the user.
- **Disable if true:** Password Manager for AD LDS will hide the configured workflow for the user if they meet the condition of the sub-setting.
- **Disable if false:** Password Manager for AD LDS will hide the configured workflow for the user if they do not meet the condition of the sub-setting.

IMPORTANT: If an unregistered user registers the first time, and enters an incorrect password beyond the specified limit, their profile will be locked. The user then must wait for the duration configured with the **Reset lockout account** setting.

4. (Only for helpdesk workflows) Set the **Show the workflow on the Helpdesk Site** setting to specify when the configured helpdesk workflow must appear under the **Manage User** workflow lists of the Password Manager Helpdesk Site. This setting has three values:
 - **Always:** The configured workflow is always listed.
 - **Never:** The configured workflow is never listed.
 - **Only if the workflow is available for the user:** The configured workflow is listed in the workflow lists only if it is available for the currently administered user.

NOTE: If the configured workflow is not available for a user, then selecting this option will result in the configured workflow not appearing in any of the **Manage User** workflow lists on the Helpdesk Site (including the **Disabled Tasks** list).

5. To apply your changes, click **OK**.

NOTE: To make sure that a custom workflow does not appear for users, set its **Workflow Settings > Availability > Workflow availability** setting either to **Never available** or to **Disable workflow if**, with the available disable conditions set according to your needs.

For example, to make sure that a custom workflow is only available for registered users, set the **Disable workflow if > User is registered** sub-setting to **Disable if false**.

To set the customization settings of a workflow

1. On the Password Manager for AD LDS Administration Site, under **Home > <management-policy>**, click the workflow that you want to configure.
2. On the page of the configured workflow, click **Workflow settings**.
3. Under **Workflow Settings > Customization > Choose an icon for the workflow**, select the icon of your choice for your workflow.
4. (Optional) Under **Workflow group name**, specify a group name that acts as a grouping key for workflows.

NOTE: Consider the following:

- Workflows that have the same group name are grouped together in the Password Manager for AD LDS Self-Service Site. If you do not want to add the current workflow to a group, leave the **Workflow group name** setting clear.
- If no translation is defined for the current language, **Workflow group name** will appear as entered in the Password Manager for AD LDS Self-Service Site.

5. To define translations for the **Workflow group name**, add a new key-value pair as "`<workflow-group-name>`": "`<translated-workflow-group-name>`" inside the opening and closing braces of the language's JSON file. The file is located in the following folder:

```
<password-manager-installation-folder>\One Identity\Password Manager\Web\SelfService\assets\i18n\<language>.json
```

NOTE: Consider the following when looking for workflow groups:

- Workflow groups appear in the Password Manager for AD LDS Self-Service Site in a way that is visually slightly different from that of workflows.
- Workflow groups are listed before the non-grouped workflows.
- A maximum of 4 icons from a workflow group are presented as a workflow group icon.

6. To apply your changes, click **OK**.

Custom workflows

To extend and customize the functionality provided by built-in workflows for your organization, create custom workflows. Similar to the built-in workflows, you can create 2 types of custom workflows: Self-Service and Helpdesk workflows.

To create a custom workflow

1. To open the **Add New Workflow** dialog, in the Password Manager Administration Site, under **Home > <management-policy>**, click **New Workflow** at the heading of the management policy for which you want to configure the new workflow.
2. In the **Select the workflow type** drop-down list, select the site where the workflow must appear (Self-Service Site or Helpdesk Site).
3. Enter the **Workflow name**.
4. Enter a **Workflow description**.
5. To apply your changes, click **Save**.

TIP: Consider the following when creating a new workflow:

- When you add a new custom workflow, it does not contain any activities. To add activities, click the workflow to open the Workflow Designer.
- You must specify the name and description for each workflow in the default language used on the Self-Service Site or Helpdesk Site. In addition, you can also specify the workflow name and description in other languages, as long as localization for those languages is available in the Self-Service Site and Helpdesk Site). For more information on configuring language settings, see [Workflow settings](#).

NOTE: To make sure that a custom workflow does not appear for users, set its **Workflow Settings > Availability > Workflow availability** setting either to **Never available** or to **Disable workflow if**, with the available disable conditions set according to your needs.

For example, to make sure that a custom workflow is only available for registered users, set the **Disable workflow if > User is registered** sub-setting to **Disable if false**.

Importing and exporting workflows

To share your configured workflows among management policies, import and export the workflows between them.

Prerequisites

Importing and exporting workflows between management policies is available only if you enable extensibility features.

To enable extensibility features

1. On the Password Manager Administration Site, navigate to **General Settings > Extensibility**.
2. Select **Extensibility on**.
3. To apply your changes, click **Save**.

To export a workflow

1. On the Password Manager Administration Site, under **Home > <management-policy>**, click the workflow of a management policy you want to export.
2. On the page of the workflow, click **Export workflow**. Depending on the browser settings, the workflow is then either downloaded to the default download folder, or you can specify the download location.

To import a workflow

IMPORTANT: Before importing a workflow, consider the following:

- If you import a workflow, Password Manager will replace existing workflows with the same name. To avoid accidental overwrites, One Identity recommends backing up existing workflows by exporting them when prompted.
- One Identity strongly recommends auditing scripts of custom activities in imported workflows before using them in a production environment. This is required because attackers could potentially access sensitive information via PowerShell scripts in a custom activity. Make sure you import workflows from a trusted source only.
- If the imported workflow contains activities that are missing from the current configuration, import the missing activities first (from the same workflow archive file), then import the workflow.

1. On the Password Manager Administration Site, under **Home > <management-policy>**, navigate to the management policy for which you want to import a new workflow, then click **Import Workflow**.
2. To select the workflow archive file, in the **Import Workflow** dialog, click **Upload**, then click **OK**.
3. To perform the import, click **OK**. If the import procedure would overwrite an existing workflow with the same name, click the link to export the affected workflow.

Custom Activities

There are two options to create a custom activity: you can create a custom activity from scratch or convert a built-in activity to custom.

For any custom activity, you can specify a display name, a short name (used to address the activity in scripts), a description (used on the Administration Site), and add PowerShell script to the activity. When you create the custom activity from scratch, you can also select user interface elements and enter the main instruction for the page of the Self-Service or Helpdesk Site that will be displayed when the activity is executed.

NOTE: You cannot specify any user interface elements for custom activities converted from built-in ones. If you want set user interface elements for your custom activity, create it from scratch.

For more information on writing PowerShell scripts for custom activities, refer to the Password Manager SDK.

IMPORTANT: You can create custom activities only after you turn on the extensibility features. You can turn on the extensibility features on the General Settings tab of the Administration Site.

Custom activity settings in Password Manager for AD LDS

If you use custom activities in your Password Manager for AD LDS workflows, consider how the shared settings of custom activities work.

- If you create a new custom activity from scratch, then all settings (display name, short name, description, PowerShell script, and user interface elements) will be shared. Because of this, if you change any of these settings for a custom activity included in or excluded from a workflow, the changes will be automatically propagated to all instances of the configured activity in all workflows and Management Policies.
- If you create a custom activity by converting a built-in activity, the custom activity will contain two types of settings: built-in and shared.
 - Built-in settings are inherited from the built-in activity and are not shared. If you modify them, the changes will be applied only to the current activity instance.
 - Shared settings (display name, short name, description, PowerShell script), however, will be propagated throughout all instances of the activity.

For example, if you modify the PowerShell script for the custom activity **My Custom CAPTCHA** and save your changes, the modified PowerShell script will

be applied to all instances of the **My Custom CAPTCHA** activity used in other workflows and Management Policies. However, if you modify the built-in settings (for example, the **Noise level**) of the **My Custom CAPTCHA** activity and save your changes, then the changes will be applied only to the currently configured instance of the activity. This means that the **Noise level** setting of other **My Custom CAPTCHA** activity instances will not be changed.

Creating custom activities

When you create a custom activity from scratch or by converting a built-in activity, the created custom activity in the **Custom** group of the activities list in the workflow designer. If you want to copy the created activity, hover over the activity in the left pane of the workflow designer, and click **Copy**.

Note, that this functionality is available only after you turn on the extensibility features.

To turn extensibility features on

1. Open the Administration Site and click the **General Settings** tab.
2. On the General Settings page, select the **Extensibility** tab.
3. On the Extensibility settings page, click the upper **Turn on** button.

To create a custom activity from scratch

1. On the Administration Site, open the workflow designer, expand the **Custom** group in the left pane, and click **Add new custom activity**.
2. On the **User Interface Designer** tab, enter the main instruction for the activity in the default language. You can translate the main instruction text into other languages by clicking the **Add new language** link. This text will be displayed on the page of the Self-Service or Helpdesk Site page when the activity is executed. Any user interface elements that you add will be displayed below the main instruction.
3. To add user interface elements, click **Add new element** in the **User interface elements** section.
4. In the **Add New Element** dialog, select the user interface element you want to add and enter the element's ID and label. Select the following options if required:
5. Click **OK**:
 - **Disable the element on the user interface:** Select this check box if you want to make this element disabled on the Self-Service or Helpdesk Site.
 - **Hide the element on the user interface:** Select this check box if you want to hide this element from the Self-Service or Helpdesk Site.
6. On the **Activity Name** tab, specify the following options:
 - **Activity short name:** The activity name that should be used in PowerShell scripts to refer to the activity.

- **Activity display name:** The activity name displayed in the activities list and workflow designer.
 - **Activity description :** Your description of the custom activity.
7. On the **PowerShell Script** tab, enter the PowerShell script to set the activity behavior. For more information on how to create and use activity scripts, refer to the Password Manager SDK.
 8. Click **OK**.

Any built-in activity (Self-Service or Helpdesk) can be converted to a custom one by clicking the **Convert to custom activity** link on a built-in activity in the activities list or the workflow designer. If you want to copy the created activity, hover over the activity in the left pane of the workflow designer, and click **Copy**.

To convert a built-in activity to a custom activity

1. On the Administration Site, open the workflow designer, select the built-in activity you want to convert, and click the **Convert to custom activity** link on the activity.
2. Hover over the created activity and click the **Shared settings** link.
3. On the **Activity Name** tab, specify the following options:
 - **Activity short name** . The activity name that should be used in PowerShell scripts to refer to the activity.
 - **Activity display name.** The activity name displayed in the activities list and workflow designer
 - **Activity description** . Your description of the custom activity.
4. On the **PowerShell Script** tab, enter the PowerShell script to set the activity behavior. For more information on how to create and use activity scripts, refer to the Password Manager SDK.
5. Click **OK**.

Importing and exporting custom activities

Using the import and export custom activity functionality, you can effortlessly share and copy custom activities that you created. If you want to reuse a custom activity in another workflow, export the activity to an archive file and then import it to the required workflow.

Note that you can import and export custom activities only. This functionality is available only after you turn on the extensibility features.

To turn extensibility features on

1. Open the Administration Site and click the **General Settings** tab.
2. On the General Settings page, select the **Extensibility** tab.
3. On the Extensibility settings page, click the upper **Turn on** button.

To export custom activity

1. On the Administration Site, open the workflow designer, expand the **Custom** group in the left pane of the workflow designer, hover over the custom activity you want to export, and click **Export**.
2. Depending on your browser settings, specify where you want to save the archive file and download the archive.

When you import custom activities, note that existing custom activities with the same name will be replaced. You can back up existing activities by exporting them when prompted.

IMPORTANT: When you import custom activities, it is strongly recommended to audit activities' scripts before using activities in a production environment. This is required because security-sensitive information can be accessed via PowerShell scripts included in a custom activity. Import custom activities from a trusted source only.

To import custom activity

1. On the Administration Site, open the workflow designer, expand the **Custom** group in the left pane of the workflow designer, and click **Import custom activity**.
2. In the **Import Custom Activity** dialog, click **Upload** to select the activity archive file and then click **OK**.

Removing Custom Activities

To remove a custom activity, click the **Remove** link on the custom activity in the workflow designer or in the activities list. Note, you can permanently remove the custom activity only if it is removed from all workflows where it is used first.

Password Manager Self-Service Site workflows

By configuring the self-service workflows you can specify what tasks will be available for users on the Self-Service Site, and configure options for each available task. Preconfigured self-service workflows are available out of the box. You can always customize the workflow, add activities to or remove them from the workflow. You can also create custom activities and custom workflows. For more information, see [Custom workflows](#) on page 80 and [Custom Activities](#) on page 82.

The following are the available built-in self-service workflows:

- Register
- Manage My Profile
- Forgot My Password
- Manage My Passwords
- Unlock My Account
- My Notifications
- I Have a Passcode

All built-in workflows have required activities and are ready-to-use.

The self-service workflows correspond to the tasks on the Self-Service Site. If you enable a self-service workflow, the corresponding task will be available to users on the Self-Service Site.

The self-service workflows provide the ability to combine different authentication options in a single workflow. For example, you can configure the authentication activities so that all secret questions are displayed on a single page, or only one secret question is displayed at a time. You can combine different authentication options such as authentication with Questions and Answers profile, Defender and phone-based authentication in a single workflow.

Register

Use this workflow to select which registration method(s) to display on the Self-Service Site.

This activity has the following settings:

- **Select registration mode:** Specifies which registration methods are allowed for users. By default, Password Manager for AD LDS supports the following authentication methods:
 - **Authentication with Questions and Answers Profile**
 - **Authentication with Telephone**
 - **Authentication with Passcode**
 - **Authentication with RADIUS Two-Factor Authentication**
 - **Authentication with Secure Token Server**

The selected authentication options will be added to the Password Manager for AD LDS Self-Service Site.

- **Select the registration method that must be set as the mandatory registration method for users in the User site:** Allows you to set an authentication method as mandatory for every user. If an authentication method is set as mandatory, all users must authenticate with it when registering to the Self-Service Site.
- **Restart activity on failure:** If this setting is selected and this activity fails for any

reason, then Password Manager will attempt to restart the workflow from this activity.

Configuring country code drop-down menu

You can configure the options to add, remove, or modify the country code drop-down menu.

To modify the view of the drop-down menu to display the country name or the country code, navigate to the location where Password Manager is installed. Open the `QPM.Service.Host.exe.config` file. Add the required details in the `<CountryConfig ShowWith="Attribute">` tag, where `<"Attribute">` can be **CountryName** or **CountryCode**.

To add a new country code, provide the required details in the `<add CountryName="<required country name>" CountryCode="<required country code>" ISDCode="<required ISD code>">`.

Restart the Password Manager service to view the updates in the country code drop-down menu.

Manage My Profile

The **Manage My Profile** workflow allows Password Manager for AD LDS administrators to manage user profiles in Active Directory via the Password Manager for AD LDS Administration Site. The **Manage My Profile** workflow uses the same settings as the **Register** workflow.

NOTE: Use this workflow only if the update of a user's Questions and Answers Profile is pending.

To configure the Manage My Profile workflow

1. Select the **Manage My Profile** workflow in the Password Manager for AD LDS Administration Site.
2. Click **Settings**.
3. Select **Run this activity only if user's profile should be updated**.
4. (Optional) To restart the activity if it fails for any reason, select **Restart activity on failure**.

Forgot My Password

You can use this workflow to configure the **Forgot My Password** task for the Self-Service Site. The **Forgot My Password** task allows users to reset passwords for their accounts in AD LDS by using the Self-Service Site.

IMPORTANT: To display password policies on the Self-Service Site when users reset passwords, add connections to AD LDS instances on the Password Policies tab of the Administration Site. For more information see [Creating a Password Policy](#) on page 188.

The default configuration of this workflow is the following:

1. Authentication Methods
2. Lock Q&A profile.
3. Reset password in AD LDS.
4. Restart workflow if error occurs.
5. Email user if workflow succeeds.
6. Email user if workflow fails.

Manage My Passwords

You can use this workflow to configure the **Manage My Passwords** task for the Self-Service Site. By using this task, users can manage passwords for their accounts in AD LDS by using the Self-Service Site.

IMPORTANT: To display password policies on the Self-Service Site when users change passwords, add the required application director partitions on the Password Policies tab of the Administration Site. For more information see [Creating a Password Policy](#) on page 188.

The default configuration of this workflow is the following:

1. Authenticate with password.
2. Change password in AD LDS.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

Unlock My Account

You can use this workflow to configure the **Unlock My Account** task for the Self-Service Site. Users use this task to unlock their accounts if they are locked out.

The default configuration of this workflow is the following:

1. Authentication Methods
2. Lock Q&A profile.

3. Unlock account.
4. Restart workflow if error occurs.
5. Email user if workflow succeeds.
6. Email user if workflow fails.

My Notifications

You can use this workflow to configure the **My Notifications** task for the Self-Service Site. Users perform this task to select what email notifications they want to receive when specified events occur.

The default configuration of this workflow is the following:

1. Authenticate with password.
2. Subscribe to notifications.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

I Have a Passcode

You can use this workflow to configure the **I Have a Passcode** task for the Self-Service Site. Users perform this task when they have forgotten their passwords and, at the same time, are not registered with Password Manager or have forgotten their answers to secret questions. In this case, they must obtain a temporary passcode from the help desk before they can create or update Questions and Answers profiles and reset passwords.

The default configuration of this workflow is the following:

1. Authenticate with passcode.
2. Edit Q&A Profile.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

Overview of built-in Password Manager Self-Service Site activities

Activities available for Password Manager Self-Service Site workflows are grouped into 3 categories:

- **Authentication:** These activities provide various authentication options (for example, authenticating with password, Questions and Answers Profiles, or by phone). For the list of these activities, see [Authentication activities](#).
- **Actions:** These activities include core steps for self-service workflows (for example, registering, automatic registering, unlocking accounts, or editing Questions and Answers profiles). For a list of these activities, see [Action activities](#).
- **Notifications:** These activities allow you to configure email notifications for users and administrators, including the conditions under which Password Manager sends notifications. For the list of these activities, see [Notification activities](#).

Authentication activities

This section lists the available built-in activities that provide various authentication options.

Display CAPTCHA

Use this activity to display a CAPTCHA image on the Password Manager for AD LDS Self-Service Site and require users to enter the displayed characters before beginning a workflow. This feature provides enhanced protection against automated attacks.

Figure 5: CAPTCHA configuration settings

Display CAPTCHA

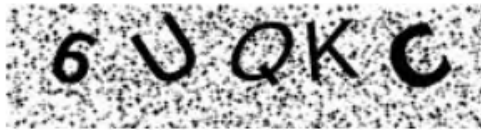
Specify the following settings for a CAPTCHA image.

Number of characters:

Noise level:

- Enable random scaling
- Enable random rotation
- Enable random skewing

Example image:



General activity settings

- Restart activity on failure

This activity has the following settings:

- **Number of characters:** Specifies the number of characters that will be displayed in the CAPTCHA.
- **Noise level:** Sets the noise level for the CAPTCHA. The higher the level, the more difficult it will be to read the characters.
- **Enable random scaling:** If selected, the size of the generated CAPTCHA will be scaled randomly.

- **Enable random rotation:** If selected, the characters will be randomly rotated in the generated CAPTCHA.
- **Enable random skewing:** If selected, the characters will be randomly distorted in the generated CAPTCHA.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

The **Display CAPTCHA** dialog also provides a preview window, showing an **Example image** of how a generated CAPTCHA will look like based on the configured settings.

NOTE: If you provide incorrect input, Password Manager for AD LDS generates a new CAPTCHA.

Display reCAPTCHA

Use this activity to require reCAPTCHA verification on the Self-Service Site and provide enhanced protection against automated attacks. If configured, users must click on an **I'm not a robot** check box before beginning a workflow, after which the user is either:

- Passed immediately (with no reCAPTCHA test required).
- Challenged to validate that they are human.

NOTE: reCAPTCHA is a free CAPTCHA service provided by Google. To start using reCAPTCHA, sign up and create reCAPTCHA keys on the following website:

<http://www.google.com/recaptcha>

When creating the keys, provide the DNS name of the domain where the Password Manager Self-Service Sites are installed. If the Self-Service Sites are installed in different domains, then create a global key by selecting **Enable this key on all domains**.

For more information on how to configure and use reCAPTCHA, see the following Google resource:

<http://www.google.com/recaptcha/learnmore>

This activity has the following settings:

- **Site key:** Specifies the site key that you received when configuring reCAPTCHA.
- **Secret key:** Specifies the secret key you received when configuring reCAPTCHA.
- **Theme:** Select the theme (Light or Dark) for the reCAPTCHA widget.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Authentication methods

Use this activity to select which authentication methods to display in the configured Password Manager site (Helpdesk Site or Self-Service Site). The available authentication methods are the following:

- Authentication with Questions and Answers Profile
- Authentication with Telephone
- Authentication with Passcode
- Authentication with RADIUS Two-Factor Authentication
- Authentication with Secure Token Server

NOTE: Consider the following when selecting an authentication method:

- Not all of the authentication methods might be available on the Password Manager Self-Service Site and/or Helpdesk Site. Instead, Password Manager administrators can select the registration method(s) to be visible on the Helpdesk Site and/or the Self-Service Site.
- If Password Manager administrators do not select the **Allow user to edit corporate details in corporate authentication of registration mode** setting, then the users cannot update their corporate email address and corporate mobile number even if they are already populated.
- To restart the workflow from the selected authentication activity if the activity fails for any reason, select **Restart activity on failure**.

Authentication with Questions and Answers Profile

Use this activity to authenticate a user with their personal Questions and Answers profile. If users select this authentication method, they must answer the question(s) that appear on the page. For increased security, users can select **Hide my answers for security purposes** to prevent displaying the entered answers.

Password Manager administrators can specify the number of questions that users must answer from their Questions and Answers profile to successfully authenticate.

For more information about the available Questions and Answers Profile authentication variations, see the following resources:

- [Authenticate with Q&A profile \(random questions\)](#)
- [Authenticate with Q&A Profile \(specific questions\)](#)
- [Authenticate with Q&A Profile \(User-selected questions\)](#)

Authentication with Telephone

Use this activity to authenticate a user with a mobile device. This authentication method has two types:

- Authenticating via text message (SMS)
- Authenticating via automated voice call

If users select this authentication method, they must specify the phone number that is used for authentication, then select the authentication type (sending an SMS or initiating the automated voice call).

For more information, see [Phone-based authentication service overview](#).

Authentication with Passcode

Use this activity to authenticate a user via a passcode sent in email and SMS. Password Manager administrators can set the passcode length and expiration time.

If users select this authentication method, they must click **Get Passcode**, then enter the received **Passcode** for authentication.

This authentication method uses the email address and phone number that is registered by the user in the **Register** or **Manage My Profile** workflow pages.

Authentication with RADIUS Two-Factor Authentication

Use this activity to authenticate users via RADIUS Two-Factor Authentication. This method uses one-time passwords (OTPs) generated by hardware or software tokens for authentication.

You can use RADIUS Two-Factor Authentication to authenticate users before allowing them to reset or change their passwords, to unlock accounts, or to manage Questions and Answers profiles.

NOTE: Authentication with RADIUS Two-Factor Authentication is available only if it is already configured on the **General Settings > RADIUS Two-Factor** page of the Password Manager Administration Site. For more information, see [RADIUS Two-Factor Authentication](#).

Authentication with Secure Token Server

Use this activity to authenticate users with an external provider that is configured with Secure Token Server (STS).

This authentication activity has two settings:

- **Choose from the configured providers to use in this activity for authentication:** Select the external provider to use in this activity of the current workflow. The external provider is configured in the **General Settings > Secure Token Server** page of the Password Manager for AD LDS Administration Site as described in [Configuring Password Manager Secure Token Server](#).
- **Choose the behaviour of the authentication:** Select if Password Manager for AD LDS must display the login interface in an **iframe** or in a **popup**.

NOTE: Select the **popup** behavior if your login provider sends the content with an **X-Frame-Options : Deny** header.

Authenticate with Password

Use this activity to authenticate users with their passwords when running a workflow.

This activity has the following settings:

- **Authenticate users with expired passwords:** Specifies if users with expired passwords can access the Self-Service Site.
 - Select this setting if you want to give access to the Self-Service Site for users who are required to change their passwords during their next login attempt.
 - Clear this setting if you want to deny access to the Self-Service Site for users whose passwords expired, and if you want to force them to change their passwords during their next login attempt.
- **Authenticate users with disabled accounts:** If selected, users with disabled accounts can access the Self-Service Site to:
 - Unlock and re-enable their accounts.
 - Reset and manage their passwords with their Q&A Profiles.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Authenticate with Q&A Profile (Random Questions)

Use this activity to authenticate a user with their personal Questions and Answers Profile. When using this activity, you can specify how many questions the users must answer from their Questions and Answers Profile for authentication.

NOTE: You cannot select specific questions from the Q&A Profile of the user with this authentication method. To require users to answer specific questions from their Q&A Profiles, use the [Authenticate with Q&A Profile \(Specific Questions\)](#) activity.

TIP: You can configure this activity to display all questions on a single page, only one question at a time, or the specified number of questions at a time. Making only one question or a specified number of questions visible at a time is useful if you do not want users to see the upcoming questions before answering the current ones.

- To display all questions on a single page, add the activity one time to a workflow.
- To display questions consecutively on several pages, add multiple instances of the activity in a row to the workflow.

This activity has the following settings:

- **All questions from user's Q&A profile:** If selected, users must answer all questions from their Q&A Profiles during authentication.
- **This number of randomly selected questions:** Sets the number of questions required to authenticate users. To specify the type(s) of secret questions (mandatory, optional, or user-defined) used for authenticating the user, select the corresponding check boxes.
- **Do the following if the number of questions in user's Q&A profile is less than specified:** Specifies if Password Manager allows or denies authenticating users if their Q&A Profiles do not have enough secret questions.
 - If you allow authentication, then Password Manager will use all questions from the Q&A Profile to authenticate users.
 - If you deny authentication, Password Manager will not complete the workflow that uses this activity until the affected users update their Q&A Profiles. After their Q&A Profiles are updated, users can perform the workflow that contains the authentication activity.
- **Allow users to see what questions were answered incorrectly:** If selected, users can see which questions they answered incorrectly during authentication.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Authenticate with Q&A Profile (Specific Questions)

Use this activity to authenticate a user with their personal Questions and Answers Profile. With this activity, you can select specific questions from the Q&A Profile of the user that they must answer for authentication.

TIP: You can configure this activity to display all questions on a single page, only one question at a time, or the specified number of questions at a time. Making only one question or a specified number of questions visible at a time is useful if you do not want users to see the upcoming questions before answering the current ones.

- To display all questions on a single page, add the activity one time to a workflow.
- To display questions consecutively on several pages, add multiple instances of the activity in a row to the workflow.

This activity has the following settings:

- **Mandatory questions:** Specifies the mandatory questions from the Q&A Profiles of the users. Users must always answer these questions during authentication.
- **Optional questions:** Specifies the optional questions from the Q&A Profiles of the users. Users can answer these questions optionally during authentication.
- **User-defined questions:** Specifies the user-defined questions from the Q&A Profiles of the users that they can answer during authentication.

- **Allow users to see what questions were answered incorrectly:** If selected, users can see which questions they answered incorrectly during authentication.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

IMPORTANT: If the questions you selected in this activity do not exist in the Q&A Profile of a user, Password Manager for AD LDS will not authenticate that user and will not run the workflow that uses this activity. Password Manager for AD LDS will complete the workflow only if the user updates their Q&A Profile so that they can answer the required secret questions.

Authenticate with Q&A Profile (User-selected questions)

Use this activity to authenticate a user with their personal Questions and Answers Profile. When using this activity, you can specify how many questions the users must answer from their Questions and Answers Profile for authentication. However, the users can select the questions that they want to answer themselves.

This activity has the following settings:

- **Number of questions that a user must answer during authentication:** Specifies the number of questions that the users must answer for authentication.
- **Do the following if the number of questions in user's Q&A profile is less than specified:** Specifies if Password Manager allows or denies authenticating users if their Q&A Profiles do not have enough secret questions.
 - If you allow authentication, then Password Manager will use all questions from the Q&A Profile to authenticate users.
 - If you deny authentication, Password Manager will not complete the workflow that uses this activity until the affected users update their Q&A Profiles. After their Q&A Profiles are updated, users can perform the workflow that contains the authentication activity.
- **Specify question categories which users will be able to choose from:** Specifies which question categories the users can choose from when attempting to authenticate with this activity. This option has the following settings:
 - **Use all questions from user's profile:** Allows users to select any questions to authenticate with from their answered questions.
 - **Specify questions categories:** Allows Password Manager administrators to choose which question categories the users can choose questions from when attempting to authenticate with this activity.
- **Allow users to see what questions were answered incorrectly:** If selected, users can see which questions they answered incorrectly during authentication.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Authenticate with Defender

IMPORTANT:

- Authenticating with Defender is an activity not supported with the current release of Password Manager ADLDS.
- Change or Reset password in Active Directory and connected systems is not supported in ADLDS.

You can use this activity to configure Password Manager to use Defender to authenticate users.

Defender is a two-factor authentication solution that authenticates users without forcing them to remember another new password. Defender uses one-time passwords (OTP) generated by special hardware or software tokens. Even if an attacker captures the password, there will be no security violation, since the password is valid only for one-time-use and can never be re-used.

You can use the Defender authentication to authenticate users before allowing them to reset or change their passwords, to unlock accounts, or manage Questions and Answers profiles.

Before configuring the settings in this activity, install and configure Defender as described in the Defender documentation.

IMPORTANT: To make Password Manager use the Defender authentication, you must install the Defender Client SDK on the server on which Password Manager Service is installed.

This activity has the following settings:

- **Defender Server:** Specify the IP address of the computer running the Defender Server.
- **Port number:** Type the port number that the Defender Access Node uses to establish a connection with the Defender Server.
- **Server timeout:** Specify Defender Server time-out (in minutes).
- **Defender shared secret:** Provide the secret that the Defender Access Node will share when it attempts to establish a connection with the Defender Server.

Authenticate with Secure Token Server

Use this activity to authenticate users with an external provider that is configured with Secure Token Server (STS).

This activity has the following settings:

- **Choose from the configured providers to use in this activity for authentication:** Select the external provider to use in this activity of the current

workflow. The external provider is configured in the **General Settings > Secure Token Server** page of the Password Manager Administration Site as described in [Configuring Password Manager Secure Token Server](#).

- **Choose the behaviour of the authentication:** Select if Password Manager must display the login interface in an **iframe** or in a **popup**.

NOTE: Consider the following:

- Select the **popup** behavior if your login provider sends the content with an **X-Frame-Options : Deny** header.
- For LDAP type authentication providers, set the **User's Unique ID Attribute** attribute mapping to objectGUID.

- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Authenticate with RADIUS Two-Factor Authentication

Use this activity to configure Password Manager to use a RADIUS server for two-factor authentication.

It uses one-time passwords (OTP) generated by hardware or software tokens for authentication.

You can use RADIUS Two-Factor Authentication to authenticate users before allowing them to reset or change their passwords, to unlock accounts, or manage Questions and Answers profiles.

Before using **RADIUS Two-Factor Authentication** for authentication, users have to configure it in **General Settings** tab on the home page of the Administration Site. For more information, see [RADIUS Two-Factor Authentication](#) on page 169.

Authenticate via phone in a self-service workflow

Use the **Authenticate via phone** activity to include phone-based authentication in a self-service workflow.

IMPORTANT: Phone-based authentication is available only if the feature is configured in the **General Settings > Phone Authentication** page of the Password Manager Administration Site. For more information on configuring this feature, see [Configuring phone-based authentication for Password Manager for AD LDS](#).

Before enabling phone-based authentication, make sure that the user phone numbers stored in AD LDS are in the correct format. The phone numbers must meet the following requirements:

- The numbers must start with either 00 or +, followed by the country code and the subscriber's number. For example: +1 555-789-1314 or 00 1 5554567890.
- Numbers support extensions. To specify an extension, use the ext word, such as: + 555 123-45-67 ext 890.
- In phone numbers, you can separate digits by space, hyphen (-), comma (,), period (.), plus (+) and minus (-) signs, slash (/), backslash (\), asterisk (*), hash (#), or tab characters.
- Phone numbers can contain the following brackets: parentheses (), curly braces {}, square brackets [], and angle brackets <>. However, only one set of brackets is allowed within the number. The opening bracket must be in the first half of the number. For example, the number +15551234(567) will be considered invalid.

USA phone numbers do not need to start with 00 or a + sign, if they comply with all other requirements and contain 11 digits. For example, the number 1-555-123-3245 will also be considered valid.

This activity has the following settings:

- **Authentication method:** Specifies whether to authenticate via a phone call or a text message. You can also allow users to choose the authentication method in the Self-Service Site by selecting the **Allow users to choose between an automated voice call and SMS** option.
- **SMS template:** Specifies the text message that will contain a one-time PIN code and will be sent to users during phone authentication.
- **telephoneNumber, homePhone, mobile** and other attributes: Select one or several attributes of a user account from which the telephone numbers will be used during phone-based authentication. You can also specify other attributes.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

To test the configured settings, click **Test settings** and enter the phone number to which the one-time PIN code will be sent.

Authenticate with Passcode

Use this activity to allow users to authenticate with a passcode for creating or updating their Questions and Answers Profile. Passcodes are assigned by helpdesk operators to users if the users:

- Forgot their passwords and are not registered to the Password Manager Self-Service Site.
- Forgot the answers to their secret questions.

For more information on configuring settings for assigning passcodes, see [Assign Passcode](#) on page 119.

By default, this authentication activity is used only in the **I Have a Passcode** workflow.

This activity has a single setting:

- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Action activities

The following sections list the activities that provide core functions for Password Manager for AD LDS self-service workflows, such as **Register**, **Automatic register**, **Reset password in Active Directory**, **Unlock account**, and so on.

Automatic register

Use the **Automatic register** activity to automatically provide access to the self-service workflows containing it in the Password Manager for AD LDS Self-Service Site. For example, adding this activity to the **Forgot My Password** self-service workflow results in making the Password Manager for AD LDS Self-Service Site and the **Forgot My Password** workflow automatically available for users.

TIP: One Identity recommends using the **Automatic register** activity if you do not want to configure Q&A Profiles, or you do not want forcing your users to manually register to the Password Manager for AD LDS Self-Service Site for accessing specific self-service workflows.

Prerequisites

The **Automatic register** activity only provides access to the Password Manager for AD LDS Self-Service Site and the self-service workflow containing the activity if the users have a working corporate phone and/or corporate email address set in their AD LDS user accounts.

NOTE: Consider the following:

- Password Manager checks the users' corporate email addresses in the `mail` AD LDS attribute, and by default, checks the corporate phone number in the `mobile` AD LDS attribute. You can modify the AD LDS attribute where Password Manager for AD LDS will check for the corporate phone number in the **Configuration > Reinitialization > Corporate phone** setting of the Password Manager for AD LDS Administration Site.
- The **Automatic register** activity will work if either a **Corporate phone** or a **Corporate email** is specified for a user. It does not require both values to be available at once.

Configuration

The **Automatic register** activity has no settings available for configuration. If included in a self-service workflow, then the Self-Service Site and that workflow will be automatically available for Password Manager for AD LDS users.

To include the Automatic register activity in a self-service workflow

1. On the Password Manager for AD LDS Administration Site, navigate to **Home > <management-policy> > Self-Service Workflows**, then click the self-service workflow in which you want to include the **Automatic register** activity.
2. In the list of workflows, scroll down to the list of **Action** activities.
3. From the list of **Action** activities, drag-and-drop the **Automatic register** activity's rectangle into the workflow diagram.
4. To apply your changes to the self-service workflow, click **Save**.

Edit Q&A Profile

This activity is part of the **Register** and **Manage My Profile** workflows, and allows users to create and update their Questions and Answers Profiles.

This activity has the following settings:

- **Run this activity only if user's Q&A profile should be updated:** Forces users to update their Q&A Profiles in the Self-Service Site only if their Q&A Profiles are not compliant with the current requirements.

TIP: Select this setting if you want to use the **Edit Q&A Profile** activity in the **Forgot My Password** and/or **Unlock My Account** workflows. This will ensure that users will be forced to update their Q&A Profiles after they reset their passwords or unlock their accounts, if their Q&A Profiles are not compliant with the current Q&A policy of your organization.

- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Reset Password in AD LDS

This is a core activity of the **Forgot My Password** workflow. The activity allows users to reset passwords in AD LDS instances.

In this activity you can configure the **Enforce password history** option. Password history determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.

Before selecting this option, you should consider the following by-design behavior of Password Manager when that the **Enforce password history** option is enabled:

- Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, One Identity recommends that you double the password history value. For example, if you want to prevent users from using the last 10 passwords, enter the value **20**.
- Having entered a new password that is not policy compliant, users may end up with a randomly generated password that they do not know.

The **Use auto generated password** option enables HelpDesk users to generate a new password during password reset process.

The **Use manual password** option enables HelpDesk users to reset the password manually.

Change Password in AD LDS

This is a core activity of the **Manage My Passwords** workflow. The activity allows users to change passwords in AD LDS instances.

Run this activity only when user must change password at next logon: Select this check box when you use this activity in workflows other than **Manage My Passwords**. By using this option you can force users who are required to change password at next logon to change password while performing other tasks on the Self-Service Site.

For example, if you add the **Change password in AD LDS** activity with this option selected to the **My Questions and Answers Profile** workflow, you will force users who are required to change password at next logon to change password when creating or updating their Q&A profiles.

Unlock Account

This activity is a core activity of the **Unlock My Account** workflow. It allows users to unlock their accounts using the Self-Service Site.

You do not need to configure any settings for this activity.

Enable Account

Use this activity to enable users' disabled accounts. You can use the activity in different workflows. It is recommended to place this activity after authentication activities in a workflow.

For example, to enable users with disabled accounts to reset passwords and enable their accounts, you can use the **Enable account** activity in the **Forgot My Password** workflow:

1. Authenticate with Q&A profile (random questions).
2. Enable account.

3. Reset password in AD LDS.
4. Restart workflow if error occurs.
5. Email user if workflow succeeds.
6. Email user if workflow fails.

Force User to Change Password at Next Logon

Use this activity when users want to change their passwords during the next logon.

For example, you can use this activity in the **Reset Password** workflow and can force users to change passwords at the next logon once the password has been reset by a helpdesk operator.

To allow users to change password at the next logon, the helpdesk operator must select **Helpdesk operators can choose whether to force users to change password at next logon** check box available in the **Force user to change password at next logon** activity.

It is recommended to place this activity after the **Reset Password** in AD LDS activity in a workflow.

Subscribe to Notifications

This is a core activity of the **My Notifications** workflow, allowing users to select notification events on the Self-Service Site. For example, users can enable notifications for password changes or account unlocks.

The list of notification events that is available on the Self-Service Site depends on the settings that you can configure in the user notification activities of the Self-Service Site workflows. Each user notification activity (**Email user if workflow succeeds** and **Email user if workflow fails**) has settings that allow you to:

- Subscribe users to the specific notification.
- Allow users to choose if they want to receive the notification.

If no user notification activity is included in a workflow, users will not receive any email notifications about that workflow.

The **Subscribe to notifications** workflow also has a **Restart activity on failure** setting. Use this setting to restart the workflow from the **Subscribe to notifications** activity if it fails for any reason.

The notification text depends on the workflow in which you use the notification activity. For example, if the **Email user if workflow succeeds** activity is used in the **Forgot My Password** workflow, then the successful completion of this task on the Self-Service Site will result in notifying the user that their password has been reset. By default, each Self-Service Site workflow includes the **Email user if workflow succeeds** and **Email user if workflow fails** activities and offer notification templates as well.

NOTE: Consider the following when configuring notifications for a workflow:

- If a user notification activity is included in a Helpdesk workflow, the user will always receive the corresponding notification. You cannot change the user subscription settings of notifications for helpdesk workflows.
- Notification templates are only available for built-in activities and built-in workflows.

For more information on configuring user notification activities, see [Notification activities](#) on page 106.

Lock Q&A Profile

If you want to lock the user's Questions and Answers profile after several failed authentication attempts, place the **Lock Q&A profile** activity before the **Restart workflow if error occurs** activity in a workflow. The **Lock Q&A profile** activity locks the profile when the total number of attempts to authenticate the user by using any of the following activities equals or exceeds the lockout threshold value:

- Authenticate with Q&A profile
- Authenticate via phone
- Authenticate with passcode

By default, the **Lock Q&A profile** activity is included in the **Forgot My Password** and **Unlock My Account** workflows.

IMPORTANT:

- If the user's Q&A profile gets locked, all tasks on the Self-Service Site will be unavailable for the user. In this case, the user must contact help desk to obtain a passcode and unlock the Q&A profile.
- If an unregistered user is registering for the first time and tries to enter a wrong password beyond the specified limit, the profile shall be locked out. The user has to wait for the duration configured for **Reset lockout Account**.

This activity has the following settings:

- **Lockout duration:** Specify the number of minutes the profile remains locked out before automatically becoming unlocked.
- **Lockout threshold:** Specify the number of failed authentication attempts that will cause a the profile to be locked out.
- **Reset account lockout counter after:** Specify the number of minutes that must elapse from the time a user fails to authenticate before the failed authentication attempt counter is reset to 0 bad authentication attempts.

Display User Agreement

Depending on local legislative requirements, organizations might be required to explicitly obtain their users' consent to store their personal information that is included in their Questions and Answers Profile.

You can use the **Display user agreement** activity for this purpose. When added to a workflow, running that workflow will result in the Self-Service Site asking users to agree that Password Manager for AD LDS will store their personal information.

TIP: Use this activity in the **Register** and/or **Manage My Profile** workflows. One Identity recommends placing this activity after authentication activities and before the **Edit Q&A profile** activity.

To configure the Display user agreement activity

1. Open the **Display user agreement** activity included in the workflow.
2. Edit the agreement text in the default language as required.

TIP: When editing the agreement text, you can use the parameters available in the editor, for example #USER_ACCOUNT_NAME# and others.

3. To edit the agreement text in the available additional languages, click the language link in the **Additional languages** list. By default, the agreement text template is available in 16 languages.
4. Click the **Add new language** link to select more languages for the agreement text.
5. To restart the workflow that includes the configured **Display user agreement** activity if the activity fails for any reason, select **Restart activity on failure**.
6. Click **OK**.

Restart Workflow if Error Occurs

This activity is performed when an error occurs during workflow execution. In this case, the activity reruns any self-service workflow from the very beginning. If a critical error occurs (user's account or Q&A profile gets locked, for example), then the **Restart workflow if error occurs** activity is skipped and the workflow stops.

It is recommended to place this activity before notifications activity in a workflow.

You do not need to configure this activity.

Notification activities

Build-in notifications have two types: user notifications and administrator notifications. Each notification type is divided into success and failure notifications. As such, for each workflow, 4 notification activities are available:

- **Email user if workflow succeeds**
- **Email user if workflow fails**
- **Email administrator if workflow succeeds**
- **Email administrator if workflow fails**

IMPORTANT: Before configuring notifications, make sure that you configured the outgoing mail servers. For more information on how to specify the SMTP server settings, see [Outgoing Mail Servers](#) on page 147.

Customizing Notifications

By default, **Email user if workflow succeeds** and **Email user if workflow fails** activities are included in every self-service and helpdesk workflow. These activities contain predefined notification templates that correspond to a workflow. For example, user notification activities in the **Forgot My Password** workflow offer templates about successful/failed password reset.

The notification templates are available in 17 languages: Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Swedish.

By default, for each user notification activity included in the default workflow configuration 17 languages are available: English as the default language and the others as additional languages. You can also select more languages by clicking the **Add new language** link in the notification activity dialog.

The language of notification corresponds to the language of a user's Q&A profile. If the Q&A profile is configured in a language that is not included in the list of languages available for Password Manager email notifications, the user will receive the notification in the default language.

NOTE: Predefined notification templates in 17 languages are available for user notifications only (**Email user if workflow succeeds** and **Email user if workflow fails** activities).

You can customize email notification messages distributed by Password Manager to meet specific requirements in your organization.

The following table describes parameters that you can use in email notifications:

Table 5: Email notification parameters

Parameter	Description	Examples
#PRODUCT_NAME_FULL#	Full name of the software product. The parameter value is a constant.	Password Manager
#PRODUCT_	Short name of the software	Password Manager

Parameter	Description	Examples
NAME_SHORT#	product. The parameter value is a constant.	
#COMPANY_NAME_FULL#	Full name of the company. The parameter value is a constant.	One Identity LLC
#COMPANY_NAME_SHORT#	Short name of the company. The parameter value is a constant.	One Identity
#PRODUCT_NAME_SHORT_CUSTOM#	Short name of the software product. The parameter value can be set manually by the user.	Password Manager Custom
#USER_ACCOUNT_NAME#	User's CN.	CN=JSmith
#USER_DISPLAY_NAME#	User's display name.	John Smith
#USER_FIRST_NAME#	User's first name.	john
#USER_LAST_NAME#	User's last name	Smith
#USER_UPN_NAME#	User Principle name is the name of a system user in an email address format.	JSmith@corp.contoso.com
#MACHINE_HOST_NAME#	A hostname is the label (the name) assigned to a device (a host) on a network and is used to distinguish one device from another on a specific network or over the internet.	MachineHostName.corp.contoso.com
#WINDOWS_LOGON_NAME#	Login name for wWindows.	corp\JSmith
#OPERATOR_IP#	Helpdesk operator's IP address.	172.16.254.1
#WORKFLOW_NAME#	Name of the workflow that was executed. All workflow names are available on the Administration Site.	Forgot My Password
#WORKFLOW_RESULT#	Result of a workflow execution displayed on the status page of	Your password was successfully changed.

Parameter	Description	Examples
	the Self-Service Site.	
#WORKFLOW_SUMMARY#	Text displayed in the details pane on the status page of the Self-Service Site.	Notification was sent to your email.

The notifications are sent either in plain text or as HTML.

To configure user email notifications

1. Open the user notification activity included in the workflow.
2. Edit the subject and body of the notification template in the default language as required. When editing the notification template, you can use the parameters available in the notification editor, for example, #USER_ACCOUNT_NAME#, #WORKFLOW_RESULT#, and so on.
3. To edit the notification message template in the available additional languages, click the language link in the **Additional languages** list.
4. Click the **Add new language** link to select more languages for the notification message.
5. In the **Message format** box, select the format to use for the notifications. You can select from two options: either **HTML** or **Plain text**.
6. In the **User notification settings**, select one of the following:
 - Subscribe users to this notification. Allow users to unsubscribe.
 - Subscribe users to this notification. Do not allow users to unsubscribe.
 - Do not subscribe users to this notification. Allow users to subscribe to this notification.
7. Verify the changes you have made by sending a test message. Click the **Test notification settings** button and enter an email address for a test email notification and select the notification language.
8. Click **OK**.

Email User if Workflow Succeeds

You can use this activity in any self-service workflow to notify users about a successfully performed workflow. For example, to notify a user that his account has been unlocked, use this activity in the **Unlock My Account** workflow.

Email User if Workflow Fails

You can use this activity in any helpdesk workflow to notify users about errors occurred in a workflow. For example, to notify a user an error occurred when a helpdesk operator attempted to reset password, use this activity in the **Reset Password** workflow.

Email Administrator if Workflow Succeeds

You can use this activity in any self-service workflow to notify an administrator about a successfully performed workflow. For example, to notify the administrator that a specific user has successfully unlocked the account, use this activity in the **Unlock My Account** workflow.

In the **Administrator's email address** text box, specify the email address of the administrator you want to receive notifications.

Email Administrator if Workflow Fails

You can use this activity in any self-service workflow to notify an administrator about errors occurred in a workflow. For example, to notify the administrator that errors occurred when a user tried to reset password, use this activity in the **Forgot My Password** workflow.

In the **Administrator's email address** text box, specify the email address of the administrator you want to receive notifications.

Helpdesk Workflows

By configuring the helpdesk workflows you can specify what tasks will be available to helpdesk operators on the Helpdesk Site, and configure options for each available task. You can also create custom activities and custom workflows. For more information, see [Custom workflows](#) on page 80 and [Custom Activities](#) on page 82.

The following helpdesk built-in workflows are available:

- Verify User Identity
- Assign Passcode
- Reset Password
- Unlock Account
- Unlock Q&A Profile
- Enforce Update of Q&A Profile

The helpdesk workflows correspond to the tasks on the Helpdesk Site. If you enable a helpdesk workflow, the corresponding task will be available to operators on the Helpdesk Site.

Verify User Identity

You can use this workflow to configure the **Verify User Identity** task for the Helpdesk Site. A helpdesk operator should verify user identity before performing any password management task.

The default configuration of this workflow is the following:

1. Authentication Methods.
2. Restart workflow if error occurs.
3. Email user if workflow succeeds.
4. Email user if workflow fails.

Assign Passcode

You can use this workflow to configure the **Assign Passcode** task for the Helpdesk Site. By using this task helpdesk operators can assign temporary passcodes to users who have forgotten their passwords and are not registered with Password Manager or have forgotten their answers to secret questions.

The default configuration of this workflow is the following:

1. Assign passcode.
2. Unlock Q&A profile.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

Reset Password

You can use this workflow to configure the **Reset Password** task for the Helpdesk Site. Helpdesk operators use this task to reset user passwords in managed AD LDS instances and other connected data sources, if applicable.

The default configuration of this workflow is the following:

1. Authentication Methods.
2. Reset password in AD LDS.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

Unlock Account

You can use this workflow to configure the **Unlock Account** task for the Helpdesk Site.

The default configuration of this workflow is the following:

1. Authentication Methods.
2. Unlock account.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

Unlock Profile

You can use this workflow to configure the **Unlock Profile** task for the Helpdesk Site. By using this task, helpdesk operators can unlock user's profiles that are locked out as a result of a sequence of failed attempts to provide the correct answers to secret questions.

The default configuration of this workflow is the following:

1. Unlock profile.
2. Restart workflow if error occurs.
3. Email user if workflow succeeds.
4. Email user if workflow fails.

Enforce Update of Profile

You can use this workflow to configure the **Enforce Update of Profile** task for the Helpdesk Site. Helpdesk operators can perform this task to require users to update their Q&A profiles so that the profiles meet requirements of the current Q&A policy.

The default configuration of this workflow is the following:

1. Enforce update of profile.
2. Restart workflow if error occurs.
3. Email user if workflow succeeds.
4. Email user if workflow fails.

Overview of Built-in Helpdesk Activities

All built-in activities available in the helpdesk workflows fall into the following categories: authentication, actions and notifications.

Authentication activities are a group of activities that provide different authentication options, for example authentication with Questions and Answers profiles, or phone-based authentication.

The actions category includes activities that are core components of the helpdesk workflows, for example Unlock Account, Assign Passcode, and other activities.

Notification activities are activities that you can use to configure email notifications for users and administrators, and specify conditions under which the notifications should be sent.

The following sections describe the helpdesk activities and provide information about the settings specific to each activity.

Authentication Activities

This section describes workflow activities that provide different authentication options.

Authentication methods

Use this activity to select which authentication methods to display in the configured Password Manager site (Helpdesk Site or Self-Service Site). The available authentication methods are the following:

- Authentication with Questions and Answers Profile
- Authentication with Telephone
- Authentication with Passcode
- Authentication with RADIUS Two-Factor Authentication
- Authentication with Secure Token Server

NOTE: Consider the following when selecting an authentication method:

- Not all of the authentication methods might be available on the Password Manager Self-Service Site and/or Helpdesk Site. Instead, Password Manager administrators can select the registration method(s) to be visible on the Helpdesk Site and/or the Self-Service Site.
- If Password Manager administrators do not select the **Allow user to edit corporate details in corporate authentication of registration mode** setting, then the users cannot update their corporate email address and corporate mobile number even if they are already populated.
- To restart the workflow from the selected authentication activity if the activity fails for any reason, select **Restart activity on failure**.

Authentication with Questions and Answers Profile

Use this activity to authenticate a user with their personal Questions and Answers profile. If users select this authentication method, they must answer the question(s) that appear on the page. For increased security, users can select **Hide my answers for security purposes** to prevent displaying the entered answers.

Password Manager administrators can specify the number of questions that users must answer from their Questions and Answers profile to successfully authenticate.

For more information about the available Questions and Answers Profile authentication variations, see the following resources:

- [Authenticate with Q&A profile \(random questions\)](#)
- [Authenticate with Q&A Profile \(specific questions\)](#)
- [Authenticate with Q&A Profile \(User-selected questions\)](#)

Authentication with Telephone

Use this activity to authenticate a user with a mobile device. This authentication method has two types:

- Authenticating via text message (SMS)
- Authenticating via automated voice call

If users select this authentication method, they must specify the phone number that is used for authentication, then select the authentication type (sending an SMS or initiating the automated voice call).

For more information, see [Phone-based authentication service overview](#).

Authentication with Passcode

Use this activity to authenticate a user via a passcode sent in email and SMS. Password Manager administrators can set the passcode length and expiration time.

If users select this authentication method, they must click **Get Passcode**, then enter the received **Passcode** for authentication.

This authentication method uses the email address and phone number that is registered by the user in the **Register** or **Manage My Profile** workflow pages.

Authentication with RADIUS Two-Factor Authentication

Use this activity to authenticate users via RADIUS Two-Factor Authentication. This method uses one-time passwords (OTPs) generated by hardware or software tokens for authentication.

You can use RADIUS Two-Factor Authentication to authenticate users before allowing them to reset or change their passwords, to unlock accounts, or to manage Questions and Answers profiles.

NOTE: Authentication with RADIUS Two-Factor Authentication is available only if it is already configured on the **General Settings > RADIUS Two-Factor** page of the Password Manager Administration Site. For more information, see [RADIUS Two-Factor Authentication](#).

Authentication with Secure Token Server

Use this activity to authenticate users with an external provider that is configured with Secure Token Server (STS).

This authentication activity has two settings:

- **Choose from the configured providers to use in this activity for authentication:** Select the external provider to use in this activity of the current workflow. The external provider is configured in the **General Settings > Secure Token Server** page of the Password Manager for AD LDS Administration Site as described in [Configuring Password Manager Secure Token Server](#).
- **Choose the behaviour of the authentication:** Select if Password Manager for AD LDS must display the login interface in an **iframe** or in a **popup**.

NOTE: Select the **popup** behavior if your login provider sends the content with an **X-Frame-Options : Deny** header.

Authenticate with Q&A Profile

Use this activity to authenticate a user with a personal Questions and Answers Profile. To configure the activity, specify mandatory and helpdesk questions from the user's Q&A Profile that the user must answer for authentication.

IMPORTANT: If the questions you selected in this activity are not found in the Q&A Profile of the user, then the user will not be authenticated and the workflow containing this activity will not be performed for the user.

This activity has the following settings:

- **Answers to the specified questions (user's answer is shown):** In this mode, helpdesk operators will ask users to provide the correct answers for the specified questions, then compare them to the answers displayed in the identity verification page.

IMPORTANT: This option cannot be used if the user answers are not stored using reversible encryption. To store answers using reversible encryption, select the corresponding option in the Q&A Profile settings. For more information, see [Configuring Q&A Profile Settings](#) on page 72.

- **Answers to the specified questions (user's answer is not shown):** In this mode, helpdesk operators will ask users to provide the correct answers to the specified questions, then enter the answers in the identity verification page.
- **Random characters of answers to the specified questions:** In this mode, helpdesk operators will ask users to tell the specified number of characters in the answer of the specified question, then enter those characters in the correct positions on the identity verification page.

- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Authenticate via phone in a helpdesk workflow

Use the **Authenticate via phone** activity to include phone-based authentication in a helpdesk workflow.

IMPORTANT: Phone-based authentication is available only if the feature is configured in the **General Settings > Phone Authentication** page of the Password Manager Administration Site. For more information on configuring this feature, see [Configuring phone-based authentication for Password Manager for AD LDS](#).

Before enabling phone-based authentication, make sure that the user phone numbers stored in AD LDS are in the correct format. The phone numbers must meet the following requirements:

- The numbers must start with either 00 or +, followed by the country code and the subscriber's number. For example: +1 555-789-1314 or 00 1 5554567890.
- Numbers support extensions. To specify an extension, use the ext word, such as: + 555 123-45-67 ext 890.
- In phone numbers, you can separate digits by space, hyphen (-), comma (,), period (.), plus (+) and minus (-) signs, slash (/), backslash (\), asterisk (*), hash (#), or tab characters.
- Phone numbers can contain the following brackets: parentheses (), curly braces {}, square brackets [], and angle brackets <>. However, only one set of brackets is allowed within the number. The opening bracket must be in the first half of the number. For example, the number +15551234(567) will be considered invalid.

USA phone numbers do not need to start with 00 or a + sign, if they comply with all other requirements and contain 11 digits. For example, the number 1-555-123-3245 will also be considered valid.

This activity has the following settings:

- **Authentication method:** Specifies whether to authenticate via a phone call or a text message. You can also allow users to choose the authentication method in the Self-Service Site by selecting the **Allow users to choose between an automated voice call and SMS** option.
- **SMS template:** Specifies the text message that will contain a one-time PIN code and will be sent to users during phone authentication.
- **telephoneNumber, homePhone, mobile** and other attributes: Select one or several attributes of a user account from which the telephone numbers will be used during phone-based authentication. You can also specify other attributes.
- **Restart activity on failure:** If this setting is selected and this activity fails for any

reason, then Password Manager will attempt to restart the workflow from this activity.

To test the configured settings, click **Test settings** and enter the phone number to which the one-time PIN code will be sent.

Authenticate with Defender

IMPORTANT:

- Authenticating with Defender is an activity not supported with the current release of Password Manager ADLDS.
- Change or Reset password in Active Directory and connected systems is not supported in ADLDS.

You can use this activity to configure Password Manager to use Defender to authenticate users.

Defender is a two-factor authentication solution that authenticates users without forcing them to remember another new password. Defender uses one-time passwords (OTP) generated by special hardware or software tokens. Even if an attacker captures the password, there will be no security violation, since the password is valid only for one-time-use and can never be re-used.

You can use the Defender authentication to authenticate users before resetting their passwords or unlocking their Q&A profiles.

Before configuring the settings in this activity, install and configure Defender as described in the Defender documentation.

IMPORTANT: To make Password Manager use the Defender authentication, you must install the Defender Client SDK on the server on which Password Manager Service is installed.

This activity has the following settings:

- **Defender Server (IP address or DNS name):** Specify Defender Server IP address or DNS name.
- **Port number:** Type the port number that the Defender Access Node uses to establish a connection with the Defender Server.
- **Server timeout:** Specify Defender Server time-out (in minutes).
- **Defender shared secret:** Provide the secret that the Defender Access Node will share when it attempts to establish a connection with the Defender Server.

Authenticate with RADIUS Two-Factor Authentication

IMPORTANT: This activity is available only if Password Manager for AD LDS administrators have configured RADIUS authentication in the **General Settings** tab of the Password Manager for AD LDS Administration Site. For more information, see [RADIUS Two-Factor Authentication](#) on page 169.

Use this activity to configure Password Manager to use a RADIUS server for two-factor authentication (2FA).

RADIUS 2FA uses one-time passwords (OTPs) generated by hardware or software tokens for authentication. If configured, users must authenticate with the received OTP before they can:

- Reset or change their passwords.
- Unlock their accounts.
- Manage their Questions and Answers Profiles.

This activity has a single setting:

- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Action Activities

This section describes activities that provide core actions of the helpdesk workflows, such as Reset password in AD LDS, Unlock account, and so on.

Reset Password in AD LDS

This is a core activity of the **Reset Password** workflow. The activity allows helpdesk operators to reset user passwords in AD LDS instances only.

In this activity you can configure the **Enforce password history** option. Password history determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.

Before selecting this option, you should consider the following by-design behavior of Password Manager when that the **Enforce password history option** is enabled:

- Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, One Identity recommends that you double the password history value. For example, if you want to prevent users from using the last 10 passwords, enter the value **20**.

- Having entered a new password that is not policy compliant, users may end up with a randomly generated password that they do not know.

Unlock Account

This activity is a core activity of the **Unlock Account** workflow. It allows helpdesk operators to unlock users' accounts using the Helpdesk Site.

You do not need to configure any settings for this activity.

Enable Account

Use this activity to enable users' disabled accounts. You can use the activity in different workflows. It is recommended to place this activity after authentication activities in a workflow.

For example, to enable users with disabled accounts to reset passwords and enable their accounts, you can use the **Enable Account** activity in the **Forgot My Password** workflow:

1. Authenticate user with Q&A profile.
2. Enable account.
3. Reset password in AD LDS.
4. Restart workflow if error occurs.
5. Email user if workflow succeeds.
6. Email user if workflow fails.

Force User to Change Password at Next Logon

Use this activity when users want to change their passwords during the next logon.

For example, you can use this activity in the **Reset Password** workflow and can force users to change passwords at the next logon once the password has been reset by a helpdesk operator.

To allow users to change password at the next logon, the helpdesk operator must select **Helpdesk operators can choose whether to force users to change password at next logon** check box available in the **Force user to change password at next logon** activity.

It is recommended to place this activity after the **Reset Password** in AD LDS activity in a workflow.

Assign Passcode

This is a core activity of the **Assign Passcode** workflow, allowing helpdesk operators to assign a passcode to users who:

- Forgot their passwords and are not registered to the Password Manager Self-Service Site.
- Forgot the answers to their secret questions.

This activity has the following settings:

- **Passcode length:** Specifies how many characters the passcode must contain.
- **Passcode lifetime:** Specifies how long the passcode will be valid after sent by helpdesk operators.
- **Restart activity on failure:** If this setting is selected and this activity fails for any reason, then Password Manager will attempt to restart the workflow from this activity.

Helpdesk operators can send the passcode in text message or via email.

- To send the passcode via text message, select **Generate Passcode and send it in SMS**.

NOTE: This setting is available only if phone-based authentication is configured. For more information, see [Phone-based authentication service overview](#).

- To send the passcode via email, select **Generate Passcode and send it in e-mail**.

NOTE: This setting is available only if at least one SMTP server is configured for Password Manager for AD LDS. For more information, see [Outgoing Mail Servers](#) on page 147.

Unlock a Q&A Profile

This activity is a core activity of the **Unlock Q&A Profile** workflow. It allows helpdesk operators to unlock users' Q&A profiles using the Helpdesk Site.

You do not need to configure any settings for this activity.

Enforce Update of Q&A Profile

This activity is a core activity of the **Enforce Update of Q&A Profile** workflow. It allows helpdesk operators to immediately enforce update of users' Q&A profiles if the profiles are not compliant with the current Questions and Answers policy.

Restart Workflow if Error Occurs

This activity is performed when an error occurs during workflow execution. In this case, the activity reruns any helpdesk workflow from the very beginning. If a critical error occurs, for example, user's account or Q&A profile gets locked, then the **Restart workflow if error occurs** activity is skipped and the workflow stops.

It is recommended to place this activity before notification activities in a workflow.

You do not need to configure any settings for this activity.

Notification Activities

All built-in notifications are divided into two groups: user notifications and administrator notifications. Each notification group is further subdivided into success and failure notifications. So, for each workflow four notification activities are available:

- Email user if workflow succeeds
- Email user if workflow fails
- Email administrator if workflow succeeds
- Email administrator if workflow fails

By using these activities you can configure email notifications that will be sent to users and specified administrators when workflows are completed successfully or fail.

IMPORTANT: Before configuring notifications, ensure that you have configured the outgoing mail servers. To specify the SMTP server settings, use the procedure outlined in [Outgoing Mail Servers](#) on page 147.

Customizing Notifications

By default, **Email user if workflow succeeds** and **Email user if workflow fails** activities are included in every self-service and helpdesk workflow. These activities contain predefined notification templates that correspond to a workflow. For example, user notification activities in the **Reset Password** workflow offer templates about successful/failed password reset.

The notification templates are available in 17 languages: Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Swedish.

By default, for each user notification activity included in the default workflow configuration 17 languages are available: English as the default language and the others as additional languages. You can also select more additional languages by clicking the **Add new language** link in the notification activity dialog.

The language of notification corresponds to the language of a user's Q&A profile. If the Q&A profile is configured in a language that is not included in the list of languages available for Password Manager email notifications, the user will receive the notification in the default language.

NOTE: Predefined notification templates in 17 languages are available for user notifications only (**Email user if workflow succeeds** and **Email user if workflow fails** activities).

You can customize email notification messages distributed by Password Manager to meet specific requirements in your organization. The notifications are sent either in plain text or as HTML.

To modify user email notifications

1. Open the user notification activity included in the workflow.
2. Select either to customize the email template or use from general settings section. If you choose to select **Use email template from general settings** section, the user receives email in default template from general setting section.
3. To customize, edit the subject and body of the notification template in the default language as required. When editing the notification template, you can use the parameters available in the notification editor, for example #USER_ACCOUNT_NAME#, #WORKFLOW_RESULT#, and others.
4. To edit the notification message template in the available additional languages, click the language link in the **Additional languages** list.
5. Click the **Add new language** link to select more languages for the notification message.
6. In the **Message format** box, select the format to use for the notifications. You can select from two options: either **HTML** or **Plain Text**.
7. Verify the changes you have made by sending a test message. Click the **Test notification settings** button and enter the email address for a test email notification and select the notification language.
8. Click **Save**.

Email User if Workflow Succeeds

You can use this activity in any helpdesk workflow to notify users about a successfully performed workflow. For example, to notify a user that the Q&A profile has been unlocked, use this activity in the **Unlock Q&A Profile** workflow.

Email User if Workflow Fails

You can use this activity in any helpdesk workflow to notify users about errors occurred in a workflow. For example, to notify a user an error occurred when a helpdesk operator attempted to reset password, use this activity in the **Reset Password** workflow.

Email Administrator if Workflow Succeeds

You can use this activity in any helpdesk workflow to notify an administrator about a successfully performed workflow. For example, to notify the administrator that a helpdesk operator has successfully unlocked user's Q&A profile, use this activity in the **Unlock Q&A Profile** workflow.

In the **Administrator's email address** text box, specify the email address of the administrator you want to receive notifications.

Email Administrator if Workflow Fails

You can use this activity in any helpdesk workflow to notify an administrator about errors occurred in a workflow. For example, to notify the administrator that errors occurred when a helpdesk operator attempted to reset user's password, use this activity in the **Reset Password** workflow.

In the **Administrator's email address** text box, specify the email address of the administrator you want to receive notifications.

User Enforcement Rules

User enforcement rules allow you to force users to create and update their Q&A profiles and notify users about password expiration. Password Manager offers three user enforcement rules: **Invite users to create/update Q&A profiles**, **Remind users to create/update Q&A profiles**, and **Remind users to change password**.

Invite Users to Create/Update Profiles

By using this user enforcement rule you can configure Password Manager to invite users to register with Password Manager or update their Questions and Answers profiles. If you configure this enforcement rule, users will be notified by email.

The notification schedule is defined by the **Invitation to Create/Update Profile** scheduled task. Note that notification starts only after this scheduled task has run. For more information on the scheduled tasks, see [Invitation to Create/Update Profile Task](#) on page 149.

NOTE: If you disable the **Invitation to Create/Update Profile** scheduled task, users will not be enforced to create or update their profiles.

This enforcement rule is disabled by default. To enable the rule, on the Home page of the Administration Site, expand the required enforcement rules section, click **Invite Users to Create/Update Q&A Profiles**, then click **Enable**.

To configure this enforcement rule, you must specify a user scope, conditions when an email notification should be sent and an email notification text.

To configure this enforcement rule

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. Select the Management Policy you want to modify.
3. Expand the **Enforcement Rules** section and click **Invite Users to Create/Update Profiles**.
4. To set the user scope of this rule, click **Configure** under **Configure the rule's scope**, specify the following settings and click **Save**:

Table 6: Configure scope of rule

Option	Description
Users from the user scope of the Management Policy	Select this option to include all users from the Management Policy user scope to the enforcement rule scope.
The following users	Select this option to specify groups included to and excluded from the enforcement rule scope.
Users included both in the Management Policy user scope and the following groups	Specify groups included in the enforcement rule scope. Note, that only users belonging both to the Management Policy user scope and the specified groups will be included in the enforcement rule scope. To browse for groups, click Add , select the required groups and click Save .
Users excluded from the rule's scope	Specify groups excluded from the enforcement rule scope. To browse for groups, click Add , select the required groups and click Save .

5. To specify the conditions under which users should be notified to create or update their Q&A profiles, click **Configure** under **Notify users who meet the following condition**, select one or more of the following options and click **OK**:

Table 7: User notifications

Option	Description
User is not registered with Password	Select to force users to register with Password Manager by creating Q&A profiles, if users are not registered with Password Manager.

Option	Description
Manager	
The question user answered to register was modified or deleted	Select to have users update their Q&A profiles if one or more questions which users answered to register were modified or deleted.
User's Q&A profile contains fewer questions than required for registration	Select to have users update their Q&A profiles if you have added one or more questions required for registration, thus making the list of such questions longer than it was before users' profiles were last updated.
User's answers are shorter than required	Select to have users update their Q&A profiles if any of users' answers contain fewer characters than the current settings require.
User-defined questions are shorter than required	Select to have users update their Q&A profiles if any of the user-defined questions contain fewer characters than the current settings require.
User has specified the same answer for several questions	Select to have users update their Q&A profiles if Q&A profiles contain the same answer for different questions if the current settings specify the opposite.
Settings for encrypting user's answers have been changed since Q&A profile creation	Select to have users update their Q&A profiles if the current encryption setting (defined by the Store answers using reversible encryption option in the Q&A profile settings) has been changed since Q&A profile creation. For example, when users created their profiles, the option was disabled, and later the option became enabled, and vice versa.
The question list users answered to create Q&A profile was removed or disabled	Select to have users update their Q&A profiles if the question list they used when registering was deleted or disabled. For example, if the question list in a particular language was deleted.
User's Q&A	Select to force users to update their Q&A profiles, if their last

Option	Description
profile is older than the specified value	update exceeds the specified maximum value (in days).
6.	To edit the notification template, use a WYSIWYG editor in the Configure email notification section.
7.	To define the default notification language, click the language link next to the Default language option and select the required language.
8.	To specify the notification text in another language, click Add new language and select the required language. Notification templates in 17 languages are available out of the box (English, Chinese (Simplified), Chinese (Traditional), Danish, Dutch, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Polish, Czech, Swedish). The language of the notification message corresponds to the language of a user's Q&A profile. If the corresponding language is not available, the notification message is sent in the default language.
9.	To specify the daily number of new users who will be invited to create or update their Q&A profiles, enter the number in the Set the daily number of users to be invited spin box. Use this option to reduce server load and enhance performance.
10.	Click Save .

IMPORTANT: To send email notifications to users, you must specify an outgoing mail server (SMTP server). For more information on how to configure the SMTP server, see [Outgoing Mail Servers](#) on page 147.

Remind Users to Create/Update Profiles

By using this enforcement rule, you can configure Password Manager to remind users to create or update their Q&A profiles. If you configure this enforcement rule, users will be notified by email.

For this enforcement rule you can configure multiple notification scenarios depending on the invitation date.

The notification is performed by the Reminder to Create/Update Profile scheduled task. Note that email notification starts only after this scheduled task has run. For more information on the scheduled tasks, see [Reminder to Create/Update Profile Task](#) on page 150.

IMPORTANT: To notify users by email, the Reminder to Create/Update Q&A Profile scheduled task should be enabled.

This enforcement rule is disabled by default. To enable the rule, on the Home page of the Administration Site, expand the required enforcement rules section, click **Remind Users to Create/Update Q&A Profiles**, then click **Enable**.

To configure this enforcement rule, you must specify a user scope and notification scenarios.

To configure the enforcement rule user scope

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. Select the Management Policy you want to modify.
3. Expand the **Enforcement Rules** section and click **Remind Users to Create/Update Q&A Profiles**.
4. To set the user scope of this rule, click **Configure** under **Configure the rule's scope**, specify the following settings and click **Save**:

Table 8: Configure the scope of the rule

Option	Description
Users from the user scope of the Management Policy	Select this option to include all users from the Management Policy user scope to the enforcement rule scope.
The following users	Select this option to specify groups included to and excluded from the enforcement rule scope.
Users included both in the Management Policy user scope and the following groups	Specify groups included in the enforcement rule scope. Note, that only users belonging both to the Management Policy user scope and the specified groups will be included in the enforcement rule scope. To browse for groups, click Add , select the required groups and click Save .
Users excluded from the rule's scope	Specify groups excluded from the enforcement rule scope. To browse for groups, click Add , select the required groups and click Save .

To configure notification scenarios

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. Select the Management Policy you want to modify.
3. Expand the **Enforcement Rules** section and click **Remind Users to Create/Update Q&A Profiles**.
4. To add a new notification scenario, click **Add**, or to modify an existing notification scenario click **Edit** in the **Apply the following notification scenarios to users from the rule's scope** section.
5. In the **User was invited to create/update Q&A profile N days ago** option, enter the required number of days to apply this enforcement rule to users who were invited to register with Password Manager or update their Q&A profiles the specified number of days ago. Click **Next**.
6. Edit the email notification template if necessary. Specify the following settings if required and click **OK**:
 - To define the default notification language, click the language link next to the **Default language** option and select the required language.
 - To specify the notification text in another language, click **Add new language** and select the required language. Notification templates in 17 languages are available out of the box (English, Chinese (Simplified), Chinese (Traditional), Danish, Dutch, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Polish, Czech, Swedish).

IMPORTANT: To send email notifications to users, you must specify an outgoing mail server (SMTP server). For more information on how to configure the SMTP server, see [Outgoing Mail Servers](#) on page 147.

Remind Users to Change Password

By using this enforcement rule you can configure Password Manager to notify users about password expiration. If you configure this notification, users will be notified by email.

The notification schedule is defined by the Reminder to Change Password scheduled task. Note that notification starts only after this scheduled task has run. For more information on the scheduled tasks, see [Reminder to Change Password Task](#) on page 151.

IMPORTANT: If you disable the Reminder to Change Password scheduled task, users will not be reminded of password expiration.

To enable the rule, on the Home page of the Administration Site, expand the required enforcement rules section, click **Remind Users to Change Password**, then click **Enable**.

To configure this enforcement rule, you must specify a user scope, conditions when an email notification should be sent and an email notification text.

To configure this rule

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. Select the Management Policy you want to modify.
3. Expand the **Enforcement Rules** section and click **Remind Users to Change Password**.
4. To set the user scope of this rule, click **Configure** under **Configure the rule's scope**, specify the following settings and click **Save**:

Table 9: Configure the scope of rule

Option	Description
Users from the user scope of the Management Policy	Select this option to include all users from the Management Policy user scope to the rule's scope.
The following users	Select this option to specify groups included to and excluded from the rule's scope.
Users included both in the Management Policy user scope and the following groups	Specify groups included in the rule's scope. Note, that only users belonging both to the Management Policy user scope and the specified groups will be included in the rule's scope. To browse for groups, click Add , select the required groups and click Save .
Users excluded from the rule's scope	Specify groups excluded from the rule's scope. To browse for groups, click Add , select the required groups and click Save .

5. To specify the conditions under which users should be notified to change their passwords, click **Configure** under **Notify users who meet the following condition**, specify the number of days before password expiration and click **OK**.
6. To edit the notification template, use a WYSIWYG editor in the **Configure email notification** section.
7. To define the default notification language, click the language link next to the **Default language** option and select the required language.
8. To specify the notification text in another language, click **Add new language** and select the required language. Notification templates in 17 languages are available out of the box (English, Chinese (Simplified), Chinese (Traditional), Danish, Dutch, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Portuguese

(Portugal), Russian, Spanish, Polish, Czech, Swedish). The language of the notification message corresponds to the language of a user's Q&A profile. If the corresponding language is not available, the notification message is sent in the default language.

9. Click **Save**.

IMPORTANT: To send email notifications to users, you must specify an outgoing mail server (SMTP server). For more information on how to configure the SMTP server, see [Outgoing Mail Servers](#) on page 147.

General Settings

- General Settings Overview
- Search and Logon Options
- Import/Export Configuration Settings
- Outgoing Mail Servers
- Diagnostic Logging
- Scheduled Tasks
- Web Interface Customization
- Instance Reinitialization
- Realm Instances
- AD LDS Instance Connections
- Enabling Password Manager for AD LDS extensibility features and troubleshooting mode
- RADIUS Two-Factor Authentication
- Internal Feedback
- Customizing help link URL
- Password Manager components and third-party applications
- Unregistering users from Password Manager
- Bulk Force Password Reset
- Fido2 key management
- Working with Redistributable Secret Management account
- Email templates

General Settings Overview

This section outlines the procedures required to configure general settings that apply to all created Management Policies, such as:

- Search and logon options
- Import/export of configuration settings
- Outgoing mail servers
- Diagnostic logging
- Scheduled tasks
- Web interface customization
- Reinitialization
- Realm instances
- AD LDS instance connections

Search and Logon Options

By configuring the search and logon options you specify how users and helpdesk operators search for their accounts and log in on the Self-Service and Helpdesk sites.

You can also configure Password Manager to display CAPTCHA or reCAPTCHA images and allow or prohibit account search on the Self-Service Site.

Configuring Search Options for the Self-Service Site

You can use the **General Settings > Search and Logon Options** tab of the Password Manager for AD LDS Administration Site to configure the following account search and security options:

Table 10: Search and Logon options

Option	Description
Do not allow users to search for their accounts	<p>When selected, users must either select the applicable directory partition to log in, or must specify an additional user account attribute (for example, their email address) when logging in either to the Self-Service Site or the Helpdesk Site.</p> <ul style="list-style-type: none"> • Show the list of application directory partitions to allow users to select the partition for logging in: When selected, the Self-Service Site will show all application directory partitions registered to Password Manager for AD LDS, allowing users to select the application directory partition their accounts belongs to.

Option	Description
Allow users to search for their accounts	<p>NOTE: The list will display all aliases that the user specified in their partition connections.</p> <ul style="list-style-type: none"> • Users must enter the following user account attribute for identification (this may slow down the performance): When selected, users must search for their accounts by using the specified AD LDS user account attribute. Use the text boxes under this setting to specify the attribute (for example, the email address) that users must enter on the Find User page of the Self-Service Site to search for their user account.
	<p>When selected, users can search for their accounts by simply providing their first name, last name, or account email address.</p> <ul style="list-style-type: none"> • Allow user search from external network: When selected, users can search their account on the Self-Service Site also from an external network. <p>TIP: Clear this setting to restrict searches only to IP addresses specified in the corporate IP address range of your organization, and to increase security. For more information on defining corporate IP address ranges, see Location sensitive authentication.</p> <p>For more information on user search in an external network, see Partial user search on external network.</p> <p>NOTE: If the Allow user search from external network setting is cleared, but no corporate IP address range is specified in the organization, every network from which a user search is performed will be treated by Password Manager for AD LDS as an external network.</p> <ul style="list-style-type: none"> • Search in multiple application directory partitions: When selected, users can search for their accounts in all application directory partitions registered with Password Manager for AD LDS. • Number of users to display in search results: Specifies the number of user accounts (between 1 and 99) displayed in the search results. • Automatically show available self-service tasks if only one account is found: When selected, Password Manager for AD LDS automatically opens the Home page of the Self-Service Site for the user if only one user account is found that matches the search criteria.

Option	Description
--------	-------------

- **User account attributes to display in search results:** Allows you to specify the user attributes (such as first name, last name, user logon name, email address) to display in the search results.

Partial user search on external network

When you search for a user from an external network and the **Allow user search from external network** check box is cleared, the application still displays the self-service tasks for certain users based on the below mentioned criteria:

- Users can reach the **Dashboard** page only when the search criteria exactly matches with the search results.
- If the user name to be searched is a substring of a different user name, Search Results get listed only for the single user, based on the exact match.
- If the user name to be searched is a substring of multiple user names, Search Results show **No accounts matching your search criteria have been found. Check the information you entered and try again** message.

Let us consider the below mentioned users in the user scope. Search behavior and result are as given in the table.

- ABCEFG_1
- ABCEFG_2
- ABCEFG_3
- ABCEFG_11
- XYZEFG

S.No	Search String	Dashboard Status	Search Results	Comments
1	XYZ	✗	✗	"No accounts matching your search criteria have been found. Check the information you entered and try again." message is displayed even though the search string is part of XYZEFG.
2	XYZEFG	✓	✗	Takes user to dashboard of XYZEFG.
3	ABCE	✗	✗	"No accounts matching your search criteria have been found. Check the information you entered and try again" message displayed since there are multiple users matching the

				search string.
4	ABCEFG_1	✗	✓	Only ABCEFG_1 is listed even though search string is part of ABCEFG_11.
5	ABCEFG_3	✓	✗	Takes us to dashboard of ABCEFG_3.

Conventions:

Dashboard Status - It indicates whether the user is able to view the respective workflow tasks in the Self-Service Site.

Search Results - It indicates the possible search results obtained after the search criteria.

✓ - It Indicates that the workflow page appears for the user.

✗ - It indicates that the workflow page does not appear for the user.

Configuring CAPTCHA or reCAPTCHA for the Find Your Account page

To prevent bot attacks when using the **Find Your Account** page, you can configure CAPTCHA or reCAPTCHA images to appear for validation.

NOTE: reCAPTCHA is a free CAPTCHA service provided by Google. To start using reCAPTCHA, sign up and create reCAPTCHA keys on the following website:

<http://www.google.com/recaptcha>

When creating the keys, provide the DNS name of the domain where the Password Manager Self-Service Sites are installed. If the Self-Service Sites are installed in different domains, then create a global key by selecting **Enable this key on all domains**.

For more information on how to configure and use reCAPTCHA, see the following Google resource:

<http://www.google.com/recaptcha/learnmore>

To configure CAPTCHA or reCAPTCHA settings for the Find Your Account page

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. To enable the CAPTCHA or reCAPTCHA settings, select **Show a security image to prevent bot attacks**.
4. (Optional) To enable the Self-Service Site showing CAPTCHA images on the **Find Your Account** page, select **Display CAPTCHA**, then click **Settings** and configure

the following options:

- **Number of characters:** Specifies the number of characters that will be displayed in the CAPTCHA.
 - **Noise level:** Sets the noise level for the CAPTCHA. The higher the level, the more difficult it will be to read the characters.
 - **Enable random scaling:** If selected, the size of the generated CAPTCHA will be scaled randomly.
 - **Enable random rotation:** If selected, the characters will be randomly rotated in the generated CAPTCHA.
 - **Enable random skewing:** If selected, the characters will be randomly distorted in the generated CAPTCHA.
5. (Optional) To enable the Self-Service Site showing reCAPTCHA images on the **Find Your Account** page, select **Display reCAPTCHA**, then click **Settings** and configure the following options:
 - **Public key:** Specify the public key you received when configuring reCAPTCHA on the reCAPTCHA website.
 - **Private key:** Specify the private key you received when configuring reCAPTCHA on the reCAPTCHA website.
 - **Theme:** Select a color theme for the reCAPTCHA widget.
 6. To perform the configured anti-bot protection check each time a user performs a search in the **Find Your Account** page of the Self-Service Site, under **Security Settings**, select **Show a security image every time the search is performed**.

TIP: Enable this setting for an increased protection against bot attacks.

7. To apply your changes, click **Save**.

Configuring Search Options for the Helpdesk Site

This section describes how to configure search options for the Helpdesk Site. For more information on the Helpdesk Site, see [Helpdesk Site](#).

To configure search options

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. On the menu bar, click **General Settings**, then click the **Search and Logon** tab, and select the **Helpdesk Site** option from the drop-down list.
3. In the displayed text box, specify the attribute of helpdesk operators' accounts in AD LDS that helpdesk operators should use to log in on the Helpdesk Site. For example, `userPrincipalName`.
4. Select the **Hide the list of application directory partitions if only one application directory partition is added to the helpdesk scope** option if required. If several application directory partitions are included in the helpdesk scope, helpdesk operators will be required to select the corresponding partition before logging in.

Configuring Security Settings

The Password Manager for AD LDS Administration Site offers several security options under **General Settings > Search and Logon Options > Security Settings**. Use these options to:

- Enable or disable showing security-sensitive user information on the Password Manager Self-Service Site. For more information, see [Hiding the domain user name on the Self-Service Site](#).
- Enable or disable showing the personally identifiable information (PII) for the currently logged in user. For more information, see [Hiding personally identifiable information for logged-in users](#).
- Create a custom pattern for Active Directory (AD)LDS attributes to show on the Self-Service Site. For more information, see [Creating a custom pattern from AD attributes to show on the Self-Service Site](#).
- Apply regular expressions on the UPN or username, when it is shown on the Password Manager user interface. For more information, see [Applying regular expression on UPN or username](#).
- Enable or disable CAPTCHA or reCAPTCHA checks to prevent bot attacks. For more information, see [Configuring anti-bot security settings](#).

Hiding the domain user name on the Self-Service Site

By default, the toolbar and the logout pop-up of the Self-Service Site display both the display name and the domain user name of the logged-in user (in the <User Display Name> <domain>\<username> format). For example:

Sam Smith (domainname\SSmith)

If the security policies of your organization require hiding security-sensitive information (such as the user logon name), you can change this so that the Self-Service Site will show only the user display name (for example: Sam Smith), but not the domain user name.

To hide the domain user name of the logged-in user on the Self-Service Site

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. Under **Standard security**, enable **Show only user display name on the Self-Service Site**.
4. To apply the changes, click **Save**.

Once you are ready, logging in next time to the Self-Service Site with any user will display only the user display name of the logged-in user.

Hiding personally identifiable information for logged-in users

By default, the toolbar and the logout pop-up of the Self-Service Site display both the display name and the AD LDS domain name where the user is logged in (in the <User Display Name> (<AD LDS domain>) format). For example:

Sam Smith (ADLDS-domain)

If the security policies of your organization require hiding personally identifiable information (PII) on the user interface, you can configure Password Manager for AD LDS to truncate PII on the Self-Service Site, for example as:

S** S**** (ADLDS-domain)

To hide PII on the Self-Service Site for the logged-in users

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. Under **Standard security**, enable **Do not show personally identifiable information (PII) for the logged in user**.
4. To apply the changes, click **Save**.

Once you are ready, logging in next time to the Self-Service Site with any user will display truncated PII for the logged-in user.

NOTE: The amount of user information truncated by the **Do not show personally identifiable information (PII) for the logged in user** setting is affected by the configured user account search options described in [Configuring Search Options for the Self-Service Site](#)

- Truncating PII with the **Do not allow users to search for their accounts** option also selected will truncate the entire expanded PII. For example, setting the **Users must enter the following user account attribute... > Self-Service Site** sub-setting to `mail` will result in both the user display name and their email address being truncated. For example, Sam Smith (`sam.smith@example.com`) will be truncated as:

```
S** S**** (s*****)
```

- Truncating PII with the **Allow users to search for their accounts** option also selected will truncate only the user name of the logged-in user, but not the name of the AD LDS instance they are connected to. For example:

```
S** S**** (adlds-instance)
```

Creating a custom pattern from AD attributes to show on the Self-Service Site

You can specify the **Custom security** options for the display name and the domain user name settings of the logged-in user to create unique display names. This is usually recommended or required if the **Standard security** settings described in [Hiding the domain user name on the Self-Service Site](#) and [Hiding personally identifiable information for logged-in users](#) do not fulfill your organization's information security needs.

To create a custom pattern from Active Directory (AD) LDS attributes to show on the Self-Service Site

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. Under **Custom security**, select **Create a custom pattern from AD LDS attributes to show unique display names on the Self-Service Site**.

To create unique display names, specify AD LDS attributes between \$ symbols.

For example, `$displayName$ - $mail$` results in the following dashboard message:

Hello, ExampleUser - example@domain.com

4. To apply your changes, click **Save**.

Applying regular expression on UPN or username

You can mask specific characters in the display name shown on the Self-Service Site.

Depending on whether you set the **Create a custom pattern from AD LDS attributes to show unique display names on the Self-Service Site** setting with the **Specify a regular expression to mask characters in the UPN/username shown on the UI** setting, you have the following options:

- If no custom pattern is set, the default display name is in a <User Display Name> <domain>\<username> format.
- If you set a custom pattern, the display name is already masked with the **Create a custom pattern from AD LDS attributes to show unique display names on the Self-Service Site** option.

To mask specific characters in the display name

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. Under **Custom security**, enable **Specify a regular expression to mask characters in the UPN/username shown on the UI**.

To mask specific characters in the display name, specify a regular expression.

For example, the regular expression [a-c] masks the display name of **TestacUser** to **Test**User**.

4. To apply the changes, click **Save**.

Configuring anti-bot security settings

To prevent bot attacks against your Password Manager deployment, you can configure anti-bot security measures for the **Find User** page of the Self-Service Site. Password Manager supports configuring CAPTCHA images and reCAPTCHA v2 or v3 security solutions.

- For more information on configuring CAPTCHA, see [Configuring CAPTCHA security images for the Password Manager for AD LDS Self-Service Site](#).
- For more information on configuring reCAPTCHA, see [Configuring reCAPTCHA security settings](#).

Configuring CAPTCHA security images for the Password Manager for AD LDS Self-Service Site


You can configure the Password Manager for AD LDS Self-Service Site to display CAPTCHA images on its **Find User** page as an anti-bot security measure.

Figure 6: CAPTCHA image test on the Self-Service Site

Enter your user name *
sam.smith

o1d.local ▼

Enter the characters you see on the picture



[Get new image](#)

Enter Captcha Text *
QZUEA

Search

To configure CAPTCHA images for the Self-Service Site

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. To enable the CAPTCHA settings, select **Show a security image to prevent bot attacks**, then select **Display CAPTCHA** and click **Settings**.
4. In the **Display CAPTCHA** dialog, configure the following options:
 - **Number of characters:** Specifies the number of characters that will be displayed in the CAPTCHA.
 - **Noise level:** Sets the noise level for the CAPTCHA. The higher the level, the more difficult it will be to read the characters.

- **Enable random scaling:** If selected, the size of the generated CAPTCHA will be scaled randomly.
- **Enable random rotation:** If selected, the characters will be randomly rotated in the generated CAPTCHA.
- **Enable random skewing:** If selected, the characters will be randomly distorted in the generated CAPTCHA.

To apply your changes, click **OK**.

TIP: The **Display CAPTCHA** dialog also provides a preview window, showing an **Example image** of how a generated CAPTCHA will look like based on the configured settings.

5. Under **Security Settings**, select **Show a security image every time the search is performed** to perform the configured anti-bot protection check each time a user performs a search in the **Find User** page of the Self-Service Site.

TIP: Enable this setting for an increased protection against bot attacks.

6. To apply your changes, click **Save**.

Configuring reCAPTCHA security settings

You can configure the **Find User** page of the Password Manager for AD LDS Self-Service Site to include reCAPTCHA anti-bot protection. Password Manager supports the reCAPTCHA v2 and v3 engines.

NOTE: Password Manager for AD LDS supports only the **"I'm not a robot" Checkbox** challenge of reCAPTCHA v2. It does not support the **Invisible reCAPTCHA badge** and **reCAPTCHA Android app** validations.

Prerequisites

Before you configure reCAPTCHA v2 or v3 protection for the Password Manager for AD LDS Self-Service Site, make sure that the following conditions are met:

- The server running Password Manager for AD LDS has an active Internet connection and can communicate with the Google reCAPTCHA endpoint.
- You must sign up and generate a reCAPTCHA site key and secret key from Google. For more information, see the [Google reCAPTCHA portal](#).

NOTE: When generating the keys on the [Google reCAPTCHA Administration Site](#), provide the domain name(s) where the Password Manager for AD LDS Self-Service Site(s) are deployed. If multiple Self-Service Sites are deployed in

several different domains, provide all the domains to generate the required number of site keys and secret keys.

To configure reCAPTCHA protection for the Self-Service Site

1. In the Password Manager for AD LDS Administration Site, navigate to **General Settings > Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. To enable the CAPTCHA or reCAPTCHA settings, select **Show a security image to prevent bot attacks**.
4. To configure the reCAPTCHA settings, select **Display reCAPTCHA** and click **Settings**.
5. In the **reCAPTCHA Settings** dialog, configure the following options:
 - **Version:** Select the reCAPTCHA version to use (**v2** or **v3**).
 - **Site key:** Enter the site key that was generated on the [Google reCAPTCHA Administration Site](#).
 - **Secret key:** Enter the secret key that was generated on the [Google reCAPTCHA Administration Site](#).
 - **Theme:** Select the visual theme (**Light** or **Dark**) to use with the reCAPTCHA widget.

NOTE: This setting is available only for reCAPTCHA v2.

- **Enter reCAPTCHA v3 Score:** Specify the reCAPTCHA v3 score threshold (0.0–1.0) under which the interaction is considered to be a bot attempt. The default value is 0.5, and One Identity recommends using it until further adjustments are made based on the actual site traffic.

NOTE: This setting is available only for reCAPTCHA v3.

Click **OK**.

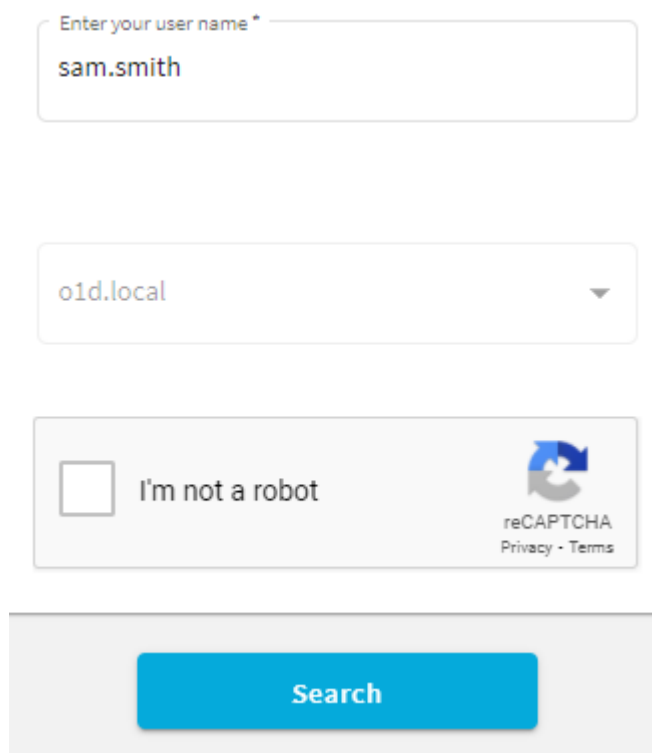
6. Under **Security Settings**, select **Show a security image every time the search is performed** to perform the configured anti-bot protection check each time a user performs a search in the Self-Service Site.

TIP: Enable this setting for an increased protection against bot attacks.

7. To apply your settings, click **Save**.

Once you configured reCAPTCHA, the **Find User** page of the Self-Service Site will be updated to include the configured anti-bot protection method:

- If reCAPTCHA v2 is configured, the **I'm not a robot** check box widget appears.



The screenshot shows a login form with the following elements:


- A text input field with the placeholder text "Enter your user name *" and the value "sam.smith".
- A dropdown menu with the value "oid.local".
- A reCAPTCHA v2 widget consisting of an unchecked checkbox labeled "I'm not a robot" and the reCAPTCHA logo with links for "Privacy - Terms".
- A blue "Search" button.

- If reCAPTCHA v3 is configured, the reCAPTCHA widget appears at the bottom right corner of the screen.

Find User

Enter a part of your first and/or last name or user name:

[Search](#)



Import/Export Configuration Settings

You can export configuration settings from the current Password Manager instance to a configuration file to back up the instance or create replicas of the existing instance.

Exporting Configuration Settings

By exporting configuration settings to a configuration file, you can back up the current instance or use the configuration file to create a Password Manager realm.

A realm is a group of Password Manager instances using common realm settings (encryption and hashing algorithms, realm affinity ID, and so on.) and configuration settings, including but not limited to Management Policies, general settings, password policies, and so on.

If you want to create a realm, you need to export the configuration settings from a Password Manager instance and create a replica of this instance by importing the configuration settings. To learn more about creating Password Manager realms, see [Installing multiple instances of Password Manager for AD LDS](#) on page 21.

To export configuration settings

1. To connect to the Administration Site, enter the Administration Site URL in the address bar of your web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the menu bar, click **General > Settings**, then click the **Import/Export** tab and select the **Export configuration settings** option.
3. Enter the password to protect the configuration file and click **Export**.

NOTE: Remember and store the password that is generated while exporting the configuration file. You must enter this password when importing the configuration file for a new instance when, you want to join to a realm or restoring the configuration. Losing this password requires re-installation of the application.

Export the configuration settings and save in a secure location. Use these settings to create secondary instances of Password Manager, and to recover data in the event of server disaster, or serious data loss.

Importing Configuration Settings

To restore a Password Manager instance or to join an instance to a realm, you need to import the configuration settings to such an instance.

To import configuration settings

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the menu bar, click **General Settings**, then click the **Import/Export** tab and select the **Import configuration settings** option.
3. Click **Upload** to select the configuration file that you exported earlier.
4. Enter the password and click **Import**.

Outgoing Mail Servers

You can configure one or more outgoing mail servers to send email notifications. If there are several servers, Password Manager will first attempt to use the top one in the list.

To add outgoing mail servers (SMTP)

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. On the menu bar, click **General Settings > SMTP Servers** and then click **Add SMTP server**.
3. In the **Add SMTP Server** dialog, configure the following options and click **Save**:

Table 11: SMTP server details

Option	Description
Server name	Enter the SMTP server name. If the SMTP server uses the port which is different from the default SMTP port 25 , you may specify the port using the following format: <server name>:<port number> where <server name> is the server name and <port number> is the port number used for SMTP communication.
Sender email address	Enter the sender's email address.
This server requires authentication	Select if the SMTP server requires authentication.
User name	Enter the user name under which Password Manager will access the SMTP server.
Password	Enter the password for this account.
Confirm password	Enter the password again.
The server requires an encrypted connection (SSL)	Select if the SMTP server requires an encrypted connection (SSL).

4. Follow steps 2-3 to add any additional SMTP servers.

NOTE: You can use the **Test settings** button to validate the SMTP server that you have configured. An email will be sent to the specified email address if the provided details are valid. If any of the details are invalid, an error message is displayed. You can configure the subject text of the email by configuring the value of Resource Id, `Admin.Scenario.Action.TestSMTP.Settings.TestEmail.Subject` in the `Admin.xml` file.

5. Use the **Move Up** and **Move Down** buttons to change the order of the SMTP servers in the list.

The order of the servers in the list specifies how Password Manager uses the servers to send email notification messages. Password Manager will first attempt to use the servers at the top of the list.

To remove a server from the list of outgoing SMTP mail servers

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the menu bar, click **General Settings**, and then click the **SMTP Servers** tab.
3. On the **SMTP Servers** page, select the SMTP server you want to remove and click **Remove**.

Diagnostic Logging

Password Manager provides a simple and convenient way to collect the diagnostic information about the activity of Password Manager. Diagnostic logging is mainly intended to be used by support personnel for troubleshooting purposes.

To enable diagnostic logging in Password Manager

1. On the home page of the Administration Site, click **General Settings**, then click the **Logging Settings** tab.
2. Configure the following options as required:

Table 12: Diagnostic logging options

Option	Description
Specify the path to the log folder:	Type a path to the folder to store the diagnostic information.
Set log level	The following log levels are available: Turn off logging: Select this option to turn off logging. Log errors only: Select this option to log only errors. Verbose logging: Select this option to log the most extended diagnostic information.

IMPORTANT: Do not enable verbose logging for long periods of time. Verbose logging creates log files that can accumulate quickly. Always monitor available disk space when verbose logging is enabled.

3. Click **Save**.

Scheduled Tasks

When installing Password Manager, the Password Manager setup adds the following scheduled tasks on the computer where Password Manager is installed: Invitation to Create/Update Profile, Reminder to Create/Update Profiles, Reminder to Change Password, Maximum Password Age Policy, update RADIUS server status, and User Status Statistics.

NOTE: Active Directory sites scheduled task is not applicable for Password Manager ADLDS.

Invitation to Create/Update Profile Task

This task is used to enumerate users who are not registered with Password Manager or must update their Q&A profiles and send email notifications to such users. This task is applied to users who have not been invited to create or update their Q&A profiles.

The scope of this task corresponds to the scope of the **Invite Users to Create/Update Q&A Profiles** user enforcement rule.

To each user from the user scope, the task is applied only once. After a user has been invited to create or update his Q&A profile, the **Reminder to Create/Update Profile** task will be applied to this user if configured.

You should configure this scheduled task to enable the **Invite Users to Create/Update Q&A Profiles** user enforcement rule. If you disable this scheduled task, the user

enforcement rule will not be implemented. For more information on this user enforcement rule, see [Invite Users to Create/Update Profiles](#) on page 123.

To schedule this task

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **Invitation to Create/Update Profile** task.
4. Select the **The task is enabled** check box.
5. From the drop-down list, select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
6. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
7. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

8. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

Reminder to Create/Update Profile Task

This task is used to send notifications to users who have been invited to create or update their Q&A profiles. If you configure the notification schedule, the task will send email notification messages to corresponding users.

The scope of this task corresponds to the scope of the **Remind Users to Create/Update Q&A Profiles** user enforcement rule.

You should configure this scheduled task to enable the **Remind Users to Create/Update Q&A Profiles** user enforcement rule. If you disable the scheduled task, the user enforcement rule will not be implemented. For more information on this user enforcement rule, see [Remind Users to Create/Update Profiles](#) on page 126.

To schedule this task

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **Reminder to Create/Update Profile** task.
4. Select the **The task is enabled** check box.
5. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
6. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
7. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

8. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

Reminder to Change Password Task

This task is used to send notifications about password expiration. Notifications will be sent to users whose passwords expire in the number of days specified in the Remind Users to Change Password user enforcement rule.

The scope of this task corresponds to the scope of the Remind Users to Change Password user enforcement rule.

You should configure this scheduled task to enable the Remind Users to Change Password user enforcement rule. If you disable the scheduled task, the user enforcement rule will not be implemented. For more information on this user enforcement rule, see [Remind Users to Change Password](#) on page 128.

To schedule this task

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **Reminder to Change Password** task.
4. Select the **The task is enabled** check box.
5. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
6. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
7. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

NOTE: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

8. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

Retry Failed Auditing Messages task

This task sends auditing data stored locally in the machine running Password Manager for AD LDS to the SQL Server that stores the Password Manager database.

Password Manager for AD LDS stores auditing data locally if the retry queue for auditing data that could not be sent to the SQL Server has been enabled with the **SQL Server Connection Settings > Enable retry queue for failed messages** option. For more information on configuring the retry queue, see [Using Password Manager for AD LDS reports](#).

If the **Retry Failed Auditing Messages** scheduled task can successfully write the auditing messages to the SQL Server database, it will automatically delete them from the local storage afterwards.

To schedule, run or disable the Retry Failed Auditing Messages scheduled task

1. Open the Administration Site by entering the following address in a web browser:

http(s)://<computer-name>/PMAAdmin

In the above URL, <computer-name> is the name of the computer on which Password Manager is installed.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. In the Administration Site, navigate to **Configuration > Scheduled Tasks**. Then, in the list of scheduled tasks, find the **Retry Failed Auditing Messages** task.
3. (Optional) To edit the current task run settings, click **Edit**. Then, in the **Task Settings** dialog, configure the following settings:
 - **The task is enabled:** Specifies if the task automatically runs with the configured regularity or is disabled. This setting is enabled by default.
 - From the drop-down list, select how frequently the task must run: **Run hourly, Run daily, or Run weekly**.
 - Depending on the selected frequency, specify the time and/or days of the week when this task must run.
 - Under **Run the task on this Password Manager instance**, select the Password Manager for AD LDS server on which the task must run.

IMPORTANT: You can view the task status only on the Password Manager instance on which the task is scheduled to run.

After you configured all settings, click **Save**.

4. (Optional) To disable the scheduled task, in the list of scheduled tasks, under **Retry Failed Auditing Messages**, click **Disable**.
5. (Optional) To manually run the scheduled task, in the list of scheduled tasks, under **Retry Failed Auditing Messages**, click **Run now**.

Maximum Password Age Policy Task

This task is used to force users to change passwords at next logon if password's maximum age is reached.

The scope of this task is the scopes of all configured One Identity password policies. For more information on One Identity password policies, see [Creating a Password Policy](#) on page 188.

This task applies the maximum password age rule set in the configured One Identity password policies. If the maximum password age is reached, users will be required to change password at next logon.

To schedule this task

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your web browser. By default, the URL is `http://<ComputerName>/PAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **Maximum Password Age Policy** task.
4. Select the **The task is enabled** check box.
5. From the drop-down list, select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
6. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
7. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

NOTE: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

8. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

Update RADIUS server status

This section describes how to schedule the task that updates the RADIUS server status. By default, the schedule task runs every 5 minutes.

To schedule the task

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **Update RADIUS server status** task.
4. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

NOTE: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

User Status Statistics Task

By default, the User Status Statistics task runs every day. Normally, it is not recommended to change the schedule, although if you have other heavy-duty tasks running at that time, we recommend that you reschedule the User Status Statistics task to run in off-peak hours. The User Status Statistics task is used to do the following:

- Enumerating users for licensing purposes. Password Manager is licensed for a specific number of user accounts enabled for management. The task checks whether the managed user count is within the license limit.
- Collecting statistic information about users including the total user count, the number of users registered and the users not-registered with Password Manager, the number of users required to register with Password Manager, and the number of users required to update profile. This information is collected for all application directory partitions managed by a specific Password Manager instance and displayed on the Reports page of the Administration Site.

The scope of this task corresponds to user scopes of all configured Management Policies.

To schedule this task

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a `<domain-name>\<user-name>` format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **User Status Statistics** task.
4. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

NOTE: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

Clear Old Records from Reporting Database

Use this task to clean up records in the reporting database. The administrator needs to provide a date range and select particular record types to delete the records. The administrator can schedule a task on a specific date and time.

To schedule the task:

1. Connect to the Administration Site by typing the Administration Site URL in the address bar of your Web browser. By default, the URL is `http://<ComputerName>/PMAAdminADLDS/`.

NOTE: When prompted to log in, provide your domain user name in a <domain-name>\<user-name> format.

2. On the menu bar, click **General Settings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under **Clear Old Records from Reporting Database** to open the console.
4. Select the **The task is enabled** checkbox.
5. Select **Archive and Clear Records** or **Clear Records**.
6. Select the date range from the **From Date** and **To Date** date pickers.
7. Select the checkboxes corresponding to the record types that you want to clear, in **Select Record Types** section.
8. Alternatively, select the **Select All** checkbox to select all the record types to clear.
9. Select the date and time from the **Start at** date picker to schedule the task to clear the records.
10. Select the Password Manager instance to run the task.
11. Click **Save** to save all the settings, and schedule the task.

Web Interface Customization

Web Interface Customization provides a simple and convenient way to customize the appearance of the Self-Service and Helpdesk sites. For example, you can change the company and product logos, splash screen logos, and modify the color scheme.

Enabling Self-Service UI 5.16

The following options appear only in case of an Inplace Upgrade of Password Manager to version 5.16.

- Maintain Self-Service Site (pre-5.9.5)
- Switch to Self-Service Site (5.9.5 or later)

To replace product and company logos with custom images

1. On the home page of the Administration Site, click **General Settings**, then click the **Web Interface Customization** tab.
2. Under the **Product logo (all interfaces and versions)** option, click **Upload** to browse your custom image. The uploaded image appears as a preview. Note, the image size must be **400** by **48** pixels and the image must be saved as a PNG with transparency.
3. Under the **Company logo (all interfaces and versions)** option, click **Upload** to browse your custom image. The uploaded image appears as a preview. Note, the image size must be **210** by **48** pixels and the image must be saved as a PNG with transparency.
4. Click **Save**.

NOTE: When you click **Reset to Default**, the customized product logo/ company logo gets reset to default.

To replace splash screen product and company logos with custom images

1. On the home page of the Administration Site, click **General Settings**, then click the **Web Interface Customization** tab.
2. Under the **Splash Screen Product logo (Self-Service UI 5.9.5 onwards)** option, click **Upload** to browse your custom image. The uploaded image appears as a preview. Note, that the image size must be 600 by 150 pixels and the image must be saved as a PNG with transparency. The Splash Screen Product logo appears as soon as you launch the self-service and help-desk sites.
3. Under the **Splash Screen Company logo (Self-Service UI 5.9.5 onwards)** option, click **Upload** to browse your custom image. The uploaded image appears as a preview. Note, the image size must be 400 by 200 pixels and the image must be saved as a PNG with transparency.
4. Click **Save**.

NOTE: When you click **Reset to Default**, the customized product logo/ company logo gets reset to default.

To replace large product logo for the Helpdesk Site

1. Under the **Large product logo (Helpdesk Site logon page)** option, click **Upload** to browse your custom image. The uploaded image appears as a preview. Note, the image size must be 440 by 70 pixels and the image must be saved as a PNG with transparency.
2. Click **Save**.

NOTE: When you click **Reset to Default**, the customized product logo/ company logo gets reset to default.

By modifying the color scheme you can customize the appearance of the Self-Service and Helpdesk sites to fit your corporate standards. Each color scheme offers a main color, page title, text, hyperlink, icon, button, button text and error text colors. The main color defines the logo bar color.

To modify the color scheme

1. On the home page of the Administration Site, click **General Settings**, then click the **Web Interface Customization** tab.
2. Under the **Color scheme** option, select the required color scheme for the Self-Service and Helpdesk sites.
3. To preview the selected color scheme on the Password Manager Self-Service Site, click **Preview (Self-Service UI version 5.9.5 onwards)** link.
4. To preview the selected color scheme on the Self-Service Site and Helpdesk Site, click **Preview (Self-Service UI / Helpdesk pre 5.9.3)** link.
5. To adjust your own color scheme, click **Custom** and navigate to various components listed for the customization of the Helpdesk Site and the Self-Service Site. The components that can be customized are Main color, page title color, text color, hyperlink color, icon color, button color, button text color, error text color.
6. Click **Save**.

NOTE:

- **Reset to Default** option resets the customized components and resets it back to the default in the Helpdesk Site and the Self-Service Site.
- Custom color scheme cannot be applied to the Password Manager Self-Service Site (**Self-Service UI version 5.9.5 onwards**)

Feedback Form

Feedback form is introduced in Password Manager Self service site (**Self-Service UI version 5.9.5 onwards**). The feedback form allows the users of the Password Manager Self service site to share the feedback on the user experience.

NOTE: No personal information of the users are collected and stored, and the survey is anonymous. By default, the Feedback form is enabled in the Password Manager Self service site.

To enable or disable feedback option

1. On the home page of the Administration Site, click **General Settings**, then click the **Web Interface Customization** tab.
2. In the **Customize the appearance of the Self-Service and HelpDesk sites** section, switch the toggle key in the **Self-Service feedback form (5.9.5 onwards)** to enable or disable the feedback option. By default, the feedback option is enabled.
3. Click **Save**.

Instance Reinitialization

This section provides information on how to reinitialize an instance of the Password Manager Service or the Password Manager Workflow Service. "Reinitialization" means changing any of the settings you specified during initialization, including:

- The certificate for encrypting traffic between the standalone Self-Service Site / Helpdesk Site and the Password Manager Workflow Service.
- The port number.
- The encryption algorithm and key length.
- The hashing algorithm.

Reinitialization of the Password Manager for AD LDS instance is typically required if you must change any of the settings you specified during the original initializing the Password Manager for AD LDS instance.

Modifying service connection settings

Use the **Service connection settings** page of the Password Manager Administration Site to configure communication between:

- The Password Manager Service and the Administration Site.
- The Password Manager Workflow Service and the Helpdesk Site / Self-Service Site.

To modify the service connection settings


1. Open the Administration Site by entering the following address in a web browser:
http(s)://<computer-name>/PMAdmin
In the above URL, <computer-name> is the name of the computer on which Password Manager is installed.
2. In the Password Manager Administration Site, navigate to **Configuration > Reinitialization**.
3. Expand the **Service connection settings** node.

Figure 7: Configuration > Reinitialization – Service connection settings

Use the following options to modify basic instance settings.

● Service connection settings

Select the certificate issued for the computer running the Password Manager Service.

Certificate name: 

---Built-in certificate---

Built-in certificate issued by One Identity
If you install the Self-Service site on a computer other than the computer running the Password Manager Service, it is recommended to replace the default certificate to enhance security.

Specify the port number that the Admin site will use to connect to the Password Manager Service.

Password Manager Service port number:

8081

Specify the port number that the Self-Service and Helpdesk sites will use to connect to the Password Manager Workflow Service.

Password Manager Workflow Service port number:

20002

4. From the **Certificate name** drop-down, select the required certificate for authentication and traffic encryption between the Password Manager services and the Password Manager sites.

NOTE: By default, Password Manager for AD LDS uses a built-in certificate issued by One Identity. If you install the Password Manager sites on a standalone server, One Identity recommends that you replace the default certificate with a custom certificate issued by a trusted Windows-based authentication authority for additional security.

For more information on obtaining and installing custom certificates, see [Specifying custom certificates for authentication and traffic encryption on page 22](#).

5. In the **Password Manager Service port number** text box, enter the port number that the Administration Site will use to connect to the Password Manager Service. The default value is 8081.

6. In the **Password Manager Workflow Service port number** text box, enter the port number that the Helpdesk Site and the Self-Service Site will use to connect to the Password Manager Workflow Service. The default value is 20002.

IMPORTANT: If you change the certificate and port number, the Self-Service Site and the Helpdesk Site installed on standalone servers will be unavailable to users until you reinitialize the sites using the updated settings. For more information, see [Installing the Password Manager for AD LDS Self-Service Site and Helpdesk Site on a standalone server](#) on page 18.

7. To apply your changes, click **Save**.

Modifying the advanced settings of instance reinitialization

Use the advanced settings of instance reinitialization to specify encryption, hashing and Q&A Profile data-specific settings.

CAUTION: If the configured Password Manager for AD LDS instance is part of a Password Manager for AD LDS realm, then changing the encryption settings and the attribute for storing Q&A Profiles will result in:

- The configured Password Manager for AD LDS instance being excluded from the realm it belongs to.
- Users potentially losing their Q&A Profiles.

To prevent potential data loss and keep the users's Q&A profiles, always update encryption settings and attributes in a Password Manager for AD LDS realm in the following order:

- Export the current configuration when saving updated instance settings.
- Update the Q&A profiles in the currently configured Password Manager for AD LDS instance.
- Replicate the new settings and updated Q&A Profiles by exporting the updated configuration from the current instance, then importing the configuration to other instances.

To modify the advanced settings of instance reinitialization

1. On the home page of the Administration Site, click **General Settings > Reinitialization**, then expand the **Advanced settings** section.
2. From the **Encryption algorithm** drop-down list, select the encryption algorithm for encrypting the users' answers to secret questions and other security-sensitive data. You can select from two options: **Triple DES** (default) and **AES**.

NOTE: If the **Store answers using reversible encryption** option of the Q&A Profile settings is selected, the answers will be encrypted. If this setting is not selected, the answers will be hashed.

3. From the **Encryption key length** drop-down list, select whether a 192-bit or 256-bit encryption key will be used to encrypt data.
4. From the **Hashing algorithm** drop-down list, select the algorithm that will be used to hash the users' authentication answers. The following algorithms are available: **MD5** and **SHA-256** (default).

NOTE: Consider the following when configuring hashing:

- If the **Store answers using reversible encryption** option of the Q&A Profile settings is not selected, the answers will be hashed. If this setting is selected, the answers will be encrypted.
- If you change the hashing algorithm, the selected algorithm will be applied to newly-created Q&A Profiles only. Existing Q&A Profiles will still be hashed with the previously selected algorithm.

5. In the **Select the attribute of user's account in AD LDS in which user's Questions and Answers profile and Corporate phone will be stored** section, provide the following data.
 - **Security questions:** Enter the required security question.
 - **Corporate phone:** Enter the mobile number of the user.
 - **Corporate email:** Enter the corporate's email of the user.

NOTE: By default, Password Manager for AD LDS:

- Stores Q&A Profile data in the `Comment` attribute of each user's account.
- Stores configuration data in the `Comment` attribute of a configuration storage account. This configuration storage account is automatically created when installing Password Manager for AD LDS.

6. Click **Save**. The **Reinitialize Instance** dialog then appears.
7. In the **Reinitialize Instance** dialog, a password is generated for the configuration file. To save this password to update the users' Q&A Profiles later, click **Export**.
8. Click **Save**.

After you updated the Q&A Profiles with new instance settings, join other Password Manager for AD LDS instances to this realm by exporting the configuration from the current instance and importing it to other Password Manager for AD LDS instances. For more information on importing and exporting configuration settings, see [Import/Export Configuration Settings](#) on page 145.

Realm Instances

On the Administration Site you can view a list of installed Password Manager instances belonging to one realm. This information is available on the Realm Instances page.

To open the Password Manager Service Instances page, on the Administration Site click **General Settings**. On the **General Settings** page, click the **Realm Instances** tab.

In Realm instances, the Primary instance is in red for easy identification.

All Password Manager Service instances belonging to one realm share the following settings: certificate name, port number, encryption algorithm, encryption key length, hashing algorithm, attribute for storing Q&A profile data, realm affinity ID, and configuration data. These options are configured when initializing a Password Manager Service instance. To change any of these settings, see [Instance Reinitialization](#) on page 159.

AD LDS Instance Connections

This section provides information on creating, modifying, and using connections to AD LDS instances.

Using Connections to AD LDS Instances

On the **General Settings > AD LDS Instance Connections** tab of the Administration Site, you can view a list of available connections.

To manage AD LDS instance with Password Manager you need to create a connection to the required AD LDS instance. When adding a connection, you can select an existing connection or create a new one. It is possible to use the same connection in different sections: user and helpdesk scopes, and password policies.

You can add a connection to an AD LDS instance either on the **AD LDS Instance Connections** tab or from the User scope, Helpdesk scope, and Password Policies pages.

NOTE: When you modify the connection on the User scope, Helpdesk scope or Password Policies pages, you can select how you want to apply the updated connection settings: only for the specified section, or everywhere this connection is used. If you choose to update settings for the specified section only, a copy of the connection will be created with these settings and will be added to the list of available connections to AD LDS instances.

IMPORTANT: When you modify the connection on the **AD LDS Instance Connections** tab, the updated settings will be automatically applied everywhere the

connection is used.

If you want to remove the connection from the list on the **AD LDS Instance Connections** tab, you should first remove it from all sections where it is used, and only then remove the connection from the list.

Specifying Access Account for AD LDS Instance Connections

When creating a connection, you must specify an access account - an account under which Password Manager will access an AD LDS instance and a specified application directory partition. You can use the Password Manager Service account, an Active Directory account or an AD LDS account. These accounts must have the following minimum set of permissions:

- Membership in the `Domain Users` group (for the Password Manager Service account and the Active Directory account only)
- Membership in the `Readers` group in the application directory partition (for the AD LDS account only)
- Membership in the `Administrators` group in the configuration directory partition
- The **Read** permission for all attributes of user objects
- The **Write** permission for the following attributes of user objects: `pwdLastSet`, `comment`, `unicodePwd`, `lockoutTime`, `msDS-UserAccountDisabled`
- The right to reset user passwords
- The permission to create user accounts and containers in the `Users` container
- The **Read** permission for attributes of the `organizationalUnit` object and container objects
- The **Write** permission for the `gpLink` attribute of the `organizationalUnit` objects and container objects
- The **Read** permission for the attributes of the container and `serviceConnectionPoint` objects in Group Policy containers
- The permission to create container objects in the `System` container
- The permission to create the `serviceConnectionPoint` objects in the `System` container
- The permission to delete the `serviceConnectionPoint` objects in the `System` container
- The **Write** permission for the `keywords` attribute of the `serviceConnectionPoint` objects in the `System` container

If you want to use the same connection in password policies as well, make sure the account has the following permissions:

- The **Read** permission for attributes of the `groupPolicyContainer` objects.
- The **Write** permission to create and delete the `groupPolicyContainer` objects in the System Policies container.
- The permission to create and delete container and the `serviceConnectionPoint` objects in Group Policy containers.
- The **Read** permission for the attributes of the container and `serviceConnectionPoint` objects in Group Policy containers.
- The **Write** permission for the `serviceBindingInformation` and `displayName` attributes of the `serviceConnectionPoint` objects in Group Policy containers.

To add connection

1. On the home page of the Administration Site, click the **General Settings > AD LDS Instance Connections** tab.
2. To add a connection, click **Connect to AD LDS instance**.
3. In the **Connect to AD LDS Instance** dialog, configure the following options:
 - In the **Server name on which AD LDS instance is installed** field, enter the name of the server to which you want to connect.
 - In the **Port number (LDAP or SSL)** field, enter the port number that you specified when installing the AD LDS instance. If you select the **Use SSL** check box, enter the SSL port number; otherwise, LDAP port number. It is recommended to use SSL in your production environment.
 - In the **Application directory partition** field, enter the name of the application directory partition from the AD LDS instance to which you want to connect.
 - In the **Application directory partition alias** field, type the alias for the application directory partition which will be used to address the partition on the Self-Service Site.
 - In the **Access account** section, select **Password Manager Service account** to have Password Manager access the AD LDS instance using the Password ManagerService account, otherwise, select **The following Active Directory account** or **The following AD LDS account** and enter the required user name and password.
4. Click **Save**.

NOTE: After you create a connection on the **General Settings > AD LDS Instance Connections** tab, you can use it in the user scope, helpdesk scope and password policies by selecting the connection in the **Connect to AD LDS Instance** dialog on the corresponding page of the Administration Site. For example, to use the connection in the user scope of your Management Policy, open the user scope of this Management Policy, click **Connect to AD LDS instance**, and select the corresponding connection from the list.

Changing Access Account for AD LDS Instance Connections

After setting up domain connections, you can change the access account. Under access accounts, Password Manager will access the AD LDS instance and a specified application directory partition.

To change access account

1. On the home page of the Administration Site, click the **General Settings > AD LDS Instance Connections** tab.
2. Select the connection you want to modify and click **Edit**.
3. In the **Edit AD LDS Instance Connection** dialog, select **Password Manager Service account** to have Password Manager access the managed instance using the Password Manager Service account. Otherwise, select **The following Active Directory account** or **The following AD LDS account**, then enter the required user name and password. Note, that the selected account should have the required permissions.
4. Click **Save**.

NOTE: The updated settings will be applied everywhere where this connection is used.

Removing Connection to AD LDS Instance

This section describes how to remove a connection to an AD LDS instance.

To remove a connection

1. On the Administration Site, click the **General Settings > AD LDS Instance Connections** tab.
2. On the **AD LDS Instance Connections** page, select the connection you want to delete and click **Remove**.

NOTE: To permanently remove the connection, it should be removed from all sections where it is used. The **Remove** link becomes available only after the connection is removed from all sections where it is used.

Enabling Password Manager for AD LDS extensibility features and troubleshooting mode

Extensibility features allow you to customize and extend the functionality of Password Manager for AD LDS with the following features:

- Custom activities
- Custom web services
- Importing and exporting activities and workflows
- Troubleshooting mode

IMPORTANT: These features are available only if you enable extensibility.

NOTE: The Password Manager extensibility features are only supported by One Identity Professional Services, and are not covered by One Identity Technical Support.

To enable extensibility features

1. In the Password Manager Administration Site, navigate to **General Settings > Extensibility**.
2. On the **Extensibility settings** page, click the upper **Turn on** button.

If you enable extensibility features, you can also enable **Troubleshooting mode**. If this feature is enabled, Password Manager for AD LDS also displays:

- Workflow and activity identifiers on the Administration Site.
- PowerShell output on the Self-Service Site.
- Human-readable summary messages and additional details about the completed workflows and activities in the Self-Service Site.

To enable Troubleshooting mode

1. In the Password Manager Administration Site, navigate to **General Settings > Extensibility**.
2. On the **Extensibility settings** page, under **Troubleshooting mode**, click **Turn on**.

About Password Manager for AD LDS extensibility features

Password Manager provides the following additional features to customize and extend your Password Manager instance:

- Custom activities
- Custom web services
- Importing and exporting activities and workflows
- Troubleshooting mode

IMPORTANT: These features are available only if you enable extensibility and/or troubleshooting mode as described in [Enabling Password Manager for AD LDS extensibility features and troubleshooting mode](#).

NOTE: The Password Manager extensibility features are only supported by One Identity Professional Services, and are not covered by One Identity Technical Support.

Custom activities

Custom activities are activities that are defined by a PowerShell script. You can create a custom activity either from scratch or convert a built-in activity to a custom one. For more information, see [Custom Activities](#) on page 82 and the Password Manager SDK.

Custom web services

Custom web services allow you to further extend the functionality of Password Manager by enabling scenarios that cannot be implemented with custom activities and the built-in web service. For example, you can create a custom web service that assigns passcodes to users. For more information, see the Password Manager SDK.

Importing and exporting activities and workflows

You can import and export activities and workflows, which is useful if you want to copy and share custom activities and workflows. For more information, see [Importing and exporting workflows](#) on page 80 and [Importing and exporting custom activities](#) on page 84.

Troubleshooting mode

Troubleshooting mode provides additional information for Password Manager administrators, helpdesk agents or One Identity Professional Services specialists about workflows and activities. If this mode is enabled, Password Manager provides the following additional information:

- Workflow and activity identifiers on the Administration Site.
- PowerShell output on the Self-Service Site.
- Human-readable summary messages and additional details about the completed workflows and activities in the Self-Service Site.

Use this data to troubleshoot workflows, activities and scripts, or use workflow identifiers and activity identifiers in your own PowerShell scripts.

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.

To configure RADIUS Two-Factor Authentication:

1. On the home page of the Administration Site, click **General Settings > RADIUS Two-Factor**.

The **RADIUS Two-Factor Authentication** page is displayed.

2. To add a new RADIUS server for authentication, click **Add RADIUS server**.

RADIUS Two-Factor Authentication page is displayed.

NOTE: You can add only two servers, one is used as a primary server and the other as a secondary server. The server that is created first is considered as the primary server and used for RADIUS authentication.

3. In the **RADIUS Server (IP address or hostname)** field, enter the RADIUS server IP address.
4. In the **Port number** field, enter the port number assigned during configuration of RADIUS.
5. In the **RADIUS Shared Secret** field, enter the password set during RADIUS configuration.
6. Specify the ADLDS attribute to authenticate the user from the drop-down menu.
7. From the **Additional RADIUS Attribute** section, select the required RADIUS attribute from the drop-down menu. Specify the value for the selected attribute and click **+**.

The RADIUS attributes and the corresponding values that you add is displayed.

NOTE: The following RADIUS attributes are supported: *NAS-IP-Address*, *NAS-Port*, *NAS-Port-Type*, and *NAS-Identifier*.

8. Click **Save**.

Internal Feedback

Administrators can define URLs and labels to form a link on Administration Site, Helpdesk Site and Self-Service Site, to allow users to give feedback on Password Manager.

To enable feedback on a site

1. Navigate to **General Settings > Internal Feedback**.
2. Enable feedback, and provide a non-empty label and a non-empty URL.

NOTE: If the provided label or URL is empty, the feedback link will not appear on the configured site.

In case of Administration Site feedbacks, the **Feedback** button will be displayed after a new session is opened, for example, by logging out and then logging in.

Customizing help link URL

You can customize the URL of the help link to redirect users to a chosen site when clicking the help icon.

To customize the help link URL on the Self-Service Site

1. Open the `config.json` file in the following location:
`<password-manager-install-folder>\folder\Web\SelfService\Scripts\libs\assets\config.json`
2. Set the `helpLink` property to the desired URL.

NOTE: The help icon can be hidden when the URL is configured to be empty.

To customize the help link URL on other Password Manager sites

1. Open the `sitemenu.xml` file:
`<password-manager-install-folder>\Web\<Admin/User/Helpdesk>\App_Data\sitemenu.xml`
2. Set the `SiteMenu.Help.Link` item's attribute to the desired URL.

Password Manager components and third-party applications

The following sections describe Password Manager components and third-party applications.

Password Manager Secure Token Server

Password Manager Secure Token Server (STS) is installed with Password Manager version 5.10.0. You can configure STS to use internal or external providers with optional Multi-Factor Authentication (MFA).

This feature can only be used on the new Password Manager Self-Service Site to authenticate users in a workflow. It is installed as a service called Password Manager Secure Token Server (STS). It has a configuration and user login interface.

How to use Password Manager STS features

To use the Password Manager STS feature, drag the **Authenticate with Secure Token Server** activity into any workflow.

- If you did not set up any Secure Token Server connection or did not have any valid providers configured in authentication providers, you cannot use this activity.
- If you set up one provider, you can start using it by dragging the activity in the workflow.
- If you set up more than one provider, you can select a specific provider for each activity that is used in workflows.

Authenticate with external provider in the Self-Service Site

If **Authenticate with Secure Token Server** is the current activity in a workflow, users will receive a login form where they must specify the credentials for the configured authentication provider. If the configured provider is using multi-factor authentication, the user is prompted for the next step. For more information, see [Authenticate with Secure Token Server](#).

This login interface uses the browser language, and supports the following languages:

- Argentinean (ar)
- Chinese (zh)
- Dutch (nl)
- English (en)
- French (fr)

- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Russian (ru)
- Spanish (es)

Password Manger STS account restrictions

By default, the Password Manager STS account is set to be the same account as the Password Manager Service Account by the Password Manager installer. The account requires read rights on domain.

Using STS features in a Password Manager realm

The Password Manager STS settings are stored separately from other Password Manager settings in a file on each server. That file will be encrypted using the service user's DPAPI key by default, or a specified certificate and can be replicated to other servers in a realm. For the replication to work the Password Manager STS instances should use the same ports.

Using Certificate to protect STS configuration

A trusted X.509 certificate with a private key needs to be installed on each server in the LocalMachine's certificate store. The provided `Rsts.exe.config` XML configuration file (`\One Identity\Password Manager\Service\SecureTokenServer\`) will need to be modified on each machine running a PasswordManager STS instance. An example of the XML configuration file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="rstsConfigSource" type="Rsts.Config.RstsConfigSource, Rsts"/>
  </configSections>
  <rstsConfigSource xmlns="urn:Rsts.Config">
    <source type="FileConfigProvider">
      <fileConfigProvider fileName="rstsConfig.bin">
        <protection type="RsaDataProtection">
          <rsaDataProtection certificateStore="LocalMachine"
certificateLookupType="FindByThumbprint"
certificateLookupValue="b23655f8ac0b81c5b00bac0bc0a15e7e1d2b78be"/>
        </protection>
      </fileConfigProvider>
    </source>
  </rstsConfigSource>
</configuration>
```

The thumbprint of the certificate used to encrypt the Password Manager STS settings file is set in the `rsaDataProtection` element's `certificateLookupValue` attribute. Change the value of the `certificateLookupValue` attribute to match the used certificate's thumbprint. In case of swapping to certificate encryption, copy the protection element and its child nodes and replace the existing protection element in the `masterConfigProvider` and `slaveConfigProvider` node.

NOTE: This configuration will be used after the restart of Password Manager Secure Token Server service.

NOTE: The specified certificate must be valid, trusted and it must exist in the Local Computer's certificate store. It must have a private key. Access to the private key must be granted to the service account that is running the Password Manager Secure Token Server Windows Service. The private key must be an RSA key, of any length. A certificate with an ECC key is not supported.

CAUTION: The current `rstsConfig.bin` will be unusable. For master (or single) instances of STS, reconfiguration has to take place from start. In case of slave instances, if the replication process works correctly, no reconfiguration is needed.

Pre-configuration steps after swapping between encryption methods on master (or single) instance

Pre-configuration takes place on the Administration Site **General Settings > Secure Token Server** page. Password Manager will check if a reset happened, then try to configure the basic options needed for STS to work properly. If the configuration is successful, no modal should show up. After a page refresh, STS is useable again.

If Password Manager STS settings are not replicated automatically

To replicate the Password Manager STS settings manually, copy the `rstsConfig.bin` file from the server where you configured Password Manager STS to all other servers. After you copy the file, you must restart the Password Manager STS Windows Service.

NOTE: You can find `rstsConfig.bin` in `<installdir>/One Identity/Password Manager-/Service/SecureTokenServer/`.

NOTE: This process needs to be repeated every time Password Manager STS settings are modified.

NOTE: For this copy-paste process, the encryption method of the Password Manager STS has to be set to **certification based encryption** before configuration. See: [Using Certificate to protect STS configuration](#).

Configuring Password Manager Secure Token Server

Before the first visit of STS settings, you need to have a binding for your Password Manager site in IIS with the same port that is present in the <Password Manager installation folder>\One Identity\Password Manager\Service\QPM.Service.Host.exe.config under the StsHttpsPort key. By default 20000 is used.

To start using Password Manager STS

1. Open the IIS manager and create an HTTPS binding with this port for Password Manager sites.
2. On the home page of the Administration Site, click **General Settings > Secure Token Server**. The **Secure Token Server** page is displayed.
3. To change the Password Manager STS settings, if you are prompted to enter RSTS client secret, provide the password. The default password is **admin**.

The default secret for Password Manager STS is **admin**. Password Manager will prompt administrators to change the current secret if it is still set to **admin**. This password will be shared between Password Manager and Password Manager STS instances.

CAUTION: For security reasons, you must change the password immediately after you have logged in to the configuration interface the first time.

To change the password, go to **Server settings > Administration Password**.

To configure the port used by Password Manager STS

1. On the home page of the Administration Site, navigate to **General Settings > Secure Token Server**. The **Secure Token Server** page is displayed.
2. Click **Set SSL**. A modal is displayed with **Port setting, SSL Certificate setting and Firewall setting**.
3. Set the desired port number and set a certificate which will be used for encrypting the communication. The selected certificate will be used only if there are no other settings are set in IIS for that port.
4. (Optional) Administrators can select whether Password Manager should create the firewall rules for the newly selected port.

To set authentication providers

1. On the home page of the Administration Site, navigate to **General Settings > Secure Token Server**. The **Secure Token Server** page is displayed.
2. Under **Add, edit or remove Secure Token Server authentication providers**, click **Add**. A modal is displayed.

3. Select an authentication provider type and its settings will be displayed in the modal. After entering the required settings, you can submit the form to create the authentication provider.
4. The new authentication provider is displayed in the table above the **Add** button. To create and attach a new 2FA provider to the newly created authentication provider, click **Add new 2FA**.

To configure STS Server Settings

1. On the home page of the Administration Site, navigate to **General Settings > Secure Token Server**. The **Secure Token Server** page is displayed.
2. Click **Server Settings**. A modal is displayed.
3. After you have set the desired settings, click **Save**.

Provider-specific informations: Duo

In the Duo admin interface you need to create a Web SDK type application to connect with Password Manager STS.

IP range-based rules for hostname resolution

The **IP range-based hostname resolution** feature allows administrators to define specific IPv4 ranges using IP addresses and subnet masks, and associate hostnames with these ranges.

When a client makes a request to the server, it checks the client's IP address against the predefined ranges. If the client's IP falls within any of the defined ranges, the server responds by providing the corresponding hostname associated with that range to access Secure Token Server (STS).

This feature is particularly useful for network administrators who want to assign custom hostnames or apply specific configurations based on the clients' IP addresses. It enhances security and control by allowing targeted responses based on IP range assignments.

To access this configuration feature on the Administration Site, navigate to **General Settings > Secure Token Server page**.

Unregistering users from Password Manager

Using the unregister feature, users registered to the Password Manager can be removed. Note that the user is removed only from the Password Manager and not Active Directory.

To unregister a user from the Password Manager

1. On the home page of the Administration Site, click **General Settings > Unregister Users**.
2. On the **Unregister Users** page:
 - If you want to unregister individual users, expand the **Select Users** tree, click **Add**, manually search for the individual user, select the required user from the results, and click **Save**.
 - If you want to select a user group, expand the **Select Groups** tree, click **Add**, manually search for the individual groups, select the required group from the results, and click **Save**.
 - If you want to select the entire organization unit (OU), expand the **Select Organizational Units** tree, click **Add**, manually search for the individual OU, select the required OU from the results, and click **Add**.
3. Click **Unregister User** to unregister the users.

NOTE:

- To run the task at a specified time, select the **Schedule at**, specify a time to run the task, and click **Save**.
- If a task to unregister an user is scheduled at a later time and you want to unregister the user at the current instance, click **Remove Setting** to delete the scheduled task settings and click **Save**.
- If you have the **Domain management account** configured with a user other than the Active Directory Administrator then, make sure that the Write permissions are available to the storage attribute of the security questions (comment, by default) for all the users/ groups/OUs that is configured to be unregistered.
- If the users/ groups/ OUs that needs to be unregistered are a member of Readers/ Administrators group in the ADLDS then, the Write Permissions are already inherited.

Bulk Force Password Reset

Use the Bulk Force Password Reset feature to force selected users, groups and Organizational Units to change their passwords.

To enforce a password change for users

1. On the home page of the **Administration** site, click **General Settings > Bulk Force Password Reset**.
2. On the **Bulk Force Password Reset** page:

- If you want to enforce password change for individual users, expand the **Select Users** tree, click **Add**, manually search for the individual user, select the required user from the results, and click **Save**.
- If you want to enforce password change for a user group, expand the **Select Groups** tree, click **Add**, manually search for the individual groups, select the required group from the results, and click **Save**.
- If you want to enforce password change for the entire Organizational Unit (OU), expand the **Select Organizational Units** tree, click **Add**, manually search for the individual OU, select the required OU from the results, and click **Save**.

3. Click **Reset Passwords**.

NOTE: Consider the following when using the Bulk Force Password Reset feature:

- Password reset is achieved by setting the **Users must change password at next logon** flag of the selected user(s) to true. This flag cannot be set to true, if the **Password never expires** flag is also true.
- If you have the **Domain management account** configured with a user other than the Active Directory Administrator, make sure that write permissions are given to the `pwdlastset` attribute.

Fido2 key management

Use the Fido2 key management feature to unpair FIDO2 keys from selected users, groups and Organizational Units.

TO unpair Fido2 keys

1. On the home page of the Administration Site, navigate to **General Settings > Fido2 key management**.
2. On the **Fido2 key management** page:
 - If you want to unpair Fido2 keys from individual users, expand the **Select Users** tree, click **Add**, manually search for the individual user, select the required user from the results, and click **Save**.
 - If you want to unpair Fido2 keys from a user group, expand the **Select Groups** tree, click **Add**, manually search for the individual groups, select the required group from the results, and click **Save**.
 - If you want to unpair Fido2 keys from the entire Organizational Unit (OU), expand the **Select Organizational Units** tree, click **Add**, manually search for the individual OU, select the required OU from the results, and click **Save**.
3. Click **Delete Fido2 Key(s)**.

Working with Redistributable Secret Management account

Redistributable Secret Management Service (rSMS) is used to manage users password across multiple connected systems. Using rSMS service you can synchronize the passwords across connected systems. The rSMS service is installed with the Password Manager software.

An rSMS account must be created and configured to interact with the rSMS service to execute password change functionality on connected systems. After creating the rSMS account and configuring certificate binding settings (optional), you can configure the settings to reset the password in connected systems.

To create rSMS account and configure certificate binding settings

1. On the home page of the Administration Site, click **General Settings**.
2. Click the **rSMS Settings** tab from the options.

The **Redistributable Secret Management Service** page is displayed.

NOTE: An rSMS account must be created before working with rSMS activity. An rSMS user is automatically created if the imported configuration file has the rSMS account details.

3. In the **Create Account** section, click **Create Account** to create an rSMS account.
4. In the **Certificate binding** section, select a custom certificate from the drop-down list, if available. By default, the built-in certificate is used.

NOTE: If you import a configuration file, the rSMS certificate binding details are not imported. The default binding settings or the certificate binding settings of the system is used.

5. Select the IP address from the **rSMS IP address** drop-down list.

NOTE: For built-in certificates, the Port number field is automatically populated with the value **20001**. For custom certificates, custom port number can be provided.

6. Click **Save Settings** to save the certificate binding settings.

NOTE:

- By default, all Password Manager logs are available in C:\Windows\TEMP folder. If the default Password Manager log path is changed during an update, rSMS automatically uses the updated log path instead of the

default path used earlier.

- Additional rSMS logs are available in the `rSMS.Service-{Date}.log` file. Enable Password Manager logging from the Administrator site under **General Settings > Logging Settings**.

Redistributable Secret Management Service supported platforms

Redistributable Secret Management Service (rSMS) supports the platforms that are mentioned here.

Platform	Description
WindowsServer	A name for a group of server operating systems released by Microsoft.
SolarisSsh	A Unix operating system, using an SSH connection.
PanosSsh	An operating system developed by Acorn Computers, using an SSH connection.
Aixssh	A series of proprietary Unix operating systems developed by IBM, using an SSH connection.
OdbcMysql	An open-source relational database management system, using an ODBC Driver.
postgres	An open-source relational database management system (RDBMS).
vsphere	Server virtualization software
IloSsh	HP Integrated Lights-Out (iLO) is a proprietary embedded server management technology, using an SSH connection
OdbcSqlServer	A relational database management system, using an ODBC Driver.
ad	Microsoft Windows Active Directory
SonicWall	SonicWall Secure Mobile Access (SMA) is a unified secure access gateway.
Aws	Amazon Web Services (AWS), an on-demand cloud computing platform.
Acf2Tn3270	IBM's Access Control Facility (z-Series), using a TN3270 connection.
F5BigIpSsh	A load balancer and a full proxy, using an SSH connection
TopSecretTn3270	CA TopSecret is a streamlined and scalable mainframe security for IBM's zseries operating system, using a TN3270 connection.

OdbcSybase	Used to manage and analyze information in relational databases, using an ODBC Driver.
PixSsh	Cisco PIX (Private Internet eXchange) is an IP firewall, using an SSH connection.
FreeBsdSsh	FreeBSD is a free and open-source Unix-like operating system, using an SSH connection.
DracSsh	Dell Remote Access Controller (DRAC) is an out-of-band management platform, using a SSH connection.
Hpuxssh	Hewlett Packard Unix Operating systems, using a SSH connection.
Acf2Ldap	Access Control Facility, a discretionary access control software security system over LDAP authentications.
RacfLdap	Resource Access Control Facility is an IBM security system that provides access control and auditing functionality for zSeries operating systems over LDAP authentications.
SapHana	A relational database management system.
LinuxSsh	Linux Operating system, using a SSH connection.
RacfTn3270	IBM's Resource Access Control Facility (z-Series), using a TN3270 connection.
SonicSsh	SonicOS, an operating system for SonicWall network security appliances (firewalls), using a SSH connection.
TopSecretLdap	CA TopSecret is a streamlined and scalable mainframe security for IBM's zseries operating system, using a SSH connection.
MongoDb	MongoDb is a cross-platform document-oriented database program.
JunosSsh	Junos OS is the FreeBSD-based operating system used in Juniper Networks hardware routers, using an SSH connection.
SapNetweaver	SAP NetWeaver is an open application server platform.
OdbcOracle	Oracle Database is a multi-model database management system, using an ODBC driver.
As400Tn3270	IBM's Application System/400, using a TN3270 driver.
FortinetSsh	Fortinet firewall client, using an SSH connection.
Ldap	A protocol used for accessing Active Directory object, user authentication, and authorization in windows server.
MacOsSsh	Apple Mac Operating system, using a SSH connection.

Customizing Redistributable Secret Management log path

By default, the rSMS logs are available in C:\Windows\Temp\rSMS. You have the option to customize the log path to record the logs at a different location.

Customizing rSMS log path

1. On the system where the Password Manager Administration Site is installed, click **Start > Services**.
2. On the **Services** window, right-click on **One Identity rSMS Service**.
3. Select **Properties** and check the location from the **Path to executable** section.
4. Open the command prompt with administrator privileges and navigate to the directory where **One Identity rSMS Service** is installed.
5. From the directory where **One Identity rSMS Service** is installed, run the `rSMS.Config.exe LogPath` command to view the rSMS log path.
The log path currently used to record rSMS logs is displayed.
6. To update the log path, run the `rSMS.Config.exe LogPath -f <new path>` command. For example, `rSMS.Config.exe LogPath -f C:\PM`.
The log path is updated. To confirm the log path run the `rSMS.Config.exe LogPath` command again.
7. Restart the **One Identity rSMS Service**.

Email templates

Password Manager provides the option to set the default template for confirmation e-mail. To send an auto generated email to user if workflow succeeds or fails, configure the email template from the **General Settings** tab for authentication.

To configure default e-mail template:

1. On the home page of the Administration Site, click **General Settings**, then click the **Email Template** tab.
2. Select the desired language from the **Select language to customize template** drop-down menu, to customize the email template.
3. Click the **+** sign before the desired workflow to edit the template. Edit the subject and body of the notification template in the default language as required. When editing the notification template, you can use the parameters available in the notification editor, for example `#USER_ACCOUNT_NAME#`, `#WORKFLOW_RESULT#`, and others.

4. In the **Message format** drop-down, select the format to use for the notifications. You can select from two options: either HTML or Plain text.
5. Select the default language from the **Select default language for email** drop down menu, to select the default email template to send to the user.
6. In the **User notification settings**, select one of the following options for user notification subscription:
 - Subscribe users to this notification. Allow users to unsubscribe.
 - Subscribe users to this notification. Do not allow users to unsubscribe.
 - Do not subscribe users to this notification. Allow users to subscribe to this notification.
7. Click **Save**, to save the settings

Upgrading Password Manager for AD LDS

This section describes how to upgrade Password Manager for AD LDS to the latest version (5.16).

You can upgrade to Password Manager 5.16 from version 5.10.0 or newer.

NOTE: Consider the following before starting an upgrade procedure:

- One Identity recommends backing up your current Password Manager for AD LDS configuration.
- One Identity recommends reinstalling the license file from the Administration Site once the upgrade is complete. Before installing the license, delete the existing **SoftLicense** binary value from the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Quest Software

- To avoid end-user data corruption, manually merge any workflows that have been customized in the previous versions of Password Manager for AD LDS into the respective workflows of the latest Password Manager for AD LDS version.

For example, if you have made any changes to the **Register** Self-Service workflow, such as adding or updating any authentication steps compared to the default configuration, then re-create the default configuration manually after upgrading to Password Manager for AD LDS 5.16.

- To update storage files with new encryption mechanisms, update all Password Manager for AD LDS realm instances with the Password Manager for AD LDS 5.16 configuration and with the same encryption key.

To do so, log in to the Administration Site from the primary Password Manager for AD LDS instance of the realm, then navigate to **General Settings > Import/Export > Export**. Copy and save the password securely, then import the configuration data in all other Password Manager for AD LDS instances by selecting the exported configuration data and providing the password.

- If the secondary instances of the Password Manager for AD LDS realm are not updated with the new configuration, the **Import configuration settings from primary instance** notification will appear in the Administration Site of every

affected Password Manager for AD LDS instance.

To import the required configuration settings, navigate to **General Settings > Import/Export > Import**, select the exported data from the primary Password Manager for AD LDS instance, then enter the saved password.

- The Shared.storage file will be encrypted and copied to AD LDS only if all replication instances of the Password Manager for AD LDS realm are updated with the Password Manager for AD LDS 5.16 configuration and encryption key.
- If all realm instances are updated with Password Manager for AD LDS 5.16, the Q&A Profiles of the users will be updated with new encryption key when the users update their Q&A Profiles.

To perform an in-place upgrade or a manual upgrade, see the applicable section:

- [Performing an in-place upgrade from an older Password Manager for AD LDS version to Password Manager for AD LDS 5.16](#)
- [Upgrading Password Manager for AD LDS manually from an older version](#)

Performing an in-place upgrade from an older Password Manager for AD LDS version to Password Manager for AD LDS 5.16

This section describes how to perform an in-place upgrade from an older version of Password Manager for AD LDS to version 5.16.

You can upgrade to Password Manager 5.16 from version 5.10.0 or newer.

To perform an in-place upgrade from an older version of Password Manager for AD LDS to version 5.16

1. From the autorun window of the installation media, click **Install against Password Manager**. Read the contents, then click **Next**.
2. Read the contents of the **Risk of data loss!** window, then select **I acknowledge the above instructions** and click **Next**.
3. Select **I accept the terms in License Agreement**, then click **Next**.
4. In the **Configuration Backup** window, provide the **File Location** and set a new password, then click **Next**.

NOTE: Do not forget to store the password securely as it is required to import the configuration post upgrade. The backup of the configuration data is now saved in the provided file location.

5. In the **Password Manager Service Account Information** window, enter the account name and the password details, and then click **Next**.
6. In the **Specify Web Site and Application Pool Identity** window, choose the website name, enter the account name and the password, and then click **Next**.
7. After completing the above process, click **Install**.

Upon successful installation, the Password Manager for AD LDS installs the following sites:

- Administration Site
- Helpdesk Site
- Password Manager Self-Service Site

Upgrading Password Manager for AD LDS manually from an older version

You can upgrade Password Manager for AD LDS manually from an older version to the newest version by:

- Uninstalling the previous Password Manager for AD LDS version.
- Installing Password Manager for AD LDS 5.16 on the computer where the earlier version of Password Manager for AD LDS was installed.

You can upgrade to Password Manager 5.16 from version 5.10.0 or newer.

NOTE: Consider the following if you plan to perform a manual upgrade of Password Manager for AD LDS:

- Make sure that you backed up your current configuration settings.
- After you uninstall the previous version of Password Manager for AD LDS, the new Password Manager for AD LDS version will automatically detect all configuration settings. For more information on how to install Password Manager for AD LDS, see [Installing Password Manager for AD LDS](#).
- If you have multiple Password Manager for AD LDS instances installed, then during the upgrade, the **Realm Instances** page of the Administration Site might display an incorrect list of installed instances. After upgrading all instances, the page will show the correct list.

To manually upgrade from an older version of Password Manager for AD LDS to version 5.16

1. From the autorun window of the Password Manager for AD LDS installation media, click **Install against Password Manager**. Read the contents, then click **Next**.
2. Select **I accept the terms in License Agreement**, then click **Next**.
3. In the **User Information** page, enter the user details such as the user name and the organization to which the user belongs to, then click **Next**.

To verify your license information, click **Licenses...**, then check the license status.

NOTE: If the license has expired, click **Browse license...**, then select the appropriate license to keep Password Manager operational.

4. In the **Custom Setup** page, click the respective option that you want to install, then click **Next**.
5. In the **Password Manager Service Account Information** page, the account name appears by default. Enter the password, then click **Next**.

NOTE: To change the account name, click **Browse...** and select the applicable Password Manager service account name.

6. In the **Specify Web Site and Application Pool Identity** page, specify the website name. Then, in the **Application pool identity** section, the account name appears by default. Enter the password, then click **Next**.

NOTE: To change the account name, click **Browse**, then select the appropriate **Application Pool Identity** account name.

7. To begin installation, click **Install**.

After completing the installation procedure, Password Manager for AD LDS deploys the following sites:

- Administration Site
- Helpdesk Site
- Self-Service Site

IMPORTANT: The option to switch to the Password Manager Self-Service Site appears only if you perform an in-place upgrade.

Password Policies

- About Password Policies
- Creating a Password Policy
- Managing Password Policy Scope
- Configuring Password Policy Rules
- Deleting a Password Policy

About Password Policies

By default, an AD LDS instance applies existing local or domain password policies. If a server on which AD LDS is installed belongs to a workgroup, the server's local password policy settings and account lockout settings are enforced. If the server on which AD LDS is running belongs to a domain, the password policy settings and account lockout settings from the domain are enforced.

You can use Password Manager to create additional password policies that define which passwords to reject or accept. For each policy, you can configure a number of rules, for example, a password age rule, complexity and length rules, custom rule, and others. It is recommended to use the custom rule to display the settings of the local or domain password policy applied to the server on which AD LDS is running. For more information, see [Custom Rule](#) on page 201.

Password policy settings are stored in Group Policy objects (GPOs). A GPO is applied to a target Organizational Unit. Group Policy objects from parent containers are inherited by default. When multiple Group Policy objects are applied, the policy settings are aggregated. For information on how to apply a password policy and change the policy priority, see [Managing Password Policy Scope](#) on page 189.

Creating a Password Policy

To create a password policy, you need add a connection to the AD LDS instance to which this policy will be applied.

The account you use to access the AD LDS instance for which you want to create password policies should have the following permissions:

- The Read permission for attributes of the `groupPolicyContainer` objects.
- The Write permission to create and delete the `groupPolicyContainer` objects in the System Policies container.
- The permission to create and delete container and the `serviceConnectionPoint` objects in Group Policy containers.
- The Read permission for the attributes of the container and `serviceConnectionPoint` objects in Group Policy containers.
- The Write permission for the `serviceBindingInformation` and `displayName` attributes of the `serviceConnectionPoint` objects in Group Policy containers.

To connect to AD LDS instance

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click **Connect to AD LDS instance** to add an instance for which you want to create password policies.
3. If connections already exist, select a connection from the list. If you want to create a new connection, click **Add new connection**.
4. If you selected to create the new connection, in the **Connect to AD LDS Instance** dialog, configure the following options:
 - In the **Server name on which AD LDS instance is installed** text box, type the name of the server to which you want to connect.
 - In the **Port number (LDAP or SSL)** text box, enter the port number that you specified when installing the AD LDS instance. If you select the **Use SSL** check box, enter the SSL port number; otherwise, LDAP port number. It is recommended to use SSL in your production environment.
 - In the **Application directory partition** text box, enter the name of the application directory partition from the AD LDS instance to which you want to connect.
 - In the **Application directory partition alias** text box, type the alias for the application directory partition which will be used to address the partition on the Self-Service Site.
 - In the **Access account** section, select **Password Manager Service account** to have Password Manager access the AD LDS instance using the Password Manager Service account, otherwise, select **The following Active Directory**

account or **The following AD LDS account** radio button and enter the required user name and password.

5. Click **Save**.

For more information on modifying settings for the connection, see [AD LDS Instance Connections](#) on page 163.

To create a password policy

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click the **<N> One Identity Password Policies** or **One Identity Password Policies are not configured** link under the application directory partition that you want to manage.
3. On the **One Identity Password Policies for <application directory partition>** page, click the **Add a policy** button or **Add new password policy** link.
4. In the **Add New Policy** dialog, type a name for the new policy and click **Save**.

To configure settings for a password policy

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click the **<N> One Identity Password Policies** link under the application directory partition that you want to manage.
3. On the **One Identity Password Policies for <application directory partition>** page, click **Edit** under the policy whose properties you want to view or modify.
4. On the **Policy Settings** tab of the **Password Policy Properties** dialog, view or modify the following options, and then click **Save**:

Table 13: Password Policy Properties

Option	Description
Disable this policy	Select this check box to temporarily turn off the policy.
Policy name	View or modify the name of the password policy.

5. Click the **Policy Rules** tab to configure the password policy rules by using the procedure outlined in [Configuring Password Policy Rules](#) on page 192, then click **Save**.
6. Click the **Policy Scope** tab to manage the password policy links by using the procedure outlined in [Managing Password Policy Scope](#) on page 189, then click **Save**.

Managing Password Policy Scope

This section provides information on how to apply a password policy to Organizational Units and groups in a managed AD LDS instance.

Applying Password Policies

In Password Manager (Password Manager) application, scopes can be defined at multiple levels. Scopes act as a boundary in which you can define the groups and Organizational Unit (OU), and can also associate policies into it.

The **Default Management Policy** allows you to configure both the user scope and the help desk scope. In the Management Policy scope, an admin can also associate the workflows, activities, and Q&A policy to the configured user groups and OU.

While configuring the user scope/help desk scope, an admin must define either a **Group** or an **OU** to indicate which group or OU can access the Self-Service Site/Helpdesk Site. This means the users who are part of the configured group/OU comes under included group category. You could also define a different group/OU under an excluded group category. This means users who are part of these excluded group or OU cannot access Self-Service Site/Helpdesk Site.

In case of Password Policy scope, admin needs to ensure the following

- Password policies should only be applied to the user groups/ OUs that are part of the user scope.
- Group that will be associated into the password policy scope must be part of the OU as well. This means users who are part of the group must also be the part of the OU as those users will have the same set of activities to be performed in the Self-Service Site.
- An Administrator can create one or more password policies and can map each policy to single/ multiple user groups or OUs.
- By default, the newly created password policy is linked to the Domain name created in the management policy scope and gets applied to the "Authenticated users group. It means that all the users that are part of the usergroups and OUs configured in the user scope, will have the password policy applied.
- Group that will be associated into the password policy scope must be part of the OU as well. This means users who are part of the group must also be the part of the OU as those users will have the same set of activities to be performed in the Self-Service Site.

NOTE:

- While configuring the Policy Scope in Password Policy Properties window, it is mandatory to add both the group and the Organizational Unit that the user is part of, for the policy rules to get applied for the users accessed in the Self-Service Site.
- It is not possible to configure the same domain multiple times in a user scope, whereas multiple domains can be configured to the user scope.

The table below provides more information on different scenarios.

Let us consider the following groups/OU

NOTE: Do not define both OU and the group in the Management policy scope for the set password policy rule to get applied in the Self-Service Site.

S.No	User scope				Password Policy Scope		Password Policy	Logged in Self-Service Site	Is Password Policy applicable?
	Included Group	Included OU	Excluded Group	Excluded OU	OU	Group			
1.	Group1	OU1			OU-1	Group1	Password Policy1	User1	Yes
2.	Group1	OU2	Group2		OU-1	Group2	Password Policy2	User2	No
3.	Group3	OU1	Group1		OU 2	Group3		User2	No
4.	Group3	OU3		OU1	OU 3	Group3	Password Policy3	User3	Yes
5.	Group2	OU2			OU 1	Group2		User2	No
6.	Group1	OU1		OU4	OU 4	Group1	Password Policy4	User1	No
7.	Group2	OU2		OU5	OU 5	Group2		User2	No
8.	Group3	OU3	Group1			Group3	Password Policy 5	User3	No
9.	Group3	OU3	Group2		OU 3			User3	No

To link a password policy to Organizational Units and groups

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click the **One Identity Password Policies** link under the application directory partition that you want to manage.
3. On the **One Identity Password Policies for <application directory partition>** page, click **Edit** under the policy whose properties you want to view or modify.
4. Click the **Policy Scope** tab.
5. Click the **Add** button under **This policy is applied to the following Organizational Units**, and then browse for an Organizational Unit.
6. Click the **Add** button under **This policy is applied to the following groups**, and then browse for a group.
7. Click **Save**.

Changing Policy Priority

When multiple password policies affect an Organizational Unit or a group, only the policy with the highest priority is applied to such group or Organizational Unit. A newly created password policy is disabled by default.

NOTE: Only priority of policies with the same scope can be changed.

To change policy priority

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click the **One Identity Password Policies** link under the AD LDS instance for which you want to change the policy link order and click **Policy priority**.
3. In the **Change Policy Priority** dialog, move policies up or down in the list by selecting them and clicking the **Move Up** or **Move Down** buttons.

Configuring Password Policy Rules

Password Manager uses a set of powerful and flexible rules to define requirements for passwords. Each password policy has rules that are configured independently of the rules in other policies.

NOTE: Password Manager for ADLDS does not support Dictionary rule in OI Password policies.

For each password policy, you can set up the following rules:

- **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.
- **Symmetry rule:** Ensures that password or its part does not read the same in both directions.
- **Custom rule:** Use this rule to enter the settings of the local or domain password policy applied to the server on which AD LDS is running, if you want to display these settings to users on the Self-Service Site when users reset or change passwords. You can also use this rule to display your custom messages and to hide the configured policy rules.

Password Compliance

When you use **Forgot My Password** or **Manage My Passwords** workflow to set or reset the password, you can view the compliance of the password with the configured password policy. You can expand a policy and view the rules set for the policy. When you enter a new password, you can instantly get the feedback about the compliance of the password with the defined rules. A green tick mark against the rules in a policy indicates that the password is in compliance with the rule, and help you to set a compliant password.

You can also view the strength of the password using the Password strength meter, which get displayed as a progress bar when you enter a new password in the **New password** text box. The Password strength meter assess the strength of the password by verifying the password with the configured password policy rules and the basic requirements (one upper case letter, one lower case letter, one numeric value, one special character and minimum of seven characters) for a password. This will help to improve the security of the password. You can enable or disable this feature and configure the Password strength status. For more details see [Customization of Password Strength Meter](#) on page 227.

The following is a general procedure for configuring the password policy rules.

To configure rules for a password policy

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click the **<N> One Identity Password Policies** link under the AD LDS instance that you want to manage.
3. On the **One Identity Password Policies for <application directory partition>** page, click the policy whose properties you want to modify, and then click the **Policy Rules** tab.
4. On the **Policy Rules** tab, click the rule that you want to configure, and, under the rule's name, modify the appropriate rule settings.
5. Repeat step 4 for each of the rules that you want to configure for this password policy, and then click **Save**.

NOTE: Starting from version 5.9.5, if a Password Manager policy is applied, then the **Next** button remains disabled in the Forgot my password/ Manage My Passwords screen and gets enabled only when all the Password Manager's policies are met and shows GREEN.

For information about how to configure each of the policy rules, see the sections below.

Password Age Rule

The password age rule ensures that users cannot use expired passwords or change their passwords too frequently.

Specify **Minimum password age** so that passwords cannot be changed until they are more than a certain number of days old. If a minimum password age is defined, users must wait for the specified number of days to change their passwords.

Specify **Maximum password age** so that passwords expire as often as necessary for your environment.

To configure the password age rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Password Age Rule** to expand the rule settings.
3. Under **Password Age Rule**, select the **Specify password age** check box, then specify the following options as required:

Table 14: Password age limit

Option	Description
Minimum password age	Specifies for how many days users must keep new passwords before they can change them.
Maximum password age	Specifies for how many days a password can be used before the user is required to change it.

Length Rule

The length rule ensures that passwords contain the required number of characters.

Define a minimum length so that passwords must consist of at least a specified number of characters. Long passwords - seven or more characters - are usually stronger than short ones. With this setting, users cannot use blank passwords, and they have to create passwords that are a certain number of characters long.

To configure the length rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Length Rule** to expand the rule settings.
3. Under **Length Rule**, select the **Password must contain** check box, and then specify the following options as required:

Table 15: Password length limit

Option	Description
Minimum characters	Set the minimum number of characters that a password must contain.
Maximum characters	Set the maximum number of characters allowed in a password.

Complexity Rule

The complexity rule ensures that passwords meet the following minimum complexity requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (Supported characters are ~`!#\$%^&*+=-[]; ,/ { } . _ | " : < > ? () @

The complexity rule imposes the same requirements as the standard Windows policy "Password must meet complexity requirements."

To configure the complexity rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Complexity Rule** to expand the rule settings.
3. Under **Complexity Rule**, select the **Password must meet complexity requirements** check box.

Required Characters Rule

The required characters rule ensures that passwords contain certain character categories. Required characters are necessary to make a password stronger. For example, if you set the minimum number of uppercase characters to 4, then the password "ElEPhant" will be rejected.

To configure the required characters rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Required Characters Rule** to expand the rule settings.
3. Under **Required Characters Rule**, select the **Password must contain at least** check box, and then specify the following options as required:

Table 16: Required character rules

Option	Description
Alphabetic characters	Set the minimum number of alphabetic characters (A-z) that must appear in a password.
Lowercase characters	Set the minimum number of lowercase characters (a-z) that must appear in a password.
Uppercase characters	Set the minimum number of uppercase characters (A-Z) that must appear in a password.
Unique characters	Set the number of characters that must be unique within a password. To require case sensitivity for this setting, select Case sensitive .
Digits (0-9)	Specify whether passwords must contain digits (0-9): To set the minimum number of digits that must appear in a password, select Minimum and then enter the required number. In the In positions field, enter the number of the character positions within a password where digits must appear. For example, 1, 3, 5-10 . To specify how many digits must be at the end of a password, use Number of ending characters ,

Option	Description
Special characters	<p>Specify whether passwords must contain special characters:</p> <p>To set the minimum number of special characters that must appear in a password, select Minimum and then enter the required number.</p> <p>In the In positions field, enter the number of the character positions within a password where special characters must appear. For example, 1,3,5-10.</p> <p>To specify how many special characters must be at the end of a password, use Number of ending characters,</p> <p>Special characters include the following characters: - !"#\$\$%&'()*+,-./:;<=>?@[\\]^_`{ }~</p>

Disallowed Characters Rule

The disallowed characters rule rejects passwords that contain certain character categories. The categories include digits from 0-9 and special characters such as "#\$%". If you specify that special characters must not appear in the beginning of a password, then the password "@work" will be rejected.

To configure the disallowed characters rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Disallowed Characters Rule** to expand the rule settings.
3. Under **Disallowed Characters Rule**, select the **Password must not contain** check box, and then specify the following options as required:

Table 17: Disallowed character rule

Option	Description
Digits (0-9)	<p>Specify whether the rule will reject passwords containing digits.</p> <p>Select the In positions check box, and then type the numbers of positions within a password where digits must not appear. For example, 1,3,5-10.</p> <p>Select the Number of ending characters check box, and then specify how many digits there must not be in the end of a password.</p>
Special characters	<p>Specify whether the rule will reject passwords containing special characters.</p> <p>Select the In positions check box, and then type the numbers of positions within a password where special characters must not appear. For example, 1,3,5-10.</p>

Option	Description
	Select the Number of ending characters check box, and then specify how many special characters there must not be in the end of a password. Special characters include the following characters: - !"#%&'()*+,-./:;<=>?@[\\]^_`{ }~

Sequence Rule

The sequence rule rejects passwords that contain more repeated characters than it is allowed.

Repeated characters can appear in succession or in different positions in a password. This policy also includes characters typed in direct or inverse numerical or alphabetical order. For example, if you set the maximum number of same characters that appear in succession to 3, then the password "eeeege1e" will be rejected.

To configure the sequence rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. To expand the rule settings, on the **Policy Rules** tab, click **Sequence Rule**.
3. Under **Sequence Rule**, select **Password must not contain more than** and then specify the following options:

Table 18: Password sequence rule

Option	Description
Number of characters repeated in succession (AAAB)	Set the maximum number of same characters in a row that the policy will tolerate before rejecting a password.
Number of identical characters (ABCA)	Set the maximum number of same characters typed in different positions of password that the policy will tolerate before rejecting a password.
Number of characters in direct or inverse numerical or alphabetical order (ABC_321)	Set the maximum number of characters typed in direct or inverse numerical or alphabetical order that the policy will tolerate before rejecting a password.
Case sensitive	Select this check box to require case sensitivity for this rule.

User Properties Rule

The user properties rule rejects passwords that contain part of a user account property value.

This rule splits the user account property value by non-alphanumeric characters (for example, “_”), and then checks if any part of the value is available in the password. For example, if user’s name is “Peter_US”, Password Manager splits the property into: “Peter” and “US”, and checks if any part can be found in the password. For example, the password “US_US” will be rejected.

To configure the user properties rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **User Properties Rule** to expand the rule settings.
3. Under **User Properties Rule**, select the **Prevent users from using account properties as part of passwords** check box, and then specify the following options:

Table 19: User properties rule

Option	Description
Initial characters of a user property value	<p>Set the maximum number of initial characters from a user property value that users are allowed to use as part of their passwords.</p> <p>For example, if a user's full name is “Anna Fairweather”, and the option value is set to 3, then the user is allowed to type the strings “Ann” and “Fai” as part of her password. The password will be rejected if it contains “Anna” or “Fair”.</p> <p>You can select from the following user account properties:</p> <ul style="list-style-type: none"> • displayNamePrintable • mailNickname • userPrincipalName • displayName • title • sn • samAccountName • personalTitle • middleName • mail • givenName • employeeID • cn

NOTE: The administrator can add other user attributes to the existing list of attributes and select to use. Click **Add other attribute to the list** to add other user attributes.

Option	Description
The entire value of a user property	Select to reject passwords containing the entire value of a user property. You can select any of the user account properties listed in the description of the Initial characters of a user property value option above.
Case sensitive	Select this check box to require case sensitivity for this rule.
Enable bi-directional analysis	Select to reject passwords containing the entire value of a user property or its part (depending on which of the two previous options you have selected), if read backwards.

Symmetry Rule

The symmetry rule ensures that a password or its part does not read the same in both directions.

For example, if you enable the **Reject passwords that read the same in both directions** option, then the password "redivider" will be rejected.

To configure the symmetry rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Symmetry Rule** to expand the rule settings.
3. Under **Symmetry Rule**, select the **Password must comply with symmetry criteria** check box, and then specify the following options:

Table 20: Symmetry criteria

Option	Description
Reject passwords that read the same in both directions (pass8ssap)	Select to reject passwords that are palindromes.
Maximum number of initial characters that match ending characters of password if read backwards (pas47sap)	Specify the number of initial characters matching the ending characters of password, if read backwards, which the policy will tolerate before rejecting a password.
Maximum number of consecutive characters within a password, that read the same in both directions (pass4554word)	Specify the number of password characters in a row that read the same in both directions, which the policy will tolerate before rejecting a password.
Case sensitive	Select to define this rule as case sensitive.

Custom Rule

You can use this rule to create your own password policy message to be displayed on the Self-Service Site when users change or reset their passwords. For example, use this rule to enter the settings of the local or domain password policy applied to the server on which AD LDS is running.

If you want to hide all other policy messages and display your custom message to users, enable this policy rule, enter the message text, and select the **Hide messages from other policy rules and display only this message** check box. If you do not select this check box, messages from all enabled policy rules will be displayed.

Note, that this rule does not check the password compliance with the configured password policy. Configure this rule to display your custom message instead of or together with other policy messages when users change or reset passwords on the Self-Service Site.

To configure the custom rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 192.
2. On the **Policy Rules** tab, click **Custom Rule** to expand the rule settings.
3. Under **Custom Rule**, select the **Enable** check box to enable this rule.
4. Select the **Hide messages from other policy rules and display only this message** check box if you want users to see only the custom password rule message and hide all other password policy messages.
5. In the text box, enter the rule message in the default language (English). To enter the message in other languages, click the **Add new language** link, select the language, specify the message and click **OK**.

NOTE: Only languages of the user interface of the Self-Service Site are available in the list

Deleting a Password Policy

In Password Manager, you can delete password policies after creating them.

For more information on password policies, see [About Password Policies](#).

To delete a password policy

1. On the home page of the Administration Site, click the **Password Policies** tab.
2. Click the **One Identity Password Policies** link under the AD LDS instance that you want to manage.
3. Click **Remove** under the policy that you want to delete.

NOTE: When you delete a password policy, the deleted policy is no longer valid for an AD LDS instance. To restore a deleted password policy, create a new policy and manually configure its settings as required.

Enable 2FA for Administrators and Enable 2FA for HelpDesk Users

This section describes the steps to enable 2FA to protect AD LDS Administration Site and Helpdesk Site users.

To enable 2FA for Administrators and HelpDesk Users

1. On the home page of the AD LDS Administration Site, click the **Management/2FA enforcement** tab.
2. Select **Use Secure Token Server for authentication** checkbox for admin authentication and/or helpdesk authentication, then choose one of the Secure Token Server providers, which you need to use for 2FA authentication. The login interface presentation can be selected from the **Choose the behaviour of the authentication** dropdown.
3. Click **Save** to save the settings.

NOTE: At least one Secure Token Server provider needs to be configured. If there is an external provider, which loads their content while sending a **X-Frame-Options : Deny** header, then the **iframe** option will not work. In this case, the **redirect** or the **popup** option is required.

Reporting

[Reporting and User Action History Overview](#)

[Best Practices for Configuring Reporting Services](#)

Reporting and User Action History Overview

Password Manager provides a simple and convenient way to view, print, and save reports and charts allowing you to analyze information on how the application is used. The reporting functionality within the solution is based on Microsoft SQL Server Reporting Services as a common reporting environment.

The Reports section of the Administrator 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

The user action history provides records of all actions performed by users registered with Password Manager. You can search for records using a full-text search functionality. The user action history is provided by Enterprise Auditing Service embedded in Password Manager.

To use Password Manager reports, you need to connect to an SQL Server and a Report Server.

To use the user action history functionality, you need to connect to an SQL Server only.

Alternative options

You can use predefined Power BI templates to generate interactive reports as an alternative to **Reporting**. For more information on Power BI, see [Working with Power BI templates](#).

Setting Up Reporting Environment

To enable the reporting functionality of Password Manager, ensure that the following requirements are met:

- A SQL Server is deployed in your environment and the Password Manager database is configured on that server.
- A SQL Server Reporting Services report server is installed in your working environment.
- You have configured a connection to the report server through the Administration Site.

The interactive Web-based reports are built on data that the report server retrieves from the Password Manager SQL database, and can be either viewed online or exported into multiple file formats.

Using Password Manager for AD LDS reports

You can create and view Password Manager for AD LDS reports using the Password Manager for AD LDS Administration Site, and can also save them to multiple file formats. Password Manager for AD LDS generates reports based on the data stored in the Password Manager for AD LDS database with a report server.

Prerequisites

To use the Password Manager for AD LDS reporting functionalities, make sure that you meet the following requirements:

- You have an SQL Server to store the Password Manager for AD LDS database and the Password Manager for AD LDS log data.

NOTE: Make sure that the account that is used by Password Manager to access the SQL Server has `db_owner` permissions to create and write data to the database.

- The SQL Server is connected to a report server.

NOTE: When connecting to the report server for the first time, Password Manager for AD LDS attempts to publish the reports to the report server and

populate the list of reports on the **Reporting** page of the Password Manager for AD LDS Administration Site.

Because of this, before connecting to a report server, make sure that the account that Password Manager for AD LDS uses has administrator rights on the report server.

Configuring Password Manager for AD LDS reporting

You can configure reporting for Password Manager in the Password Manager for AD LDS Administration Site.

To configure Password Manager for AD LDS reports

1. On the Password Manager Administration Site, click **Reporting**.
2. Under **Reporting and User Action History**, click **Reports > Connect to SQL Server and Report Server**.
3. In the **SQL Server Connection Settings** dialog that appears, specify the following settings, then click **Next**:

Table 21: SQL server connection settings

Setting	Description
SQL Server	Specifies the SQL Server that is used to store the Password Manager database. You can specify the server's name, FQDN, or IP address.
Database name	Specifies the name of the SQL database where Password Manager will log data for the reports. If the specified database does not exist, you will need to confirm creating it, and you will also need to select an account for creating the database.
Force server certificate trust	If selected, then Password Manager will trust the certificate of the SQL Server, even if it is invalid or otherwise not trusted by the machine running Password Manager. IMPORTANT: One Identity strongly recommends using a trusted SQL Server and selecting this setting only temporarily until a trusted certificate is configured for the SQL Server.
Select an account for connecting to the SQL server	Specifies the account that is used for connecting to the SQL Server. The following options are available: <ul style="list-style-type: none">• Password Manager Service account: If selected, Password Manager will attempt to access the SQL Server and database with the Password Manager Service account.

Setting	Description
	<ul style="list-style-type: none"> • Specific SQL Server account: If selected, Password Manager will attempt to access the SQL Server and database with the specified SQL account credentials.
Enable retry queue for failed messages	<p>If selected, Password Manager stores audit data in a local database whenever it cannot write them to the SQL Server. Password Manager then attempts to send the locally stored audit data with the Retry failed auditing messages scheduled task to the SQL Server, according to the run settings of the scheduled task. After the locally stored auditing messages are successfully written to the SQL Server, they are deleted from the local database.</p>

NOTE: If you use Password Manager to manage a large number (10,000s or 100,000s) of users and the SQL Server remains unreachable for a longer period of time, then storing auditing data locally with this setting enabled might use up substantial disk space over time.

If this happens, then to free up disk space, you can delete locally-stored audit data as follows:

1. In the machine running Password Manager, open `services.msc`.
2. In the list of services, find the following two services and stop them:
 - Password Manager Service
 - Password Manager Workflow Service
3. Delete the following file:

`C:\ProgramData\One Identity\Password Manager\auditing.db`

If the **Retry failed auditing messages** scheduled task succeeds in writing local audit data to the SQL Server database, then Password Manager will automatically delete the sent audit data from the `auditing.db` local storage.

TIP: Consider the following:

- One Identity recommends selecting this setting if you frequently experience network interruptions and access issues towards the SQL Server.
- To prevent potential service interruptions and timeouts in the Password Manager processes accessing the SQL

Setting	Description
	Server, One Identity strongly recommends configuring an SQL Server that is accessed only by Password Manager processes.

If selected, this setting has two options:

- **Local SQL writer process timeout:** Specifies the time interval (in milliseconds) after which the attempts of the Password Manager SQL writer process to resend locally stored audit data to the SQL Server database are considered to be timed out. The allowed value range is 10–600,000 ms and the default value is 60,000 ms.

TIP: One Identity recommends setting a lower value for this option if the Password Manager processes have exclusive access to the SQL Server, and a higher value if other, non-Password Manager services and processes can also access the SQL Server database.

This is because SQL Server databases can only be written by a single process at a time, which might result in process queuing if the SQL Server is accessed by multiple processes.

- **Local SQL command timeout:** Specifies the default SQL command timeout, that is the time interval (in seconds) after which Password Manager SQL queries sent to the configured SQL Server are considered to be timed out. The allowed value range is 1–600 seconds, and the default value is 60 seconds.

4. In the **Report Server Connection Settings** dialog, specify the following settings:

Table 22: Report server connection settings

Setting	Description
Report Server URL	Specifies the URL of the report server in the following format: http://<server-name>/<report-instance> In this syntax, <server-name> is the name of the server where the report server resides, while <report-instance> is the name of the report server instance.
Report Manager URL	(Optional) Specifies the URL of the report manager in the following format:

Setting	Description
	<p>http://<server-name>/<manager-instance></p> <p>In this syntax, <server-name> is the name of the server where the report manager resides, while <manager-instance> is the name of the report manager instance.</p>
Specify the account for deploying SSRS reports	<p>Specifies the user name and password of the user account that Password Manager for AD LDS will use when accessing the report server.</p> <p>NOTE: The specified account must have the necessary permissions to deploy reports. For more information, see Grant users access to a report server in the <i>Microsoft SQL documentation</i>.</p>
Specify the account that the Report Server will use to connect to the data source	<p>Specifies the user name and password of the user account that the report server will use when accessing the data source.</p> <p>You can specify either Windows credentials or SQL Server credentials. If you select Windows credentials, then select the Use as Windows credentials when connecting to the data source check box as well.</p> <p>NOTE: The specified account must have db_owner permissions to the database.</p>

Creating and previewing a Password Manager for AD LDS report

After you configured reporting as described in [Configuring Password Manager for AD LDS reporting](#), you can create and preview Password Manager for AD LDS reports in the Password Manager for AD LDS Administration Site.

To create and preview Password Manager for AD LDS reports

1. On the Password Manager for AD LDS Administration Site, click **Reporting**.
2. Under **Reporting and User Action History**, click **Reports**.
3. On the **Reports** page that appears, click the report that you want to create and preview. The following table lists the reports included with Password Manager for AD LDS.

IMPORTANT: To view Password Manager for AD LDS reports, the account used to view reports must have permissions to read data from the report server database. By default, Windows integrated authentication is used to access the

report server database. If you want to change access settings to the report server database, edit the appropriate settings on the report server.

Table 23: Reports and user action history

Report Name	Description
User status (table)	<p>A table report that displays:</p> <ul style="list-style-type: none"> • The list of users in the managed domains. • The states of the users' Q&A profiles in Password Manager for AD LDS. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p>TIP: Use this report to:</p> <ul style="list-style-type: none"> • Check the registered and unregistered users managed by Password Manager for AD LDS. • Check which users must re-create their Q&A profiles or which users are scheduled for a Q&A profile update. </div>
User status (pie chart)	A pie chart that shows the percentage of the total number of users for each Q&A Profile states.
Actions by user (table)	<p>A table report that shows:</p> <ul style="list-style-type: none"> • The actions that each user performed in Password Manager for AD LDS. • Whether the result of a user action was successful or not. <p>You can specify the time interval for this report to check.</p>
Actions by user (pie chart)	A pie chart that shows the percentage of the total number of user actions for all user action types within the specified time interval, such as registering to Password Manager for AD LDS or password reset attempts.
Registrations by month (bar chart)	A bar chart that shows the number of users who registered to Password Manager for AD LDS in the specified monthly period.
Actions by month (bar chart)	A bar chart that shows the number of user actions that were performed in Password Manager for AD LDS in the specified monthly period.
Actions by type (table)	A table report that shows the user actions performed in Password Manager for AD LDS within the specified time period, sorted by action type.
Help desk usage by	A table report that shows the actions performed in the Password Manager for AD LDS Helpdesk Site within the specified time

Report Name	Description
actions (table)	period.
Help desk usage by operators (table)	A table report that shows: <ul style="list-style-type: none"> The actions that each helpdesk operator performed in the Password Manager for AD LDS Helpdesk Site within the specified time period. Whether the results of their actions were successful or not.
Help desk usage by users (table)	A table report that shows the actions that each helpdesk operator performed in the Password Manager for AD LDS Helpdesk Site for specific users within the specified time period.
E-mail notifications by user (table)	A table report that lists the email notifications sent to specific users within the specified time period.
E-mail notifications by type (table)	A table report that summarizes the email notifications sent to users within the specified time period, sorted by action type.

4. After the selected report is created, it appears in the Report Viewer in a new browser window. If needed, select the zoom ratio in the drop-down list on the toolbar.
5. (Optional) To go to a particular page, enter the page number in the leftmost text box on the toolbar and press **Enter**. Alternatively, use the navigation arrows besides the text box.
6. (Optional) To modify report parameters, set the new parameter values by using the group of controls in the upper area of the Report Viewer. Then, click **View Report**.
7. To close the Report Viewer and return to the **List of Reports** page, close the **Report Viewer** window.

Searching, exporting and printing a Password Manager for AD LDS report

If you have previously created Password Manager for AD LDS reports, you can search, export and print them later with the Report Viewer.

To search, export or print Password Manager for AD LDS reports

1. (Optional) In the Report Viewer, in the **Find Text** text box of the menu bar, enter the text you are looking for, then click **Find**. In case of multiple results, to find the next occurrence, click **Next**.
2. (Optional) To export a report, from the **Select a format** drop-down list on the menu bar, select the target file format, then click **Export**. The Report Viewer supports the following file formats:

- XML file (.xml)
 - Microsoft Excel Comma Separated Values file (.csv)
 - TIFF file (.tiff)
 - Portable Document Format (.pdf)
 - Web archive file (.mhtml)
 - Microsoft Excel Worksheet (.xls)
3. (Optional) To print a report, click the printer icon on the menu bar, then in the **Print** window, click **OK**.

Browsing the User Action History

"User action history" is a history of all actions that have been performed by all users registered in Password Manager for AD LDS. This functionality is provided by the Enterprise Auditing Service. This service is installed along with Password Manager for AD LDS, and does not require any manual configuration.

Prerequisites

To view user action history, you must have an active connection configured to an SQL Server.

To connect to an SQL Server for using user action history

1. On the Password Manager Administration Site, click **Reporting**.
2. Under **Reporting and User Action History**, click **History** > **Connect to SQL Server**.
3. On the **History** page, click **Connect to SQL Server**.
4. In the **SQL Server Connection Settings** dialog that appears, specify the following settings, then click **Next**:

Table 24: SQL server connection settings

Setting	Description
SQL Server	Specifies the SQL Server that is used to store the Password Manager database. You can specify the server's name, FQDN, or IP address.
Database name	Specifies the name of the SQL database where Password Manager will log data for the reports. If the specified database does not exist, you will need to confirm creating it, and you will also need to select an account for creating the database.

Setting	Description
Force server certificate trust	<p>If selected, then Password Manager will trust the certificate of the SQL Server, even if it is invalid or otherwise not trusted by the machine running Password Manager.</p> <p>IMPORTANT: One Identity strongly recommends using a trusted SQL Server and selecting this setting only temporarily until a trusted certificate is configured for the SQL Server.</p>
Select an account for connecting to the SQL server	<p>Specifies the account that is used for connecting to the SQL Server. The following options are available:</p> <ul style="list-style-type: none"> • Password Manager Service account: If selected, Password Manager will attempt to access the SQL Server and database with the Password Manager Service account. • Specific SQL Server account: If selected, Password Manager will attempt to access the SQL Server and database with the specified SQL account credentials.
Enable retry queue for failed messages	<p>If selected, Password Manager stores audit data in a local database whenever it cannot write them to the SQL Server. Password Manager then attempts to send the locally stored audit data with the Retry failed auditing messages scheduled task to the SQL Server, according to the run settings of the scheduled task. After the locally stored auditing messages are successfully written to the SQL Server, they are deleted from the local database.</p> <p>NOTE: If you use Password Manager to manage a large number (10,000s or 100,000s) of users and the SQL Server remains unreachable for a longer period of time, then storing auditing data locally with this setting enabled might use up substantial disk space over time.</p> <p>If this happens, then to free up disk space, you can delete locally-stored audit data as follows:</p> <ol style="list-style-type: none"> 1. In the machine running Password Manager, open <code>services.msc</code>. 2. In the list of services, find the following two services and stop them: <ul style="list-style-type: none"> • Password Manager Service • Password Manager Workflow Service 3. Delete the following file: <pre>C:\ProgramData\One Identity\Password Manager\auditing.db</pre>

Setting	Description
---------	-------------

If the **Retry failed auditing messages** scheduled task succeeds in writing local audit data to the SQL Server database, then Password Manager will automatically delete the sent audit data from the `auditing.db` local storage.

TIP: Consider the following:

- One Identity recommends selecting this setting if you frequently experience network interruptions and access issues towards the SQL Server.
- To prevent potential service interruptions and timeouts in the Password Manager processes accessing the SQL Server, One Identity strongly recommends configuring an SQL Server that is accessed only by Password Manager processes.

If selected, this setting has two options:

- **Local SQL writer process timeout:** Specifies the time interval (in milliseconds) after which the attempts of the Password Manager SQL writer process to resend locally stored audit data to the SQL Server database are considered to be timed out. The allowed value range is 10–600,000 ms and the default value is 60,000 ms.

TIP: One Identity recommends setting a lower value for this option if the Password Manager processes have exclusive access to the SQL Server, and a higher value if other, non-Password Manager services and processes can also access the SQL Server database.

This is because SQL Server databases can only be written by a single process at a time, which might result in process queuing if the SQL Server is accessed by multiple processes.

- **Local SQL command timeout:** Specifies the default SQL command timeout, that is the time interval (in seconds) after which Password Manager SQL queries sent to the configured SQL Server are considered to be timed out. The allowed value range is 1–600 seconds, and the default value is 60 seconds.

Searching for user action history records

After connecting to the SQL Server, you can search among user action history entries, either by performing a full text search, or by looking for various user actions by user name,

email, activity, domain, and so on.

To search for user action history records

1. On the Password Manager Administration Site, click **Reporting**.
2. Under **Reporting and User Action History**, click **History**.
3. To search for a user action, on the **History** page, enter the search term then click **Search**. Then, sort the search results by their relevance or date.

Managing Connections to SQL Server and Report Server

On the Reporting page of the Administration Site, you can edit or remove existing connections to SQL and Report Servers.

To edit connections, under **Reporting and User Action History**, click the **Edit Connections** link and specify required values.

To remove connections, under **Reporting and User Action History**, click the **Disconnect Servers** link. Note, that all existing connections will be removed.

Best Practices for Configuring Reporting Services

This section provides instructions on how to configure the Reporting Services component. SQL Server Reporting Services component builds reports using the data that SQL Server stores in the Password Manager database. This database must be configured on the SQL Server.

SQL Server Reporting Services allows you to create and view reports that provide statistical data on how Password Manager is used, for example how many users have created their Questions and Answers profiles, how many users need to update their Questions and Answers profiles, what actions each user or helpdesk operator has performed in Password Manager, and so on.

The following topics are covered:

- Reporting Services default configuration
- Reporting Services authorization issues
- Reporting Services firewall issues

Reporting Services Default Configuration

The SQL Server Reporting Services component and the Management Tools component must be installed to use the Password Manager Reporting functionality. Make sure that you select the required features when running the Microsoft SQL Server Setup.

Use the Reporting Services Configuration tool to configure SQL Server Reporting Services. If you installed a report server using the **Install but do not configure the server** option, you must use this tool to configure the server prior to using it. If you installed a report server using the **Install the default configuration** option, you can use this tool to verify or modify the settings that were specified during setup.

It is recommended to select the **Install the default configuration** option during SQL Server and Reporting Services setup on the **Report Server Installation Options** page of the Setup Wizard. In most cases this will save you much time and effort as long as Reporting Services default configuration is concerned.

Reporting Services Configuration tool can be used to configure a local or a remote report server instance. You must have local system administrator permissions on the computer that hosts the report server you want to configure.

NOTE: Remote data sources are not supported by SQL Server Reporting Services included in Microsoft SQL Server Express Edition.

To configure the Reporting Services default configuration

1. Start the **Reporting Services Configuration** tool.
2. Enter the SQL Server machine name and the Report Server Instance name and then click **Connect**.

IMPORTANT: Sequentially configure the Report Server options listed in the left pane of the Reporting Services Configuration tool. There must not be any Not configured options after the configuration is finished.

3. Open the **Report Server Virtual Directory Settings** section.
4. Click **New** to create a new virtual directory. This opens a dialog with the default settings entered. To accept the default settings click **OK**.
5. Click **Apply**.
6. Check the **Apply default settings** checkbox and click **Apply**.
7. Open the **Report Manager Virtual Directory Settings** section.
8. Click **New** to create a new virtual directory. This opens a dialog with the default settings entered. To accept the default settings click **OK**.
9. Click **Apply**.
10. Open the **Web Service Identity** section.

11. Click **Apply** to accept the default application pool names for the Report Server and the Report Manager
 - OR -
 - Click **New** to specify your own application pool names.
12. Click **Apply**.

The Reporting Services feature requires an SQL Server database (different from the Password Manager database) to store report server service data.

You can create the report server database in the following ways:

- Automatically through Setup, if you choose the default configuration installation option in the SQL Server Installation Wizard, by selecting the **Install the default configuration** option in the **Report Server Installation Options** page.
- Manually through Reporting Services Configuration tool.

To create a report server database

1. Start the Reporting Services Configuration tool and connect to the report server instance you want to configure (the default instance name is **MSSQLSERVER** for SQL Server and **SQLEXPRESS** for SQL Server Express Edition).
2. In the **Database Setup** page, click **Connect**. This opens a SQL Server Connection dialog.
3. Type the name of the SQL Server database engine you want to use.
4. Select the type of credentials used to connect to the SQL Server. You can specify a SQL Server login or use your credentials. The credentials you specify must have permission to log on to the server. Click **OK**.
5. In the **Database Setup** page, click **New**. This reopens the SQL Server Connection dialog.
6. Type the name of the SQL Server database engine and select credentials. The credentials you specify must have permission to create a database.
7. Type the name of the report server database. A temporary database is created along with the primary database.
8. Choose the language to use, and then click **OK**.
9. In the **Database Setup** page, specify the credentials used by the report server to connect to the report server database.
 - Select the **Service credentials** option to use the Windows service account and Web service account to connect through integrated security.
 - Select the **Windows credentials** option to specify a domain user account. A domain user account must be specified as **<domain>\<user>**.
 - Select the **SQL Server credentials** option to specify a SQL Server login.
10. Click **Apply**.

A report server database can be created on a local or on a remote SQL Server database engine instance.

When you finish the Report Server configuration restart the Report Server instance for the changes to take effect. You can restart the Report Server by sequential clicking the **Stop** button and then the **Start** button at the **Server Status** tab of the Reporting Services Configuration tool. If the configuration is performed correctly, the Initialization will be successfully passed for the Report Server instance.

Follow this checklist to verify Password Manager reporting functionality configuration and settings.

Table 25: Reporting functionality configuration and settings

Step	Reference
Ensure that MS SQL Server with the Reporting Services component is installed and configured.	See the MS SQL Server documentation.
Install Password Manager and its components.	See Installing Password Manager for AD LDS on page 12.
Ensure that the DefaultAppPool , PMAdminADLDS , PMSelfServiceADLDS , PMHelpdeskADLDS , and ReportServer application pools are running in the IIS Manager on the Password Manager and the Report Services servers. If any of these pools are not running, start them manually.	
Ensure that the Default Web Site is running in the IIS Manager on the Password Manager and the Report Services servers. If the web site is not running – start it manually.	
Connect to the Reporting Services server through the Password Manager Administration Site.	

The interactive Web-based reports are built using the data that the report server retrieves from the Password Manager SQL database.

For more information on Reporting Services setup and configuration, refer to SQL Server documentation.

Reporting Services Firewall Issues

If Password Manager fails to operate properly when Reporting Services are separated from Password Manager by a firewall, specific ports should be open in the firewall.

To get the complete list of Password Manager server port numbers, that have to be open for the application to function properly, see [Appendix B: Open Communication Ports for Password Manager for AD LDS](#) on page 222.

Accounts Used in Password Manager for AD LDS

The following accounts can be used in Password Manager:

- Password Manager Service account
- Application pool identity
- Access account for AD LDS
- Password policy account

The Password Manager Service Account

Password Manager Service account is used to install Password Manager. For Password Manager to run successfully, the Password Manager Service account must be a member of the Administrators group on the Web server where Password Manager is installed.

Application Pool Identity

Application pool identity is an account under which the application pool's worker process runs. The account you specify as the application pool identity during Password Manager setup will be used to run Password Manager websites.

Application pool identity account must meet the following requirements:

- This account must be a member of the **IIS_IUSRS** local group on the Web server in IIS 7.0.
- This account must have permissions to create files in the <Password Manager installation folder>\App_Data folder.
- Application pool identity account must the full control permission set for the following registry keys: HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager for AD LDS.

Access Account for Application Directory Partition Connection

When you connect to an AD LDS instance, you can create a new connection or use existing connections, if any. When creating the connection, you must specify an access account - an account under which Password Manager will access the AD LDS instance and a specified application directory partition. You can use the Password Manager Service account, an Active Directory account or an AD LDS account. These accounts must have the following minimum set of permissions:

- Membership in the Domain Users group (for the Password Manager Service account and the Active Directory account)
- Membership in the Readers group in the application directory partition (for the AD LDS account)
- Membership in the Administrators group in the configuration directory partition
- The Read permission for all attributes of user objects
- The Write permission for the following attributes of user objects: `pwdLastSet`, `comment`, `unicodePwd`, `lockoutTime`, `msDS-UserAccountDisabled`
- The right to reset user passwords
- The permission to create user accounts and containers in the Users container
- The Read permission for attributes of the `organizationalUnit` object and container objects
- The Write permission for the `gpLink` attribute of the `organizationalUnit` objects and container objects
- The Read permission for the attributes of the container and `serviceConnectionPoint` objects in Group Policy containers
- The permission to create container objects in the System container
- The permission to create the `serviceConnectionPoint` objects in the System container
- The permission to delete the `serviceConnectionPoint` objects in the System container
- The Write permission for the `keywords` attribute of the `serviceConnectionPoint` objects in the System container

If you want to use the same connection in password policies as well, make sure the account has the following permissions:

- The Read permission for attributes of the `groupPolicyContainer` objects.
- The Write permission to create and delete the `groupPolicyContainer` objects in the System Policies container.
- The permission to create and delete container and the `serviceConnectionPoint` objects in Group Policy containers.

- The Read permission for the attributes of the container and serviceConnectionPoint objects in Group Policy containers.
- The Write permission for the serviceBindingInformation and displayName attributes of the serviceConnectionPoint objects in Group Policy containers.

Corporate Authentication

In the Register workflow, if the Admin selects **Corporate authentication**, the user can only review the corporate account details during the registration process. If the Admin selects **Allow user to edit corporate details**, the user can update the respective corporate details, for example, **Corporate email** and **Corporate phone number**, if the details are not previously populated by the administrator in the AD.

If **Corporate authentication** registration mode is selected in the **Register** activity, make sure that **Domain management account** has the following set of permissions.

1. The read permission for **Corporate email** attribute and **Corporate phone** attribute where, **Mobile** is the default attribute for the **Corporate phone**.
2. If **Allow user to edit corporate details** checkbox is selected under **Corporate authentication** check box, both Read and Write permission must be available for **Corporate email** attribute and **Corporate phone** attribute, where **Mobile** is the default attribute for the **Corporate phone**.

NOTE: If the **Corporate phone** attribute under **Reinitialization** page is a custom value (for example, **pager**) then the Read/Write Permissions need to be provided for that attribute instead of the **mobile** attribute.

Appendix B: Open Communication Ports for Password Manager for AD LDS

This section provides a list of communication ports that need to be open in the firewall for Password Manager to function properly.

Administration Site

- Port **80** (Default HTTP) TCP Inbound
- Port **443** (Default HTTPS) TCP Inbound/Outbound
- Port **8081** TCP Inbound/Outbound
- Port **25** (Default SMTP port) TCP Outbound
- Port **135** TCP Inbound/Outbound

Helpdesk Site

- Port **80** (Default HTTP) TCP Inbound
- Port **443** (Default HTTPS) TCP Inbound/Outbound
- Port **8081** TCP Inbound/Outbound

Password Manager Service

- Port **53** (Outgoing DNS lookups) UDP Outbound
- Port **88** (Kerberos Authentication) TCP/UDP Outbound
- Port **389** (LDAP Access) TCP/UDP Outbound
- Port **636** (LDAP Access) TCP Outbound
- Port **137** (NetBIOS Name Service) TCP Outbound
- Port **139** (NetBIOS Session Service) TCP Outbound
- Port **8081** TCP Inbound

NOTE: To modify the default port of **8081**, see [Modifying service connection settings](#).

Port **20000** (Secure Token Service) TCP Inbound

Port **20001** (rSMS) TCP Inbound

SQL Server

Port **1433** (SQL Server) TCP/UDP Outbound

Port **1434** (SQL Server Browser Service) TCP/UDP Outbound

Password Manager Workflow Service

Port **20002** TCP Inbound

NOTE: To modify the default port of **20002**, see [Modifying service connection settings](#).

Password Manager Self-Service (PMSelfService) and Helpdesk (PMHelpdesk) standalone hosts

Port **20002** TCP Outbound

NOTE: To modify the default port of **20002**, see [Modifying service connection settings](#).

Report Server

Port **80** (SQL Server Report Services) TCP Outbound

Email Notification

Port **25** (Default SMTP port) TCP Outbound

Telesign

Port **443** TCP Outbound

Defender

Port specified in the activity settings (Authenticate with Defender) is used.

Customization Options Overview

There are multiple ways to customize the Self-Service and Helpdesk sites. You can customize email notifications, change company and product logos and Web sites color scheme, and so on.

The following customization options are available in Password Manager:

- [Customization of Steps in Password Manager Self-Service Site, and Helpdesk Tasks](#)
- [Email Notification Customization](#)
- [User Agreement Customization](#)
- [Account Search Options Customization](#)
- [Web Interface Customization](#)
- [Customization of Password Policies List](#)
- [Customization of Password Strength Meter](#)

Customization of Steps in Password Manager Self-Service Site, and Helpdesk Tasks

You can change the steps and the order of steps in self-service and helpdesk tasks by modifying the workflows that correspond to these tasks. For example, to modify the Forgot My Password task on the Self-Service Site you need to modify the Forgot My Password workflow on the Administration Site.

A workflow consists of activities; each activity can be configured independently of other activities. Almost each activity corresponds to a single step in a task, that is a single page in the wizard a user goes through to complete the task.

By adding and removing activities and changing activities' order in a self-service workflow you can define what wizard pages and in what order users will go through when performing a task on the Self-Service Site. The same applies to the Helpdesk Site and helpdesk workflows.

To edit a workflow, open the workflow on the Administration Site and add or remove activities in the workflow designer.

For more information on configuring workflows, see [Workflow structure](#) on page 74.

For more information on modifying self-service workflows and activities, see [Password Manager Self-Service Site workflows](#)

For more information on modifying helpdesk workflows and activities, see [Helpdesk Workflows](#) on page 110.

Email Notification Customization

By adding the notification activities into a workflow, you can send notifications to users and administrators about successful or failed workflows. The following notification activities are available:

- Email user if workflow succeeds
- Email user if workflow fails
- Email administrator if workflows succeeds
- Email administrator if workflow fails

Password Manager offers user notification templates for all predefined workflows in 16 languages. You can customize the notification template by editing the **Email user if workflow succeeds** and **Email user if workflow fails** activities.

Templates are not provided for administrator notifications. To create administrator notifications, edit the **Email administrator if workflows succeeds** and **Email administrator if workflow fails** activities.

If you want to send email notifications in other languages, you can add more languages to the language list for the required notifications.

For more information on customizing email notifications, see [Customizing Notifications](#) on page 107.

User Agreement Customization

In any self-service task Password Manager allows you to include a page with an end-user agreement. You can use it to obtain users' consent to store their personal information that may be available in their Q&A profiles.

To do this, add the **Display user agreement** activity to required workflows. When configuring this activity, you can use the predefined end-user agreement template or create your own. You can also specify the agreement text in several languages. The default agreement text template is available in 16 languages.

For more information on configuring the end-user agreement, see [Display User Agreement](#) on page 106.

Account Search Options Customization

Account search options allow you to customize the Find Your Account page of the Self-Service Site. You can allow users to search for their accounts on the Self-Service Site or turn off the search options and require them to enter their logon names.

If you allow users to search for their accounts, you can specify how many user accounts and what user properties will be displayed in search results.

To configure account search options, on the Administration Site, open **General Settings** and click the **User Identification** tab.

For more information on account search options, see [Search and Logon Options](#) on page 132.

Web Interface Customization

Using Password Manager Administration Site, you can customize the Web interface of the Self-Service and Helpdesk sites, that is, change company and product logos and modify the sites' color scheme.

To customize the Web interface of the Self-Service and Helpdesk sites, on the Administration Site, open **General Settings** and click the **Web Interface Customization** tab.

For more information, see [Web Interface Customization](#) on page 156.

Customization of Password Policies List

When a user changes or resets password on the Self-Service Site, the password policy rules specified for the user's application directory partition can be displayed on the page where the user is required to enter a new password.

To modify the list of password policy rules displayed on the Self-Service Site, edit the rules specified for the application directory partition on the Password Policies tab of the Administration Site.

For more information, see [Configuring Password Policy Rules](#) on page 192.

Customization of Password Strength Meter

You can customize the Password strength meter on the Helpdesk Site and Self-Service Site.

To enable Password strength meter:

- In the web.config file, set the value of PasswordStrengthMeterEnable to **true** as follows:

```
<appSettings>
  <add key="PasswordStrengthMeterEnable" value="true"/>
</appSettings>
```

To disable Password strength meter, set the value of PasswordStrengthMeterEnable to **false**.

You can customize the text displaying the strength of the Password strength meter.

To customize the text:

- In the Common.xml file present in the LocalizationStorage folder, you can modify values in the Resource Ids to display the required text:

```
<Resource Id="PasswordStrengthMeter.Text">
  <Value><[[Password strength:]]></Value>
</Resource>
```

```
<Resource Id="PasswordStrengthMeter.VeryWeak">
  <Value><[[Very weak]]></Value>
</Resource>
```

```
<Resource Id="PasswordStrengthMeter.Weak">
  <Value><[[Weak]]></Value>
</Resource>
```

```
<Resource Id="PasswordStrengthMeter.Good">
  <Value><[[Good]]></Value>
</Resource>
```

```
<Resource Id="PasswordStrengthMeter.Strong">
  <Value><[[Strong]]></Value>
</Resource>
```

```
<Resource Id="PasswordStrengthMeter.VeryStrong">  
  <Value><[[Very strong]]></Value>  
</Resource>
```

For more information, see [Password Compliance](#).

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product