



One Identity Password Manager for AD LDS 5.13.1

Administration Guide

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.




Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

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

Password Manager for AD LDS Administration Guide
Updated - October 2023
Version - 5.13.1

Contents

About Password Manager for AD LDS	1
Password Manager for AD LDS overview	1
Getting Started	3
Different sites for Different roles	3
Password Manager for AD LDS Components	4
Licensing	4
Installing the License	5
Updating the license	9
Telephone Verification feature license	9
Checklist: Installing Password Manager for AD LDS	10
Installing Password Manager for AD LDS for AD LDS	10
Configuring Password Manager for AD LDS Service Account and Application Pool Identity	11
Enabling HTTPS	11
Installing Password Manager for AD LDS	12
Extending AD LDS Schema	13
Initializing instance	14
Installing Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk Sites on a Standalone Server	15
FailSafe support in Password Manager for AD LDS	18
Installing multiple instances of Password Manager for AD LDS	18
Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites	19
Step 1: Obtain and install custom certificates from a trusted Windows-based Certification Authority	20
Step 2: Providing certificate issued for server computer to Password Manager for AD LDS service	21
Step 3: Providing certificate issued for client computers to Self-Service and Helpdesk Sites	22
Password Manager for AD LDS Architecture	23
Password Manager for AD LDS Components and Third-Party Solutions	23
The Password Manager for AD LDS Service and the Administration site	25

Self-Service site	25
Helpdesk site	26
TeleSign	26
SQL Server Database and SQL Server Reporting Services	26
One Identity Quick Connect Sync Engine	26
Defender	27
Password Manager Secure Token Server	27
RADIUS Two-Factor Authentication	30
Redistributable Secret Management Service	31
Location sensitive authentication	31
Working with Power BI templates	32
Password Manager for AD LDS Credential Checker	33
Typical Deployment Scenarios	34
Simple Deployment	35
Deployment of the Legacy Self-Service, Password Manager for AD LDS Self-Service and Helpdesk Sites on Standalone Servers	35
Realm deployment	37
Multiple Realm Deployment	38
Password Manager for AD LDS in a perimeter network	39
Installing Password Manager for AD LDS in Perimeter Network with Reverse Proxy ..	39
Management Policy Overview	40
Management Policy components	40
Management Policy and other Password Manager for AD LDS settings	42
Password Policy Overview	42
reCAPTCHA Overview	43
How it works	44
How to Use reCAPTCHA on Password Manager for AD LDS Sites	45
System Requirements for Using reCAPTCHA	45
References	45
User Enrollment Process Overview	45
Questions and Answers Policy Overview	46
Q&A Policy and Authentication	47
Q&A Policy and User Enforcement	47
Data Replication	48
Storing Data	48

Replicating data	48
Changing replication settings	49
Phone-Based Authentication Service Overview	50
How It Works	51
How to use phone-based authentication	52
System requirements	52
Configuring Management Policy	53
Configuring Permissions for Access Account	53
Connecting to AD LDS Instance	54
Changing Access Account	56
Removing Connection to AD LDS Instance	57
Adding Secret Questions	57
Editing and Deleting secret questions	58
Management Policies	60
Checklist: Configuring Password Manager for AD LDS	60
Understanding Management Policies	61
Configuring Access to the Administration Site	62
Configuring Access to the Legacy Self-Service Site and Password Manager for AD LDS Self-Service site	63
Configuring Access to the Helpdesk Site	63
Changing Access Account	65
Removing Connection to AD LDS Instance	66
Configuring Questions and Answers Policy	66
Creating Secret Questions	66
Editing and Deleting secret questions	69
Configuring Q&A Profile Settings	70
Workflow overview	72
Workflow structure	72
Workflow states	73
Workflow settings	74
Custom workflows	77
Importing and exporting workflows	78
Custom Activities	79
Custom Activity Settings	79
Creating custom activities	80

Importing and exporting custom activities	81
Removing Custom Activities	82
Legacy Self-Service or Password Manager for AD LDS Self-Service site workflows	82
Register	83
Configuring country code drop-down menu	84
Manage My Profile	84
Forgot My Password	85
Manage My Passwords	85
Unlock My Account	86
My Notifications	86
I Have a Passcode	86
Overview of Built-in Legacy Self-Service and Password Manager for AD LDS Self-Service site Activities	87
Authentication Activities	87
Action Activities	94
Notification Activities	102
Helpdesk Workflows	105
Verify User Identity	106
Assign Passcode	106
Reset Password	106
Unlock Account	107
Unlock Profile	107
Enforce Update of Profile	107
Overview of Built-in Helpdesk Activities	108
Authentication Activities	108
Action Activities	111
Notification Activities	116
User Enforcement Rules	118
Invite Users to Create/Update Profiles	118
Remind Users to Create/Update Profiles	121
Remind Users to Change Password	123
General Settings	125
General Settings Overview	125
Search and Logon Options	126
Configuring Search Options for the Self-Service Site	126

Partial user search on external network	128
Configuring Security Options	129
Configuring Search Options for the Helpdesk Site	130
Configuring Security Settings	131
Hiding personally identifiable information for logged-in users	131
Configuring anti-bot security settings	132
Import/Export Configuration Settings	137
Exporting Configuration Settings	137
Importing Configuration Settings	138
Outgoing Mail Servers	138
Diagnostic Logging	140
Scheduled Tasks	141
Invitation to Create/Update Profile Task	141
Reminder to Create/Update Profile Task	142
Reminder to Change Password Task	143
Maximum Password Age Policy Task	144
Update RADIUS server status	144
User Status Statistics Task	145
Clear Old Records from Reporting Database	146
Web Interface Customization	147
Instance Reinitialization	149
Modifying Service Connection Settings	150
Modifying Advanced Settings	150
Realm Instances	153
AD LDS Instance Connections	153
Using Connections to AD LDS Instances	153
Specifying Access Account for AD LDS Instance Connections	154
Changing Access Account for AD LDS Instance Connections	156
Removing Connection to AD LDS Instance	156
Extensibility Features	156
Extensibility Features Overview	157
RADIUS Two-Factor Authentication	158
Internal Feedback	159
Password Manager for AD LDS components and third-party applications	159
Password Manager for AD LDS Secure Token Server	159

Configuring Password Manager Secure Token Server	162
Unregistering users from Password Manager for AD LDS	164
Bulk Force Password Reset	165
Fido2 key management	165
Working with Redistributable Secret Management account	166
Redistributable Secret Management Service supported platforms	167
Customizing Redistributable Secret Management log path	169
Email Templates	169
Upgrading Password Manager for AD LDS	171
In-place upgrade from 5.8.2 or later versions to 5.13.1	173
Manual upgrade from 5.9.x or later versions	173
Password Policies	176
About Password Policies	176
Creating a Password Policy	177
Managing Password Policy Scope	178
Applying Password Policies	179
Changing Policy Priority	181
Configuring Password Policy Rules	181
Password Compliance	182
Password Age Rule	183
Length Rule	183
Complexity Rule	184
Required Characters Rule	184
Disallowed Characters Rule	185
Sequence Rule	186
User Properties Rule	187
Symmetry Rule	188
Custom Rule	189
Deleting a Password Policy	190
Enable 2FA for Administrators and Enable 2FA for HelpDesk Users	191
Reporting	192
Reporting and User Action History Overview	192
Setting Up Reporting Environment	193
Using Reports	193

User Action History	197
Managing Connections to SQL Server and Report Server	198
Best Practices for Configuring Reporting Services	198
Reporting Services Default Configuration	199
Reporting Services Firewall Issues	202
Accounts Used in Password Manager for AD LDS	203
The Password Manager for AD LDS Service Account	203
Application Pool Identity	203
Access Account for Application Directory Partition Connection	204
Account for Using One Identity Quick Connect	205
Appendix B: Open Communication Ports for Password Manager for AD LDS	206
Customization Options Overview	208
Customization of Steps in Legacy Self-Service site, Password Manager for AD LDS Self-Service site, and Helpdesk Tasks	208
Email Notification Customization	209
User Agreement Customization	210
Account Search Options Customization	210
Web Interface Customization	210
Customization of Password Policies List	211
Customization of Password Strength Meter	211
Feature imparities between the legacy and the new Self-Service Sites	213
About us	214
Contacting us	214
Technical support resources	214
Glossary	215

About Password Manager for AD LDS

[Password Manager for AD LDS overview](#)

Password Manager for AD LDS overview

Password Manager for AD LDS is a web-based application that provides an easy-to-implement and use, yet highly secure, password management solution. Users can connect to Password Manager by using their favorite browser and perform password self-management tasks, thus eliminating the need for assistance from high-level administrators and reducing help desk workload. The solution offers a powerful and flexible password policy control mechanism that allows the Password Manager for AD LDS administrator to ensure that all passwords in the organization comply with the established policies.

Password Manager for AD LDS allows managing users that do not have accounts in the Active Directory. For example, using Password Manager for AD LDS you can manage passwords for contractors and other external users.

Integration with One Identity Quick Connect Sync Engine, Redistributable Secret Management Service facilitates cross-platform password synchronization that enables Password Manager for AD LDS to change user passwords across multiple connected data sources.

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

- **Global access.** Password Manager for AD LDS provides 24/7/365 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 logon options.
- **Strong data encryption and secure communication.** The solution relies on industry-leading technologies for enhanced communication security and data encryption.
- **Cross-platform password synchronization.** Password Manager for AD LDS has been designed to use One Identity Quick Connect Sync Engine, Redistributable Secret Management Service, which makes it possible to automatically synchronize

users' passwords across multiple connected data sources.

- **Web interface for a Helpdesk service.** Password Manager for AD LDS features the Helpdesk site that allows administrators to delegate Helpdesk tasks to dedicated operators. These tasks include resetting user passwords, managing users' Questions and Answers profiles, and assigning temporary passcodes to users.
- **x64 version of Password Policy Manager.** An x64 version of Password Policy Manager module has been designed for use on domain controllers running an x64 Microsoft Windows Server operating system.
- **E-mail 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-organization 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 users provide their secret answers when registering with Password Manager for AD LDS.
- **Enhanced user name search options.** Users can be allowed to view their account attributes, such as user logon name, first name, display name, and SMTP address, when searching for their forgotten user names. A more specific search query returns 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 a Web farm environment.

Getting Started

[Different sites for Different roles](#)

[Password Manager for AD LDS Components](#)

[Licensing](#)

[Checklist: Installing Password Manager for AD LDS](#)

[Installing Password Manager for AD LDS for AD LDS](#)

[Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites](#)

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 Sites:**
 - **legacy Self-Service site:** provides users with the ability to easily and securely manage their passwords, thus eliminating the need for assistance from high-level administrators and reducing Helpdesk workload.
 - **Password Manager for AD LDS Self-Service Site:** In Password Manager for AD LDS version 5.13.1, you have the option to access the Password Manager for AD LDS Self-Service site. The Password Manager for AD LDS self-service site provides functionality similar to the legacy Self-Service site. The

Password Manager for AD LDS Self-Service site includes enhancements to the user interface to improve the usability of the site. The Password Manager for AD LDS Self-Service site and the legacy Self-Service site can coexist and it is possible to revert to the legacy Self-Service site.

Password Manager for AD LDS Components

Password Manager for AD LDS includes the following components:

Table 1: Password Manager for AD LDS Components

Component	Description	Importance
Password Manager for AD LDS x64	The suite of role-based sites that expose the functionality of Password Manager for AD LDS to end users. NOTE: One Identity recommends that you do not install Password Manager for AD LDS on the machine where the Domain Controller (DC) server is installed.	Required

Licensing

The Password Manager for AD LDS license specifies the maximum number of user accounts in the Password Manager for AD LDS across all domains. The Admin can identify whether the installation is legally compliant running the User Status Statistics (USS) tasks, where the scheduler counts the actual number of user accounts, and compares it with the maximum number specified by the license. If a deviation occurs between the actual licenses purchased and the number of users using it, the status of the license changes accordingly in the Admin site indicating whether the installation is compliant or not.

To view the compliance statuses of the license

1. Login to the Admin site.
2. On the left pane, click **Licensing**. The Licenses page appears.
3. Click the **Licenses** tab and view the **Compliant** column.

In the Licenses page, you can view the licensing information of both Password Manager for AD LDS and Telephone Verification, if installed.

The table below provides more information on various compliant status.

Conditions	Status	Description
If the total number of users in the user scope exceeds the purchased license or if the license expires	✖	Appears when the license is not compliant.
If the total number of users in the user scope matches with the purchased license or when the user count does not exceed, and the license does not expire	✔	Appears when the license is compliant.
If the total number of users exceeds the purchased license or if the license expires	?	Appears when the license is not compliant. By clicking this icon, a pop up window appears indicating the reason for not being compliant.

To view the license number, navigate to the **About** section in the Administration site and click **Licenses** tab. The License Number appears.

In the event of a license violation, you have the following options

- Exclude the additional number of user accounts from the user accounts managed by Password Manager for AD LDS to bring your license count in line with the licensed value and run the User Status Statistics(USS) scheduled task in the Administration site to recalculate and display the new user counts.
- Remove one or more managed domains to decrease the number of managed user accounts.
- Purchase a new license with a greater number of user accounts, and then update your license using the instructions provided later in this section.

Note that the following items are not limited by the license

- The number of computers connected to the Administration, Self-Service, and Helpdesk sites of Password Manager for AD LDS.
- The number of Password Manager for AD LDS instances in a large enterprise. Password Manager for AD LDS can be installed on multiple computers for enhanced performance and fault tolerance.

Installing the License

The license is initially installed when you install the Password Manager for AD LDS:

1. In the Installation Wizard, click **Licenses** to display the **License status** dialog.
2. Click **Browse license**, locate and open your license key file using the **Select License File** dialog, and then click **Close**.

Some license types may include counters for managed persons and managed external persons along with a counter for user accounts. Managed persons are users that have several accounts; for example, one managed person can have three user accounts. Managed external persons are external or temporary employees. The same license violation policy is applied 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 for AD LDS.

NOTE: License scopes are available only if your license includes managed persons and managed external persons.

To add AD LDS instance to the managed persons scope

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, 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.
 - 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, 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 for AD LDS access the AD LDS instance using the Password Manager for AD LDS 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](#) on page 53.

6. 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. 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 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. 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. 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, 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 for AD LDS 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](#) on page 53.

6. 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. 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. Click **Save**.

Updating the license

If you have purchased a new license, you need to 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 that is already installed.

To update the license

1. On the menu bar of the Administration site, click **Licensing**.
2. On the **Licenses** page, click **Install License**.
3. Select the license key file.
4. Click **Save**.

Telephone Verification feature license

Password Manager for AD LDS requires a separate license for the Telephone verification feature that allows users to authenticate themselves via one-time PINs received as text messages or through automated voice calls. For more information about this feature, see [Phone-Based Authentication Service Overview](#).

You can install this license during Password Manager for AD LDS installation or provide the license file later on the Administration site. To install the license after Password Manager for AD LDS installation, see [Updating the license](#).

You must specify a separate scope of users for telephone verification service. Only users included in the scope will have access to the service.

License violation occurs in the following cases:

- The actual number of users exceeds the maximum licensed number for the telephone verification service. In this case, users will not be able to authenticate via phone if you do not decrease the number of user accounts set in the scope or do not update the license.
- The license for the telephone verification service expired. In this case, you will have a grace period of 30 days during which the telephone verification service is available. Once the grace period has expired, users will not be able to authenticate via phone, but, other authentication mechanisms (for example, Q&A), are not affected by expiry/non-compliance of this Telephone Verification license.

Checklist: Installing Password Manager for AD LDS

This checklist provides tasks that an administrator should perform when installing Password Manager for AD LDS.

Table 2: Checklist for installing Password Manager for AD LDS

Step	Reference
Before you install Password Manager for AD LDS, you should configure Password Manager Service account and application pool identity.	Configuring Password Manager for AD LDS Service Account and Application Pool Identity on page 11
It is strongly recommended that you enable HTTPS on the server where Password Manager for AD LDS is installed.	Enabling HTTPS on page 11
Install an instance of Password Manager for AD LDS.	Installing Password Manager for AD LDS
Extend AD LDS schema	Extending AD LDS Schema on page 13
Initialize a Password Manager for AD LDS Instance	Initializing instance on page 14

Installing Password Manager for AD LDS for AD LDS

This section describes how to install Password Manager for AD LDS. 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 AD LDS. For more information see [Typical Deployment Scenarios](#) on page 34.

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 for AD LDS Service Account and Application Pool Identity

When installing Password Manager for AD LDS, you are prompted to specify two accounts: Password Manager for AD LDS Service account and application pool identity. Password Manager for AD LDS Service account is an account under which Password Manager for AD LDS Service runs. You can also use Password Manager for AD LDS 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 for AD LDS 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 for AD LDS Web sites.

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

- Password Manager for AD LDS Service account must be a member of the Administrators group on the web server where Password Manager for AD LDS 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 for AD LDS, make sure that the Password Manager for AD LDS Service account and application pool identity have the rights listed above.

Enabling HTTPS

We strongly recommend that you use HTTPS with Password Manager for AD LDS. 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 [Configuring Secure Sockets Layer in IIS 7](#) in the *Microsoft Windows Server 2008 R2 and Windows Server 2008 documentation*.

NOTE: To enable the Password Manager for AD LDS installation to be redirected from HTTP to use HTTPS by default, the HSTS (web security policy mechanism) functionality must be enabled. To enable HSTS in Password Manager for AD LDS, in the HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager registry key, set the registry value of the HSTSEnabled string to **true**.

Installing Password Manager for AD LDS

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

To install Password Manager for AD LDS

1. Depending on the hardware, run **Password Manager x86** or **Password Manager x64** from the installation media autorun window.
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**: Click **Licenses** and specify the path to the license file

NOTE: A license file is a file with the .asc extension that you have obtained from your One Identity representative.

4. On the **Custom Setup** page, select the components to install, and then click **Next**:
 - a. **Full Installation**: Select this option to install the Password Manager for AD LDS Service and the Administration, Self-Service and Helpdesk sites on this computer.
 - b. **Legacy Self-Service Site**: Select this option to install only the legacy Self-Service site.
 - c. **Password Manager Self-Service Site**: Select this option to install only the Password Manager for AD LDS Self-Service site.
 - d. **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 Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk sites on a standalone server. For more information about installing the Self-Service and Helpdesk sites on a standalone server, see [Installing Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk Sites 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 for AD LDS Service. If you want Secure Password Extension to use another Self-Service site. For more information, see [Locating Self-Service Site](#).

5. On the **Password Manager Service Account Information** page, specify the name and password for the Password Manager for AD LDS Service account, and then click **Next**. Use the following user name format: **DOMAIN\Username**. For more information on the requirements for the Password Manager for AD LDS Service account, see [Configuring Password Manager for AD LDS 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, and then click **Next**. For more information on the requirements for the application pool identity, see [Configuring Password Manager for AD LDS 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 Password Manager for AD LDS websites and Password Manager for AD LDS Service. After installing Password Manager for AD LDS, if the Web sites (Self-Service and Helpdesk) and the Password Manager for AD LDS Service are installed on different computers, it is recommended to replace these certificates with new ones. For more information, see [Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites](#).

Extending AD LDS Schema

To use Password Manager for AD LDS 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 for AD LDS 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 instance

After installing Password Manager for AD LDS on your computer, you need to initialize an instance before you begin to configure a new Management Policy: that is, before configuring the user and Helpdesk scopes, Questions and Answers policy, and managing workflows. When initializing a Password Manager for AD LDS instance, you can choose one of the two options: Create a unique instance or a replica of an existing instance. When you create a replica of the existing instance, the new instance shares its entire configuration with the existing instance. Password Manager for AD LDS instances sharing the same configuration are referred to as a Password Manager for AD LDS realm. For more information about Password Manager for AD LDS realms, see [Installing multiple instances of Password Manager for AD LDS](#).

To initialize Password Manager for AD LDS instance

1. Open the Administration site by entering the following address: **http(s)://<ComputerName>/PMAAdmin**, where <ComputerName> is the name of the computer on which Password Manager for AD LDS is installed. You can obtain the URL path to the Admin site from your system administrator. On the logon page, enter your user name and password and click **Log on**. The **Instance Initialization** page will be displayed automatically.
NOTE: For Password Manager for AD LDS versions 5.8.x or later, users must be a part of the local PMAAdmin group and either of IIS_IUSRS or Administrators group to access the PMAAdmin site.
2. 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.
3. If you have selected the option **Replica of an existing instance**, follow the instructions provided later in [Installing multiple instances of Password Manager for AD LDS](#).
4. If you have 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 for AD LDS Service. If you decide to install the Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk sites separately from the Password Manager for AD LDS Service, it is recommended to replace the built-in certificate that is used encrypt traffic between the Service and the sites. For more information, see [Specifying](#)

Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites.

- **Port number:** Specify the port that the Self-Service and Helpdesk sites will use to connect to the Password Manager for AD LDS Service. By default, port **8081** is used.

5. Under **Advanced settings**, specifying the following:

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

NOTE: Users' answers will be encrypted if the **Store answers using reversible encryption** option is selected in the Q&A Profile settings. 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 for AD LDS uses SHA-256 hashing algorithm. Password Manager for AD LDS will hash users' answers if **Store answers using reversible encryption** option is not selected in the Q&A profile settings.
- d. **Store user's Questions and Answers profile in the following attribute of user's account in Active Directory-** In the text box, type the attribute name that will be used for storing Q&A profile data. By default, Password Manager for AD LDS stores Q&A profile data in the comment attribute of each user's account and configuration data in the comment attribute of a configuration storage account, which is automatically created when installing Password Manager for AD LDS.

6. Click **Save** to complete instance initialization.

Installing Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk Sites on a Standalone Server

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

When deploying Password Manager for AD LDS in a perimeter network, it is recommended to install the Password Manager for AD LDS Service and the sites in a corporate network at first (that is, use the Full Installation option in the Password Manager for AD LDS setup),

and then install only the legacy Self-Service or the Password Manager for AD LDS Self-Service site in the perimeter network.

When you use this installation scenario, only one port should be open in the firewall between the corporate network and the perimeter network (by default, port number **8081** is used).

To install Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk sites on a standalone server

1. Depending on the hardware, run **Password Manager x64** from the installation media autorun window.
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, and then click **Next**:
 - a. **Full name**: Enter your name.
 - b. **Organization**: Enter the name of your organization.
 - c. **Licenses**: Click this button and specify the path to the license file.

NOTE: A license file is a file with the .asc extension that you have obtained from your One Identity representative.

4. On the **Custom Setup** page, select the **Legacy Self-Service Site**, **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 for AD LDS Service Account and Application Pool Identity](#).
6. Click **Install**.
7. When installation is complete, click **Finish**.

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

To initialize the Legacy Self-Service site and the Password Manager Self-Service site

1. Open the Legacy Self-Service site by entering the following address: **http(s)://<ComputerName>/PMUser**, where <ComputerName> is the name of the computer on which Self-Service site is installed.

For the Password Manager Self-Service site, enter the following address: **http(s)://<ComputerName>/PMSelfService**.

The **Self-Service Site Initialization** page will be displayed automatically.
2. In the **Computer name or IP address** text box, specify the Password Manager Service host name or IP address.

3. In the **Port number** text box, specify the port number that the Self-Service site will use to connect to the Password Manager Service.
4. From the **Certificate name** drop-down list, select the name of the certificate to be used by this site. By default, Password Manager for AD LDS uses a built-in certificate issued by Password Manager for AD LDS. You can specify a custom certificate for authentication and traffic encryption between the Password Manager Service and the websites (Self-Service and Helpdesk). For more information on using custom certificates, see [Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites](#).

NOTE: Before selecting a custom certificate on the Self-Service site, specify a custom certificate on the Administration site.

5. Click **Save**.

To initialize the Helpdesk site

1. Open the Helpdesk site by entering the following address: **http(s)://<ComputerName>/PMHelpdesk**, where <ComputerName> is the name of the computer on which Helpdesk site is installed. The **Helpdesk Site Initialization** page will be displayed automatically.
2. In the **Computer name or IP address** text box, specify the Password Manager Service host name or IP address.
3. In the **Port number** text box, specify the port number that the Helpdesk site will use to connect to the Password Manager Service.
4. From the **Certificate name** drop-down list, select the name of the certificate to be used by this site. By default, Password Manager for AD LDS uses a built-in certificate issued by One Identity. You can specify a custom certificate for authentication and traffic encryption between the Password Manager Service and the websites (Self-Service and Helpdesk). For more information on using custom certificates, see [Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites](#).

NOTE: Before selecting a custom certificate on the Helpdesk site, specify a custom certificate on the Administration site.

5. Click **Save**.

NOTE: After the initialization of Helpdesk and Self-Service site, **WcfServiceRealms.xml** file is created. **WcfServiceRealms.xml** file has records of all the instances of Password Manager Services installed. **WcfServiceRealms.xml** file is used to help the user to use one of the realm instances from the list, in case of unavailability of services in the primary instance of Password Manager Service. For more information, see [FailSafe support in Password Manager for AD LDS](#)

FailSafe support in Password Manager for AD LDS

This feature allows a user to login to the Helpdesk or Self-Service site when the Password Manager for AD LDS Service is unavailable.

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

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

NOTE: Failsafe works in distributed environment. If all the Password Manager for AD LDS 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 for AD LDS Service.

Installing multiple instances of Password Manager for AD LDS

Several Password Manager for AD LDS instances sharing common configuration are referred to as a realm. A realm is a group of Password Manager for AD LDS Service instances sharing all settings and having the same set of management policies, that is, the same user and Helpdesk scopes, Q&A policy, and workflow settings. Password Manager for AD LDS realms provide for enhanced availability and fault tolerance.

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

To create a Password Manager for AD LDS Realm

1. Export a configuration file from the instance belonging to the target realm:
 - To export instance settings to the configuration file, connect to the Administration site of the instance belonging to the target realm.
 - On the menu bar, click **General Settings**, then click **Import/Export**.
 - On the **Import/Export Configuration Settings** page, select the **Export configuration settings** option and click **Export** to save the configuration file.

IMPORTANT: Remember the password that is generated while exporting the configuration file. You should enter this password when importing the configuration file for a new instance you want to join to the target realm.
2. Install a new Password Manager for AD LDS instance by running **Password Manager x86** or **Password Manager x64** from the installation media autorun window. For more information on the installation procedure, see [Installing Password Manager for AD LDS](#).
3. Open the Administration site by entering the following address: `http(s)://<ComputerName>/PMAdmin`, where <ComputerName> is the name of the computer on which Password Manager for AD LDS is installed. On the **Instance Initialization** page, select the **Replica of existing instance** option.
4. Click **Upload** to select the configuration file that you exported from the instance belonging to the target realm.
5. Enter the password to the configuration file and click **Save**.

Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites

When the Password Manager for AD LDS Service is installed on one computer and the Self-Service and Helpdesk sites are installed on some other computers, certificate-based authentication and traffic encryption is used to protect traffic between these components.

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

To start using custom certificates for authentication and traffic encryption between Password Manager for AD LDS components

1. [Step 1: Obtain and install custom certificates from a trusted Windows-based Certification Authority](#)

2. [Step 2: Providing certificate issued for server computer to Password Manager for AD LDS service](#)
3. [Step 3: Providing certificate issued for client computers to Self-Service and Helpdesk Sites](#)

Step 1: Obtain and install custom certificates from a trusted Windows-based Certification Authority

You must obtain two certificates from a trusted Windows-based certification authority: one for the computer running the Password Manager for AD LDS Service (server computer), and another for computers running the Self-Service or Helpdesk site (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** option is NOT selected in a certificate request.

The following is a sample procedure describing how to obtain a certificate through the Windows 2012 Certificate Services Web interface.

IMPORTANT: When obtaining a certificate for the server computer, perform the following procedure on a computer where the Password Manager Service runs and 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 or Helpdesk site and use the Application Pool Identity account to run a supported web browser.

To request a certificate using Windows 2012 Certificate Services Web Interface

1. Use a browser to open <https://servername/certsrv>, where *servername* refers to the name of the web server running Windows Server 2012 where the certification authority that you want to access is located.
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** field, 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 **Mark keys as exportable**.
 - Clear **Enable strong private key protection**.
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 needs to be approved by your administrator first, wait for the approval and then go to <https://servername/certsrv>. Then, click **View the status of a pending certificate request**, and then install the issued certificate.

Step 2: Providing certificate issued for server computer to Password Manager for AD LDS service

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

To provide the certificate to the Password Manager for AD LDS Service

1. Open the Administration site by entering the following address: [http\(s\)://<ComputerName>/PMAdmin](http(s)://<ComputerName>/PMAdmin), where <ComputerName> is the name of the computer on which Password Manager for AD LDS is installed.
2. Click **General Settings > Instance Reinitialization**. Under the **Service connection settings**, select the custom certificate issued for the server computer from the **Certificate name** drop-down list.
3. Click **Save**.

Step 3: Providing certificate issued for client computers to 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 for AD LDS Service.

To provide the certificate to the Legacy Self-Service Site and the Password Manager for AD LDS Self-Service site

1. Open the Self-Service site by entering the following address: `http(s)://<ComputerName>/PMUser`, where `<ComputerName>` is the name of the computer on which Self-Service site is installed.

For the Password Manager for AD LDS Self-Service site, enter the following address: `http(s)://<ComputerName>/PMNewUser`,

The **Self-Service Site Initialization** page will be displayed 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. Click **Save**.

To provide the certificate to the Helpdesk Site

1. Open the Helpdesk site by entering the following address: `http(s)://<ComputerName>/PMHelpdesk`, where `<ComputerName>` is the name of the computer on which Helpdesk site is installed. The **Helpdesk Site Initialization** page will be displayed 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. Click **Save**.

Password Manager for AD LDS Architecture

[Password Manager for AD LDS 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 for AD LDS Components and Third-Party Solutions

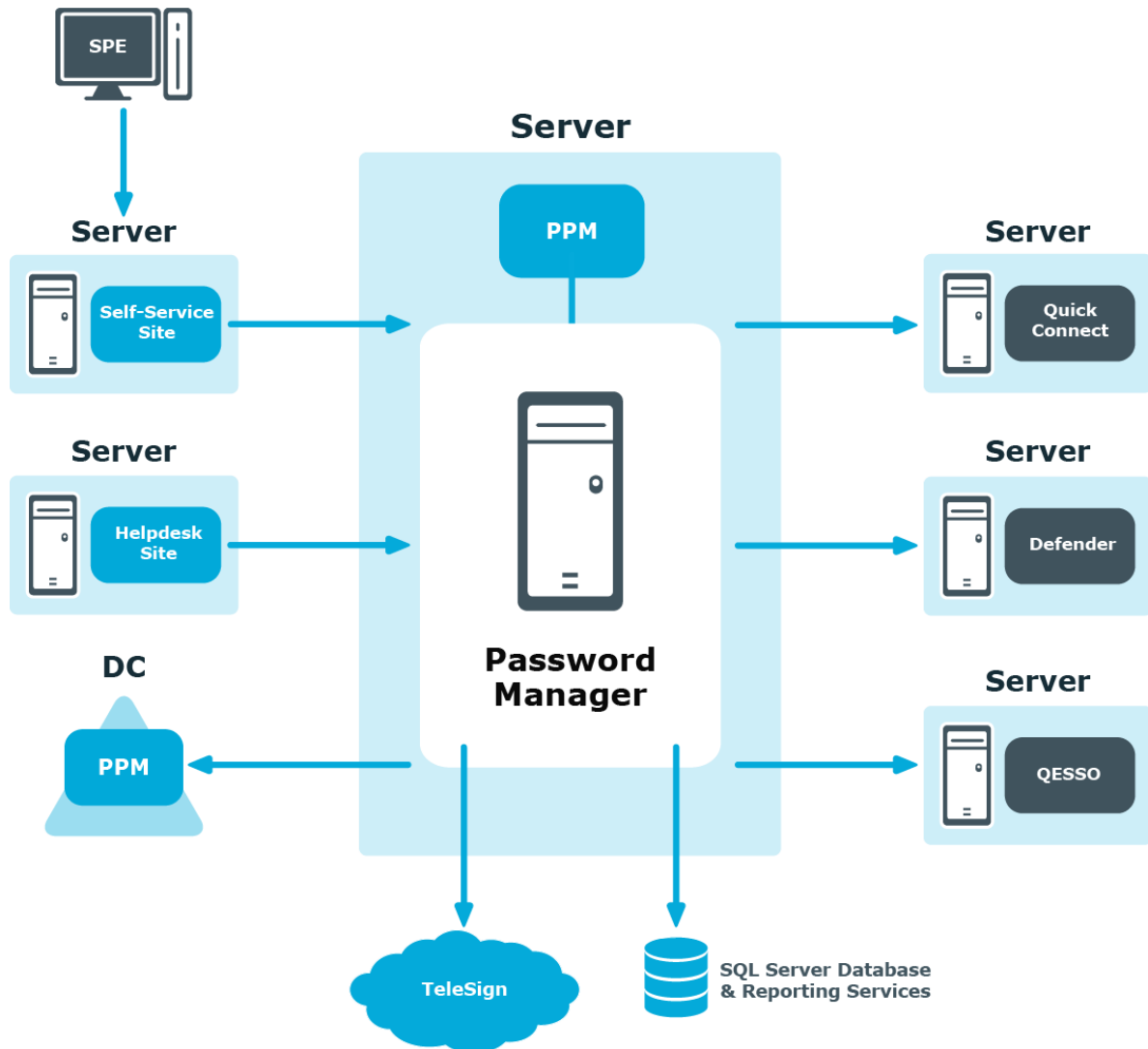
This section provides information Password Manager for AD LDS components and third-party applications that can be used by Password Manager for AD LDS.

The following is a list of Password Manager for AD LDS components:

- [The Password Manager for AD LDS Service and the Administration site](#)
- [Self-Service site](#)
- [Helpdesk site](#)

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

- TeleSign
- SQL Server Database and SQL Server Reporting Services
- One Identity Quick Connect Sync Engine
- Defender
- Password Manager Secure Token Server
- RADIUS Two-Factor Authentication



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

The Password Manager for AD LDS Service and the Administration site

Password Manager Service and the Administration site are a core component of Password Manager for AD LDS.

The Password Manager for AD LDS Service is a Windows service that provides core functionality and runs under the Password Manager for AD LDS Service account, which is specified during Password Manager for AD LDS installation.

The Administration site provides all the necessary settings for an administrator to configure and use Password Manager. Using the Administration site, the administrator can configure user and Helpdesk scopes, management policies, password policy rules.

Note that the Administration site cannot be installed separately from the Password Manager for AD LDS Service.

When installing the Administration site and the Password Manager for AD LDS Service, the Self-Service and Helpdesk sites are also installed.

Self-Service site

The Self-Service site provides users with the ability to easily and securely manage their passwords, thus eliminating the need for assistance from high-level administrators and reducing Helpdesk workload.

The Self-Service site can be installed on the same server as the Administration Site and Password Manager for AD LDS Service, or on a stand-alone server, for example, if you want to install the Self-Service site in a perimeter network (DMZ).

Password Manager for AD LDS Self-Service site

The Password Manager for AD LDS Self-Service site provides functionality similar to the Legacy Self-Service site. The Password Manager for AD LDS Self-Service site includes enhancements to the user interface to improve the usability of the site.

Limitations & Restrictions of the Password Manager for AD LDS Self-Service site

- The Password Manager for AD LDS Self-Service site can coexist along with the Legacy Self-Service site.
- It is possible to revert to the Legacy Self-Service site at any time.
- The Password Manager for AD LDS Self-Service site is only available in English.

Alternative option

As an alternative to using the Password Manager for AD LDS Self-Service site, use the Legacy Self-Service site.

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.

The Helpdesk site can be installed either on the same server as the as the Administration Site and Password Manager for AD LDS Service, or on a standalone server.

TeleSign

TeleSign is a service that provides phone-based authentication for Password Manager for AD LDS users. To enable the TeleSign service, it must be covered by your license and the administrator must configure the Authenticate via Phone activity and include the activity in corresponding workflows. If TeleSign is enabled, when performing a task on the Self-Service or Helpdesk site, users will be prompted to select their phone number, to which a one-time code will be sent by TeleSign, and then enter the code on the site for verification.

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](#).

One Identity Quick Connect Sync Engine

One Identity Quick Connect Sync Engine is a One Identity product that provides unified identity and access management. Integrating Password Manager with Quick Connect Sync Engine allows you to enable users and Helpdesk operators to manage their passwords across different connected data sources.

To use Quick Connect Sync Engine, configure **Change password in Active Directory and connected systems** or **Reset password in Active Directory and connected systems activities**.

To communicate with Quick Connect Sync Engine, Password Manager uses Transmission Control Protocol (TCP).

For more information, see [Reset Password in AD LDS and Connected Systems](#).

Defender

IMPORTANT: Authenticating with Defender is an activity not supported with the current release of Password Manager for AD LDS 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 for AD LDS is integrated with Defender, users can use one-time passwords to authenticate themselves on the Self-Service Site.

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

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

Password Manager Secure Token Server

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

You can use this feature on the new PM 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 for AD LDS 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 "Authenticate with external provider" activity into any workflow.

- If you have not set up Secure Token Server connection or did not have valid providers configured in authentication providers, you cannot use this activity.
- If you set up at least one provider, you can start using it.
- If you set up more than one, you can select a provider for each activity used in workflows.

Authenticate with external provider on Self Service site

When Authenticate with external provider is the current activity in a workflow, the user is presented with a login form, where they need to provide the credentials for the configured authentication provider. If the configured provider is using MFA, the user will be prompted for the next step. For more information, see [Authenticate with external provider](#).

This login interface uses the browser's language. The supported languages are the following:

- Argentinean (ar)
- Chinese (zh)
- Dutch (nl)
- English (en)
- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Russian (ru)
- Spanish (es)

Password Manager 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 for AD LDS realm

The Password Manager for AD LDS STS settings are stored separately from other Password Manager for AD LDS 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 for AD LDS 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="rstConfigSource" type="Rsts.Config.RstsConfigSource, Rsts"/>
</configSections>
<rstConfigSource xmlns="urn:Rsts.Config">
  <source type="FileConfigProvider">
    <fileConfigProvider fileName="rstConfig.bin">
      <protection type="RsaDataProtection">
        <rsaDataProtection certificateStore="LocalMachine"
certificateLookupType="FindByThumbprint"
certificateLookupValue="b23655f8ac0b81c5b00bac0bc0a15e7e1d2b78be"/>
      </protection>
    </fileConfigProvider>
  </source>
</rstConfigSource>
</configuration>

```

The thumbprint of the certificate used to encrypt the Password Manager for AD LDS 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 for AD LDS 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 for AD LDS 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 `rstConfig.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 PMAdmin site **General Settings > Secure Token Server** page. Password Manager for AD LDS 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 for AD LDS STS settings are not replicated automatically

To replicate the Password Manager for AD LDS STS settings manually, copy the `rstConfig.bin` file from the server where you configured Password Manager for AD LDS

STS to all other servers. After you copy the file, you must restart the Password Manager for AD LDS 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 for AD LDS STS settings are modified.

NOTE: : For this copy-paste process, the encryption method of the Password Manager for AD LDS 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 for AD LDS. 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 for AD LDS, you have to configure the RADIUS server details in Password Manager for AD LDS.

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 for AD LDS software.

Alternative option

The Redistributable Secret Management Service (rSMS) feature, can be used as an alternative to [One Identity Quick Connect Sync Engine](#).

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 for AD LDS 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 for AD LDS Credential Checker

The Password Manager for AD LDS 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 for AD LDS credential checker

1. To enable the Password Manager for AD LDS credential checker, after the Password Manager for AD LDS is installed, on the Password Manager for AD LDS Administrator portal, navigate to **General settings > Extensibility** and select **Turn the credential checker mode on or off**.
2. On the Password Manager for AD LDS 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.

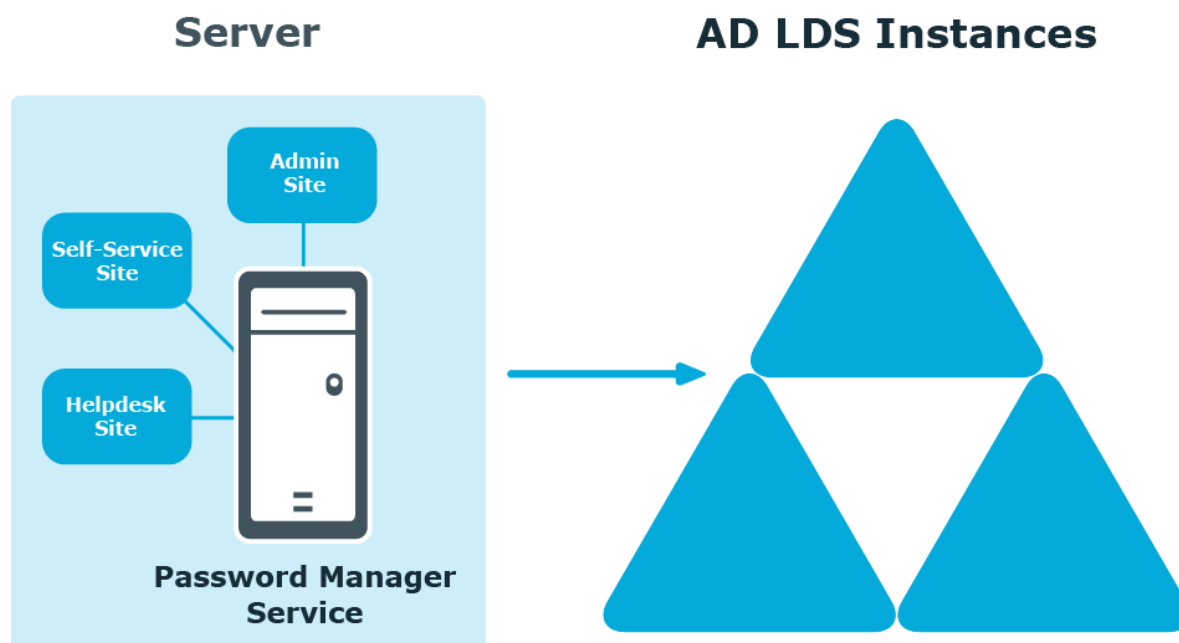
When you enter a new password on the Self-Service site using any of the workflows, such as, **Forgot Password** or **Manage My Passwords**, the Credential Checker validates the new password and check if it matches with the passwords listed in the **VeriClouds**. If the password matches, **Provided password 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

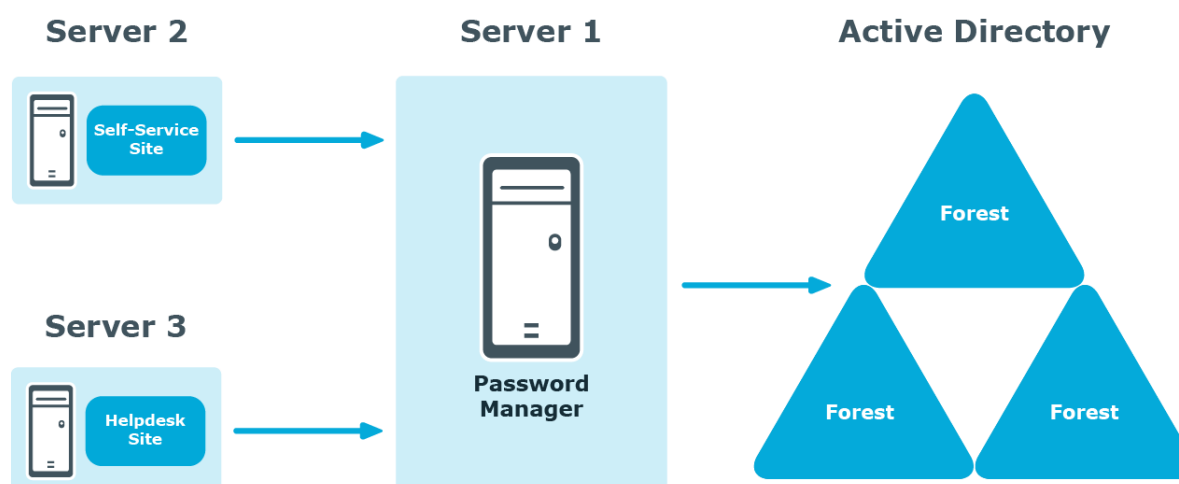
This section describes typical deployment scenarios for Password Manager for AD LDS, including scenarios with installation of the Self-Service and Helpdesk sites on standalone servers, using realms, and so on.

Simple Deployment



In this scenario, you install all main Password Manager for AD LDS components, that is, the Password Manager for AD LDS Service, Administration, Self-Service and Helpdesk sites on a single server. This is the simplest deployment scenario, which can be used in small environments and for demonstration purposes.

Deployment of the Legacy Self-Service, Password Manager for AD LDS Self-Service and Helpdesk Sites on Standalone Servers



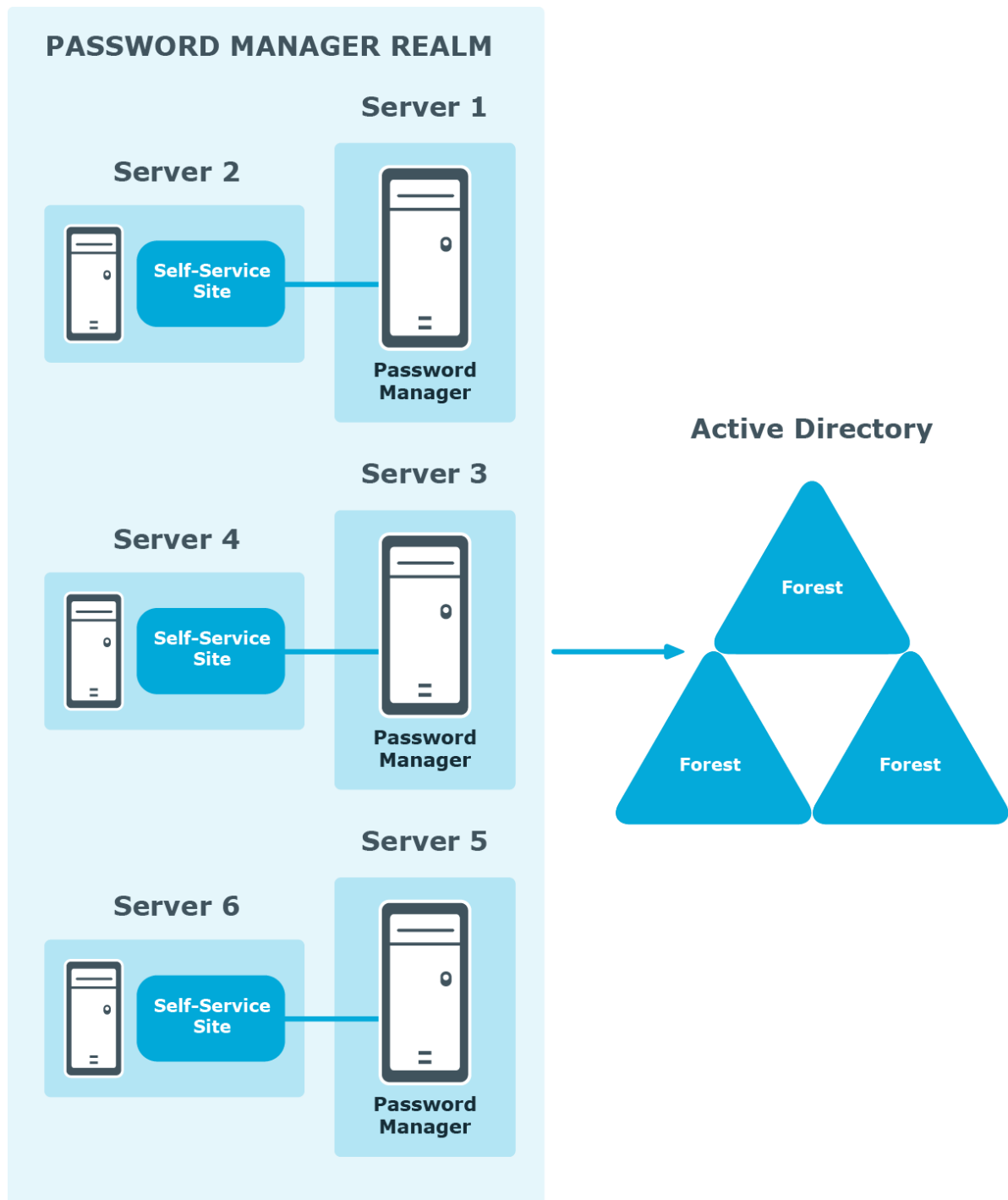
In this scenario, you install the Legacy Self-Service site, Password Manager for AD LDS Self-Service site, Helpdesk site, or both on a standalone server. Note that the Administration site cannot be installed separately from the Password Manager for AD LDS Service.

You can use this scenario to deploy Password Manager for AD LDS in an environment with a perimeter network. Installation of the Legacy Self-Service site or the Password Manager for AD LDS Self-Service site in the perimeter network enhances the security of your environment while preventing access to your internal network.

When deploying Password Manager for AD LDS in an environment with the perimeter network, it is recommended to do a full installation of Password Manager for AD LDS in the internal corporate network, and then install the Self-Service site in the perimeter network.

When you use this installation scenario, only one port should be open in the firewall between the corporate network and the perimeter network (by default, port number 8081 for the Legacy Self-Service site or Password Manager for AD LDS Self-Service site).

Realm deployment



In this scenario, you install several Password Manager for AD LDS Services on separate servers. If all the instances of Password Manager for AD LDS 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.

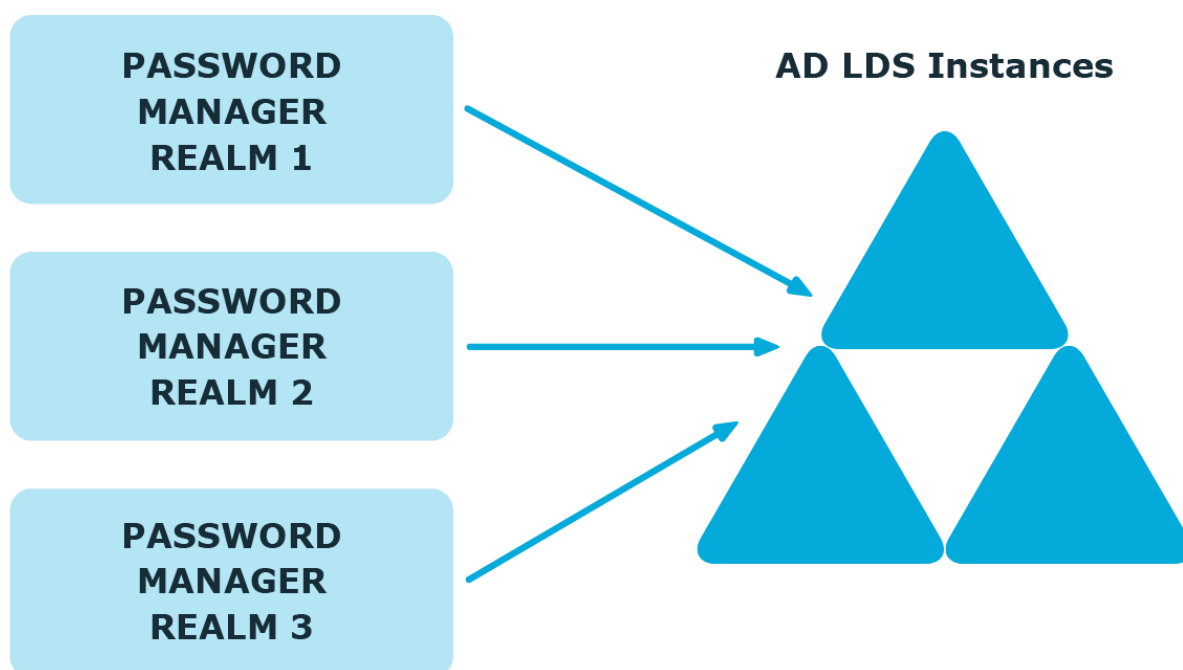
The realm provides for high availability of the service, load balancing, and fault tolerance.

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

To create the Password Manager for AD LDS 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



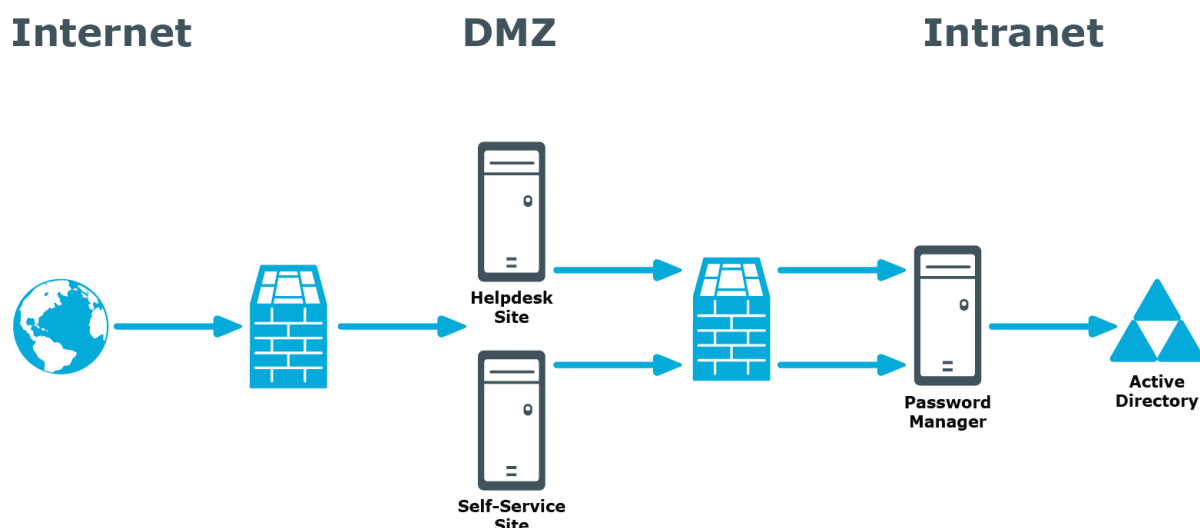
In this scenario, you deploy several Password Manager realms in your environment. You can use this scenario in complex environment, when several Password Manager configurations are required.

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



When you use this installation scenario, only one port should be open in the firewall between the corporate network and the perimeter network (by default, port number 8081 is used).

For more information on installing the Self-Service and Helpdesk site separately from the Password Manager for AD LDS Service, see [Installing Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk Sites on a Standalone Server](#).

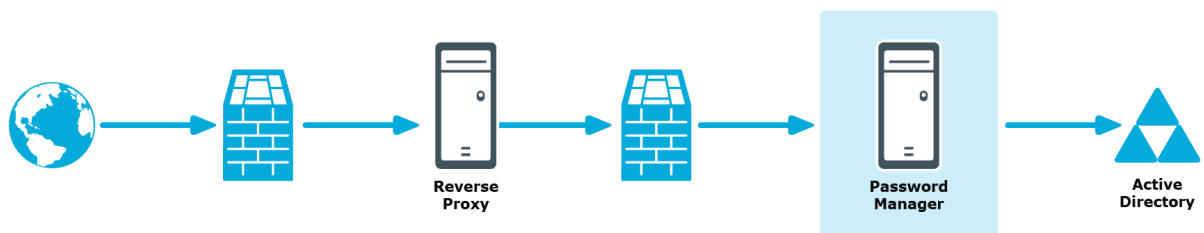
Installing Password Manager for AD LDS in Perimeter Network with Reverse Proxy

A reverse proxy is a proxy server that is typically deployed in a perimeter network to enhance 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 an external attack.

Internet

DMZ

Intranet



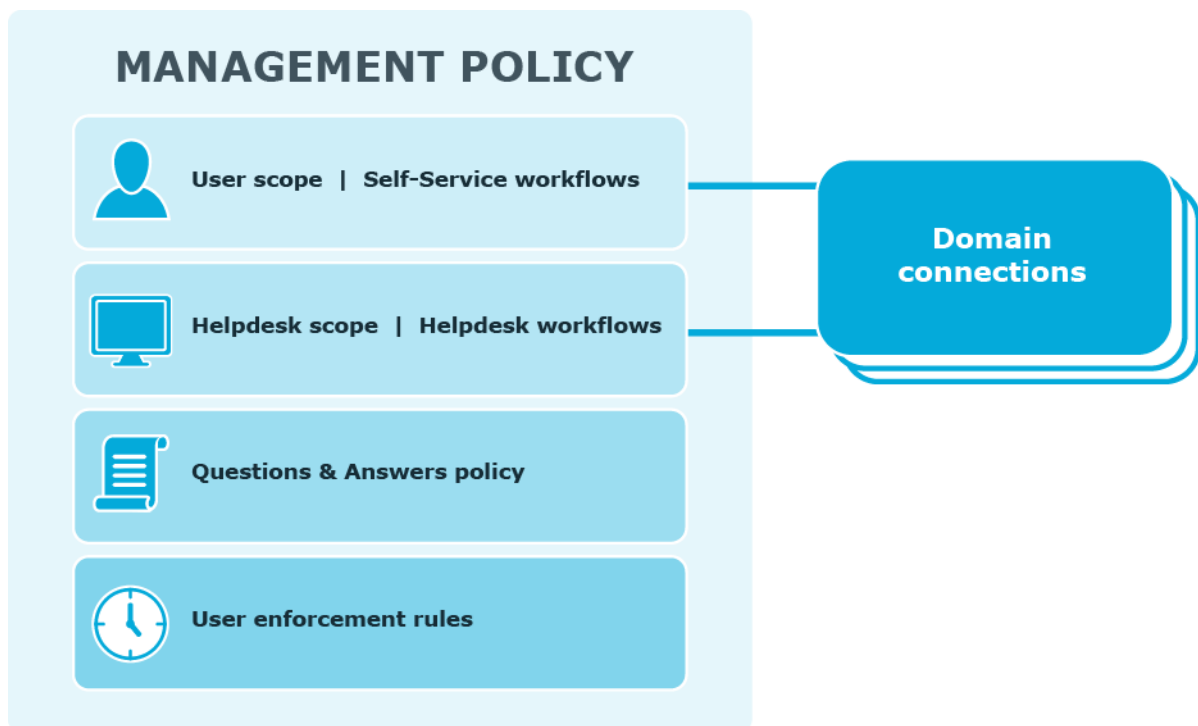
If you have the reverse proxy deployed in the perimeter network in your environment, it is recommended to install the Password Manager Service and the Self-Service and Helpdesk sites in the intranet and configure the reverse proxy to redirect requests from external users to the correct intranet URLs of the Password Manager sites.

Management Policy Overview

A Management Policy is a core concept in Password Manager for AD LDS. 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.

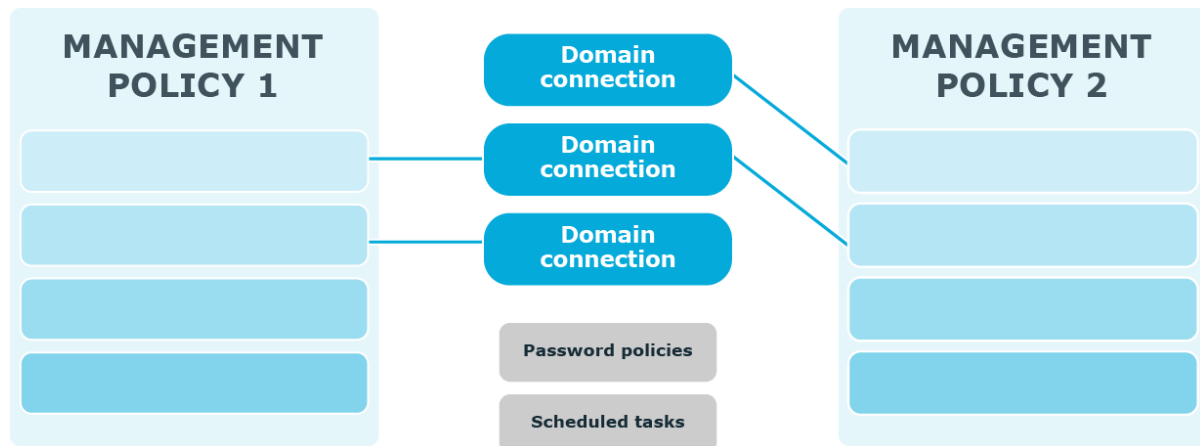
Self-Service and helpdesk workflows define the tasks that are available to users and Helpdesk operators on the Self-Service and Helpdesk sites: for example, **Forgot My Password**, **Assign Passcode**, **Unlock Account**, and so on.

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 for AD LDS installation.

Management Policy and other Password Manager for AD LDS settings

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



In a single Password Manager for AD LDS 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.

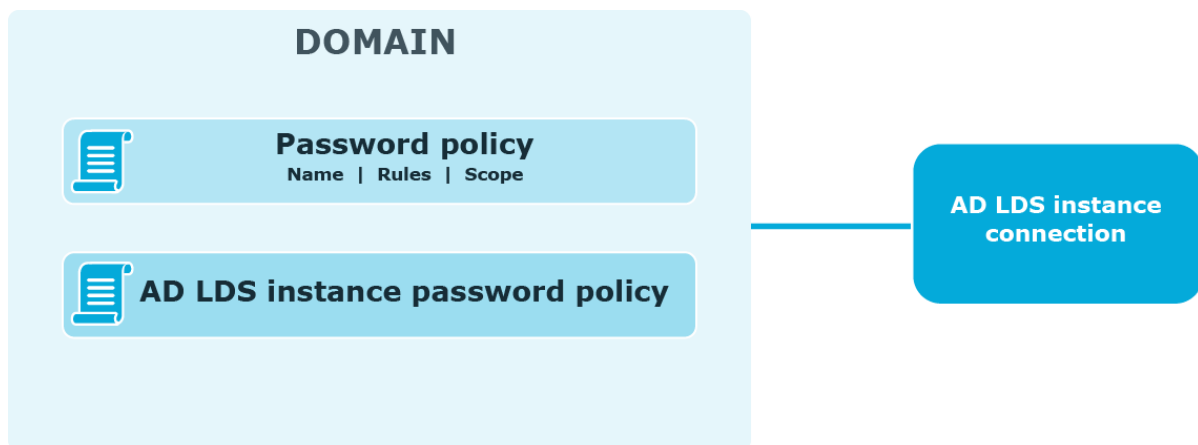
The **Invitation to Create/Update Profile**, **Reminder to Create/Update Profiles**, **Reminder to Change Password** scheduled tasks allow notifying users from scopes of user enforcement rules configured in Management Policies. For more information, see [Scheduled Tasks](#) and [User Enforcement Rules](#).

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 for AD LDS 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.

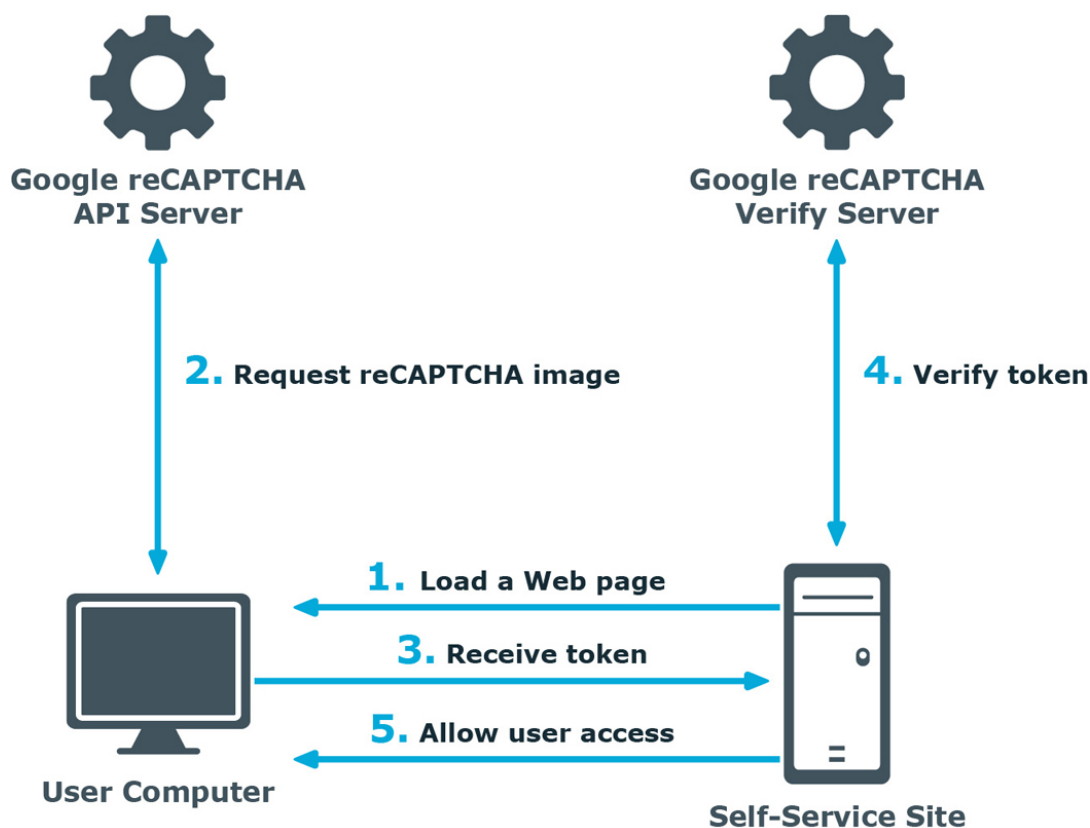
reCAPTCHA Overview

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 for AD LDS site.

How to Use reCAPTCHA on Password Manager for AD LDS 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 88.

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 Security Options](#) on page 129.

System Requirements for Using reCAPTCHA

To be able to use reCAPTCHA on the Password Manager for AD LDS 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 for AD LDS 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 for AD LDS, 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 70. For more information on configuring this enforcement rule, see [Invite Users to Create/Update Profiles](#) on page 118.

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 121.

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 89.
- **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 90.
- **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 118.

Data Replication

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

Storing Data

There are two types of data stored by Password Manager for AD LDS: 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 for AD LDS instance; for more information, see [Instance Reinitialization](#) on page 149.

Password Manager for AD LDS 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**, etc.

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

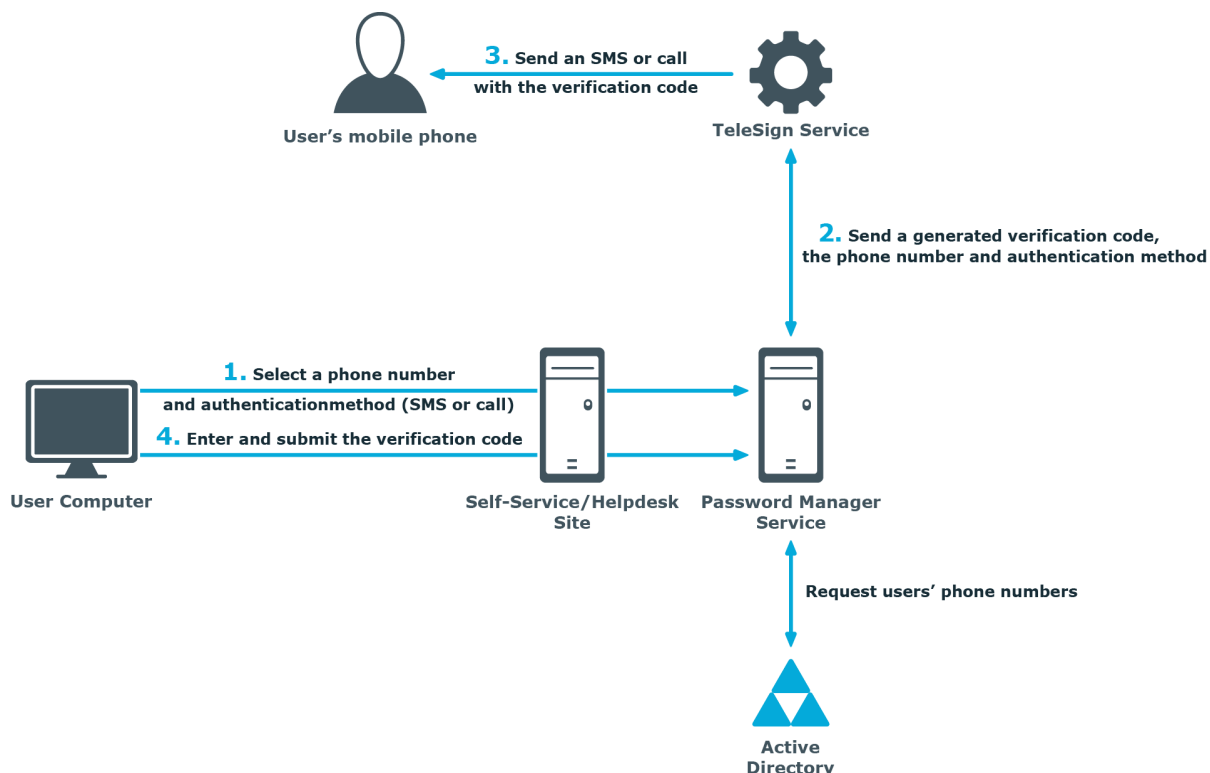
1. On the computer where Password Manager is installed, open the QPM.Service.Host.exe.config file located in the <Password Manager installation folder>\Service folder with a text editor.
2. In the **replication** node, specify the following:

- 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 for AD LDS 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 for AD LDS realm.

Phone-Based Authentication Service Overview

One of the authentication options offered by Password Manager for AD LDS is a phone-based authentication. It enables you to require users to enter a verification code on the Self-Service or Helpdesk site. The verification code can be sent as an SMS (text message) or automated call. The phone-based authentication service is by provided by TeleSign.

How It Works



When starting a workflow containing phone-based authentication, Password Manager for AD LDS checks whether the phone-based authentication service is enabled in the provided license. The workflow is executed only if this service is enabled in the license.

1. On the Self-Service 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 Service. Password Manager for AD LDS Service gets the phone numbers from the Active Directory attributes specified in the workflow settings.
2. Password Manager for AD LDS Service generates a verification code and transfers the code, selected phone number, and verification method to TeleSign Service. HTTPS is used to send the data. The generated verification code is stored until the workflow is ended. Only one code is stored at a time.
3. 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 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 Service.
5. Password Manager for AD LDS Service checks the verification code, if it is correct, the user is granted access to further steps on the Self-Service site.

How to use phone-based authentication

To use phone-based authentication on the Self-Service and Helpdesk sites, add the Authenticate via Phone activity in self-service and helpdesk workflows. When configuring this activity, you can specify Active Directory attributes from which phone numbers can be retrieved, and available authentication methods: that is, SMS or automated voice call.

Phone numbers that belong to Private Branch Exchange (PBX) are also supported. PBX phones require either a live switchboard operator or an automated attendant to complete the call. By default, Password Manager for AD LDS supports automated attendant scenario. It can be configured for live operators by changing `PhoneNumberExtensionType` parameter in `QPM.Service.Host.exe.config` file. For automated attendants, set `PhoneNumberExtensionType` to 1 and for live operators, set `PhoneNumberExtensionType` to 2.

For `PhoneNumberExtensionType` set to 1 (DTMF digits are dialed), include commas in the `PhoneNumberExtensionTemplate`, where each comma represents one second pause in the dialing sequence. To increase the pause in the dialing sequence, add the required number of commas in `PhoneNumberExtensionTemplate` in the configuration file.

NOTE: The phone number extension must be configured with extension separator in the Active Directory. Phone number with extension must have "x" or "X" in it to separate the extension number from the phone number as given 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](#).

System requirements

To use the phone-based authentication service, the following requirements must be met:

- You have a valid license for the phone-based authentication service (see the About page of the Administration site for the service status).
- Outbound SSL connections are allowed from the computer on which Password Manager for AD LDS Service runs to the following address: `https://*.telesign.com`. * can be replaced with any valid subdomain name; for example, `https://api.telesign.com` or `https://www.telesign.com`.

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 for AD LDS will access the AD LDS instance and a specified application directory partition. You can use the Password Manager for AD LDS 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 for AD LDS 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 will be able to 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 Administration site, select the Management Policy you want to configure and click the **User Scope** link.
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. 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 for AD LDS access the AD LDS instance using the Password Manager for AD LDS 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](#) on page 53.

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, click **Add** under **Groups allowed access to the Self-Service site**.
- To specify the OUs, click **Add** under **Organizational units allowed access to the Self-Service site**.

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, OUs that are added as **Included groups**, and **Included OUs** in the userscope.

If the users/ groups/ OUs included in the userscope, are a member of Readers/ Administrators group in the AD LDS 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 for AD LDS 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 53. Password Manager for AD LDS Service account is the account that was configured during Password Manager for AD LDS installation. Password Manager for AD LDS 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

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 66.

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>/PMAAdminADLDS/`.
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 box, 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 118.

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.

Management Policies

[Checklist: Configuring Password Manager for AD LDS](#)

[Understanding Management Policies](#)

[Configuring Access to the Administration Site](#)

[Configuring Access to the Legacy Self-Service Site and Password Manager for AD LDS Self-Service site](#)

[Configuring Access to the Helpdesk Site](#)

[Configuring Questions and Answers Policy](#)

[Workflow overview](#)

[Custom workflows](#)

[Custom Activities](#)

[Legacy Self-Service or Password Manager for AD LDS Self-Service site workflows](#)

[Helpdesk Workflows](#)

[User Enforcement Rules](#)

Checklist: Configuring Password Manager for AD LDS

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

Table 3: Checklist to configure Password Manager for AD LDS

Step	Reference
Prepare an access account to AD LDS instance.	Configuring Permissions for Access Account on page 53

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 57
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 63
Configure self-service and helpdesk workflows to define what tasks will be available on the Self-Service and Helpdesk sites.	Legacy Self-Service or Password Manager for AD LDS Self-Service site workflows Helpdesk Workflows on page 105
If required, configure rules for enforcing users to register with Password Manager for AD LDS.	User Enforcement Rules on page 118
Configure general settings that apply to all Management Policies (such as account search options, SMTP servers, scheduled tasks, etc.)	General Settings Overview on page 125
Create password policies and configure password policy rules.	Creating a Password Policy on page 177
If you want to use Password Manager for AD LDS for cross-platform password synchronization, install One Identity Quick Connect Sync Engine and configure the product to integrate with Password Manager for AD LDS.	Reset Password in AD LDS and Connected Systems on page 96
Ensure that all Password Manager for AD LDS 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 for AD LDS. 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 for AD LDS. 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 63.

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 for AD LDS 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 66.

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 72.

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 118.

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 for AD LDS installation.

NOTE: The account that you specified as Application Pool Identity when installing Password Manager for AD LDS 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 for AD LDS configuration may require dealing with user-sensitive information.

Configuring Access to the Legacy Self-Service Site and Password Manager for AD LDS Self-Service site

The Password Manager for AD LDS Self-Service site has all functionality similar to the Legacy Self-Service site with a new and improved user interface. The Password Manager for AD LDS Self-Service site can co-exist along with the already existing Legacy Self-Service site and it is possible to revert at any time to the Legacy Self-Service site.

To configure access to the Legacy 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 for AD LDS 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 153.

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 for AD LDS 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 for AD LDS 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 53.

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 for AD LDS 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 53. Password Manager for AD LDS Service account is the account that was configured during Password Manager for AD LDS installation. Password Manager for AD LDS 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 for AD LDS 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

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 for AD LDS. 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 46.

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 for AD LDS 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 for AD LDS 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 70.

Password Manager for AD LDS 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 118.

Secret questions can contain the following types of questions:

Table 4: 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>/PMAAdminADLDS/`.
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 box, 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 box.

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 118.

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>/PMAAdminADLDS/`.
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 box, select an additional language for secret questions.
5. In the **Translate Questions** dialog box, 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 box.

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 118.

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\username 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 box, specify the following options:

Table 5: 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-	Set the required number of user-defined questions that a user must specify to create a Questions and Answers profile.

Option	Description
defined questions to register	
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 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 for AD LDS 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 for AD LDS Administration Site. Workflows have 2 types:

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

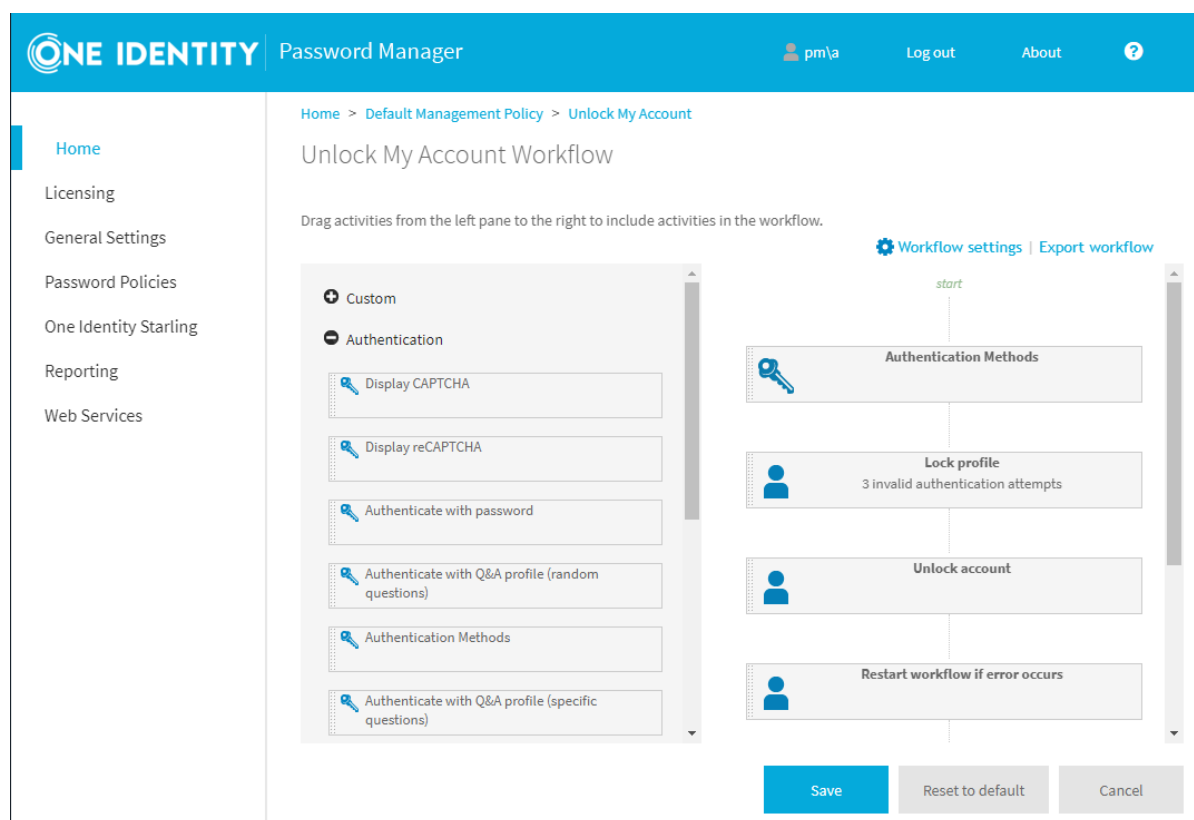
- **Authentication** provides authentication options, such as password-based authentication, Questions and Answers profiles, or phone-based authentication.
- **Actions** are core components in workflows, including activities like unlocking accounts, editing Q&A profiles, or resetting passwords.
- **Notifications** 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 1: 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

For each workflow, you can set 3 options:

- **Language settings** 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.
- **Availability settings** specify if the workflow must appear on the Password Manager for AD LDS Self-Service Site or in the Helpdesk Site.
- **Customization settings** specify a custom icon for the workflow and a possible grouping key.

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.

To set the language settings

1. On the Password Manager for AD LDS Administration Site, under **Home** > **<management-policy>**, click the workflow of the management policy 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. 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

1. On the Password Manager for AD LDS Administration Site, under **Home** > **<management-policy>**, click the workflow of the management policy you want to

configure.

2. On the page of the configured workflow, click **Workflow settings**.
3. Under **Workflow Settings > Availability > Enable the workflow**, select the availability option of your workflow:
 - **Always:** The workflow is always enabled for users on the Password Manager for AD LDS Self-Service Site or for operators on the Helpdesk Site.
 - **Never:** The workflow is always disabled on the Password Manager for AD LDS Self-Service Site or Helpdesk Site.
 - **Depending on the current user status:** The availability of the configured workflow depends on the user status.

The default criteria for enabling or disabling workflows on the Password Manager for AD LDS Self-Service Site are the following:

- For unregistered users, only the **Register** workflow is enabled.
- For registered users, the **Forgot My Password** and **Manage My Passwords** workflows are enabled.
- Both for registered and unregistered users, the **I Have a Passcode** workflow is enabled only if a helpdesk user performs an **Assign Passcode** workflow for them.
- For registered users with a locked account, only the **Forgot My Password** and **Unlock My Account** workflows are enabled.
- For users with a locked Q&A profile, no workflows are enabled on the Password Manager for AD LDS Self-Service Site. Users must contact the helpdesk in this case.

The default criteria for enabling or disabling workflows on the Password Manager for AD LDS Helpdesk Site are the following:

- For unregistered users, the **Reset Password**, **Unlock Account** and **Assign Passcode** workflows are enabled.
- For registered users with a locked Q&A profile, all Helpdesk workflows are enabled.

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. Under **Show the workflow**, specify the visibility of the configured workflow on the Password Manager for AD LDS Self-Service Site or Helpdesk Site for users:
 - **Always:** The workflow is always visible, regardless of whether it is enabled or disabled for the current user.
 - **Never:** The workflow is always hidden, regardless of whether it is enabled or disabled for the current user.

- **Only if the workflow is enabled:** The workflow appears only if it is enabled for the current user.

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

NOTE: Custom workflows appear on the Password Manager for AD LDS Self-Service Site for users even if the **Enable the workflow** setting is set to **Depending on the current user status** and the **Show the workflow** setting is set to **Only if the workflow is enabled**.

To force these settings for custom workflows

1. Stop the Password Manager for AD LDS Service.
2. Open the C:\ProgramData\One Identity\Password Manager for AD LDS\Shared.storage file.
3. Replace the <DisabledReasons /> line with the following entry:


```
<disabledReasons>
  <reason name="userRegistered" value="DisableIfFalse" />
</disabledReasons>
```
4. Save the file, then restart the Password Manager for AD LDS Service.

To set the customization settings

1. On the Password Manager for AD LDS Administration Site, under **Home** > **<management-policy>**, click the workflow of a management policy 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 desired icon for your workflow.
4. Under **Workflow group name**, specify a group name that acts as a grouping key for workflows.

NOTE: Workflows that have the same group name will be grouped together in the Password Manager for AD LDS Self-Service site. Leave **Workflow group name** empty if no grouping is desired for the current workflow.

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 **Workflow group name**, edit the following file by adding a new key-value pair as "<workflow-group-name>":"<translated-workflow-group-name>" inside the opening and closing braces:

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

NOTE: Workflow groups are displayed on Password Manager for AD LDS Self-Service site in a way that is visually slightly different from that of workflows. Also, workflow groups are ordered 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 for AD LDS 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. However, 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: Custom workflows appear on the Password Manager for AD LDS Self-Service Site for users even if the **Enable the workflow** setting is set to **Depending on the current user status** and the **Show the workflow** setting is set to **Only if the workflow is enabled**.

To force these settings for custom workflows

1. Stop the Password Manager for AD LDS Service.
2. Open the C:\ProgramData\One Identity\Password Manager for AD LDS\Shared.storage file.
3. Replace the <DisabledReasons /> line with the following entry:

```
<disabledReasons>  
  <reason name="userRegistered" value="DisableIfFalse" />  
</disabledReasons>
```
4. Save the file, then restart the Password Manager for AD LDS Service.

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 for AD LDS 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 for AD LDS 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 for AD LDS 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 for AD LDS 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 for AD LDS 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

When you use custom activities in your workflows, you need to understand how shared settings of custom activities work.

All settings (display name, short name, description, PowerShell script, and user interface elements) that you specify for custom activities created from scratch are shared i.e. if you modify 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 this activity in all workflows and Management Policies.

If you create a custom activity by converting a built-in activity, the custom activity has two types of settings: built-in and shared. Built-in settings are the settings inherited from the built-in activity. Such settings are not shared: if you modify them, the changes will be applied only to the current activity instance. But if you modify the shared settings (display name, short name, description, PowerShell script), such changes will be propagated throughout all instances of this activity.

For example, if you modify the PowerShell script for your custom activity "My Custom CAPTCHA", when you save the activity, the updated settings will be applied to all instances of the "My Custom CAPTCHA" activity used in other workflows and Management Policies. But if you modify the built-in setting (noise level) of the "My Custom CAPTCHA" activity, when you save the activity, the changes will be applied only to this instance of the activity.

The noise level setting of other instances of the “My Custom CAPTCHA” activity 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 for AD LDS 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 for AD LDS 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 box, 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.

Legacy Self-Service or Password Manager for AD LDS Self-Service site workflows

The Password Manager for AD LDS Self-Service site has all functionality similar to the Legacy Self-Service site with a new and improved user interface. The Password Manager for AD LDS Self-Service site can co-exist along with the already existing Self-Service site and you can select to revert anytime to the Legacy Self-Service site.

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 77 and [Custom Activities](#) on page 79.

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 methods to display on the User site.

Select registration mode allows the administrator to configure, which registration methods are allowed for registration to the users. Following are the three methods available for the users to register.

- Corporate Authentication
- Security Questions
- Personal contact method: Email and Mobile

The selected options will be added in the Password Manager User site.

NOTE: When the administrator select registration method(s), only the respective authentication methods are visible to the administrator in **Authentication methods**.

Select one of the radio buttons to set the method as mandatory registration method. The administrator can set a method mandatory from **Select the registration method that must be set as the mandatory registration method for users in the User site**. When the administrator selects a method as mandatory, it is compulsory for users for registration in the User site. To set as mandatory registration method for the users in the Password Manager for AD LDS User site, select one of the following options.

- Corporate Authentication
- Security Questions
- Personal contact method: Email and Mobile
- Allow user to choose

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 for AD LDS 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 for AD LDS service to view the updates in the country code drop-down menu.

Manage My Profile

The **Manage My Profile** workflow allows the administrator to manage user profiles in Active Directory by using the Admin site. Manage My Profile uses settings of Register workflow.

Use this workflow only if the user's Questions and Answers profile is pending for update.

To configure the Manage My Profile workflow

1. Select **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**.

NOTE: In case of an upgrade from 5.8.2 to 5.9.x, if the user is registered with **Personal Contact Method(Mobile)** in 5.8.2, then the user will be prompted to re-enter the country code as well as the mobile number, the very first-time (post-upgrade to 5.9.x) while trying to update the profile through the **Manage My Profile** workflow.

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 and in connected data sources (if integration with One Identity Quick Connect Sync Engine is configured) by using the Self-Service site. For more information on using One Identity Quick Connect Sync Engine, see [Reset Password in AD LDS and Connected Systems](#) on page 96.

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 177.

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 and in connected data sources (if integration with One Identity Quick Connect Sync Engine is configured), by using the Self-Service site. For more information on using One Identity Quick Connect Sync Engine, see [Change Password in AD LDS and Connected Systems](#) on page 97.

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 177.

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 for AD LDS 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 Legacy Self-Service and Password Manager for AD LDS Self-Service site Activities

The Password Manager Self-Service site has functionalities similar to those of the Legacy Self-Service site, with a new and improved user interface. The Password Manager Self-Service site can co-exist along with the already existing Self-Service site and you can select to revert anytime to the Legacy Self-Service site.

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

Authentication activities are activities that provide different authentication options, for example authentication with password or Q&A profiles, or phone-based authentication.

The actions category includes activities that are core components of the built-in self-service workflows, for example Unlock Account, Edit Q&A Profile, 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 built-in self-service activities and provide information about the settings specific to each activity.

Authentication Activities

This section describes built-in activities that provide different authentication options.

Display CAPTCHA

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

This activity has the following settings:

- **Number of characters:** Specify the number of characters that will be displayed on a CAPTCHA image.
- **Noise level:** Select the noise level for a CAPTCHA image. The higher the level the more difficult it will be to read the characters.

Display reCAPTCHA

Use this activity to display a reCAPTCHA image on the Self-Service site and require users to enter the displayed characters before beginning a workflow. This feature provides enhanced protection against automated attacks.

reCAPTCHA is a free CAPTCHA service provided by Google.

To start using reCAPTCHA you need to sign up and get reCAPTCHA keys on the following Web site: <http://www.google.com/recaptcha>.

When getting the keys, provide the DNS name of the domain where Password Manager for AD LDS Self-Service sites are installed. If the Self-Service sites are installed in different domains, select the **Enable this key on all domains** check box to create a global key.

To learn more about using and configuring reCAPTCHA, go to <http://www.google.com/recaptcha/learnmore>.

This activity has the following settings:

- **Public key:** Specify the public key you received when configuring reCAPTCHA.
- **Private key:** Specify the private key you received when configuring reCAPTCHA.
- **Theme:** Select a color theme for the reCAPTCHA widget.

Authentication Methods

Use this activity to select which authentication methods to display in the User site. The three types of authentication methods available to select for the administrator are as follows:

- Security Questions
- Corporate Authentication
- Personal Email

IMPORTANT: The administrator can select any one of the activities selected in the registration method, to make it default mode for authentication for the users on the **User** site. Select one of the settings radio buttons from the right side to make it default authentication method.

NOTE:

- When the administrator select registration method(s), only the respective authentication methods are visible to the administrator in **Authentication methods**. See [Register](#).
- If the Administrator has selected **Allow user to edit corporate details** in corporate authentication of registration mode, a user cannot update the corporate email and corporate mobile number, if they are already populated.

Security Questions

Use this activity to authenticate a user with the personal Questions and Answers profile. In this activity, the administrator can specify how many questions from the Questions and

Answers profile the user must answer for authentication. There are two methods to authenticate the users using the Q&A method.

- **Authenticate with Q&A Profile (Random Questions):** See [Authenticate with Q&A Profile \(Random Questions\)](#).
- **Authenticate with Q&A Profile (Specific questions):** See [Authenticate with Q&A Profile \(Specific Questions\)](#).
- **Authenticate with Q&A profile (user-selected questions):** See [Authenticate with Q&A Profile \(User-selected questions\)](#).

Corporate Authentication

Use this activity to authenticate a user with a mobile device. There are two methods to authenticate the users using a mobile device.

- **Authenticate with RADIUS Two-Factor Authentication:** See [Authenticate with RADIUS Two-Factor Authentication](#).
- **Authenticate via Phone:** See [Authenticate via Phone](#).

Personal Email

Authenticate via Passcode: Use this activity to authenticate the users with a passcode. The administrator can configure passcode length and expiry time limit for the passcode.

Authenticate with Password

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

This activity has the following settings:

- **Authenticate users with expired passwords:** Select this check box to grant access to the Self-Service site to users who are required to change their passwords at next login. If you clear this check box, users will be denied any access to Password Manager for AD LDS functionality when their passwords are expired or should be changed at next login.
- **Authenticate users with disabled accounts:** If you select this check box, Password Manager for AD LDS will allow users whose accounts are disabled to unlock and re-enable their accounts, reset and manage passwords by using their Q&A profiles.

Authenticate with Q&A Profile (Random Questions)

Use this activity to authenticate a user with the personal Questions and Answers profile. In this activity you can specify how many questions from the Questions and Answers profile the user must answer to be authenticated. But you cannot select specific questions from user's Q&A profile. To require users to answer specific questions from their Q&A profiles, use the **Authenticate with Q&A profile (specific questions)** activity.

You can configure this activity to display all questions on a single page or only one or the specified number of questions at a time, so that users will not be able to see next questions before they answer the current ones. To display all questions on a single page, use this activity one time in a workflow. To display questions consecutively on several pages, use this activity several times in a workflow (place several **Authenticate with Q&A profile (random questions)** activities in a row).

This activity has the following settings:

- **All questions from user's Q&A profile:** Select this option to have users answer all questions from their Q&A profiles during authentication.
- **This number of randomly selected questions:** Select this option to set the number of questions required to authenticate users. You can specify what types of secret questions (mandatory, optional or user-defined) should be used to authenticate the user by selecting corresponding check boxes.
- **Do the following if the number of questions in user's Q&A profile is less than specified:** Using this option you can either allow or prohibit authentication for users if their Q&A profiles do not have enough secret questions. If you allow authentication, then all questions from the Q&A profile will be used to authenticate a user. If you decide to prohibit authentication, the workflow in which this activity is used will not be performed. The user will have to update his Q&A profile first, after that he will be able to perform the task that contains this authentication activity.
- **Allow users to see what questions were answered incorrectly:** Select this check box to allow users to see to what questions they have provided incorrect answers during authentication.

Authenticate with Q&A Profile (Specific Questions)

Use this activity to authenticate a user with the personal Questions and Answers profile. In this activity you can select specific questions from user's Q&A profile that the user must answer to be authenticated.

You can configure this activity to display all questions on a single page or only one or specified number of questions at a time, so that users will not be able to see next questions before they answer the current ones. To display all questions on a single page, use this activity one time in a workflow and select the required questions. To display questions consecutively on several pages, use this activity several times in a workflow (place several **Authenticate with Q&A profile (specific questions)** activities in a row).

This activity has the following settings:

- **Mandatory questions:** Specify mandatory questions from users' Q&A profiles that users will answer during authentication.
- **Optional questions:** Specify optional questions from users' Q&A profiles that users will answer during authentication.
- **User-defined questions:** Specify user-defined questions from users' Q&A profiles that users will answer during authentication.

- **Allow users to see what questions were answered incorrectly:** Select this check box to allow users to see to what questions they have provided incorrect answers during authentication.

IMPORTANT: If the questions you selected in this activity cannot be found in user's Q&A profile, the user will not be authenticated and the workflow containing this activity will not be performed for this user. The user will have to update his Q&A profile to answer the required secret questions.

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

Use this activity to authenticate a user with the personal Questions and Answers profile. In this activity, you can specify how many questions from user's Q&A profile must be answered to be authenticated. Users will have to choose the required amount of questions from their Q&A profile and answer them.

This activity has the following settings:

- **Number of questions that a user must answer during authentication:**
Specify the number of questions users must answer to be authenticated.
- **Do the following, if the number of questions in user's Q&A profile is less than specified:** Using this option you can either allow or prohibit authentication for users if their Q&A profiles do not have enough secret questions. If you allow authentication, then all questions from the Q&A profile will be used to authenticate a user. If you decide to prohibit authentication, the workflow in which this activity is used will not be performed. The user will have to update their Q&A profile first, after that they will be able to perform the task that contains this authentication activity.
- **Specify question categories which users will be able to choose from:**
Specify which question categories users can choose from when attempting to authenticate with this activity.
 - **Use all questions from user's profile:** This option will let users select any questions to authenticate with from their answered questions.
 - **Specify questions categories:** This option will let the administrators choose which question categories users can choose from when attempting to authenticate with this activity.
- **Allow users to see what questions were answered incorrectly:** Select this check box to allow users to see which questions they have provided incorrect answers to during authentication.

Authenticate with Defender

IMPORTANT:

- Authenticating with Defender is an activity not supported with the current release of Password Manager for AD LDS ADLDS.

- Change or Reset password in Active Directory and connected systems is not supported in AD LDS.

You can use this activity to configure Password Manager for AD LDS 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 for AD LDS use the Defender authentication, you must install the Defender Client SDK on the server on which Password Manager for AD LDS 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 external provider

Use this activity to authenticate users with an external provider, configured with Secure Token Server.

This activity has the following settings:

- **Choose from the configured providers to use in this activity for authentication:** A provider set up in **General Settings > Secure Token Server**, to be used when this activity is the current in a workflow.
- **Choose the behaviour of the authentication:** You can choose if the login interface is shown in an **iframe** or in a **popup**.

NOTE: Use **popup** behaviour when your login provider sends the content with **X-Frame-Options : Deny** header.

NOTE: For LDAP type Authentication Providers the **User's Unique ID Attribute** attribute mapping has to be objectGUID.

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 158.

Authenticate via Phone

Use this activity to include phone-based authentication in a self-service workflow. If your license includes phone-based authentication service, you will be able to configure and use this activity.

If your Password Manager for AD LDS license does not include phone-based authentication service and you want to use this service, please access the Support Portal at <https://support.oneidentity.com/>.

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

- The number starts with either **00** or **+** followed by a country code and subscriber's number. For example, **+1 555-789-1314** or **00 1 5554567890**.
- The number can have extensions. For example, the number **+1 555 123-45-67 ext 890**.
- Digits within the number can be separated by a space, hyphen, comma, period, plus and minus signs, slash (/), backward slash (\), asterisk (*), hash (#), and a tab character.
- The number can contain the following brackets: parentheses (), curly braces { }, square brackets [], and angle brackets < >. 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.

The USA numbers may not start with **00** or **+** sign, if they comply with all other requirements and contain 11 digits. For example, the number **1-555-123-3245** will be considered valid.

This activity has the following settings:

- **Authentication method:** You can specify whether you want users to receive a call or an SMS with a one-time PIN code by selecting the corresponding option. You can

also allow users to choose the authentication method on the Self-Service site by selecting the **Allow users to choose between an automated voice call and SMS** option.

- **SMS template:** Enter the text message that will contain a one-time PIN code and will be sent to users during phone-based authentication.
- **telephoneNumber, homePhone, mobile and other attributes:** Select one or several attributes of a user account from which telephone numbers will be used during phone-based authentication. You can also specify other attributes.

You can test the configured settings by clicking the **Test settings** button and entering the phone number to which a one-time PIN code will be sent.

Authenticate with Passcode

Use this activity to allow users to use passcode for creating or updating Questions and Answers profile. Passcodes are assigned by helpdesk operators to users who have forgotten their passwords and at the same are not registered with Password Manager for AD LDS or have forgotten their answers to secret questions.

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

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

For more information on configuring settings for assigning passcodes, see [Assign Passcode](#) on page 115.

Action Activities

This section describes built-in activities that provide core actions of the self-service workflows, such as Reset password, Unlock account, and so on.

Edit Q&A Profile

This activity is a core activity of the **My Questions and Answers Profile** workflow. Use this activity to enable users to create and update their Questions and Answers profiles.

You can also use this activity in the **Forgot My Password** and **Unlock My Account** workflows, if you want to force users to update their Q&A profiles after they reset passwords or unlock their accounts. When you use this activity in the **Forgot My Password** and **Unlock My Account** workflows, select the **Run this activity only if user's Q&A profile should be updated** check box to make users update their Q&A profiles only if the profiles are not compliant with the current requirements.

The activity has the following settings:

- **Run this activity only if user's Q&A profile should be updated:** When you use this activity in workflows other than **My Questions and Answers Profile**, for example, in **Forgot My Password** and **Unlock My Account** workflows, select this

check box to make users update their Q&A profiles only if the profiles are not compliant with the current Q&A policy.

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. If you want to enable users to reset passwords in several systems, configure the **Reset password in AD LDS and connected systems** activity. For more information on configuring this activity and using One Identity Quick Connect Sync Engine, see [Reset Password in AD LDS and Connected Systems](#) on page 96.

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 for AD LDS when that the **Enforce password history** option is enabled:

- Password Manager for AD LDS 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. If you want to enable users to change passwords in several systems, configure the **Change password in AD LDS and connected systems** activity. For more information on configuring this activity and using One Identity Quick Connect Sync Engine, see [Change Password in AD LDS and Connected Systems](#) on page 97.

Run this activity only when user must change password at next login: 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 login 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.

Reset Password in AD LDS and Connected Systems

Using this activity, you can configure Password Manager for AD LDS to use One Identity Quick Connect to reset passwords in connected systems. If used in conjunction with Quick Connect, Password Manager for AD LDS allows you to enable users and helpdesk operators to manage passwords across a wide variety of connected systems. To be able to integrate Password Manager for AD LDS with Quick Connect, you must have a working knowledge of Quick Connect Sync Engine.

To enable Password Manager for AD LDS to set passwords in connected systems through a Quick Connect server, the account used to access Quick Connect must be a member of the local administrators group on the Quick Connect server.

Before you can configure Password Manager for AD LDS to use a Quick Connect server for cross-platform password synchronization, you must do the following in Quick Connect:

- Create a connection to the AD LDS instances managed by Password Manager for AD LDS.
- Create connections to the systems you want Password Manager for AD LDS to synchronize passwords with.
- Map users from the managed AD LDS instances to users in the connected systems.

For more information on how to configure Quick Connect to set passwords in connected systems, see One Identity Quick Connect documentation.

To enable Password Manager for cross-platform password synchronization

1. Include the **Reset password in AD LDS and connected systems** activity in a workflow and click the activity to edit its settings.
2. In the **Quick Connect server name** text box specify the IP address or the fully qualified domain name of the Quick Connect server.
3. Select the account to be used to access the Quick Connect server. You can use either Password Manager Service account or specify another account.
 - To specify the user name, you can use either a pre-Windows 2000 logon name (such as **DomainName\UserName**) or a User Principal Name (such as **UserName@DomainName.com**).
4. Specify how you want Password Manager for AD LDS to act when the Quick Connect server is unavailable. To do it, select one of the following and click **Next**:
 - **Act as if no Quick Connect server was specified**: Users can manage their passwords only in the AD LDS instances. No warnings are displayed to users if Quick Connect server is not available.
 - **Alert users and allow them to reset passwords only in AD LDS**: Users are notified that other connected data sources are temporarily unavailable, and

are allowed to continue managing their passwords only in the AD LDS instances.

- **Do not allow users to reset passwords:** Users cannot perform any password management tasks in AD LDS instances and connected data sources, if the Quick Connect server is not available.
5. From the list of connected systems, select the systems in which you want to manage user passwords. For each selected system, specify the following options and click **Next**:
- **System alias**
 - **Reset password in this system independently from AD LDS:** Select this option to allow users to reset their passwords in a connected system independently from AD LDS. If you select this option, users will be able to enter different passwords for their accounts in AD LDS and the connected system.
 - **Do not allow resetting password in this system independently from AD LDS:** Select this option to prevent users from resetting their passwords in a connected system independently from AD LDS. Note, if you select this option, a user's password will be reset in the connected system only after the password has been successfully reset in AD LDS. If the user's password is not reset in AD LDS, it will be not reset in the connected system. Users can specify a different password for the connected system, if you select the **Allow users to specify different password for this system** option.

To enforce password history in AD LDS instances managed by Password Manager, select the **Enforce password history** check box. 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.

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

Password Manager for AD LDS 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 for AD LDS checks only the last five passwords. Therefore, it is advised that you double the password history value.

Having entered a new password that is not policy compliant, users may end up with a randomly generated password they don't know.

6. To close the wizard, click **OK**.

Change Password in AD LDS and Connected Systems

Using this activity, you can configure Password Manager for AD LDS to use One Identity Quick Connect to reset passwords in connected systems. If used in conjunction with Quick Connect, Password Manager for AD LDS allows you to enable users and helpdesk operators to manage passwords across a wide variety of connected systems. To be able to integrate Password Manager for AD LDS with Quick Connect, you must have a working knowledge of Quick Connect Sync Engine.

To enable Password Manager for AD LDS to set passwords in connected systems through a Quick Connect server, the account used to access Quick Connect must be a member of the local administrators group on the Quick Connect server.

Before you can configure Password Manager for AD LDS to use a Quick Connect server for cross-platform password synchronization, you must do the following in Quick Connect:

- Create a connection to the AD LDS instances managed by Password Manager for AD LDS.
- Create connections to the systems you want Password Manager for AD LDS to synchronize passwords with.
- Map users from the managed AD LDS instances to users in the connected systems.

For more information on how to configure Quick Connect to set passwords in connected systems, see One Identity Quick Connect documentation.

To enable Password Manager for cross-platform password synchronization

1. Include the **Change password AD LDS and connected systems** activity in a workflow and click the activity to edit its settings.
2. In the **Quick Connect server name** text box specify the IP address or the fully qualified domain name of the Quick Connect server.
3. Select the account to be used to access the Quick Connect server. You can use either Password Manager for AD LDS Service account or specify another account.
To specify the user name, you can use either a pre-Windows 2000 logon name (for example, **DomainName\UserName**) or a User Principal Name (for example, **UserName@DomainName.com**).
4. Specify how you want Password Manager for AD LDS to act when the Quick Connect server is unavailable. To do it, select one of the following and click **Next**:
 - **Act as if no Quick Connect server were specified:** Users can manage their passwords only in AD LDS instances. No warnings are displayed to users if Quick Connect server is not available.
 - **Alert users and allow them to change passwords only in AD LDS:** Users are notified that other connected data sources are temporarily unavailable, and are allowed to continue managing their passwords only in AD LDS instances.
 - **Do not allow users to change passwords:** Users cannot perform any password management tasks in AD LDS instances and connected data sources, if the Quick Connect server is not available.
5. From the list of connected systems, select the systems in which you want to manage user passwords. For each selected system, specify the following options and click **OK**:
 - **System alias**
 - **Change password in this system independently from AD LDS:** Select this option to allow users to change their passwords in a connected system

independently from AD LDS. If you select this option, users will be able to enter different passwords for their accounts in AD LDS and the connected system.

- **Do not allow changing password in this system independently AD LDS:** Select this option to prevent users from changing their passwords in a connected system independently from AD LDS. Note, if you select this option, a user's password will be changed in the connected system only after the password has been successfully changed in AD LDS. If the user's password is not changed in AD LDS, it will be not changed in the connected system. Users can specify different password for the connected system, if you select the **Allow users to specify different password for this system** option.

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 activity is a core activity of the **My Notifications** workflow. It allows users to select on the Self-Service site the events they want to be notified about, such as when their password is changed or account is unlocked.

The event list available on the Self-Service site depends on the settings you configure in the user notification activities included in the self-service workflows. Each user notification activity (**Email user if workflow succeeds** and **Email user if workflow fails**) has the settings that allow you to subscribe users to this notification or to allow users to choose whether they want to receive this notification or not.

If user notifications activities are not included in a workflow, users will not receive any email notifications about this workflow.

A notification text depends on the workflow in which the notification activity is used. For example, if the **Email user if workflow succeeds** activity is used in the **Forgot My Password** workflow, after successfully performing this task on the Self-Service site the user will be notified that his password has been reset. By default, the **Email user if workflow succeeds** and **Email user if workflow fails** activities are included in each built-in self-service workflow and offer notification templates.

Note that notification templates are available for built-in activities and built-in workflows only.

For more information on configuring user notification activities, see [Notification Activities](#) on page 102.

IMPORTANT: If a user notification activity is included in a helpdesk workflow, the user will receive the corresponding notification. You cannot change user subscription settings of notifications about helpdesk workflows.

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 the legislation requirements, organizations may be required to explicitly obtain users' consent to store their personal information which is available in Questions and Answers profile.

You can use this activity to have the Self-Service site ask users to agree that Password Manager for AD LDS will store their personal information.

For example, you can use this activity in the **My Questions and Answers Profile** workflow; it is recommended to place the 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. 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. 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

All built-in notifications can be of two types: user notifications and administrator notifications. Each notification type is divided 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

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 138.

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 box.

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 for AD LDS to meet specific requirements in your organization.

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

Table 6: Email notification parameters

Parameter	Description	Examples
#PRODUCT_NAME_FULL#	Full name of the software product. The parameter value is a constant.	One Identity Password Manager for AD LDS
#PRODUCT_NAME_SHORT#	Short name of the software product. The parameter value is a constant.	Password Manager for AD LDS
#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 for AD LDS 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 of the workflow that was	Forgot My Password

Parameter	Description	Examples
NAME#	executed. All workflow names are available on the Administration Site.	
#WORKFLOW_RESULT#	Result of a workflow execution displayed on the status page of the Self-Service Site.	Your password was successfully changed.
#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 77 and [Custom Activities](#) on page 79.

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 for AD LDS 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 User site. The three types of authentication methods available to select for the administrator are as follows:

- Security Questions
- Corporate Authentication
- Personal Email

IMPORTANT: The administrator can select any of the activities selected in the registration method, to make it default mode for authentication for the users on the User site. Select one of the settings radio buttons from the right side to make it default authentication method.

NOTE: When the administrator selects registration method(s), only the respective authentication methods are visible to the administrator in Authentication methods. See the *Register* section.

Security Questions

Use this activity to authenticate a user with the personal Questions and Answers profile. In this activity, the administrator can specify how many questions from the Questions and Answers profile the user must answer for authentication.

- **Authenticate with Q&A Profile** : See Authenticate with Q&A Profile.

Corporate Authentication

Use this activity to authenticate a user with a mobile device. There are two methods to authenticate the users using a mobile device.

- **Authenticate with RADIUS Two-Factor Authentication**: See Authenticate with RADIUS Two-Factor Authentication.
- **Authenticate via Phone**: See Authenticate via Phone.

Personal Email

Authenticate via Passcode: Use this activity to authenticate the users with a passcode. The administrator can configure passcode length and expiry time limit for the passcode.

Authenticate with Q&A Profile

Use this activity to authenticate a user with a personal Questions and Answers profile. In this activity you can specify mandatory and helpdesk questions from user's Q&A profile that a user must answer to be authenticated.

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

You can select one of the following authentication methods:

- **Answers to the specified questions (user's answer is shown)**: In this mode, a helpdesk operator will ask a user for complete answers to the specified questions, and then compare them to the answers displayed on the identity verification page.
IMPORTANT: This option cannot be used if user answers to mandatory questions 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 70.
- **Answers to the specified questions (user's answer not shown)**: In this mode, a helpdesk operator will ask a user for complete answers to the specified questions, and enter the answers on the identity verification page.
- **Random characters of answers to the specified questions**: In this mode, a helpdesk operator will ask a user to tell the specified number of characters in the user's answer to a specified question, and then type in those characters in the appropriate positions on the identity verification page.

Authenticate via Phone

Use this activity to include phone-based authentication in a helpdesk workflow. If your license includes phone-based authentication service, you will be able to configure and use this activity.

If your license does not include phone-based authentication service and you want to use this service, you can access the Support Portal at <https://support.oneidentity.com/>.

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

- The number starts with either **00** or **+** followed by a country code and subscriber's number. For example, **+1 555-789-1314** or **00 1 5554567890**.
- The number can have extensions. For example, the number **+1 555 123-45-67 ext 890**.
- Digits within the number can be separated by a space, hyphen, comma, period, plus and minus signs, slash (/), backward slash (\), asterisk (*), hash (#), and a tab character.
- The number can contain the following brackets: parentheses (), curly braces { }, square brackets [], and angle brackets < >. 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.

The USA numbers may not start with **00** or **+** sign, if they comply with all other requirements and contain 11 digits. For example, the number **1-555-123-3245** will be considered valid.

This activity has the following settings:

- **Authentication method:** You can specify whether you want users to receive a call or an SMS with a one-time PIN code by selecting a corresponding option. You can also allow helpdesk operators to offer users to choose the authentication method by selecting the **Allow users to choose between an automated voice call and SMS** option.
- **SMS template:** Enter 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 telephone numbers will be used during phone-based authentication. You can also specify other attributes.

You can test the configured settings by clicking the **Test settings** button and entering the phone number to which a 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 for AD LDS 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 for AD LDS 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 for AD LDS use the Defender authentication, you must install the Defender Client SDK on the server on which Password Manager for AD LDS 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

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 158.

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. If you want to enable helpdesk operators to reset passwords in several systems, configure the **Reset password in AD LDS and connected systems** activity. For more information on configuring this activity and using One Identity Quick Connect Sync Engine, see [Reset Password in AD LDS and Connected Systems](#) on page 112.

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 for AD LDS when that the **Enforce password history option** is enabled:

- Password Manager for AD LDS 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 for AD LDS 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.

Reset Password in AD LDS and Connected Systems

Using this activity, you can configure Password Manager for AD LDS to use One Identity Quick Connect to reset passwords in connected systems. If used in conjunction with Quick Connect, Password Manager for AD LDS allows you to enable users and helpdesk operators to manage passwords across a wide variety of connected systems. To be able to integrate Password Manager with Quick Connect, you must have a working knowledge of Quick Connect Sync Engine.

To enable Password Manager for AD LDS to set passwords in connected systems through a Quick Connect server, the account used to access Quick Connect must be a member of the local administrators group on the Quick Connect server.

Before you can configure Password Manager for AD LDS to use a Quick Connect server for cross-platform password synchronization, you must do the following in Quick Connect:

- Create a connection to the AD LDS instances managed by Password Manager for AD LDS.
- Create connections to the systems that you want Password Manager for AD LDS to synchronize passwords with.
- Map users from the managed AD LDS instances to users in the connected systems.

For more information on how to configure Quick Connect to set passwords in connected systems, see the *One Identity Quick Connect* documentation.

To enable Password Manager for cross-platform password synchronization

1. Include the **Reset password in AD LDS and connected systems** activity in a workflow and click the activity to edit its settings.
2. In the **Quick Connect server name** text box specify the IP address or the fully qualified domain name of the Quick Connect server.
3. Select the account to be used to access the Quick Connect server. You can use either Password Manager Service account or specify another account.

To specify the user name, you can use either a pre-Windows 2000 logon name (such as `DomainName\UserName`) or a User Principal Name (such as `UserName@DomainName.com`).

4. Specify how you want Password Manager for AD LDS to act when the Quick Connect server is unavailable. To do it, select one of the following and click **Next**:
 - **Act as if no Quick Connect server was specified:** Helpdesk operators can manage users' passwords only in AD LDS instances. No warnings are displayed if Quick Connect server is not available.
 - **Alert users and allow them to reset passwords only in AD LDS:** Helpdesk operators are notified that other connected data sources are temporarily unavailable, and are allowed to continue managing users' passwords only in AD LDS instances.
 - **Do not allow users to reset passwords:** Helpdesk operators cannot perform any password management tasks in AD LDS instances and connected data sources, if the Quick Connect server is not available.
5. From the list of connected systems, select the systems in which you want to manage user passwords. For each selected system, specify the following options and click **Next**:
 - **System alias**
 - **Reset password in this system independently from AD LDS:** Select this option to allow helpdesk operators to reset users' passwords in a connected system independently from AD LDS. If you select this option, helpdesk operators will be able to enter different passwords for users' accounts in AD LDS and the connected system.
 - **Do not allow resetting password in this system independently from AD LDS:** Select this option to prevent helpdesk operators from resetting users' passwords in a connected system independently from AD LDS. Note, if you select this option, a user's password will be reset in the connected system only after the password has been successfully reset in AD LDS. If the user's password is not reset in AD LDS, it will be not reset in the connected system. Helpdesk operators can specify a different password for the connected system, if you select the **Allow specifying different password for this system** option.
6. To enforce password history in the AD LDS instances managed by Password Manager for AD LDS, select the **Enforce password history** check box. 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.

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

- Password Manager for AD LDS 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 for AD LDS checks only the last five passwords. Therefore, it is advised that you double the password history value.
- Having entered a new password that is not policy compliant, users may end up with a randomly generated password they don't know.

7. Click **OK** to close the wizard.

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 activity is a core activity of the **Assign Passcode** workflow. It allows helpdesk operators to assign a passcode to the user who has forgotten password and is not yet registered with Password Manager for AD LDS or has forgotten answers to secret questions. This activity has the following settings:

- **Passcode length:** Specify how many characters a passcode must contain.
- **Passcode lifetime:** Specify how long a passcode issued by helpdesk operators is valid.

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 138.

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 box.

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 for AD LDS 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 for AD LDS 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 for AD LDS to invite users to register with Password Manager for AD LDS 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 141.

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\username 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 7: 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 8: User notifications

Option	Description
User is not registered with Password Manager	Select to force users to register with Password Manager for AD LDS by creating Q&A profiles, if users are not registered with Password Manager for AD LDS.
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	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

Option	Description
questions than required for registration	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 profile is older than the specified value	Select to force users to update their Q&A profiles, if their last 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 138.

Remind Users to Create/Update Profiles

By using this enforcement rule, you can configure Password Manager for AD LDS 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 142.

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\username 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 9: 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\username 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 for AD LDS 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 138.

Remind Users to Change Password

By using this enforcement rule you can configure Password Manager for AD LDS 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 143.

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\username 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 10: 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 138.

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
- Extensibility Features
- RADIUS Two-Factor Authentication
- Internal Feedback
- Password Manager for AD LDS components and third-party applications
- Unregistering users from Password Manager for AD LDS
- 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 for AD LDS 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 11: 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. <p>NOTE: The list will display all aliases that the user</p>

Option	Description
	<p>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.
Allow users to search for their accounts	<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> • 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. • User account attributes to display in search

Option	Description
	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 Security Options

By configuring the security options you can specify whether CAPTCHA or reCAPTCHA images should be displayed on the Find Your Account page to prevent bot attacks.

reCAPTCHA is a free CAPTCHA service provided by Google.

To start using reCAPTCHA you need to sign up and get reCAPTCHA keys on the following web site: <http://www.google.com/recaptcha>.

When getting the keys, provide the DNS name of the domain where Password Manager Self-Service sites are installed. If the Self-Service sites are installed in different domains, select the **Enable this key on all domains** check box to create a global key.

To learn more about using and configuring reCAPTCHA, go to <http://www.google.com/recaptcha/learnmore>.

To configure security 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/`.
2. On the menu bar, click **General Settings**, then click the **Search and Logon Options** tab, and select the **Self-Service site** option from the drop-down list.
3. In the **Security Settings** section select the **Show a security image to prevent bot attacks** check box to have the Self-Service site display a picture with characters and require the user to enter the characters on the picture. This feature provides enhanced protection against automated attacks.
4. Select the **Display CAPTCHA** radio button if you want the Self-Service site to show CAPTCHA images on the Find Your Account page. Click **Settings** to configure the following CAPTCHA settings:

- **Number of characters:** Specify the number of characters that will be displayed on a CAPTCHA image.
 - **Noise level:** Select the noise level for a CAPTCHA image. The higher the level the more difficult it will be to read the characters.
5. Select the **Display reCAPTCHA** radio button if you want the Self-Service site to show reCAPTCHA images on the Find Your Account page. Click **Settings** to configure the following reCAPTCHA settings:
 - **Public key:** Specify the public key you received when configuring reCAPTCHA on the reCAPTCHA Web site.
 - **Private key:** Specify the private key you received when configuring reCAPTCHA on the reCAPTCHA Web site.
 - **Theme:** Select a color theme for the reCAPTCHA widget.
 6. Select the **Show a security image every time the search is performed** check box to show a CAPTCHA or reCAPTCHA image every time the search is performed on the Find Your Account page of the Self-Service page. Selecting this option increases protection against bot attacks.
 7. Click **Save**.

Configuring Search Options for the 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\username 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 the personally identifiable information (PII) for the currently logged in user. For more information, see [Hiding personally identifiable information for logged-in users](#).
- Enable or disable CAPTCHA or reCAPTCHA checks to prevent bot attacks. For more information, see [Configuring anti-bot security settings](#).

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:

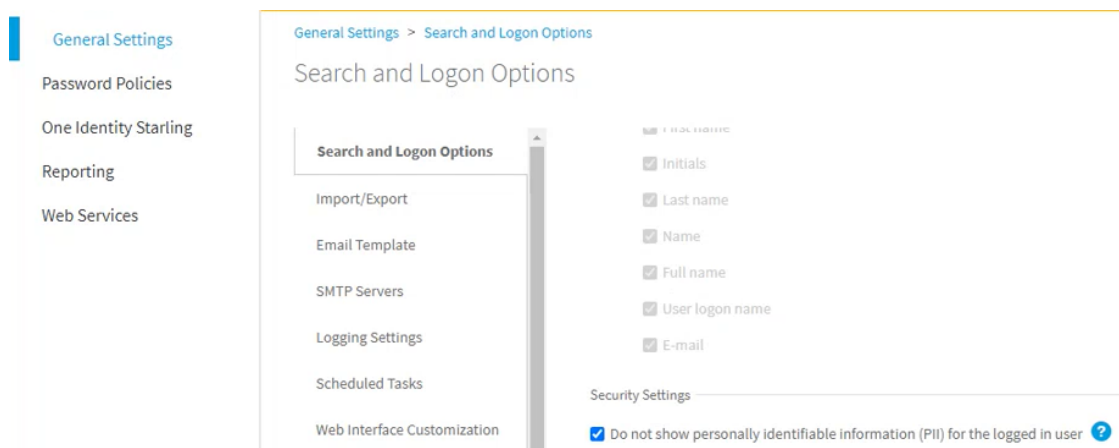
Sam Smith (ADLDS-domain)

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. 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)

Configuring anti-bot security settings

To prevent bot attacks against your One Identity Password Manager for AD LDS deployment, you can configure anti-bot security measures for the **Find User** page of the Self-Service Site. Password Manager for AD LDS supports configuring CAPTCHA images and reCAPTCHA v2 or v3 security solutions.

- For more information on configuring CAPTCHA, see [Configuring CAPTCHA security images](#).
- For more information on configuring reCAPTCHA, see [Configuring reCAPTCHA security settings](#).

Configuring CAPTCHA security images

You can configure the Password Manager for AD LDS Self-Service Site to display CAPTCHA images on the **Find User** page as an anti-bot security measure.

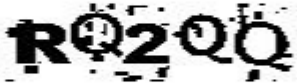
Enter your user name *

sam.smith

o1d.local

▼

Enter the characters you see on the picture



Get new image

Enter Captcha Text *

RQ2QQ

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 or reCAPTCHA settings, enable **Show a security image to prevent bot attacks**.
4. To configure the CAPTCHA settings, select **Display CAPTCHA** and click **Settings**.
5. In the **CAPTCHA Settings** dialog, configure the following options:

- **Number of characters:** Specify the number of characters (1–15) to display on the generated CAPTCHA image. The default value is 5.
- **Noise level:** Specify the number and size of noise artifacts on the generated CAPTCHA image. Higher levels mean more difficult readability.

When ready, 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 search is performed on the **Find User** page of the Self-Service Site.

TIP: Enable this setting for an increased protection against bot attacks.

7. To apply your settings, 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 for AD LDS 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 Admin 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, enable **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 Admin site](#).
- **Secret key:** Enter the secret key that was generated on the [Google reCAPTCHA Admin 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**.

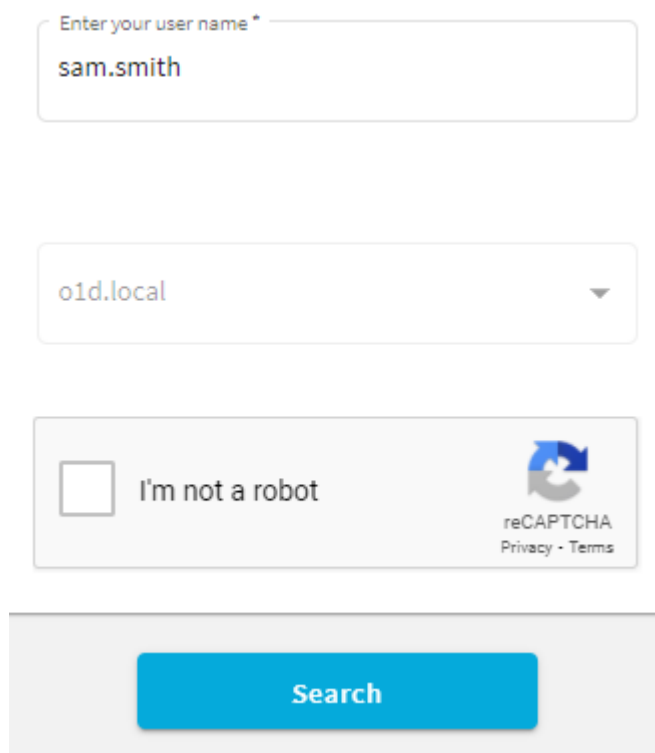
6. Under **Security Settings**, select **Show a security image every time the search is performed** to perform the configured anti-bot protection check each time a search is performed on the **Find User** page of the Self-Service Site.

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 labeled "Enter your user name *" containing the text "sam.smith".
- A dropdown menu containing the text "oid.local".
- A reCAPTCHA v2 widget consisting of an unchecked checkbox, the text "I'm not a robot", the reCAPTCHA logo, and links for "Privacy" and "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:

sam.smith

o1d.local ▼

Search


Privacy • Terms

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, etc.) and configuration settings, including but not limited to Management Policies, general settings, password policies, etc.

If you want to create a realm, you need to export the configuration settings from a Password Manager for AD LDS instance and create a replica of this instance by importing the configuration settings. To learn more about creating Password Manager for AD LDS realms, see [Installing multiple instances of Password Manager for AD LDS](#) on page 18.

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\username 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\username 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 for AD LDS 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>/PMAAdminADLDS/`.
NOTE: When prompted to log in, provide your domain user name in a domain-name\username format.
2. On the menu bar, click **General Settings > SMTP Servers** and then click **Add SMTP server**.
3. In the **Add SMTP Server** dialog box, configure the following options and click **Save**:

Table 12: 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 for AD LDS 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 for AD LDS uses the servers to send email notification messages. Password Manager for AD LDS 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>/PMAdminADLDS/`.
NOTE: When prompted to log in, provide your domain user name in a domain-name\username 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 for AD LDS provides a simple and convenient way to collect the diagnostic information about the activity of Password Manager for AD LDS. Diagnostic logging is mainly intended to be used by support personnel for troubleshooting purposes.

To enable diagnostic logging in Password Manager for AD LDS

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 13: 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 for AD LDS, the Password Manager for AD LDS setup adds the following scheduled tasks on the computer where Password Manager for AD LDS 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 for AD LDS ADLDS.

Invitation to Create/Update Profile Task

This task is used to enumerate users who are not registered with Password Manager for AD LDS 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 118.

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\username 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 for AD LDS 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 121.

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\username 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 for AD LDS server on which the task should be run.

IMPORTANT: The task status can be viewed only on the Password Manager for AD LDS 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 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\username 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 for AD LDS instance**, select the Password Manager for AD LDS server on which the task should be run.
NOTE: The task status can be viewed only on the Password Manager for AD LDS 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.

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 177.

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>/PMAAdminADLDS/`.
NOTE: When prompted to log in, provide your domain user name in a domain-name\username 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 for AD LDS server on which the task should be run.
NOTE: The task status can be viewed only on the Password Manager for AD LDS 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 task is used to update the RADIUS server status. By default, the schedule task runs for 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\username 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 for AD LDS instance**, select the Password Manager for AD LDS server on which the task should be run.
NOTE: The task status can be viewed only on the Password Manager for AD LDS 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 for AD LDS 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 for AD LDS, the number of users required to register with Password Manager for AD LDS, and the number of users required to update profile. This information is collected for all application directory partitions managed by a specific Password Manager for AD LDS 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\username 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 for AD LDS server on which the task should be run.

NOTE: The task status can be viewed only on the Password Manager for AD LDS 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\username 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 for AD LDS 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.

The default Product logo and the Company logo specific to Legacy Self Service site are transparent images which are not applicable to the Password Manager for AD LDS Self-Service site. Therefore, the transparent images may appear to be missing from the Password Manager for AD LDS Self-Service site.

Enabling Self-Service UI 5.13.1

The following options appear only in case of an Inplace Upgrade of Password Manager for AD LDS to version 5.13.1 since inplace upgrade is the only upgrade, which retains the Legacy Self Service site along with the Password Manager for AD LDS Self Service site (**Self-Service UI version 5.9.5 onwards**).

- Maintain Self-service site (pre-5.9.5)
- Switch to Self-service site (5.9.5 or later)

IMPORTANT:

- The default product logo and the company logo image used in the Legacy Self Service site may not be compatible with the Password Manager for AD LDS Self Service site as there is a limitation to the pixels in the image.
- Users could apply any valid custom product logo and company logo to the Legacy Self service site and the same gets applied on the Password Manager for AD LDS Self-service site (Self Service UI 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 Legacy 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 legacy 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 Legacy 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 Password Manager Service. Reinitialization means changing any of the settings you specified during initialization: the certificate for encrypting traffic between the standalone Self-Service and Helpdesk sites and the Password Manager Service, port number, encryption algorithm and key length, and hashing algorithm.

You may want to reinitialize the Password Manager instance to change any of the settings you specified when initializing the instance.

Modifying Service Connection Settings

Using service connection settings you can specify the following:

- **Certificate name:** use this setting to enter the name of the certificate for authentication and traffic encryption the Password Manager for AD LDS Service and the web sites (Self-Service and Helpdesk). By default, Password Manager for AD LDS uses a built-in certificate issued by One Identity for this purpose. If you install the web sites on a standalone server, it is recommended to replace the default certificate with a custom certificate issued by a trusted Windows-based authentication authority.

For more information on obtaining and installing custom certificates, see [Specifying Custom Certificates for Authentication and Traffic Encryption Between Password Manager for AD LDS Service and Web Sites](#) on page 19.

- **Port number** - use this setting to specify the port that the Self-Service and Helpdesk sites will use to connect to the Password Manager for AD LDS Service. By default, port **8081** is used.

IMPORTANT: If you change the certificate and port number, the Self-Service and Helpdesk sites installed on standalone servers will be unavailable to users until you reinitialize the sites using the updated settings. For information, see [Installing Legacy Self-Service, Password Manager for AD LDS Self-Service, and Helpdesk Sites on a Standalone Server](#) on page 15.

To modify the service connection settings

1. On the home page of the Administration site, click **General Settings**, and then click the **Reinitialization** tab.
2. Under **Service connection settings**, from the **Certificate name** drop-down list, select the required certificate for authentication and traffic encryption between the Web sites (Self-Service and Helpdesk) and the Password Manager for AD LDS Service.
3. In the **Port number** text box, enter the port number you want the web sites to use to connect to the Password Manager for AD LDS Service.
4. Click **Save**.

Modifying Advanced Settings

Using the advanced settings you can specify the following:

- **Encryption algorithm:** use this setting to select the encryption algorithm that is used to encrypt users' answers to secret questions and other security sensitive information. You can select from two options: Triple DES and AES. By default, Password Manager for AD LDS uses Triple DES algorithm to encrypt data.

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

- **Encryption key length:** use this setting to select whether a 192-bit or 256-bit encryption key will be used.
- **Attribute for storing Q&A profiles:** use this setting to enter the attribute name that will be used for storing Q&A profile data. By default, Password Manager for AD LDS stores Q&A profile data in the comment attribute of each user's account and the configuration data in the comment attribute of a configuration storage account, which is automatically created when installing Password Manager for AD LDS.

IMPORTANT: If you change encryption settings and the attribute for storing Q&A profiles, the current instance will be excluded from a realm it belongs to and users may lose their Q&A profiles.

When you change these settings, do the following to keep users' Q&A profiles:

- Export the current configuration when saving updated instance settings.
- Update Q&A profiles using the Migration wizard (upload the exported configuration to the wizard) on the current instance.
- To replicate new settings and updated Q&A profiles export the updated configuration from the current instance and import the configuration to other instances.

If you do not use the Migration wizard to update users' Q&A profile after changing the settings, users will have to re-register with Password Manager for AD LDS.

- **Hashing algorithm:** Use this setting to select 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 for AD LDS uses SHA-256 hashing algorithm. Password Manager for AD LDS will hash users' answers if **Store answers using reversible encryption** option is *not* selected in the Q&A Profile settings.

IMPORTANT: If you change the hashing algorithm, the selected algorithm will be applied to newly created Q&A profiles only. Existing Q&A profiles will be hashed with the previously selected algorithm.

To modify the advanced settings

1. On the home page of the Administration site, click **General Settings > Reinitialization**, and expand the **Advanced settings** section.
2. From the **Encryption algorithm** drop-down list, select the encryption algorithm for encrypting users' answers to secret questions and other security sensitive data.
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 users' authentication answers.

5. In the **Select the attribute of user's account in Active Directory in which user's Questions and Answers profile and Corporate phone will be stored** section, provide the following data.
 - a. **Security questions:** Enter the required security question.
 - b. **Corporate Phone:** Enter the mobile number of the user.
 - c. **Corporate email:** Enter the corporate's email id of the user.
6. Click **Save**.
Once you click **Save, Reinitialize Instance** dialog box appears.
7. In the **Reinitialize Instance** dialog box, a password is generated for the configuration file that you should export to update users' Q&A profiles and click **Export**.
8. Click **Save**.

To update users' Q&A profiles with new instance settings

Before running the Migration Wizard, update the following attributes in the Migration Wizard\Resources\productinfo.xml file:

- **<productNameFull>:** One Identity LLC for AD LDS
- **<productNameShort>:** Password Manager for AD LDS for AD LDS
- **<realmType>:** AD LDS

The values specified above can be also copied from One Identity\Password Manager for AD LDS\Service\Resources\productinfo.xml.

1. Run the Migration wizard from the Password Manager for AD LDS media autorun window.
2. On the **Welcome** page, select the **Update users' Q&A profiles with new instance settings** task.
3. On the next page, upload the configuration file you exported when reinitializing the instance. Click **Browse** to select the file, enter the password you specified for the file, and click **Next**.
4. Select users whose Q&A profiles you want to update and click **Next**. To select groups, click **Add** and do the following:
 - In the **Add Groups** dialog box, enter the group name, select the application directory partition from the list and click **Search**.
 - Select the required groups in the list and click **Save**.
5. On the next page, do one of the following and click **Next**:
 - a. **Security Questions:** Provide the required security questions.
 - b. **Corporate Phone:** Provide the required corporate phone.
 - c. **Corporate email, Personal email, and Personal phone** fields are not editable.

6. On the status page, click **View the report for detailed information** to view a detailed account of updating profiles. If you updated Q&A profiles in test mode, click **Update Q&A profiles in production mode**.

After you have updated the Q&A profiles with new instance settings, join other instances to this realm by exporting the configuration from the current instance and importing it to other instances. For more information on how to import and export configuration settings, see [Import/Export Configuration Settings](#) on page 137.

Realm Instances

On the Administration site you can view a list of installed Password Manager for AD LDS instances belonging to one realm. This information is available on the Realm Instances page.

To open the Password Manager for AD LDS 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 for AD LDS 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 for AD LDS Service instance. To change any of these settings, see [Instance Reinitialization](#) on page 149.

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 for AD LDS will access an AD LDS instance and a specified application directory partition. You can use the Password Manager for AD LDS 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 for AD LDS 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 for AD LDS access the AD LDS instance using the Password Manager for AD LDS Service 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

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 for AD LDS access the managed instance using the Password Manager for AD LDS 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

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.

Extensibility Features

Extensibility features allow you to customize and extend the Password Manager for AD LDS functionality. The features include the following:

- Custom activities
- Built-in web service
- Custom web services
- Import/export of activities and workflows
- Troubleshooting mode

All these features are available only after you turn the extensibility on.

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.

After you turn the extensibility features on, you can also turn on the troubleshooting mode. When the troubleshooting mode is on, the following additional information is displayed:

- Identifiers of activities and workflows (on the Administration site)
- PowerShell output (on the Self-Service site)

To turn the troubleshooting mode 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.
4. Click the **Turn on** button under the troubleshooting mode.

Extensibility Features Overview

Custom activities are activities whose behavior is defined by a PowerShell script. You can create a custom activity from scratch or convert a built-in activity to a custom one. For more information, see [Custom Activities](#) on page 79 and refer to the Password Manager for AD LDS SDK.

The built-in web service allows a third-party system to access a whole workflow or a specific activity using HTTP and data exchange in XML and JSON formats. You can use the built-in web service to run a workflow and to interfere in a workflow running process. For more information, see the Password Manager for AD LDS SDK. For experimenting with the built-in web service, a Swagger UI is provided. For more information on how to use Swagger UI, see <https://swagger.io/tools/swagger-ui/>.

NOTE: The extensibility features are only supported by One Identity Professional Services, and are not covered by One Identity Technical Support.

Custom web services allow you to further extend the Password Manager for AD LDS functionality and enable 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 employing the assign passcode functionality in Password Manager for AD LDS. For more information, see the Password Manager for AD LDS SDK.

Import/export of activities and workflows allows you to copy and share custom activities and workflows. For more information, see [Importing and exporting workflows](#) on page 78 and [Importing and exporting custom activities](#) on page 81.

The troubleshooting mode provides you additional information about workflows and activities and their execution. When this mode is enabled, on the Administration site you can view identifiers of workflow and activities; you can use these identifiers in PowerShell scripts. On the Self-Service site, you can view the PowerShell output that allows you to troubleshoot the scripts.

RADIUS Two-Factor Authentication

RADIUS Two-Factor Authentication enables two-factor authentication on Password Manager for AD LDS. 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 for AD LDS, you have to configure the RADIUS server details in Password Manager for AD LDS.

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 PMAdmin, PMHelpdesk and PMSelfService sites, to allow users to give feedback on Password Manager for AD LDS.

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 PMAdmin site feedbacks, the **Feedback** button will be displayed after a new session is opened, for example, by logging out and then logging in.

Password Manager for AD LDS components and third-party applications

The following sections describe Password Manager for AD LDS components and third-party applications.

Password Manager for AD LDS Secure Token Server

Password Manager for AD LDS Secure Token Server (STS) is installed with Password Manager for AD LDS 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 for AD LDS Self-Service Site to authenticate users in a workflow. It is installed as a service called Password Manager for AD LDS 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 "Authenticate with external provider" activity into any workflow.

- If you have not set up Secure Token Server connection or did not have valid providers configured in authentication providers, you cannot use this activity.
- If you set up at least one provider, you can start using it.
- If you set up more than one, you can select a provider for each activity used in workflows.

Authenticate with external provider on Self Service site

When Authenticate with external provider is the current activity in a workflow, the user is presented with a login form, where they need to provide the credentials for the configured authentication provider. If the configured provider is using MFA, the user will be prompted for the next step. For more information, see [Authenticate with external provider](#).

This login interface uses the browser's language. The supported languages are the following:

- Argentinean (ar)
- Chinese (zh)
- Dutch (nl)
- English (en)
- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Russian (ru)
- Spanish (es)

Password Manager 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 for AD LDS realm

The Password Manager for AD LDS STS settings are stored separately from other Password Manager for AD LDS 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 for AD LDS 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 for AD LDS 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 PMAAdmin 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 for AD LDS STS settings are not replicated automatically

To replicate the Password Manager for AD LDS STS settings manually, copy the `rstsConfig.bin` file from the server where you configured Password Manager for AD LDS STS to all other servers. After you copy the file, you must restart the Password Manager for AD LDS 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 for AD LDS 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 PMAAdmin site, navigate to **General Settings > Secure Token Server page**.

Unregistering users from Password Manager for AD LDS

Using the unregister feature, users registered to the Password Manager for AD LDS can be removed. Note that the user is removed only from the Password Manager for AD LDS and not Active Directory.

To unregister a user from the Password Manager for AD LDS

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 AD LDS 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 for AD LDS 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 for AD LDS logs are available in C:\Windows\TEMP folder. If the default Password Manager for AD LDS 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 for AD LDS 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 for AD LDS Admin 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 for AD LDS provides 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 the process to upgrade Password Manager for AD LDS to the latest version (5.13.1).

NOTE:

- It is recommended to back up the current configuration by exporting the settings from 5.7.1 or later versions. For more information, see [To export configuration settings from Password Manager for AD LDS 5.7.1 or later versions to 5.13.1](#) on page 172..
- Running the Migration Wizard is not required while upgrading from Password Manager for AD LDS 5.7.1 or later versions to 5.13.1.
- If you want to upgrade to 5.13.1, it is recommended to reinstall the license file from the Administration site once the upgrade is complete. Before installing the license, delete the existing SoftLicense binary value from [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Quest Software] registry key.
- Any workflows that are customized in the previous versions of Password Manager for AD LDS should be manually merged with the workflow of the latest version of the Password Manager for AD LDS to avoid any end user data corruption.

For example, changes made to the Register workflow (Self-Service workflows) such as addition/update of any authentication steps to the default configuration, should be manually recreated after upgrade to PM 5.13.1.

- To update storage files with new encryption mechanism, all realm instances must be updated with the Password Manager 5.13.1 configuration and must have the same encryption key.

To perform the same, login to PMAdmin site from the primary server, Navigate to **General Settings > Import/Export > Export**. Copy and Save the password securely. Import this configuration data in all the PM secondary replication instances by selecting the exported configuration data and providing the password.

- If the secondary instances are not updated with new configuration, a notification will be displayed in Administration site as 'Import configuration settings from primary instance'.

In the replication instances, Navigate to **General Settings > Import/Export > Import**, select the exported data from the primary server and input the password saved.

- **Shared.storage** file will be encrypted and copied to Active Directory only when all replication instances are updated with Password Manager 5.13.1 configuration and encryption key.
- When all the realm instances are updated with Password Manager for AD LDS 5.13.1, Q&A profiles of users will be updated with new encryption key when one of the following is performed:
 - User updates Q&A profile
 - Run Migration wizard to update all the user profiles automatically

This section consists of the following topics:

- [In-place upgrade from 5.8.2 or later versions to 5.13.1](#)
- [Manual upgrade from 5.9.x or later versions](#)

To export configuration settings from Password Manager for AD LDS 5.7.1 or later versions to 5.13.1

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\username format.
2. On the left pane, click **General Settings**, and click the **Import/Export** tab and select the **Export configuration settings** option, and then click **Export**.

After you have exported configuration settings from Password Manager 5.13.1 or later versions, you can uninstall it.

To uninstall Password Manager for AD LDS 5.7.1 or later versions

1. Click **Start**, click **Run**, type `appwiz.cpl`, then press **Enter**.
2. Select **One Identity Password Manager for AD LDS x86/x64** in the list, then click **Uninstall**.

After you uninstall Password Manager 5.7.1 or later versions, install Password Manager 5.13.1 on the same computer. All configuration settings will be automatically detected by the new version.

In-place upgrade from 5.8.2 or later versions to 5.13.1

To in-place upgrade from version 5.8.2 or later versions to version 5.13.1

1. From the autorun window of the installation media, click **Install against Password Manager x64** option. Read the content and click **Next**.
2. Read the content in the **Risk of data loss!** window and select **I acknowledge the above instructions**, and then 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, and 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 installs the following sites:

- Administration Site
- Helpdesk Site
- Password Manager Self-Service Site
- Legacy Self Service Site

NOTE: The above mentioned upgrade steps are not applicable for 5.7.1 or other lower versions.

Manual upgrade from 5.9.x or later versions

Uninstall Password Manager for AD LDS 5.9.x or later versions, then install Password Manager for AD LDS 5.13.1 on the computer where Password Manager for AD LDS 5.9.x or later versions was installed. For more information, see [To uninstall Password Manager for AD LDS 5.7.1 or later versions](#).

To manually upgrade from 5.9.x or later versions to version 5.13.1

1. From the autorun window of the installation media, click **Install** against Password Manager x64 option. Read the content and click **Next**.
2. Select **I accept the terms in License Agreement** check box, and then click **Next**.
3. In the **User Information** page, enter the user details such as the username and the organization to which the user belongs to, and then click **Next**.
 - To verify licenses information, click **Licenses...**, then check the statuses of the license.

NOTE: If the license has expired, click **Browse license...** and select the appropriate license to continue the Password Manager service.

4. In the **Custom Setup** page, click the respective option that needs to be installed, and then click **Next**.
5. In the **Password Manager Service Account Information** page, the account name appears by default. Enter the password, and then click **Next**.

NOTE: To change the account name, click **Browse...** and select the appropriate Password Manager for AD LDS service account name.
6. In the **Specify Web Site and Application Pool Identity** page, choose the website name, and in the Application pool identity section, the account name appears by default. Enter the password, and then click **Next**.

NOTE: To change the account name, click **Browse...** and select the appropriate Application Pool Identity account name.
7. After completing the above process, click **Install**.

Upon successful installation, the Password Manager installs the following sites:

- Administration Site
- Helpdesk Site
- Password Manager Self-Service Site

NOTE:

- Make sure that you have taken a back up of the current configuration settings. For more information, see [To export configuration settings from Password Manager for AD LDS 5.7.1 or later versions](#).
- After you uninstall Password Manager for AD LDS 5.7.1 or later versions, all configuration settings will be automatically detected by the new version. For more information on how to install Password Manager, see [Installing Password Manager for AD LDS](#).
- If you have multiple Password Manager for AD LDS instances installed, when upgrading them, you may experience the following issue: the Realm Instances page of the Administration site displays an incorrect list of installed instances. After you upgrade all instances, the page will display the correct list.

IMPORTANT:

- Switch to the Password Manager for AD LDS self Service site(**Self-Service UI version 5.9.5 onwards**) option is displayed only in case of in place upgrade.
- In case of Manual upgrade to 5.13.1, the Self-Service site gets replaced as Password Manager for AD LDS Self-Service site. Hence, post manual upgrade, you can see only one Self service site (Password Manager for AD LDS Self-Service Site) and legacy self-service site is not more accessible, by default.
- In case of manual upgrade, if the Legacy Self-Service site is required, the administrator must install it exclusively, in addition to the existing Password Manager for AD LDS Self Service site. In this case, the Enabling Self-Service UI 5.13.1 (**Switch to Self-service site 5.9.5 onwards**) option will not be applicable.

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 for AD LDS 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 189.

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 178.

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 153.

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 box, 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 box, view or modify the following options, and then click **Save**:

Table 14: 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 181, 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 178, 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 for AD LDS (PM) application, scopes can be defined at multiple levels. Scopes act as a boundary in which you can define the groups and Organization 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 Userscope.
- 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 userscope.

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.N-o	Userscope				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		OU2	Group3		User2	No
4.	Group3	OU3		OU1	OU3	Group3	Password Policy3	User3	Yes
5.	Group2	OU2			OU1	Group2		User2	No
6.	Group1	OU1		OU4	OU4	Group1	Password Policy4	User1	No
7.	Group2	OU2		OU5	OU5	Group2		User2	No
8.	Group3	OU3	Group1			Group3	Password Policy5	User3	No
9.	Group3	OU3	Group2		OU3			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 box, 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 for AD LDS 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 AD LDS 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 211.

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 for AD LDS 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 181.
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 15: 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 181.
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 16: 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 181.
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 181.
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 17: 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 ,
Special characters	Specify whether passwords must contain special characters: To set the minimum number of special characters 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 special characters must appear. For example, 1,3,5-10 . To specify how many special characters must be at the end of a password, use Number of ending characters , Special characters include the following characters: - !"#%&'()*+,-./:;<=>?@[\\]^_`{ }~

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 181.
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 18: Disallowed character rule

Option	Description
Digits (0-9)	Specify whether the rule will reject passwords containing digits. 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. Select the Number of ending characters check box, and then specify how many digits there must not be in the end of a password.
Special characters	Specify whether the rule will reject passwords containing special characters. 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. 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 “eeee1e” will be rejected.

To configure the sequence rule

1. Follow the steps outlined in [Configuring Password Policy Rules](#) on page 181.
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 19: 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 for AD LDS 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 181.
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 20: 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"</p>

Option	Description
	<p>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 <p>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.</p>
The entire value of a user property	<p>Select to reject passwords containing the entire value of a user property.</p> <p>You can select any of the user account properties listed in the description of the Initial characters of a user property value option above.</p>
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 181.
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 21: 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 181.
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

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 for AD LDS 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 for AD LDS
- 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 for AD LDS. 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 for AD LDS.

To use Password Manager for AD LDS 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 for AD LDS, ensure that the following requirements are met:

- A SQL Server is deployed in your environment and the Password Manager for AD LDS 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 Reports

You can create and view reports interactively using the Administration site, and save them to multiple file formats.

To use the reporting functionality, you have to specify the SQL Server to store the Password Manager database and connect to the Report Server that is capable of building reports using the data stored in the Password Manager for AD LDS database.

When specifying the SQL Server and the database to store the log data, ensure that the account under which Password Manager for AD LDS will access the server has the appropriate permissions to create and write to a database on the server.

When connecting to a report server for the first time, Password Manager for AD LDS publishes the reports included with the solution to the server, and populates the list of reports on the Administration site. Before connecting to a report server, ensure that the account under which Password Manager for AD LDS will access the server has the appropriate permissions to publish the Password Manager for AD LDS reports. The administrative rights on the report server will be sufficient for this account to publish reports.

To configure Password Manager for AD LDS reports

1. On the home page of the Password Manager for AD LDS Administration site, click **Reporting**.

2. On the **Statistics** page, click the **Reports** link under the **Reporting and User Action History** title.
3. On the **Reports** page, click **Configure SQL Server and Report Server**.
4. In the **SQL Server Connection Settings** dialog box, specify the following settings and click **Next**.

Table 22: SQL server connection settings

Setting	Description
SQL Server	Type the name of the SQL Server to be used for storing the Password Manager for AD LDS database.
Database name	Specify the name for the database where Password Manager for AD LDS will log information used for building reports. If the database you specified does not yet exist, you will be prompted to confirm creation of the database. When prompted, select the account for creating the database. This account must have the permission to create a database.
Select account for connecting to the SQL Server	To have Password Manager for AD LDS access the SQL Server under the Password Manager Service account, select Password Manager Service account . Otherwise, select Specific SQL Server account , and then enter user name and password of the user account you want Password Manager for AD LDS to use when accessing the SQL Server. NOTE: The account you select must have the permissions to write to the database.

5. In the **Report Server Connection Settings** dialog box, specify the following settings and click **OK**:

Table 23: Report server connection settings

Setting	Description
Report Server URL	Type in the URL address of the Report Server in the following format: <code>http://<server_name>/<report_server></code> , where <server_name> is the name of the server where Report Server resides, <report_server> is the name of the report server instance.
Report Manager URL	Type in the URL address of the Report Manager in the following format: <code>http://<server_name>/<report_server></code> , where <server_name> is the name of the server where Report Server resides, <report_server> is the name of the Report Manager instance. This is an optional setting.
Specify the account for	Enter user name and password of the user account you want Password Manager for AD LDS to use when accessing the Report Server.

Setting	Description
deploying SSRS reports	This account must have the permissions to deploy reports.
Specify the account that the Report Server will use to connect to the data source	<p>Enter user name and password of the user account you want the Report Server to use when accessing the data source. You can use either Windows credentials or SQL Server credentials. If you choose Windows credentials, select the Use as Windows credentials when connecting to the data source check box as well.</p> <p>The account you select must have the permissions to read data from the database.</p>

To create and preview a report

1. On the home page of the Administration site, click **Reporting**, and under **Reporting and User Action History**, click **Reports**.
2. On the Reports page, click the report you want to view. The following table lists the reports included with Password Manager for AD LDS:

Table 24: Reports and user action history

Report name	Description
User status (table)	<p>This is a table report displaying a list of users in the managed application directory partitions, and the states of the users' Q&A profiles in Password Manager for AD LDS.</p> <p>You can see which users have registered with Password Manager for AD LDS and which have not, who of the users must re-create their profiles, and which users are scheduled to update their profiles.</p>
User status (pie chart)	This is a pie chart showing the percentage of the total number of users for each of the Q&A profiles states.
Actions by user (table)	This is a table report showing what actions each of the users performed in Password Manager for AD LDS, and whether the result of a user action was successful or not. You can view this report for a specified period of time.
Actions by user (pie chart)	This is a pie chart displaying the percentage of the total number of user actions for all types of user actions such as registration with Password Manager for AD LDS or password reset. You can view this report for a specified period of time.
Registrations by month (bar chart)	This is a bar chart showing the monthly numbers of users registered with Password Manager for AD LDS. You can view this report for a specified month range.

Report name	Description
Actions by month (bar chart)	This is a barchart showing the monthly numbers of user actions performed in Password Manager for AD LDS. You can view this report for a specified month range.
Actions by type (table)	This is a table report showing a summary of user actions in Password Manager for AD LDS sorted by action type. You can view this report for a specified period of time.
Help desk usage by actions (table)	This is a table report showing a summary of actions on the Helpdesk site. You can view this report for a specified period of time.
Help desk usage by operators (table)	This is a table report showing what actions each of the helpdesk operators performed in Password Manager for AD LDS, and whether the result of an operator action was successful or not. You can view this report for a specified period of time.
Help desk usage by users (table)	This table report shows what actions each helpdesk operator has performed for specific users. You can view this report for a specified period of time.
Email notifications by user (table)	This table report lists the email notifications sent to specific users. You can view this report for a specified period of time.
Email notifications by type (table)	This is a table report showing a summary of email notifications sent to users. The notifications are sorted by action type. You can view this report for a specified period of time.

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.

- Once the report is generated, it is displayed in the Report Viewer, in a new browser window.
- Select the zoom ratio in the drop-down list on the toolbar.
- To go to a particular page, type in a page number in the leftmost text box on the toolbar and press **Enter**, or use the navigation arrows beside this text box.
- To modify report parameters, set the new parameter values by using the group of controls in the upper area of the Report Viewer, and then click the **View Report** button.
- To close the Report Viewer and return to the **List of Reports** page, close the Report Viewer window.

When previewing a report, you can easily locate specific records, or find certain values within the report. The Report Viewer finds each occurrence of the item you are looking for.

To search a report

1. Enter the text you are looking for in the **Find Text** text box on the menu bar.
2. Click **Find**.
3. Click **Next** to find the next occurrence.

In the Report Viewer, you can also save the report in a file, or print the report.

To save a report, select the target file format from the **Select a format** drop-down list on the menu bar, and 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)

To print a report, click the printer icon on the menu bar, and in the **Print** window, click **OK**.

User Action History

User action history is a history of all actions performed by all users registered with Password Manager for AD LDS. This functionality is provided by the Enterprise Auditing Service. This service is installed during Password Manager for AD LDS installation and does not require any configuration.

To view user action history, you need to add a connection to an SQL server.

To connect to an SQL server

1. On the home page of the Password Manager for AD LDS Administration site, click **Reporting**.
2. On the **Statistics** page, click the **History** link under the **Reporting and User Action History** title.
3. On the **History** page, click **Connect to SQL Server**.
4. In the **SQL Server Connection Settings** dialog box, specify the following settings and click **OK**.

Table 25: SQL server connection settings

Setting	Description
SQL Server	Type the name of the SQL Server to be used for storing the Password Manager database.

Setting	Description
Database name	<p>Specify the name for the database where Password Manager for AD LDS will log information used for building reports.</p> <p>If the database you specified does not yet exist, you will be prompted to confirm creation of the database.</p> <p>When prompted, select the account for creating the database. This account must have the permission to create a database.</p>
Select account for connecting to the SQL Server	<p>To have Password Manager access the SQL Server under the Password Manager Service account, select Password Manager Service account. Otherwise, select Specific SQL Server account, then enter user name and password of the user account you want Password Manager for AD LDS to use when accessing the SQL Server.</p> <p>Note that the account you select must have the permissions to write to the database.</p>

After you connect to SQL Server, you can perform full-text search for various user actions by user names, emails, activity names, etc.

On the History page of the Administration site, enter a value you want to search for and click **Search**. You can sort the search results by relevance or date. To search for actions performed by an Example User, enter **Example User**.

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 for AD LDS 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 for AD LDS, etc.

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 for AD LDS 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 box 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 box 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 box.
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 box.
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 please 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 26: 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 for AD LDS and its components.	See Installing Password Manager for AD LDS for AD LDS on page 10.
Ensure that the DefaultAppPool , PMAdminADLDS , PMUserADLDS , PMHelpdeskADLDS , and ReportServer application pools are running in the IIS Manager on the Password Manager for AD LDS 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 for AD LDS 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 for AD LDS Administration site.	

The interactive Web-based reports are built using the data that the report server retrieves from the Password Manager for AD LDS SQL database.

For more information on Reporting Services setup and configuration, refer to SQL Server documentation.

Reporting Services Firewall Issues

If Password Manager for AD LDS fails to operate properly when Reporting Services are separated from Password Manager for AD LDS by a firewall, specific ports should be open in the firewall.

To get the complete list of Password Manager for AD LDS 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 206.

Accounts Used in Password Manager for AD LDS

The following accounts can be used in Password Manager for AD LDS:

- Password Manager for AD LDS Service account
- Application pool identity
- Access account for AD LDS
- Password policy account
- Account for One Identity Quick Connect

The Password Manager for AD LDS Service Account

Password Manager Service account is used to install Password Manager for AD LDS. For Password Manager for AD LDS to run successfully, the Password Manager for AD LDS Service account must be a member of the Administrators group on the Web server where Password Manager for AD LDS 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 for AD LDS setup will be used to run Password Manager for AD LDS 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 for AD LDS installation folder>\App_Data folder.
- Application pool identity account must have 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 for AD LDS will access the AD LDS instance and a specified application directory partition. You can use the Password Manager for AD LDS 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 for AD LDS 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.

Account for Using One Identity Quick Connect

You can configure cross-platform password synchronization using One Identity Quick Connect. If used in conjunction with Quick Connect Sync Engine, Password Manager for AD LDS allows you to enable users and helpdesk operators to manage their passwords across a wide variety of connected systems.

To enable Password Manager for AD LDS to set passwords in connected systems, the account used to access Quick Connect must be a member of the local administrators group on the Quick Connect server.

For more information on using Quick Connect with Password Manager for AD LDS, see [Reset Password in AD LDS and Connected Systems](#) on page 96.

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 for AD LDS 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

Legacy Self-Service site and Password Manager for AD LDS Self-Service site

The Password Manager for AD LDS Self-Service site has all functionality similar to the Legacy Self-Service site with a new and improved user interface. The Password Manager for AD LDS Self-Service site can co-exist along with the already existing Legacy Self-Service site and it is possible to revert at any time to the Legacy Self-Service site.

Helpdesk Sites

- 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

SQL Server

Port **1433** (SQL Server) TCP/UDP Outbound
Port **1434** (SQL Server Browser Service) TCP/UDP Outbound

Report Server

Port **80** (SQL Server Report Services) TCP Outbound

Email Notification

Port **25** (Default SMTP port) TCP Outbound

One Identity Quick Connect Sync Engine

Port **808** 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, etc.

The following customization options are available in Password Manager for AD LDS:

- [Customization of Steps in Legacy Self-Service site, Password Manager for AD LDS 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 Legacy Self-Service site, Password Manager for AD LDS Self-Service site, and Helpdesk Tasks

The Password Manager Self-Service site has all functionality similar to the Legacy Self-Service site with a new and improved user interface. The Password Manager Self-Service site can co-exist along with the already existing Self-Service site and it is possible to revert at any time to the Legacy Self-Service site.

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 72.

For more information on modifying self-service workflows and activities, see [Legacy Self-Service or Password Manager for AD LDS Self-Service site workflows](#)

For more information on modifying helpdesk workflows and activities, see [Helpdesk Workflows](#) on page 105.

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 for AD LDS 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 102.

User Agreement Customization

In any self-service task Password Manager for AD LDS allows you to include a page with a 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 101.

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 126.

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 147.

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 181.

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](#).

Feature imparities between the legacy and the new Self-Service Sites

Password Manager for AD LDS does not provide feature parity between the legacy Self-Service Site (PMUser) and new Self-Service Site (PMSelfService) for self-service related activities. All new feature developments are only done for the new Self-Service Site (PMSelfService) site.

The following new features are affected:

- Password Manager for AD LDS Secure Token Server: The Authenticate with external provider action cannot be used on the legacy Self-Service Site (PMUser).

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Glossary

A

Account

A record that consists of all the information that defines a user to Active Directory or AD LDS. This includes the user name and password required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the computer and network and accessing their resources.

Administration site

A website for Password Manager for AD LDS administrators. On this website, they can configure Management Policies by adding managed application directory partitions, creating question lists, specify Q&A policy, etc.

Application directory partition alias

Enter the name that will be used to address the application directory partition on the Self-Service and Helpdesk sites.

Application log

The log that lists all actions performed by Password Manager for AD LDS.

Attribute

A piece of data that stores information that is specific to an object. A set of attributes stores the data that defines an object.

C

Certificate

A certificate is used to encrypt traffic and provide authentication between Password Manager for AD LDS Service and web sites installed on different servers. [View more.](#)

Configuration storage account

An account used by Password Manager for AD LDS for storing its configuration data, that is, settings configured in Password Manager for AD LDS, for example, Management Policies, general settings, and so on. The configuration storage account is automatically created in the Users container of a managed application directory partition when the managed partition is added. The configuration storage account is named QPMStorageContainer.

Custom activity

Custom activity is an activity with PowerShell handlers. Create custom activities from scratch or convert built-in activities to custom. [View more.](#)

Custom password policy rule

This rule does not check the password compliance with the configured password policy. Configure the rule to display your custom message instead of or together with other policy messages.

D

Do not show personally identifiable information (PII) for the logged in user

When selected, the Self-Service Site truncates personally identifiable information (PII) on the user interface. Select this option if the security policies of your organization require hiding PII.

E

Encryption algorithm

This algorithm is used to encrypt users' answers to secret questions. Users' answers will be encrypted if the **Store answers using reversible encryption** option is selected in the Q&A profile settings. Otherwise, the answers will be hashed.

F

Find

Provide regular expression based on the selected Active Directory attribute to find a matching pattern in the target system.

G

Group Policy

An administrator's tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization.

H

Hashing algorithm

This algorithm is used to hash users' answers to secret questions if reversible encryption is not used to store the answers.

Helpdesk site

A website for helpdesk operators. On this website, they can reset users' passwords, unlock accounts, assign temporary passcodes, and so on.

I

In-place upgrade

The installation of the latest version of Password Manager for AD LDS without removing the older version.

L

Locked Questions and Answers Profile

A Questions and Answers Profile that temporarily cannot be used.

A Questions and Answers Profile can become locked after a number of unsuccessful attempts to answer the questions.

M

Mailbox

The delivery location for all incoming mail messages addressed to a designated owner. Information in a user's mailbox is stored in the private information store on a Microsoft® Exchange server computer. A mailbox can contain received messages, message attachments, folders, folder hierarchy, and more. Server applications for Microsoft® Exchange server are often designed with a mailbox for communication.

Mandatory question

A question, the same for all users in an application directory partition, that users must answer in order to authenticate themselves using Password Manager for AD LDS.

Management Policy

Management Policy allows you to configure workflows and secret questions for specified groups of users, and select helpdesk operators to manage these users. See [Management Policy components](#).

O

Optional question

A question that users should select from a list of pre-defined questions and answer to authenticate themselves using Password Manager for AD LDS.

P

Password Manager for AD LDS realm

Realm is a set of Password Manager for AD LDS Service instances sharing realm settings and configuration. You can use the realm to provide enhanced availability and load balancing.

Password Manager for AD LDS Service Account

An account used to install Password Manager for AD LDS. The Password Manager for AD LDS Service account must be a member of the Administrators group on the Web Server where Password Manager for AD LDS is installed.

Password Policy Manager

A component of Password Manager for AD LDS that enforces password policies configured in Password Manager for AD LDS, when users change their passwords using tools other than Password Manager for AD LDS.

Q

Questions and Answers Profile (Q&A Profile)

A set of questions selected by a user from the Question list and user's answers to them. A Questions and Answers Profile is used to authenticate a person using Password Manager for AD LDS.

Question list

A set of questions used in creating users' Questions and Answers profiles. The list is defined by the administrator and contains a series of questions in a certain language that users from a specific application directory partition must answer in order to create or update their personal Questions and Answers profiles. A question list defines the number of questions of each type and the wording of mandatory and optional questions.

R

Replace

Provide a value to replace the matched pattern in the target system.

S

Self-Service site

A website for Password Manager for AD LDS end-users. On this site, end-users can create their Questions and Answers Profiles and manage their passwords.

Special character

A character that is neither alphabetic nor numeric.

T

Test attribute value

Provide a sample Active Directory attribute value, to evaluate the matching pattern.

U

User-defined question

A question that users must provide along with the answer in order to authenticate themselves using Password Manager for AD LDS.

W

Workflow availability (helpdesk)

If a user is not registered, then only Reset Password, Unlock Account, and Assign Passcode workflows are enabled. For more information, see [Workflow settings](#).

Workflow availability (self-service)

If a user is not registered, only My Questions and Answers Profile and I Have a Passcode workflows are enabled. For more information, see [Workflow settings](#).