One Identity Password Manager 5.11.0

Administration Guide

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 Administration Guide
Updated - October 2022
Version - 5.11.0

Contents

About Password Manager

Password Manager overview

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

Password Manager allows managing users that do not have accounts in the Active Directory. For example, using Password Manager 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 to change user passwords across multiple connected data sources.

The key features and benefits of Password Manager include:

- **Global access**. Password Manager 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 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 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 is capable of managing domains across trust boundaries (no trust relationship required).
- **Powerful password policies**. Password Manager 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.
- **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 is designed to work with network load balancing clusters and in a Web farm environment.

Getting started

Different sites for Different roles

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

- **Administration site** is for individuals who are responsible for implementing password self-management through performing administrative tasks, such as configuring site-specific settings and enforcing password policies, to suit the specific needs of their organization.
- **Helpdesk site** handles typical tasks performed by Helpdesk operators, such as resetting passwords, unlocking user accounts, assigning temporary passcodes, and managing users' Questions and Answers profiles.
- **Self-Service site** 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 Self-Service Site** In Password Manager version 5.11.0, you have the option to access the Password Manager Self-Service site. The Password Manager self-service site provides functionality similar to the legacy Self-Service site. The Password Manager Self-Service site includes enhancements to the user interface to improve the usability of the site. The

Password Manager Self-Service site and the legacy Self-Service site can co-exist and it is possible to revert to the legacy Self-Service site.

Password Manager components

Password Manager includes the following components:

Table 1: Password Manager Components

Component	Description	Importance
Password Manager x64	The suite of role-based sites that expose the functionality of Password Manager to end users. NOTE: It is recommended not to install Password Manager on the machine where Domain Controller (DC) server is installed.	Required
Password Policy Manager x64	Password Policy Manager is designed to enforce domain password policies set with Password Manager. If you choose to install this component, you must install it on all domain controllers running a 64-bit Microsoft Windows Server operating system.	Optional
Secure Password Extension x86	Secure Password Extension x86 facilitates access to the Self-Service site from the Windows login screen and displays registration notifications. Secure Password Extension x86 is intended to be deployed on computers running 32-bit versions of Microsoft Windows operating systems.	Optional

Component	Description	Importance
Secure Password Extension x64	The Secure Password Extension facilitates access to the Self-Service site from the Windows login screen and displays registration notifications. Secure Password Extension x64 is intended to be deployed on computers running a 64-bit operating system.	Optional
Offline Password Reset x86	Offline Password Reset enables users to use the offline password reset functionality provided by Password Manager. This functionality allows resetting passwords when users have forgotten their current passwords and their computers are not connected to the intranet (Active Directory is not available). Offline Password Reset x86 is intended to be deployed on computers running a 32-bit operating system.	Optional
Offline Password Reset x64	Offline Password Reset enables users to use the offline password reset functionality provided by Password Manager. This functionality allows resetting passwords when users have forgotten their current passwords and their computers are not connected to the intranet (Active Directory is not available). Offline Password Reset x64 is intended to be deployed on computers running a 64-bit operating system.	Optional

Component	Description	Importance
Migration Wizard (part of Password Manager 5.11.0)	Migration wizard allows users to update profile whenever the administrator reinitializes the Password Manager instance	Optional

Licensing

The Password Manager license specifies the maximum number of user accounts in the Password Manager across all domains. The Admin can identify whether the installation is legally compliant or not by 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 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 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.
- The number of Password Manager instances in a large enterprise. Password Manager 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:

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.

Note that such scopes are available only if your license includes managed persons and managed external persons.

To add a domain 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 **Add domain connection**.

4. If domain connections already exist, select a domain connection from the list. If you want to create a new connection, click **Add domain connection**.
5. If you selected to create the new domain connection, in the **Add New Domain Connection** dialog, configure access to the domain by doing the following:
    - In the **Domain name** text box, type the name of the domain that you want to register with Password Manager.
    - In the **Domain alias** text box, type the alias for the domain that will be used to address the domain on the Self-Service site.
    - To have Password Manager access the managed domain using the Password Manager Service account, select **Password Manager Service account**. Otherwise, select **Domain management account**, and then enter user name and password for the domain management account. Note that if Password Manager Service account is used to access the domain, it should have the same permissions as the domain management account.

    For information on how to prepare a domain management account, see Configuring Permissions for Domain Management Account on page 23.
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 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 persons**.
    - To specify the OUs, click **Add** under **Organizational units excluded from the scope of managed persons**.

5. Click **Save**.

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

To add a domain 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 **Add domain connection**.
4. If domain connections already exist, select a domain connection from the list. If you want to create a new connection, click **Add domain connection**.
5. If you selected to create the new domain connection, in the **Add New Domain Connection** dialog, configure access to the domain by doing the following:
    - In the **Domain name** text box, type the name of the domain that you want to register with Password Manager.
    - In the **Domain alias** text box, type the alias for the domain that will be used to address the domain on the Self-Service site.
    - To have Password Manager access the managed domain using the Password Manager Service account, select **Password Manager Service account**. Otherwise, select **Domain management account**, and then enter user name and password for the domain management account.

    Note that if Password Manager Service account is used to access the domain, it should have the same permissions as the domain management account.

    For information on how to prepare a domain management account, see Configuring Permissions for Domain Management Account on page 23.
6. Click **Save**.

To specify groups or OUs included in the scope of managed external 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 included into the scope of managed external persons**.
    - To specify the OUs, click **Add** under **Organizational units included into the scope of managed external persons**.
5. Click **Save**.

To specify groups or OUs excluded from the scope of managed external 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 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 on page 71.

You can install this license during Password Manager installation or provide the license file later on the Administration site. To install the license after Password Manager 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 such as Q&A, are not affected by expiry/non-compliance of this Telephone Verification license.

Installing Password Manager: Checklist

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

1. Before you install Password Manager, you should configure Password Manager Service account and application pool identity. For more information, see *Configuring Password Manager Service Accountand Application Pool Identity*.
2. It is strongly recommended that you enable HTTPS on the server where Password Manager is installed. For more information, see *Enabling HTTPS*.
3. Install an instance of Password Manager. See *Installing Password Manager*.

Installing Password Manager

This section describes how to install Password Manager. You will learn how to configure Password Manager Service account and application pool identity. A separate section will guide you through the steps required to install Password Manager.

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

Configuring Password Manager service account and application pool identity

When installing Password Manager, you are prompted to specify two accounts: Password Manager Service account and application pool identity. Password Manager Service account is an account under which Password Manager Service runs. You can also use Password Manager Service account as a domain management account (the account that is necessary to add managed domains when configuring the user and Helpdesk scopes). To do this, ensure that Password Manager Service account has the minimum permissions required to successfully perform password management tasks in the domain. For more information, see Configuring Permissions for Domain Management Account on page 23.

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

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

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

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

Enabling HTTPS

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

For instructions on how to configure SSL in order to support HTTPS connections from client applications, see the article "Configuring Secure Sockets Layer in IIS 7" at http://technet.microsoft.com/en-us/library/cc771438%28WS.10%29.aspx.

NOTE: To enable the Password Manager 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, 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 an overview of various installation scenarios, see Typical deployment scenarios on page 46.

To install Password Manager

1. Depending on the hardware, run **Password Manager x86** or **Password Manager x64** from the installation CD autorun window.
2. Read the license agreement, select **I accept the terms in the license agreement**, and then click **Next**.

3. On the **User Information** page, specify the following options, and then click **Next**:
    a. Full name- Type your name
    b. Organization- Type 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 components to install, and then click **Next**:
    a. Full Installation- Select this option to install Password Manager 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 Self-Service site.
    d. Helpdesk Site- Select this option to install only the Helpdesk site.

    You can install all Password Manager components together on a single server or you can deploy the Legacy Self-Service, Password Manager Self-Service, and Helpdesk sites on a standalone server. To learn more about installing the Self-Service and Helpdesk sites on a standalone server, see Installing Legacy Self-Service, Password Manager Self-Service, and Helpdesk Sites on a Standalone Server on page 15.

IMPORTANT: Note, that by default Secure Password Extension uses the Self-Service site that is installed on the same server with the Password Manager Service. If you want Secure Password Extension to use another Self-Service site, see Locating Self-Service site on page 60 for more information.

5. On the **Password Manager Service Account Information** page, specify the name and password for the Password Manager Service account, and then click **Next**. Use the following user name format: `DOMAIN\Username`. For more information on the requirements for the Password Manager Service account, see Configuring Password Manager service account and application pool identity on page 11.
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 service account and application pool identity on page 11.
7. Click **Install**.

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

IMPORTANT: By default, Password Manager uses built-in certificates to encrypt traffic between Password Manager websites and Password Manager Service. After installing Password Manager, if the Web sites (Self-Service and Helpdesk) and the Password Manager 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 Service and Websites on page 19.

Initializing instance

After installing Password Manager 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 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 instances sharing the same configuration are referred to as a Password Manager realm. For more information about Password Manager realms, see Installing multiple instances of Password Manager on page 18.

To initialize Password Manager instance

1. 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 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 versions 5.8.x or later, users must be a part of the local PMAdmin group and either of IIS_IUSRS or Administrators group to access the PMAdmin 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 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.
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 Service. If you decide to install the Legacy Self-Service, Password Manager Self-Service, and Helpdesk sites separately from

the Password Manager 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 Service and Websites on page 19.

- **Port number**- Specify the port that the Self-Service and Helpdesk sites will use to connect to the Password Manager 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 uses Triple DES algorithm to encrypt data. Note that 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 uses SHA-256 hashing algorithm. Password Manager 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 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.
6. Click **Save** to complete instance initialization.

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

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

When deploying Password Manager in a perimeter network, it is recommended to install the Password Manager Service and the sites in a corporate network at first (that is, use the Full Installation option in the Password Manager setup), and then install only the legacy Self-Service or the Password Manager 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 Self-Service, and Helpdesk sites on a standalone server

1. Depending on the hardware, run **Password Manager x64** from the installation CD autorun window.
2. Read the license agreement, select **I accept the terms in the license agreement**, and then click **Next**.
3. On the **User Information** page, specify the following options, and then click **Next**:
   a. Full name- Type your name
   b. Organization- Type 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, and 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, and then click **Next**. For more information on the requirements for the application pool identity, see Configuring Password Manager service account and application pool identity on page 11.
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.

1. In the **Computer name or IP address** text box, specify the Password Manager Service host name or IP address.
2. In the **Port number** text box, specify the port number that the Self-Service site will use to connect to the Password Manager Service.

3. From the **Certificate name** drop-down list, select the name of the certificate to be used by this site. By default, Password Manager uses a built-in certificate issued by Password Manager. 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 Service and Websites on page 19.

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

4. 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 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 Service and Websites on page 19.

   IMPORTANT: 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

FailSafe support in Password Manager

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

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

After the initialization of Helpdesk and Self-Service site, **WcfServiceRealms.xml** file is created. This file has records of all the instances of Password Manager Services installed. The user can use one of the realm instances listed in **WcfServiceRealms.xml** file, in case of unavailability of services in the primary instance of Password Manager Service.

For example, helpdesk site is connected to **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 components are installed on the same server, the FailSafe operation might not work as expected.

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

Installing multiple instances of Password Manager

Several Password Manager instances sharing common configuration are referred to as a realm. A realm is a group of Password Manager 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 realms provide for enhanced availability and fault tolerance.

IMPORTANT: 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.

To create a Password Manager 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 instance by running **Password Manager x86** or **Password Manager x64** from the installation CD autorun window. For more information on the installation procedure, see Installing Password Manager on page 12.
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 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 Service and Websites

When the Password Manager 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 uses built-in certificates issued by Password Manager. However, you may want to install and use custom certificates issued by a trusted Windows-based certification authority.

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

Complete the following steps:

1. Obtain and install custom certificates from a trusted Windows-based certification authority.
2. Providing certificate issued for a server computer to the Password Manager Service.
3. Providing certificate issued for client computers to the 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 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 Internet Explorer.

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 Internet Explorer.

To request a certificate using Windows 2012 Certificate Services Web Interface

1. Use Internet Explorer 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** text box, enter the name of the server for which you are requesting a certificate.
6. In **Type of Certificate Needed**, select **Server Authentication Certificate**.
7. In **Key Options**, select **Create new key set**, and specify the following options:
    - In **CSP** (Cryptographic service provider), select **Microsoft Enhanced RSA and AES Cryptographic Provider**.
    - In **Key Usage**, click **Both**.
    - In **Key Size**, set **1024** or more.

- Select **Automatic key container name**.
- Select the **Mark keys as exportable** check box.
- Clear the **Enable strong private key protection** check box.

8. In **Additional Options**, specify the following:
   - In **Request Format**, select **CMC**.
   - In **Hash Algorithm**, select **sha256**.
   - Do not select the **Save request** check box.
   - Specify attributes if necessary and a friendly name for your request.
9. Click **Submit**.
10. If you see the **Certificate Issued** web page, click **Install this certificate**. If your request needs to be approved by your administrator first, wait for the approval and then go to the https://*servername*/certsrv, 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 Service

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

To provide the certificate to the Password Manager Service

1. 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 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 Service.

To provide the certificate to the Legacy Self-Service Site and the Password Manager 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 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**.

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 user scope

To configure the user scope, add one or more domain connections. Domain connections created for the user scope can also be used in the Helpdesk scope and password policies. The same domain connection can be used in different management policies. Wherever you create a domain connection, you can use it elsewhere, that is, a domain connection configured for password policies can be used in the Helpdesk scope.

To manage all domain connections from a single place, click **General Settings | Domain Connections** on the Administration site. For more information, view Domain Connections on page 178.

Configuring Permissions for Domain Management Account

When you add a domain connection, you can create a new one or use existing connections, if any. When creating the domain connection, you must specify a domain management account — an account under which Password Manager will access the domain.

For the domain connection that you want to use in the user and Helpdesk scopes, make sure the domain management account has the following minimum set of permissions:

- Membership in the Domain Users group
- The Read permission for all attributes of user objects
- The Write permission for the following attributes of user objects: *pwdLastSet*, *comment*, *userAccountControl,* and *lockoutTime*

  NOTE: If the **Storage attribute** for **Security questions** under the **Reinitialization** page is a custom value (such as **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 domain objects
- The Write permission for the *gpLink* attribute of the *organizationalUnit* objects and domain 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 domain 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 Read permission for the *nTSecurityDecriptor* attribute of the *groupPolicyContainer* objects.
- 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.
- The Write permission for the following attributes of the *msDS-PasswordSettings* object:
    - msDS-LockoutDuration
    - msDS-LockoutThreshold
    - msDS-MaximumPasswordAge
    - msDS-MinimumPasswordAge
    - msDS-MinimumPasswordLength
    - msDS-PasswordComplexityEnabled
    - msDS-PasswordHistoryLength
    - msDS-PasswordReversibleEncryption
    - msDS-PasswordSettingsPrecedence
    - msDS-PSOApplied
    - msDS-PSOAppliesTo
    - name

Corporate Authentication

In the Register workflow, if the Admin selects **Corporate authentication** check box, user will only be able to review the corporate account details while registration. If **Allow user to edit corporate details** check box is selected, user will be able to update the respective corporate details such as **Corporate email** and **Corporate phone number**, provided that the details are not previously populated by 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(say, **pager**) then, the Read/ Write Permissions need to be provided for that attribute instead of the **mobile** attribute.

Adding Domain Connection

After adding a domain connection to the user scope, you need to specify groups from the domain that will be able to access the Self-Service site. By default, the group Domain Users is included in the scope when you add the domain connection to the user scope. You can also restrict some domain groups from accessing the Self-Service site.

NOTE: When you add a domain to the user scope, the group Domain Users from this domain is automatically included in the user scope.

To add a domain connection

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>/PMAdmin, 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 **Add domain connection**.
4. If domain connections already exist, select a domain connection from the list. If you want to create a new connection, click **Add domain connection**.
5. If you selected to create the new domain connection, in the **Add New Domain Connection** dialog, configure access to the domain by doing the following:
    - In the **Domain name** text box, type the name of the domain that you want to register with Password Manager.
    - In the **Domain alias** text box, type the alias for the domain that will be used to address the domain on the Self-Service site.
    - To have Password Manager access the managed domain using the Password Manager Service account, select **Password Manager Service account**. Otherwise, select **Domain management account**, and then enter user name and password for the domain management account. Note that if Password Manager Service account is used to access the domain, it should have the same permissions as the domain management account.

    For information on how to prepare a domain management account, see Configuring Permissions for Domain Management Account on page 23.
6. Click **Save**.

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 domain 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, provide the **Security** permissions to all the groups, OUs that are added as **Included groups**, and **Included OUs** in the userscope. To provide **Security** permissions to a user/ group/ OU, go to the domain object properties -> security tab -> Add the configured **Domain Management account** to the **Group or usernames** in the Active Directory.

If the users/ groups/ OUs included in the userscope, are the member of DomainAdmins/ Administrators group in the Active Directory, 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 domain 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**.

Enabling LDAP over SSL

Password Manager supports both LDAP and LDAPS for communicating with the Active Directory Server. This section explains how to enable LDAP over SSL.

NOTE: Configuration is required for all installations of Password Manager servers.

On a computer where Password Manager is installed, create the following value in the **HKLM/SOFTWARE/One Identity/Password Manager** registry key using the Registry Editor:

Value type: **REG_SZ**

Value name: **PasswordEncodeMethod**

Value data: **ADS_PASSWORD_ENCODE_REQUIRE_SSL**

Value type: **REG_DWORD**

Value name: **PasswordSetPortNumber**

Value data: **636**

NOTE: The default port for REG_DWORD is 636.

Specifying advanced settings for domain connection

After you have created a domain connection, you can specify advanced settings for the connection: domain controllers and Active Directory sites of the managed domain.

Domain Controller

Selecting the domain controller allows you to specify what domain controller Password Manager should use when connecting to the managed domain. By default, two options are available: **domain controller used by user computer** and **default domain controller**.

Domain controller used by user computer is a domain controller that a user computer connects to. It may not be the same as the domain controller used by the computer running the Password Manager Service. The information about this domain controller is passed to Password Manager in requests made by Secure Password Extension.

Default domain controller is a domain controller that is automatically identified as a preferred domain controller for the computer running the Password Manager Service.

You can also add any other domain controller from the specified domain by pressing the Add button under the domain controllers table on the **Advanced settings** tab of the **Edit Domain Connection** dialog.

You can select several domain controllers to ensure fault tolerance in your environment. By default, the first domain controller in the list will be used by Password Manager to connect to the domain. But if the first domain controller is not available, Password Manager will attempt to connect to the next domain controller in the list, and so on.

When Password Manager uses a domain controller other than the first one in the list of domain controllers, the Environment Health Checker scheduled task checks whether the first domain controller (with the highest priority) is available. When it becomes available, Password Manager switches back to using this domain controller. For more information, see Environment Health Checker Task on page 169.

To specify domain controllers

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 domain connection for which you want to specify domain controllers and click **Edit**.
3. On the **User Scope Settings for #Domain#** page, click **Edit**.

4. On the **Advanced settings** tab of the **Edit Domain Connection** dialog, click **Add** under the domain controllers table then select required domain controllers, and click **Add**.
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 domain connection is used.

Active Directory sites

By specifying Active Directory sites in the domain connection settings you select the site in which you want Password Manager to replicate changes as soon as they occur in other sites. This reduces downtime that users may experience when your environment has several Active Directory sites and changes do not get immediately replicated between the sites.

For example, when users unlock their accounts on the Self-Service site, this operation may occur in one site. But when they attempt to log in to their computers, this operation may occur in another site, to which the information about the unlocked account has not been replicated yet. In this case, users will not be able to log in until the information is replicated to the second site. To mitigate this issue, select the Active Directory sites in which you want to replicate changes immediately in the domain connection settings.

When specifying the site, you can select either the default writable domain controller (automatically selected in Active Directory) or select several writable domain controllers from this site. If you specify several domain controllers, changes will be propagated to the first available domain controller in the site.

Specifying Active Directory sites

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 domain connection for which you want to specify Active Directory sites and click **Edit**.
3. On the **User Scope Settings for #Domain#** page, click **Edit**.
4. On the **Advanced Options** tab of the **Edit Domain Connection** dialog, click **Add** under the Active Directory sites table, select required sites, and click **Add**.
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 domain connection is used.

Changes propagation

After you specify the Active Directory sites in which you want to push changes, you can also select what kind of changes to propagate. The following options are available:

- Propagate changes related to the user's account in Active Directory
- Propagate changes related to the user's Questions and Answers profile

- Propagate password-related changes

Propagating account-related changes

Select this option to propagate information about unlocking and enabling user accounts in Active Directory. It is recommended to use this option when a managed domain has users in multiple Active Directory sites.

Propagating Q&A profile-related changes

Select this option to propagate information about editing, locking and unlocking Questions and Answers profile, and passcodes issued by Helpdesk. It is recommended to use this option when users and Password Manager Service use domain controllers from different sites. In this case, if users update their Q&A profiles using Secure Password Extension (via the domain controller in one site), and then attempt to use the profiles on the Self-Service (via the domain controller in another site), they may encounter the issue when the updated Q&A profile is not yet available because of intersite replication latency.

Propagating password-related changes

Select this option to propagate information about changing or resetting user password. It is recommended to use this option in the following environment. You have several Active Directory sites in your environment; a user's computer and Password Manager Service are located in different sites. User authentication is performed via a read-only domain controller (RODC).

In this environment, users may experience downtime in the following scenario:

- A user changes password via a domain controller used by Password Manager Service in site A.
- The user attempts to authenticate to an RODC in site B, the RODC forwards the authentication request to a writable domain controller in the site, but the password has not be replicated yet to site B.
- User authentication is failed because of intersite replication latency.

To mitigate this issue, after selecting the corresponding Active Directory site (in which the RODC is located) and the writable domain controller from the site, select the **Propagate password-related changes** check box to immediately propagate password changes to the selected writable domain controller and enable user authentication via the RODC.

Changing domain management account

To access a managed domain, you can use either a domain management account or Password Manager Service account. For more information on how to configure a domain management account, see Configuring Permissions for Domain Management Account on page 23. Password Manager Service account is the account that was configured during Password Manager installation. Password Manager Service account may be used as a

domain management account only when the Service account has all the permissions required for the domain management account.

To modify account used to access a domain

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 domain connection for which you want to change access account and click **Edit**.
3. On the **User Scope Settings for #Domain#** page, click **Edit**.
4. In the **Access account** section of the **Edit Domain Connection** dialog, select **Password Manager Service account** to have Password Manager access the managed domain using the Password Manager Service account. Otherwise, select **Domain management account**, and then enter user name and password for the domain management account.
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 domain connection is used.

Removing a domain connection

To remove a domain connection

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 domain connection you want to delete and click **Remove**. Note that the domain connection will be removed from this user scope only. If you want to permanently remove the domain connection, remove it from everywhere where it is used, and then on the **General Settings|Domain Connections** tab, click **Remove** under the required connection.

User Logon Requirements

In the Active Directory, the **logonWorkstation** or **userWorkstations** attribute is available for the user accounts. The **Log On** option is under the **Account** tab in Active Directory Users and Computers (ADUC). By default, the value is set to **all** computers. However, if users want to limit access to the account for security reason, they can do so by listing the computers which the user account is used from, to authenticate in the **logonWorkstation** or **userWorkstations** attribute. The users are allowed to use only these computers for authentication.

Password Manager redirects the authentication to Active Directory. When the users in PMUsers enters their credentials, the Active Directory identifies this as an authentication from the PM server. When the **logonWorkstation** or **userWorkstations** attribute is used, and the computer is not listed in the attribute, the Active Directory restricts the login.

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 82.

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*>/PMAdmin/.
2. On the Administration site home page, click the **Add secret questions** 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 the order of questions by clicking the appropriate links.
7. Click **Save** to save the questions and close the dialog.

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 138.

Password Manager Architecture

Password Manager components and third-party applications

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

The following is a list of Password Manager components:

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

TeleSign

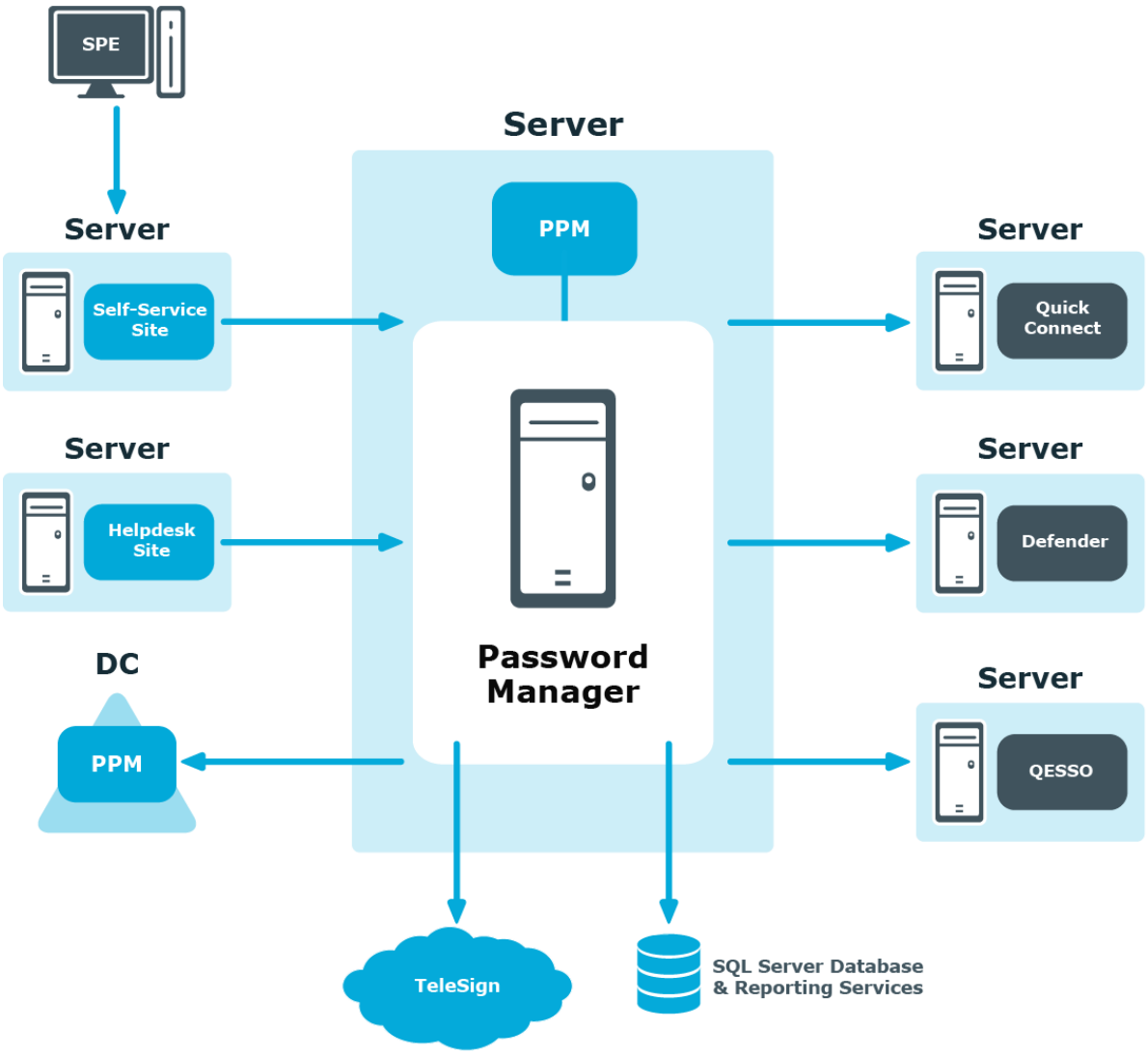
Quick Connect Sync Engine

Defender

Password Manager Secure Token Server

RADIUS Two-Factor Authentication

Quest Enterprise Single Sign-On (QESSO)



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

Password Manager Service and Administration site

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

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

When installing the Administration site and Password Manager 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 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 Self-Service site

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

Limitations & Restrictions of the Password Manager Self-Service site

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

Alternative option

As an alternative to using Password Manager 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 Service, or on a standalone server.

Password Policy Manager

Password Policy Manager is an independently deployed component of Password Manager. Password Policy Manager is necessary to enforce password policies configured in Password Manager in those cases where users change their passwords using means other than Password Manager. For example, when user change their password on the Self-Service site, a new password is checked against password policy rules immediately, and if it complies with password policies configured in Password Manager, the new password is accepted. But when user change their password by pressing CTRL+ALT+DELETE, for example, the password's compliance with password policies cannot be checked by Password Manager unless Password Policy Manager is deployed on all domain controllers in a managed domain. Password Policy Manager installs the dictionary file in the SYSVOL folder to set a dictionary rule for new passwords. If the dictionary file already exists in the SYSVOL folder, Password Policy Manager setup will not replace the file while installing.

If Password Policy Manager is not installed on all domain controllers in the domain, password policies configured in Password Manager will be ignored when users change password by means other than Password Manager.

NOTE: The user account that is used to install Password Policy Manager must have write access to the SYSVOL folder in domain controller.

NOTE: When the user uninstalls Password Policy Manager, the installer will not remove the dictionary file from the SYSVOL folder. The user must remove the dictionary file manually if the file is not needed.

CAUTION: Removing the dictionary file from the SYSVOL folder in one Domain Controller will result deletion of the dictionary file in all Domain Controllers .

For more information on Password Policy Manager, see About Password Policies on page 234.

Secure Password Extension

Secure Password Extension is an independently deployed component that provides one-click access to the complete functionality of the Self-Service site from the Windows login

screen. Secure Password Extension also provides dialog displayed on end-user computers that notify users who must create or update their Questions and Answers profiles with Password Manager.

Secure Password Extension should be installed on users' computers through group policy.

For more information, see Secure Password Extension overview on page 59.

Offline password reset

Offline Password Reset (OPR) is an independently deployed component that enables users to use the offline password reset functionality provided by Password Manager. This functionality allows resetting passwords when users have forgotten their current passwords and their computers are not connected to the intranet (Active Directory is not available).

Offline Password Reset should be installed on users' computers through group policy.

The password can be reset by two methods when the user is offline. Do one of the following to reset the password when the system is not connected to corporate network.

With mobile QRcode scanner:

1. Scan the QRcode from the welcome page and click **Next**.
2. Scanning the QRcode redirects to Password self-Service site on the mobile device.
3. On the Password Self-Service site, select the **Forgot My Password** option. This will give a response code to reset your password on the offline system.
4. Type the response code in the **Response code** text box.
5. Type the new password and confirm the new password in relevant text boxes.
6. Click **Next** to reset the password.

NOTE:

- If you don't have latest .NET Framework to display QRCode Image, click **Next** to reset your password using the challenge code.
- Use the latest **`prm_gina.admx`** file by removing the older flle from group policy.

If the user fails to reset the password three times on Password Reset wizard for any reason, **Offline Password Reset Wizard** generates a new QR code. The user must scan the new QR code and follow the steps again to reset the password.

NOTE:

- For the QR code to work, make sure that Password Manager Self-Service site URL exists in the registry.
- To update the registry entry of the Password Manager Self-Service site URL, navigate to **Generic Settings** folder in the Administrative templates node and enable **Specify URL path to the Password Self-Service site** setting.
- If Password Manager Self-Service site URL is not present in the registry, Password Manager Self-Service site will not appear on 32 char challenge code window of OPR.

Without mobile QRcode scanner:

1. Select the **Select the checkbox if you do not have the QRcode scanner and click Next.** checkbox, and click **Next**.
2. On a device connected to the internet, open the Password Self-Service site and access your account.
3. Select the **Forgot My Password** option.
4. Enter the challenge code that appeared on the **Password Reset** page of One Identity Secure Password Extension Wizard in the text box and click **Next**.
5. Type the response code in the **Response code** text box.
6. Type the new password and confirm the new password in relevant text boxes.
7. Click **Next** to reset the password.

For more information, see Reset Password in Active Directory on page 110.

Migration Wizard

Migration Wizard (part of Password Manager 5.11.0) users to update profile whenever the administrator reinitializes the Password Manager instance. For more information, see To update users' Q&A profiles with new instance settings and clear old Q&A data for user objects in Active Directory on page 176.

TeleSign

TeleSign is a service that provides phone-based authentication for Password Manager 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 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 on page 256.

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 Active Directory and Connected Systems on page 113.

Defender

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

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

For more information, see Authenticate with Defender on page 130.

Password Manager Secure Token Server

Password Manager Secure Token Server (STS) is installed with Password Manager version 5.10.0. You can configure STS to use internal or external providers with optional Multi-Factor Authentication (MFA).

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 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.

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 Manger STS account restrictions

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

Using STS features in a Password Manager realm

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

Using Certificate to protect STS configuration

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

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

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

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

NOTE: The specified certificate must be valid, trusted and it must exist in the Local Computer's certificate store. It must have a private key. Access to the private key must be

granted to the service account that is running the Password Manager Secure Token Server Windows Service. The private key must be an RSA key, of any length. A certificate with an ECC key is not supported.

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

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

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

If Password Manager STS settings are not replicated automatically

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

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

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

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

RADIUS Two-Factor Authentication

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

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

To configure RADIUS Two-Factor Authentication

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

   The **RADIUS Two-Factor Authentication** page is displayed.
2. Click **Add RADIUS server** to add a new RADIUS server for authentication.

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 on page 131.

Quest Enterprise Single Sign-On

Quest Enterprise Single Sign-on (QUESSO) is a One Identity product that provides users with the ability to access all applications on their desktop using a single user ID and password. After users have logged in, they can access password-protected applications on their desktop without the need to enter any further account details.

The account details for password-protected applications are encrypted by using the user login password. When the user resets or changes this password, the encrypted data is lost. To prevent data loss, Password Manager should be configured to notify QUESSO about password changes and QUESSO will re-encrypt the data using the new password.

For more information, see Quest Enterprise Single Sign-On (QESSO) on page 268.

Redistributable Secret Management Service

Redistributable Secret Management Service (rSMS) can be used to manage user passwords across multiple connected systems. Using the rSMS service it is possible to quickly

synchronize the passwords across connected systems. By default, the rSMS service is installed with the Password Manager software.

For more information on creating an rSMS account, see Working with Redistributable Secret Management account

For more information on resetting passwords in connected systems through embedded systems, see Reset password in connected systems through embedded connectors.

Alternative options

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

NOTE: Target platform IP address or the Hostname should not be same server where 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 Configuring Account Search Options.

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)
- 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**. Click **Remove** to delete the defined corporate IP address.

Password Manager permission checker

The Password Manager permission checker is a script used to check the user permissions and privileges. The basic permissions for a user includes the local system permissions and the Active Directory read, write, and delete permissions. Using the permission checker script, you can evaluate the local and Active Directory permissions for the domain account to check if sufficient permissions are available to the Password manager with all privileges.

IMPORTANT:

- Active Directory module for Windows PowerShell version 5.0 or later must be installed to run the tool. You can download relevant dependent script modules from the PowerShell Gallery, if not available before executing the permission checks.
- Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 operating systems are supported.

Configuring Password Manager permission checker

1. Login to the server by providing the domain account credentials where the Password Manager is to be installed.
2. From the installation folder, <Password Manager\Setup\Tools\Permission Checker>, copy the Permission Checker folder and paste it on to the server.
3. Update the Configuration.xml file with the required domain objects information that needs to be validated from the tool.

   The permissions associated with the user account is displayed. The PermissionChecker.log file available at the same location where the tool is placed and it contains the same permission report displayed in the script console.

IMPORTANT: If the data in the Configration.xml is not specified or incorrect, permission checks are ignored for those sections. After this, the Permission check Warning Summary Report is displayed that is part of the tool which specifies the reasons for the domain account which doesn't have sufficient privileges.

Working with Power BI templates

Microsoft Power BI is an analytics service that is used to visualize large data with business intelligence. You can generate multiple interactive reports and customize dashboards with

data insights and plot them on graphs to simplify data visualization.

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

The predefined Password Manager PowerBI template is available in `Password Manager\Setup\Template\PowerBI Template` of the installation CD. 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 section.

Password Manager Credential Checker

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

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

Configuring Password Manager credential checker

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

   $url=<valid URL>

   $api_key=<valid Key>

   $api_secret=<valid api secret>
4. Save the file.

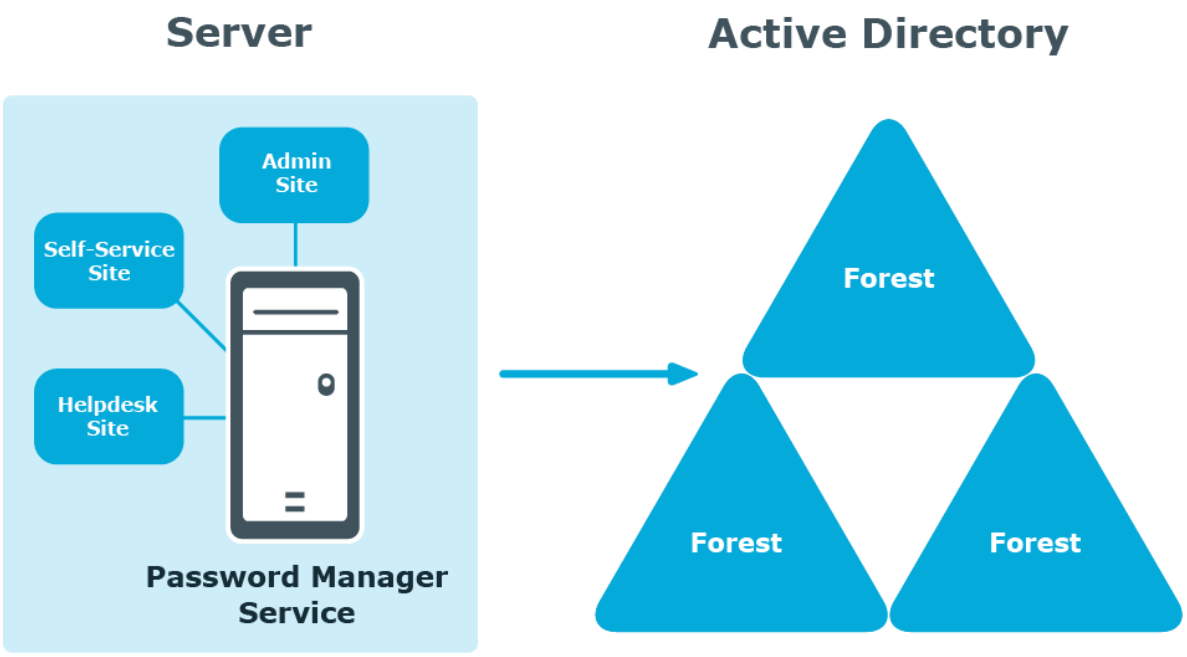
When you enter a new password on the Self-Service site using any of the workflows, such as, **Forgot Password** or **Manage My Passwords**, the Credential Checker validates the new password and check if it matches with the passwords listed in the **VeriClouds**. If the password matches, **Provided password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

This feature is not applicable if the user changes the password using **CTRL+ALT+DELETE** on the Windows logon screen.

Typical deployment scenarios

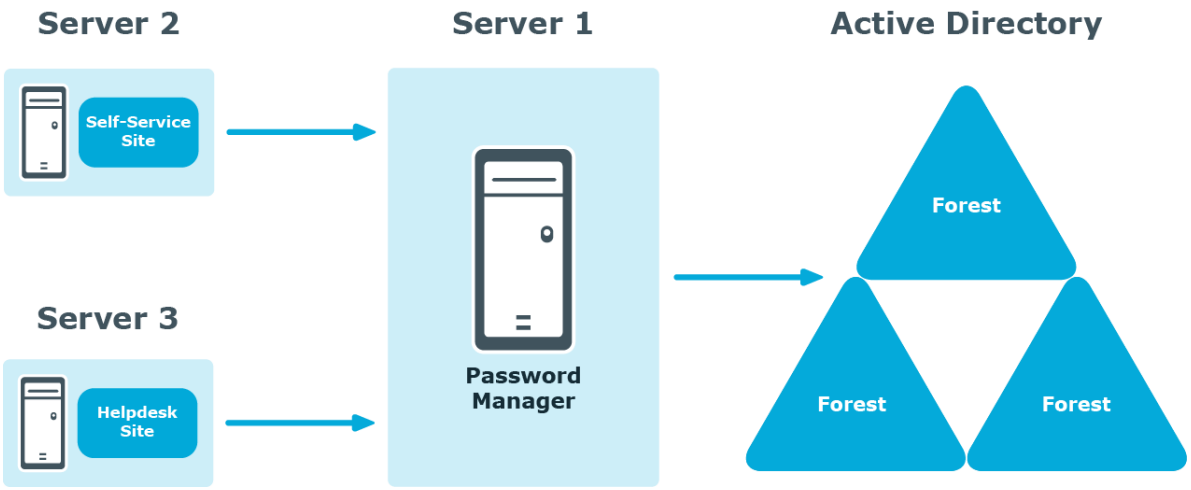
This section describes typical deployment scenarios for Password Manager, including scenarios with installation of the Self-Service and Helpdesk sites on standalone servers, using realms, and others.

Simple Deployment



In this scenario, you install all main Password Manager components, that is, the Password Manager 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 Self-Service and Helpdesk Sites on Standalone Servers



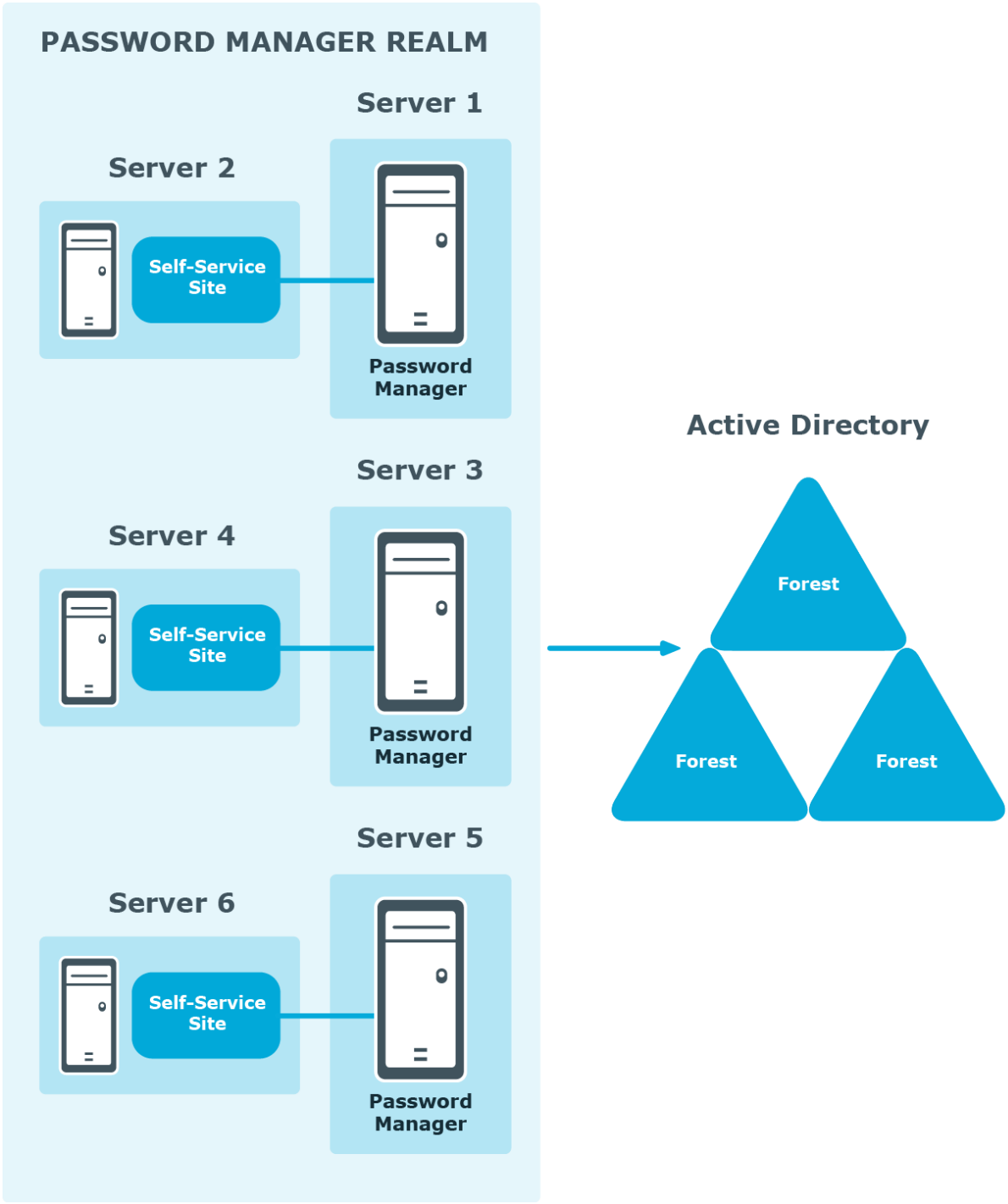
In this scenario, you install the Legacy Self-Service site, Password Manager Self-Service site, Helpdesk site, or both on a standalone server. Note that the Administration site cannot be installed separately from the Password Manager Service.

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

When deploying Password Manager in an environment with the perimeter network, it is recommended to do a full installation of Password Manager 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 Self-Service site).

Realm deployment



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

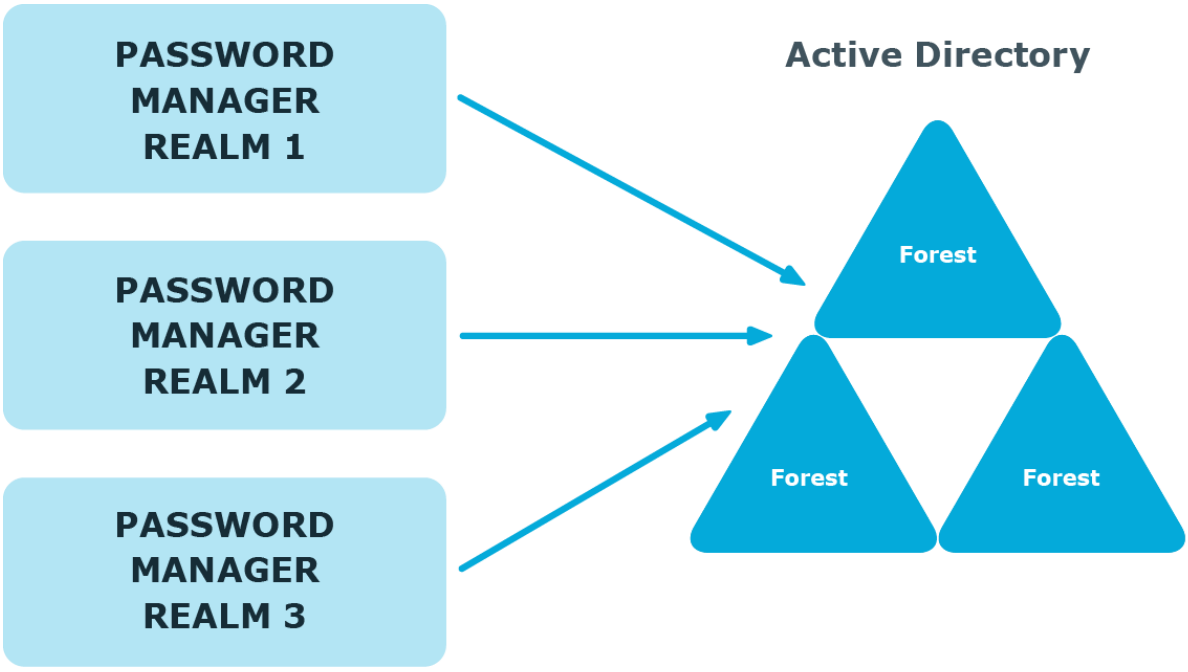
The realm provides for high availability of the service, load balancing, and fault tolerance.

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

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

For more information on how to create realms, see Import/Export Configuration Settings on page 159.

Multiple realm deployment



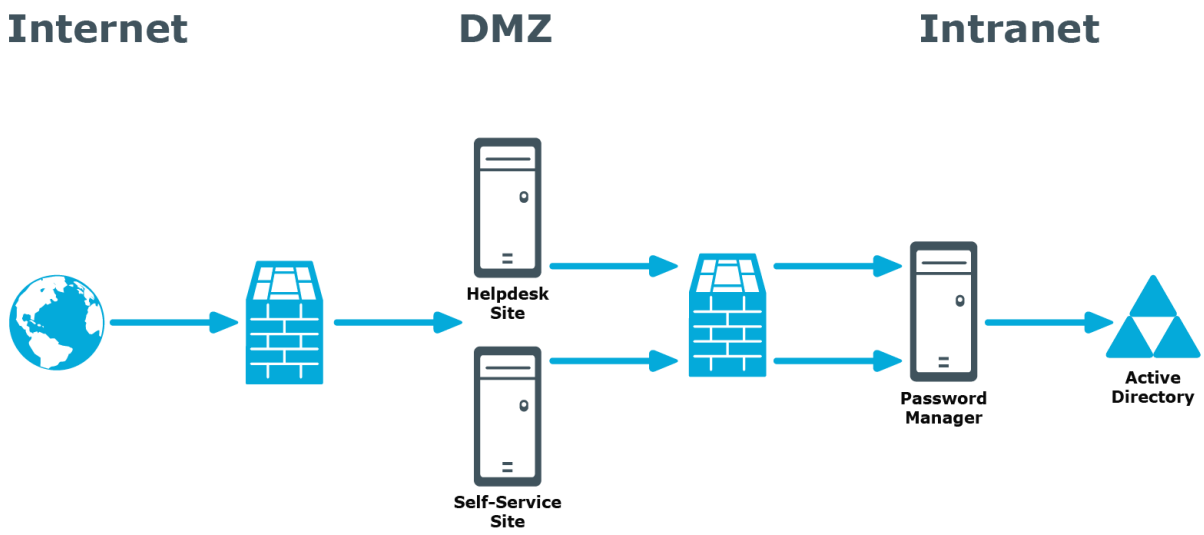
In this scenario, you deploy several Password Manager realms in your environment. You can use this scenario in a complex environment, when several Password Manager configurations are required.

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

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

Password Manager in a perimeter network

When deploying Password Manager in a perimeter network (also known as a DMZ), it is recommended to install the Password Manager Service and the sites in a corporate network at first (that is,use the Full installation option in the Password Manager 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 Service, see Installing Legacy Self-Service, Password Manager Self-Service, and Helpdesk Sites on a Standalone Server on page 15.

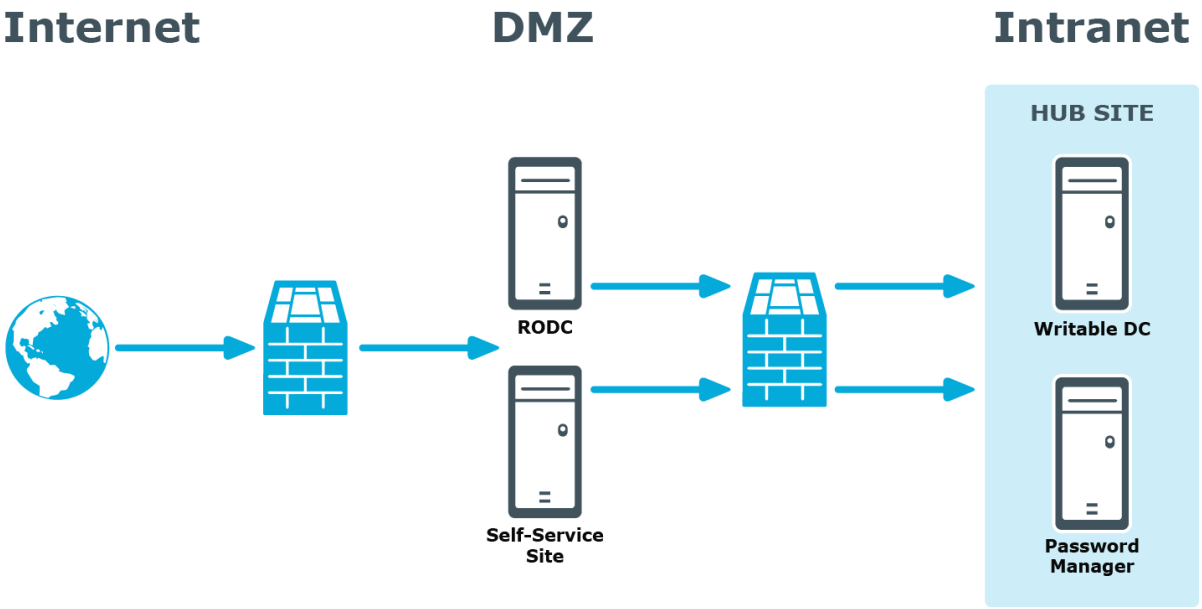
Installing Password Manager in Perimeter Network with Read-Only Domain Controllers

If your network topology includes a perimeter network (DMZ) that contains only read-only domain controllers (RODCs), you should consider the following when installing Password Manager in this environment.

Because password changes may not get immediately replicated to RODCs, users may experience downtime when authenticating using an RODC if their passwords were changed or reset on a DC in another Active Directory site.

To mitigate this issue, it is recommended to do either of the following when installing Password Manager in the perimeter network:

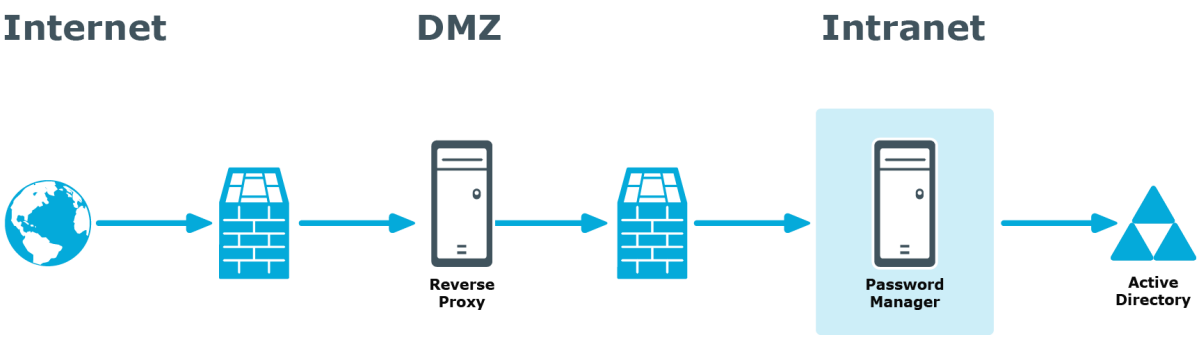
- Install Password Manager Service in a dedicated RODC replication hub site (as shown below), if this hub site exists in your environment.



- If Password Manager Service cannot be installed in the dedicated RODC replication hub site, do either of the following:
  - For your Management Policy, specify the appropriate writable DC from the hub site in the advanced settings of the domain connection. For more information, see Specifying advanced settings for domain connection on page 27.
  - For your Management Policy, specify the hub site in the list of Active Directory sites to which replication changes will be forced. For more information, see Specifying advanced settings for domain connection on page 27.
  - Enable change notification on the site link between the dedicated RODC replication hub site (or the site in which an RODC is installed) and the site in which Password Manager Service is installed.

Installing Password Manager 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.



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.

Installing Password Manager in Perimeter Network without AD DS

If Active Directory Domain Services (AD DS) is not deployed in a perimeter network in your environment, you may still install Password Manager in this perimeter network.

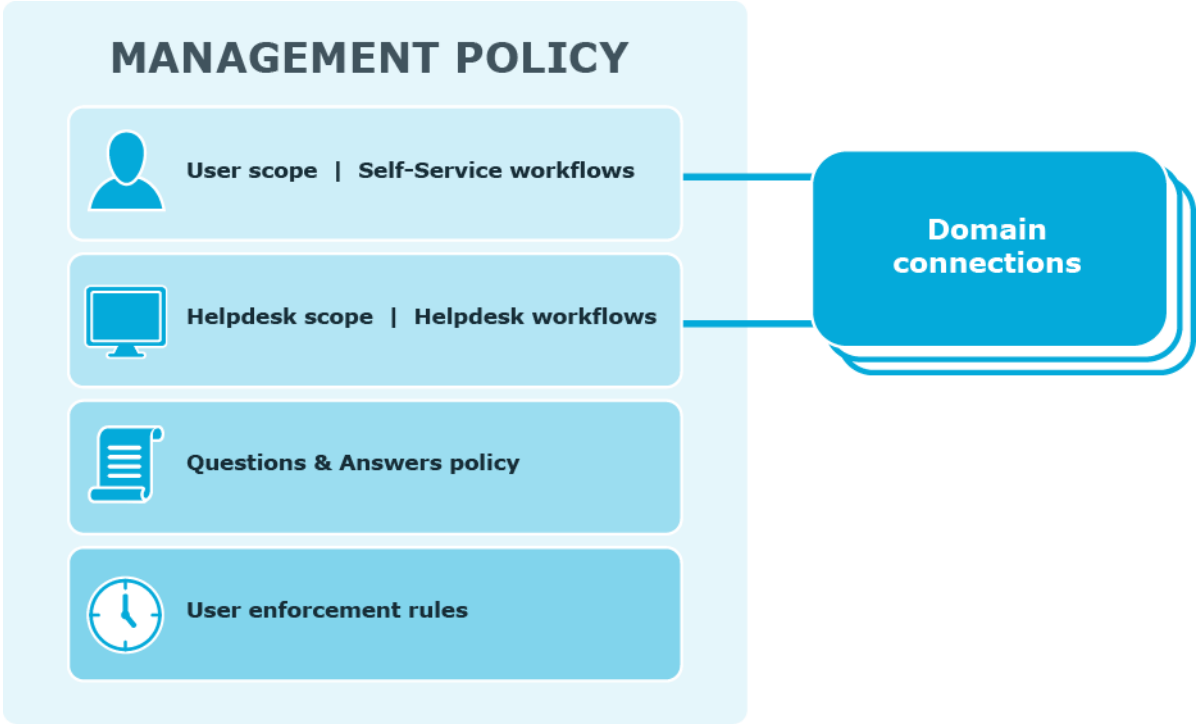
When AD DS is not deployed in the perimeter network, servers are placed in a workgroup. Password Manager allows installing the Self-Service and Helpdesk sites on servers that are not placed in any domain.

Management Policy overview

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

Management Policy components

The following diagram illustrates the Management Policy components.



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

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

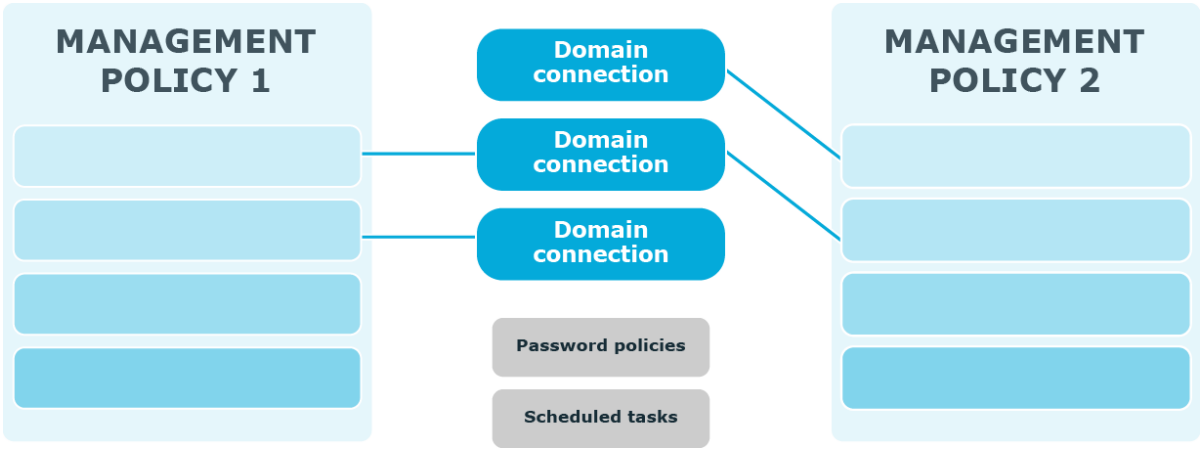
Self-Service and helpdesk workflows define the tasks that are available to users and Helpdesk operators on the Self-Service and Helpdesk sites: for example, Forgot My Password, Assign Passcode, Unlock Account, and so on.

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

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

Management Policy and other Password Manager settings

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



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

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

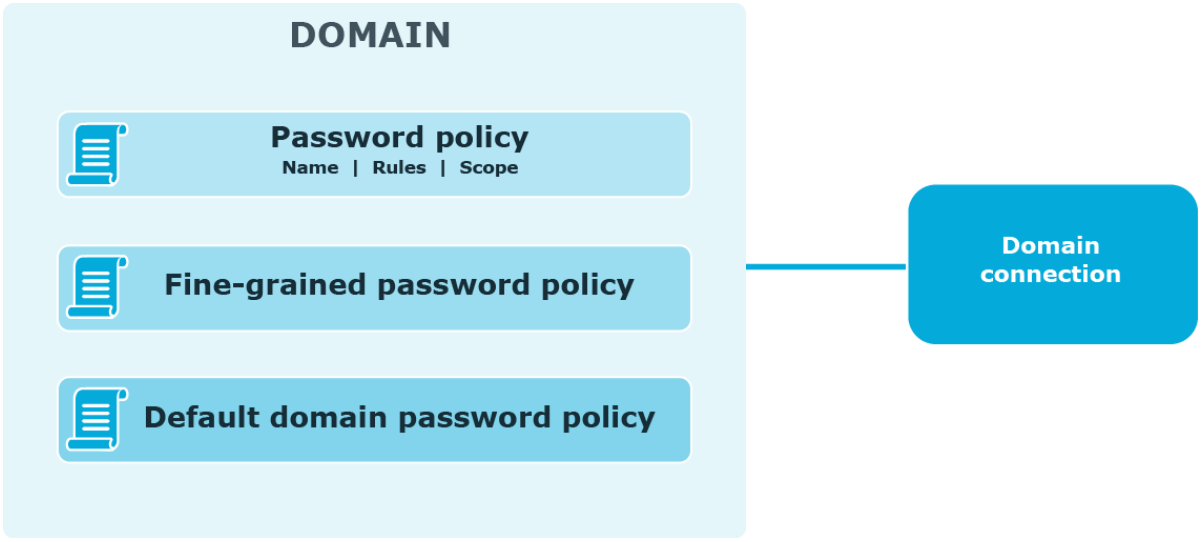
The **Invitation to Create/Update Profile, Reminder to Create/Update Profiles, Reminder to Change Password** scheduled tasks allow notifying users from scopes of user enforcement rules configured in Management Policies. For more information, see Scheduled Tasks on page 163 and User Enforcement Rules on page 138.

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 and Configuring a Password Policy on page 237.

Password policy overview

Password Manager provides the opportunity to apply and manage custom One Identity password policies and Windows fine-grained password policies.

The following diagram shows available password policies and their structure.



Using One Identity password policies

With Password Manager, you can create custom password policies that extend the system password policy rules.

To create and manage One Identity password policies, you need to add a domain connection on the **Password Policies** tab of the Administration site. When adding the domain connection, you specify the domain to which password policies will be applied and the credentials that will be used to access the domain.

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

NOTE: Password policy rules are applied and displayed on the Self-Service site when users change or reset passwords only after you have added the domain connection and created policies for the corresponding domain.

Using fine-grained password policies

By default, existing fine-grained password policies are applied to users from fine-grained password policies' scopes. But to be able to manage fine-grained password policies and to have the Self-Service site display the password policy rules when users reset or change passwords, you need to add a domain connection on the **Password Policies** tab of the Administration site.

When adding the domain connection, you specify the domain to which password policies will be applied and the credentials that will be used to access the domain.

NOTE: The default domain password policy is applied to users from the policy scope, but the policy itself is not displayed in the policy list on the Administration site.

NOTE: Creating a new **Windows fine-grained password policies**, does not contain a **Policy Scope** by default. Hence, by clicking **Edit** on the newly created **Windows fine-grained password policies** and configuring the required **Policy Scope** in the **Password Policy Properties** window, one can view these policies for the configured users in the Self service site.

Applying multiple password policies

If a user is found in the scopes of a default domain password policy, a fine-grained password policy, and a One Identity password policy, the applicable policy is selected in the following algorithm. The default domain policy is ignored. The rules from the fine-grained and One Identity policies are merged with the strictest value selected for each rule.

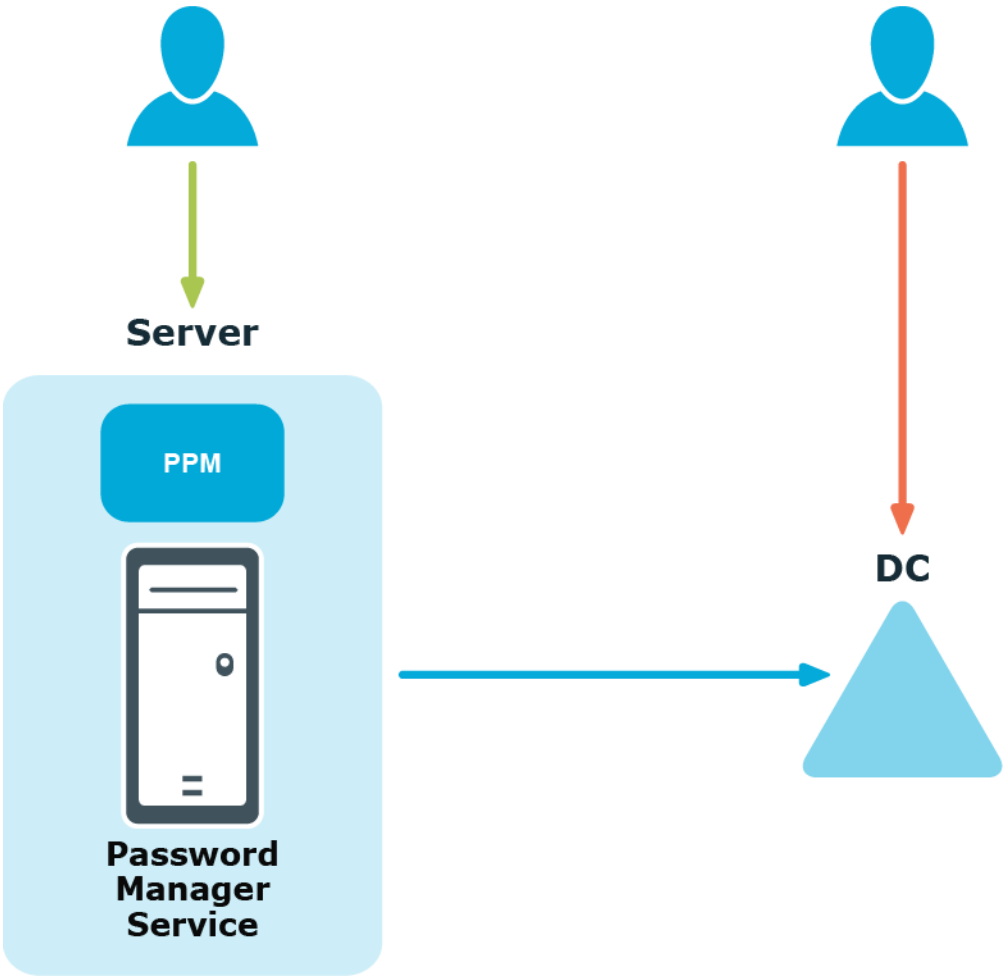
If a user is found in the scopes of several fine-grained password policies, the applicable policy is selected automatically in Active Directory.

If a user is found in the scopes of several One Identity 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.

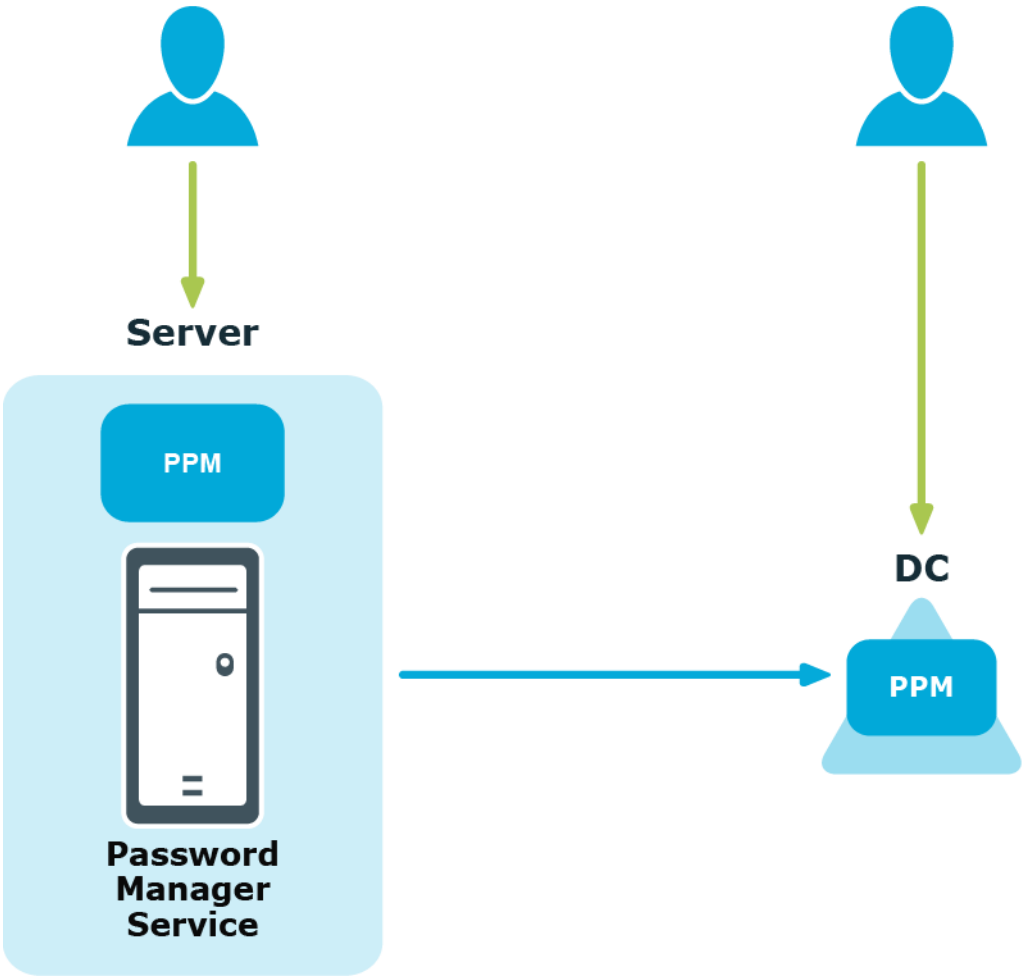
Using Password Policy Manager

Password Policy Manager is a separate component of Password Manager that allows enforcing One Identity password policy rules when users change or reset passwords by means other than the Self-Service site.

For example, you have configured a One Identity password policy for users from domain "My Domain." When users from this domain change or reset passwords on the Self-Service site (the user on the left in the diagram below), the configured One Identity password policy is applied, and corresponding policy rules are displayed. This happens because Password Policy Manager is always available with the Password Manager service. But when users try to change or reset passwords by pressing CTRL+ALT+DELETE, for example (the user on the right in the diagram below), the configured One Identity password policy will not be enforced.



To enforce the configured One Identity password policy in cases when users change or reset passwords *not* via the Self-Service site, you must install Password Policy Manager on all domain controllers in the domain. In the case when Password Policy Manager is installed on domain controllers in the managed domain, when the same users change or reset password by pressing CTRL+ALT+DELETE, the One Identity password policy will be applied.



Therefore, if users from your managed domain change or reset their password on the Self-Service site only, you do not need to install Password Policy Manager on all domain controllers in the domain. But if you want to ensure that password policies are enforced when users change or reset passwords by means other than the Self-Service site, you must install Password Policy Manager on all domain controllers in the domain.

For more information on how to install Password Policy Manager, see Installing Password Policy Manager on page 235.

Secure Password Extension overview

This section explains how Secure Password Extension locates the Self-Service site and launches notification dialog boxes on end-user computers that remind users to create or update their Questions and Answers profiles.

Locating Self-Service site

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

For more information, see:

- Obtaining the Self-Service site URL from a service connection point
- Changing the Self-Service site URL on the Administration site
- Changing Self-Service Site URL in the Administrative Template

Obtaining Self-Service Site URL from service connection Point

Every Password Manager instance publishes its service connection points in Active Directory. Secure Password Extension uses service connection points to automatically locate the Self-Service site.

Service connection points are objects in Active Directory that hold information about services. Services can publish information about their existence by creating service connection points in Active Directory. Client applications use this information to find and connect to instances of the service. When an instance of Password Manager is installed, the Password Manager Service publishes its service connection points in Active Directory. To locate the server where the Self-Service site is deployed, Secure Password Extension uses the service connection points published by Password Manager Service instances in Active Directory.

1. Password Manager instance publishes a service connection point in Active Directory.
2. Secure Password Extension locates the service connection point.
3. Secure Password Extension obtains the necessary data from the service connection point (URL path to the Self-Service site).
4. Secure Password Extension opens the Self-Service site.

Changing Self-Service Site URL on the Administration site

If you want to change the default Self-Service site URL published in service connection points, use the Administration site to specify a new URL. This may be necessary if you enabled HTTPS binding for the Self-Service site after Password Manager installation, or if you want Secure Password Extension to use the Self-Service site installed on a stand-alone server.

Changing the Self-Service site URL

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*>/PMAdmin/.

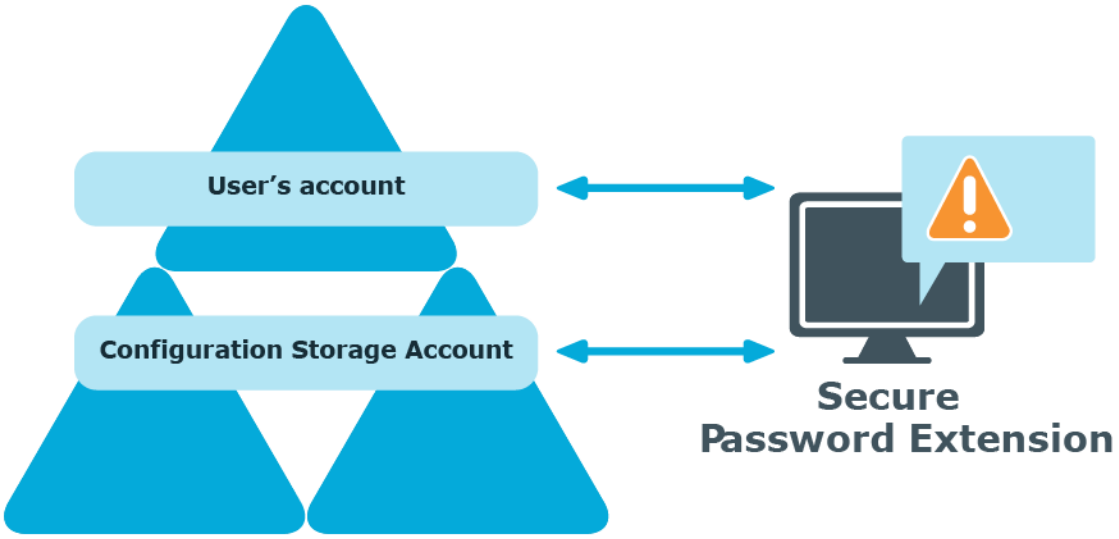
   NOTE: When prompted to log in, provide your domain user name in a `domain-name\username` format.

2. On the menu bar, click **General Settings**, then click the **Realm Instances** tab.
3. Click **Edit** under the service instance for which you want to specify a different Self-Service site URL.
4. In the **Edit Self-Service Site URL** dialog, specify a new URL and click **Save**. The specified URL will then be published in service connection points.

Launching user notification

Every unique Password Manager instance creates a configuration storage account in Active Directory. Password Manager uses this account to store its configuration data. Secure Password Extension uses the account to launch user notification.

1. Secure Password Extension locates the configuration storage account and obtains information on notification schedule.
2. Secure Password Extension locates the user's account to check whether the user has been marked by the Password Manager scheduled task and should be notified to create or update their Questions and Answers profile.



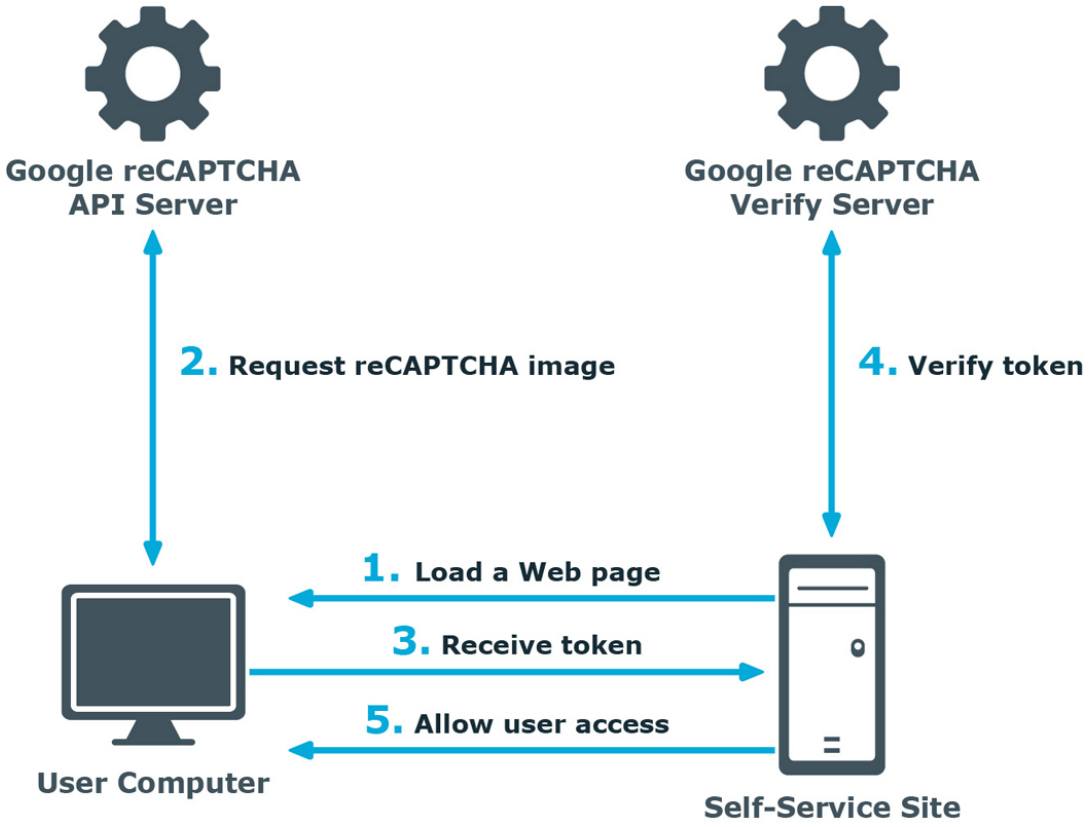
reCAPTCHA overview

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

How to use reCAPTCHA V2 on Password Manager sites

To display reCAPTCHA V2 on the Self-Service site, include the Display reCAPTCHA activity in required workflows. To require users to respond to a reCAPTCHA V2 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 102.

You can also use reCAPTCHA on the Find Your Account page of the Self-Service site and require users to respond to the reCAPTCHA V2 challenge before searching for their accounts. For more information, see Configuring Security Settings.

System requirements for using reCAPTCHA

To be able to use reCAPTCHA V2 on the Password Manager sites, make sure the following requirements are met:

- The Self-Service site has access to the address:
  http://www.google.com/recaptcha/api/siteverify

References

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

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

User enrollment process overview

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

To start the enrollment process, you need to enable and configure the **Invite users to create/update Q&A profiles** rule. This rule sends email notifications to the users specified in the rule's scope, inviting them to create or update their Questions and Answers profiles. When configuring email notifications for this rule, you can insert a hyperlink to the

Self-Service site. To add the hyperlink, enter the required URL in the email notification body. For example, http://mydomain.com/user. Note that you cannot specify the hyperlink text.

To configure the **Invite users to create/update Q&A profiles** enforcement rule, you need to specify the conditions under which users should be notified. For example, users are not registered with Password Manager, users' answers are shorter than required, or users have specified the same answers for several questions. These conditions correspond to the Q&A profile settings that are part of the Q&A policy. For more information, Configuring Q&A profile settings. For more information on configuring this enforcement rule, see Invite Users to Create/Update Profiles on page 138.

NOTE: 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 and via notification dialog displayed by Secure Password Extension installed on users' computers. When configuring this rule, you can specify several notification scenarios. For each scenario, you should set the time period since the invitation date and notification option (email or Secure Password Extension).

For example, you can configure the following scenarios:

- Users were invited 5 days ago: For this case, you may want to notify users by email only.
- Users were invited 10 days ago: For this case, you may want to notify users via Secure Password Extension only. Note, that users will not receive any email notifications during this period.
- Users were invited 20 days ago: For this case, you may want to notify users by email and via Secure Password Extension. So, starting from day 20 users will receive both emails and Secure Password Extension notifications.

For more information on configuring this enforcement rule, see Remind Users to Create/Update Profiles on page 141.

NOTE: If the user does not create or update his Q&A profile in the specified number of days, you can disable the user account. For more details see Forced Enrollment.

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 Questions and Answers 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 questions 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 Questions and Answers 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 104.
- 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 105.
- 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. Answers to Helpdesk questions are always stored using reversible encryption. Answers to mandatory questions are hashed, unless you select the **Store answers using reversible encryption** option in the Q&A profile settings. Note that if answers to 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 Questions and Answers 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 138.

Password change and reset process overview

Password Manager uses standard Active Directory methods to reset and change password, applying password policies specified in the Active Directory. Thus, resetting or changing password in Password Manager is essentially the same as resetting or changing password using Active Directory Users and Computers (ADUC).

Resetting and changing password in connected systems

If you have configured Password Manager to use One Identity Quick Connect Sync Engine to reset and change passwords in multiple systems, Password Manager will at first reset or change the password in the managed domain. If this operation is performed successfully, then the password will be reset in all connected systems, otherwise Password Manager will attempt to reset the password in the systems in which the password can be reset independently from Active Directory, and all other systems will be skipped.

Enforcing password history when resetting password

When you use Password Manager to reset your password, Active Directory does not automatically check the new password against the password history. As a result, the "Enforce password history" policy setting may have no effect. To ensure that this password policy setting is applied in Active Directory when your password is reset by using Password Manager, the **Enforce password history** option must be selected in the **Reset password in Active Directory** and **Reset password in Active Directory and connected systems** activities.

Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, it is advised that you double the password history value for all managed domains.

When the password history is enforced for resetting passwords, Password Manager resets users' old password to an automatically generated password that complies with password policies. It is required for the user to go through the Quick Connect workflow once again where the Reset password in Active Directory and connected systems activity is configured. This time the password is changed to the one provided by the user. Note that, if an error occurs when changing the password, users may end up with the automatically generated password they do not know.

For more information, see Reset Password in Active Directory on page 110.

Replicating password changes

You can manage how password-related changes are replicated in your environment. If you want to force password changes and resets in the required Active Directory sites, select the corresponding sites on the **Advanced settings** tab of the **Edit Domain Connection** dialog, and select the **Replicate password-related changes** check box.

Data replication

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

Storing data

There are two types of data stored by Password Manager: Password Manager configuration data, and users' Questions and Answers 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 Active Directory that you specify during instance initialization. By default, it is the comment attribute. You can also change it after initializing a Password Manager instance. For more information, see Instance Reinitialization on page 173.

Password Manager configuration data is stored in the C:\ProgramData\One Identity\Password Manager 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, domain connections, custom activities and workflows, instance settings, and so on.

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

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

Replicating data

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

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

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

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

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

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

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

Note that the domain management account must have the permission to create user accounts and containers in the Users container for configuration data to be replicated. For more information on configuring the domain management account, see Configuring Permissions for Domain Management Account on page 23.

Changing replication settings

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

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

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

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

Changing replication settings

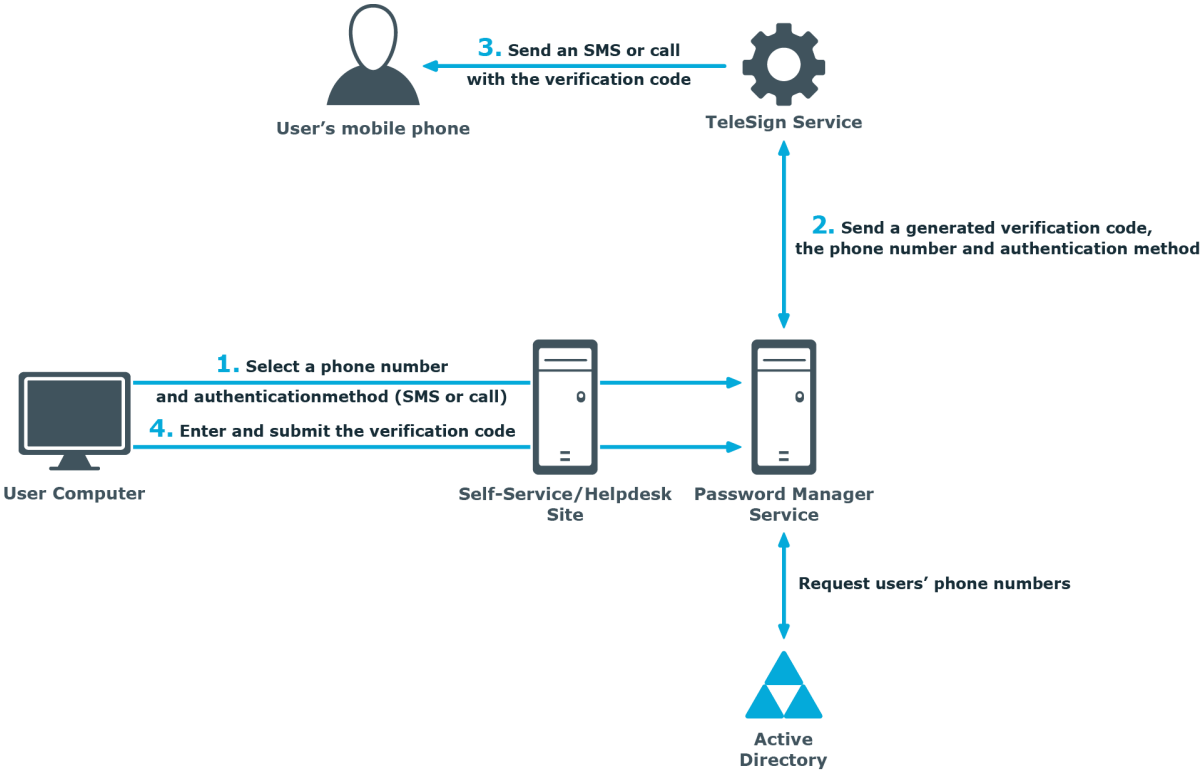
1. On the computer where Password Manager is installed, open the `QPM.Service.Host.exe.config` file located in the *<Password Manager installation folder>*\Service folder with a text editor.
2. In the **replication** node, specify the following:
    - To divide the configuration data into segments by a segment size, set the packetLimitMode to LimitSize (packetLimitMode="LimitSize").
    - To divide the configuration data into segments by a number of segments, set the packetLimitMode to LimitCount (packetLimitMode="LimitCount").
    - If you set the packetLimitMode to LimitSize, specify the maximum segment size in bytes in the maxPacketSize parameter. For example, maxPacketSize="100000". Set the maxPacketsCount parameter to zero (maxPacketsCount="0").
    - If you set the packetLimitMode to LimitCount, specify the maximum number of segments to be created in the maxPacketsCount parameter. For example, maxPacketCount="10". Note, that this value must be greater than 1. Set the maxPacketsSize parameter to zero (maxPacketsSize="0").
3. In the **storageManager** node, specify the following:
    - To change the name of the storage container, in the storageContainerReplicationPath element specify the required name. The default value is CN=PMReplication.
    - To change the container for storing replication data, in the storageContainerPath element specify the required container. The default value is CN=Users.
    - To change the names of user accounts used to store data segments, in the storageContainerPartName element specify the required name. The default value is strg.
4. Save the `QPM.Service.Host.exe.config` file.

5. Restart the Password Manager Service in the **Services** console. Type **services.msc** at a command prompt, select **Password Manager Service** in the console, and click **Restart.**
6. Repeat steps 1-4 on each instance belonging to a Password Manager realm.

Phone-based authentication service overview

One of the authentication options offered by Password Manager is a phone-based authentication. It allows 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 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 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 Service. Password Manager Service gets the phone numbers from the Active Directory attributes specified in the workflow settings.
2. Password Manager 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 Service.
5. Password Manager 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 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 on page 107.

System requirements

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

1. You have a valid license for the phone-based authentication service (see the About page of the Administration site for the service status).
2. Outbound SSL connections are allowed from the computer on which Password Manager 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.

4

Management policies

Checklist: Configuring Password Manager

When you have installed Password Manager, follow this checklist to configure the solution to implement automated and secure password management in an Active Directory domain.

Table 2: Checklist to configure Password Manager

Step	Reference
Prepare a domain management account.	Configuring Permissions for Domain Management Account on page 23

Step	Reference
Configure a user scope.	Configuring user scope on page 22
Configure the Questions and Answers policy: Create language-specific question lists, and configure Q&A profile settings if required.	Configuring Questions and Answers policy on page 82
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 78
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 Self-Service site workflows on page 97 Helpdesk Workflows on page 124
If required, configure rules for user registration notification and enforcement by specifying a registration schedule and enabling registration notification.	User Enforcement Rules on page 138
Configure general settings that apply to all user scopes (such as account search options, SMTP servers, scheduled tasks, and so on.)	General Settings Overview
If you want to provide access to the Self-Service site from the Windows login screen and notify users that they should create or update Q&A profiles, install Secure Password Extension.	Deploying and Configuring Secure Password Extension on page 218
If you want to use Password Manager to enforce password policies, you must install Password Policy Manager (PPM) on all domain controllers in the domain. Then, create password policies and configure password policy rules.	Installing Password Policy Manager on page 235
If you want to use Password Manager for cross-platform password synchronization, install One Identity Quick Connect Sync Engine and configure the product to integrate with Password Manager.	Reset Password in Active Directory and Connected Systems on page 113
Ensure that all Password Manager users have Java Script enabled in Microsoft Internet Explorer settings.	

Step	Reference
Ensure that the users know the Self-Service site URL and can access the site to register and perform password self-management tasks.	

Understanding Management Policies

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

A Management Policy consists of the following components:

- Questions and Answers policy
- User scope
- Helpdesk scope
- Workflows
- User enforcement rules and reminders

User scope is a group or several groups of users managed by Password Manager. When configuring a user scope for a Management Policy, you can add user groups from different domains. For more information about the user scope, see Configuring user scope on page 22.

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 78.

Questions and Answers policy (Q&A policy) is a policy within which secret questions and Q&A profile settings are defined. Secret questions are a set of mandatory, optional, and Helpdesk questions for users' Questions and Answers profiles. These questions are used to register users with Password Manager and later to authenticate users when they use the Self-Service site. Q&A profile settings define how many questions a user must answer to create Q&A profile settings and set requirements for user's questions and answers. For more information about Q&A policy, see Configuring Questions and Answers policy on page 82.

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 that can be easily customized. For more information about workflows, see Workflow overview on page 87.

User enforcement rules and reminders 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 138.

Configuring access to the Administration site

By default, the access to the Administration site is granted to only the domain user from the AD, who is a member of the local Administrators group and to the PMAdmin group, that is created during Password Manager installation.

To provide access to the Administration site, add the delegated administrators' accounts to the PMAdmin group and also add them to the IIS_IUSRS or Administrators group. Members of the referenced groups have access to the complete functionality of the Administration site.

Note that the account that you specified as Application Pool Identity when installing Password Manager is automatically added to the PMAdmin group.

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

Configuring access to the Legacy Self-Service site or Password Manager Self-Service site

To configure access to the Legacy Self-Service site or the Password Manager 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 groups from different domains to a single user scope.

For more information, see Configuring user scope on page 22.

Configuring access to the Helpdesk site

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

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 domain connection to the scope at first, and then specify groups from the selected domain.

To manage all domain connections from a single place, click **General Settings | Domain Connections** on the Administration site. For more information, view Domain Connections on page 178.

To add domain connection

1. Open the Administration site by entering the Administration site URL in the in the address bar of your browser. By default, the URL is http://<ComputerName>/PMAdmin, where <ComputerName> is the name of the computer on which Password Manager is installed.
2. On the Administration site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.
3. On the **Helpdesk Scope** page, click **Add domain connection**.
4. If domain connections already exist, select a domain connection from the list. If you want to create a new connection, click **Add domain connection**.
5. If you selected to create the new domain connection, in the **Add New Domain Connection** dialog, configure the following options:
    - In the **Domain name** text box, type in the name of the domain that you want to add to the Helpdesk scope.
    - In the **Domain alias** text box, type the alias for the domain that will be used to address the domain on the Self-Service site. This field is required because you can reuse the domain connection in the user scope.
    - To have Password Manager access the domain using the Password Manager Service account, click **Password Manager Service account**. Otherwise, click **Domain management account**, and then enter user name and password for the domain management account. Note, that if Password Manager Service account is used to access the domain, it should have the same permissions as the domain management account.

    For information on how to prepare a domain management account, see Configuring Permissions for Domain Management Account on page 23.
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 domain 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 or OUs 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 domain 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.**

Specifying advanced settings for domain connection

After you have created a domain connection, you can specify advanced settings for the connection: domain controllers and Active Directory sites of the managed domain. For more information about domain controllers, seeDomain Controller.

To specify domain controllers

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 domain connection for which you want to specify domain controllers and click **Edit**.
3. On the **Helpdesk Scope Settings for #Domain#** page, click **Edit**.

4. On the **Advanced settings** tab of the **Edit Domain Connection** dialog, click **Add** under the domain controllers table and select required domain controllers, and click **Add**.
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 domain connection is used.

Active Directory Sites

By specifying Active Directory sites in the domain connection settings you select the site in which you want Password Manager to replicate changes as soon as they occur in other sites. This can reduce downtime that users may experience when your environment has several Active Directory sites and changes may not get immediately replicated between the sites.

For example, when helpdesk operators unlock users' accounts, this operation may occur in one site. But when users attempt to log in to their computers, this operation may occur in another site, to which the information about the unlocked account has not been replicated yet. In this case, users will not be able to log in until the information is replicated to the second site. To mitigate this issue, select the Active Directory sites in which you want to replicate changes immediately in the domain connection settings.

To specify Active Directory sites

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 domain connection for which you want to specify Active Directory sites and click **Edit**.
3. On the **Helpdesk Scope Settings for #Domain#** page, click **Edit**.
4. On the **Advanced Settings** tab of the **Edit Domain Connection** dialog, click **Add** under the Active Directory sites table, select required sites, and click **Add**.
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 domain connection is used.

Changes Propagation

After you specify the Active Directory sites in which you want to push changes, you can also select what kind of changes to propagate. The following options are available:

- Propagate changes related to the user's account in Active Directory
- Propagate changes related to the user's Questions and Answers profile
- Propagate password-related changes

Propagating account-related changes

Select this option to propagate information about unlocking and enabling user accounts in Active Directory. It is recommended to use this option when a managed domain has users in multiple Active Directory sites.

Propagating Q&A profile-related changes

Select this option to propagate information about editing, locking and unlocking Q&A profile, and passcodes issued by help desk. It is recommended to use this option when users and Password Manager Service use domain controllers from different sites. In this case, if a helpdesk operator assigns a passcode to a user (via the domain controller in one site), and then the user attempts to use the passcode on the Self-Service (via the domain controller in another site), the user may encounter the issue when the information about the passcode has not been replicated yet because of intersite replication latency.

Propagating password-related changes

Select this option to propagate information about changing or resetting user password. For more information, see Propagating password-related changes on page 29.

Changing Domain Management Account

To access a managed domain you can use either a domain management account or Password Manager Service account. For more information, see Changing domain management account on page 29.

To modify account used to access a domain

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 domain connection for which you want to change access account and click **Edit**.
3. On the **Helpdesk Scope Settings for #Domain#** page, click **Edit**.
4. In the **Access account** section of the **Edit Domain Connection** dialog, select **Password Manager Service account** to have Password Manager access the managed domain using the Password Manager Service account. Otherwise, select **Domain management account**, and then enter user name and password for the domain management account.
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 domain connection is used.

Removing a Domain Connection

To remove a domain connection

On the Administration site, select the Management Policy you want to configure and click the **Helpdesk Scope** link.

On the **Helpdesk Scope** page, select the domain connection you want to delete and click **Remove**. Note, that the domain connection will be removed from this helpdesk scope only. If you want to permanently remove the domain connection, remove it from everywhere where it is used, and then on the **General Settings|Domain 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 questions and answers profile settings. Secret questions are questions to which users provide answers when registering with Password Manager. Using the Q&A profile settings you can specify requirements for user's questions and answers. For example, you can prevent users from using the same answer for multiple questions.

Creating secret questions

Secret questions are questions to which users provide their own answers, thus creating a personal Questions and Answers profile. Before users can register with Password Manager by creating their personal Questions and Answers profiles, you must configure a question list containing the questions that will be presented to users.

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

Password Manager uses personal Question and Answers profiles as an authentication method to allow users and Helpdesk operators to manage user passwords in Active Directory domains 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 86.

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

For information on how to enforce update of Q&A profiles, see User Enforcement Rules on page 138.

Secret questions can contain the following types of questions:

Table 3: Secret questions

Question type	Description
Mandatory questions	Questions of this type are an integral part of a user's Q&A profile. Users must provide an answer to each of these questions.
Optional questions	Users can select what optional questions to answer. Administrator specifies only the number of questions that users must answer.
Helpdesk questions	Security questions used by Helpdesk to verify user's identity before performing password and account management tasks. Answers to 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*>/PMAdmin/.
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 the order of questions 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.

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 138.

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*>/PMAdmin/.
2. On the Administration site home page, click the **Q&A Policy** link under the Management Policy you want to configure.
3. On the **Configure Questions and Answers Policy** page, under **Question List,** click the **Translate questions** link.
4. In the **Select Additional Language** dialog, select an additional language for secret questions.
5. In the **Translate Questions** dialog, translate mandatory, optional, and Helpdesk questions from the default language into the additional language.
6. To change the language, click the **Change language** link.
7. To temporarily hide secret questions in the selected language, select the **Make questions in this language unavailable to users** check box. This setting will prevent users from creating or updating their Q&A profiles using the question list in this language.
8. Click **Save** to save changes and close the dialog.

IMPORTANT: If you delete 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 138.

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. 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>/PMAdmin/.
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, and then click **Save**.

To delete questions of a specific 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>/PMAdmin/.
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**, and 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**.

NOTE:

- 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

Question and Answers 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.

For an overview of Q&A policy and profile settings, see Questions and Answers policy overview on page 65.

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>/PM/Admin/.

   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, specify the following options:
   a. **Question Settings**
      i. 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.
      ii. Users must answer this number of user-defined questions to register: Set the required number of user-defined questions that a user must specify to create a Questions and Answers profile.
      iii. Minimum length of user-defined questions: Set the least number of characters that user-defined questions can contain.
   b. **Answer Settings**
      i. Minimum length of answers: Set the least number of characters that users' answers can contain.

ii. Reject the same answers for different questions: Select to prevent users from specifying same answers for different questions.

iii. Reject answers that contain corresponding questions: Select to prevent users from specifying answers that contain corresponding questions.

iv. Store answers using reversible encryption: Select to store users' answers using reversible encryption. If you do not select this check box, answers to secret questions (mandatory, optional, and user-defined) will be hashed using the hashing algorithm you specified when initializing the instance. If you want to change the hashing algorithm, you need to re-initialize the instance. For more information, see Instance Reinitialization on page 173. Note that answers to helpdesk questions are always stored using reversible encryption.

c. **Security Settings**

i. 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.

ii. Hide users' answers by default: Select this check box to have Password Manager display users' answers as asterisks while they are typing in their answers.

iii. 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, configure workflows in the Password Manager Administration Site. Workflows have 2 types:

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

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

Workflow structure

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

Workflow activities have 3 types:

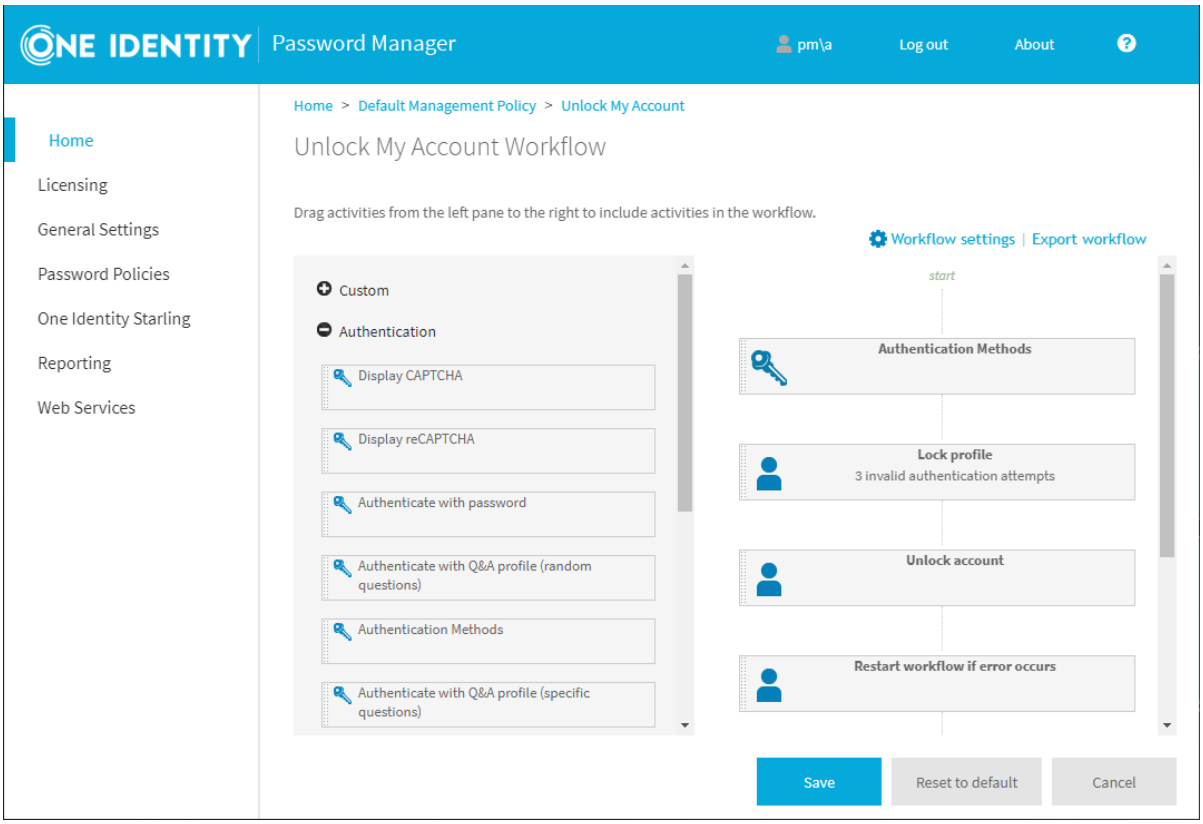
- **Authentication** provides authentication options, such as password-based authentication, Questions and Answers profiles, or phone-based authentication.
- **Actions** are core components in workflows, including activities like unlocking accounts, editing Q&A profiles, or resetting passwords.
- **Notifications** let you configure email notifications for users and administrators, and specify the conditions under which Password Manager will send these notifications.

You can also create custom activities. For more information, see Custom activities .

Password Manager 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 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 state

Workflow states determine how Password Manager 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 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 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 performs only the following activities:
  - **Email user if workflow fails**
  - **Email administrator if workflow fails**

Workflow settings

For each workflow, you can set 2 options:

- **Language settings** specify a custom name and description for the selected workflow on the Password Manager Self-Service Site or Helpdesk Site, either in the default language, or in additional languages.
- **Availability settings** specify if the workflow must appear in the Password Manager Self-Service Site or in the Helpdesk Site.

NOTE: You can specify custom names and descriptions only for the languages for which localization is available in the Password Manager Self-Service Site and Helpdesk Site.

To set the language settings

1. On the Password Manager 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** > **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 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** > **Availability** > **Enable the workflow**, select the availability option of your workflow:
    - **Always**: The workflow is always enabled for users on the Password Manager Self-Service Site or for operators on the Helpdesk Site.
    - **Never**: The workflow is always disabled on the Password Manager 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 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 Self-Service Site. Users must contact the helpdesk in this case.

      The default criteria for enabling or disabling workflows on the Password Manager 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 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 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 Service.
2. Open the `C:\ProgramData\One Identity\Password Manager\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 Service.

Custom workflows

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

To create a custom workflow

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

TIP: Consider the following when creating a new workflow:

- When you add a new custom workflow, it does not contain any activities. To add activities, click the workflow to open the Workflow Designer.
- You must specify the name and description for each workflow in the default language used on the Self-Service Site or Helpdesk Site. 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 on page 89.

NOTE: Custom workflows appear on the Password Manager 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 Service.
2. Open the `C:\ProgramData\One Identity\Password Manager\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 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 Administration Site, navigate to **General Settings** > **Extensibility**.
2. Select **Extensibility on**.
3. To apply your changes, click **Save**.

To export a workflow

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

To import a workflow

IMPORTANT: Before importing a workflow, consider the following:

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

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

Custom activities

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

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

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

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

IMPORTANT: Note, 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 that is, 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.

    a. **Hide the element on the user interface**. Select this check box if you want to hide this element from the Self-Service or Helpdesk site.
6. On the **Activity Name** tab, specify the following options:
    - **Activity short name** . The activity name that should be used in PowerShell scripts to refer to the activity.
    - **Activity display name**. The activity name displayed in the activities list and workflow designer.
    - **Activity description** . Your description of the custom activity.
7. On the **PowerShell Script** tab, enter the PowerShell script to set the activity behavior. For more information on how to create and use activity scripts, refer to the Password Manager SDK.
8. Click **OK**.

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

To convert a built-in activity to a custom activity

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

Importing and exporting custom activities

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

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

To turn extensibility features on

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

To export custom activity

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

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

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

To import custom activity

1. On the Administration site, open the workflow designer, expand the **Custom** group in the left pane of the workflow designer, and click **Import custom activity**.
2. In the **Import Custom Activity** dialog 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 that 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 Self-Service site workflows

By configuring the Legacy Self-Service or the Password Manager Self-Service workflows, you can specify what tasks will be available for users on the Legacy Self-Service site and on the Password Manager 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.

The following are the available Legacy Self-Service and Password Manager Self-Service workflows:

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

All available workflows are preconfigured and ready to use.

The Self-Service and the 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 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. The Following are the three methods available for the users to register:

- Corporate authentication
- Security questions
- Personal contact method: Email and Mobile

The selected options is 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 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 is installed. Open the

QPM.Service.Host.exe.config file. Add the required details in the **<CountryConfig ShowWith="*Attribute*">** tag, where **<"*Attribute*">** can be **CountryName** or **CountryCode**.

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

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

Manage My Profile

The Manage My Profile workflow allows 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, do the following:

1. Select **Manage My Profile** workflow in the Password Manager Administration site.
2. Click **Settings**.
3. Select **Run this activity only if user's profile should be updated** check box.

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 Active Directory 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 Quick Connect Sync Engine, see Reset Password in Active Directory and Connected Systems on page 113.

IMPORTANT: To display password policies on the Self-Service site when users reset passwords, add the required domains on the Password Policies tab of the Administration site. For more information see Creating and Configuring a Password Policy on page 237.

Depending on the selected registration methods in **Register activity** settings in **Register** workflow, authentication modes (corporate authentication, security questions, and

personal contact method) is displayed in **Authentication Mode** activity settings in **Forgot My Password** workflow.

For example: if administrator has configured only Q&A as registration method, only Random and Specific authentication modes display in Authentication Mode activity settings.

The default configuration of this workflow is the following:

1. Authentication Methods.
2. Lock Q&A profile.
3. Reset password in Active Directory.
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 Active Directory 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 Quick Connect Sync Engine, see Change Password in Active Directory and Connected Systems on page 114.

IMPORTANT: To display password policies on the Self-Service site when users change passwords, add the required domains on the Password Policies tab of the Administration site. For more information see Creating and Configuring a Password Policy on page 237.

The default configuration of this workflow is the following:

1. Authenticate with password.
2. Change password in Active Directory.
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.

Depending on the selected registration methods in **Register activity** settings in **Register** workflow, authentication modes (corporate authentication, security questions, personal

contact method) is displayed in **Authentication Mode** activity settings in **Unlock My Account** workflow.

The default configuration of this workflow is the following:

1. Authentication Methods.
2. Lock Q&A profile.
3. Unlock account.
4. Restart workflow if error occurs.
5. Email user if workflow succeeds.
6. Email user if workflow fails.

My Notifications

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

The default configuration of this workflow is the following:

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

I Have a Passcode

You can use this workflow to configure the **I Have a Passcode** task for the Self-Service site. Users perform this task when they have forgotten their passwords and, at the same time, are not registered with Password Manager or have forgotten their answers to secret questions. In this case, they must obtain a temporary passcode from the Helpdesk 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. Manage My Profile.
3. Restart workflow if error occurs.
4. Email user if workflow succeeds.
5. Email user if workflow fails.

Legacy Self-Service and the Password Manager Self-Service site activities overview

All activities available in the Legacy Self-Service and Password Manager Self-Service site 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 Questions and Answers profiles, or phone authentication.

The actions category includes activities that are core components of the 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 self-service activities and provide information about the settings specific to each activity.

Authentication activities

This section describes workflow 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:

1. **Number of characters** Specify the number of characters that will be displayed on a CAPTCHA image.
2. **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 verify reCAPTCHA on the Self-Service site and require users to click on 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.

reCAPTCHA V2 is a free CAPTCHA service provided by Google.

To start using reCAPTCHA V2, you need to sign up and get reCAPTCHA V2 keys on the following website: 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 V2, go to https://support.google.com/recaptcha/?hl=en#6081880.

This activity has the following settings:

- **Site key** Specify the site key you received when configuring reCAPTCHA V2.
- **Secret key** Specify the secret key you received when configuring reCAPTCHA V2.
- **Theme** Select from Light or Dark theme for the reCAPTCHA V2 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 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 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).

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

Use this activity to authenticate a user with 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 functionality when their passwords are expired or should be changed at the next login.
- **Authenticate users with disabled accounts**: If you select this check box, Password Manager 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:

1. **All questions from user's Q&A profile**:Select this option to have users answer all questions from their Q&A profiles during authentication.
2. **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.
3. **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.
4. **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: Note that 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 their Q&A profile to answer the required secret questions.

Authenticate with Defender

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

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

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

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

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

This activity has the following settings:

- **Defender Server**: Specify the IP address of the computer running the Defender Server.
- **Port number**: Type the port number that the Defender Access Node uses to establish a connection with the Defender Server.
- **Server timeout**: Specify Defender Server timeout (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 an 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.

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

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.

> IMPORTANT: To enable users to use phone-based authentication, configure the user scope for this feature. For more information, see Telephone Verification feature license on page 10.

If your Password Manager license does not include phone-based authentication service and you want to use this service, please contact One Identity Software Support to obtain the necessary license at https://support.oneidentity.com/.

Before enabling phone-based authentication, make sure that users' phone numbers stored in Active Directory are in a 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, or 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.
- **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 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 a passcode for creating or updating their Questions and Answers profile. The users need to register an email address using **Register** or **Manage My Profile** workflow to receive the generated passcode, in case they forget their password and are not registered with Password Manager or have forgotten their answers to secret questions.

The Administrator must create a workflow to generate passcode for the users. When the user clicks the **Get Passcode** option on the Self-Service site, an auto-generated passcode is sent to their registered email address.

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

Use this authentication activity in the **I Have a Passcode** workflow only.

Action activities

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

Register

This is a core activity of Register workflow. Use this activity 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. The 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 selects 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 the 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 User site, select one of the following options.

- Corporate authentication
- Security questions
- Personal contact method: Email and Mobile
- Allow user to choose

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, do the following:

1. Select **Manage My Profile** activity.
2. Click **Settings**.
3. Select the check box **Run this activity only if user's profile should be updated**.

Edit Q&A Profile

This activity is a part of the **Register** and **Manage My Profile** workflow. Use this activity to allow 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.

When you use **Run this activity only if user's profile should be updated** activity in workflows other than **Register** and **Manage My 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 Active Directory

This is a core activity of the **Forgot My Password** workflow. The activity allows users to reset passwords in Active Directory only. If you want to enable users to reset passwords in several systems, configure the Reset password in Active Directory and connected systems, Reset password in connected systems through embedded connectors(Preview) activity. For more information on configuring this activity and using One Identity Quick Connect Sync Engine, see Reset Password in Active Directory and Connected Systems on page 113.

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. Password history is defined for a domain through Group Policy settings.

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

- Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, it is advised that you double the password history value for all managed domains.
- Having entered a new password that is not policy compliant, users may end up with a randomly generated password they don't know.

The **Use auto generated password** option enables Helpdesk users to send the password via email or SMS to reset password.

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

NOTE: Send password via SMS or email is the most secure password reset option in Password Manager. It is recommended to use this option in combination with **Random characters of answers to the specified questions** option from **Authenticate with Q&A Profile** for most secure password reset process. To use **Random characters of answers to the specified questions** configure Helpdesk questions.

The **Enable QESSO integration** option allows you to integrate Password Manager with Quest Enterprise Single Sign-On (QESSO) and notify QESSO about user's password changes. For more information, see Quest Enterprise Single Sign-On (QESSO) on page 268.

Select the **Allow users to reset passwords offline** option to enable users to use the offline password reset functionality provided by Password Manager. This functionality allows resetting passwords when users have forgotten their current passwords and their computers are not connected to the intranet (Active Directory is not available).

This functionality is based on resetting user password in locally cached logon data. The security is provided by using the challenge-response mechanism that guarantees the following:

- A user can reset the locally cached password only after resetting the password online on the Self-Service site.
- A user must specify the same password on the Self-Service site and on the computer in the Offline Password Reset wizard.

When offline password reset is enabled on users' computers, a user must perform the following steps to reset his or her password:

1. Open the Offline Password Reset wizard by clicking the corresponding link on the Windows login screen.
2. In the wizard, enter the user name (this step is optional). Click **Next**.
3. Open the Self-Service site on a computer connected to the internet and find their account.
4. Select the corresponding task to reset password.
5. When performing the task, the user must specify a new password. When the task is successfully performed, a response code is displayed for the user.
6. Then, in the Offline Password Reset wizard, the user must enter the response code and the new password the user specified on the Self-Service site. Click **Next**.
7. If the password is successfully reset, click **Finish** to close the wizard.

Enabling the offline password reset functionality

1. Install the offline password reset component on target user computers via group policy. Use the **`OfflinePasswordReset_x64.msi`** or **`OfflinePasswordReset_x86.msi`** files located in the \Password Manager\Setup folder on the installation CD.

   Note that Secure Password Extension must be installed on target user computers, as well. For more information on installing Secure Password Extension, see Deploying and Configuring Secure Password Extension on page 218.

2. Set the required number of cached user login attempts. This is necessary because the offline password reset functionality will be available only for users who have previously logged in on their computers. You can use this Microsoft knowledge base article, http://support.microsoft.com/kb/172931 to change the number of cached login attempts. It is recommended to use the default value.
3. Use the administrative template `prm_gina.admx` to turn on the offline password reset functionality. The administrative template file is located in the \Password Manager\Setup\Template\Administrative Template\ folder of the installation CD. In the template, enable the following settings: **Display the Offline Password Reset button (command link)** and **Set custom name for the Offline Password Reset button (command link) in <Language>**. For more information on using the administrative template, see Managing Secure Password Extension UsingAdministrative Templates on page 222.

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

NOTE: Use the latest `prm_gina.admx` file by removing the older file from group policy.

To provide authentication during the offline password reset procedure, a shared secret is used. The shared secret is stored locally on a user computer and its copy is published in Active Directory in the computer's account during the first login if the computer is connected to the domain. By default, only domain administrators and the computer account have access to the shared secret. You can specify other users and groups who will have the permission to read the shared secret from the domain. To do it, use the **Configure scope for accessing the shared secret in Active Directory** setting in the administrative template. For more information on the administrative template, see Managing Secure Password Extension UsingAdministrative Templates on page 222.

IMPORTANT: Note that the domain management account must have the permission to read the shared secret from the domain for the offline password reset functionality to work.

You can also use the **Shared secret update period (hours)** setting in the administrative template to specify how often the shared secret should be updated. The recommended value is every 24 hours. For more information on the administrative template, see Managing Secure Password Extension UsingAdministrative Templates on page 222.

Change Password in Active Directory

This is a core activity of the **Manage My Passwords** workflow. The activity allows users to change passwords in Active Directory only. If you want to enable users to change passwords in several systems, configure the **Change password in Active Directory and connected systems** activity. For more information on configuring this activity and using One Identity Quick Connect Sync Engine, see Change Password in Active Directory and Connected Systems on page 114.

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

For example, if you add the **Change password in Active Directory** activity with this option selected to the **Manage My 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.

The **Enable QESSO integration** option allows you to integrate Password Manager with Quest Enterprise Single Sign-On (QESSO) and notify QESSO about user's password changes. For more information, see Quest Enterprise Single Sign-On (QESSO) on page 268.

Reset Password in Active Directory and Connected Systems

Using this activity, you can configure Password Manager to use One Identity Quick Connect to reset passwords in connected systems. If used in conjunction with Quick Connect, Password Manager 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 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 to use a Quick Connect server for cross-platform password synchronization, you must do the following in Quick Connect:

- Create a connection to the Active Directory domains managed by Password Manager.
- Create connections to the systems you want Password Manager to synchronize passwords with.
- Map users from the managed domains 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 Active Directory 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. You can use either pre-Windows 2000 login name (such as DomainName\UserName) or User Principal Name (such as UserName@DomainName.com) to specify the user name.
4. Specify how you want Password Manager 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 Active Directory domain. No warnings are displayed to users if Quick Connect server is not available.
    - **Alert users and allow them to reset passwords only in Active Directory**: Users are notified that other connected data sources are temporarily unavailable, and are allowed to continue managing their passwords only in the Active Directory domain.
    - **Do not allow users to reset passwords**: Users cannot perform any password management tasks in the Active Directory domain and in 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 Active Directory**: Select this option to allow users to reset their passwords in a connected system independently from Active Directory.
    - **Do not allow resetting password in this system independently from Active Directory**: Select this option to prevent users from resetting their passwords in a connected system independently from Active Directory. Note that 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 Active Directory. If the user's password is not reset in Active Directory, 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.
6. To enforce password history in the Active Directory domains 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. Password history is defined for a domain through Group Policy settings.

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

- Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, it is advised that you double the password history value for all managed domains.
- Having entered a new password that is not policy compliant, users may end up with a randomly generated password they don't know.

7. Select the **Enable QESSO integration** to integrate Password Manager with Quest Enterprise Single Sign-On (QESSO) and notify QESSO about user's password changes. For more information, see Quest Enterprise Single Sign-On (QESSO) on page 268.
8. Click **OK** to close the wizard.

Change Password in Active Directory and Connected Systems

Using this activity, you can configure Password Manager to use One Identity Quick Connect to reset passwords in connected systems. If used in conjunction with Quick Connect, Password Manager 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 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 to use a Quick Connect server for cross-platform password synchronization, you must do the following in Quick Connect:

- Create a connection to the Active Directory domains managed by Password Manager.
- Create connections to the systems you want Password Manager to synchronize passwords with.
- Map users from the managed domains 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 in connected systems and Active Directory** 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.

   You can use either pre-Windows 2000 logon name (such as DomainName\UserName) or User Principal Name (such as UserName@DomainName.com) to specify the user name.
4. Specify how you want Password Manager to act when the Quick Connect server is unavailable. To do it, select one of the following and click **Next**:
   a. **Act as if no Quick Connect server were specified**: Users can manage their passwords only in the Active Directory domain. No warnings are displayed to users if the Quick Connect server is not available.
   b. **Alert users and allow them to change passwords only in Active Directory**: Users are notified that other connected data sources are temporarily unavailable, and are allowed to continue managing their passwords only in the Active Directory domain.
   c. **Do not allow users to change passwords**: Users cannot perform any password management tasks in the Active Directory domain and in 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

- **Change password in this system independently from Active Directory.** Select this option to allow users to change their passwords in a connected system independently from Active Directory.
- **Do not allow changing password in this system independently from Active Directory.** Select this option to prevent users from changing their passwords in a connected system independently from Active Directory. Note that 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 Active Directory. If the user's password is not changed in Active Directory, 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.

6. Select the **Enable QESSO integration** to integrate Password Manager with Quest Enterprise Single Sign-On (QESSO) and notify QESSO about user's password changes. For more information, see Quest Enterprise Single Sign-On (QESSO) on page 268.
7. Click **OK** to close the wizard.

Reset password in connected systems through embedded connectors

You can use this activity to reset the password in connected systems through embedded connectors. This activity has to be added after the reset or change password in Active Directory activity in the workflow.

The default configuration of this workflow is the following:

1. Reset password in Active Directory.
2. Change password in Active Directory.

To configure settings to reset passwords on connected systems through embedded connectors

1. On the home page of the Administration site, click **Default Management Policy**.
2. Click **Forgot My Password** or **Manage My Profile**.
3. In the workflows, click **Change/Reset password in connected systems through embedded connectors (preview)**.
4. Select the required platform from the **Select platform** drop-down menu.
5. Provide configuration information for the selected platform.

   IMPORTANT: Configuration settings may vary depending on the platform you select.

   a. You also have the option to enter the AD attribute regular expression phrase to find in the **Find** text field.

b. You also have the option to enter the AD attribute regular expression phrase to replace in the **Replace** text field.

6. Click **Test Connection** to check the connectivity and click **OK**.

You can verify the regular expression results in target systems by entering the sample AD attribute find and replace fields views the results to understand how target user attributes are mapped. For example, from the email *<user>@<website>.com* in the AD and the email *<user>@<website>.co.in* in the target systems, you can find and replace the domain from *.co.in* to *.com*.

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.

NOTE: If you want to enable only the user accounts disabled through force enrollment, in the activity settings, select **Enable user accounts disabled by force enrollment** check box.

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 Active Directory.
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 to require users to change their passwords at next logon. For example, you can use this activity in the **Forgot My Password** workflow to force users to change passwords at the next logon, after the password has been reset by Password Manager.

It is recommended to place this activity after the **Reset password in Active Directory** or **Change password in Active Directory** activities 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 the 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 self-service workflow and offer notification templates.

For more information on configuring user notification activities, see Notification Activities on page 120.

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 will store their personal information.

For example, you can use this activity in the **Register** and **Manage My 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, or Active Directory is not available during workflow execution), 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.

Issue BitLocker Recovery Key

If client computers use BitLocker Drive Encryption, users may need BitLocker recovery keys if they are locked out of their computers.

Note, to use retrieve BitLocker recovery keys via Password Manager, BitLocker must be configured to store recovery information in AD DS. For more information, see *http://technet.microsoft.com/en-us/library/dd875529(v=ws.10).aspx*.

To retrieve a recovery key, users should use the **Issue BitLocker Recovery Key** activity. You can create a new workflow and add this activity to the workflow. On the Self-Service site, when performing the corresponding task, users will be prompted to enter the recovery key ID displayed by their BitLocker-enabled computers. After entering the recovery key ID, users will receive the recovery key that they need to enter on their computers to unlock them.

If you have Microsoft BitLocker Administration and Monitoring (MBAM) installed in your environment, you need to specify the URL to the MBAM Administration Service and the account to access the MBAM Administration Service in the activity settings to enable Password Manager to use MBAM.

If you use MBAM with Password Manager, when retrieving BitLocker recovery keys, Password Manager will be able to verify that the user is associated with the computer for which the recovery key is retrieved. If the user is associated with this computer, the recovery key will be issued, otherwise, the user will not be allowed to get the recovery key.

Provide product feedback

You can provide product feedback from the Password Manager Web Interface. On the title bar of the Password Manager Web Interface, click feedback button at the upper right corner to provide product feedback. You are redirected to a new browser that allows you to provide feedback.

Notification Activities

All 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 160.

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.

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

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

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

Table 4: Email notification parameters

Parameter	Description	Example
#PRODUCT_NAME_FULL#	Full name of the software product. The parameter value is a constant.	Password Manager
#PRODUCT_NAME_SHORT#	Short name of the software product. The parameter value is a constant.	Password Manager
#COMPANY_NAME_FULL#	Full name of the company. The parameter value is a constant.	Password Manager
#COMPANY_NAME_SHORT#	Short name of the company. The parameter value is a	Password Manager

Parameter	Description	Example
	constant.	
#PRODUCT_NAME_SHORT_CUSTOM#	Customized short name of the software product. The parameter value can be manually set by the administrator.	Password Manager [Custom name]
#USER_ACCOUNT_NAME#	User's sAMAccountName.	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 e-mail 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 distin-guish 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
#USER_DOMAIN_NAME_LONG#	Fully qualified name of the domain that a user belongs to.	corp.contoso.com
#USER_DOMAIN_ALIAS#	Alias of a managed domain specified by an administrator.	My domain
#USER_IP#	User's IP address.	191.168.1.0
#OPERATOR_ACCOUNT_NAME#	User name of a	corp\JDoe

Parameter	Description	Example
	helpdesk operator in the following format: <domain name>\<user name>.	
#OPERATOR_IP#	Helpdesk operator's IP address.	172.16.254.1
#WORKFLOW_NAME#	Name of the workflow that was executed. All workflow names are available on the Administration site.	Forgot My Password
#WORKFLOW_RESULT#	Result of a workflow execution displayed on the status page of 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 others.
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 self-service workflow to notify users about errors occurred in a workflow. For example, to notify a user an error occurred during password reset, use this activity in the **Forgot My 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 e-mail 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 e-mail 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.

The following helpdesk workflows are available:

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

All available workflows are preconfigured and ready to use.

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.

Assign Passcode

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

The default configuration of this workflow is the following:

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

Reset Password

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

The default configuration of this workflow is the following:

1. Authentication Methods.
2. Reset password in Active Directory.
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 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.

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.

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.

Helpdesk Activities Overview

All 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 Register.

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: Note, 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 are not stored using reversible encryption. To store answers using reversible encryption, select the corresponding option in the Q&A profile settings.

NOTE: By default, the answers on the **Verify User Identity** page are not displayed. To display the answers, you can clear the **Hide my answers for security purposes** checkbox on the **Verify User Identity page**.

- **Answers to the specified questions (user's answer is 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.

  NOTE: By default, the answers on the **Verify User Identity** page are not displayed. To display the answers, you can clear the **Hide my answers for security purposes** checkbox on the **Verify User Identity 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, please contact One Identity Software Support to obtain the necessary license at https://support.oneidentity.com/.

Before enabling phone-based authentication, make sure that users' phone numbers stored in Active Directory are in a 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

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

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

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

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

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

This activity has the following settings:

- **Defender Server**: Specify the IP address of the computer running the Defender Server.
- **Port number**: Type the port number that the Defender Access Node uses to establish a connection with the Defender Server.
- **Server timeout**: Specify Defender Server timeout (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

Action Activities

This section describes activities that provide core actions of the helpdesk workflows, such as Reset password in Active Directory, Unlock account, etc.

Reset Password in Active Directory

This is a core activity of the **Reset Password** workflow. The activity allows helpdesk operators to reset user passwords in Active Directory only. If you want to enable helpdesk operators to reset passwords in several systems, configure the **Reset password in connected systems and Active Directory** activity. For more information on configuring this activity and using One Identity Quick Connect Sync Engine, see Reset Password in Active Directory and Connected Systems on page 132.

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. Password history is defined for a domain through Group Policy settings.

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

- Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, it is advised that you double the password history value for all managed domains.
- Having entered a new password that is not policy compliant, users may end up with a randomly generated password they don't know.

Reset Password in Active Directory and Connected Systems

Using this activity, you can configure Password Manager to use One Identity Quick Connect to reset passwords in connected systems. If used in conjunction with Quick Connect, Password Manager 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 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 to use a Quick Connect server for cross-platform password synchronization, you must do the following in Quick Connect:

- Create a connection to the Active Directory domains managed by Password Manager.
- Create connections to the systems you want Password Manager to synchronize passwords with.
- Map users from the managed domains 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 Active Directory 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.

   You can use either pre-Windows 2000 logon name (such as DomainName\UserName) or User Principal Name (such as UserName@DomainName.com) to specify the user name.
4. Specify how you want Password Manager 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 the Active Directory domain. No warnings are displayed if Quick Connect server is not available.
   - **Alert users and allow them to reset passwords only in Active Directory.** Helpdesk operators are notified that other connected data sources are temporarily unavailable, and are allowed to continue managing users' passwords only in the Active Directory domain.

- **Do not allow users to reset passwords.** Helpdesk operators cannot perform any password management tasks in the Active Directory domain and in 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 Active Directory.** Select this option to allow helpdesk operators to reset users' passwords in a connected system independently from Active Directory.
   - **Do not allow resetting password in this system independently from Active Directory.** Select this option to prevent helpdesk operators from resetting users' passwords in a connected system independently from Active Directory. 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 Active Directory. If the user' password is not reset in Active Directory, 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 Active Directory domains 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. Password history is defined for a domain through Group Policy settings.

   IMPORTANT: Before selecting this option,you should consider the following by-design behavior of Password Manager when that the Enforce password history option is enabled:
   - Password Manager uses two slots from the password history every time a password is reset. For example, if the password history value defines that users cannot reuse any of the last 10 passwords, then Password Manager checks only the last five passwords. Therefore, it is advised that you double the password history value for all managed domains.
   - 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 Active Directory.
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** 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 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.

Select the **Generate Passcode and send it in SMS** checkbox to send the passcode via SMS or select the **Generate Passcode and send it in e-mail** to send the passcode in e-mail to the user's device to authenticate on the Password Manager self-service site.

NOTE: To select **Generate Passcode and send it in SMS**, you must have a valid license with telephone verification. To select **Generate Passcode and send it in e-mail**, you must configure at least one SMTP server.

Unlock Q&A Profile

This activity is a core activity of the **Unlock Q&A Profile** workflow. It allows helpdesk operators to unlock users' Questions and Answers 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.

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 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 160.

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.

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

You can customize email notification messages distributed by Password Manager to meet specific requirements in your organization. The notifications are sent either in plain text or as HTML.

To modify user email notifications

1. Open the user notification activity included in the workflow.
2. Select either to customize the e-mail 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 e-mail 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 e-mail address of the administrator you want to receive notifications.

User Enforcement Rules

User enforcement rules allow you to force users to create and update their Q&A profiles and notify users about password expiration. Password Manager offers three user enforcement rules: **Invite users to create/update Q&A profiles**, **Remind users to create/update Q&A profiles**, and **Remind users to change password**.

Invite Users to Create/Update Profiles

By using this user enforcement rule you can configure Password Manager to invite users to register with Password Manager or update their Questions and Answers profiles. If you configure this enforcement rule, users will be notified by email.

The notification schedule is defined by the Invitation to Create/Update Profile scheduled task. Note that notification starts only after this scheduled task has run. For more information on the scheduled tasks, see Scheduled Tasks on page 163.

IMPORTANT: 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 Profiles**, and 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*>/PMAdmin/.

   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 **User 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 5: 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 6: User notifications

Option	Description
User is not registered with Password Manager	Select to force users to register with Password Manager by creating Q&A profiles, if users are not registered with Password Manager.
The question user answered to register was modified or deleted	Select to have users update their Q&A profiles if one or more questions which users answered to register were modified or deleted.
User's Q&A profile contains fewer questions than required for registration	Select to have users update their Q&A profiles if you have added one or more questions required for registration, thus making the list of such questions longer than it was before users' profiles were last updated.
User's answers are shorter than required	Select to have users update their Q&A

Option	Description
	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.

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 160.

Remind Users to Create/Update Profiles

The 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 Profiles**, and then click **Enable**.

To configure this enforcement rule, you must specify a user scope and the required number of 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*>/PMAdmin/.

   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 **User Enforcement Rules** section and click **Remind 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 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**.

Option	Description
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*>/PMAdmin/.

   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 **User 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. Select the condition for applying this enforcement rule. Use the **User is not registered and not invited to create Q&A profile** option to apply this rule to users who are not registered with Password Manager and have not been invited to create Q&A profile. Select the **User was invited to create/update Q&A profile N days ago** option and enter the required number of days to apply this enforcement rule to users who were invited to register with Password Manager or update their Q&A profiles the specified number of days ago.

   IMPORTANT: If you select the **User is not registered and not invited to create Q&A profile** option, such users will be immediately notified through a dialog box displayed on their desktop screens. The Reminder to Create/Update Profile scheduled task is not required to carry out such notification scenario. Use this option with caution when the number of users managed by Password Manager is large. Immediate enforcement of a large number of users may drastically decrease the performance of your production environment.

   IMPORTANT: If you select the **User is not registered and not invited to create Q&A profile** option, such users can be notified only with Secure Password Extension dialog box. Email notification option is not available for such notification scenario.

6. To configure email notification, select the **Notify users by email** check box. To configure notification by a dialog box, select the **Notify users via Secure Password Extension** check box. Click **Next**.
7. If you selected the **Notify users by email** check box, edit the notification template if necessary. Specify the following settings if required and click **Next**:

- 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 16 languages are available out of the box (English, Chinese (Simplified), Chinese (Traditional), Danish, Dutch, French, German, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Polish, Czech, Swedish).

8. If you selected the **Notify users via Secure Password Extension** check box, configure the postpone options that will be available to users on the notification dialog box: select check boxes with required time intervals and click **OK**.

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 the Administrator Guide.

NOTE: If the user does not create or update his Q&A profile in the specified number of days, you can disable the user account. For more details see Forced Enrollment.

Forced Enrollment

This option is used to force users to enroll to Password Manager. If users do not create or update their Q&A profiles after a series of reminders, their accounts will be disabled. They will receive the notification either by email or through the Secure Password Extension (notification dialog box). The accounts can be enabled with a customized Enable Account workflow.

Disable user account

To disable the user account after a series of reminders

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*>/PMAdmin/.

   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 **User Enforcement Rules** section and click **Remind Users to Create/Update Q&A Profiles**.
4. In the **Apply the following notification scenarios to users from the rule's scope** section, click **Add** to add a new notification scenario, or click **Edit** to modify an existing notification scenario.

5. In **Configure Notification Scenario** window, do the following:
6. Select the **User was invited to create/update Q&A profile N days ago** option and enter the required number of days within which the users have to create or update their Q&A profiles.
7. Select **Disable user account**.
8. Select **Notify users by email** check box to configure email notification, or select **Notify users via Secure Password Extension** check box to configure notification by a dialog box and click **Next**.
    - If you have selected the **Notify users by email** check box, edit the notification template if necessary. Specify the following settings if required and click **Next**:
        - 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 16 languages are available out of the box (English, Chinese (Simplified), Chinese (Traditional), Danish, Dutch, French, German, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Polish, Czech, Swedish).
    - If you have selected the **Notify users via Secure Password Extension** check box, configure the postpone options that will be available to users on the notification dialog box: select check boxes with required time intervals and click **OK**.
9. Click **Save**.

Enable User Account

You can enable the accounts disabled through forced enrollment, using a customized enable account workflow.

NOTE: The custom workflow must be executed only through Secure Password Extension or through mobile browsers. Because user login is restricted on workstation after disabling of the account.

To enable the account, use the following activities in the workflow:

1. Authenticate with password or any 2FA procedure such as Radius.

    NOTE: In the activity settings, you must select **Authenticate users with disabled accounts** check box to unlock and re-enable the disabled user accounts.

2. Edit Q&A profile

3. Enable account.

   NOTE: In the activity settings, you must select **Enable user accounts disabled by forced enrollment** check box to unlock and re-enable the disabled user accounts disabled through forced enrollment. If you do not select the check box, all the disabled user accounts in the organization are enabled.

4. Restart workflow if error occurs.

Remind Users to Change Password

By using this enforcement rule you can configure Password Manager to notify users about password expiration. If you configure this notification, users will be notified by email.

The notification schedule is defined by the Reminder to Change Password scheduled task. Note that notification starts only after this scheduled task has run. For more information on the scheduled tasks, see Scheduled Tasks on page 163.

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**, and 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 reminder

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*>/PMAdmin/.

   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 **User 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 8: 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.

Option	Description
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 160.

5

General Settings

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
- Domain connections

Search and Logon Options

By configuring the search and logon options you specify how users and helpdesk operators search for their accounts and log in on the Self-Service and Helpdesk sites.

You can also configure Password Manager to display CAPTCHA or reCAPTCHA V2 and allow or prohibit account search on the Self-Service site.

Configuring Account Search Options

To configure account 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*>/PMAdmin/.

   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 Options** tab, and configure the following options as required:

Table 9: Search and Logon options

Option	Description
Do not allow users to search for their accounts	Select this radio button to require users to enter either their logon names. Other user account attributes can be configured to Self-Service site or HelpDesk Site to find their accounts.
Show the domain list to allow users to select their domain	Select this check box to allow users to see the list of managed domains registered with Password Manager on the Self-Service site. If the domain list is

Option	Description
	displayed, users will be able to select the domain their accounts belong to. If you do not select this option and if several domains are registered with Password Manager, users will be required to enter their logon names in one of the following formats: johndoe@mydomain.com or MYDOMAIN\johndoe.
Users must enter their logon names for identification	If there are multiple managed domains registered with Password Manager and the domain list is hidden, the user must enter the logon name in one of the following formats: johndoe@mydomain or MYDOMAIN\johndoe. Otherwise, the user account will not be found. If there is only one managed domain or the domain list is displayed, then the user is required to enter only the username (for example, johndoe) and select the domain from the list.
Users must enter the following user account attribute for identification (this may slow down the performance)	Select this option to require users to search for their accounts by using the specified attribute of user account in Active Directory. In the text box under the radio button, enter the attribute name. For example, you can use the attribute email to require users to enter their emails to search for accounts on the Self-Service site.
Allow users to search for their accounts	Select this radio button to allow users to perform account search by using the locate account functionality of the Self-Service site. Users can enter their first or last name, or email address to find their accounts. By selecting this option, you can specify the number of user accounts that are displayed in search results. To do this, specify the required number in the "Number of users to display in search results" field.

Option	Description
Allow user search from external network	Select the check box to allow user searching capabilities on Self-Service Site from an external network or unselect the check box to disable searching capabilities on Self-Service Site from an IP address not specified in the defined **Corporate IP Address Ranges**. For more information on specifying a defined **Corporate IP Address Ranges**, see Location sensitive authentication For more information on how a user search works on the external network, see Partial user search on external network If **Allow user search from external network** check box is unchecked and corporate range in not configured, by default, every network is treated as an External network until it is defined under **Corporate IP Address Ranges**. Hence user search behaves as though the user site is accessed from external network.
Search in multiple domains	Select this option to enable users to search for their accounts in all domains registered with Password Manager.
Automatically show available self-service tasks if only one account is found	Select this option to automatically open the Home page of the Self-Service site for the user if only one user account matching the search criteria is found.
User account attributes to display in search results	Select check boxes next to the user account attributes that you want users to view in search results. You can select any of the following attributes: • First name • Initials • Last name • Name • Full name

Option	Description
	• User logon name • E-mail

3. Click **Save**.

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 un-checked, the application would still display the self-service tasks for certain users based on the below mentioned criteria:

- Users can reach **Dashboard** page only when the search criteria exactly matches with the search results.
- If the user name to be searched is part (substring) of another username, Search Results get listed only for the single user, based on the exact match.
- If the user name to be searched is part (substring) of multiple usernames, Search Results show "No accounts matching your search criteria have been found. Check the information you entered and try again".

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." even though 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" 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 Settings

The One Identity Password Manager Administration Site offers several security options under **General Settings** > **Search and Logon Options** > **Security Settings**. Use these options to:

- Enable or disable showing security-sensitive user information on the Password Manager Self-Service Site. For more information, see Hiding the domain user name on the Self-Service Site.
- Enable or disable showing the personally identifiable information (PII) for the currently logged in user. For more information, see Hiding personally identifiable information for logged-in users.
- Enable or disable CAPTCHA or reCAPTCHA checks to prevent bot attacks. For more information, see Configuring anti-bot security settings.

Hiding the domain user name on the Self-Service Site

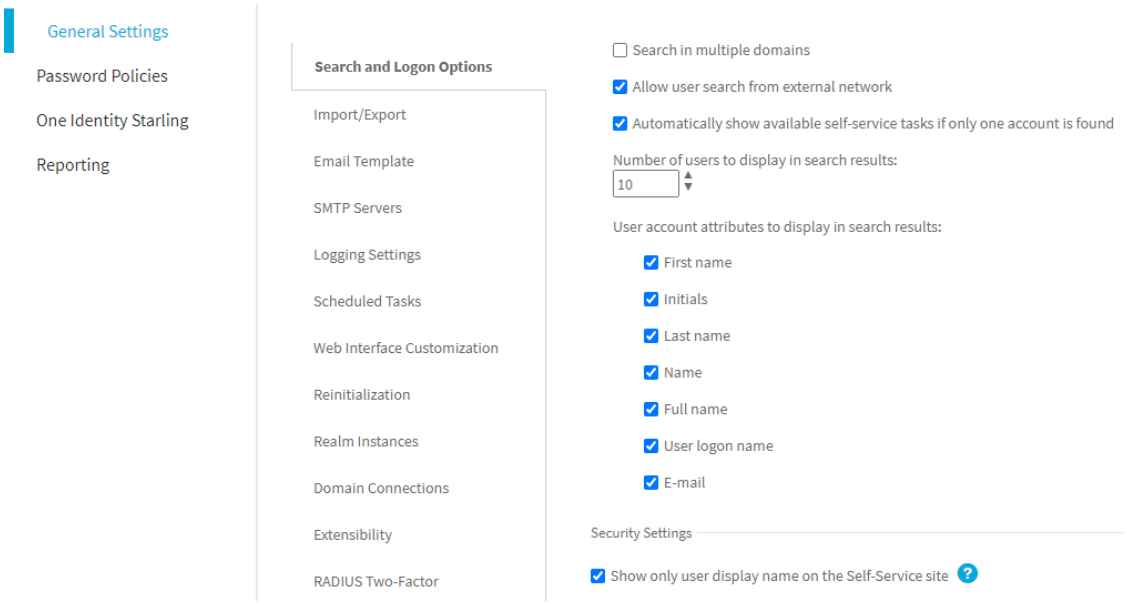
By default, the toolbar and the logout pop-up of the Self-Service Site display both the display name and the domain user name of the logged-in user (in the `<User Display Name> <domain>\<username>` format). For example:

```
Sam Smith (domainname\SSmith)
```

If the security policies of your organization require hiding security-sensitive information (such as the user logon name), you can change this so that the Self-Service Site will show only the user display name (for example: `Sam Smith`), but not the domain user name.

To hide the domain user name of the logged-in user on the Self-Service Site

1. In the Password Manager Administration Site, navigate to **General Settings** > **Search and Logon Options**.
2. Scroll down to **Security Settings**.
3. Enable **Show only user display name on the Self-Service site**.



4. To apply the changes, click **Save**.

Once you are ready, logging in next time to the Self-Service Site with any user will display only the user display name of the logged in user.

Hiding personally identifiable information for logged-in users

By default, the toolbar and the logout pop-up of the Self-Service Site display both the display name and the domain user name of the logged-in user (in the `<User Display Name> <domain>\<username>` format). For example:

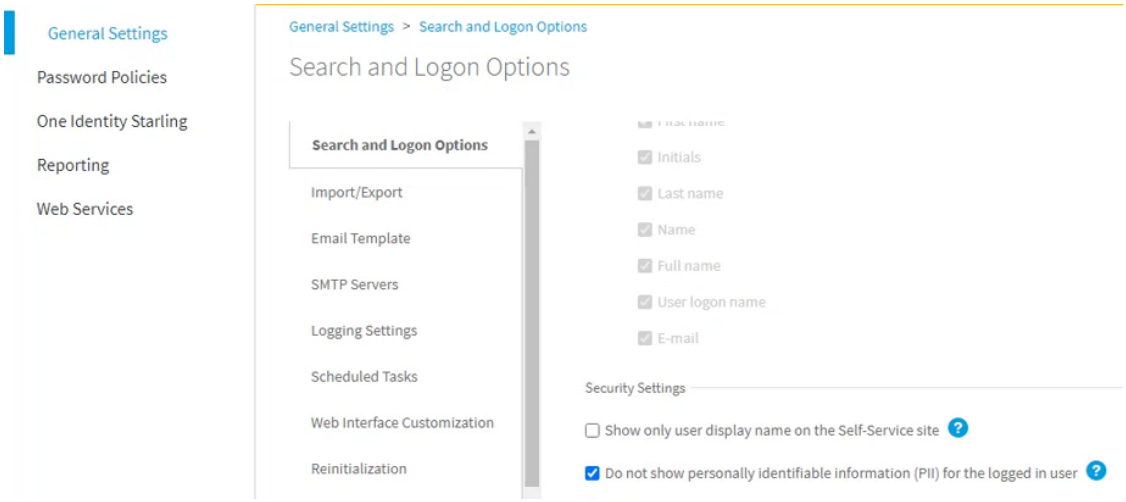
```
Sam Smith (domainname\SSmith)
```

If the security policies of your organization require hiding personally identifiable information (PII) on the user interface, you can configure Password Manager to truncate PII on the Self-Service Site, for example as:

```
S** S**** (domainname\S*****)
```

To hide PII on the Self-Service Site for the logged-in users

1. In the Password Manager 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 following options (also configured on the **General Settings** > **Search and Logon Options** page):

- 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** setting also selected will truncate both the user display name and the domain user name (with the exception of the domain name). For example, `Sam Smith (domainname\samsmith)` will be truncated as:

  `S** S**** (domainname\s*******)`

- Truncating PII with the **Show only user display name on the Self-Service site** option also selected will show only the truncated user display name. For example, `Sam Smith` will be truncated as:

  `S** S****`

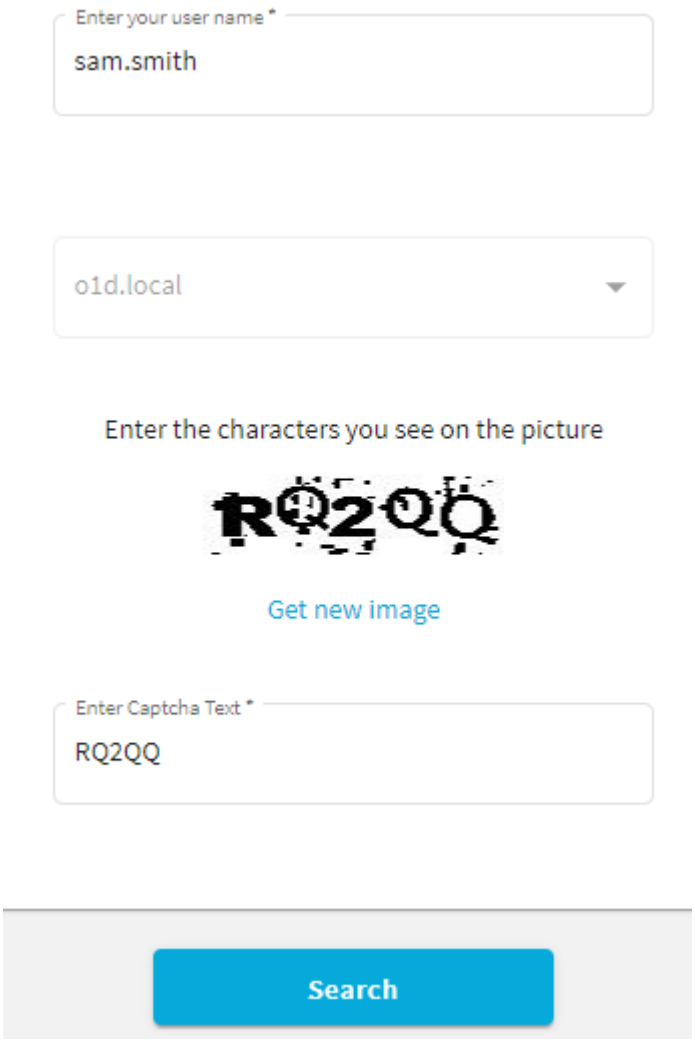
Configuring anti-bot security settings

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

- For more information on configuring CAPTCHA, see Configuring CAPTCHA security images.
- For more information on configuring reCAPTCHA, see Configuring reCAPTCHA security settings.

Configuring CAPTCHA security images

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



To configure CAPTCHA images for the Self-Service Site

1. In the Password Manager 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 One Identity Password Manager Self-Service Site to include reCAPTCHA anti-bot protection. Password Manager supports the reCAPTCHA v2 and v3 engines.

NOTE: Password Manager 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 Self-Service Site, make sure that the following conditions are met:

- The server running Password Manager 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 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 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 generated on the Google reCAPTCHA Admin site.

- **Secret key**: Enter the secret key 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 actual site traffic.

  NOTE: This setting is available only for reCAPTCHA v3.

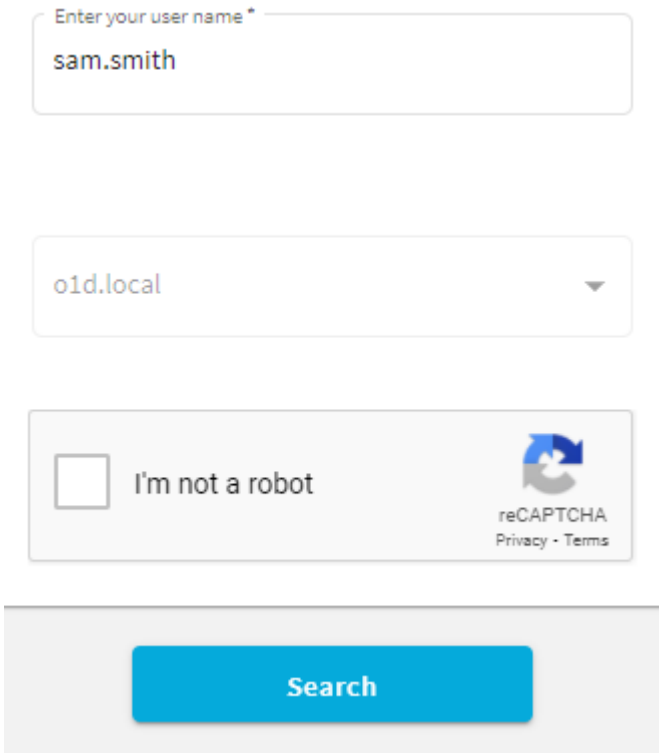
When ready, click **OK**.

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.

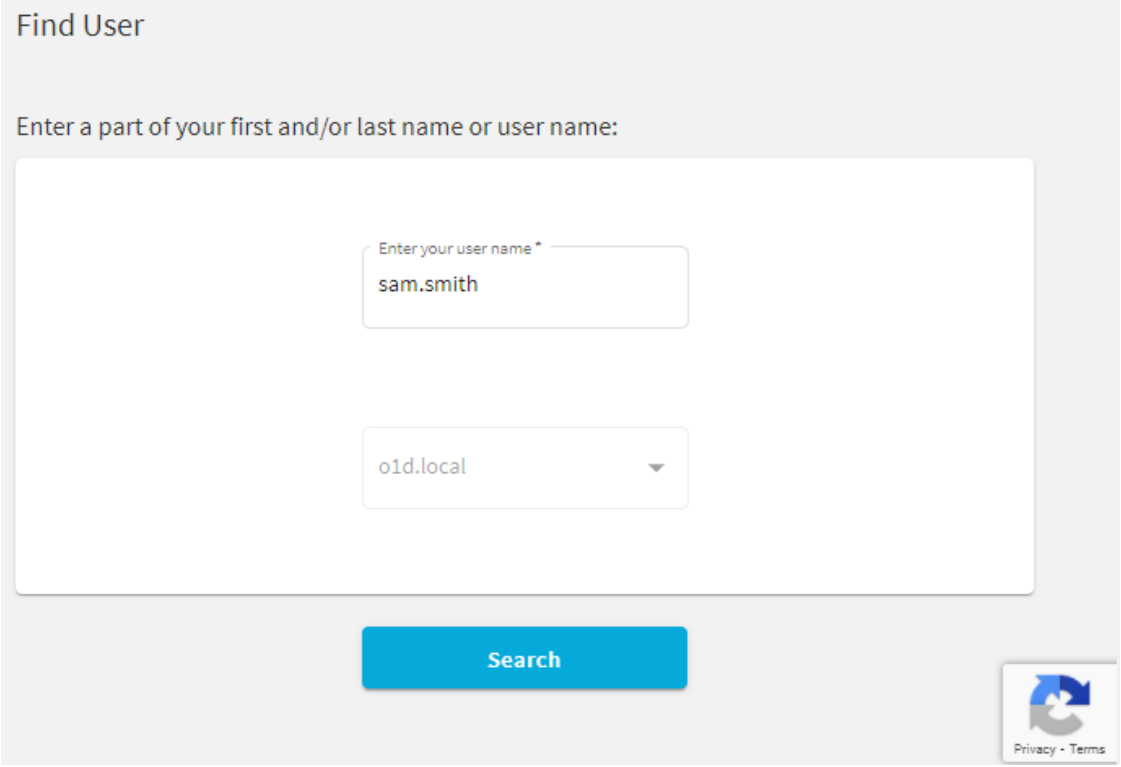
   TIP: Enable this setting for an increased protection against bot attacks.
7. To apply your settings, click **Save**.

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.



- If reCAPTCHA v3 is configured, the reCAPTCHA widget appears at the bottom right corner of the screen.



Import/Export Configuration Settings

You can export and import the configuration settings of Password Manager instance. You can export the configuration to a configuration file to back up the instance or create replicas of the existing instance. You can import the configuration to join the current Password Manager instance to an existing realm.

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 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 instance and create a replica of this instance by importing the configuration settings. To learn more about creating Password Manager realms, see Installing multiple instances of Password Manager on page 18.

To export 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*>/PMAdmin/.

   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 and click **Export**.

   IMPORTANT: 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*>/PMAdmin/.

   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 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*>/PMAdmin/.

   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 10: SMTP server details

Option	Description
Server name	Type 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	Type the sender's email address.
This server requires authentication	Select if the SMTP server requires authentication.
User name	Type the user name under which Password Manager will access the SMTP server.
Password	Type the password for this account.
Confirm password	Re-type the password.
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, a error message is displayed. You can configure the subject text of the email by configuring the value of Resource Id, `"Admin.Scenario.Action.TestSMTP.Settings.TestEmail.Subject"` in the Admin.xml file.

5. Use the **Move Up** and **Move Down** buttons to change the order of the SMTP servers in the list.

   The order of the servers in the list specifies how Password Manager uses the servers to send notification mail messages. Password Manager will first attempt to use the servers at the top of the list.

To remove a server from the list of outgoing SMTP mail servers

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

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

2. On the **SMTP Servers** page, select the SMTP server you want to remove and click **Remove**.
3. On the menu bar, click **General Settings**, and then click the **SMTP Servers** tab.

Diagnostic Logging

Password Manager provides a simple and convenient way to collect the diagnostic information about the activity of Password Manager. Diagnostic logging is mainly intended to be used by support personnel for troubleshooting purposes.

To enable diagnostic logging in Password Manager

1. On the home page of the Administration site, click **General Settings**, and then click the **Logging tab**.
2. Configure the following options as required:

Table 11: Diagnostic logging options

Option	Description
Specify the path to the log file:	Type a path to the file 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.

3. Click **Save**.

   IMPORTANT: Do not enable verbose logging tracing for long periods of time. Verbose logging creates log files that can accumulate quickly. Always monitor available disk space when verbose logging is enabled.

Scheduled Tasks

When installing Password Manager, the Password Manager setup adds the following scheduled tasks on the computer where Password Manager is installed: Invitation to Create/Update Profile, Reminder to Create/Update Profiles, Reminder to Change Password, Active Directory Sites, Maximum Password Age Policy, update RADIUS server status, and User Status Statistics.

Invitation to Create/Update Profile Task

This task is used to enumerate users who are not registered with Password Manager or must update their Q&A profiles and send email notifications to such users. This task is applied to users who have not been invited to create or update their Q&A profiles.

The scope of this task corresponds to the scope of the Invite Users to Create/Update Q&A Profiles user enforcement rule.

To each user from the user scope, the task is applied only once. After a user has been invited to create or update his Q&A profile, the Reminder to Create/Update Profile task will be applied to this user.

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 138.

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*>/PMAdmin/.

   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. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.

5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

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 notification messages (email and/or Secure Password Extension notifications) 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 141.

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*>/PMAdmin/.

   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. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

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 145.

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*>/PMAdmin/.

   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. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

Active Directory Sites

This task is used to update Active Directory sites in the **Domain Connection** settings. Currently, it is a manual task where you specify the Active Directory sites in the domain connection settings by selecting the site in which you want Password Manager to replicate changes as soon as they occur in other sites. You can automate and schedule this task by using this option.

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*>/PMAdmin/.

   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 **Active Directory Sites** task.
4. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

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 the One Identity password policies, see Creating and Configuring a Password Policy on page 237.

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*>/PMAdmin/.

   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. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

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 (for instance, an Active Directory backup task) running at that time, we recommend that you reschedule the User Status Statistics task to run in off-peak hours. The User Status Statistics task is used to do the following:

- **Enumerating users for licensing purposes.** Password Manager is licensed for a specific number of user accounts enabled for management by Password Manager in all managed domains. 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, number of users required to register with Password Manager, and the number of users required to update profile. This information is collected for all the domains managed by a specific Password Manager instance and displayed on the Reports page of the Administration site.

The scope of this task corresponds to user scopes of all configured Management Policies.

To schedule this task

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

   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 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.

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 and archive the cleared records. 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>/PMAdmin/.

   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 instance to run the task.
11. Click **Save** to save all the settings, and schedule the task.

Environment Health Checker Task

This scheduled task is used to check the status of all domain controllers from all domain connections and select the best available domain controller for each connection.

For example, to connect to a managed domain "mydomain.com" three domain controllers can be used: domain controller (DC)1, 2 and 3; the best available domain controller is DC 1. By default, the best available domain controller is used to connect to the domain. If this domain controller becomes unavailable, the next available domain controller is automatically selected. For example, DC 2 is now used to connect to the domain. But if DC 1 becomes available again, the connection will not be automatically switched to DC 1. To switch back to DC 1, the environment health checker task should be run. This task checks the availability of domain controllers for domain connections, and selects the best domain controller for each connection.

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*>/PMAdmin/.

   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 **Environment Health Checker** task.
4. To enable the task select the **The task is enabled** check box.
5. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
6. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
7. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

8. Click **Save**.

To force the task to run earlier than scheduled, click the **Run now** link under the task.

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 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*>/PMAdmin/.

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

2. On the menu bar, click **GeneralSettings**, then click the **Scheduled Tasks** tab.
3. Click **Edit** under the **Update RADIUS server status** task.
4. From the drop-down list select one of the following options: **Run hourly**, **Run daily** or **Run weekly**.
5. Depending on the option selected above, specify the time and/or days of the week when this task should be run.
6. Under **Run the task on this Password Manager instance**, select the Password Manager server on which the task should be run.

   IMPORTANT: The task status can be viewed only on the Password Manager instance on which the task is scheduled to run.

7. Click **Save**.

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 Self-Service site. Hence, the transparent images may appear to be missing in the Password Manager Self-Service site.

Enabling Self-Service UI 5.11.0

The following options appear only in case of Inplace Upgrade and the clean installation of version 5.11.0 since inplace upgrade is the only upgrade which retains the Legacy Self Service site along with the Password Manager 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 onwards)

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 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 Self-service site (**Self Service UI 5.9.5 onwards**).

To replace product and company logos with custom images

1. On the home page of the Administration site, click **General Settings**, and 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**, and 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**, and 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 in 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**, and 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 Service and the Web sites (Self-Service and Helpdesk). By default, Password Manager 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 Service and Websites 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 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 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 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 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 uses Triple DES algorithm to encrypt data. Note, that 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 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.
- **CAUTION: 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.

- **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 uses SHA-256 hashing algorithm. Password Manager 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**.

Use one of the following methods to clear old hives from AD user objects.

To update users' Q&A profiles with new instance settings and clear old Q&A data for user objects in Active Directory

1. Run the Migration wizard from the Password Manager CD autorun window.
2. On the **Welcome** page, select the **Update users' Q&A profiles with new instance settings and clear old Q&A data for user objects in Active Directory** task.
3. On the next page, upload the configuration file you exported. Click **Browse** to select the file, enter the password generated while exporting the configuration file, and click **Next**.
4. On the **Select users** page, do one of the following and click **Next**:
    a. If you want to convert the Q&A profiles of users from the user scope of a Management Policy, select the required policy in the **Select Management Policy** drop-down box and click **Next**.
    b. If you want to convert the Q&A profiles of a user in a user group, select **The following groups**. To select groups, click **Add** and do the following:
        i. In the **Add Groups** dialog box, enter the group name, select the domain from the list and click **Search**.
        ii. Select the required groups in the list and click **Save**.
    c. If you want to convert the Q&A profiles of a user in an OU, select **The following OUs**. To select OUs, click **Add** and do the following:
        i. In the **Add OUs** dialog box, enter the OU name, select the domain from the list and click **Search**.
        ii. Select the required OUs in the list and click **Save**.
5. On the next page, do one of the following and click **Next**:
    a. Click Update Q&A profiles in test mode to update profiles in test mode. Use this mode to preview the result of updating profiles.
    b. Click Update Q&A profiles in production mode to update profiles in production mode.

NOTE: For production mode, select **Clear old Q&A data for user objects in Active Directory** checkbox to clear old user Q&A data.

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**.

Once 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 159.

Clear old Q&A data for user objects in Active Directory

1. Run the Migration wizard from the Password Manager CD autorun window.
2. On the **Welcome** page, select the **Clear old Q&A data for user objects in Active Directory** task.
3. On the Select users page, do one of the following and click **Next**:
    a. If you want to clear the old Q&A profiles of users from the user scope of a Management Policy, select the required policy in the **Select Management Policy** drop-down box and click **Next**.
    b. If you want to clear the old Q&A profiles of a user in a user group, select **The following groups**. To select groups, click **Add** and do the following:
        i. In the **Add Groups** dialog box, enter the group name, select the domain from the list and click **Search**.
        ii. Select the required groups in the list and click **Save**.
    c. If you want to clear the old Q&A profiles of a user in an OU, select **The following OUs**. To select OUs, click **Add** and do the following:
        i. In the Add OUs dialog box, enter the OU name, select the domain from the list and click **Search**.
        ii. Select the required OUs in the list and click **Save**.
4. On the status page, click **View the report for detailed information** to view a detailed account of updating profiles. Click **Finish**.

NOTE: The latest version of Q&A, which is currently in use will not be deleted.

Realm Instances

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

To open the Password Manager Service Instances page, on the Administration site click **General Settings.** On the **General Settings** page, click the **Realm Instances** tab.

For each Service instance the Self-Service site URL is specified. If necessary, you can edit the URL by clicking **Edit** under the corresponding Service instance. In Realm instances, the Primary instance is in red for easy identification.

All Password Manager Service instances belonging to one realm share the following settings: certificate name, port number, encryption algorithm, encryption key length, hashing algorithm, attribute for storing Q&A profile data, and realm affinity ID. These options are configured when initializing a Password Manager Service instance. To change any of these settings, see Instance Reinitialization on page 173.

A Redistributable Secret Management Service (rSMS) user must be created in all the Password Manager realm instances. An rSMS user is automatically created if the imported configuration file has the rSMS account details.

Domain Connections

This section provides information on creating, modifying, and using domain connections.

Using Domain Connections

On the **General Settings|Domain Connections** tab of the Administration site, you can view a list of available domain connections.

To register a domain with Password Manager you need to create a connection to the required domain. When adding a domain connection you can select an existing connection or create a new one. It is possible to use the same domain connection in different sections: user and helpdesk scopes, and password policies.

The same domain connection can also be used in different Management Policies.

You can add a domain connection either on the **Domain Connections** tab or from the User scope, Helpdesk scope, and Password Policies pages.

Note, that when you modify the domain connection on the User scope, Helpdesk scope or Password Policies pages, you can select how you want to apply the updated connection settings: either for the specified section only or everywhere where this domain connection is used. If you choose to update settings for the specified section only, a copy of the domain connection will be created with these settings and will be added to the list of available domain connections.

But when you modify the domain connection on the **Domain Connections** tab, the updated settings will be automatically applied everywhere where this connection is used.

If you want to remove the domain connection from the list on the **Domain Connections** tab, you should first remove it from all sections where it is used, and only then remove the domain connection from the list.

Specifying Access Account for Domain Connections

Before adding the domain connection, make sure the account you want to use to access the domain has the required permissions.

The following permissions must be granted to the account in case you want to add the domain to the user or helpdesk scopes:

- Membership in the *Domain Users* group
- The Read permission for all attributes of user objects
- The Write permission for the following attributes of user objects: *pwdLastSet*, *comment*, *userAccountControl,* and *lockoutTime*

- 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 domain objects
- The Write permission for the *gpLink* attribute of the *organizationalUnit* objects and domain 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 domain 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 Read permission for the *nTSecurityDecriptor* attribute of the *groupPolicyContainer* objects.
- 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.
- The Write permission for the following attributes of the *msDS-PasswordSettings* object:
    - msDS-LockoutDuration
    - msDS-LockoutThreshold
    - msDS-MaximumPasswordAge
    - msDS-MinimumPasswordAge
    - msDS-MinimumPasswordLength
    - msDS-PasswordComplexityEnabled
    - msDS-PasswordHistoryLength
    - msDS-PasswordReversibleEncryption
    - msDS-PasswordSettingsPrecedence
    - msDS-PSOApplied

- msDS-PSOAppliesTo
- name

To add domain connection

1. On the home page of the Administration site, click the **General Settings|Domain Connections** tab.
2. Click **Add domain connection** to add a domain connection.
3. If domain connections already exist, select a domain connection from the list. If you want to create a new connection, click **Add domain connection**.
4. In the **Add New Domain Connection** dialog, configure the following options:
    - In the **Domain name** text box, type in the name of the domain that you want to add.
    - In the **Domain alias** text box, type the alias for the domain which will be used to address the domain on the Self-Service site. This field is required because you can use the domain connection in the user scope.
    - To have Password Manager access the domain using the Password Manager Service account, click **Password Manager Service account**. Otherwise, click **Specified user name and password** and then enter user name and password in the corresponding text boxes. Note, that the selected account should have the required permissions.
5. Click **Save.**

    IMPORTANT: After you create a domain connection on the General Settings|Domain Connections tab, you can use it in the user scope, helpdesk scope and password policies by selecting the connection in the **Add Domain Connection** dialog on the corresponding page of the Administration site. For example, to use the domain connection in the user scope of your Management Policy, open the user scope of this Management Policy, click **Add domain connection**, and select the corresponding connection from the list.

Changing Access Account for Domain Connections

To change domain access account

1. On the home page of the Administration site, click the **General Settings|Domain Connections** tab.
2. Select the domain connection you want to modify and click **Edit**.
3. In the **Edit Domain Connection** dialog, select **Password Manager Service** account to have Password Manager access the domain using the Password Manager Service account. Otherwise, click **Specified user name and password** and then

enter user name and password in the corresponding text boxes. Note, that the selected account should have the required permissions.

4. Click **Save**. Note, that the updated settings will be applied everywhere where this domain connection is used.

Specifying Advanced settings for Domain Connection

After you have created a domain connection, you can specify advanced settings for the connection: domain controllers and Active Directory sites of the managed domain. For more information about domain controllers, see Domain Controller

To specify domain controllers

1. On the Administration site, click the **General Settings|Domain Connections** tab.
2. On the **Domain Connections** page, select the domain connection for which you want to specify domain controllers and click **Edit**.
3. On the **Advanced settings** tab of the **Edit Domain Connection** dialog, click **Add** under the domain controllers table and select required domain controllers, and click **Add**.
4. Click **Save.** Note, that the updated settings will be applied everywhere where this domain connection is used.

Active Directory Sites

By specifying Active Directory sites in the domain connection settings you select the site in which you want Password Manager to replicate changes as soon as they occur in other sites. This can reduce downtime that users may experience when your environment has several Active Directory sites and changes may not get immediately replicated between the sites.

For example, when users unlock their accounts on the Self-Service site, this operation may occur in one site. But when they attempt to log in to their computers, this operation may occur in another site, to which the information about the unlocked account has not been replicated yet. In this case, users will not be able to log in until the information is replicated to the second site. To mitigate this issue, select the Active Directory sites in which you want to replicate changes immediately in the domain connection settings.

Note, that you cannot force replication of changes related to password policies. Such changes are replicated by Active Directory.

To specify Active Directory sites

1. On the Administration site, click the **General Settings|Domain Connections** tab.
2. On the **Domain Connections** page, select the domain connection for which you want to specify domain controllers and click **Edit**.
3. On the **Advanced Settings** tab of the **Edit Domain Connection** dialog, click **Add** under the Active Directory sites table, select required sites, and click **Add**.
4. Click **Save.** Note, that the updated settings will be applied everywhere where this domain connection is used.

Changes propagation

After you specify the Active Directory sites in which you want to push changes, you can also select what kind of changes to propagate. The following options are available:

- Propagate changes related to the user's account in Active Directory
- Propagate changes related to the user's Questions and Answers profile
- Propagate password-related changes

Propagating account-related changes

Select this option to propagate information about unlocking and enabling user accounts in Active Directory. It is recommended to use this option when a managed domain has users in multiple Active Directory sites.

Propagating Q&A profile-related changes

Select this option to propagate information about editing, locking and unlocking Questions and Answers profile, and passcodes issued by Helpdesk. It is recommended to use this option when users and Password Manager Service use domain controllers from different sites. In this case, if users update their Q&A profiles using Secure Password Extension (via the domain controller in one site), and then attempt to use the profiles on the Self-Service (via the domain controller in another site), they may encounter the issue when the updated Q&A profile is not yet available because of intersite replication latency.

Propagating password-related changes

Select this option to propagate information about changing or resetting user password. For more information, see Propagating password-related changes on page 29.

Removing a Domain Connection

To remove a domain connection

1. On the Administration site, click the **General Settings|Domain Connections** tab.
2. On the **Domain Connections** page, select the domain connection you want to delete and click **Remove**. Note, to permanently remove the domain 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 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 94 and refer to the Password Manager SDK.

Built-in web service allow 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 execute a workflow and to interfere in a workflow execution process. For more information refer the Password Manager SDK.

Custom web services allow you to further extend the Password Manager functionality and enable scenarios that cannot be implemented using 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 more information refer the Password Manager 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 92 and Importing and exporting custom activities on page 96.

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. RADIUS Two-Factor Authentication uses one-time passwords to authenticate users on the Self-Service site and Helpdesk site.

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

To configure RADIUS Two-Factor Authentication

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

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

2. Click **Add RADIUS server** to add a new RADIUS server for authentication.

   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 on page 131.

Working with RADIUS servers

You can create two RADIUS servers to authenticate users on the Self-Service site and Helpdesk site through RADIUS Two-Factor authentication.

To configure RADIUS Two-Factor Authentication in Password Manager, you have to configure the RADIUS server details in Password Manager. For more information on creating and configuring a RADIUS server, see RADIUS Two-Factor Authentication.

To swap RADIUS servers

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

   The **RADIUS Two-Factor Authentication** page is displayed along with the primary and secondary servers.
2. Click **Interchange RADIUS servers** to swap the priority of the RADIUS servers between primary and secondary priority.

To modify RADIUS servers

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

   The **RADIUS Two-Factor Authentication** page is displayed along with the primary and secondary servers.
2. Click the modify icon to modify the properties and attributes of RADIUS servers.

NOTE: The status of the RADIUS server is periodically scanned every 5 minutes.

To disable RADIUS servers

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

   The **RADIUS Two-Factor Authentication** page is displayed along with the primary and secondary servers.
2. Click **Disable** to disable a RADIUS server.
3. A message is displayed to confirm, click **Disable**.

   The server is disabled.

   NOTE:
   - On disabling a RADIUS server, the other RADIUS server by default becomes the primary server.
   - You can enable a server that was disabled earlier.

To delete RADIUS servers

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

   The **RADIUS Two-Factor Authentication** page is displayed along with the primary and secondary servers.
2. Click **Delete** permanently delete the RADIUS server.
3. A message is displayed to confirm, click **Delete**.

   The server is Deleted.

During a workflow execution, the ping to the RADUIS server to check the status of the RADIUS server is temporarily interrupted. The status check continues after the authentication process in the workflow is completed successfully.

For more information, see Authenticate with RADIUS Two-Factor Authentication on page 131.

Password Manager components and third-party applications

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

Password Manager Secure Token Server

Password Manager Secure Token Server (STS) is installed with Password Manager version 5.10.0. You can configure STS to use internal or external providers with optional Multi-Factor Authentication (MFA).

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 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.

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 Manger STS account restrictions

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

Using STS features in a Password Manager realm

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

Using Certificate to protect STS configuration

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

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

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

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

NOTE: The specified certificate must be valid, trusted and it must exist in the Local Computer's certificate store. It must have a private key. Access to the private key must be

granted to the service account that is running the Password Manager Secure Token Server Windows Service. The private key must be an RSA key, of any length. A certificate with an ECC key is not supported.

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

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

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

If Password Manager STS settings are not replicated automatically

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

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

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

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

Configuring Password Manager Secure Token Server

Before the first visit of STS settings, you need to have a binding for your Password Manager site in IIS with the same port that is present in the `<Password Manager installation folder>\One Identity\Password Manager\Service\QPM.Service.Host.exe.config` under the `StsHttpsPort` key. By default **`20000`** is used.

To start using Password Manager STS,

1. Open the IIS manager and create an HTTPS binding with this port for Password Manager sites.
2. On the home page of the Administration site, click **General Settings** > **Secure Token Server**. The **Secure Token Server** page is displayed.

3. To change the Password Manager STS settings, if you are prompted to enter RSTS client secret, provide the password. The default password is **admin**.

   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. To change the Password Manager STS settings, if you are prompted to enter RSTS client secret, provide the password.
3. Navigate to **Server Settings** > **Listening Ports**.
4. In the **HTTPS Port** field, enter the port that is the same as the HTTPS port of the website binding in IIS.
5. In the **SSL Certificate** section, select the certificate that is the same as the HTTPS certificate of the website binding in IIS.
6. To save your settings, click **Save**.
7. Refresh the page.
8. Follow the instructions in the **Secure Token Server error** popup window.
9. Enter your modified port number in the text field. To create or modify a firewall rule, select **Create firewall rules for the port automatically**.
10. To save your settings, click **Save**.
11. Open the Registry Editor and modify the `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PasswordManagerSTS@ImagePath` key value. At the end of the string, change the value of `https-port` to the modified port number.
12. Modify the port number of the HTTPS binding in IIS for your Password Manager site.
13. Restart the Password Manager service and the Password Manager STS service.

To set authentication providers,

1. On the home page of the Administration site, click **General Settings** > **Secure Token Server**. The **Secure Token Server** page is displayed.
2. To change the Password Manager STS settings, if you are prompted to enter RSTS client secret, provide the password.
3. Navigate to **Authentication Providers**, then click **Add Authentication Provider**, or select an existing one to edit by clicking on its name.
4. In the **Display Name** field, enter the name of the current provider. It is only displayed on the administration site.

5. Follow the instructions of this page to specify the **Directory Type**, the **Connection Information** and the **Authentication Schemes** for the current authentication provider.
6. Follow the instructions of this page to specify the Two Factor Authentication Settings for the current authentication provider. Your options are the following:
    - **None**
    - **OneLogin MFA**
    - **RADIUS**
    - **FIDO2/WebAuthn**
    - **Duo Web iFrame**

    To validate and save your settings, click **Finish**.

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. To change the Password Manager STS settings, if you are prompted to enter RSTS client secret, provide the password.
3. Navigate to **Server Settings**.
4. You can edit the **Issuer Name** that will be used by the STS server to identify itself to relying party applications.
5. You can change the **Administration Password** for STS settings. Note: Every time you change this password, you need to revisit **General Settings** > **Secure Token Server** page and provide the new password in the popup window.
6. You can edit general STS server wide settings in **General Settings**.
7. You can set the HTTPS port that the STS service will use to accept incoming requests from relying party applications in Listening Ports. Also, choose an available SSL certificate to be used for HTTPS requests.

    NOTE: Every time you change the port and/or the certificate, you need to revisit **General Settings** > **Secure Token Server** page and follow the instructions on the popup window.
8. You do not need to specify any login page image under **Login Page Images**, it will not be displayed.
9. If you have an authentication provider which uses OneLogin you can set a proxy server in **Proxy Settings** to be used with OneLogin communication.

NOTE: To be able to use STS features, you do not need to create an application in **Applications** of the **Secure Token Server Home page** for Password Manager.

Provider-specific informations: Duo

In the Duo admin interface you need to create a Web SDK type application to connect with Password Manager STS.

Unregistering users from Password Manager

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

To unregister a user from the Password Manager

1. On the home page of the Administration site, click **General Settings | Unregister Users**.
2. On the **Unregister Users** page:
    - If you want to unregister individual users, expand the **Select Users** tree, click **Add**, manually search for the individual user, select the required user from the results, and click **Save**.
    - If you want to select a user group, expand the **Select Groups** tree, click **Add**, manually search for the individual groups, select the required group from the results, and click **Save**.
    - If you want to select the entire organization unit (OU), expand the **Select Organizational Units** tree, click **Add**, manually search for the individual OU, select the required OU from the results, and click **Add**.
3. Click **Unregister User** to unregister the users.

NOTE:

- If you want to run the task at a specified time, select the **Schedule at** check box to specify the 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 Write permissions are available to the storage attribute of the security questions (comment, by default) for all the users/ groups/OUs that are configured to be unregistered.
- If the users/ groups/ OUs that need to be unregistered are a member of DomainAdmins/ Administrators group in the Active Directory then, the Write Permissions are already inherited.

Bulk Password Reset

Use the Bulk 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 Password Reset**.
2. On the **Bulk 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 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.

Working with Redistributable Secret Management account

Redistributable Secret Management Service (rSMS) can be used to manage user passwords across multiple connected systems. Using the rSMS service it is possible to quickly synchronize the passwords across connected systems. By default, the rSMS service is installed with the Password Manager software.

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 the certificate binding settings (optional), you can configure the settings to reset the password in connected systems. For more information, see Reset password in connected systems through embedded connectors.

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. If the certificate binding settings are modified you must restart the One Identity rSMS Service.

   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 are 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 a custom certificates, custom port number can be provided.

6. Click **Save Settings** to save the certificate binding settings.

   NOTE:

   - By default, all Password Manager logs are available in `C:\Windows\TEMP` folder. If the default Password Manager log path is changed during an update, rSMS automatically uses the updated log path instead of the default path used earlier.
   - Additional rSMS logs are available in the `rSMS.Service-{Date}.log` file. Enable Password Manager logging from the Administrator site under **General Settings | Logging Settings**.

Redistributable Secret Management Service supported platforms

Redistributable Secret Management Service (rSMS) supports the platforms that are mentioned here.

Table 12: rSMS supported platforms

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 Admin site is installed, click **Start** and then **Services**.
2. On the **Services** window, right-click on **One Identity rSMS Service**.
3. Select **Properties** and check the location from the **Path to executable** section.
4. Open the command prompt with administrator privileges and navigate to the directory where **One Identity rSMS Service** is installed.
5. From the directory where **One Identity rSMS Service** is installed, run the `rSMS.Config.exe LogPath` command to view the rSMS log path.

   The log path currently used to record rSMS logs is displayed.
6. To update the log path, run the `rSMS.Config.exe LogPath -f <new path>` command. For example, `rSMS.Config.exe LogPath -f C:\PM`.

The log path is updated. To confirm the log path run the `rSMS.Config.exe LogPath` command again.

7. Restart the **One Identity rSMS Service**.

Email Templates

Password Manager provides 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**, and 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** box, 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

6

Upgrading Password Manager

Upgrade Requirements

Before you start the upgrade process, follow this checklist to ensure you have made the necessary preparations and met the essential upgrade requirements.

Table 13: Upgrade checklist

Step	Comment
Back up the current configuration by doing one of the following: • Export the configuration file using the **Import/Export** option in **General Settings** and import the same file after the upgrade. • Create a copy of the **ProgramData** folder in the **C:\ProgramData\One Identity\Password Manager** for future reference.	UI customizations will be lost during upgrade. Follow the steps to save the configuration. For more information on saving the configuration, see Import/Export Configuration Settings on page 159.
Ensure that you installed or upgraded the third-party redistributable packages required for the latest version of Password Manager.	

Step	Comment
Ensure that you know the user name and password for domain management accounts.	For more information on what permissions are required for a domain management account, see Configuring Permissions for Domain Management Account on page 23.
Ensure that Password Manager Service account is a member of the Administrators group on the Web server where Password Manager is installed.	
Ensure that in IIS 7.0 or later, application pool identity account is a member of the IIS_IUSRS local group. This account must also have permissions to create files in the *<Password Manager installation folder>*\App_Data folder.	
Ensure that you know the user name and password for SQL database account.	That is needed only if Password Manager Service account is configured to use special SQL account (different from Password Manager Service account) to access the SQL database.
Ensure that the account, that is used to upgrade Password Manager, is a member of the local Administrators group on the server where you upgrade the product.	
Ensure that the account, that is used to upgrade Password Manager, is a member of the database creators (db_creator) fixed role on the SQL server hosting the Password Manager configuration database.	

About Secure Password Extension

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

Secure Password Extension is included on the installation CD and is deployed through Group Policy. For information on how to deploy and configure Secure Password Extension on end-user workstations in the managed domain, see Deploying and Configuring Secure Password Extension on page 218.

IMPORTANT: Secure Password Extension may be deployed on different workstations by applying different GPOs. This allows you to not upgrade Secure Password Extension on all the workstations at one time, but do it in several steps depending on your needs and preferences.

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

IMPORTANT: By default, Secure Password Extension uses the URL of the Self-Service site installed on the computer where Password Manager Service runs. You can modify the URL on the General Settings|Realm Instances page of the Administration site.

To remove the existing and assign a latest-version package

1. Remove the assigned package (Quest Secure Password Extension x86.msi or Quest Secure Password Extension x64.msi) from the list of software to be installed.
2. Add the latest-version MSI packages to the list of software to be installed.

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

During upgrade of **prm_gina.admx** administrative template, the previously made template settings are preserved and picked up by newer versions.

Upgrading Multiple Instances of Password Manager

This step is optional. It should be performed only if you have installed multiple instances of Password Manager.

To upgrade multiple instances of Password Manager, you need to export the configuration settings from the first configured instance of Password Manager and then import the settings to other instances. You should upgrade all instances of Password Manager to the latest version.

To import configuration settings

1. Open the Administration site of the target instance.
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**.
5. Repeat steps 1-4 for other instances of Password Manager.

Upgrading Password Manager

This section briefs about the process to upgrade Password Manager to the latest version (5.11.0).

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 5.7.1 or later versions
- Running the Migration Wizard is not required while upgrading from Password Manager 5.7.1 or later versions to 5.11.0.
- If you are upgrading to 5.9.x, 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 should be manually merged with the workflow of the latest version of the Password Manager 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 5.11.0.
- To update storage files with new encryption mechanism, all realm instances must be updated with the Password Manager 5.11.0 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 5.11.0 configuration and encryption key.
- When all the realm instances are updated with Password Manager 5.11.0, 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 5.11.0
- Manual upgrade from 5.7.1 or later versions

To export configuration settings from Password Manager 5.7.1 or later versions

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*>/PMAdmin/.

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

2. On the left pane of the Admin site, 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 5.7.1 or later versions, you can uninstall it.

To uninstall Password Manager 5.7.1 or later versions

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

After you uninstall Password Manager 5.7.1 or later versions, install Password Manager 5.11.0 on the same computer. All configuration settings will be automatically detected by the new version. For more information on how to install Password Manager, see Installing Password Manager.

If you have multiple Password Manager 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.

In-place upgrade from 5.8.2 or later versions to 5.11.0

1. From the autorun window of the installation CD, 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** ,and 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 5.7.1 or later versions

Uninstall Password Manager 5.7.1 or later versions, and then install Password Manager 5.11.0 on the computer where Password Manager 5.7.1 or later versions was installed. For more information, see To uninstall Password Manager 5.7.1 or later versions on page 202.

1. From the autorun window of the installation CD, 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**.
    a. To verify licenses information, click **Licenses...** and 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 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 5.7.1 or later versions on page 202.
- After you uninstall Password Manager 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 .
- If you have multiple Password Manager 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 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 5.11.0, the Self-Service site gets replaced as Password Manager Self-Service site. Hence, post Manual upgrade, you can see only one Self service site (Password Manager 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, Admin has to install it exclusively, in addition to the existing Password Manager Self Service site. In this case, point to note is that the Enabling Self-Service UI 5.11.0 (**Switch to Self-service site 5.9.5 onwards**) option will not be applicable.

Running the Migration Wizard

NOTE: In the **Shared.storage** file in **ProgramData** folder of primary instance, verify whether **AESEncryption** value is **true** in all hosts. After installing Password Manager 5.11.0 and importing the configuration file into secondary instances, replication from all PM instances takes time to update the hosts' information and to set **AESEncryption** value to **true**. If the **AESEncryption** value is not **true**, when you run the Migration Wizard 5.11.0, it displays the error message with the list of hosts which are not updated with Password Manager 5.11.0 configuration.

NOTE: Set **AESEncryption** value to **true** in all the hosts and run the Migration Wizard 5.11.0 under Password Manager Service account.

To run the Migration Wizard 5.11.0, see To update users' Q&A profiles with new instance settings and clear old Q&A data for user objects in Active Directory.

NOTE: In older version Password Manager, if you are using an existing database, after installing the Password Manager 5.11.0, disconnect SQL connection and reconnect with the same or a new database.

NOTE: After installing Password Manager 5.11.0, if service account has to be modified, see Modifying the service account .

Modifying the service account

NOTE: If you want to modify the service account after installing Password Manager 5.11.0, you cannot modify it by changing the account on Password Manager service because the new account will not be able to read the current configuration.

To modify the service account after installing Password Manager 5.11.0***:***

1. On the menu bar, click **General Settings**, then click the **Import/Export** tab and export the configuration file of the primary instance of Password Manager.

   NOTE: Due to security enhancements, a complex password is generated while exporting the configuration. You must remember the password or store it in a secure place, to use while importing the configuration.

2. Stop the Password Manager Service.
3. At the command prompt, type **services.msc** and select **Password Manager Service** in the console and change the log on details.
4. Start the Password Manager Service.

NOTE: Before you continue, it is recommended to back up the **One Identity** folder at **C:\ProgramData**.

5. Delete the One Identity folder at ***C:\ProgramData.***
6. Restart the computer.
7. Open the Administration site.
8. On the **Instance Initialization** page, select **Unique instance** and click **Save**.
9. On the menu bar, click **General Settings**, then click the **Import/Export** tab and import the configuration file, which was exported before changing the service account.

Converting Q&A Profiles

After you have configured Password Manager 5.11.0, you can convert users' Q&A profiles to make it compatible with the latest Password Manager version. To convert Q&A profiles, you must use the Migration Wizard.

When converting users' Q&A profiles, specify whether to convert profiles of all users belonging to the user scope, users in a specified group or users of a Management policy. You can also select whether to convert Q&A profiles in test or production mode.

IMPORTANT:

- Before converting users' Q&A profiles it is recommended to prevent users from accessing the Self-Service site. For more information, see To specify groups or OUs that are denied access to the Self-Service site on page 26.
- To avoid bad data error during user migration, run the migration wizard in test mode. View the report to check if the user information have been migrated successfully.

To convert Q&A profiles

1. On the computer where Password Manager is installed, run the Migration Wizard from the Password Manager autorun window. It is recommended to run the Migration Wizard under the Password Manager Service account.
2. On the **Welcome** page, select the **Convert users' Q&A profiles** task.
3. In the **Select management policy** drop-down box, select the Management Policy to convert Q&A profiles of users from its user scope and click **Next**.
4. On the second page, do one of the following and click **Next**:
   - Click **All users from the user scope** to convert Q&A profiles of all users from the user scope of the selected Management Policy.
   - Click **The following groups** to specify the groups of users whose Q&A profiles will be converted. To select groups, click **Add** and do the following:

- In the **Add Groups** dialog box, enter the group name, select the domain from the list and click **Search**.
- Select the required groups in the list and click **Save**.

5. On the third page, do one of the following and click **Next**:
   - Click **Convert Q&A profiles in test mode** to covert profiles in test mode. The existing profiles will not be replaced.
   - Click **Convert Q&A profiles in production mode** to convert profiles in production mode. All existing profiles will be replaced.
6. On the status page, click **View the report for detailed information** to view a detailed account of profile conversion. If you converted Q&A profiles in test mode, click **Convert Q&A profiles in production mode**.
7. Click **Finish** to close the wizard.

> IMPORTANT: After profile conversion, some users may not be able to edit their Q&A profiles. Such users will be able to reset their passwords and unlock accounts on the Self-Service site, but if they want to edit their Q&A profiles, they will be forced to create new Q&A profiles.
>
> If users' Q&A profiles have been skipped during profile conversion, such users will not be able to use Password Manager 5.11.0 until they create new Q&A profiles.

Upgrading Secure Password Extension

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

To remove the existing and assign a latest-version package

1. Remove the assigned package (Quest One Secure Password Extension x86.msi or Quest One Secure Password Extension x64.msi) from the list of software to be installed.
2. Add the latest-version MSI packages to the list of software to be installed.

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

During the upgrade of **prm_gina.admx** administrative template, the previously made template settings are preserved and picked up by newer versions.

Upgrading Password Policy Manager

Both removal and installation of Password Policy Manager (PPM) requires computer restart. Upgrade PPM on all domain controllers in sequential order. Perform the upgrade during off-peak hours to cause minimal impact to your organization's operations.

To guarantee that all the passwords in your organization comply with the established policies, Password Policy Manager must be deployed on all domain controllers in the managed domain.

To upgrade from Password Policy Manager version 5.7.1 or later versions

1. Remove the previous version of Password Policy Manager from a domain controller and restart the computer when prompted. For more information on uninstalling PPM, see Uninstalling Password Policy Manager on page 236.
2. Install the new version of Password Policy Manager on that domain controller and restart the computer when prompted. For more information on installing PPM, see Installing Password Policy Manager on page 235.
3. Repeat the steps 2 and 3 for each domain controller in the managed domain.

If the previous version of Password Policy Manager has been deployed through Group Policy, it should be uninstalled by removing the previously assigned MSI package from the Software installation list. For more information, see Uninstalling Password Policy Manager on page 236. After the previous version is removed from the domain controllers, the new version may be deployed to those DCs through Group Policy.

Administrative Templates

The Password Manager distribution package includes Group Policy administrative templates, which you can use to configure the additional features and options that are not available in the Password Manager Administration Console by default.

In the Password Manger installation package, you can find the below mentioned files in **Password Manager\Setup\Template\Administrative Template**\ folder of the installation CD.

These administrative templates are supplied in the following files.

File	Description
prm_ gina.admx	Contains the administrative policies defined by OneIdentity Password Manager.
prm_ gina.adml	Allows Group Policy Object Editor to display a policy setting in the configured locale(supported language).

This chapter consists of the following sections

Installing Administrative Templates

To install the administrative templates (.admx) on Domain Controller

1. Login to the Active Directory Domain Controller machine with Administrative Privileges.
2. Copy **Administrative Template Configuration** folder from the **<CD>/Password Manager/Setup/Tools** .
3. Copy the **Administrative Template** folder into the Machine from **<CD>/Password Manager/Setup/Template**.
4. Double click **QPM.AdministrativeTemplateConfiguration.exe** from the **Administrative Template Configuration** folder.
5. In the **Password Manager Administrative Template Configuration** window, browse the Administrative Template folder path and verify the path to Policy

Definitions.

6. Click **Execute** to run the tool.
7. Once the execution is complete, click **Exit** to close the window.

To install the administrative templates (.admx) on the client computer manually

1. Copy the **prm_gina.admx** file into **%windir%\PolicyDefinitions** folder directory.
2. Copy the **prm_gina.adml** file into **%windir%\PolicyDefinitions\en-us** directory.
3. Open the Local Group Policy Editor (**gpedit.msc**).
    a. In the left pane (console tree) of the Local Group Policy Editor, expand **Computer Configuration\Administrative Templates**.

NOTE:

- You can now see the node One Identity Password Manager appearing automatically.
- The .admx policies applied on the client computer takes priority.

Configuring Administrative Templates

To configure the settings of the administrative templates on the Domain Controller

1. Open the Group Policy Management Editor (**gpmc.msc**).
2. Right click the domain node and, then on the short cut menu, click **Create a GPO in the domain and Link it here**' to link the policy.
    a. Enter a name to the New GPO, say "OneIdentity".
3. Right click the new GPO (OneIdentity) and set **Enforced** to apply the policy.
4. Right click the new GPO (OneIdentity) and select **Edit**.
5. Expand the newly created GPO and perform the following
6. To view the latest Administrative Template
    a. Expand the newly created GPO.
    a. Go to **Computer Configuration** >> **Policies**.
    b. Expand **Administrative Templates: Policy Definitions(ADMX files) retrieved from the central store** >> **One Identity Password Manager** >> **Generic Settings**.

Updating Administrative Templates

To update the administrative templates from .adm to .admx on both Domain Controller and Client computer, follow the steps mentioned below

Updating Templates on Domain Controller

Before updating the templates, you must remove the existing .adm templates and then proceed updating the templates.

To remove the administrative templates (.adm) on Domain Controller

1. Open the Group Policy Management (**gpmc.msc**).
2. Right click on the GPO you have created and set **Enforced** to disable.
3. Again, right click on the GPO, and on the shortcut menu, click **Edit**. Group Policy Management Editor opens.
4. On the left pane (console tree) of Group Policy Management Editor, expand **Computer Configuration\Policies**.
5. Right-click the Administrative Templates node, and then click **Add/Remove Templates**.
6. In the **Add/Remove Templates** dialog box, select the **prm_gina.admx** file and click **Remove**.

To update the administrative templates (.admx) on Domain Controller

1. Copy the **Administrative Template Configuration** folder from **<CD>/Password Manager/Setup/Tools**.
2. Copy the **Administrative Template** folder into the Machine from **<CD>/Password Manager/Setup/Template**.
3. Double click **QPM.AdministrativeTemplateConfiguration.exe** tool.
4. Browse the **Administrative Template** folder path and verify the Path to Policy Definitions.
5. Click **Execute** to run the tool.
6. Once the execution is complete, launch the **Group Policy Management** utility.
7. Right click the domain node, then on the shortcut menu, click **Create a GPO in the domain and Link it here** to link the policy.
8. Enter a name to the New GPO, say "OneIdentity".
9. Right click the new GPO (OneIdentity) and select **Enforced** to apply the policy.
10. Again, right click the new GPO (OneIdentity) and select **Edit**.

11. Go to Computer Configuration ->Policies ->Expand "Administrative Templates: Policy Definitions (ADMX files) retrieved from the central store" ->Expand "One Identity Password Manager" -> Click on "Generic Settings" to view the newly checked in Administrative Template.

Updating templates on client computer

To remove the administrative templates (.adm) on client computer

1. Open the Local Group Policy Management Editor (**gpedit.msc**).
2. Expand **Computer Configuration\Policies**.
3. Right-click the Administrative Templates node, and then on the shortcut menu, click **Add/Remove Templates**.
4. In the **Add/Remove Templates** dialog box, select the **prm_gina.admx** file and click **Remove**.

To update the administrative templates (.admx) on the client computer manually

1. Copy the **prm_gina.admx** file into **%windir%\PolicyDefinitions** folder directory.
2. Copy the **prm_gina.adml** file into **%windir%\PolicyDefinitions\en-us** directory.
3. Open the Local Group Policy Management Editor (gpedit.msc) and navigate to the **Computer Configuration\Administrative Templates\One Identity Password Manager** directory to see the policy settings.

Removing Administrative Templates

To remove the administrative templates (.admx) on Domain Controller

1. Open the Group Policy Management (**gpmc.msc**).
2. Right click on the GPO you have created and set **Enforced** to disable.
3. Navigate to **C:\Windows\SYSVOL\sysvol\domain name\Policies\PolicyDefinitions** path.
4. Delete **prm_gina.admx** file.
5. Navigate to the **%systemroot%\SYSVOL\sysvol\domain name\Policies\PolicyDefinitions\en-US** folder and delete **prm_gina.adml** file.

To remove the administrative templates (.admx) on the client computer manually

1. Navigate to the **%windir%\PolicyDefinitions** folder directory. Delete the **prm_gina.admx** file.
2. Navigate to the **%windir%\PolicyDefinitions\en-us** folder. Delete the **prm_gina.adml** file.
3. Update the policy.

Secure Password Extension

Configuring Access to Self-Service Site from Windows Logon Screen

It is very common for business users to forget their password and be unable to log on to the system. Password Manager allows users to securely and conveniently reset their forgotten network passwords, or manage their passwords in multiple enterprise systems, before even logging on to the system. To enable user's access to the Self-Service site from the Windows logon screen, Password Manager implements Secure Password Extension.

Introducing Secure Password Extension

Secure Password Extension is an application that provides one-click access to the complete functionality of the Self-Service site from the Windows logon screen. Secure Password Extension also provides dialog boxes displayed on end-user computers, these dialog boxes notify users who must create or update their Questions and Answers profiles with Password Manager. Secure Password Extension is included on the installation CD and is deployed through Group Policy. For information on how to deploy and configure Secure Password Extension on end-user workstations in the managed domain, see Deploying and Configuring Secure Password Extension on page 218.

Secure Password Extension supports the authentication model in the following systems

- Windows 8.1
- Windows 10

On workstations running windows 8.1 and 10, Secure Password Extension adds an icon under the **Sign-in** options to the user tile of the windows logon screen. By clicking these buttons and links, users can open the Self-Service site.

When users connect to the Self-Service site from the Windows logon screen, anonymous access is enabled and the functionality of Microsoft Internet Explorer is restricted, thereby preventing the actions that may pose a security threat. Once users open the Self-Service site search page from the Windows logon screen, they cannot access any other Web site, or open a new browser window or a context menu.

Understanding How Secure Password Extension Works

This section explains how Secure Password Extension locates the Self-Service site and launches notification dialog boxes on end-user computers that remind users to create or update their Q&A profiles.

Locating Self-Service Site

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

For more information, see:

- Obtaining Self-Service Site URL from Service Connection Point
- Changing Self-Service Site URL on the Administration Site
- Changing Self-Service Site URL in the Administrative Template

Obtaining Self-Service Site URL from Service Connection Point

Every Password Manager instance publishes its service connection points in Active Directory. Secure Password Extension uses service connection points to automatically locate the Self-Service site.

Service connection points are objects in Active Directory that hold information about services. Services can publish information about their existence by creating service connection points in Active Directory. Client applications use this information to find and connect to instances of the service. When an instance of Password Manager is installed, the Password Manager Service publishes its service connection points in Active Directory. To locate the server where the Self-Service site is deployed, Secure Password Extension uses

the service connection points published by Password Manager Service instances in Active Directory.

1. Password Manager instance publishes a service connection point in Active Directory.
2. Secure Password Extension locates the service connection point.
3. Secure Password Extension obtains the necessary data from the service connection point (URL path to the Self-Service site).
4. Secure Password Extension opens the Self-Service site.

Changing Self-Service Site URL on the Administration Site

If you want to change the default Self-Service site URL published in service connection points, use the Administration site to specify a new URL. It may be necessary if you enabled HTTPS binding for the Self-Service site after Password Manager installation, or if you want Secure Password Extension to use the Self-Service site installed on a stand-alone server.

To change the Self-Service site URL

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*>/PMAdmin/.

   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 **Realm Instances** tab.
3. Click **Edit** under the service instance for which you want to specify a different Self-Service site URL.
4. In the **Edit Self-Service Site URL** dialog, specify a new URL and click **Save**. The specified URL will then be published in service connection points.

Changing Self-Service Site URL in the Administrative Template

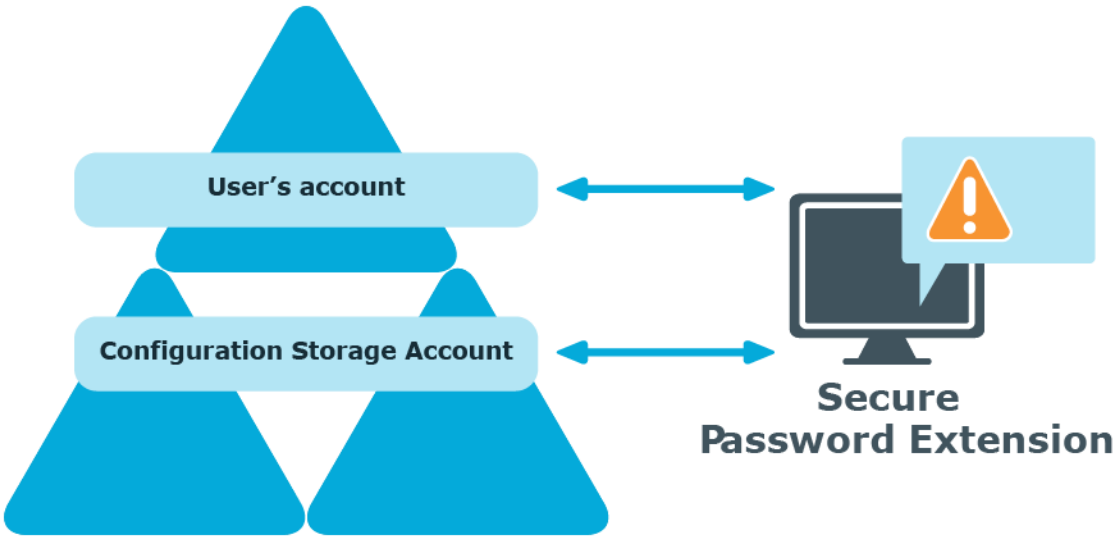
Another option to change the Self-Service URL used by Secure Password Extension is to use the administrative template prm_gina.admx located in \Password Manager\Setup\Template\Administrative Template\ folder of the installation CD.

The administrative template offers two options to override the automatic Self-Service site location: **Specify URL path to the Self-Service site** and **Override URL path to the Self-Service site.** If you want Secure Password Extension to use the specified URL only when service connection points are unavailable, for example when domain users access the Self-Service site from an external network, use the **Specify URL path to the Self-Service site** setting. If you want Secure Password Extension to always use the specified URL, enable the **Override URL path to the Self-Service site** setting after specifying the URL in the Specify URL path to the Self-Service site setting. The administrative template allows you to apply the settings to selected users.

For more information on how to apply administrative template, see Overriding Automatic Self-Service Site Location on page 219.

Launching User Notification

Every unique Password Manager instance creates a configuration storage account in Active Directory. Password Manager uses this account to store its configuration data. Secure Password Extension uses the account to launch user notification.



1. Secure Password Extension locates the configuration storage account and obtains information on notification schedule.

2. Secure Password Extension locates the user's account to check whether the user has been marked by the Password Manager scheduled task and should be notified to create or update his Questions and Answers profile.

Deploying and Configuring Secure Password Extension

This section describes the prerequisites and steps for deploying and configuring Secure Password Extension to provide access to the Self-Service site from the Windows logon screen on end-user computers. Secure Password Extension also provides dialog boxes displayed on end-user computers, these dialog boxes notify users who must create or update their Questions and Answers profiles with Password Manager.

Deploying Secure Password Extension

Secure Password Extension is deployed on client computers through Group Policy. You can create a new Group Policy object (GPO) or use an existing one to assign the installation package with Secure Password Extension for installing it on the destination computers. Secure Password Extension is then installed on computers to which the GPO applies. Depending on the operating system running on the destination computers, you must apply either of the following installation packages included on the installation CD:

- **SecurePasswordExtension_x86.msi** - Installs Secure Password Extension on computers running x86 versions of operating systems.
- **SecurePasswordExtension_x64.msi** - Installs Secure Password Extension on computers running x64 versions of operating systems.

You can modify the behavior and on-screen appearance of Secure Password Extension components by configuring an administrative template's settings, and then applying the template to the target computers through Group Policy.

The administrative template is available in only one format: prm_gina.admx.

The prm_gina.admx administrative template file is located in the \Password Manager\Setup\Template\Administrative Template\ folder of the installation CD. This administrative template is designed to be used with Windows Server 2012 R2 or later operating systems. Before using this administrative template, copy the prm_gina.admx and prm_gina.adml files from the installation CD to the following locations: `%systemroot%\SYSVOL\domain\Policies\PolicyDefinitions`(for the prm_gina.admx file) and `%systemroot%\SYSVOL\sysvol\domain\Policies\PolicyDefinitions\en-US` (for the prm_gina.adml file).

Alternatively, you could use the Administrative Template configuration tool to copy and use the admx templates.

Follow the steps below to configure and deploy the Secure Password Extension on end-user computers.

To deploy and configure Secure Password Extension

1. Copy the required installation package (**SecurePasswordExtension_x86.msi** or **SecurePasswordExtension_x64.msi**) from the installation CD to a network share accessible from all domain controllers where you want to install Secure Password Extension. The MSI packages are located in the \Password Manager\Setup\ folder of the installation CD.
2. Create a GPO and link it to all computers, sites, domains, or organizational units where you want to use Secure Password Extension. You may also choose an existing GPO to use with Secure Password Extension.
3. Open the **Group Policy Management Editor** in the Group Policy Management, and then do the following
    - Expand **Computer Configuration/Policies/Software Settings**, right-click **Software installation**, and then **select New | Package**.
    - Browse for the MSI package you have copied in step 1, and then click **Open**.
    - In **the Deploy Software** window, select a deployment method and click **OK**.
    - Verify and configure the properties of the installation, if needed.

Configuring Secure Password Extension

This section describes how to override automatic location of the Self-Service site and customize Secure Password Extension.

Overriding Automatic Self-Service Site Location

By default, Secure Password Extension uses service connection points published in Active Directory to locate the Self-Service site. If you need to override the default behavior and force Secure Password Extension to use a specific Self-Service site, you must manually specify the URL path and override the default behavior of Secure Password Extension.

To override automatic Self-Service site location on a computer running Windows Server 2012 R2 or later

1. Click the **Start** button, click **Run**, and type **mmc**. Click **OK**.
2. In the Console window on the **File** menu, click **Add/Remove Snap-in**.
3. Double-click **Group Policy Management Editor** in the list of available snap-ins.
4. In the **Group Policy Wizard** window, click **Browse**, select **Default Domain Policy** and click **OK**.
5. Click **Finish** to exit **Group Policy Wizard**.

6. Click **OK**.
7. Login to the Active Directory Domain Controller machine with Administrative Privileges.
8. Copy the **Administrative Template Configuration** folder from **<CD >/Password Manager/Setup/Tools**.
9. Copy the **Administrative Template** folder into the Machine from **<CD>/Password Manager/Setup/Template**.
10. Double click **QPM.AdministrativeTemplateConfiguration.exe** tool from the **Administrative Template Configuration** folder.
11. In the **Password Manager Administrative Template Configuration** windows, browse the **Administrative Template** folder path and verify the path to Policy Definitions.
12. Click **Execute** to run the tool.
13. Once the execution is complete, click **Exit** to close the window.
14. Launch the **Group Policy Management** utility.
15. Right click the domain, and then on the shortcut menu, click **Create a GPO in the domain and Link it here** to link the policy.
16. Enter a name to the New GPO, say "OneIdentity".
17. Right click the new GPO (OneIdentity) and select **Enforced** to apply the policy.
18. Right click the new GPO (OneIdentity) and select **Edit**.
19. To view the latest Administrative Template, follow the steps mentioned below
    a. Expand the newly created GPO.
    b. Go to **Computer Configuration** >> **Policies**.
    c. Expand **Administrative Templates: Policy Definitions(ADMX files) retrieved from the central store** >> **One Identity Password Manager** >> **Generic Settings .**
20. Double-click **Specify URL path to the Self-Service site.**
21. Select the **Enabled** option on the **Settings** tab and then enter the URL path to the Self-Service site into the entry field using the following format: https://COMPUTER_NAME/PMUser/, where COMPUTER_NAME is the name of the server in which the Self-Service site is installed. Substitute https:// with http:// if you don't use HTTPS.

    IMPORTANT: It is strongly recommended that you enable HTTPS on the Password Manager server.

22. Click **OK.** The specified URL will be used only if service connection points are unavailable or if the Self-Service site URL specified in the service connection point cannot be found. If you want Secure Password Extensions to always use the specified URL, perform the following steps.
23. Double-click **Override URL path to the Self-Service site.**
24. Select the **Enabled** option on the **Settings** tab.

25. Click **OK.**
26. Apply the updated policy to the computers in the managed domain.

    NOTE: Application of the updated policy to the computers in the managed domain may take some time to complete.

Password Manager Realm Affinity

In some instances, you may want Secure Password Extension to contact only specific Password Manager Service instances when locating the Self-Service site. You can force Secure Password Extension to use only Password Manager Service instances that belong to a specific Password Manager realm.

Password Manager realm is one or more Password Manager instances sharing common configuration (the same user and helpdesk scopes, Management Policies and workflow configuration, general settings). Normally, you add a member to a Password Manager realm by installing a new Password Manager instance and selecting the "A replica of an existing instance" option during instance initialization. To learn more about Password Manager realms, see Installing multiple instances of Password Manager on page 18.

To force Secure Password Extension to use only Password Manager Service from a specific realm, you must set the Secure Password Extension affinity for that realm.

To set Secure Password Extension affinity for a Password Manager realm on a computer running Windows Server 2012 R2 or later

1. Open the Administration site of the Password Manager Service instance that belongs to the target realm.
2. On the Administration site home page, click **General Settings|Realm Instances**.
3. Select the value of the **Realm affinity ID** setting, right-click the selection and select **Copy**.
4. On the domain controller machine, click the **Start** button, click **Run**, and type **mmc**. Click **OK**.
5. In the Console window on the **File** menu, click **Add/Remove Snap-in**.
6. Double-click **Group Policy Management Editor** in the list of available snap-ins.
7. In the **Group Policy Wizard** window, click **Browse**, select **Default Domain Policy** and click **OK**.
8. Click **Finish** to exit **Group Policy Wizard**.
9. Click **OK**.
10. Login to the Active Directory Domain Controller machine with Administrative Privileges.
11. Copy the **Administrative Template Configuration** folder from <CD>/Password Manager/Setup/Tools.

12. Copy the **Administrative Template** folder into the Machine from <CD>/Password Manager/Setup/Template.
13. Double click **QPM.AdministrativeTemplateConfiguration.exe** from the **Administrative Template Configuration** folder.
14. In the **Password Manager Administrative Template Configuration** windows, browse the **Administrative Template** folder path and verify the path to Policy Definitions.
15. Click **Execute** to run the tool.
16. Once the execution is complete click Exit to close the window, and launch the Group Policy Management utility.
17. Right click the domain node, and on the shortcut menu, click **Create a GPO in the domain and Link it here** to link the policy.
18. Enter a name to the New GPO, say "OneIdentity"
19. Right click the new GPO (OneIdentity) and select **Enforced** to apply the policy.
20. Right click the new GPO (OneIdentity) and select **Edit**.
21. To view the latest Administrative Template, follow the steps mentioned below.
    a. Expand the newly created GPO.
    b. Go to **Computer Configuration** >> **Policies**.
    c. Expand **Administrative Templates: Policy Definitions(ADMX files) retrieved from the central store** >>**One Identity Password Manager** >> **Generic Settings**.
12. In the right pane, double-click **Password Manager Realm Affinity.**
13. Select the **Enabled** option on the **Settings** tab, then right-click the **Realm Affinity ID** text box, and select **Paste**.
14. Click **OK.**
15. Apply the updated policy to the computers in the managed domain.

    NOTE: Application of the updated policy to the computers in the managed domain may take some time to complete.

Managing Secure Password Extension Using Administrative Templates

The administrative template features a powerful set of options that allow you to customize the behavior and appearance of Secure Password Extension according to your requirements.

The administrative template layout includes the following folders:

- **Generic Settings** - includes policy settings that can be applied to computers running Windows 8.1, and 10 operating systems.

Brief descriptions of the administrative template policy settings are outlined in the tables below.

Generic Settings

The following table outlines generic administrative template policy settings you can use to customize the behavior of Secure Password Extension.

Table 14: Generic administrative template policy settings

Policy name	Description
Generic Settings	
Specify URL path to the Self-Service site	This policy lets you specify the link for the access to the Self-Service site from the Windows logon screen. This link is opened when users click the Open the Self Service site link, which is displayed as default. Use the following URL path format: https://COMPUTER_NAME/PMUser, where COMPUTER_NAME is the name of the server on which the Self-Service site is installed. Substitute https:// with http:// if you don't use HTTPS.
Override URL path to the Self-Service site	By default, Secure Password Extension automatically locates the Self-Service site in its domain with the help of the service connection point created in the Active Directory. This policy setting lets you override the default behavior and force Secure Password Extension to use the Self-Service site specified in the "Specify URL path to the Self-service site" setting.
Password Manager realm affinity	This policy setting lets you force Secure Password Extension to use only Password Manager Service instances that belong to specific Password Manager realm.
Maximum number of attempts to connect to the Self-Service site	This setting specifies the maximum number of attempts to connect to the Self-Service site from Secure Password Extension. If this setting is disabled or not configured,

Policy name	Description
	the default number of attempts is 5.
Add the Forgot My Password link to credential provider tile	This policy setting allows adding the Forgot my password link on the logon screen to the tile of the selected credential provider. If you enable this policy setting, the Forgot my password link will be added to the tile of the selected credential provider on the logon screen. If you disable or do not configure this policy setting, the Forgot my password link will be added to the default Microsoft Password provider tile. You can select a credential provider from the list or specify the GUID of another credential provider. GUID should be specified in the following format: {00000000-0000-0000-0000-000000000000}
Refresh interval	This policy setting allows you to change the default settings refresh interval. This policy setting determines how often domain settings are refreshed for Secure Password Extension. The default value is five minutes. If you want to reduce network load, you can increase the refresh interval. If you disable or do not configure this policy setting, the default refresh interval will be used.
Set the recurrence interval for toast notification	This policy setting allows you to specify the recurrence interval for displaying the toast notification. This policy setting determines how often toast notification reminding users to create or update their Q&A profiles is displayed. The default value is five minutes. If you disable or do not configure this policy setting, the default recurrence interval will be used.
Proxy Settings	
Enable proxy server access	This policy setting determines whether connections to the Self-Service from the Windows logon screen are established through the specified proxy server.
Configure required proxy settings	Specifies the settings required to enable proxy server access to the Self-Service site

Policy name	Description
	from the Windows logon screen.
Configure optional proxy settings	Specifies optional settings for the proxy server access.
Shortcut Policies	
Restore desktop shortcuts for the Self-Service site	This policy setting lets you define whether the desktop shortcut to the Self-Service site on a user's computer should be re-created by Secure Password Extension if the user deletes the desktop shortcut.
Do not create desktop shortcuts for the Self-Service site	This policy setting lets you define whether the desktop shortcuts to the Self-Service site on users' computers should not be created by Secure Password Extension.
Do not create any shortcuts for the Self-Service site	This policy setting lets you define whether any shortcuts to the Self-Service site on users' computers (on the desktop and in the Start menu) should not be created by Secure Password Extension.
Secure Password Extension Title Settings	
Display custom names for the Secure Password Extension window title	This policy setting lets you define whether to replace the default language-specific names of the Secure Password Extension window title with the names that you specify for the required logon languages.
Set custom name for the Secure Password Extension window title in <Language>	This group of policy setting allows you to specify custom name for the Secure Password Extension window title. You can specify the title for each of the required logon languages. 36 language-specific policy settings are available out-of-the-box. The name you specify must not exceed 32 characters. If a hieroglyphic font is used, the name is limited by 14 characters because of hieroglyph’s width. The URL length must not exceed 256 characters.
Usage Policy Settings	
Display the usage policy button (command link)	Defines whether to display the usage policy buttons and command links for which you have specified the logon language-specific

Policy name	Description
	names and URLs. The usage policy command link on Windows operating system is displayed on the Windows logon screen, and is intended to open a HTML document that describes the enterprise usage policy or contains any information that you may want to make available to end-users.
Set default URL	This policy lets you specify an URL referring to the usage policy document that will be opened by clicking the usage policy button (command link) if no logon language-specific URLs are set. The default URL may refer to a a DOC, TXT, and HTML file.
Set name and URL for the usage policy button (command link) in <Language>	This group of policy setting allows you to specify the name of the usage policy button (command link) and set the link to the usage policy document that will be opened by clicking the usage policy button or command link. You can specify the name and URL for each of the required logon languages. 36 language-specific policy settings are available. The name you specify must not exceed 32 characters. If a hieroglyphic font is used, the name is limited by 14 characters because of hieroglyph's width. The URL length must not exceed 256 characters.
Notification Customization	
Set background image for registration notification dialog box	This policy setting allows you to change the default background by specifying an image that will be used as a new background.
Customize registration notifications	This policy setting allows you to define whether you want to replace the default text on language-specific registration notification dialog boxes with your custom text.
Registration Notification	
Customize registration notification in <Language>	This group of policy settings allows you to customize texts in notification dialog boxes individually for each of the required logon

Policy name	Description
	languages. 36 language-specific policy settings are available.
Q&A Profile Update Notification	
Customize Q&A profile update notification in <Language>	This group of policy settings allows you to customize notifications that request users to update their Q&A profiles individually for each of the required logon languages. 36 language-specific policy settings are available.
Secure Password Extension Tile Settings	
Credential Provider's Description	
Note: If the **Credential Provider's Description** and the **Icon's Text Label** in the ADMx template are configured with different custom labels, then as per Microsoft's Windows10 design, the Credential Provider Icon will get the same pop-up text(on hovering the Icon) as provided in the **Credential Provider's Description** instead of the label from the **Icon's Text Label**. However, it is a different case with Windows 8.1 and other flavors of Windows released before Windows 8.1 and hence, the Credential Provider Icon will get the pop-up text from the **Icon's Text Label** and the title will have the label provided in the **Credential Provider's Description**.	
Display custom description of the Secure Password Extension credential provider	This policy setting lets you define whether to replace the default description the Secure Password Extension credential provider with the text that you specify for required logon languages. The credential provider description is displayed when users select the Secure Password Extension credential provider in the Sign-in options under their user tiles on the logon screen. If you enable this policy setting, the customized description will be displayed for the Secure Password Extension credential provider. If you disable or do not configure this policy setting, then the default language-specific description of the Secure Password Extension credential provider will be displayed.
Set the custom description in <Language>	This policy setting lets you specify custom description of the Secure Password Extension credential provider in the selected language. If you enable this policy

Policy name	Description
	setting, then the custom text will be displayed when users select the Secure Password Extension credential provider in the Sign-in options under their user tiles on the logon screen on computers that use the specified as the logon language. If you disable or do not configure this policy setting, then the default language-specific description of the Secure Password Extension credential provider will be displayed. **Note:** If the **Display custom description of the Secure Password Extension credential provider**policy is disabled, then this policy has no effect.
Icon's Text Label	
Display custom labels for the Secure Password Extension credential provider's icon	This policy setting lets you define whether to replace the default text label for the Secure Password Extension credential provider's icon with the text that you specify for required logon languages. The text label for the credential provider icon appears in a pop-up when a user hovers over the credential provider's icon under the Sign-in options on the logon screen. If you enable this policy setting, the custom label will be displayed for the Secure Password Extension credential provider's icon. If you disable or do not configure this policy setting, then the default language-specific label for the Secure Password Extension credential provider's icon will be displayed.
Set the custom label in <Language>	This policy setting lets you specify custom text labels for the Secure Password Extension credential provider's icon in the selected language. If you enable this policy setting, then the custom label will be displayed when users hover over the credential provider's icon under the Sign-in options on the logon screen on computers that use the specified language as the logon language. If you disable or do not configure

Policy name	Description
	this policy setting, then the default language-specific label for the Secure Password Extension credential provider's icon will be displayed. Note: If the "Display custom label for the Secure Password Extension credential provider's icon" policy is disabled, then this policy has no effect.
Link to the Self-Service Site	
Display custom names of the Open the Self-Service site link	This policy setting lets you define whether to replace the default name of the Open the Self-Service site link with the names that you specify for required logon languages. This link is intended to open the Self-Service site from the logon screen. If you enable this policy setting, the link will be displayed under the specified language-specific names. If you disable or do not configure this policy setting, then the default language-specific names of the Open the Self-Service site link will be displayed.
Set the custom names of the Open the Self-Service site link in <Language>	This policy setting lets you specify custom name of the Open the Self-Service site link in the specified language. If you enable this policy setting, then the link will be displayed under the specified name under user tile on the logon screen on computers that use the specified language as the logon language. If you disable or do not configure this policy setting, then the default language-specific name of the link will be displayed. Note: If the "Display custom names of the Open the Self-Service site link" policy is disabled, then this policy has no effect.
Offline Password Reset Settings	
Display the Offline Password Reset button (command link)	This policy setting lets you define whether to display the Offline Password Reset buttons and command links for which you have specified the logon language-specific names. The Offline Password Reset button on

Policy name	Description
	Windows operating systems are displayed on the Windows logon screen, and are intended to open the Offline Password Reset wizard. These buttons and command links will be available only if the offline password reset feature is installed on target user computers. To use this setting, you must specify the button (link) name for each of the required logon languages. If you enable this policy setting, the Offline Password Reset button (command link) will be displayed on user computers under the specified language-specific names. Clicking the button or the command link will open the Offline Password Reset wizard. If you disable or do not configure this policy setting, the Offline Password Reset buttons and command links will not appear on user computers.
Shared secret update period (hours)	This policy setting lets you define how often the shared secret used for authentication during the offline password reset should be updated. Set the update period in hours. Lower values provide better security, but setting very low values for the update period may cause replication issues. It is recommended to make this value greater than the intersite replication period in the Active Directory domain. Note: If the Display the Offline Password Reset button (command link) policy is disabled, then this policy has no effect.
Set custom name for the Offline Password Reset button (command link) in <Language>	This policy setting lets you specify the name of the Offline Password Reset button (command link) in <Language>. If you enable this policy setting, then the Offline Password Reset button (command link) will be displayed under the specified name on computers that use <Language> as the logon language.

Policy name	Description
	If you disable or do not configure this policy setting, then the default language-specific name will be displayed on the Offline Password Reset button (command link). The text you specify must not exceed 32 characters. Note: If the Display the Offline Password Reset button (command link) policy is disabled, then this policy has no effect.
Configure scope for accessing the shared secret in Active Directory	This policy setting, when deployed to the client, lets you define a list of users and groups that will have the permission to read the shared secret's copy published in Active Directory. Note, that the domain management account must have this permission for the offline password reset functionality to work. Note, that the computer account used to store the shared secret's copy and the domain administrators group always have the permission to read the shared secret's copy.

Uninstalling Secure Password Extension

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

To remove an assigned MSI package

1. Start the Group Policy Management snap-in. To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. In the console tree, click the group policy object with which you deployed the package, and then click **Edit**.
3. Expand the **Software Settings** container that contains the **Software installation** item with which you deployed the package.
4. Click the **Software installation** container that contains the package.

5. In the right pane of the **Group Policy** window, right-click the package name, point to **All Tasks**, and then click **Remove**.
6. Click **Immediately uninstall the software from users and computers**, and then click **OK**.
7. Quit the Group Policy Object Editor snap-in, and then quit the Group Policy Management snap-in.

Logging in Secure Password Extension

For diagnostic purposes you can turn on logging in Secure Password Extension. The log file can contain the following information: exceptions and errors, debug messages and functions' returns, etc. You can use this diagnostic data to identify issues with Secure Password Extension.

> **CAUTION: This section describes how to modify the Registry. However, incorrectly modifying the Registry may severely damage the system. Therefore, you should follow the steps carefully. It is also recommended to back up the Registry before you modify it.**

To enable logging in Secure Password Extension

1. On a computer where Secure Password Extension is installed, click the **Start** button, click **Run**, and type **regedit**. Click **OK.**
2. In the Registry tree (the left tab), create the following key: HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging.
3. Add a new string value to the HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging registry key. To do it, click the HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging registry key. On the **Edit** menu, select **New**, and then click **String Value**.
4. Type **LogLevel** and then press ENTER to name the string value.
5. Right-click the **LogLevel** value and select **Modify**.
6. In the **Edit String** dialog box, type **All** under **Value data**. Click **OK**.
7. Add a new string value to the HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging registry key. To do it, click the HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging registry key. On the **Edit** menu, select **New**, and then click **String Value**.
8. Type **LogFolder** and then press ENTER to name the string value.
9. Right-click the **LogFolder** value and select **Modify**.
10. In the **Edit String** dialog box, type the path to the log file under **Value data**. For example, C:\Logs. Click **OK**.
11. Exit the Registry Editor.
12. Restart the computer.

To disable logging in Secure Password Extension

1. On a computer where Secure Password Extension is installed, click the **Start** button, click **Run**, and type **regedit**. Click **OK.**
2. In the HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging registry key, select the **LogLevel** value.
3. Right-click the **LogLevel** value and select **Modify**.
4. In the **Value data** box, type **Off**, and click **OK**.

8

Password Policies

About Password Policies

You can use Password Manager to create password policies that define which passwords to reject or accept. Password policy settings are stored in Group Policy objects (GPOs). A GPO is applied by linking the GPOs to a target container defined in Active Directory, such an organizational unit or a group.

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 policy link order, see Managing Password Policy Scope on page 251.

Password Policy Manager

Password Policy Manager is an independently deployed component of Password Manager. Password Policy Manager is required to enforce Password Manager password policies when users change their passwords using tools other than Password Manager. To enforce Password Manager password policies, you must deploy Password Policy Manager on all Domain Controllers (DC) of your managed domain.

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

However, when a user changes their password outside of Password Manager (for example, within the operating system by pressing **Ctrl+Alt+Delete**), Password Manager can not check the new password immediately. Instead, the compliance of the new password to the password policy rules is checked on a DC of the managed domain where Password Policy Manager is installed. If PPM is not installed on the DCs of the managed domain, then new passwords set outside Password Manager will not be checked against the password policies configured in Password Manager.

As such, Password Policy Manager extends the default password policy settings and allows administrators to configure policy scopes for each policy, so that only specified organizational units and groups are affected by the policy.

Password policy settings are stored as Group Policy Objects (GPOs). Password Policy Manager can only create new GPOs: it does not change any existing GPOs.

The installer of the Password Policy Manager component is located at the following subfolder of the Password Manager ISO image or extracted installation archive:

`/Password Manager/Setup/PasswordPolicyManager_x64.msi`

Password Policy Rules

Password Manager uses a set of powerful and flexible rules to define requirements for domain passwords. Each password policy has rules that are configured independently of the rules in other policies.

The following rules duplicate and extend system password policy rules: Password Age rule, Length rule, Complexity rule, and User Properties rule.

For information on how to create and configure a password policy, see Creating and Configuring a Password Policy on page 237.

To display the properties of 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 domain that you want to manage.
3. On the **One Identity Password Policiesfor Domain*<DomainName>*** page, click **Edit** under the policy whose properties you want to view or modify.

Installing Password Policy Manager

To install the Password Policy Manager component in your managed domain, you must deploy it on all Domain Controllers (DC) via a Group Policy. You can create a new Group Policy Object (GPO), or use an existing one, to assign the Password Manager installation package with Password Policy Manager to the destination computers. Password Policy Manager is then installed on the computers to which the GPO applies.

The installer of the Password Policy Manager component is located at the following subfolder of the Password Manager ISO image or extracted installation archive:

`/Password Manager/Setup/PasswordPolicyManager_x64.msi`

To install Password Policy Manager on a single DC

1. Run the `PasswordPolicyManager_x64.msi` installation package.
2. Restart the computer once the installation is completed.

To deploy Password Policy Manager on multiple domain controllers

1. Copy the `PasswordPolicyManager_x64.msi` installation package to a network share accessible from all DCs in the managed domain.
2. Create a GPO and link it to all DCs in your managed domain. You may also choose an existing GPO to deploy Password Policy Manager.
3. Under the selected GPO, open **Computer Configuration** > **Software Settings**.
4. Right-click **Software installation**, then select **New** > **Package**.
5. Select the `PasswordPolicyManager_x64.msi` installation package.
6. Click **Open**.
7. Select the deployment method and click **OK**.
8. Verify and configure the installation properties, if needed.

Uninstalling Password Policy Manager

To uninstall Password Policy Manager, remove it from all Domain Controllers (DC) in your managed domain.

To uninstall Password Policy Manager

1. Remove Password Policy Manager from the DC of the managed domain.
2. Restart the computer when prompted.
3. Repeat the previous steps for all remaining DCs in the managed domain.

If you have deployed Password Policy Manager via a Group Policy, then uninstall Password Policy Manager by removing the `PasswordPolicyManager_x64.msi` installation package from the **Software installation** list.

To remove the Password Policy Manager installation package from a Group Policy

1. Start the Group Policy Management snap-in. To do so, click **Start**, and navigate to **Programs** > **Administrative Tools** > **Group Policy Management**.

2. In the console tree, click the group policy object that you used to deploy the package, and click **Edit**.
3. Expand the **Software Settings** container that contains the **Software installation** item that you used to deploy the package.
4. Click the **Software installation** container that contains the `PasswordPolicyManager_x64.msi` package.
5. In the right pane of the **Group Policy** window, right-click the **`PasswordPolicyManager_x64.msi`** package, point to **All Tasks**, and then click **Remove**.
6. Click **Immediately uninstall the software from users and computers**, and then click **OK**.
7. Quit the Group Policy Object Editor snap-in, and then quit the Group Policy Management snap-in.

IMPORTANT: If you uninstall Password Manager, but do not remove Password Policy Manager from DCs in a managed domain, configured password policies will still be enforced. To stop the enforcement of password policies configured in Password Manager, uninstall Password Policy Manager from all DCs in the managed domain.

Creating and Configuring a Password Policy

To create a password policy, you need add a connection to the domain to which this policy will be applied.

IMPORTANT: By default, native Windows domain policies are not displayed on the Self-Service site when resetting or changing password. To display these policies, you must add the required domain on the Password Policies tab of the Administration site.

The account you use to access the domain 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 Read permission for the *nTSecurityDecriptor* attribute of the *groupPolicyContainer* objects.
- 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.
- The Write permission for the following attributes of the *msDS-PasswordSettings* object:
    - msDS-LockoutDuration
    - msDS-LockoutThreshold
    - msDS-MaximumPasswordAge
    - msDS-MinimumPasswordAge
    - msDS-MinimumPasswordLength
    - msDS-PasswordComplexityEnabled
    - msDS-PasswordHistoryLength
    - msDS-PasswordReversibleEncryption
    - msDS-PasswordSettingsPrecedence
    - msDS-PSOApplied
    - msDS-PSOAppliesTo
    - name

To add domain connection

1. On the home page of the Administration site, click the **Password Policies** tab.
2. Click **Add domain connection** to add a domain for which you want to create password policies.
3. If domain connections already exist, select a domain connection from the list. If you want to create a new connection, click **Add domain connection**.
4. If you selected to create the new domain connection, in the **Add New Domain Connection** dialog, configure the following options:
    - In the **Domain name** text box, type in the name of the domain that you want to add.
    - In the **Domain alias** text box, type the alias for the domain which will be used to address the domain on the Self-Service site. This field is required because you can reuse the domain connection in the user scope.
    - To have Password Manager access the domain using the Password Manager Service account, click **Password Manager Service account**. Otherwise, click **Specified user name and password** and then enter user name and password in the corresponding text boxes. Note, that if Password Manager Service account is used to access the domain, it should have the required permissions.
5. Click **Save**.

For more information on modifying settings for the domain connection, see Domain Connections on page 178.

1. To create a domain password policy
2. On the home page of the Administration site, click the **Password Policies** tab.
3. Click the **<*N*> One Identity Password Policies**or **One Identity Password Policiesare not configured** link under the domain that you want to manage.
4. On the **One Identity Password Policiesfor Domain <*DomainName*>** page, click **Add a policy**.
5. 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 domain connection that you want to manage.
3. On the **One Identity Password Policiesfor Domain <*DomainName*>** 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 15: Password Policy Properties

Option	Description
Disable this policy	Select this check box to temporarily turn off the policy.
Domain	View the name of the managed domain to which this policy is linked.
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 240, and 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 251, and then click **Save**.

   IMPORTANT: The password policies do not override domain security settings; both the Password Manager password policies and the domain security settings are applied.

In case you are running Microsoft Windows Server 2012 R2 or later, Password Manager allows configuring and using not only One Identity Password Policies, but Windows fine-grained password policies as well. For Windows fine-grained password policies, among other options, you can configure policy precedence that defines Windows fine-grained password policies application order. Note, that when configuring the scope of these password policies, you can apply the policies only to groups in the managed domain.

Configuring Password Policy Rules

For each of the domain password policies, you can configure a set of policy rules that define what passwords to reject or accept in the domain to which a particular policy is applied.

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.
- **Dictionary rule**. Rejects passwords that match dictionary words or their parts.
- **Symmetry rule**. Ensures that password or its part does not read the same in both directions.
- **Custom rule**. Use this rule to display custom messages to users or to hide configured policy rules from users when they reset or change password on the Self-Service site.

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 information, see Customization of Password Strength Meter.

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 domain that you want to manage.
3. On the **One Identity Password Policiesfor Domain** ***<DomainName>*** page, click **Edit** under the policy whose properties you want to modify, and then click the **Policy Rules** tab.
4. On the **Policy Rules** tab, click the rule that you want to configure, and, under the rule's name, modify the appropriate rule settings.
5. Repeat step 4 for each of the rules that you want to configure for this password policy, and then click **Save**.

NOTE: Starting from version 5.9.5, if a Password Manager policy is applied, then the **Next** button remains disabled in the Forgot my password/ Manage My Passwords screen and gets enabled only when all the password manager's policies are met and shows GREEN.

For information about how to configure each of the policy rules, see the sections below.

Password Age Rule

The password age rule ensures that users cannot use expired passwords or change their passwords too frequently.

Specify **Minimum password age** so that passwords cannot be changed until they are more than a certain number of days old. If a minimum password age is defined, users must wait 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 240.
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, and then specify the following options as required:

Table 16: 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 how many days a password

Option	Description
	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 240.
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 17: 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 240.
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 240.
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 18: 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 that must appear in a password.
Uppercase characters	Set the minimum number of uppercase characters 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 the **Case sensitive** check box.
Digits (0-9)	Specify whether passwords must contain

Option	Description
	digits: Set the minimum number of digits that must appear in a password by selecting the Minimum check box, and then typing the required number. In the **In positions** text box, type the numbers of positions within a password where digits must appear. For example, 1,3,5-10. Use **Number of ending characters** to specify how many digits must be in the end of a password.
Special characters	Specify whether passwords must contain special characters: Set the minimum number of special characters that must appear in a password by selecting the Minimum check box, and then typing the required number. In the **In positions** text box, type the numbers of positions within a password where special characters must appear. For example, 1,3,5-10. Use **Number of ending characters** to specify how many special characters there must be in the end of a password. Special characters include the following characters - !"#$%&'()*+,-./:;<=>?@[\]^_`{}~

NOTE: By default, the table of lowercase, uppercase, and special characters is taken from the locale settings of the domain controller where the Password Policy Manager is installed. To view the locale settings, select Start | Settings | Control Panel | Regional Options and click the General tab.

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 240.
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 19: 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 - !"#$%&'()*+,-./:;<=>?@[\]^_`{}~

NOTE: By default, the table of special characters is taken from the locale settings of the domain controller where the Password Policy Manager is installed. To view the locale settings, select Start | Settings | Control Panel | Regional Options and click the General tab.

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 three, then the password "eagle" will be rejected.

To configure the sequence rule

1. Follow the steps outlined in Configuring Password Policy Rules on page 240.
2. On the **Policy Rules** tab, click **Sequence Rule** to expand the rule settings.
3. Under **Sequence Rule**, select the **Password must not contain more than** check box, and then specify the following options:

Table 20: Password sequence rule

Option	Description
Number of characters repeated in succession (AAAB)	Set the maximum number of same characters in a row that the policy will tolerate before rejecting a password.
Number of identical characters (ABCA)	Set the maximum number of same characters typed in different positions of password that the policy will tolerate before rejecting a password.
Number of characters in direct or inverse numerical or alphabetical order (ABC_ 321)	Set the maximum number of characters typed in direct or inverse numerical or alphabetical order that the policy will tolerate before rejecting a password.
Case sensitive	Select this check box to require case sensitivity for this rule.

User Properties Rule

The user properties rule rejects passwords that contain part of a user account property value.

This rule splits the user account property value by non-alphanumeric characters (for example, "_"), and then checks if any part of the value is available in the password. For example, if user's name is "Peter_US", Password Manager splits the property into: "Peter" and "US", and checks if any part can be found in the password. For example, the password "US_US" will be rejected.

To configure the user properties rule

1. Follow the steps outlined in Configuring Password Policy Rules on page 240.
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 21: User properties rule

Rule	Description
Beginning characters of a user property value	Set the maximum number of beginning characters from a user property value that users are allowed to use as part of their passwords. For example, if a user's full name is “Anna Fairweather”, and the option value is set to 3, then the user is allowed to type the strings “Ann” and “Fai” as part of her password. The password will be rejected if it contains “Anna” or “Fair”. You can select from the following user account properties: • displayNamePrintable • mailNickname • userPrincipalName • displayName • title • sn • samAccountName • personalTitle • middleName • mail • givenName • employeeID • cn

Rule	Description
	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.
The entire value of a user property	Select to reject passwords containing the entire value of a user property. You can select any of the user account properties listed in the description of the Beginning characters of a user property value option above.
Case sensitive	Select this check box to require case sensitivity for this rule.
Enable bi-directional analysis	Select to reject passwords containing the entire value of a user property or its part (depending on which of the two previous options you have selected), if read backwards.

Dictionary Rule

The dictionary rule rejects passwords that match dictionary words or their parts.

The dictionary rule compares user passwords against a list of words stored in the QPMDictionary.txt text file (this file must use UTF-8 encoding). Depending on how you configure the rule settings, user passwords that partially or fully match dictionary words are rejected by Password Manager.

The QPMDictionary.txt (dictionary file) is located in the following folder: '\\<Domain Controller>\SYSVOL\<Domain>\31EB75A4-CD1A-4F67-94DA-9F8F5DF1F5C1', is deployed when user installs Password Policy Manager (PPM).

The dictionary file is never cached. During each password validity check, the dictionary file is read from the Password Manager server, or from the user's domain controller.

On the **Policy Rules** tab, click **Dictionary Rule** to expand the rule settings. Click **Edit Dictionary File** to edit or add new words to dictionary. After editing the file, click **Save** to save the changes. When user edits the dictionary file, the changes are saved in QPMDictionary.txt file which is in SYSVOL folder in Domain Controller. Service accounts must have access to this file from machines, where Password Manager is installed. When modifying the dictionary file, ensure that you begin every new word on a new line. It is recommended to maintain alphabetical order.

The dictionary rule is not case-sensitive which means that, on the one side, you can use either uppercase or lowercase when adding or modifying dictionary entries; and, on the

other side, user input will undergo validity check irrespective of whether users use capitals or small letters in their passwords.

1. To configure the dictionary rule
2. Follow the steps outlined in Configuring Password Policy Rules on page 240.
3. On the **Policy Rules** tab, click **Dictionary Rule** to expand the rule settings.
4. Under **Dictionary Rule**, select the **Enable dictionary lookup to reject passwords that contain** check box. This enables administrators to control a set of rules using the Dictionary Rule feature. These rules can be modified as follows:

Table 22: Dictionary rule

Option	Description
Beginning characters of a dictionary word	Specify number of characters in the password to match with the beginning of a word in dictionary before rejecting it. The characters in the password must be more than the specified number, for this option to work efficiently.
A complete word from the dictionary (QPMDictionary.txt)	Select this check box to reject passwords that represent an entire word stored in the dictionary.
Detect inclusion of non-alpha characters (pas7swo%rd)	Select this check box to remove non-alphabetic characters during analysis.
Enable bi-directional analysis	Select to reject passwords containing an entire dictionary word or its part (depending on which of the other three options you have selected), if read backwards.

NOTE: Password Policy Manager installation is not necessary, if Password Manager is installed on Domain Controller, and user wants to enable only dictionary rule.

Symmetry Rule

The symmetry rule ensures that 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 240.
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 23: Symmetry criteria

Option	Description
Reject passwords that read the same in both directions (pass8ssap)	Select to reject passwords that are palindromes.
Maximum number of beginning characters that match ending characters of password if read backwards (pas47sap)	Specify the number of beginning 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, 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.

1. To configure the custom rule
2. Follow the steps outlined in Configuring Password Policy Rules on page 240.
3. On the **Policy Rules** tab, click **Custom Rule** to expand the rule settings.
4. Under **Custom Rule**, select the **Enable** check box to enable this rule.
5. 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.
6. 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, that only languages of the user interface of the Self-Service site are available in the list.

Managing Password Policy Scope

This section provides information on how to apply a password policy to groups and organizational units in a managed domain.

Applying Password Policies

In Password Manager (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.

IMPORTANT:

- 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.

S.No	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		OU-2	Group3		User2	No
4.	Group3	OU3		OU1	OU-3	Group3	Password Policy3	User3	Yes
5.	Group2	OU2			OU-1	Group2		User2	No
6.	Group1	OU1		OU4	OU-4	Group1	Password Policy4	User1	No
7.	Group2	OU2		OU5	OU-5	Group2		User2	No
8.	Group3	OU3	Group1			Group3	Password-	User3	No

9.	Group3	OU3	Group2		OU-3		d Policy 5	User3	No

To link a password policy to organizational units and groups

1. Display properties of a password policy by using the procedure outlined in About Password Policies.
2. Click the **Policy Scope** tab.
3. Click the **Add** button under **This policy is applied to the following organizational units,** and then browse for an organizational unit.
4. Click the **Add** button under **This policy is applied to the following groups**, and then browse for a group.
5. 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 domain 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.

Deleting a Password Policy

To delete a password policy from a domain

1. On the home page of the Administration site, click the **Password Policies** tab.
2. Click the **One Identity Password Policies** link under the domain that you want to manage.
3. Click **Remove** under the policy that you want to delete.

NOTE: When you delete a password policy from a managed domain, the deleted policy is no longer valid for this domain.

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 Administration site and Helpdesk site users.

To enable 2FA for Administrators & HelpDesk Users

1. On the home page of the Administration site, click the **Management/2FA enforcement** tab.
2. Select the **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 an "X-Frame-Options : Deny" header, then the **iframe** option will not work. In this case, the **redirect** or the **popup** option is required.

9

Reporting

Reporting and User Action History Overview

Password Manager provides a simple and convenient way to view, print, and save reports and charts allowing you to analyze information on how the application is used. The reporting functionality within the solution is based on Microsoft SQL Server Reporting Services as a common reporting environment.

The Reports section of the Administrator site includes a number of pre-defined reports that help you perform the following tasks:

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

The user action history provides records of all actions performed by users registered with Password Manager. You can search for records using a full-text search functionality. The user action history is provided by Enterprise Auditing Service embedded in Password Manager.

To use Password Manager reports, you need to connect to an SQL Server and a Report Server.

To use the user action history functionality, you need to connect to an SQL Server only.

Alternative options

You can use predefined Power BI templates to generate interactive reports as an alternative to **Reporting**. For more information on Power BI, see Working with Power BI templates.

Setting Up Reporting Environment

To enable the reporting functionality of Password Manager, ensure that the following requirements are met:

- A SQL Server is deployed in your environment and the Password Manager database is configured on that server.
- A SQL Server Reporting Services report server is installed in your working environment.
- You have configured a connection to the report server through the Administration site.

The interactive Web-based reports are built on data that the report server retrieves from the Password Manager SQL database, and can be either viewed online or exported into multiple file formats.

Using 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 database.

When specifying the SQL Server and the database to store the log data, ensure that the account under which Password Manager 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 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 will access the server has the appropriate permissions to publish the Password Manager reports. The administrative rights on the report server will be sufficient for this account to publish reports.

To configure Password Manager reports

1. On the home page of the Password Manager 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 24: SQL server connection settings

Setting	Description
SQL Server	Type the name of the SQL Server to be used for storing the Password Manager database.
Database name	Specify the name for the database where Password Manager 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. NOTE: The account you select must have the db_owner permissions to the database.
Select account for connecting to the SQL Server	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**, and then enter user name and password of the user account you want Password Manager to use when accessing the SQL Server. NOTE: The account you select must have the db_owner permissions to the database.

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

Table 25: Report server connection settings

Setting	Description
Report Server URL	Type in the URL address of the Report Server in the following format: http://<server_name>/<report_

Setting	Description
	server>), 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: http://<server_name>/<report_server>), 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 deploying SSRS reports	Enter user name and password of the user account you want Password Manager to use when accessing the Report Server. This account must have the permissions to deploy reports.
Specify the account that the Report Server will use to connect to the data source	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. NOTE: The account you select must have the db_owner permissions to the database.

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:

Table 26: Reports and user action history

Report Name	Description
User status (table)	This is a table report displaying a list of

Report Name	Description
	users in the managed domains, and the states of the users' Questions and Answers profiles in Password Manager. You can see which users have registered with Password Manager and which have not, who of the users must re-create their profiles, and who is scheduled to update their profiles.
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, 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 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. You can view this report for a specified month range.
Actions by month (bar chart)	This is a barchart showing the monthly numbers of user actions performed in Password Manager. 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 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.

Report Name	Description
Help desk usage by operators (table)	This is a table report showing what actions each of the helpdesk operators performed in Password Manager, 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.
E-mail notifications by user (table)	This table report lists the e-mail notifications sent to specific users. You can view this report for a specified period of time.
E-mail notifications by type (table)	This is a table report showing a summary of e-mail 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 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.

3. Once the report is generated, it is displayed in the Report Viewer, in a new browser window.
4. Select the zoom ratio in the drop-down list on the toolbar.
5. 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.
6. 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.
7. To close the Report Viewer and return to the **List of Reports** page, simply 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. This functionality is provided by the Enterprise Auditing Service. This service is installed during Password Manager installation and does not require any configuration.

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

To connect to SQL Server

1. On the home page of the Password Manager 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 27: 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	Specify the name for the database where Password Manager 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 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 to use when accessing the SQL Server. Note, that the account you select must have the permissions to write to the database.

After you connect to SQL Server, you can perform full-text search for various user actions by user names, emails, activity names, domain, 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 John Doe for example, enter *John Doe*.

Managing Connections to SQL Server and Report Server

On the Reporting page of the Administration site, you can edit or remove existing connections to SQL and Report Servers.

To edit connections, under **Reporting and User Action History**, click the **Edit Connections** link and specify required values.

To remove connections, under **Reporting and User Action History**, click the **Disconnect Servers** link. Note, that all existing connections will be removed.

Best Practices for Configuring Reporting Services

This section provides instructions on how to configure the Reporting Services component. SQL Server Reporting Services component builds reports using the data that SQL Server stores in the Password Manager database. This database must be configured on the SQL Server.

SQL Server Reporting Services allows you to create and view reports that provide statistical data on how Password Manager is used, for example how many users have created their Questions and Answers profiles, how many users need to update their Questions and Answers profiles, what actions each user or helpdesk operator has performed in Password Manager, 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 in order to use the Password Manager Reporting functionality. Make sure 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.**

   NOTE: 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 28: Reporting functionality configuration and settings

Step	Reference
Ensure that MS SQL Server with the Reporting Services component is installed and configured.	Refer to MS SQL Server documentation.
Install Password Manager and its components.	Refer to Installing Password Manager.
Ensure that the **DefaultAppPool**, **PMAdmin, PMUser, PMHelpdesk**, and **ReportServer** application pools are running in the **IIS Manager** on the Password Manager and the Report Services servers. If any of these pools are not	

Step	Reference
running – start them manually.	
Ensure that the **Default Web Site** is running in the **IIS Manager** on the Password Manager and the Report Services servers. If the web site is not running – start it manually.	
Connect to the Reporting Services server through Password Manager Administration site.	

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

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

Reporting Services Firewall Issues

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

To get the complete list of Password Manager server port numbers, that have to be open for the application to function properly, see Appendix B: Open Communication Ports for Password Manager.

Password Manager Integration

Quest Enterprise Single Sign-On (QESSO)

This section includes the information on how to configure Password Manager for use with Quest Enterprise Single Sign-On (QESSO). To implement the guidance in this section, you must have a working knowledge of Quest Enterprise Single Sign-On (QESSO).

Quest Enterprise Single Sign-on is a solution that provides users with the ability to access all applications on their desktop using a single user ID and password. After users have logged in, they can access password-protected applications on their desktop without the need to enter any further account details.

If an application requires login name and password to be entered, QESSO will remember the entered details. When the application is next started, QESSO will automatically enter the required login name and password.

The account details for password-protected applications are encrypted by using user logon password. When user resets or changes this password, the encrypted data is lost. To prevent data loss, Password Manager should be configured to notify QESSO about password changes and QESSO will re-encrypt the data using new password.

To enable QESSO integration

1. Run the **QESSO Client** 32-bit or 64-bit wizard on the server where Password Manager resides. The wizard is located on the **Individual Components** tab of QESSO Autorun CD.
2. Follow the wizard instructions.
3. Install at least one of the following QESSO components on the server running a Password Manager instance:
    - SSOWatch
    - Advanced Login

- Enterprise SSO Console

4. Restart the Password Manager Service.
5. On the Administration site, open workflows for which you want to configure integration with QESSO. QESSO integration settings can be found in the following activities:
   - Reset password in Active Directory
   - Change password in Active Directory
   - Reset password in Active Directory and connected systems
   - Change password in Active Directory and connected systems
6. In required activities, select the **Enable QESSO integration** check box.
7. Provide the account details for the QESSO administrator to be used for password resets.
8. Click **OK**.

For the complete information about installing and using QESSO, please refer to the documentation for QESSO.

Appendixes

Appendix A: Accounts Used in Password Manager

The following accounts can be used in Password Manager:

- Password Manager Service account
- Application pool identity
- Domain management account
- Password policy account
- Account for One Identity Quick Connect Sync Engine

Password Manager Service Account

Password Manager Service account is used to install Password Manager. For Password Manager to run successfully, Password Manager Service account must be a member of the Administrators group on the Web server where Password Manager is installed.

Application Pool Identity

Application pool identity is an account under which the application pool's worker process runs. The account you specify as the application pool identity during Password Manager

setup will be used to run Password Manager Web sites.

Application pool identity account must meet the following requirements:

- This account must be a member of the **IIS_IUSRS** local group on the Web server in IIS 7.0.
- This account must have permissions to create files in the <*Password Manager installation folder*>\App_Data folder.
- Application pool identity account must the full control permission set for the following registry keys: HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager.

Domain Management Account

Domain management account is an account under which Password Manager accesses a managed domain. Domain management account must meet the following minimum requirements to successfully perform password management tasks in the managed domain:

- Membership in the *Domain Users* group
- The Read permission for all attributes of user objects
- The Write permission for the following attributes of user objects: *pwdLastSet*, *comment*, *userAccountControl,* and *lockoutTime*
- 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 domain objects
- The Write permission for the *gpLink* attribute of the *organizationalUnit* objects and domain 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

Password Policy Account

You can use Password Manager to create password policies that define which passwords to reject or accept. Password policy account is an account that you specify when you add a domain for configuring password policies.

Password policy account must meet the following minimum requirements:

- 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 Read permission for the *nTSecurityDecriptor* attribute of the *groupPolicyContainer* objects.
- 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.
- The Write permission for the following attributes of the *msDS-PasswordSettings* object:
    - msDS-LockoutDuration
    - msDS-LockoutThreshold
    - msDS-MaximumPasswordAge
    - msDS-MinimumPasswordAge
    - msDS-MinimumPasswordLength
    - msDS-PasswordComplexityEnabled
    - msDS-PasswordHistoryLength
    - msDS-PasswordReversibleEncryption
    - msDS-PasswordSettingsPrecedence
    - msDS-PSOApplied
    - msDS-PSOAppliesTo
    - name

For more information on password policies that can be configured in Password Manager, see Creating and Configuring a Password Policy on page 237.

Corporate Authentication

In the Register workflow, if the Admin selects **Corporate authentication** check box, user will only be able to review the corporate account details while registration. If **Allow user to edit corporate details** check box is selected, user will be able to update the respective corporate details such as **Corporate email** and **Corporate phone number**, provided that the details are not previously populated by 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(say, **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, Password Manager allows you to enable users and helpdesk operators to manage passwords across a wide variety of connected systems.

To enable Password Manager to connect to Quick Connect and 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, see Reset Password in Active Directory and Connected Systems on page 113.

Appendix B: Open Communication Ports for Password Manager

This section provides a list of communication ports that need to be open in the firewall for Password Manager to function properly.

Administration Site

Port **80** (Default HTTP) TCP Inbound

Port **443** (Default HTTPS) TCP Inbound/Outbound

Port **8081** TCP Inbound/Outbound

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

Port **135** TCP Inbound/Outbound

Legacy Self-Service, Password Manager Self-Service, and Helpdesk Sites

Port **80** (Default HTTP) TCP Inbound

Port **443** (Default HTTPS) TCP Inbound/Outbound

Port **8081** TCP Inbound/Outbound

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 Legacy Self-Service site and you can select to revert anytime to the Legacy Self-Service site.

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

Secure Password Extension

Port **80** (Default HTTP) TCP Outbound

Port **88** (Kerberos Authentication) UDP Outbound

Port **389** (LDAP Access) TCP Outbound

Port **443** (Default HTTPS) TCP Outbound

Telesign

Port **443** TCP Outbound

Defender

Port specified in the activity settings (Authenticate with Defender) is used

BitLocker with MBAM

Port specified in the activity settings (Issue BitLocker recovery key) is used

Appendix C: 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:

- Customization of steps in Self-Service 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, Password Manager Self-Service site, and Helpdesk Tasks

You can change the steps and the order of steps in Legacy self-service, Password Manager Self-Service site, 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 88.

For more information on modifying self-service workflows and activities, see Legacy Self-Service or Password Manager Self-Service site workflows on page 97.

For more information on modifying helpdesk workflows and activities, see Helpdesk Workflows on page 124.

Email Notification Customization

By adding the notification activities into a workflow, you can send notifications to users and administrators about successful or failed workflows. The following notification activities are available:

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

Password Manager offers user notification templates for all predefined workflows in 16 languages. You can customize the notification template by editing the **Email user if workflow succeeds** and **Email user if workflow fails** activities.

Templates are not provided for administrator notifications. To create administrator notifications, edit the **Email administrator if workflows succeeds** and **Email administrator if workflow fails** activities.

If you want to send email notifications in other languages, you can add more languages to the language list for the required notifications.

For more information on customizing email notifications, see Customizing Notifications on page 121.

User Agreement Customization

In any self-service task Password Manager 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 Questions and Answers profiles.

To 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 119.

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 Configuring Account Search Options on page 148.

Web Interface Customization

Using Password Manager Administration site, you can customize the Web interface of the Self-Service and Helpdesk sites, i.e. 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 170.

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 domain 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 domain on the Password Policies tab of the Administration site.

For more information, see Configuring Password Policy Rules on page 240.

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><![CDATA[Password strength:]]></Value>
 </Resource>


 <Resource Id="PasswordStrengthMeter.VeryWeak">
 <Value><![CDATA[Very weak]]></Value>
 </Resource>


 <Resource Id="PasswordStrengthMeter.Weak">
 <Value><![CDATA[Weak]]></Value>
 </Resource>
```

```
<Resource Id="PasswordStrengthMeter.Good">
<Value><![CDATA[Good]]></Value>
</Resource>

<Resource Id="PasswordStrengthMeter.Strong">
<Value><![CDATA[Strong]]></Value>
</Resource>

<Resource Id="PasswordStrengthMeter.VeryStrong">
 <Value><![CDATA[Very strong]]></Value>
 </Resource>
```

For more information, see Password Compliance on page 240.

Customization of User Name

You can customize the user name that is displayed on Self-Service site and Helpdesk site. You can configure to display either the display name or the sAMAccountName as the user name.

To set display name as user name:

- In the **web.config** file, set the value of **DisplayName** to **true** as follows:

  <add key="DisplayName" value="true"/>

To set display name as sAMAccountName:

- In the **web.config** file, set the value of **DisplayName** to **false** as follows:

  <add key="DisplayName" value="false"/>

Appendix D: Feature imparities between the legacy and the new Self-Service Sites

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

Glossary

A

Account

A record that consists of all the information that defines a user to Active Directory. 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.

Active Directory site in domain connection

As soon as changes occur in one site, they will be replicated to the sites you select. Use this option to reduce potential downtime.Active Directory sites

Administration site

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

Application log

A log that lists all actions performed by Password Manager.

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 Service and web sites installed on different servers. View more.

Configuration storage account

An account used by Password Manager for storing its configuration data i.e. settings configured in Password Manager, for example Management Polices, general settings, etc. The configuration storage account is automatically created in the Users container of a managed domain when the managed domain 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

Domain

A logical collection of resources that consists of computers, printers, computer accounts, user accounts, and other related objects.

Domain alias

Enter the name that will be used to address the domain on the Self-Service site.

Domain controller

For a Windows Server domain, the server that authenticates domain logons and maintains the security policy and the security accounts master database for a domain. Domain controllers manage user access to a network, which includes logging on, authentication, and access to the directory and shared resources.

Domain controller in domain connection

Selecting several domain controllers (DCs) provides fault tolerance in your environment.If the first DC becomes unavailable, the next DC in the list will be used automatically.Domain Controller.

Domain management account

An account under which Password Manager accesses a managed domain. Domain management account must have minimum permissions required to successfully perform password management tasks in the managed domain. For more information on the minimum permissions, see Configuring Permissions for Domain Management Account on page 23.

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, etc.

I

In-place upgrade

The installation of the latest version of Password Manager 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

Mandatory question

A question, the same for all users in a domain, that users must answer in order to authenticate themselves using Password Manager.

Managed domain

A domain registered with Password Manager. You can manage multiple domains by using Password Manager.

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.

Organizational unit

An Active Directory container object used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain.

P

Password Manager realm

Realm is a set of Password Manager Service instances sharing realm settings and configuration. You can use the realm to enhance the service availability.

Password Manager realm affinity

An association between Secure Password Extension and a Password Manager Service. If you enforce an affinity to specific Password Manager realm using Group Policy, all the clients running Secure Password Extension and affected by this policy will use only the Password Manager Service instances that belong to the specified realm.

Password Manager Service Account

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

Password Policy Manager

A component of Password Manager that enforces password policies configured in Password Manager, when users change their passwords using tools other than Password Manager. Password Policy Manager is installed on domain controllers.

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.

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 domain 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

Secure Password Extension

A component of Password Manager that facilitates access to the Self-Service site from the Windows logon screen. This component is installed on end-user computers.

Self-Service site

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

Service connection point

An Active Directory object that represents instance of a service. The service connection point contains binding information which is used to connect to the service.

Show only user display name on the Self-Service site option

By default, in the toolbar of the Self-Service site a user's name is displayed as domain\username. For example, "mydomain\JDoe".

To show "John Joe" instead, select this option.

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.

Users must enter the following user account attribute for identification: Helpdesk Site

If you leave the **Helpdesk Site** field empty, Password Manager will use Ambiguous Name Resolution (ANR) by default.

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 Register, Manage My Profile and I Have a Passcode workflows are enabled. For more information, see Workflow settings.

About us

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

Contacting us

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

Technical support resources

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

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

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