One Identity Password Manager 5.12.2

Quick Start 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 Quick Start Guide
Updated - August 2023
Version - 5.12.2

Contents

1

Introduction

This guide is intended to assist in the initial configuration of Password Manager. For complete configuration options, see the Password Manager Administrator Guide.

Instance Initialization

After installing Password Manager, you have to initialize it. After initializing, you can configure the Management policies with the user and helpdesk scopes, Questions and Answers policy and workflow configuration. 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 the 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.

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. The **Instance Initialization** page will be displayed automatically.
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 the section 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 Self-Service and Helpdesk sites separately from the Password Manager Service, it is recommended to replace the built-in certificate that is used to encrypt traffic between the Service and the sites. For more information, see the Administrator Guide.
    - **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:
    - **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.
    - **Encryption key length.** Specify whether a 192-bit or 256-bit encryption key will be used.
    - **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**.**
    - **Store user's Questions and Answers profile in the following attribute of user's account in Active Directory**. In the text box below, 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 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 x64** from the installation CD autorun window.
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**.

Configuring Administration Site

After initializing the Administration site, you need to configure the default Management Policy.

The required settings you need to configure for the Management Policy are user scope, secret questions, helpdesk scope, domain connection, and configure notification.

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.

Adding Domain Connection

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 which 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.

6. Click **Save**.

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

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: Only Global Security groups can be added. Distribution groups are not supported.

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**.

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**.

Specifying Advanced Options 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.

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 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 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.

To specify 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**. You can

use the autofill option to automatically populate the table with all available sites from the current domain.

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

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. 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.
4. 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.

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.

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 questions' order by clicking the appropriate links.
7. Click **Save** to save the questions and close the dialog box.

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 the Administrator Guide.

Configuring Helpdesk Scope

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. By configuring the helpdesk scope you select groups of helpdesk operators who will have access to the Helpdesk site. The Helpdesk site handles typical tasks performed by helpdesk operators, such as resetting passwords, unlocking user accounts, assigning temporary passcodes, and others. Members of the helpdesk scope are allowed to access the Helpdesk site and manage users from the user scope of the same Management Policy only. You can also restrict groups of helpdesk operators from accessing the Helpdesk site.

To 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 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 **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.
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 Options 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.

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 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 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.

To specify 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**. You can use the autofill option to automatically populate the table with all available sites from the current domain.
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

Password Policies

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

The domain must be added in order for Password Manager to read the Domain Password Policies in order to send email notifications to users.To create and manage 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.

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**.

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 1:

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

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

6

Reporting

Reporting is an optional component in Password Manager. To use the reporting feature, you must have an SQL database. For more information, see the Administrator Guide.

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