



Password Manager 5.15

User Guide

Copyright 2026 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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


Patents


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

Trademarks

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

Legend

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

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

Password Manager User Guide
Updated - 15 January 2026, 12:24

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

Contents

Self-Service Site	4
Getting started	4
Connecting to the Self-Service Site	4
Connecting to the Self-Service Site with a web browser	4
Connecting to the Self-Service Site from the login screen	6
Register	6
Manage My Profile	7
Editing security questions	7
Creating and updating the user profile	8
Creating or updating your Questions and Answers profile via passcode	8
Changing the language of security questions	9
Resetting your password	9
Resetting your password with Offline Password Reset	10
Changing your password	10
Unlocking your account	11
Configuring your notifications	11
Changing the user interface language	12
Helpdesk Site	13
Connecting to the Helpdesk Site	13
Changing the managed user	14
Verifying user identity	14
Assigning temporary passcodes	15
Resetting user passwords	16
Unlocking a user account	17
Unlocking the Questions and Answers profile of a user	17
Enforcing the update of the user's Questions and Answers profile	18
About us	19
Contacting us	19
Technical support resources	19

Self-Service Site

- [Getting started](#)
- [Connecting to the Self-Service Site](#)
- [Register](#)
- [Manage My Profile](#)
- [Creating and updating the user profile](#)
- [Resetting user passwords](#)
- [Changing your password](#)
- [Unlocking your account](#)
- [Configuring your notifications](#)
- [Changing the user interface language](#)

Getting started

To start using Password Manager, you must register with Password Manager by creating your personal Questions and Answers profile. For more information on how to create your private Questions and Answers (Q&A) profile, see [Creating and updating the user profile](#) on page 8.

The topics covered in this section will provide you the information you need to create your personal Q&A profile and perform password management tasks by using the Password Manager Self-Service Site.

Connecting to the Self-Service Site

You can connect to the Self-Service Site either by using a Web browser or from the Windows logon screen, if the administrator has configured Password Manager to allow you to open the Self-Service Site from the Windows logon screen.

Connecting to the Self-Service Site with a web browser

You can open the Self-Service Site by clicking the desktop or Start menu shortcut to the site. If there are no such shortcuts on your computer, you can open the site by entering the

Self-Service Site URL in your Web browser. You can obtain the URL path to the Self-Service Site from your system administrator.

To connect to the Self-Service Site using a Web browser

1. Connect to the Self-Service Site by typing the Self-Service Site URL in the address bar of your web browser. By default, the URL is `http://<computer-name>/PMSelfService/` (or `http://<computer-name>/PMSelfServiceADLDS/` if using Password Manager for AD LDS), where `<computer-name>` is the name of the computer on which Password Manager is installed.

You can obtain the computer name from your system administrator.

2. On the Self-Service Site type in your user name or a part of your user name or your email in the displayed text box.

NOTE: When specifying your user account, you can use any of the following formats:

- `<user_name>`
- `<domain>\<user_name>`
- `<user_name>@<domain>`
- Any other value you use to log in.

3. (Optional) If configured, select your location from the **Location** list box.
4. If more than one account is found, identify and select your account under **Search Results**.
5. By default, on the **Home** page, you can perform the following tasks:

Task	Reference
Register with Password Manager or update your personal Questions and Answers profile	Creating and updating the user profile on page 8
Reset your forgotten passwords	Resetting your password on page 9
Change your passwords	Changing your password on page 10
Unlock your account	Unlocking a user account on page 17
Set up email notifications	Configuring your notifications on page 11

If you cannot find your account in the search results, follow the instructions on the screen.

If you enter a part of your account name, several matches may be found. In this case you will see a list of user names followed by descriptions. Select your account name from this list.

NOTE: You can change the user interface language. For more information see [Changing the user interface language](#) on page 12.

Connecting to the Self-Service Site from the login screen

If your account is locked, and if you forgot your user name or your password, you can access the Self-Service Site from the Windows logon screen, provided that the administrator has configured Password Manager to allow you to open the Self-Service Site from the Windows logon screen.

To connect to the Self-Service Site from the Windows logon screen on a computer running Windows 10 or later

1. Press **Ctrl + Alt + Delete**.
2. Select your user tile on the Windows logon screen.
3. Click **Sign-in options** and select the Password Manager icon.

Register

The **Register** workflow allows you to configure which registration method(s) to use for registration.

NOTE: The available registration methods depend on which methods have been enabled by Password Manager administrators for the Self-Service Site. Password Manager supports the following methods:





- **Authentication with Questions and Answers Profile**
- **Authentication with Telephone**
- **Authentication with Passcode**
- **Authentication with RADIUS Two-Factor Authentication**
- **Authentication with STS**

If Password Manager administrators specified a mandatory registration method, you must register by authenticating with that method. However, after registering with the mandatory method, you can update your profile by authenticating with any other available methods. For more information, see [Manage My Profile](#).

Manage My Profile

Use this activity to update your Questions and Answers Profile, mobile number and email address, or other personal contact details on the Self-Service Site. The available registration methods depend on what the Password Manager administrators enabled for the Self-Service Site. For first-time users, the **Register** workflow must be enabled and the **Manage My Profile** workflow must be disabled until they register. Users can then select one of the following authentication methods:

- **Authentication with Questions and Answers Profile:** Log in by answering the specified number of questions from the users' Questions and Answers Profile.
- **Authentication with Telephone:** Log in by authenticating via a text message or an automated voice call.
- **Authentication with Passcode:** Log in by authenticating via a passcode received in text message or email.
- **Authentication with RADIUS Two-Factor Authentication:** Log in by authenticating via a RADIUS one-time password (OTP).
- **Authentication with STS:** Log in by authenticating with an external provider configured in your organization.

NOTE: The **Manage My Profile** workflow is available only for users who have already registered to the Self-Service Site using the available registration method. You can identify the authentication methods available for updating your profile via the  (green tick) or  (red cross) icons. After you set a value for any of the available authentication methods either through the **Register** or **Manage My Profile** workflow, a  (green tick) icon will be shown for the specific registration method. If the  (red cross) icon is shown for any registration method, it indicates that you have not used that registration method or set any value for it in Active Directory.

Editing security questions

If you have already answered a security questions, you can modify it later if you are unsatisfied with your answer.

To edit security questions

1. Navigate to **Manage My Profile > Security questions**.
2. Find the question you would like to change your answer to.
3. Click **Modify** besides the question you have selected.
4. Provide a new answer, then press **ENTER**.

NOTE: If you do not want to change your answer but you have already clicked **Modify**, you can click **Cancel** to revert your changes.

Creating and updating the user profile

To register with Password Manager, you need to create a user profile. A user profile is a series of security questions (Q&A), corporate mobile number and email address, and personal contact details to which you specify the appropriate information. Later, this information is used to authenticate users when using the Self-Service Site to reset your forgotten passwords or unlock your account. When you create or update your user profile, ensure that nobody knows the correct answers to the Q&A profile questions. However, the registration methods depend on what the administrator has enabled for Self-Service Site.

To create or update your user profile

1. Connect to the Self-Service Site as described in [Connecting to the Self-Service Site](#).
2. On the **Home** page, click the **Register** or **Manage My Profile** link.
3. Follow the steps in the wizard to complete the task.

Creating or updating your Questions and Answers profile via passcode

If you have forgotten your password and, at the same time, are not registered with Password Manager or have forgotten your answers to security questions, you must obtain a temporary passcode from the help desk before you can create or update your Questions and Answers profile and reset your forgotten password.

To create or update your Q&A profile by using passcode

1. Connect to the Self-Service Site as described in [Connecting to the Self-Service Site](#).
2. On the **Home** page, click **I Have a Passcode**.

NOTE: HelpDesk can request you to check for an SMS or email message which contains the passcode.

3. Follow the steps in the wizard to complete the task.

Changing the language of security questions

During registration, an unregistered user can view the **Change language** link using which the user can view and select one of the languages configured by the administrator. When the user chooses a different language, the security questions appear in the same language and the user can register the Q&A Profile in the chosen language.

For example, if an administrator chose the default language as **English (United Kingdom)**, an unregistered user while trying to register will view the security questions in **English (United Kingdom)** as it is the configured default language and the user can change the language by clicking the **Change language** link and choose the preferred language for registration.

Both the registered and the unregistered users can view the **Change language** option in the following **Manage My profile** workflow, and in a custom action **Edit Q&A profile**.

NOTE: The **Change language** link is available in the **Register** page only for the unregistered users.

Resetting your password

You can reset your forgotten password in the Password Manager Self-Service Site, if you have the required permissions. Password Manager lets you reset your password either before logging in to the network (from the Windows login screen), or even after logging in to the system.

Depending on the settings configured by your Password Manager administrator, you can reset your password in one or several systems, and specify either the same password or different passwords for the selected systems.

To reset your password in the Self-Service Site

1. Connect to the Self-Service Site as described in [Connecting to the Self-Service Site](#).
2. On the **Home** page, click **Forgot My Password**.
3. Select one of the following methods to reset your password:
 - **Authentication with Questions and Answers Profile:** Authenticate by answering the specified number of questions from your Questions and Answers Profile.
 - **Authentication with Telephone:** Authenticate via a text message or an automated voice call.
 - **Authentication with Passcode:** Authenticate via a passcode received in text message or email.

- **Authentication with RADIUS Two-Factor Authentication:** Authenticate via a RADIUS one-time password (OTP).
- **Authentication with STS:** Authenticate with the external provider configured in your organization.

NOTE: Consider the following if you need to authenticate yourself:

- When resetting your password, not all of the default authentication methods might be available. You can only select from the authentication methods that were configured for the Self-Service Site by the Password Manager administrator of your organization.
- Helpdesk might request you to check for a text message or email message that contains the passcode.

4. After successfully authenticating yourself, enter and confirm your new password.
5. To finish resetting your password, click **Next**.

Resetting your password with Offline Password Reset

If Offline Password Reset is enabled in your environment, you can reset your password without access to Active Directory with the following steps.

To reset your password with Offline Password Reset

1. On the computer where you want to reset your password, open the Offline Password Reset wizard.
2. (Optional) In the wizard, enter your user name, then click **Next**.
3. On another device with access to the Password Manager Self-Service Site, open the Self-Service Site and find your account.
4. Select the corresponding task to reset your password.
5. Specify a new password. If the task is successfully completed, a response code will appear.
6. In the Offline Password Reset wizard, enter the response code and the new password that you specified on the Self-Service Site. To continue, click **Next**.
7. If the password is successfully reset, then to close the wizard, click **Finish**.

Changing your password

You can change your password provided that you have the appropriate permissions to do so.

Depending on the settings configured by your administrator, you can change your password in one or several systems, and provide either the same password or different passwords for selected systems.

To change your password

1. Connect to the Self-Service Site as described in [Connecting to the Self-Service Site](#) on page 4.
2. On the **Home** page, click **Manage My Passwords**.
3. Follow the steps in the wizard to complete the task.

Unlocking your account

You can unlock your account when it is locked, such as when you exceed the allowed number of attempts to enter the correct password.

NOTE: You can unlock your account only if the administrator configured to allow users unlocking their own accounts.

To unlock your account

1. On the Windows login screen, click the **Forgot My Password** button or command link to open the Self-Service Site.
2. On the **Enter Your User Name** page, enter in your user name.
If you have entered only part of your user name, then you will be redirected to the **Find Your Account** page where you can select your account or search for it.
3. On the **Home** page, click **Unlock My Account**.
4. Follow the steps in the wizard to complete the task.

Configuring your notifications

You can configure the Self-Service Site to automatically send you email notifications when specified events occur.

NOTE: You can change your notifications settings only if the administrator has configured Password Manager to allow you to do it.

To subscribe to event notifications

1. Open the Self-Service Site as described in [Connecting to the Self-Service Site](#) on page 4.
2. On the **Home** page, click **My Notifications**.
3. Follow the steps in the wizard to complete the task.

Changing the user interface language

The user interface resources of Password Manager are fully localized. You can easily change the user interface language.

NOTE: This feature is available only in multilingual versions of Password Manager.

To change the user interface language

1. On the navigation bar, click the **Language** link.
2. In the **Select Language** dialog, select your preferred language.

Helpdesk Site

- [Connecting to the Helpdesk Site](#)
- [Changing the managed user](#)
- [Verifying user identity](#)
- [Assigning temporary passcodes](#)
- [Resetting user passwords](#)
- [Unlocking a user account](#)
- [Unlocking the Questions and Answers profile of a user](#)
- [Enforcing the update of the user's Questions and Answers profile](#)

Connecting to the Helpdesk Site

Perform the following steps to connect to the Helpdesk Site. After connecting, you will have access to the following tasks.

To connect to the Helpdesk Site

1. Connect to the Helpdesk Site by entering the Helpdesk Site URL in the address bar of your web browser. By default, the URL is `http://<computer-name>/PMHelpdesk/` (or `http://<computer-name>/PMHelpdeskADLDS/` when using Password Manager for AD LDS), where `<computer-name>` is the name of the computer on which Password Manager is installed. You can get the Helpdesk Site URL from your system administrator.
2. On the logon page, enter your user name and password and click **Log on**.

NOTE: If **Use Secure Token Server for authentication in 2FA enforcement** is on for the Helpdesk Site and a second factor authentication is set for the selected Secure Token Server provider, the helpdesk user will be prompted for a second level of authentication using the configured method.

To manage a user

1. Connect to the Helpdesk Site by using the procedure outlined above.
2. On the **Find User Account** page, type either part of user's first and/or last name, or both.
3. Under **Search Results**, click the user account matching the search criteria.
4. On the **Home** page, by default, you can perform the following tasks:

NOTE: You can change the user interface language. For more information, see [Changing the user interface language](#) on page 12.

Task	Reference
Verify identity of the user	Verifying user identity on page 14
Assign a temporary passcode to the user	Assigning temporary passcodes on page 15
Reset user's password	Resetting user passwords on page 16
Unlock user's account	Unlocking a user account on page 17
Unlock user's Q&A profile	Unlocking the Questions and Answers profile of a user on page 17
Require the user to update his Q&A profile	Enforcing the update of the user's Questions and Answers profile on page 18

Changing the managed user

You can change the currently managed user with the **Change user** setting of the Helpdesk Site.

To change the managed user

1. Click the user name displayed next to the task name being performed.
2. Click the **Change user** link.
3. On the **Find User Account** page, type either part of user's first and/or last name, or both.
4. Under **Search Results**, click the user account matching the search criteria.

Verifying user identity

Before performing any password management task, you must verify the identity of the affected user.

To verify the identity of a user on the Helpdesk Site

1. Open the **Home** page as described in [Connecting to the Helpdesk Site](#) on page 13.
2. On the **Home** page, click **Verify User Identity**.

3. On the **Verify User Identity** page, select one of the following methods to authenticate.
 - **Authentication with Questions and Answers Profile:** Authenticate the user by having them answer the specified number of questions from their Questions and Answers Profile.
 - **Authentication with Telephone:** Authenticate the user via a text message or an automated voice call.
 - **Authentication with Passcode:** Authenticate the user via a passcode received in text message or email.
 - **Authentication with RADIUS Two-Factor Authentication:** Authenticate the user via a RADIUS one-time password (OTP).
 - **Authentication with Secure Token Server:** Authenticate the user via an external provider configured with Password Manager Secure Token Server (STS).

NOTE: When verifying a user's identity, not all authentication methods might be available. You can only select from the authentication methods that were configured for the Helpdesk Site by the Password Manager administrator of your organization.

4. To review the results on the status page, click **Next**.

Assigning temporary passcodes

If a user has forgotten the password and, at the same time, has not yet registered with Password Manager, or has forgotten his answers to security questions, the user cannot create or update a personal Q&A profile, or otherwise use Password Manager. To register with Password Manager, and access its self-service functionality, the user must obtain a personal temporary passcode which must be used within the specified period to complete the registration procedure.

You can assign temporary passcodes to users provided that you have the appropriate permissions.

To assign a temporary passcode to a user

1. Open the **Home** page by following the procedure in [Connecting to the Helpdesk Site](#).
2. On the **Home** page, click **Assign Passcode**.
3. On the **Assign Passcode** page, read the temporary passcode to the user. Let the user know the passcode's expiration period.

NOTE: On the Password Manager Administration Site, if the **Generate Passcode and send it in Email** or **Generate Passcode and send it in SMS**

option is enabled by the administrator, the passcode is sent using the selected method. The HelpDesk user must inform the user, that the passcode will be sent via SMS or email.

4. Click **Next** to review the results on the status page.

NOTE: Passcode expiration time is a period within which a newly generated passcode is valid. Users must update or create their Q&A profiles by using this passcode within the specified period.

Resetting user passwords

If a user has forgotten their password, you can reset the password for this user, provided that you have the appropriate permissions.

To reset user's password

1. Connect to the Helpdesk Site as described in [Connecting to the Helpdesk Site](#) on page 13.
2. On the **Home** page, click **Reset Password**.
3. Type user's answer(s) and click **Next**. The **Reset Password** page appears.
4. On the **Reset Password** page, select one of the following options to reset the password.
 - a. **Use the following auto generated password:** An auto generated password suggestion displays in text box. The user can use this password and store it in a secure location for later use.
 - b. **Enter the password manually:** The user can select this option to set a password manually. After selecting this option, type the password in the text box and, confirm the password. Click **Next**.

NOTE: On the Password Manager Administration Site, if the **Generate Passcode and send it in Email** or the **Generate Passcode and send it in SMS** option is enabled by the administrator, then the password is sent using the selected method. In this case, the HelpDesk user does not need to use the above options to reset the password. However the HelpDesk user must inform the user, that the password will be sent via SMS or Email.

5. After a successful password reset, the **Password was successfully reset** message appears.

Unlocking a user account

If a user account is locked out, you can unlock it, provided that you have the required permissions.

To unlock a user account on the Helpdesk Site

1. Open the **Home** page as described in [Connecting to the Helpdesk Site](#).
2. On the **Home** page, click **Unlock Account**.
3. On the **Unlock Account** page, select one of the following methods to authenticate.
 - **Authentication with Questions and Answers Profile:** Authenticate the user by having them answer the specified number of questions from their Questions and Answers Profile.
 - **Authentication with Telephone:** Authenticate the user via a text message or an automated voice call.
 - **Authentication with Passcode:** Authenticate the user via a passcode received in text message or email.
 - **Authentication with RADIUS Two-Factor Authentication:** Authenticate the user via a RADIUS one-time password (OTP).
 - **Authentication with Secure Token Server:** Authenticate the user via an external provider configured with Password Manager Secure Token Server (STS).

NOTE: When unlocking a user account, not all authentication methods might be available. You can only select from the authentication methods that were configured for the Helpdesk Site by the Password Manager administrator of your organization.

Unlocking the Questions and Answers profile of a user

If user's Questions and Answers profile is locked, you can unlock the profile, provided that you have the appropriate permissions.

To unlock user's Questions and Answers profile

1. Open the **Home** page as described in [Connecting to the Helpdesk Site](#) on page 13.
2. On the **Home** page, click **Unlock Q&A Profile**.
3. Follow the steps in the wizard to complete the task.

Enforcing the update of the user's Questions and Answers profile

If user's Questions and Answers profile does not comply with the current Q&A profile policy, you can require the user to update the Q&A profile, provided that you have the appropriate permissions.

To enforce update of user's Question and Answers profile

1. Open the **Home** page as described in [Connecting to the Helpdesk Site](#) on page 13.
2. On the **Home** page, click **Enforce Update of Q&A Profile**.
3. Follow the steps in the wizard to complete the task.

About us

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

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

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

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

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