



One Identity Defender 6.5.0

Token User Guide

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

 **WARNING:** A WARNING icon 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.

Contents

Using software tokens	7
Soft Token for Android™	7
Installing Soft Token for Android	8
Installing from Google Play	8
Installing using the Defender Self-Service Portal	8
Activating Soft Token for Android	9
Obtaining an activation code on the Defender Self-Service Portal	9
Importing an activation code	9
Creating a token	10
Authenticating with a token	10
Renaming a token	10
Deleting a token	11
Viewing token details	11
Uninstalling Soft Token for Android	11
Soft Token for iOS	12
Installing Soft Token for iOS	12
Installing from App Store	12
Installing Using Defender Self-Service Portal	13
Activating Soft Token for iOS	13
Obtaining an Activation Code on the Defender Self-Service Portal	13
Importing an Activation Code	14
Creating a token	14
Authenticating with a token	14
Renaming a token	15
Deleting a token	15
Viewing token details	15
Uninstalling Soft Token for iOS	16
Soft Token for Java	16
Installing Soft Token for Java	16
Installing using a setup file	16
Installing using Defender Self-Service Portal	17

Upgrading Soft Token for Java	17
Activating Soft Token for Java	18
Obtaining an Activation Code on the Defender Self-Service Portal	18
Importing an Activation Code	19
Creating a token	19
Authenticating with a token	19
Renaming a token	19
Deleting a token	20
Viewing token details	20
Uninstalling Soft Token for Java	20
Soft Token for Windows	20
Installing Soft Token for Windows	21
Installing using a setup file	21
Installing using Defender Self-Service Portal	21
Opening Soft Token for Windows	22
Activating Soft Token for Windows	22
Obtaining Activation Code on the Defender Self-Service Portal	22
Importing an Activation Code	23
Authenticating with a token	23
Changing the token passphrase	24
Resetting a forgotten passphrase	25
Setting the default token	25
Deleting a token	25
Viewing token details	26
Uninstalling Soft Token for Windows	26
Authy	26
Obtaining an Activation Code on the Defender Self-Service Portal	27
Importing an activation code	27
E-mail token	27
Google Authenticator™	27
Obtaining an Activation Code on the Defender Self-Service Portal	28
Importing an Activation Code	28
GrIDSure token	28
Signing in to a Windows-based computer	29
Authenticating on a Web site protected by GrIDSure	29

How to configure and use your Personal Identification Pattern (PIP)	31
SMS token	33
VIP credential	33
Registering VIP credential	33
Software token	34
Downloading and activating a software token	34
Enabling the use of Microsoft Authenticator	34
Obtaining an Activation Code on the Defender Self-Service Portal	35
Importing an Activation Code	35
Enabling the use of OneLogin Authenticator	35
Obtaining an Activation Code on Defender Self-Service Portal	36
Importing an Activation Code	36
Enabling the use of OneLogin Authenticator for Push Notification	36
Defender Side Configuration	36
OneLogin Side Configuration - Creating a OneLogin Developer account	37
Synchronizing User Data	38
Creating an Authentication Factor	38
Creating a Security Policy and assigning it to the user	38
Obtaining an activation code from the OneLogin portal	39
Using hardware tokens	40
DIGIPASS 280 token	40
Authenticating with DIGIPASS 280 Token	42
DIGIPASS 301 CV token	42
Authenticating with DIGIPASS 301 CV token	44
DIGIPASS GO 7 token	44
Authenticating with DIGIPASS GO 7 Token	45
Changing PIN	45
YubiKey token	46
Registering YubiKey token	46
FIDO2 compatible Hardware Yubikey	47
Basic Steps to use a FIDO2 token	47
Hardware Token	48
Registering a hardware token	49
About us	50

Contacting us50
Technical support resources50

Using software tokens

To access a resource protected with Defender, you can use a number of software tokens. A software token generates a token response also known as one-time password (OTP), with which you can authenticate to access a protected resource. From Defender 6.5.0 onwards, you can also use *Push* notifications to authenticate the access to the protected resources. For more details, please refer **Push Notifications** section in the Defender Admin Guide.

To start using a software token, you need to install and activate it. You may need to consult your system administrator to find out what software tokens you can use to authenticate.

For more information on how to use a software token, click the corresponding link below.

- [Soft Token for Android™](#)
- [Soft Token for iOS](#)
- [Soft Token for Java](#)
- [Soft Token for Windows](#)
- [Authy](#)
- [E-mail token](#)
- [Google Authenticator™](#)
- [GrIDSure token](#)
- [SMS token](#)
- [VIP credential](#)

Soft Token for Android™

- [Installing Soft Token for Android](#)
- [Activating Soft Token for Android](#)
- [Creating a token](#)
- [Authenticating with a token](#)
- [Renaming a token](#)

- [Deleting a token](#)
- [Viewing token details](#)
- [Uninstalling Soft Token for Android](#)

Installing Soft Token for Android

You can install the Soft Token for Android by using either Google Play or a dedicated self-service Web site if it exists in your organization.

The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

To start using the Soft Token for Android, you need to activate it. For more information, see [Activating Soft Token for Android](#) on page 9.

Installing from Google Play

To install from Google Play

1. On your Android device, open the Google Play app.
2. In the Google Play app, search for **Defender Soft Token**.
3. In the search results, select **Defender Soft Token**, and then tap **Install**.
4. Select **OK** to accept permissions.

To access the installed Soft Token for Android, use the **Programs** menu on your Android device.

To start using the Soft Token for Android, you need to activate it. For more information, see [Activating Soft Token for Android](#) on page 9.

You can also use the following link to download and install the Soft Token for Android from Google Play: <https://play.google.com/store>.

Installing using the Defender Self-Service Portal

To install using the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal address.
2. Sign in to the Defender Self-Service Portal.

3. Click the **Request a software token** option.
4. Follow the on-screen instructions to download and install the Soft Token for Android.

To start using the Soft Token for Android, you need to activate it. For more information, see [Activating Soft Token for Android](#) on page 9.

Activating Soft Token for Android

To start using the Soft Token for Android, you need to activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens. Activating the soft token also enables the **Push Notification** feature for the compatible devices.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Obtaining an activation code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal address.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for the Soft Token for Android.

After getting an activation code, you need to import it into your Android device.

Importing an activation code

To import an activation code

1. On your Android device, open the Defender Soft Token app.
2. On the app screen, tap **Enter Activation Code** or **Scan QR code**.

If you tap Enter activation code, you have to enter the activation code when prompted. If you tap **Scan QR code**, you have to scan the QR code provided in the activation e-mail to import the activation code.

Creating a token

To create a token

1. On your Android device, open the Defender Soft Token app.
2. In the upper right corner of the app, tap the menu icon, and then tap **New Token**.
3. Follow the on-screen instructions to name and activate the token.

Authenticating with a token

To authenticate with a token

- On your Android device, open the Defender Soft Token app.
The numeric value in the token response that appears is your one-time password (OTP). You need to enter the OTP when accessing a resource protected by Defender.
You can tap the refresh button to display the next token response.

To authenticate with push notification

- From Defender 6.2 onwards, the *pushnotification* is implicitly triggered when user initiates the login authentication process to Defender. The existing functionality with type in keyword PUSH works if the first login attempts fails to authenticate or times out.
- If the first request times out, you can type the "push" (case insensitive, without quotes) keyword in the token field and click **Submit**.
- The system will send a prompt to the device with a tap option to Approve or Deny the request.

NOTE:

- Push Notifications can be triggered as an authentication request only for the newly programmed iOS/Android tokens using Defender 6.1.0 and above.

Renaming a token

To rename a token

1. On your Android device, open the Defender Soft Token app.
2. Tap and hold the token you want to rename.

3. Tap **Rename**.
4. Enter the new name for your token, and then tap **OK**.

Deleting a token

To delete a token

1. On your Android device, open the Defender Soft Token app.
2. Tap and hold the token you want to delete.
3. Tap **Delete**.
4. When prompted, confirm that you want to delete the token.

Note: When you delete a particular token, the push notification configured for that token is also deleted.

Viewing token details

You can view the details of your token, such as token name, type as push notification, serial number, activation date, and cycle count.

To view token details

1. On your Android device, open the Defender Soft Token app.
2. Tap and hold the token whose details you want to view.
3. Tap **Token Details**.

Uninstalling Soft Token for Android

To uninstall Soft Token for Android

1. On your Android device, open the Google Play app.
2. In the Google Play app, search for **Defender Soft Token**.
3. In the search results, select **Defender Soft Token**, and then tap **Uninstall**.

Note: Uninstalling the soft token will disable the Push Notification feature.

Soft Token for iOS

- [Installing Soft Token for iOS](#)
- [Activating Soft Token for iOS](#)
- [Creating a token](#)
- [Authenticating with a token](#)
- [Renaming a token](#)
- [Deleting a token](#)
- [Viewing token details](#)
- [Uninstalling Soft Token for iOS](#)

Installing Soft Token for iOS

You can install the Soft Token for iOS by using either App Store or a dedicated self-service Web site if it exists in your organization.

The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Installing from App Store

To install from App Store

1. On your iOS device, open App Store.
2. In App Store, search for **Defender Soft Token**.
3. Install the Defender Soft Token from the search results.

To start using the Soft Token for iOS, you need to activate it. For more information, see [Activating Soft Token for iOS](#) on page 13.

Installing Using Defender Self-Service Portal

To install using Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to download and install the Soft Token for iOS.

To start using the Soft Token for iOS, you need to activate it. For more information, see [Activating Soft Token for iOS](#) on page 13.

Activating Soft Token for iOS

To start using the Soft Token for iOS, you need to activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens. Activating the soft token also enables the **Push Notification** feature for the compatible devices.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Obtaining an Activation Code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for the Soft Token for iOS.

After getting an activation code, you need to import it onto your iOS device.

Importing an Activation Code

To import an activation code

1. On your iOS device, open the Defender Soft Token app.
2. On the app screen, tap **Enter Activation Code**, or **Scan QR** code.
3. If you tap, **Enter Activation Code**, you must enter your activation code.
4. If you tap, **Scan QR Code**, you must scan the QR code provided in the activation e-mail to import the activation code.
5. Wait for the activation to complete.

Creating a token

To create a token

1. On your iOS device, open the Defender Soft Token app.
2. In the upper right corner of the app, tap the menu icon, and then tap **New Token**.
3. Follow the on-screen instructions to name and activate the token.

Authenticating with a token

To authenticate with a token

- On your iOS device, open the Defender Soft Token app.

The numeric value that appears in the token response is your one-time password (OTP). You must enter the OTP when you want to access a resource that is protected by Defender.

You can tap the refresh button to display the next response.

To authenticate with push notification

- From Defender 6.2 onwards, the *pushnotification* is implicitly triggered when user initiates the login authentication process to Defender. The existing functionality with type in keyword PUSH works if the first login attempts fails to authenticate or times out.
- If the first request times out, you can type the "push" (case insensitive, without quotes) keyword in the token field and click **Submit**.
- The system will send a prompt to the device with a tap option to Approve or Deny the request.

| NOTE:

- Push Notifications can be triggered as an authentication request only for the newly programmed iOS/Android tokens using Defender 6.1.0 and above.

Renaming a token

To rename a token

1. On your iOS device, open the Defender Soft Token app.
2. Tap and hold the token you want to rename.
3. Tap **Rename**.
4. Enter the new name for your token, and then tap **OK**.

Deleting a token

To delete a token

1. On your iOS device, open the Defender Soft Token app.
2. Tap and hold the token you want to delete.
3. Tap **Delete**.
4. When prompted, confirm that you want to delete the token.

Note: When you delete a particular token, the push notification configured for that token is also deleted.

Viewing token details

You can view the details of your token, such as token name, type as push notification, serial number, activation date, and cycle count.

To view token details

1. On your iOS device, open the Defender Soft Token app.
2. Tap and hold the token whose details you want to view.
3. Tap **Token Details**.

Uninstalling Soft Token for iOS

To uninstall Soft Token for iOS

1. On your iOS device, tap and hold the Defender Soft Token app icon until it starts to jiggle.
2. Tap the cross sign on the app icon.

Note: Uninstalling the soft token will disable the Push Notification feature.

Soft Token for Java

- [Installing Soft Token for Java](#)
- [Upgrading Soft Token for Java](#)
- [Activating Soft Token for Java](#)
- [Creating a token](#)
- [Authenticating with a token](#)
- [Renaming a token](#)
- [Deleting a token](#)
- [Viewing token details](#)
- [Uninstalling Soft Token for Java](#)

Installing Soft Token for Java

Installation methods:

- [Installing using a setup file](#)
- [Installing using Defender Self-Service Portal](#)

Installing using a setup file

You can use a setup file provided by your system administrator to install the Soft Token for Java on Windows-, Mac OS® X-, and Linux/®UNIX-based computers that are running the Java Runtime Environment (JRE).

To use this installation method, contact your system administrator to obtain the **DefenderSoftToken.jar** file with which you can install the token.

To install Soft Token for Java

1. Run the file **DefenderSoftToken.jar** on the computer where you want to install the Soft Token for Java.
2. Complete the wizard that starts.

Installing using Defender Self-Service Portal

Your system administrator may configure a special Web site called the Defender Self-Service Portal. You can use the Defender Self-Service Portal to download and install software tokens, obtain activation code for software tokens, and register your hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Before installing the Soft Token for Java on a Windows-, Mac OS X-, and Linux/UNIX-based computer, make sure the computer is running Java Runtime Environment (JRE).

To install Soft Token for Java

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to download and install the Soft Token for Java.

To start using the Soft Token for Java, you need to activate it. For more information, see [Activating Soft Token for Java](#) on page 18.

Upgrading Soft Token for Java

If you have installed Soft Token for Java 5.9 and want to upgrade to version 6.5.0

- Install Soft Token for Java 6.5.0 side by side with the previous version.
NOTE: After installation of Soft Token for Java 6.5.0, all token data is automatically available in the new token, and you do not have to activate any tokens again. For installation instructions, see [Installing Soft Token for Java](#).

After you have installed Soft Token for Java 6.5.0, you may uninstall the previous version of the token. For instructions, see [Uninstalling Soft Token for Java](#).

If you have installed Soft Token for Java 5.10.x and want to upgrade to version 6.5.0

- Install Soft Token for Java 6.5.0.

NOTE:

- The new version will replace the existing version and it will get directly upgraded to the latest version, that is, 6.5.0.
- After installation of Soft Token for Java 6.5.0, all token data is automatically available in the new token, and you do not have to activate any tokens again. For installation instructions, see [Installing Soft Token for Java](#).

Activating Soft Token for Java

To start using the Soft Token for Java, you need to activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Obtaining an Activation Code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for the Soft Token for Java.

After getting an activation code, you need to import it into the Soft Token for Java.

Importing an Activation Code

To import an activation code

1. Open the Soft Token for Java.
2. Click **Enter Activation Code**.
3. Type a token name, and then enter your activation code.
4. Click **Activate** and wait for the activation to complete.

Creating a token

To create a token

1. Open the Soft Token for Java.
2. In the upper right corner of the Soft Token for Java window, click **New Token**.
3. Follow the on-screen instructions to name and activate the token.

Authenticating with a token

To authenticate with a token

- Open the Soft Token for Java.

The token displays a token response.

The numeric value in the token response is your one-time password (OTP). You need to enter the OTP when accessing a resource protected by Defender.

You can tap the refresh button to display the next response.

Renaming a token

To rename a token

1. Open the Soft Token for Java.
2. Right-click the token you want to rename.
3. Click **Rename Token**.
4. Type a new token name, and click **OK**.

Deleting a token

To delete a token

1. Open the Soft Token for Java.
2. Right-click the token you want to delete.
3. Click **Delete Token**.
4. When prompted, confirm that you want to delete the token.

Viewing token details

You can view the details of your token, such as token type, serial number, activation date, and cycle count.

To view token details

1. Open the Soft Token for Java.
2. Right-click the token whose details you want to view.
3. Click **Token Details**.

Uninstalling Soft Token for Java

Complete the steps provided for your version of Windows in the table below.

Table 1:
[Steps to uninstall Soft Token for Java](#)

A later version of Windows

On the **Apps** screen, click the **Uninstall Defender Soft Token for Java** tile.
In the window that opens, click **Uninstall**.

Soft Token for Windows

- [Installing Soft Token for Windows](#)
- [Opening Soft Token for Windows](#)
- [Activating Soft Token for Windows](#)

- [Authenticating with a token](#)
- [Changing the token passphrase](#)
- [Resetting a forgotten passphrase](#)
- [Setting the default token](#)
- [Deleting a token](#)
- [Viewing token details](#)
- [Uninstalling Soft Token for Windows](#)

Installing Soft Token for Windows

Installation methods:

1. [Installing using a setup file](#)
2. [Installing using Defender Self-Service Portal](#)

Installing using a setup file

You can use a setup file provided by your system administrator to install the Soft Token for Windows. To use this installation method, contact your system administrator to obtain the **DefenderSoftToken.exe** file with which you can install the token.

To install Soft Token for Windows

1. Run the **DefenderSoftToken.exe** file provided to you by your system administrator.
2. Complete the wizard to install the token.

Installing using Defender Self-Service Portal

Your system administrator may configure a special Web site called the Defender Self-Service Portal. You can use the Defender Self-Service Portal to download and install software tokens, obtain activation code for software tokens, and register your hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

To install Soft Token for Windows

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.

3. Click the **Request a software token** option.
4. Follow the on-screen instructions to download and install the Soft Token for Windows.

To start using the Soft Token for Windows, you need to activate it. For more information, see [Activating Soft Token for Windows](#) on page 22.

Opening Soft Token for Windows

Complete the steps provided for your version of Windows in the table below.

Table 2:
[Steps to open the Soft Token for Windows:](#)

A later version of Windows

On the **Apps** screen, click the **Soft Token for Windows** tile.

Activating Soft Token for Windows

To start using the Soft Token for Windows, you need to activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Obtaining Activation Code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for the Soft Token for Windows.

After getting an activation code, you need to import it into the Soft Token for Windows.

Importing an Activation Code

To import an activation code

1. Open the Soft Token for Windows. For more information, see [Opening Soft Token for Windows](#) on page 22.

If you have no active tokens, a wizard starts to guide you through importing an activation code.

If you already have one or more active tokens, do the following to activate a new token:

- a. In the **Enter Passphrase** dialog box, click the **Token** button.
 - b. In the window that opens, from the main menu select **Token | Activate New Token**, and then step through the wizard.
2. In the Enter Activation Code step, click **Browse** to locate and select the .txt file that contains your activation code.
Alternatively, you can enter your activation code in the **Code** text box.
 3. Click **Next**.
 4. In the Select Storage Location step, specify where you want to store the activated token. Click **Next**.
 5. In the Choose Passphrase step, type a token passphrase. A passphrase is required to unlock the token so that it can be used for authentication.
 6. Complete the wizard to activate the token.

To open the Soft Token for Windows. For more information, see [Opening Soft Token for Windows](#) on page 22.

Authenticating with a token

To authenticate with a token

1. Take note of the challenge value displayed on the sign-in screen of the protected resource you are accessing.

The challenge is not displayed if the administrator has configured Defender to work in the synchronous mode. In this case, proceed to step 2.

2. Open the Soft Token for Windows. For more information, see [Opening Soft Token for Windows](#) on page 22.

3. In the **Enter Passphrase** dialog box, type the token passphrase, and then click **OK**.
If you want to use a different token, click the **Tokens** button, and then in the window that opens double-click the token you want to use.
4. In the dialog box that opens, use the following options:
 - **Challenge** If this text box is available, use it to enter the challenge value you took note of in step 1 of this procedure. You can use the **Paste** button to paste the challenge value you have copied. The **Challenge** text box is not available if the administrator has configured Defender to work in the synchronous mode.
 - **Response** Displays the response code generated by Defender. Use this code to access the resource protected by Defender (for example, you can click **Copy** to copy the code to the Clipboard, and then paste it into the sign-in screen of the resource you want to access).
 - **Get Response** Click this button to generate a response code that provides you with access to the resource protected by Defender.
5. Enter the generated response value on the sign-in screen of the protected resource.

Changing the token passphrase

You can change the passphrase that is used to unlock an active token. To do so, you need to know your current passphrase. If you have forgotten your current passphrase and want to reset it, follow the steps in [Resetting a forgotten passphrase](#).

To change the token passphrase

1. Open the Soft Token for Windows. For instructions, see [Opening Soft Token for Windows](#).
2. In the **Enter Passphrase** dialog box, click the **Tokens** button.
3. In the window that opens, click to select the token for which you want to change the passphrase.
4. From the main menu, select **Token | Change Passphrase**.
5. Step through the wizard until you reach the Reset Passphrase step.
6. In the Reset Passphrase step, do the following:
 - a. Provide the value displayed in the **Challenge** option to your system administrator.
 - b. In the **Unlock Code** text box, type the code returned to you by your system administrator.
 - c. Use the **New Passphrase** and **Confirm Passphrase** text boxes to set up a new passphrase for the token.
7. Complete the wizard.

Resetting a forgotten passphrase

If you have forgotten your token passphrase, you can reset it by completing the next steps.

To reset a forgotten passphrase

1. Open the Soft Token for Windows. For more information, see [Opening Soft Token for Windows](#) on page 22.
2. In the **Enter Passphrase** dialog box, click the **Tokens** button.
3. In the window that opens, click to select the token for which you want to reset the passphrase.
4. From the main menu, select **Token | Reset Passphrase**.
5. Complete the wizard to specify a new passphrase.

Setting the default token

If you have several tokens, you can set one of them as the default. The default token is automatically selected in the **Enter Passphrase** dialog box each time you open the Soft Token for Windows.

To set the default token

1. Open the Soft Token for Windows. For instructions, see [Opening Soft Token for Windows](#).
2. In the **Enter Passphrase** dialog box, click the **Tokens** button.
3. In the window that opens, right-click the token you want to set as the default.
4. On the shortcut menu, click **Default**.

Next time you open the Soft Token for Windows, this token will be automatically selected in the **Enter Passphrase** dialog box.

Deleting a token

To delete a token

1. Open the Soft Token for Windows. For instructions, see [Opening Soft Token for Windows](#).
2. In the **Enter Passphrase** dialog box, click the **Tokens** button.
3. In the window that opens, right-click the token, and then click **Delete**.
4. Complete the wizard to delete the token.

Viewing token details

You can view the token properties, such as token file name, location, serial number, encryption type, and response length and type.

To view token details

1. Open the Soft Token for Windows. For instructions, see [Opening Soft Token for Windows](#).
2. In the **Enter Passphrase** dialog box, click the **Tokens** button.
3. In the window that opens, right-click the token whose details you want to view.
4. Click **Properties**.

Uninstalling Soft Token for Windows

To uninstall Soft Token for Windows

1. Open the list of installed programs:
 - a. At a command prompt, type **appwiz.cpl**.
 - b. Press **ENTER**.
2. In the list of installed programs, click to select the **Defender Soft Token for Windows** entry.
3. Click **Uninstall** at the top of the list.

Authy

You can use the Authy app to authenticate and get access to resources protected with Defender. To start using Authy, you need to download, install, and activate the app.

For installation instructions, please refer to the Authy Web site at <https://www.authy.com>.

After installing Authy, you need to import an activation code into the app. You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Contact your system administrator to learn if the Defender Self-Service Portal is available to you and to obtain its address (URL). For more information, see [Downloading and activating a software token](#) on page 34.

Obtaining an Activation Code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for Authy.

Importing an activation code

To import an activation code

1. Open Authy.
2. Follow the on-screen instructions to import the activation code you have obtained.

You can use Authy to scan the QR code provided in the activation e-mail message and thus import the activation code into the app.

E-mail token

To use the e-mail token, you need to have access to the e-mail account to which Defender sends your one-time passwords (OTPs). For more information, contact your system administrator.

When you access a resource protected by Defender, you are prompted to enter your user name and password. You may also be prompted to enter your Defender PIN. Defender receives your request, generates a one-time password (OTP) and automatically sends it to your e-mail account. You should receive your OTP within seconds. Then, you need to enter your PIN and the OTP at the sign-in screen of the protected resource. If the entered PIN and OTP are correct, you are granted access to the protected resource.

Google Authenticator™

You can use Google Authenticator to authenticate and get access to resources protected with Defender. To start using Google Authenticator, you need to download, install, and activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Obtaining an Activation Code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for Google Authenticator.

After getting an activation code, you need to import it into Google Authenticator.

Importing an Activation Code

To import an activation code

1. Open Google Authenticator.
2. Follow the on-screen instructions to import an activation code.

You can use Google Authenticator to scan the QR code provided in the activation e-mail message and thus import the activation code into the app.

GrIDSure token

This section provides information on how to use the GrIDSure token to log on to a Windows-based computer or authenticate on a Web site protected with the GrIDSure personal identification system.

In this section:

- [Signing in to a Windows-based computer](#)
- [Authenticating on a Web site protected by GrIDSure](#)
- [How to configure and use your Personal Identification Pattern \(PIP\)](#)

Signing in to a Windows-based computer

To sign in to a Windows-based computer protected by GrIDSure

1. At the Windows sign-in screen, enter your user name and password.
Make sure you leave the **Passcode** text box empty.
2. Press ENTER.

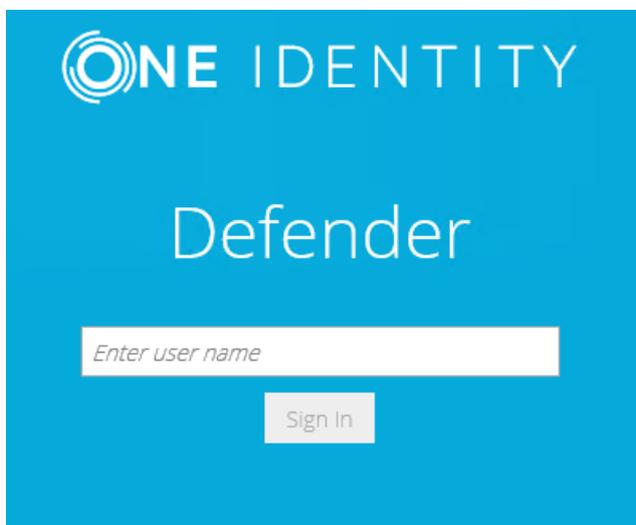
If you are using the GrIDSure token for the first time, you may be prompted to configure your GrIDSure Personal Identification Pattern (PIP). For more information, see [How to configure and use your Personal Identification Pattern \(PIP\)](#) on page 31.

3. When prompted, use the matrix of cells to type your PIP in the **Use your GrIDSure PIP** text box.
4. Press ENTER to sign in to Windows.

Authenticating on a Web site protected by GrIDSure

To authenticate on a Web site by using the GrIDSure token

1. In your Web browser, enter the address of the Web site you want to access.
If the Web site is protected with the GrIDSure personal identification system, the following page opens:

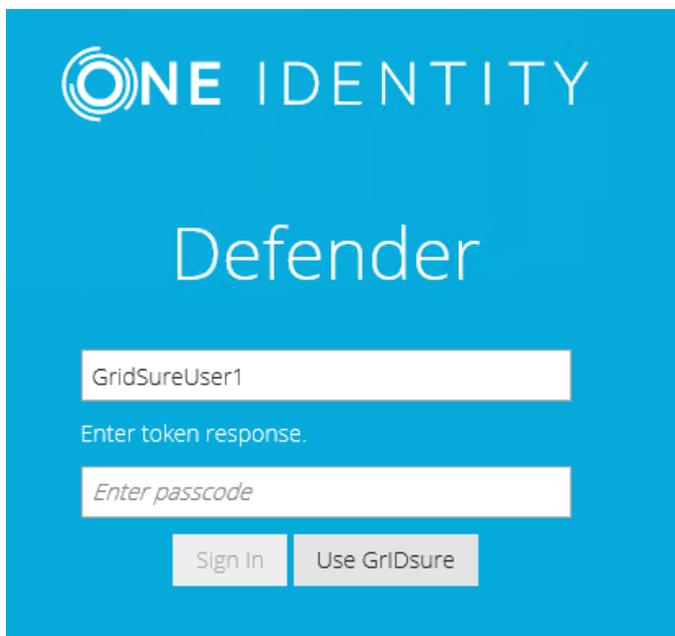


2. Type your user name, and then click **Sign In**.

The page prompts you to enter your Windows password:



Note that the page that opens may look differently if you have two or more different types of Defender Soft Token assigned:



In this case, click the **Use GrIDSure** button.

3. Type your Windows password, and then click **Sign In**.

If this is the first time you authenticate using the GrIDSure token, you may be prompted to configure your GrIDSure Personal Identification Pattern (PIP). For more information, see [How to configure and use your Personal Identification Pattern \(PIP\)](#) on page 31.

4. You are now prompted to authenticate using your GrIDSure PIP. Type the numbers located in the cells you chose when configuring your GrIDSure PIP:

The screenshot shows the ONE IDENTITY Defender authentication interface. At the top, the ONE IDENTITY logo is displayed. Below it, the word 'Defender' is centered. A text box contains the username 'GridSureUser1'. Below the username is a 6x6 grid of numbers. The numbers in the grid are: Row 1: 5, 7, 8, 1, 2, 1; Row 2: 0, 8, 3, 5, 5, 0; Row 3: 4, 2, 0, 4, 3, 2; Row 4: 4, 7, 8, 6, 3, 7; Row 5: 4, 2, 6, 9, 1, 0; Row 6: 5, 1, 6, 9, 9, 3. Below the grid is a checkbox labeled 'Reset PIP'. At the bottom, there is a text box labeled 'Enter passcode' and a 'Sign In' button.

In the **Enter passcode** text box, type your PIP, and then click **Sign In** to access the protected Web site.

You can select the **Reset PIP** check box to reset your current PIP after you sign in.

How to configure and use your Personal Identification Pattern (PIP)

To authenticate with the GrIDSure token, you need to use a special code which is called the GrIDSure Personal Identification Pattern (PIP).

When you access a resource protected with the GrIDSure personal identification system for the first time, you are prompted to configure your PIP. In this case, a matrix of cells similar to the following displays:

CC	AP	BC	AH	AI	BD
AM	AJ	BI	AD	AA	AE
AO	BF	CA	AN	AG	BN
AC	BE	AK	BG	BP	BB
BL	BJ	AB	CB	BM	BA
AF	BK	CD	AL	BO	BH

In this matrix, choose the cells you want to use for authentication, and then, in the **Configure your GrIDSure PIP** text box, type the codes contained in the cells you have chosen. Do not leave blank spaces between the codes.

For example, if you choose the first four cells in the first row of the matrix above, in the **Configure your GrIDSure PIP** text box, type **CCAPBCAH** (without spaces), and then press ENTER or click the **Login** button.

From now on, each time you authenticate with your GrIDSure token, you must use the codes displayed in the matrix cells you have chosen when configuring your PIP. These codes will be different each time the matrix of cells displays.

For example, next time the matrix may look as follows:

5	N	6	Q	I	E
9	D	7	X	4	V
0	B	G	Z	U	W
J	C	M	K	F	A
1	2	S	Y	P	H
R	8	3	T	O	L

In this case, use the **Use your GrIDSure PIP** text box to type **5N6Q**, and then press ENTER or click the **Login** button.

SMS token

To use the SMS token, you need to have an SMS-capable device that accepts SMS messages sent by Defender to your mobile phone number. For more information, contact your system administrator.

When you access a resource protected by Defender, you are prompted to enter your user name and password. You may also be prompted to enter your Defender PIN. Defender receives your request, generates a one-time password (OTP) and automatically sends it to your mobile phone number as an SMS message. You should receive your OTP within seconds. Then, you need to enter your PIN and the OTP at the prompt. If the entered PIN and OTP are correct, you are granted access to the protected resource.

VIP credential

Your system administrator may provide you with a VIP credential that allows you to authenticate and get access to resources protected with Defender. Before you start using the VIP credential for authentication, you need to register it. You can have your system administrator register the VIP credential for you or you can self-register the VIP credential on a Web site known as the Defender Self-Service Portal.

Contact your system administrator to learn if you can use the Defender Self-Service Portal to register your VIP credential and to obtain the address (URL) of the portal Web site.

Registering VIP credential

To self-register your VIP credential

1. In your Web browser, open the Defender Self-Service Portal Web site.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Click to select the **VIP credential** option, and then click **Next**.
5. Follow the on-screen instructions to register your VIP credential.

Software token

Your system administrator may configure a special Web site called the Defender Self-Service Portal. You can use the Defender Self-Service Portal to download and activate a software token with which you can then authenticate and get access to resources protected with Defender.

Contact your system administrator to learn if you can use the Defender Self-Service Portal to download and activate software tokens and to obtain the address (URL) of the portal Web site.

Downloading and activating a software token

To download and activate a software token

1. In your Web browser, open the Defender Self-Service Portal Web site.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to download and activate the software token you want.

Enabling the use of Microsoft Authenticator

You can use Microsoft Authenticator to authenticate and get access to resources protected with Defender. To start using Microsoft Authenticator, you need to download, install, and activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Obtaining an Activation Code on the Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Request a software token** option.
4. Follow the on-screen instructions to obtain an activation code for Microsoft Authenticator. After getting an activation code, you need to import it into Microsoft Authenticator.

Importing an Activation Code

To import an activation code

1. Open Microsoft Authenticator.
2. Follow the on-screen instructions to import an activation code. You can use Microsoft Authenticator to scan the QR code provided in the activation email message and thus import the activation code into the app.

Enabling the use of OneLogin Authenticator

You can use OneLogin Protect to authenticate and get access to resources protected with Defender. To start using OneLogin Protect, you need to download, install, and activate it by importing an activation code.

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

Obtaining an Activation Code on Defender Self-Service Portal

To obtain an activation code on the Defender Self-Service Portal

1. In your Web browser, open the Defender Self-Service Portal.
2. Sign in to the Defender Self-Service Portal.
3. Click the Request a software token option.
4. Follow the on-screen instructions to obtain an activation code for OneLogin Protect. After getting an activation code, you need to import it into OneLogin Protect.

Importing an Activation Code

To import an activation code

1. Open OneLogin Protect.
2. Follow the on-screen instructions to import an activation code. You can use OneLogin Protect to scan the QR code provided in the activation email message and thus import the activation code into the app.

Enabling the use of OneLogin Authenticator for Push Notification

You can use OneLogin Protect PUSH notifications to authenticate and get access to resources protected with Defender. To start using OneLogin Protect, you need to download and install it. Lastly, activate it by importing an activation code from OneLogin portal.

Defender Side Configuration

1. **Program the OneLogin Defender Token:** Program the OneLogin Token from ADUC for the user and do not activate it.
2. **Update User Properties:** Update the below User Properties from the ADUC (Active Directory Users and Computers) to sync the users with the OneLogin:
 - First Name
 - Last Name
 - Display Name

- Email (this email address will be used to login to OneLogin Portal with same AD Password)
3. **Input OneLogin API credential in Policy properties Dialog:** On install/Upgrade to Defender version 6.5.0, a new tab named **OneLogin Token** under policies **Properties Dialog** is visible. Admin needs to enter OneLogin API credentials to use OneLogin Push Notification with OneLogin protect app for that policy. Click **Apply** to save the credentials. To update credentials, click **UPDATE credentials**.

OneLogin Side Configuration - Creating a OneLogin Developer account

Create a OneLogin developer account at [Link](#). After Developer account creation, create new credentials:

1. Login to the Admin OneLogin Portal.
2. Go to Developers -> API Credentials.

3. Create a new credential.

Synchronizing User Data

Follow the below steps to Sync the AD Users with OneLogin:

1. Login using developers account credentials to the OneLogin portal using address: <subdomain>.onelogin.com.
2. Go to Users->Directories, then select Active Directory and download "onelogin_ad_connector.msi".
3. Copy the token generated and use it to install the "OneLogin Connector" tool.

Creating an Authentication Factor

To create a new "OneLogin Protect" Authentication Factor, follow the below steps:

1. Login to the Admin OneLogin portal
2. Go to "Authentication Factors" present under Security tab.
3. Create "OneLogin Protect" Authentication Factor

NOTE: OneLogin Protect App must be the primary Authentication factor.

Creating a Security Policy and assigning it to the user

Follow the below steps to create a security policy and to assign it to the user:

1. Login to the Admin OneLogin Portal.
2. Go to Security -> Policies.
3. Create a "New Users Policy" and under the "MFA" tab check the "OTP Auth Required" and "OneLogin Protect" option.
4. To assign the policy that you created, go to "Users" under "Users" tab.
5. Select the user whom you want to authenticate using OneLogin Protect Push Notification.
6. Go to "Authentication" tab and update the policy under the "User Security Policy" option.

Obtaining an activation code from the OneLogin portal

Follow the below steps to create and activate a OneLogin token:

1. Login to OneLogin portal with credentials whom you want to authenticate using OneLogin Protect Push Notification.
2. **Add the Security Factor and activate the token in “*OneLogin Protect*” App.**

Using hardware tokens

- [DIGIPASS 280 token](#)
- [DIGIPASS 301 CV token](#)
- [DIGIPASS GO 7 token](#)
- [VIP credential](#)
- [YubiKey token](#)
- [FIDO2 Compatible Yubikey](#)

DIGIPASS 280 token

The DIGIPASS 280 token is a synchronous hardware token that allows you to authenticate and get access to resources protected by Defender.



To authenticate and access resources protected by Defender, use the one-time password (OTP) application of the DIGIPASS 280 token (the OTP1 and OTP2 buttons). Currently, Defender does not support the e-signature application of the token (the SIGN1 and SIGN2 buttons).

The DIGIPASS 280 token works in synchronous mode. During the authentication process, the token generates an internal challenge. That challenge is based on an internally generated time clock. For successful authentication, Defender and the DIGIPASS 280 token must agree on the value in the token's time clock.

The value in the token's time clock can become out of sync with Defender. If this happens, you will not be able to use the token for authentication. In this case, contact your system administrator.

Before you start using the DIGIPASS 280 token for authentication, you need to register it. You can either have the system administrator register the token for you or you can register the token yourself.

Your system administrator may configure a special Web site called the Defender Self-Service Portal where you can register hardware tokens. Contact your system administrator to learn if you can use the Defender Self-Service Portal to register hardware tokens and to obtain the address (URL) of the portal Web site. For more information, see [Registering a hardware token](#) on page 49.

Authenticating with DIGIPASS 280 Token

To authenticate with the DIGIPASS 280 token

1. Access the resource protected by Defender.

A sign-in screen appears. If prompted, enter your user ID.

2. Use your DIGIPASS 280 token to generate a token response, also known as one-time password (OTP):
 - a. Press the power button to turn on the token.
 - b. When Pin appears on the token display, use the token keyboard to type the token PIN given to you by your system administrator.
 - c. When SELECT appears on the token display, press the **OTP1** or **OTP2** button on the token to generate a one-time password.

To generate the next one-time password, press the **C** or **OK** button, and when SELECT appears on the token display, press the **OTP1** or **OTP2** button.

3. Enter the generated OTP on the sign-in screen to authenticate and get access to the protected resource.

IMPORTANT: Ask your system administrator which token button you should press to generate OTPs: **OTP1** or **OTP2**. Your token may be configured so that for certain protected resources only one of these buttons generates valid OTPs.

DIGIPASS 301 CV token

The DIGIPASS 301 CV token is hardware token that allows you to authenticate and get access to resources protected by Defender.



The DIGIPASS 301 CV is designed specifically for visually impaired people. This hardware token has an internal speaker and can be used with headphones attached.

The DIGIPASS 301 CV is capable of converting generated one-time passwords (OTPs) into speech, so that token users could hear the OTPs through the internal speaker or attached headphones. This hardware token also provides speech-based user guidance and feedback of entered data and the functions the user selects.

With Defender, the DIGIPASS 301 CV token works in synchronous mode. During the authentication process, the token generates an internal challenge. That challenge is based on an internally generated time clock. For successful authentication, Defender and the DIGIPASS 301 CV token must agree on the value in the token's time clock.

The value in the token's time clock can become out of sync with Defender. If this happens, you will not be able to use the token for authentication. In this case, contact your system administrator.

Before you start using the DIGIPASS 301 CV token for authentication, you need to register it. You can either have the system administrator register the token for you or you can register the token yourself.

Your system administrator may configure a special Web site called the Defender Self-Service Portal where you can register hardware tokens. Contact your system administrator to learn if you can use the Defender Self-Service Portal to register hardware tokens and to obtain the address (URL) of the portal Web site. For more information, see [Hardware Token](#) on page 48.

Authenticating with DIGIPASS 301 CV token

To authenticate with the DIGIPASS 301 CV token

1. Access the resource protected by Defender.
A sign-in screen appears. If prompted, enter your user ID.
2. Use your DIGIPASS 301 CV token to generate a token response, also known as one-time password (OTP):
 - a. On the token keyboard, press the red  button to turn on the token.
 - b. When **PIN** appears on the token display, use the token keyboard to type the token PIN given to you by your system administrator.
 - c. When **APPLI** appears on the token display, press the **1** button on the token keyboard.
The value shown on the token display is your OTP.
3. Enter the generated OTP on the sign-in screen to authenticate and get access to the protected resource.

DIGIPASS GO 7 token

The DIGIPASS GO 7 token is a synchronous hardware token that allows you to authenticate to a protected network. The DIGIPASS GO 7 token is simple to use and administer, with no PIN or application selection required by the user and no initialization required by the administrator.

The DIGIPASS GO 7 token authenticates via a dialog between the user and the Defender Security Server. It offers the ultimate in user-friendly high security. The unique one-time password is displayed on a high contrast LCD display. The user reads the number in the display and enters it into the Defender prompt. The system uses the password as additional proof of identity. The password changes periodically, making it very difficult for an intruder to guess.

The DIGIPASS GO 7 token is a key-fob size piece of hardware.



The DIGIPASS GO 7 token can be carried in a pocket, around the neck for moving within the company, on a key ring or clipped to a belt. The token is very light - 13 grams and has an 6 - 8-character, liquid-crystal display (LCD). Each character is capable of displaying numbers (0-9).

The DIGIPASS GO 7 token works in synchronous mode. During the user authentication process, the token generates an internal challenge. The internal challenge is based on an internally generated time clock. For successful authentication with the Defender Security Server, the Defender Security Server and the Defender tokens must agree on the value in the token's time clock.

The value in the token's time clock can become out of sync with the Defender Security Server. If this happens, you will not be able to use the token for authentication. In this case, contact your system administrator.

DIGIPASS GO 7 is powered by a single 3-volt lithium battery (CR2025 or equivalent). The life of the battery is approximately 7 years from the date the token was purchased.

Before you start using the DIGIPASS GO 7 token for authentication, you need to register it. You can either have the system administrator register the token for you or you can register the token yourself.

Your system administrator may configure a special Web site called the Defender Self-Service Portal where you can register hardware tokens. Contact your system administrator to learn if you can use the Defender Self-Service Portal to register hardware tokens and to obtain the address (URL) of the portal Web site. For more information, see [Hardware Token](#) on page 48.

Authenticating with DIGIPASS GO 7 Token

To authenticate with the DIGIPASS GO 7 token

1. Access the resource protected by Defender.
2. When prompted, enter your user ID.
Defender prompts you to enter your token response.
3. Press the button on your DIGIPASS Go 7 token to generate a response.
4. Enter the response at the Defender prompt.

If this is the first time you have used your token, you can change the PIN from the one supplied by your security administrator to a PIN that only you know.

Changing PIN

To change your PIN

- During authentication, type the following syntax:
`<current initial PIN> <DIGIPASS GO 7 token response> <new PIN> <new PIN>`

YubiKey token

The YubiKey token is a device that connects to the USB port on your computer. The computer identifies the YubiKey as a USB keyboard and for this reason you can use the YubiKey on any operating system without installing a driver.



To generate a one-time password (OTP), touch the metal button on your YubiKey. The OTP is automatically entered at the current cursor position.

Before you start using the YubiKey token for authentication, you need to register it. You can either have the system administrator register the token for you or you can register the token yourself.

Your system administrator may configure a special Web site called the Defender Self-Service Portal where you can register hardware tokens. Contact your system administrator to learn if you can use the Defender Self-Service Portal to register hardware tokens and to obtain the address (URL) of the portal Web site. For more information, see [Registering a hardware token](#).

Registering YubiKey token

To self-register your YubiKey token

1. Insert the YubiKey token into a USB port on your computer.
2. In your Web browser, open the Defender Self-Service Portal page for registering your YubiKey token.
To obtain the page address (URL), contact your system administrator.
3. If prompted, sign in to the Defender Self-Service Portal.
The **Enter YubiKey one-time password** page opens.
4. Touch the metal button on your YubiKey token to insert the token serial number into the text box on the page.
5. Follow the on-screen instructions to complete the token registration.

FIDO2 compatible Hardware Yubikey

Defender 6.5.0 version supports FIDO2 compatible hardware Yubikey.

Basic Steps to use a FIDO2 token

- a. Requesting FIDO2 token on Defender Self-Service Portal
- b. Register token on ISAPI [One time operation]
- c. Authenticate/Login using FIDO2 registered token

Requesting FIDO2 Token program on the Defender Self-Service Portal

- a. Click on Request FIDO2 Token tile.
- b. Click on Program Token button.
- c. User should enter FIDO2 token Name:
 - Should be at least four characters
 - Special character and space are not allowed.
 - Maximum length of 40 characters
 - Underscore (_) is allowed
- d. Click on Next and window will display success message.
- e. FIDO2 token will appear in assigned token list of user with unique ID.
- f. FIDO2 tokens cannot be re-registered.
- g. In case an unregistered FIDO2 token is already present on the user's assigned token list, they cannot request a new token from the portal.

For more information, see Registering a hardware token.

To register a FIDO2 Token

FIDO2 tokens can be registered on ISAPI before authentication for the first time. This is a onetime operation.

- a. If FIDO2 tokens are already assigned to users, FIDO2 Registration screen will display list of unregistered FIDO2 tokens.
- b. Users need to select any one unregistered FIDO2 token to register.
- c. Users need to enter serial number of Token in serial number field.
 - Should be at least four characters
 - Special character and space are not allowed.

- Maximum length of 40 characters
 - Underscore (_) is allowed
- d. After entering the AD password, users need to click on Register button and browser pop-up will appear asking user to insert and touch on FIDO2 compatible YubiKey to complete the registration of FIDO2 token.
 - e. On successful registration, Login screen will appear for users to continue to authenticate.
 - f. During registration, users can authenticate using other assigned tokens by clicking on Sign in with another option, if they do not want to use FIDO2 token.
 - g. In case users have at least one already registered FIDO2 token, they need to click on the register button to register any unregistered tokens.

To login using a FIDO2 Token

- a. If user has registered FIDO2 tokens, they can initiate the login process by entering username on the login screen.
- b. On next screen, list of registered FIDO2 tokens will appear in combo list for User to
- c. Select one to continue authentication. If user has a single registered FIDO2 token, the browser pop-up will appear directly.
- d. After selecting registered FIDO2 token, on click of Sign in, browser pop-up will appear asking user to insert and touch the FIDO2 compatible YubiKey to match credentials stored while registration.
- e. Users need to touch the YubiKey within 20 seconds once browser pop-up appears for user input. On timeout, user can either reload session to continue login with FIDO2 token or choose Sign in with another option.
- f. If credentials match, user will be logged in to ISAPI.

For more information, see [Registering a hardware token](#).

Hardware Token

Your system administrator may provide you with a hardware token that allows you to authenticate and get access to resources protected with Defender. Before you start using the hardware token for authentication, you need to register it. You can either have the system administrator register the hardware token for you or you can register the token yourself.

Your system administrator may configure a special Web site called the Defender Self-Service Portal where you can register hardware tokens. Contact your system administrator to learn if you can use the Defender Self-Service Portal to register hardware tokens and to obtain the address (URL) of the portal Web site.

Registering a hardware token

To self-register a hardware token

1. In your Web browser, open the Defender Self-Service Portal Web site.
2. Sign in to the Defender Self-Service Portal.
3. Click the **Register a hardware token** option.
4. Follow the on-screen instructions to register your hardware token.

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