Copyright 2017 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 HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity make 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 do not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:
One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656
Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

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

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

Legend

⚠️ WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

ℹ️ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Defender Token User Guide
Updated - October 2017
Version - 5.9
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 .................................................................... 10
  Viewing token details ............................................................. 11
  Uninstalling Soft Token for Android ......................................... 11

Soft Token for BlackBerry® .......................................................... 11
  Installing Soft Token for BlackBerry .......................................... 11
    Installing from BlackBerry App World ..................................... 12
    Installing from Defender Self-Service Portal ......................... 12
  Activating Soft Token for BlackBerry ........................................ 12
    Obtaining an activation code on the Defender Self-Service Portal 13
    Importing an activation code ............................................... 13
  Creating a token ..................................................................... 13
  Authenticating with a token .................................................... 14
  Renaming a token .................................................................. 14
  Deleting a token .................................................................... 14
  Viewing token details ............................................................. 14
  Uninstalling Soft Token for BlackBerry ......................................... 15

Soft Token for iOS .................................................................... 15
  Installing Soft Token for iOS ................................................... 15
    Installing from App Store ..................................................... 15
    Installing Using Defender Self-Service Portal ......................... 16
Deleting a token

Viewing token details

Uninstalling Soft Token for Windows

Soft Token for Windows Phone

Installing Soft Token for Windows Phone
  Installing from Windows Phone Store
  Installing using Defender Self-Service Portal

Activating Soft Token for Windows Phone
  Obtaining an activation code through Defender Self-Service Portal
  Importing an activation code

Authenticating with a token

Creating an additional token

Renaming a token

Deleting a token

Viewing token details

Uninstalling Soft Token for Windows Phone

Authy
  Obtaining an Activation Code on the Defender Self-Service Portal
  Importing an activation code

E-mail token

Google Authenticator™
  Obtaining an Activation Code on the Defender Self-Service Portal
  Importing an Activation Code

GrIDsure token
  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)

SMS token

VIP credential
  Registering VIP credential

Software token
  Downloading and activating a software token

Using hardware tokens

DIGIPASS 280 token

Authenticating with DIGIPASS 280 Token
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.

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 BlackBerry®
- Soft Token for iOS
- Soft Token for Java
- Soft Token for Windows
- Soft Token for Windows Phone
- 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.

To start using the Soft Token for Android, you need to activate it (see Activating Soft Token for Android).

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 (see Activating Soft Token for Android).

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 (see [Activating Soft Token for Android](#)).

### 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.

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](#).

### 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.

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.
Viewing token details

You can view the details of your token, such as token name, type, 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.

Soft Token for BlackBerry®

- Installing Soft Token for BlackBerry
- Activating Soft Token for BlackBerry
- Creating a token
- Authenticating with a token
- Renaming a token
- Deleting a token
- Viewing token details
- Uninstalling Soft Token for BlackBerry

Installing Soft Token for BlackBerry

Installation methods:
- Installing from BlackBerry App World
- Installing from Defender Self-Service Portal
Installing from BlackBerry App World

For this method, your BlackBerry device must be connected to the Internet and have BlackBerry App World installed.

To install from BlackBerry App World

1. On your BlackBerry device, open BlackBerry App World.
2. In BlackBerry App World, search for and select Defender Soft Token.
3. Follow the on-screen instructions to download and install the Defender Soft Token. If prompted, reboot your BlackBerry device.

To start using the Soft Token for BlackBerry, you need to activate it (see Activating Soft Token for BlackBerry).

Installing from 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).

To install from 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 BlackBerry.

To start using the Soft Token for BlackBerry, you need to activate it (see Activating Soft Token for BlackBerry).

Activating Soft Token for BlackBerry

To start using the Soft Token for BlackBerry, 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.

**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 BlackBerry.

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

**Importing an activation code**

To import an activation code

1. On your BlackBerry device, open the Defender Soft Token app.
2. On the app screen, select **Enter Activation Code**.
3. Enter your activation code when prompted.

You can use a third-party QR code reader app on your device to scan the QR code provided in the activation e-mail, extract the activation code, and then copy and paste it into the Soft Token for BlackBerry.

**Creating a token**

To create a token

1. On your BlackBerry 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 BlackBerry 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.

Renaming a token

To rename a token

1. On your BlackBerry 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 BlackBerry 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.

Viewing token details

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

To view token details

1. On your BlackBerry 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 BlackBerry

To uninstall Soft Token for BlackBerry

1. On your BlackBerry device, tap and hold the Defender Soft Token app icon.
2. Depending on your BlackBerry device, either tap Delete or tap the recycle bin icon.
3. When prompted, confirm that you want to delete the app.

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.

Installing from App Store

To install from App Store

1. On your iOS device, open App Store.
3. Install the Defender Soft Token from the search results.
To start using the Soft Token for iOS, you need to activate it (see Activating Soft Token for iOS).

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.

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.

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.

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**, and then enter your activation code.
3. Wait for the activation to complete.

You can use a third-party QR code reader app on your device to scan the QR code provided in the activation e-mail, extract the activation code, and then copy and paste it into the Soft Token for iOS.

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**.

Authenticating with a token

Before you start using the Soft Token for iOS app, make sure you have activated the app. For details, see **Activating Soft Token for iOS**.

To authenticate with a token

- On your iOS 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 response.

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.

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. 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.

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
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.

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 (see Activating Soft Token for Java).

**Upgrading Soft Token for Java**

If you have Soft Token for Java 5.8 installed and want to upgrade to version 5.9, you need to install Soft Token for Java 5.9 side by side with the previous version. After installation of Soft Token for Java 5.9, 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 5.9, you may uninstall the previous version of the token. For instructions, see Uninstalling 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.

**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

<table>
<thead>
<tr>
<th>Windows 7</th>
<th>A later version of Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td>On the Apps screen, click the Uninstall Defender Soft Token for Java tile.</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>In the window that opens, click Uninstall.</td>
</tr>
</tbody>
</table>

Click Start.
Point to All Programs | One Identity| Defender Soft Token for Java
Click Uninstall Defender Soft Token for Java.
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.

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 (see Activating Soft Token for Windows).

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:

<table>
<thead>
<tr>
<th>Windows 7</th>
<th>Windows Server® 2008</th>
<th>A later version of Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Click Start.  
Point to All Programs | One Identity| Defender.  
Click Soft Token for Windows.

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.

**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 instructions, see [Opening Soft Token for Windows](#).

   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, follow the instructions in Opening Soft Token for Windows.

**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 instructions, see Opening Soft Token for Windows.

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 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 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.
Soft Token for Windows Phone

- Installing Soft Token for Windows Phone
- Activating Soft Token for Windows Phone
- Authenticating with a token
- Creating an additional token
- Renaming a token
- Deleting a token
- Viewing token details
- Uninstalling Soft Token for Windows Phone

Installing Soft Token for Windows Phone

Installation methods:
- Installing from Windows Phone Store
- Installing using Defender Self-Service Portal

Installing from Windows Phone Store

_To install from Windows Phone Store_

1. On your Windows Phone device, in the App list, tap Store (_costs). You may be prompted to sign in.
2. Tap Search to search for Defender Soft Token.
3. Download and install Defender Soft Token from the search results.

To access the installed Defender Soft Token, use the App list on your Windows Phone device.

To start using the Soft Token for Windows Phone (see Activating Soft Token for Windows Phone).

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 you can use the Defender Self-Service Portal and to obtain the address (URL) of the portal Web site.

**To install using Defender Self-Service Portal**

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 install the Soft Token for Windows Phone.

After downloading and installing the Soft Token for Windows Phone, you need to activate it (see **Activating Soft Token for Windows Phone**).

---

**Activating Soft Token for Windows Phone**

To begin using the Soft Token for Windows Phone, you need to activate it by importing an activation code. You can get an activation code from your Defender administrator or through the Defender Self-Service Portal.

- Obtaining an activation code through Defender Self-Service Portal
- Importing an activation code

---

**Obtaining an activation code through 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 you can use the Defender Self-Service Portal and to obtain the address (URL) of the portal Web site.

**To obtain an activation code**

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 obtain an activation code for the Soft Token for Windows Phone.

After getting an activation code, you need to import it onto your Windows Phone device (see **Importing an activation code**).
Importing an activation code

To start using the Soft Token for Windows Phone, you need to import an activation code onto your Windows Phone device. You can get an activation code from your Defender administrator or through the Defender Self-Service Portal.

To import the activation code
1. On your Windows Phone device, in the App list, tap the Defender Soft Token app.
2. On the start page of the token, tap Enter Activation Code.
3. When prompted, type a name and activation code for the new token.
   You can use a third-party QR code reader app on your device to scan the QR code provided in the activation e-mail, extract the activation code, and then copy and paste it into the Soft Token for Windows Phone.
4. When finished, tap the check mark icon.
   The numeric value in the token response that appears is your one-time password (OTP). Enter the OTP in the Defender Authentication text box when accessing a resource protected by Defender.

Authenticating with a token

To authenticate with a token
1. On your Windows Phone device, open the Defender Soft Token app.
2. Tap tokens, and then tap the token you want to use.
   The numeric value in the token response that appears is your One Time Password (OTP). Enter the OTP in the Defender Authentication text box when accessing a resource protected by Defender.

Creating an additional token

After creating and activating an initial token in the Defender Soft Token app, you can create additional tokens.

To create an additional token
1. On your Windows Phone device, open the Defender Soft Token app.
2. Tap the plus sign, and then enter a name and activation code for the token.
3. When finished, tap the check mark icon.
Renaming a token

To rename a token
1. On your Windows Phone 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 Windows Phone 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.

Viewing token details

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

To view token details
1. On your Windows Phone 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 Windows Phone

To uninstall Soft Token for Windows Phone
1. In the App list, tap and hold Defender Soft Token.
2. Tap Uninstall.
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.


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.

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).
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:

   ![Defender Sign In Page](image)

   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)](How%20to%20configure%20and%20use%20your%20Personal%20Identification%20Pattern%20%28PIP%29).  

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:
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:

```
<table>
<thead>
<tr>
<th>CC</th>
<th>AP</th>
<th>BC</th>
<th>AH</th>
<th>AI</th>
<th>BD</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM</td>
<td>AJ</td>
<td>BI</td>
<td>AD</td>
<td>AA</td>
<td>AE</td>
</tr>
<tr>
<td>AO</td>
<td>EF</td>
<td>CA</td>
<td>AN</td>
<td>AG</td>
<td>BN</td>
</tr>
<tr>
<td>AC</td>
<td>BE</td>
<td>AK</td>
<td>BG</td>
<td>BP</td>
<td>BB</td>
</tr>
<tr>
<td>BL</td>
<td>BJ</td>
<td>AB</td>
<td>CB</td>
<td>BM</td>
<td>BA</td>
</tr>
<tr>
<td>AF</td>
<td>BK</td>
<td>CD</td>
<td>AL</td>
<td>BO</td>
<td>BH</td>
</tr>
</tbody>
</table>
```

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:
In this case, use the **Use your GrIDsure PIP** text box to type **SN6Q**, 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.
Using hardware tokens

- DIGIPASS 280 token
- DIGIPASS 301 CV token
- DIGIPASS GO 7 token
- VIP credential
- YubiKey token

**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.

**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 your 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.
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.

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 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.
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.
Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product