Certificate Services
Document Signing Guide

(Microsoft Windows PowerShell script token pickup method)

SafeNet Authentication Client, Version 10.8

For software release 13.7

Date of issue: October 2023

Document issue: 1.0

Entrust and the Hexagon Logo are trademarks, registered trademarks and/or services marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

© 2023 Entrust Corporation. All rights reserved.

TOC

About this guide 1

Obtaining technical assistance 2
Technical support 2
Telephone numbers 2
Email address 2
Related documentation 3
Documentation feedback 3

Installing (Picking up) your Entrust certificate 5

Preparing to download the certificate 6
Supported platforms and software 6
Supported operating systems 6
Supported browsers 6
Supported versions of Adobe Acrobat 6
Supported Microsoft products 6
Before you start 7
Downloading and installing the token software (required for USB token pickup) 8
Initializing an Entrust USB token 15
Picking up your Entrust certificate 23
Prerequisites 23
Administrators using the Certificate Services interface 23
Install the certificate on an Entrust USB token using a PowerShell script 23
Install certificate to an Entrust USB token using Microsoft Internet Explorer or Microsoft Edge 33
Configuring Microsoft Edge 33
Changing the password for your token 37
Recovering a certificate 39

Signing a document 41

Signing a PDF document 42
Signing a Microsoft Word document 47

About

About this guide

This guide describes how to store an Entrust certificate on a SafeNet USB token. This includes:

- installing your token (drivers and software)
- initializing your token
- accessing the Entrust Certificate Retrieval Web pages to store the certificate on your token

This guide also provides examples of how to sign and/or certify a document or form. For more advanced features, see the documentation accompanying the software product in which you are performing the signing operation.

Revision information

Document issue	Section	Revision
Issue 1.0	N/A	First release for 13.6

Obtaining technical assistance

Entrust recognizes the importance of providing quick and easy access to our support resources. The following subsections provide details about the technical support and information available to you.

Technical support

For Entrust technical support services, visit our Web site at:

http://www.entrust.net/ssl-technical/index.htm

For technical resources, including a comprehensive Knowledge Base visit:

https://www.entrust.com/knowledgebase/ssl

Telephone numbers

For support assistance by telephone, call one of the numbers below:

- 1 (866) 267-9297 (toll free within North America)
- 1 (613) 270-2680 (outside North America)

Email address

The email address for Customer Support is:

ecs.support@entrust.com

Related documentation

This section describes related documents that may be used in conjunction with this guide.

- Token software information (https://cpl.thalesgroup.com/access-management/safenet-trusted-access)

Documentation feedback

You can rate and provide feedback about Entrust product documentation by completing the online feedback form. Any information that you provide goes directly to the documentation team and is used to improve and correct the information in our guides. You can access this form by:

- clicking the *Report any errors or omissions* link located in the footer of Entrust PDF documents.
- following this link: http://go.entrust.com/documentation-feedback

1

Installing (Picking up) your Entrust certificate

This chapter describes how to prepare a token and download an Entrust certificate.

This guide assumes that you have already submitted the certificate request, it has been approved, and you are ready to download the certificate.

This chapter includes the following sections:

- "Preparing to download the certificate" on page 6
- "Before you start" on page 7
- "Downloading and installing the token software (required for USB token pickup)" on page 8
- "Initializing an Entrust USB token" on page 15
- "Picking up your Entrust certificate" on page 23
  - "Install the certificate on an Entrust USB token using a PowerShell script" on page 23
  - "Install certificate to an Entrust USB token using Microsoft Internet Explorer or Microsoft Edge" on page 33
- "Changing the password for your token" on page 37
- "Recovering a certificate" on page 39

Preparing to download the certificate

Supported platforms and software

The software and token provided by Entrust were tested with the following operating systems. They may also work with other operating systems, but it has not been tested. Similarly, Entrust document signing certificates were tested with the Adobe and Microsoft products listed below.

Supported operating systems

The following operating systems are supported:

- Microsoft Windows 11 (version 21H2)
- Microsoft Windows 10 (version 21H1 or earlier) 32-bit or 64-bit
- Microsoft Windows Server 2019 64-bit
- Microsoft Windows Server 2016 64-bit

Supported browsers

- Microsoft Edge—latest
- Google Chrome—latest
- Mozilla Firefox—latest

Supported versions of Adobe Acrobat

The following versions of Adobe Acrobat are supported:

- Adobe Acrobat XI Standard
- Adobe Acrobat XI Pro
- Adobe Acrobat X Standard
- Adobe Acrobat X Pro
- Adobe Acrobat 9 Standard
- Adobe Acrobat 9 Pro
- Adobe Acrobat DC

Supported Microsoft products

Microsoft Office

Before you start

To download an Entrust certificate, you need:

- a supported browser with Internet access (see Supported browsers)
- a supported operating system (see Supported operating systems)
- an iKey 5110 CC token (provided by Entrust)
- a supported product for signing documents (see Supported versions of Adobe Acrobat)

To contact Certificate Services Support, ECS.Support@entrust.com.

Note:
Certificate Services offers a USB token pickup process that does not rely on the features of Microsoft Internet Explorer. The new process requires the use of a Microsoft Windows PowerShell script.

This guide provides the details for running the new pickup process. The steps are quite different from those for using Microsoft Internet Explorer or Microsoft Edge with an Entrust certificate on a SafeNet token.

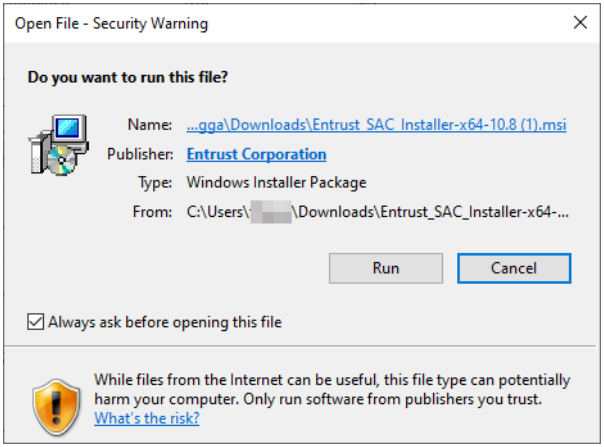
Downloading and installing the token software (required for USB token pickup)

You must install the token software provided by Entrust in order to manage your token. Once done, you can log in, initialize the token, and reset your password. If you do not have this software installed, install it as described in the following procedures.

Attention:
Do not plug your token into your computer until you have completed this procedure.

To obtain and install the token authentication client

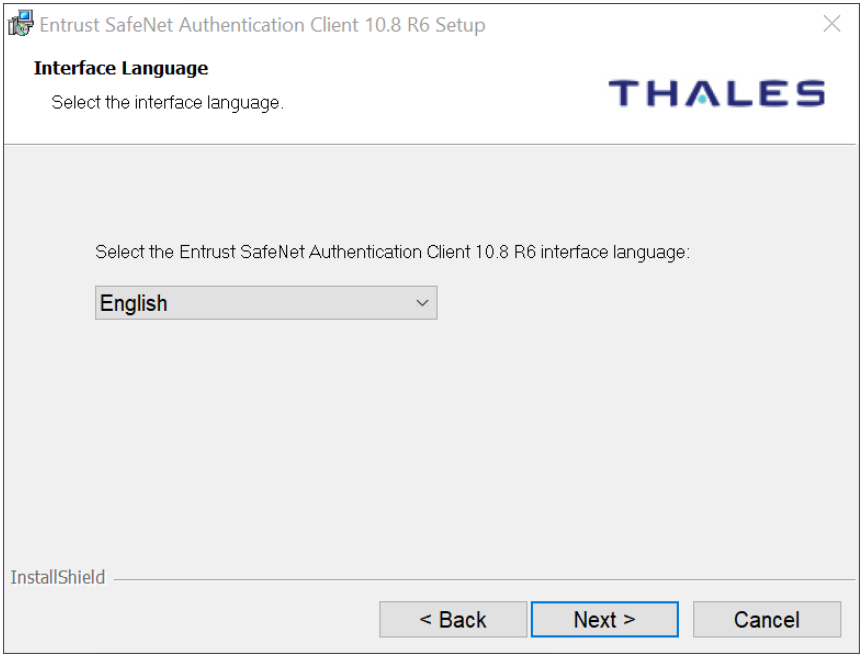
1. Download the SafeNet Token Authentication Client installer:
   - For the 32-bit installer: https://www.entrust.net/pickup/downloadSafeNetClient?xsize=32
   - For the 64-bit installer: https://www.entrust.net/pickup/downloadSafeNetClient?xsize=64
2. Double-click the `EntrustSACInstaller_<number>.msi` file to begin installing the software.
3. You may see this security warning. Click **Run**.



The installation wizard appears.

4 Click **Next**.

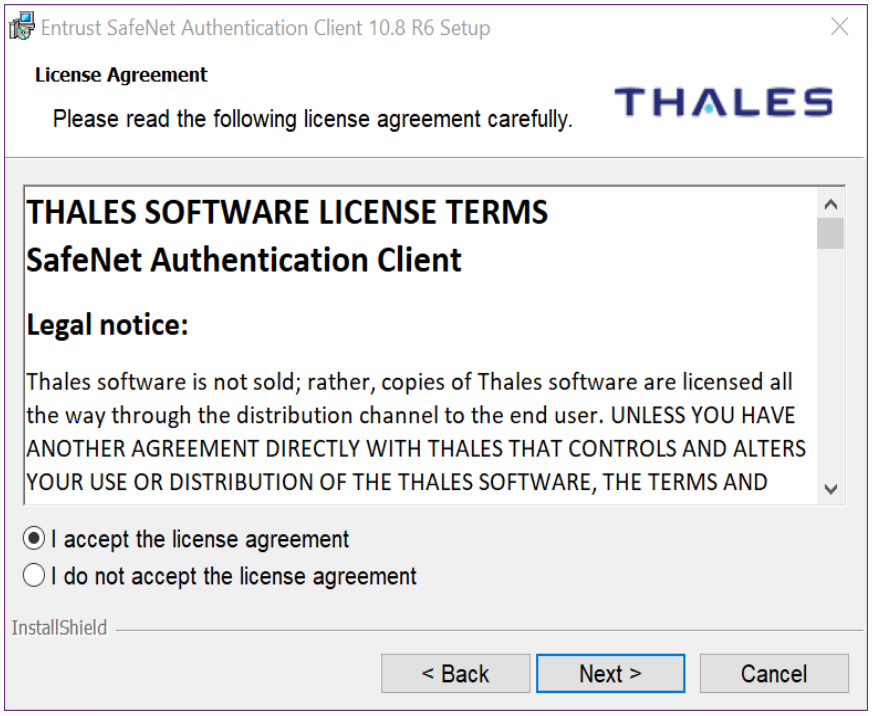
The **Interface language** page appears.



5 Select the language to use for the installation.

6 Click **Next**.

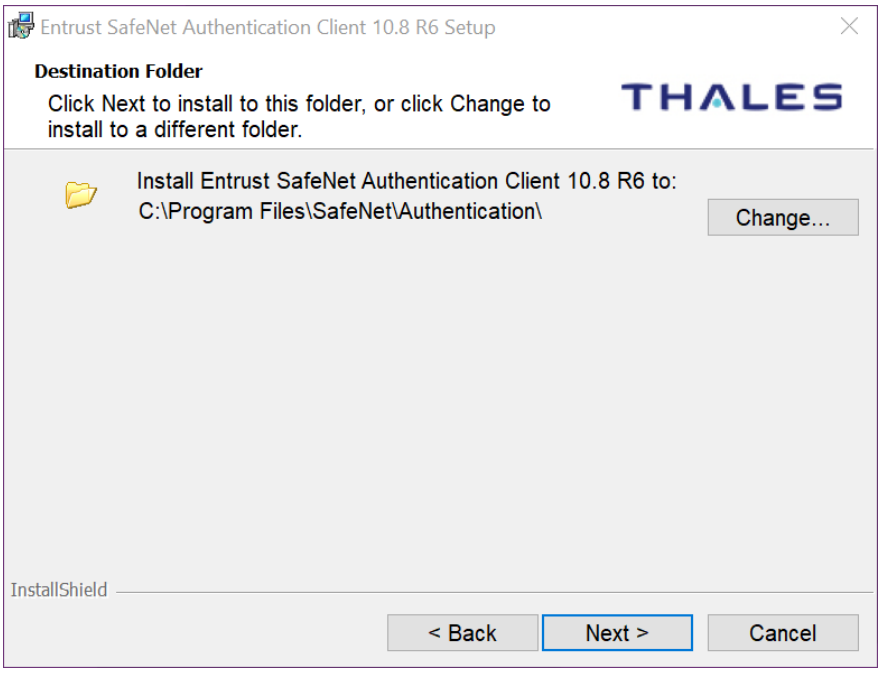
The **License Agreement** screen appears.



7 Read the agreement and select **I accept the license agreement**.

8 Click **Next**.

The Destination Folder screen appears.



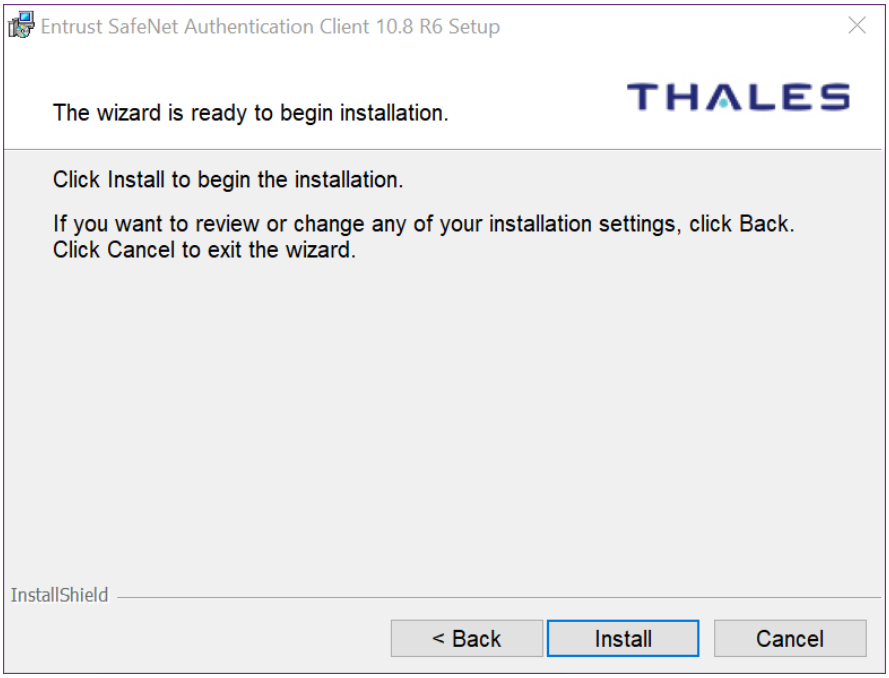
9 Accept the default folder or click **Change** to choose a new folder.

10 Click **Next**.

11 The installation screen appears. Click **Install**.

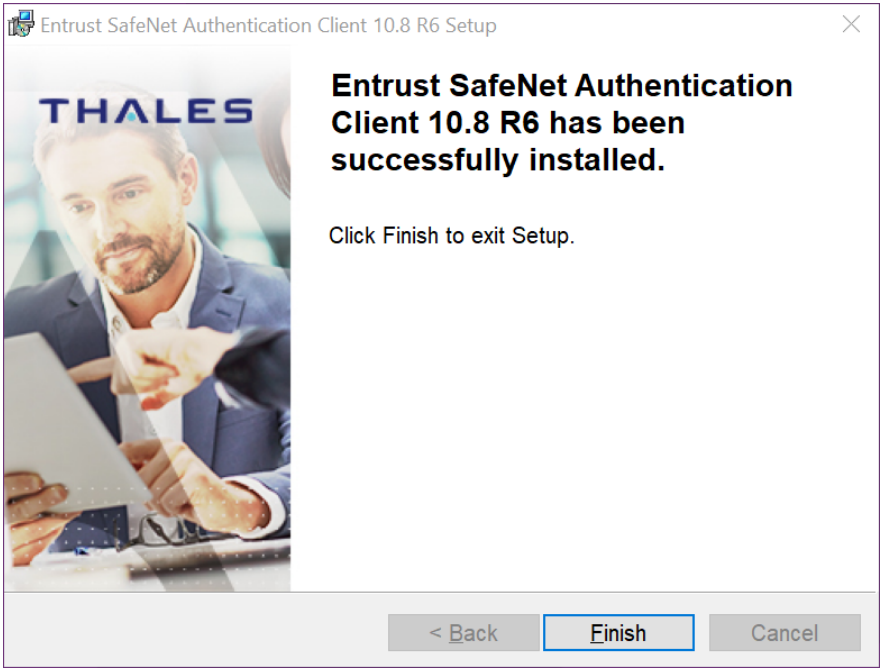
12 You may be asked to allow the installer to make changes to the hard drive of the computer. Allow it to proceed.

The installation screen appears.



13 Click **Install**.

14 When the installation is complete, a success message appears.



15 Click **Finish**. You have successfully installed the token software.

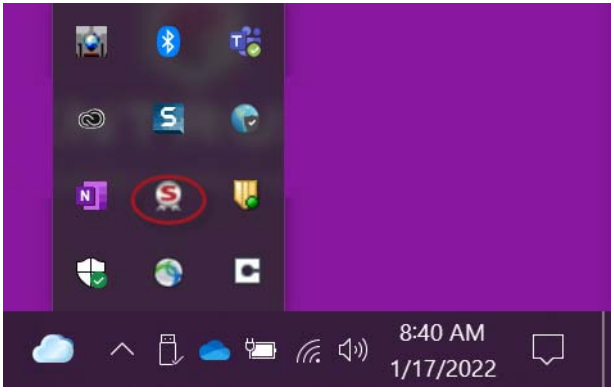
Initializing an Entrust USB token

Initialize the new token so it can store your certificate. If your token is already initialized, skip to: "Picking up your Entrust certificate" on page 23.

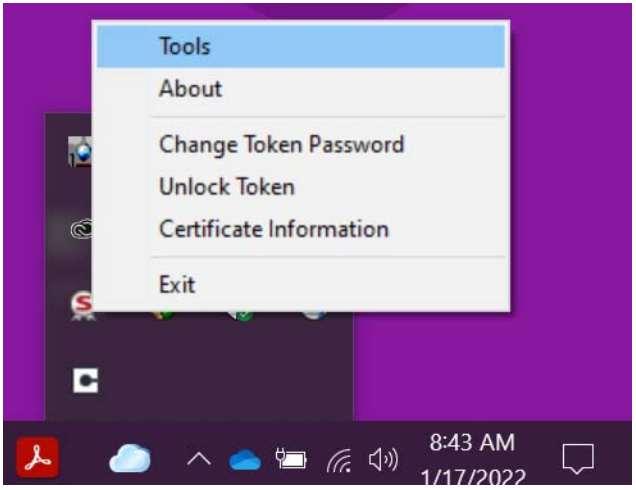
Attention:
This procedure is needed for new tokens. If the token already contains certificates, initializing the token will delete all existing certificates.

To initialize your token

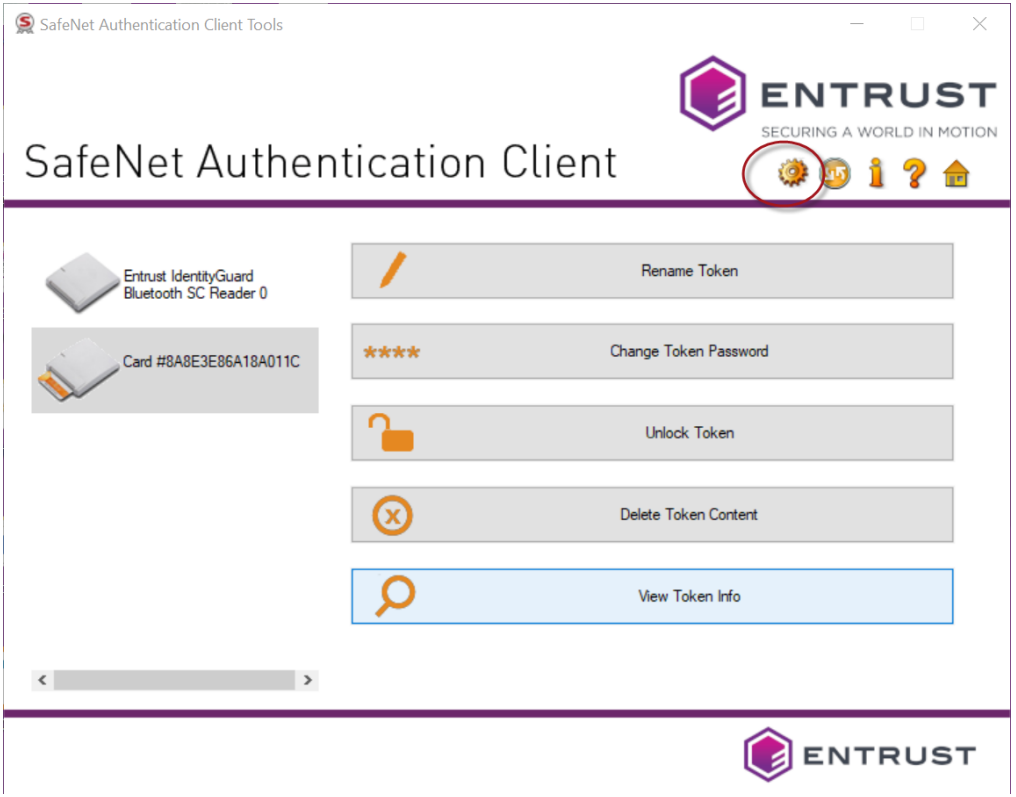
1 Insert your token into a USB port on your computer. When the token has been recognized by the computer and the drivers have been installed, the SafeNet icon in the system tray switches from grayed-out to active.



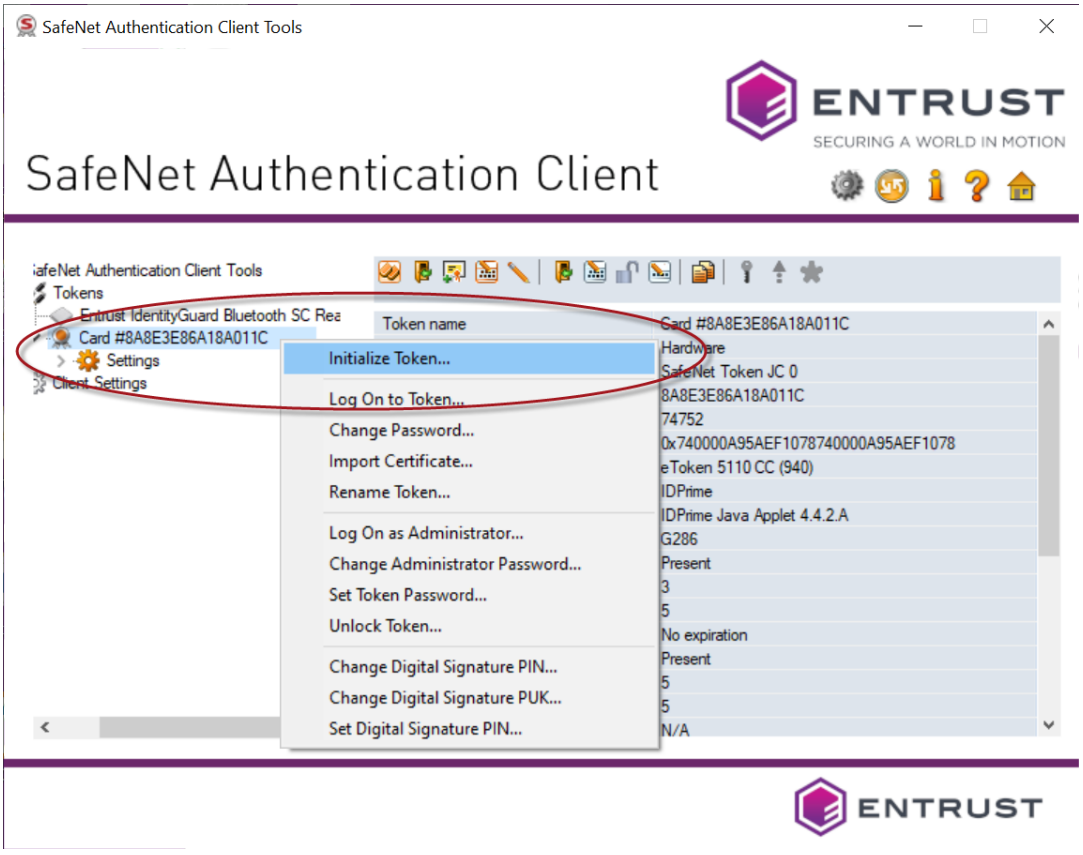
2 When the icon becomes active, right-click on it to open the menu. Select **Tools**.



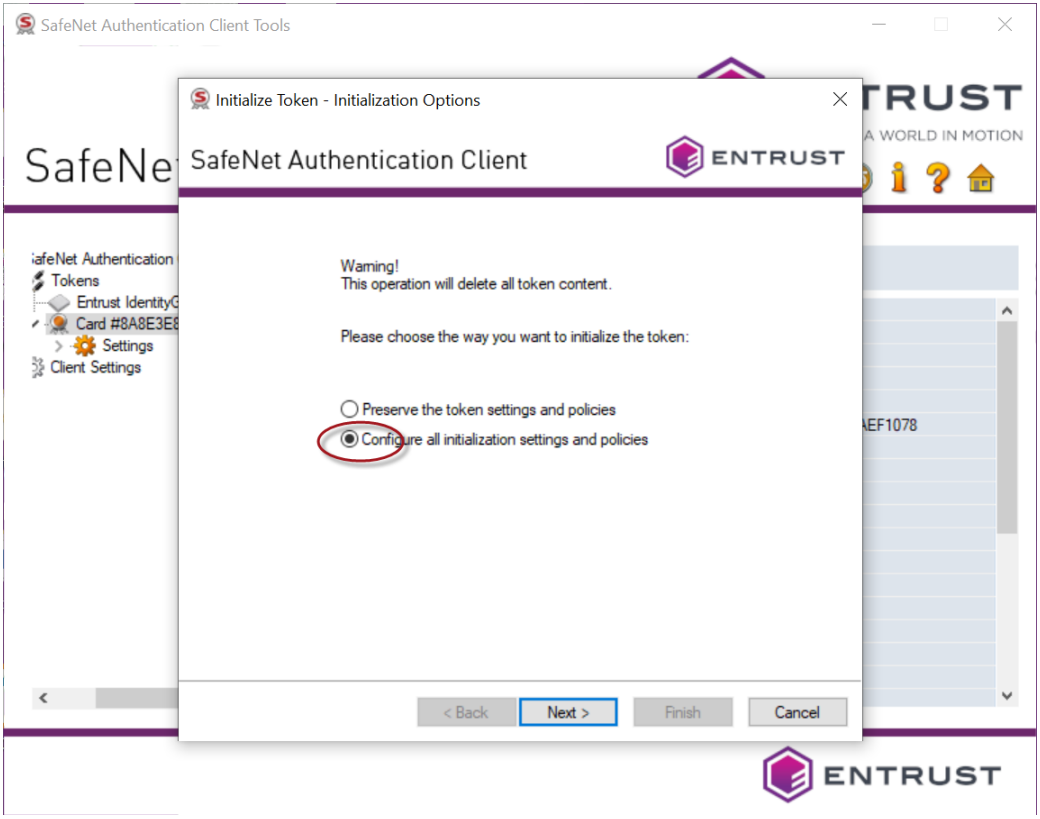
3 The SafeNet Authentication Client opens. Click the gear icon at the top right.



4 In the menu tree on the left, click to expand **Tokens**. Right-click your token and select **Initialize Token**.

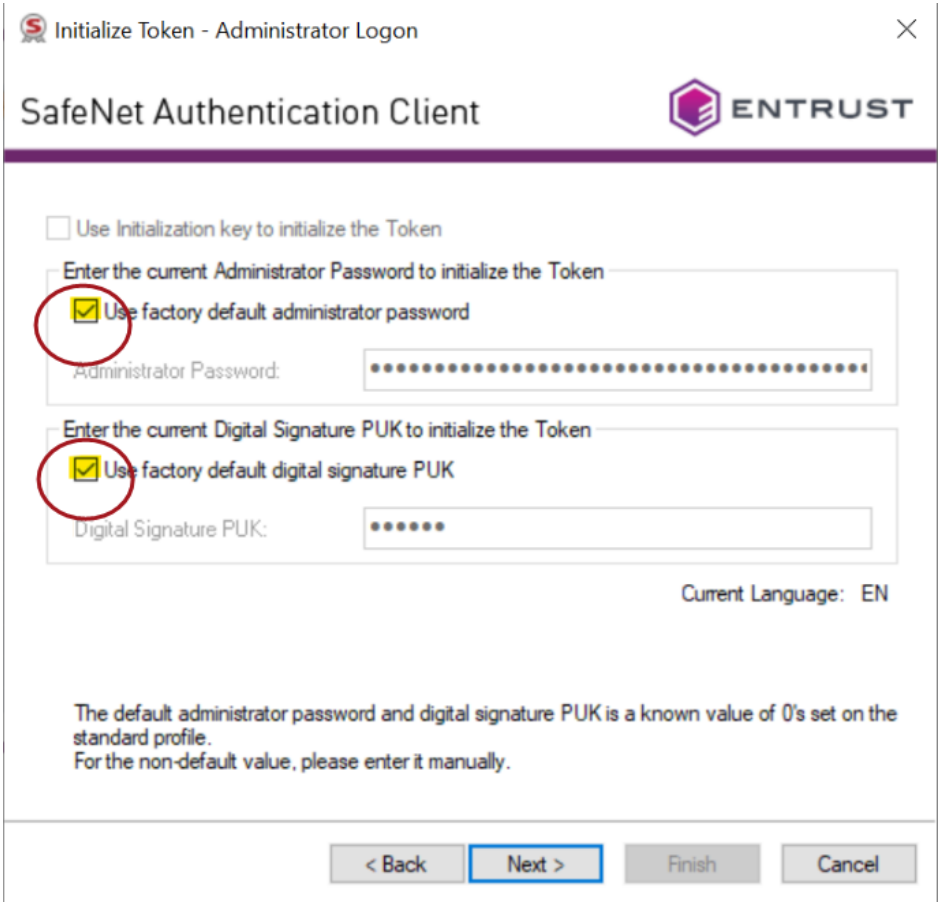


5 In the **Initialize Token - Initialization Options** window, select **Configure all initialization settings and policies**.



6 Click **Next**.

The **Administrator Logon** page appears.

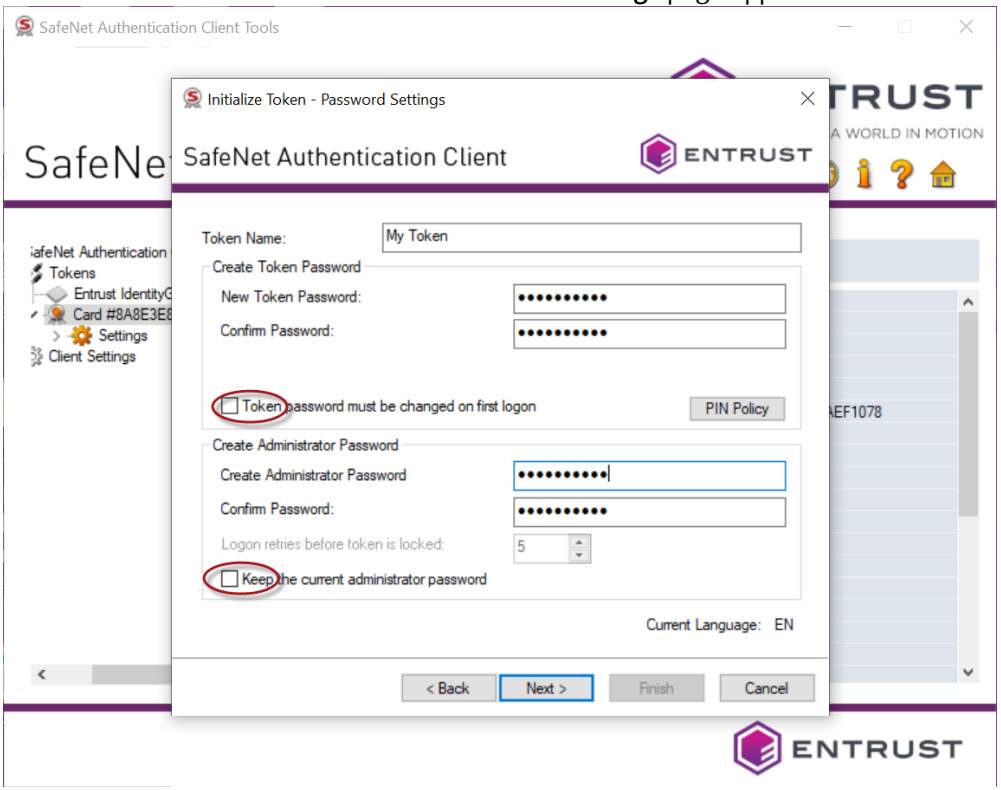


7 Select **Use factory default administrator password** and leave the default (48 zeros).

8 Select **Use factory default digital signature PUK** (Personal Unlock Key number) and leave the default value (6 zeros).

9 Click **Next**.

The **Initialize Token - Password Settings** page appears.



10 Enter the following settings and passwords.

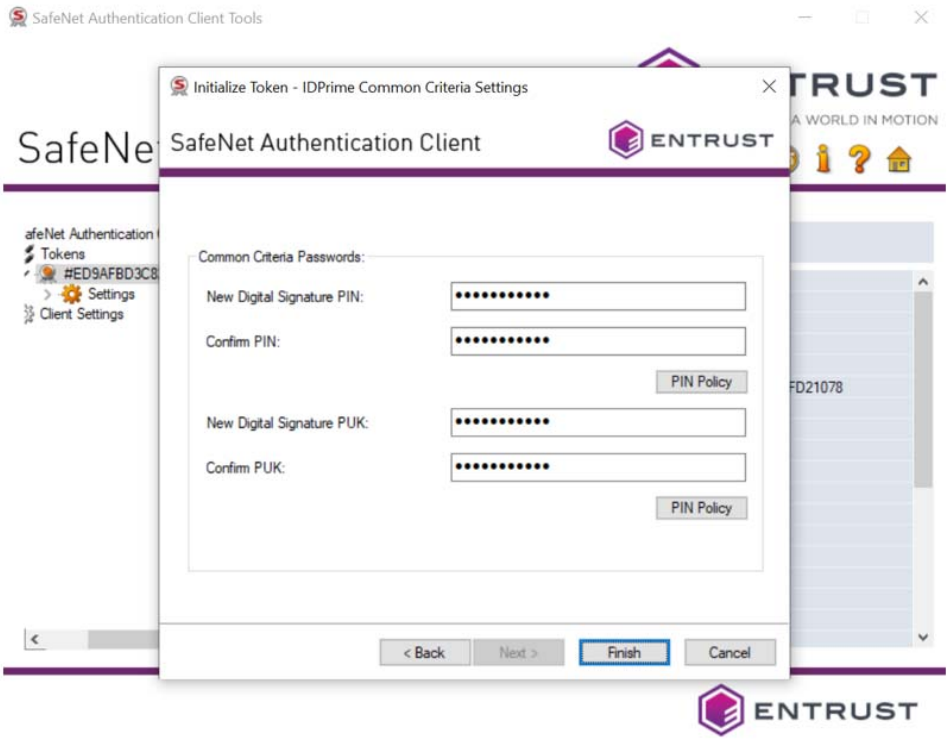
- **a** Enter a name for your token.This can be any name you choose.
- **b** Create and confirm your token password.
- **c** Deselect **Token password must be changed on first logon**.
- **d** Create and confirm your Administrator password.
- **e** Deselect **Keep the current administrator password**.

Attention:
You will be asked for this password when you use the certificate. It is important that you either remember this password or store it in a secure location. **If you enter the wrong password more than five times, the token will lock and cannot be unlocked**. You will need to buy a new token—Entrust will not replace it for free.

11 Click **Next**.

The **Initialize Token - IDPrime Common Criteria Settings** dialog box appears.

12 In the **Initialize Token - IDPrime Common Criteria Settings** window, create a new Digital Signature PIN and New Digital Signature PUK for your token.



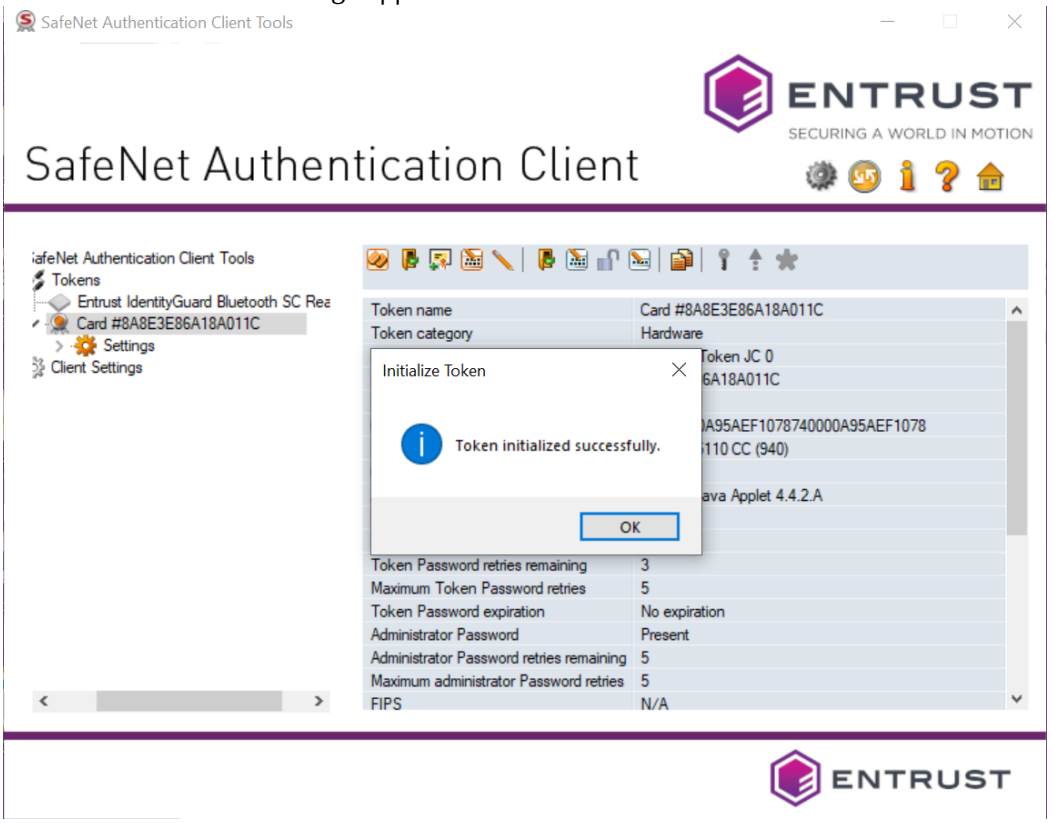
Attention:
Keep your passwords and PINs in a safe place. This includes your Token password, Administrator password, Digital Signature PIN and New Digital Signature PUK.

13 Click **Finish**.

A status bar opens, indicating the progress of the initialization. You may see a warning dialog box, **The token initialization process will delete all token content and resent all token parameters.**

14 Click **OK** to complete the initialization.

15 A success message appears. Click **OK**.



When the initialization is complete, the software displays a success message.

Picking up your Entrust certificate

Prerequisites

To pick up and install a certificate to a token, you must already have completed these two pre-conditions:

- The SafeNet Authentication Client software must be installed on your Microsoft Windows machine. If that's not been done, follow the instructions in: "Downloading and installing the token software (required for USB token pickup)" on page 8
- The Entrust USB token must be initialized. If that's not been done, follow the instructions in: "Initializing an Entrust USB token" on page 15

Installing a certificate on an Entrust USB token

There are two ways to install the certificate on a token. The first uses a PowerShell script and can be performed on any browser. The other requires the use of the Microsoft Internet Explorer or Microsoft Edge browser (legacy method).

- "Install the certificate on an Entrust USB token using a PowerShell script" on page 23
- "Install certificate to an Entrust USB token using Microsoft Internet Explorer or Microsoft Edge" on page 33

Administrators using the Certificate Services interface

This procedure explains how an Entrust Certificate Services administrator can pick up a certificate from the interface.

To pick up a certificate from the interface

1. Navigate to **Certificates** > **Managed Certificates** > **Pending User Pickup**.
2. Select the certificate.
3. To access the certificate pickup pages, click **Actions** > **Pickup**.

   Other users will receive an email message containing a link to the pickup page.

Install the certificate on an Entrust USB token using a PowerShell script

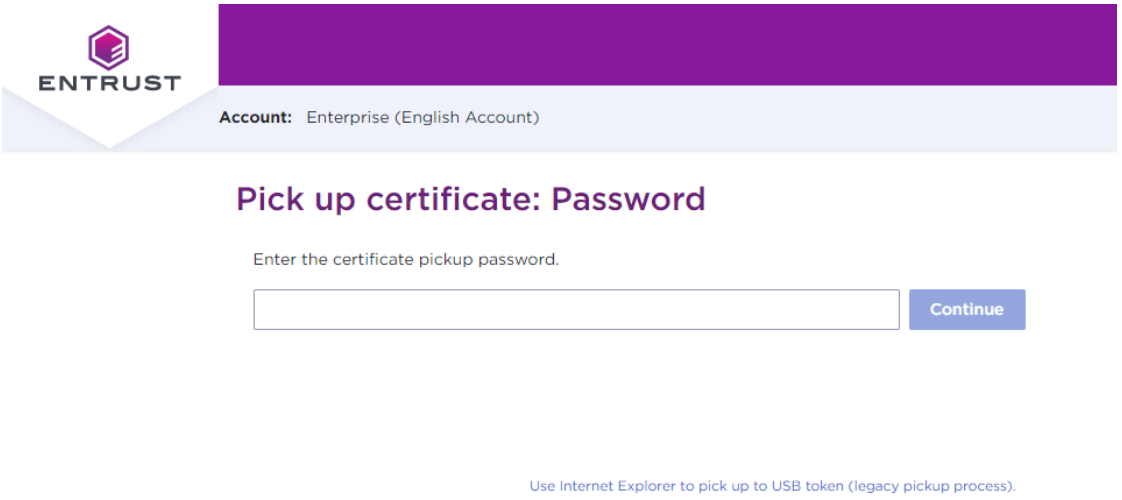
This is the recommended procedure for picking up your certificate and installing it on an Entrust USB token. It can be used with all supported browsers.

This procedure uses an Entrust-specific Microsoft Windows PowerShell script to install the certificate on your token. The steps in the following procedure will guide you through downloading and running the token-cert-installer script in a PowerShell window.

To download a certificate to an Entrust USB token using a PowerShell script

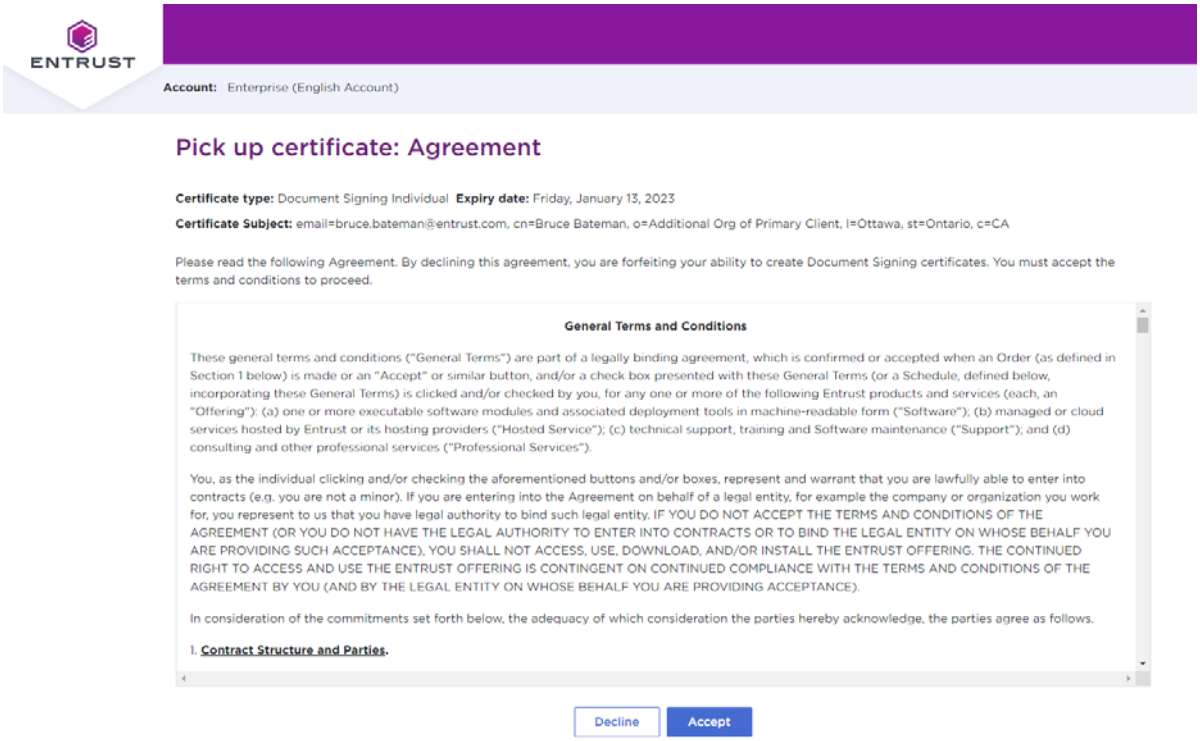
1. In the notification email sent to you by Entrust, click the link to the Entrust Certificate Retrieval Web pages.

   The Entrust Certificate Pickup page appears.

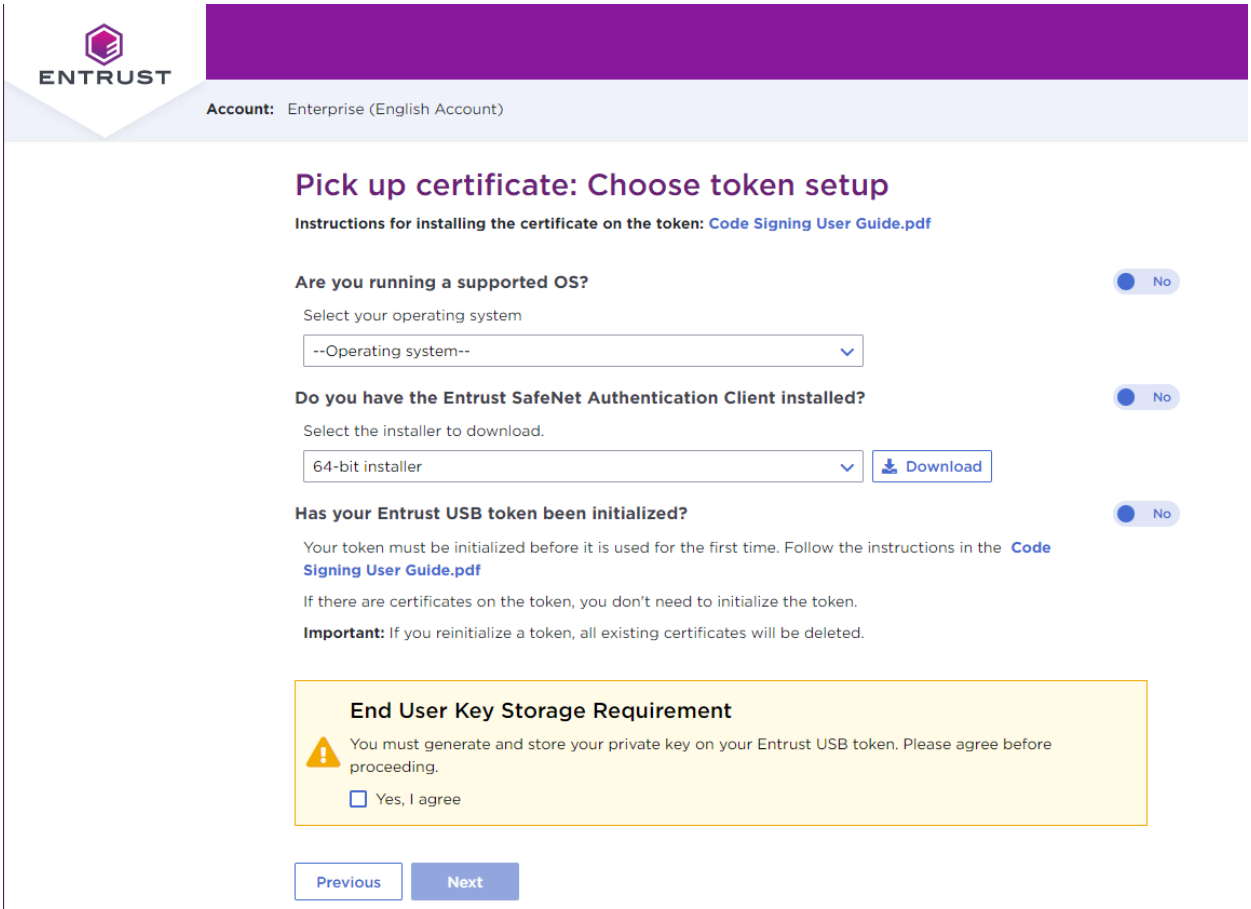


2. Enter the password that you used when you created the certificate request or the password obtained from your Certificate Administrator and click **Continue**.
3. You may see a warning that the browser is attempting to perform a certificate operation on your behalf. Allow the operation.

4 Read and accept the Entrust Certificate Services Agreement, and click **Accept**.



5 The **Choose token setup** screen appears.



6 From **Are you running a supported OS**, select your operating system. The toggle automatically switches to **Yes** when you select a supported OS.

7 In **Do you have the Entrust SafeNet Authentication Client installed**:

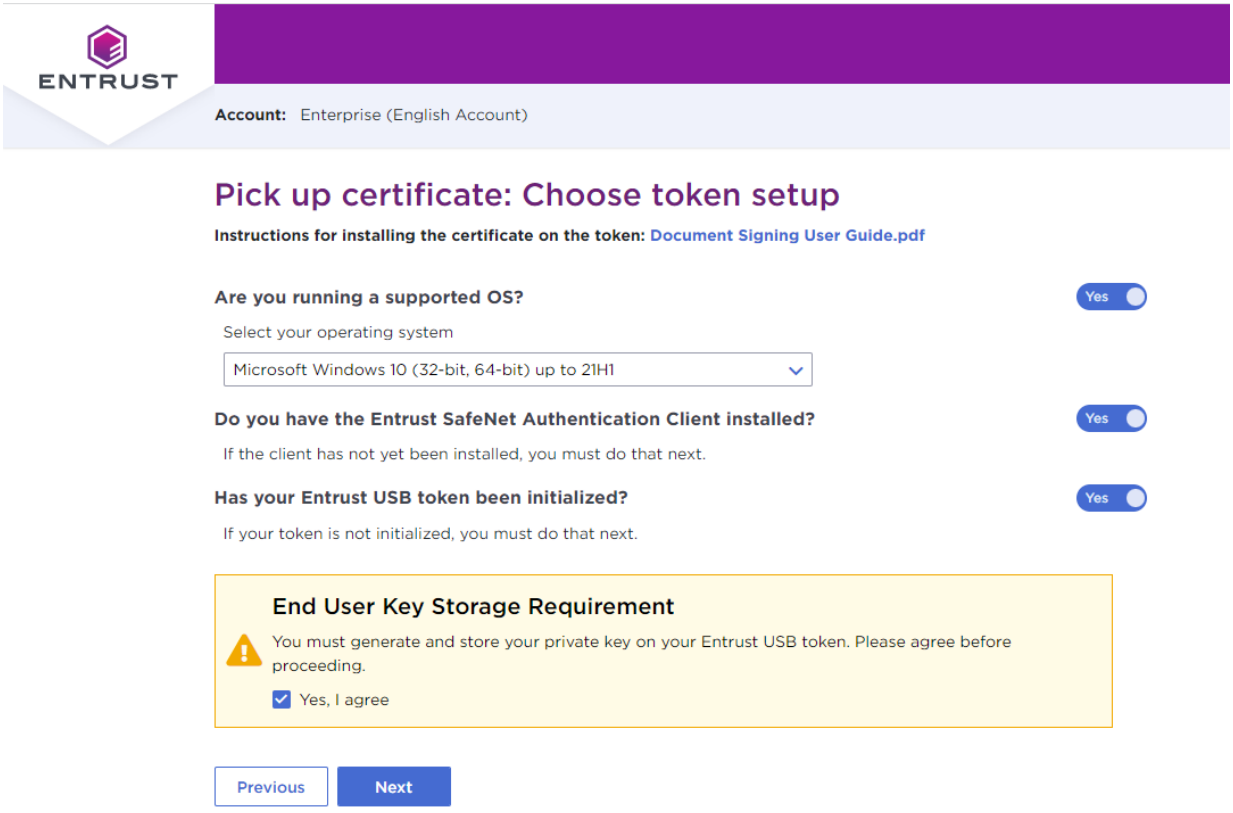
- If the SafeNet client is already installed, change the toggle to **Yes**, and continue with the next step.
- If the SafeNet client is not yet installed, follow the procedure in: "To obtain and install the token authentication client" on page 8. When the SafeNet software is installed, return to this browser page and this procedure to continue.

8 In **Has your Entrust USB token been initialized**:

- If the USB token is already initialized, click to change the toggle to **Yes**, and continue with the next step.

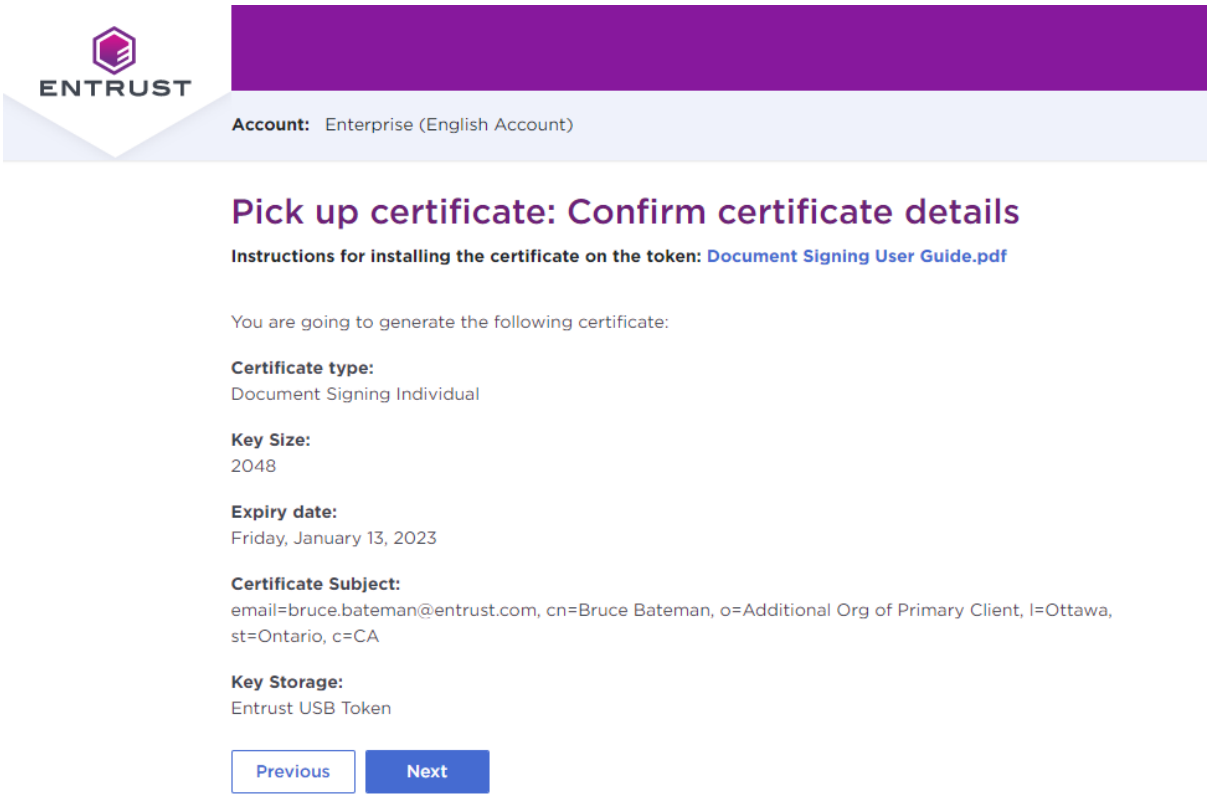
- If the USB token is not yet initialized, follow the procedure in: "To initialize your token" on page 15. When the USB token is initialized, return to this browser page and this procedure to continue.

9 Select **Yes, I agree** to indicate that your certificate will always be stored on a secure Entrust USB token.

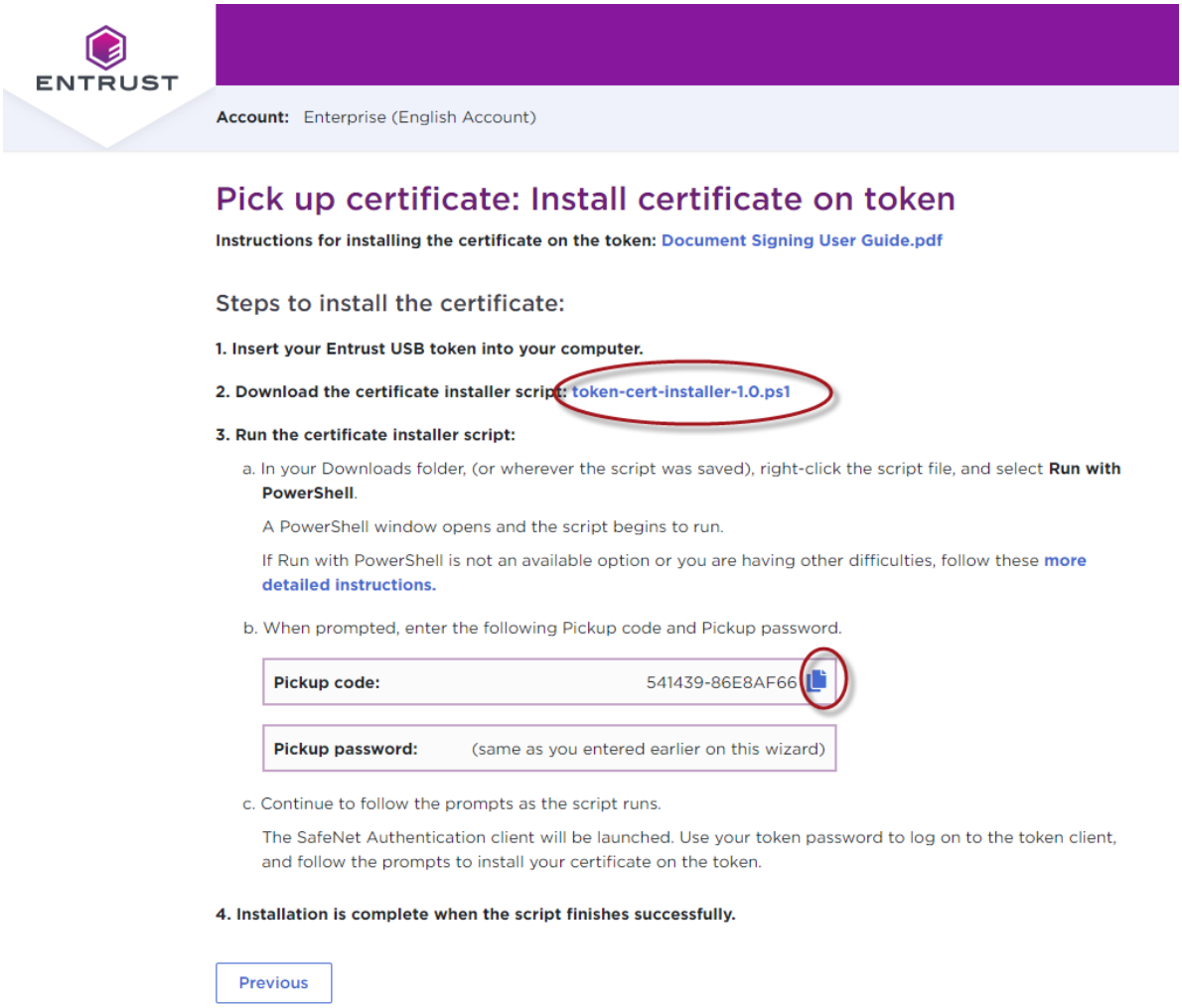


10 Click **Next** to proceed.

11 The confirmation screen appears. Review the certificate details, and click **Next**.



The **Install certificate on token** screen appears.



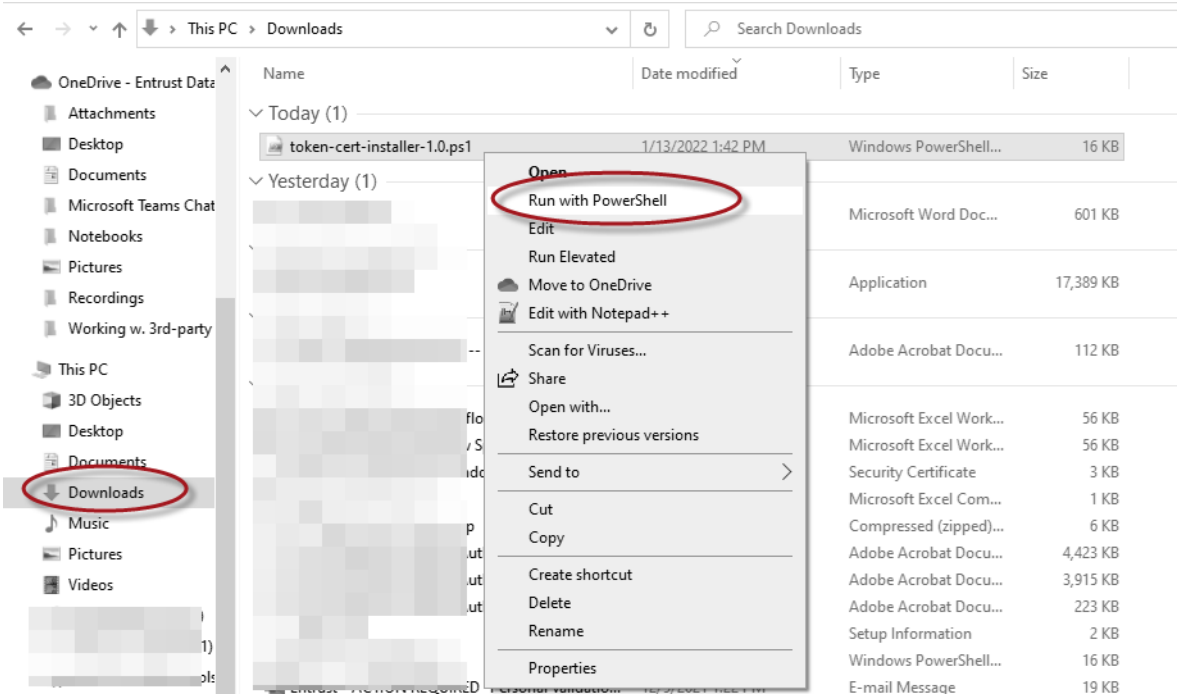
12 If necessary, insert your token into a USB port.

13 You may see a warning message. To continue, confirm that you are allowing the website to perform a digital certificate operation.

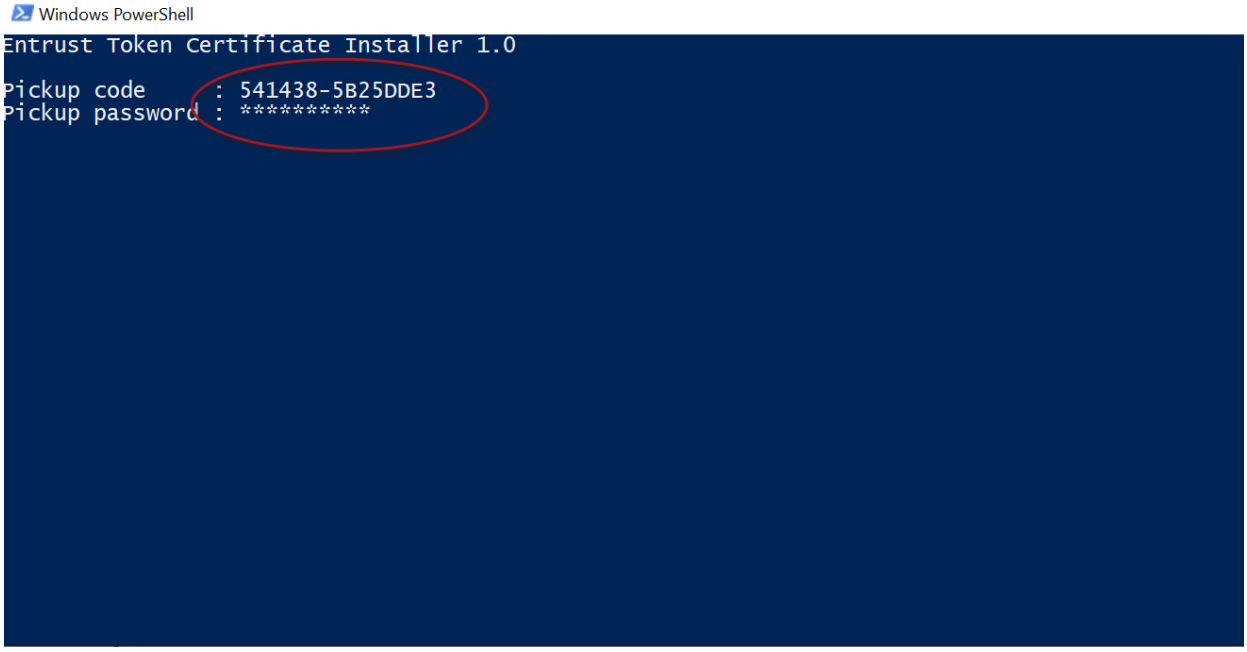
14 Download the token installer script by clicking the script name: `token-cert-installer-<version>.ps1`

15 You will need the **Pickup code** and the **Pickup Password**. Copy the **Pickup code** to the clipboard by clicking the copy icon beside the code.

16 Locate the script in your **Downloads** (or other) folder, and right-click > **Run with PowerShell**.



17 PowerShell opens, and launches the script. If you are prompted to give permission to run the script, type **R** at the prompt. Press the Enter key.

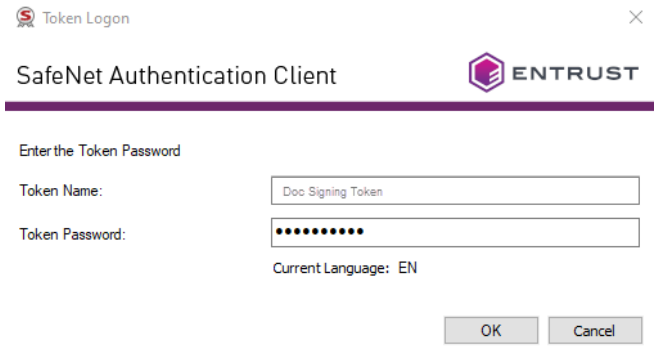


18 Paste the **Pickup code** at the **Pickup code** prompt.

19 Enter the **Pickup password** you used earlier in the pickup process.

20 Press the Enter key.

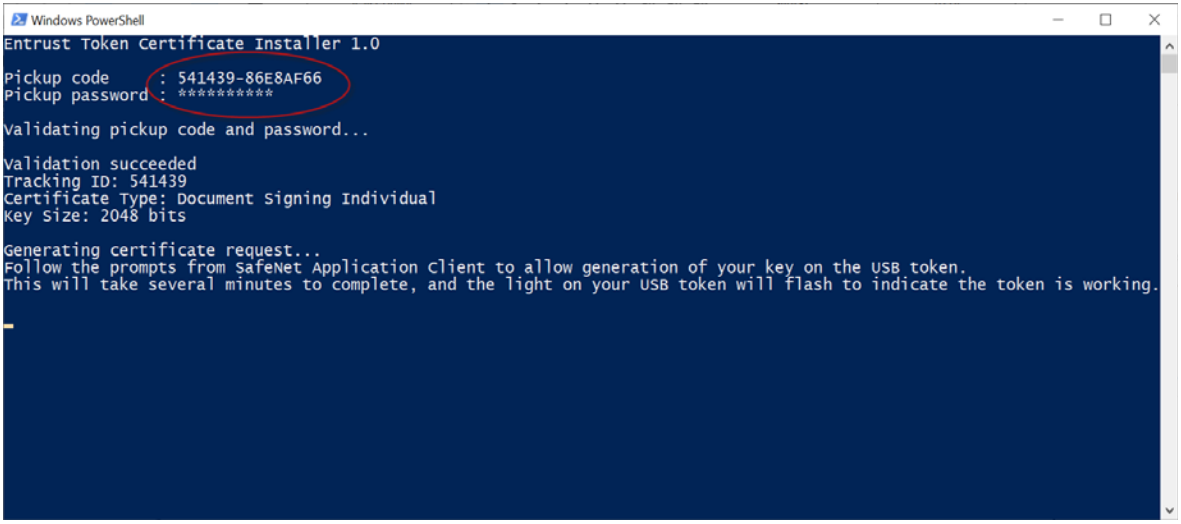
The SafeNet client is started.



21 Log in to the token using the password you set during token initialization.

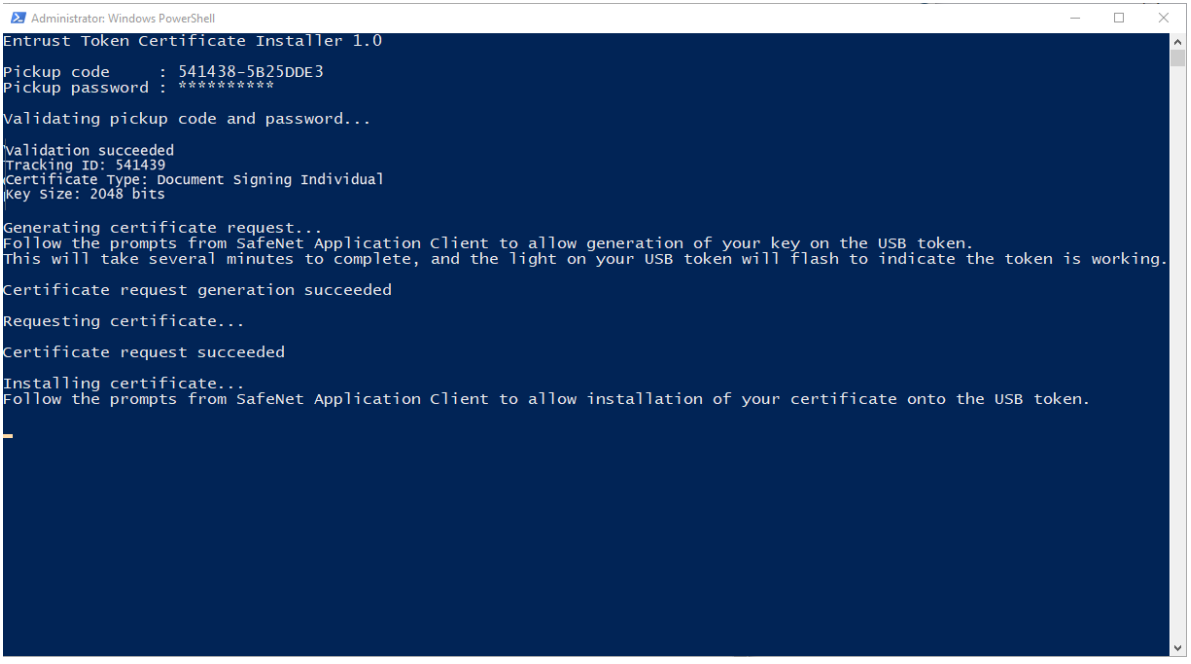
22 Click **OK**.

23 The PowerShell installation script continues to run.



Wait as the script runs. It may take a few minutes, and you will see the token light flashing through most of the process.

When this is done, you will see a screen that looks like this:



24 Follow the prompts to complete installation of the certificate on the token.

The script generates the certificate on your token. The SafeNet client will indicate that your certificate is installed on the token.

Install certificate to an Entrust USB token using Microsoft Internet Explorer or Microsoft Edge

This pickup procedure is available with the Microsoft Internet Explorer or Microsoft Edge browser. This procedure using Microsoft Internet Explorer will be deprecated when support for Internet Explorer is ended by Microsoft.

Configuring Microsoft Edge

If you are using Microsoft Edge to retrieve the certificate rather than IE or the PowerShell script, you must turn on Internet Explorer mode.

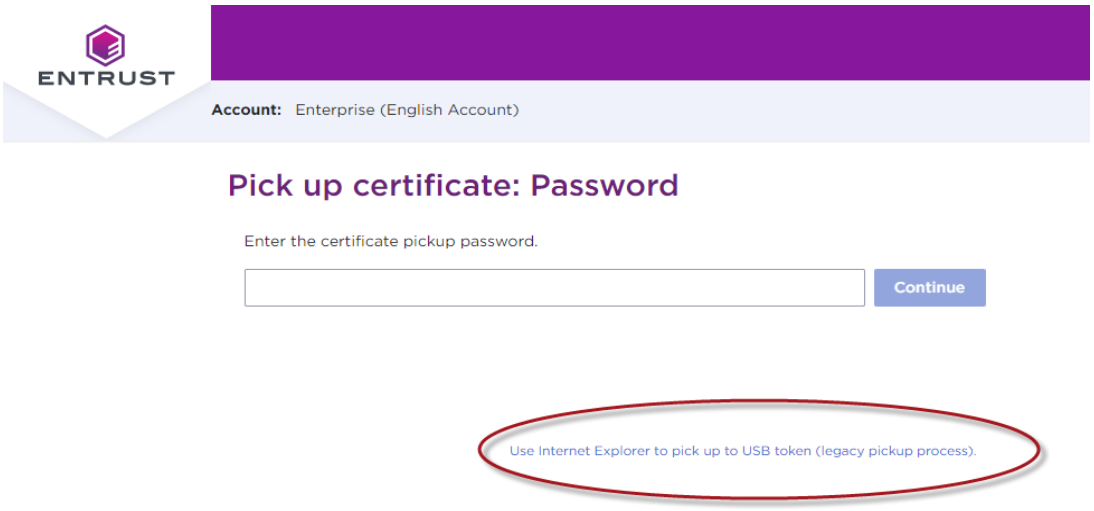
To turn on Internet Explorer mode

1. Open Microsoft Edge and click on the three dots in the upper right-hand corner of the browser window to open the menu.
2. Click on **Settings**.
3. Click on **Default browser**.
4. From **Allow Sites to be reloaded in Internet Explorer mode (IE mode)** select **Allow**.
5. From **Internet Explorer mode pages**, click **Add.**
6. Copy and paste the certificate retrieval URL that you received from Entrust into the **Add a page** dialog.
7. Click **Add** to save the URL.
8. Click **Restart**.

To download a certificate to an Entrust USB token using Microsoft Internet Explorer or Microsoft Edge

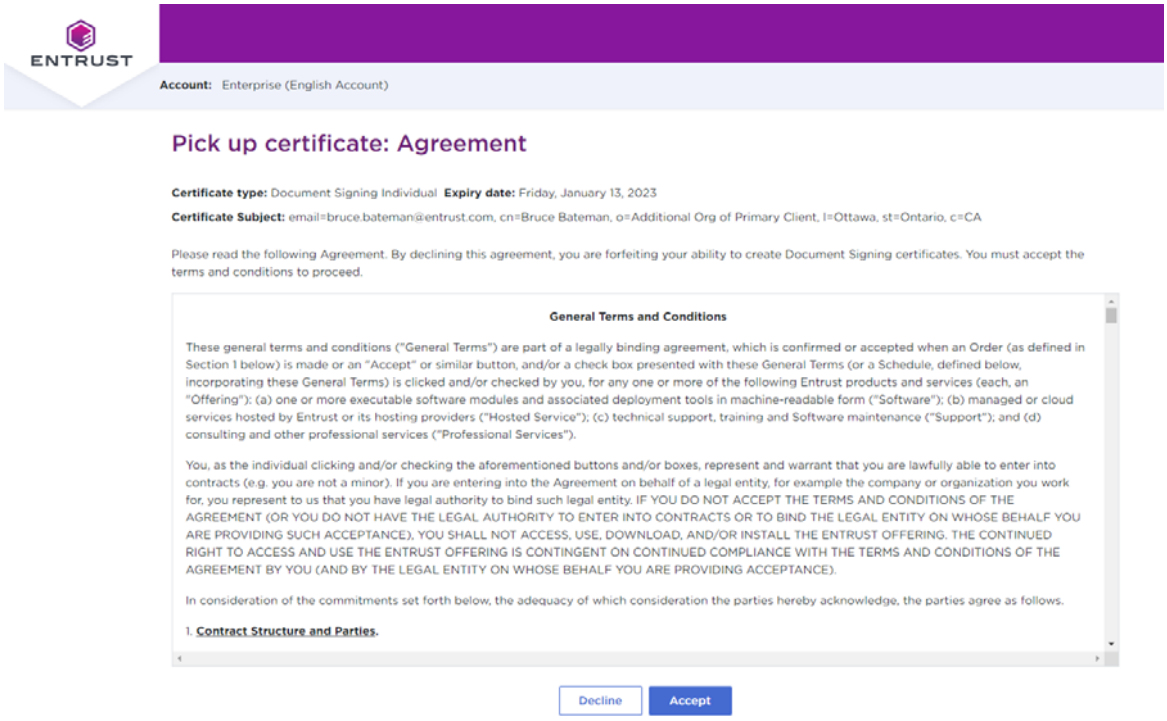
1. Insert your token into a USB port.
2. In the notification email from Entrust, click the link provided to navigate to the Certificate Pickup pages. If you are working from the Certificate Services UI, select the certificate and click **Actions** > **Pickup**.

The **Pick up certificate: Password** page appears.



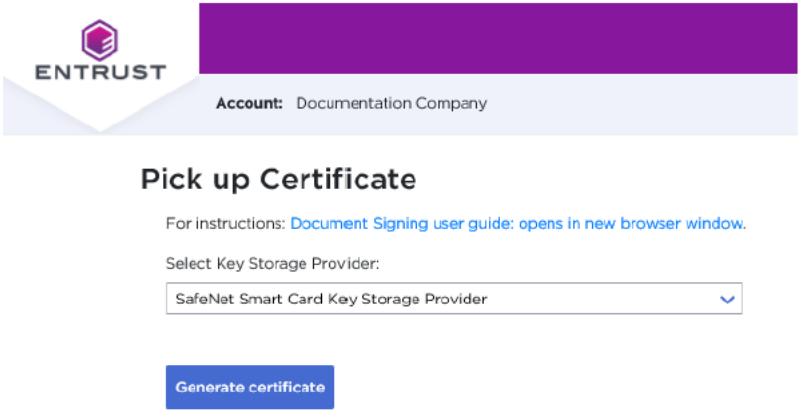
3. Click the link: **Use Internet Explorer to pick up to USB token (legacy pickup process)**.
4. On the **Password** screen that appears, enter the password created with the certificate request.
5. Click **Continue**.
6. You may see a warning message. To continue, confirm that you are allowing the website to perform a digital certificate operation. Allow the operation.
7. If the SafeNet Authentication Client software is not yet installed, you will see this screen. Select the SafeNet version to install, based on your machine type. See"Downloading and installing the token software (required for USB token pickup)" on page 8 to complete the SafeNet installation, and then return here.

8 If the SafeNet Authentication Client is already installed, the Certificate Services Subscription Agreement page appears.



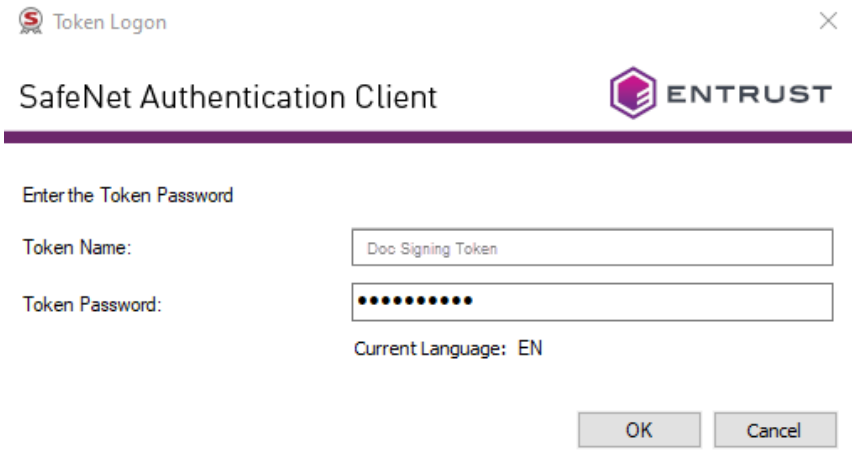
9 Read the agreement and click **Accept**.

The **Pick up Certificate** page appears.

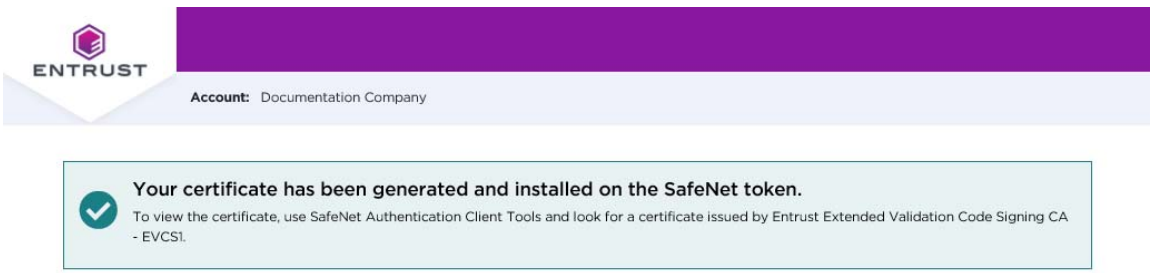


10 Click **Generate Certificate**.

11 In the **Token Logon** dialog box that appears, enter the password you created for your token during the token initialization. This is not the password used to log in to the Entrust Web site.



The certificate is generated on your token. This will take a few minutes. When the certificate has been created, you will see a success message.



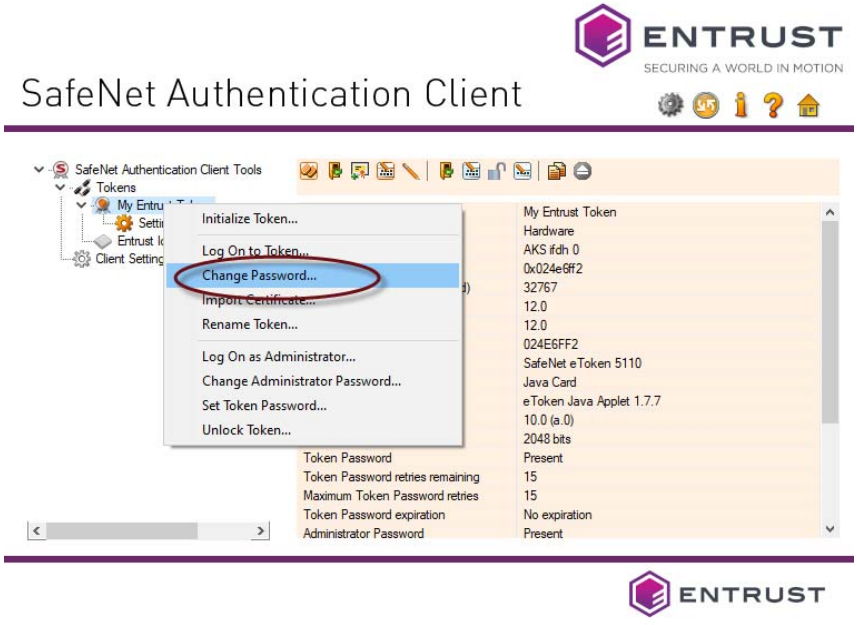
Your certificate is now ready for use. The certificate is also added to the Windows Certificate Store. This allows Adobe software to recognize the signature so that you can use the certificate. (This is not the same as validating another user's signature.)

Changing the password for your token

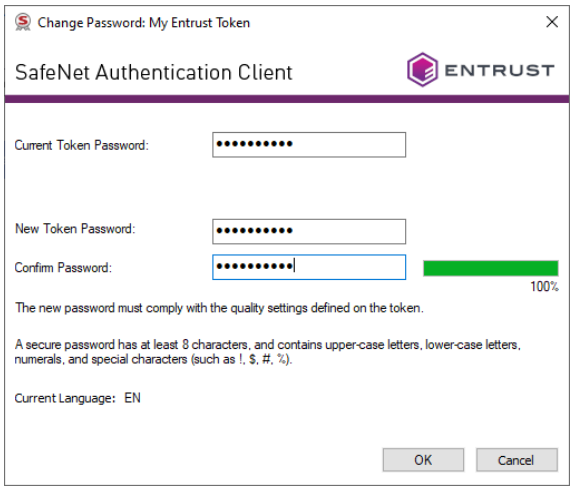
Use the following procedure when you need to change the password for your token.

To change your token password

1. Insert your token into a USB port on your PC.
2. Right-click the SafeNet icon in the Desktop tray and select **Tools**.
3. Click the **Advanced View** (gear) icon.
4. Right-click the entry for your token, and select **Change Password.**



5 Enter your current password and the new password. and confirm the new password. Be sure that your password complies with the character requirements defined for the token. Easily guessed passwords are not secure.



6 Click **OK**.

Recovering a certificate

If you need to recover your certificate, for example, because you forgot the password:

- If you need to recover your certificate within 30 days of purchasing it, Entrust Certificate Services will reissue it once for free. After the 30 day period or if you need to recover the certificate more than once, you must purchase a new certificate.
- If you forget your pickup password before the certificate is generated, Certificate Services support will reset the password for you.

Note:
The Token Utility cannot recover the certificate.

2

Signing a document

This chapter provides basic information about how to sign an Adobe PDF or a Microsoft Word file, and how to set signature preferences.

Documents can also be certified to ensure that they are not altered after the signature is applied. For more advanced configuration options, see the Adobe or Microsoft documentation. A digital signature enables recipients to verify that the document came from you or passed though your possession, providing accountability.

Signing a PDF document

You can add one or more digital signatures to a PDF file or form using Adobe Acrobat or Adobe Acrobat Reader.

One or more signature fields can be created directly on the PDF for easy viewing. The field contains details about the certificate and the signature name. This example explains how to sign a PDF using Adobe Reader and a document signing certificate on a token.

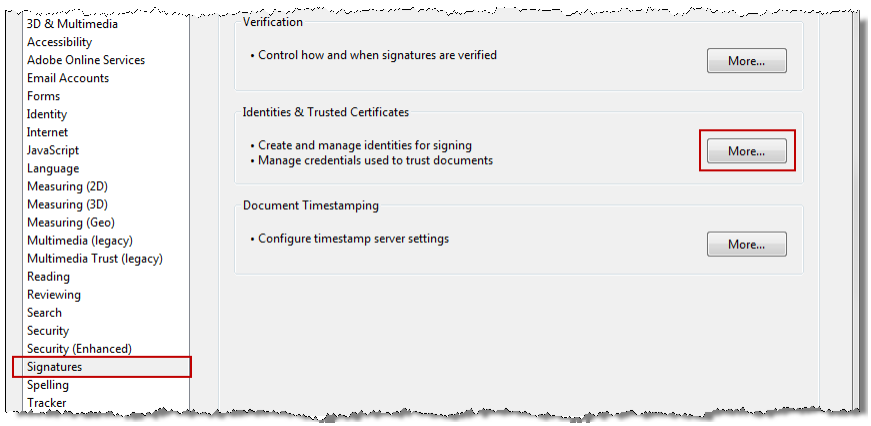
Note:
Procedures in this chapter are based on Adobe Acrobat Reader DC version 2015.010. The instructions may be differ for other versions of Adobe Reader and Adobe Acrobat.

Complete the following procedures to sign a document:

- "Select your certificate in Adobe Reader" on page 42
- "Sign the PDF document" on page 43

Select your certificate in Adobe Reader

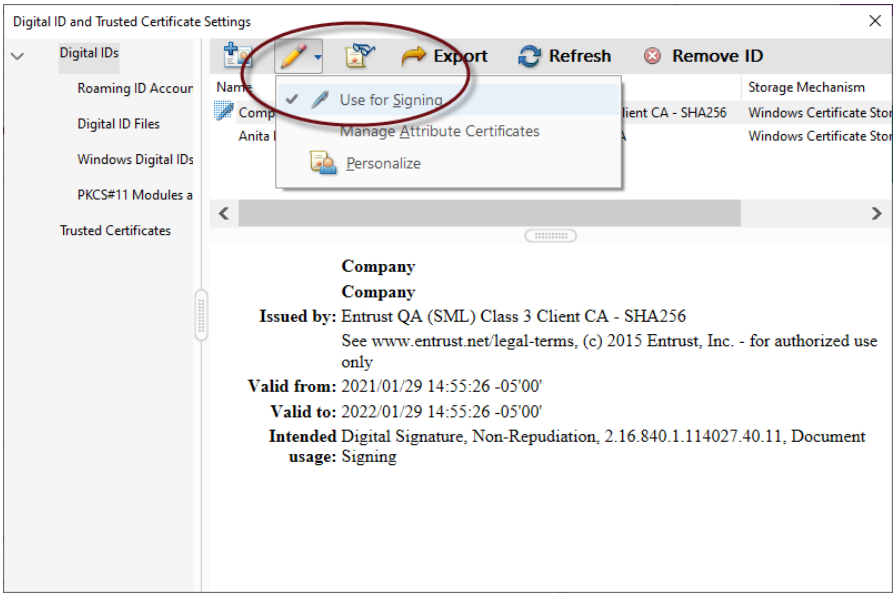
1. Insert your token in a USB port on your computer.
2. Open the PDF document in Adobe Reader.
3. From the main toolbar, click **Edit** > **Preferences**
4. In the Preferences page, select **Signatures**.



5. In the Identities and Trusted Certificates panel, click **More**.

6 In the Digital ID and Trusted Certificate Settings page select Windows Digital IDs and choose your document signing certificate from the list.

7 From the pencil icon (edit) menu select **Use for Signing**.



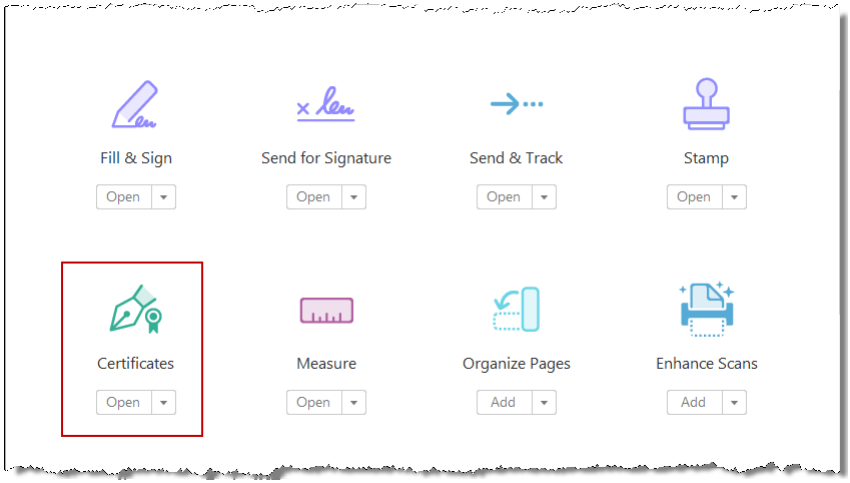
8 Close the Digital ID and Trusted Certificate Settings page and click **OK** in the Preferences page.

Sign the PDF document

1 Be sure that your token is plugged in to a USB port on your computer.

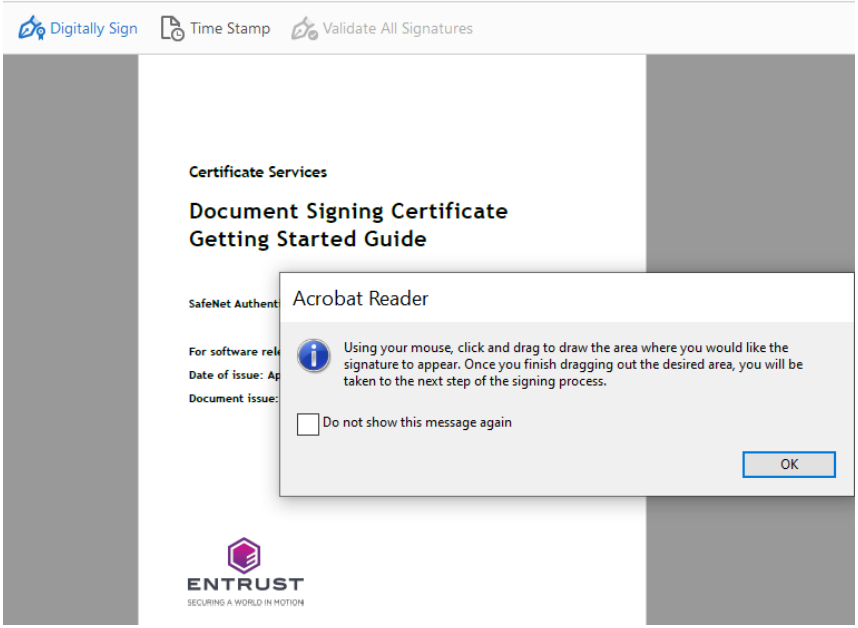
2 In the Adobe Reader ribbon, select the Tools **tab**.

3 Scroll down to the Certificates tool and click **Open**.

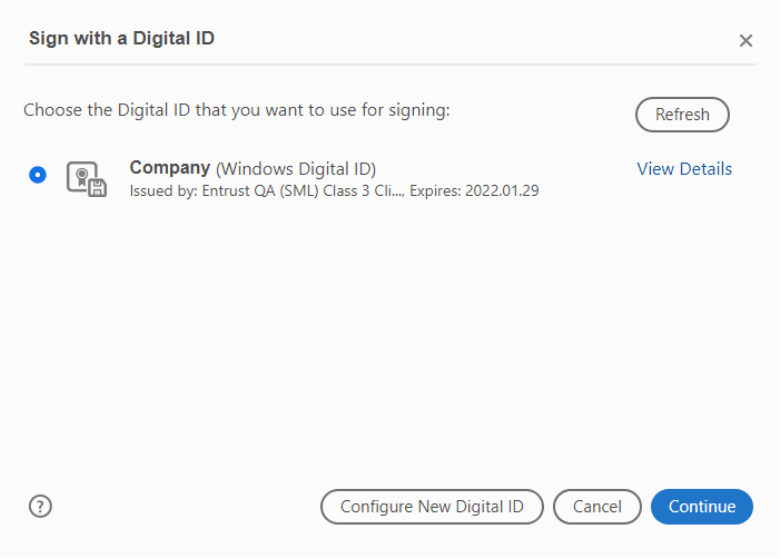


a Select **Digitally Sign** in the ribbon.

4 Read the information dialog and click **OK**.

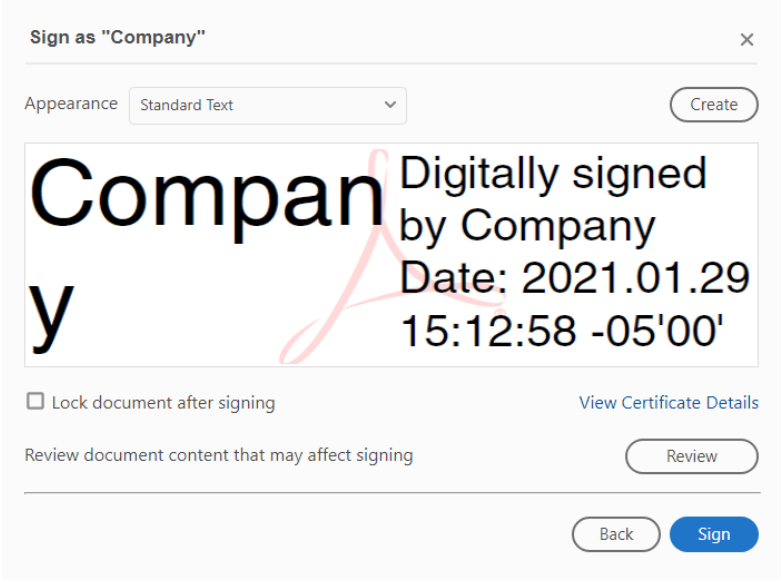


5 In the PDF, click and drag your mouse to create a signature field.



6 Make sure the correct certificate is selected, and click Continue.

7 In the Sign Document dialog, edit the appearance of the signature if required. Help is provided for this dialog.



8 Click **Sign**.

9 Adobe Reader automatically asks you to select a file name and location for the signed PDF. When you are finished click **Save**.

10 When asked, enter the password for your token to allow Reader to use the certificate.

11 You may be asked for permission to connect to the Entrust timestamp server if this option is enabled in Adobe Acrobat Reader. Click **Yes** to continue.

12 The signature appears in the selected area of the document.

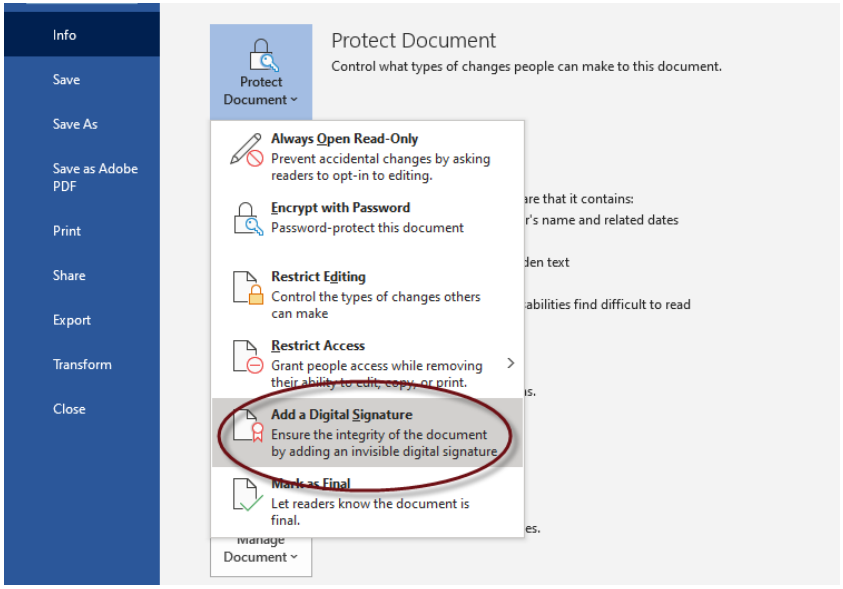
Signing a Microsoft Word document

Microsoft Word provides the ability to add signatures from one or more individuals to provide accountability and assure authenticity. This example explains how to sign a Word document using a document signing certificate on a token.

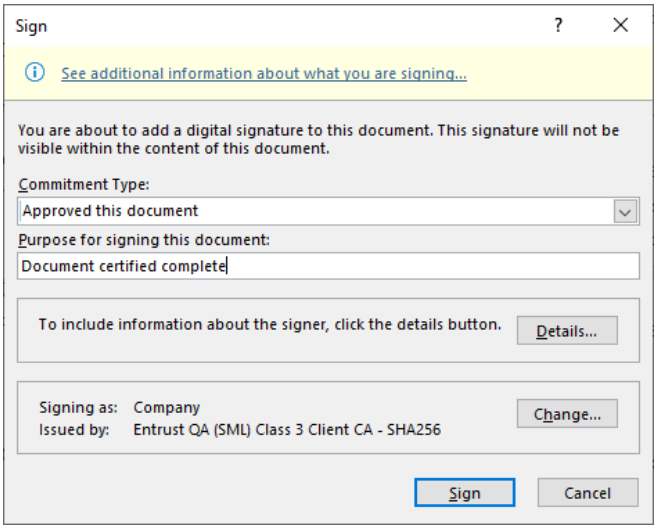
Note:
This procedure is based on Microsoft Office 2013. The procedure my differ for other Microsoft Office versions.

To sign a Word document

1. Plug the token with your Entrust Document Signing certificate into a USB port on your computer.
2. In your Word document, select **File** > **Info**.
3. Select **Protect Document** > **Add a Digital Signature.**



4 In the **Sign** dialog:



a Select the **Commitment Type**.

b Enter a purpose for signing the document.

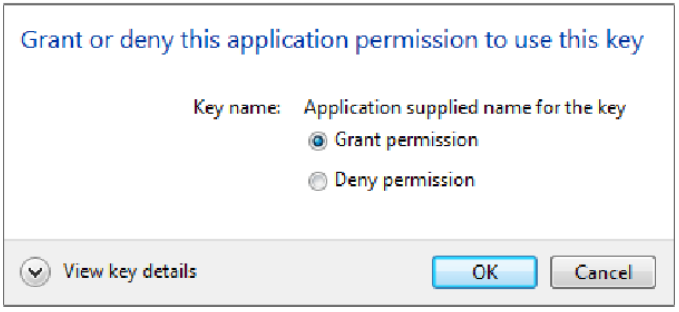
c Click **Details** to enter information about who you are (title and location). This information will become part of your signature.

d Click **Change** to select your Entrust document signing certificate, if it does not appear in the bottom panel.

e Click **Sign**.

5 Provide your token password, if requested.

6 If the Request Permission to use a Key dialog appears, select **Grant permission** to continue.



7 Word signs the document and displays a success message.

8 To view the signatures, select **File** > **Info** > **View Signatures**.

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

administrator password 20

D

Documentation feedback 3

G

Getting help
  Technical Support 2

I

Initialize Token
  IDPrime Common Criteria Settings 21
Installation
  PowerShell script (token) 23
Installing a certificate 23

M

Microsoft Edge
  Configuring 33
  Internet Explorer mode 33

P

Password
  changing 37
Picking up a certificate from the portal 23
Prerequisites 23
PUK 19

R

Recovering a certificate 39
Related documentation 3

S

SafeNet Authentication Client 16
Signing
  Microsoft Word 42
  PDF 42
Supported browsers 6
Supported operating systems 6

T

Technical Support 2
Token password 20