

ENTRUST

Certificate Services Document Signing Guide

(Microsoft Windows PowerShell script token pickup method)

SafeNet Authentication Client, Version 10.8

For software release 13.4

Date of issue: November 2022

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.

© 2022 Entrust Corporation. All rights reserved.

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.



Note:

Certificate Services now provides 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 of running the new pickup process, and the steps are quite different from those you used if you have installed an Entrust certificate on a SafeNet token before.

Supported platforms and software

The software and token provided by Entrust was tested with the following operating systems. It may also work with other operating systems, however 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 (21H2)
- Microsoft Windows 10 (32-bit, 64-bit), up to 21H1
- Microsoft Windows 8.1 (32-bit, 64-bit)
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2016 (64-bit)
- Microsoft Windows Server 2012, 2012R2 (64-bit)

Supported browsers

- Microsoft Internet Explorer 11
- Google Chrome - latest
- Mozilla Firefox - latest

Supported document software

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

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>

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](#)
- [“Before you start” on page 8](#)
- [“Downloading and installing the token software \(required for USB token pickup\)” on page 9](#)
- [“Initializing an Entrust USB token” on page 16](#)
- [“Picking up your Entrust certificate” on page 23](#)

There are three pickup methods:

- [“Install the certificate to Entrust USB token using PowerShell script” on page 23](#)
- [“Install certificate to an Entrust USB token using Microsoft Internet Explorer” on page 33](#)
- [“Changing the password for your token” on page 37](#)
- [“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 was tested with the following operating systems. It 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 (21H2)
- Microsoft Windows 10 (32-bit, 64-bit), up to 21H1
- Microsoft Windows 8.1 (32-bit, 64-bit)
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2016 (64-bit)
- Microsoft Windows Server 2012, 2012R2 (64-bit)

Supported browsers

- Microsoft Internet Explorer 11
- Google Chrome - latest
- Mozilla Firefox - latest

Supported document software

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

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 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>

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 document software](#))

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



Note:

Certificate Services now provides 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 of running the new pickup process, and the steps are quite different from those you used if you have installed an Entrust certificate on a SafeNet token before.

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

The token software provided by Entrust must be installed for you to manage your token, including logging in, initializing, and resetting your password. If you do not have this software installed, install it as described in the following procedures.

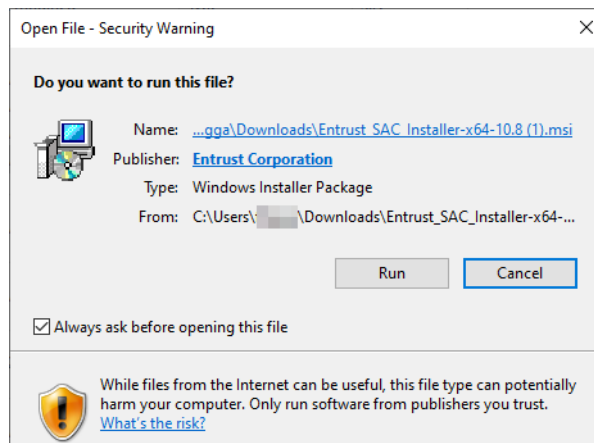


Attention:

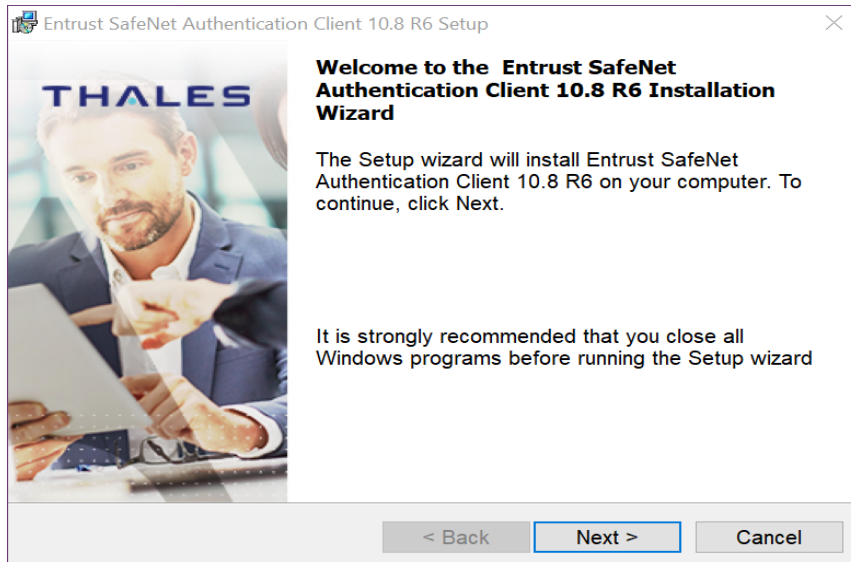
Do not plug your token into your computer until you have completed this procedure.

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**.

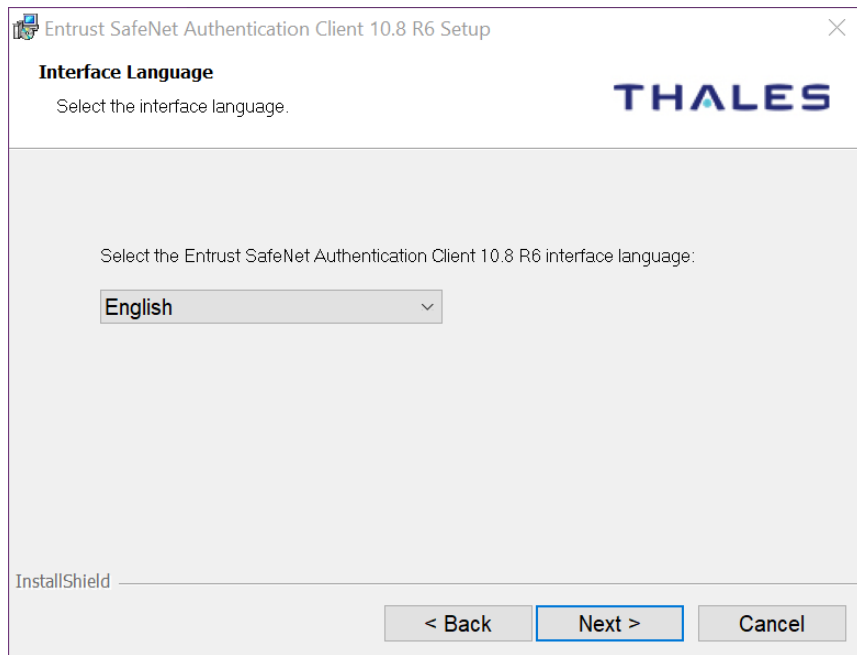


The installation wizard appears.



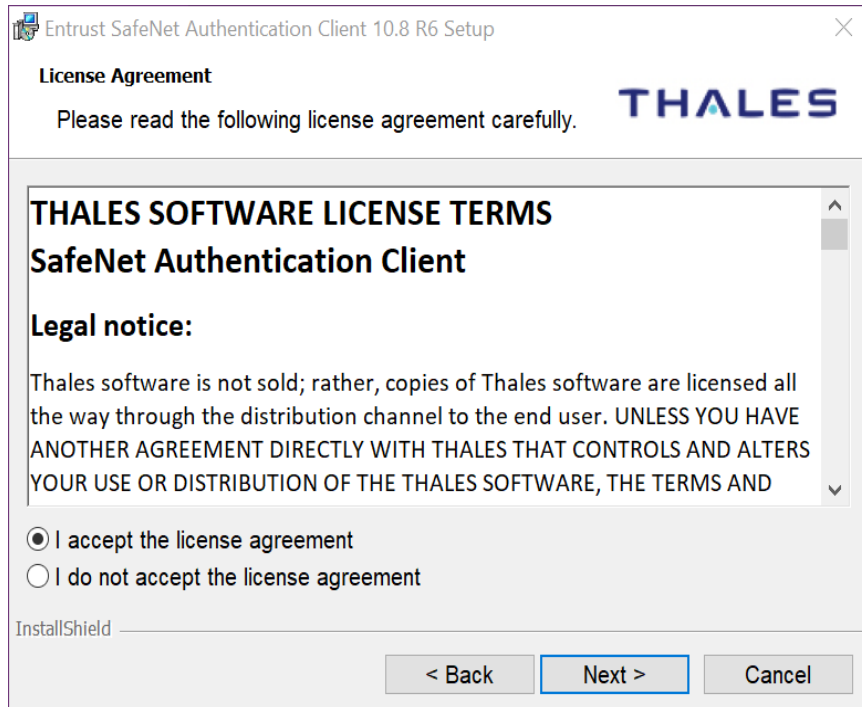
4 Click **Next**.

The **Interface language** page appears.



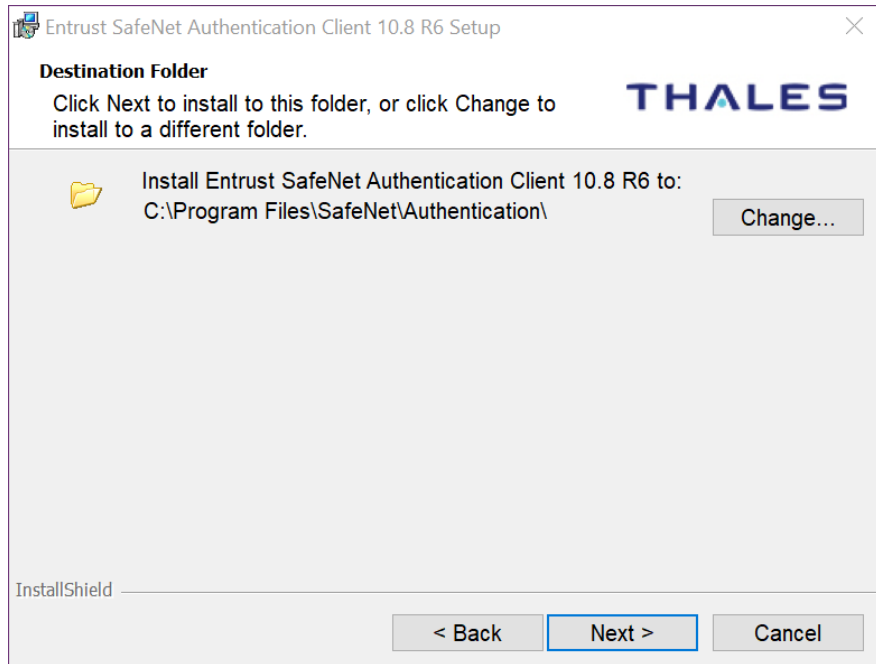
- 5 Select the language to use for the installation.
- 6 Click **Next**.

The **License Agreement** screen appears.



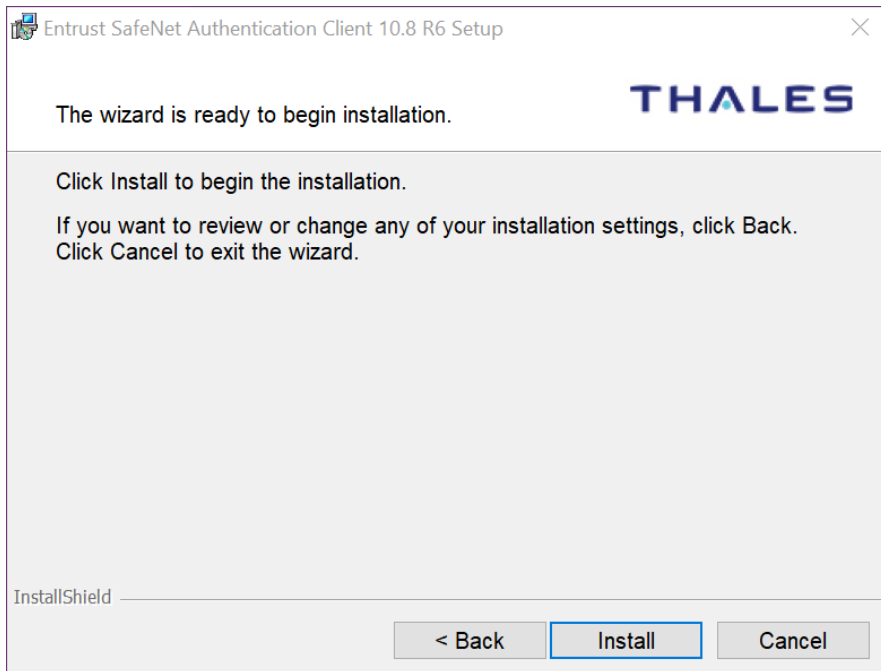
- 7** Read the agreement and select **I accept the license agreement**.
- 8** Click **Next**.

The **Destination Folder** screen appears.



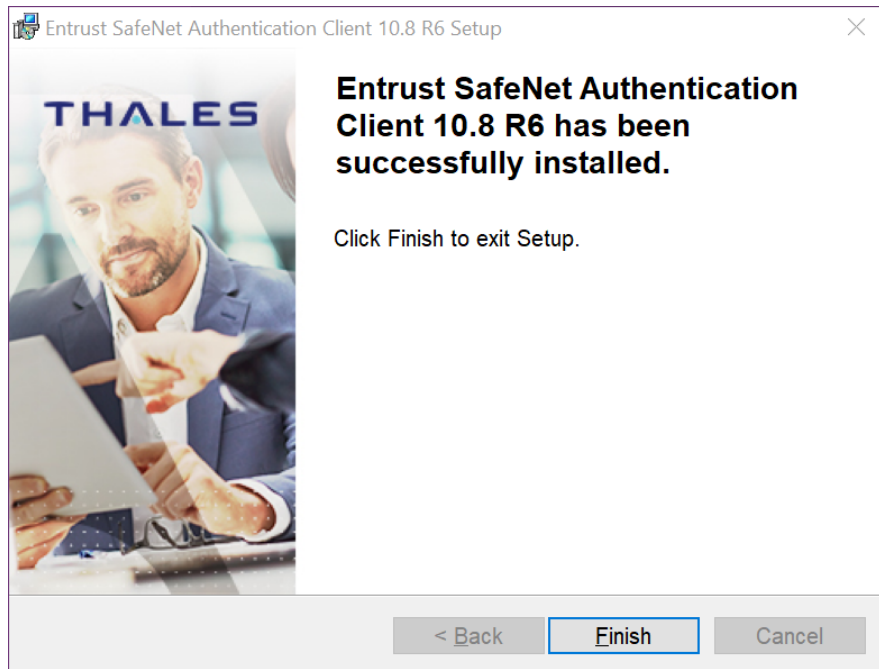
- 9** Accept the default folder or click **Change** to choose a new folder.
- 10** Click **Next**.
- 11** The installation screen appears. Click **Install**.
- 12** You may be asked to allow the installer to make changes to the hard drive of the computer. Allow it to proceed.

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.](#)

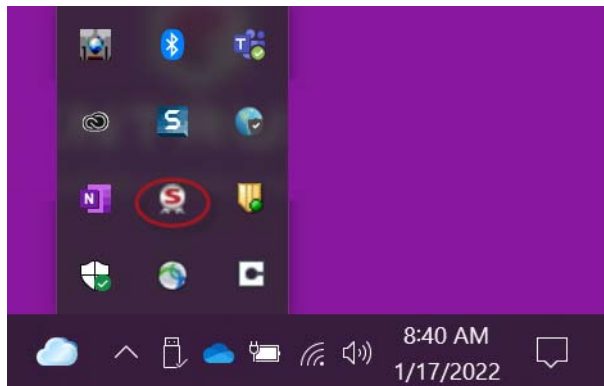


Attention:

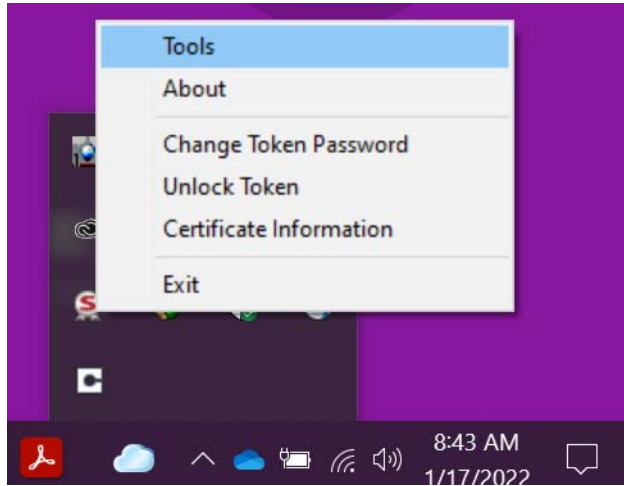
This procedure is needed for new tokens. If the token already contains certificates, initializing the token deletes all certificates stored on it.

To initialize your token

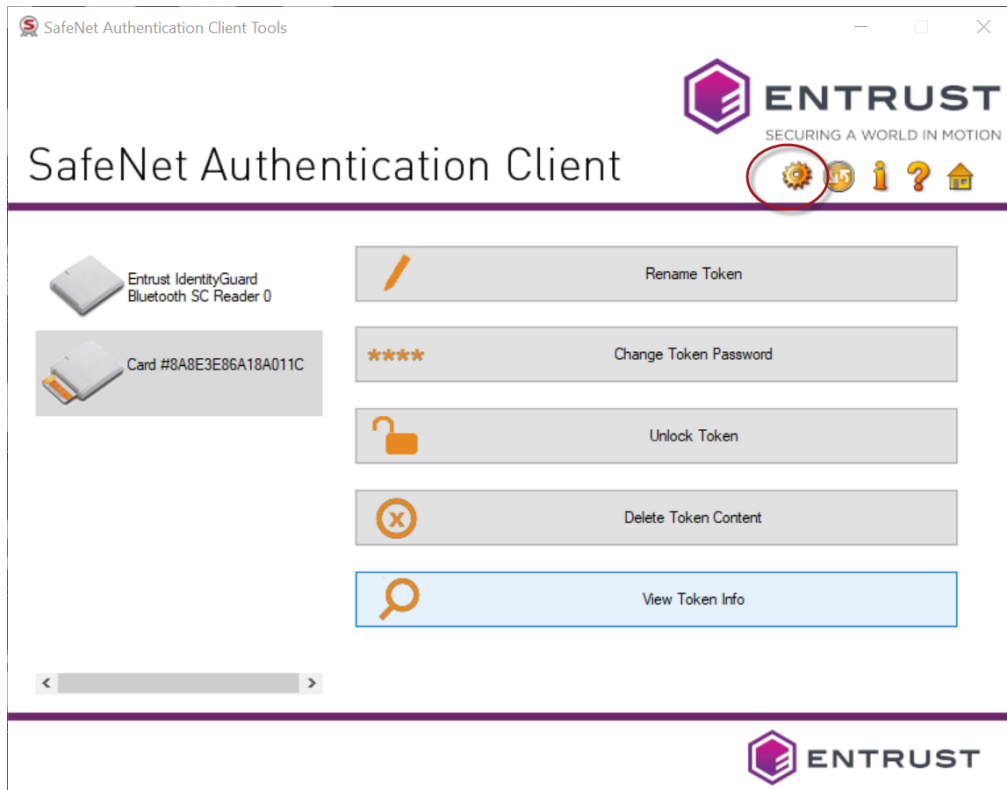
- 1 Insert your token into a USB slot on your computer. When the token has been recognized by the computer and the drivers have been installed, the Safenet icon in the system tray switches from grayed-out to active.



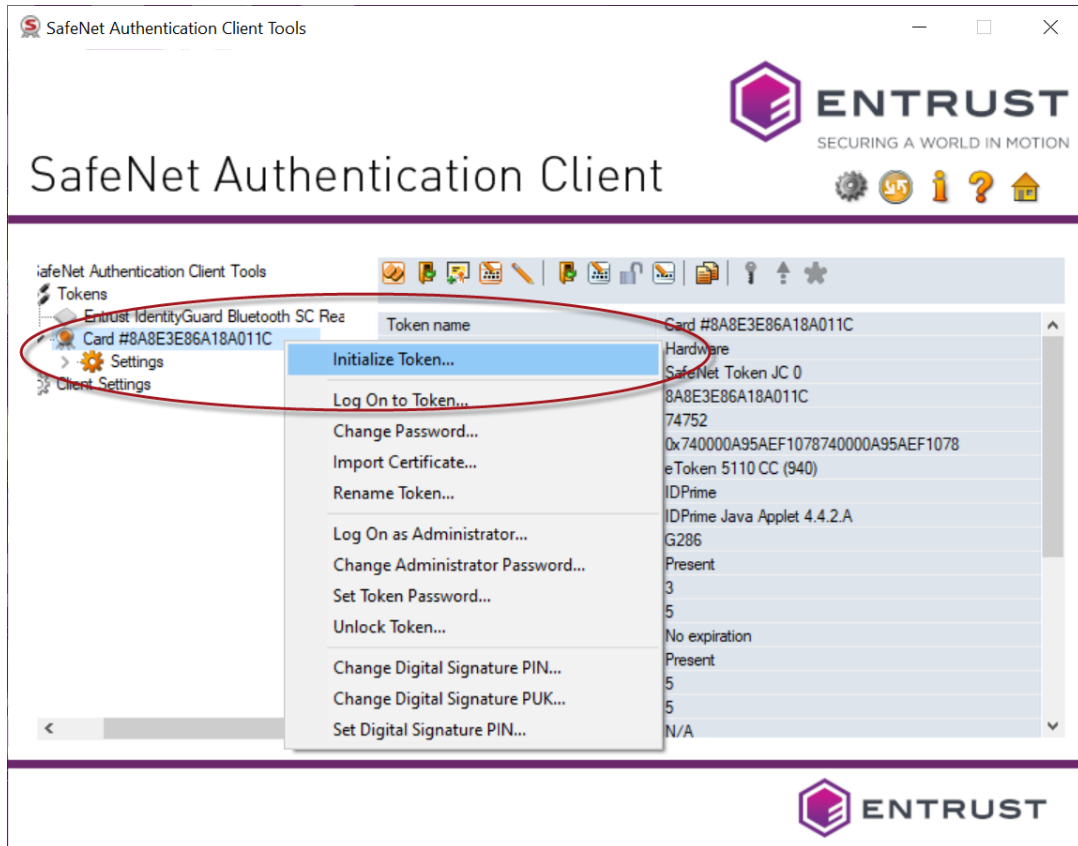
- 2 When the icon becomes active, right-click on it to open the menu. Select **Tools**.



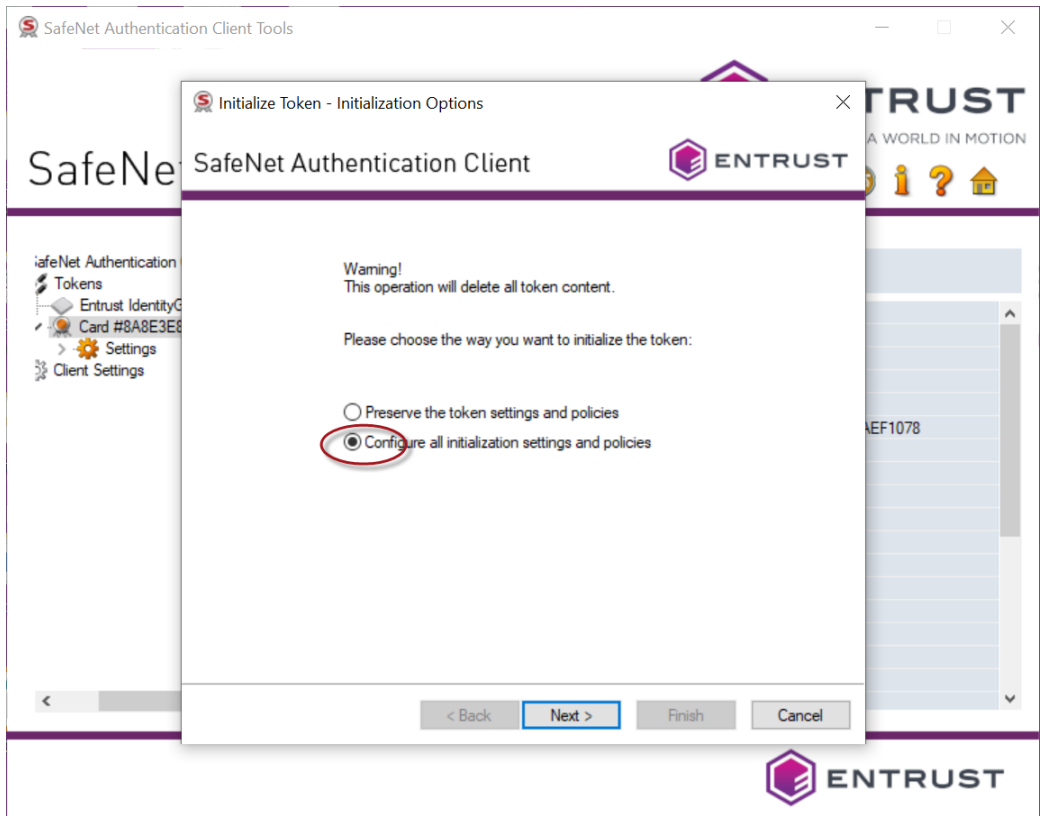
- 3 The SafeNet Authentication Client opens. Click the gear icon at the top right.



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

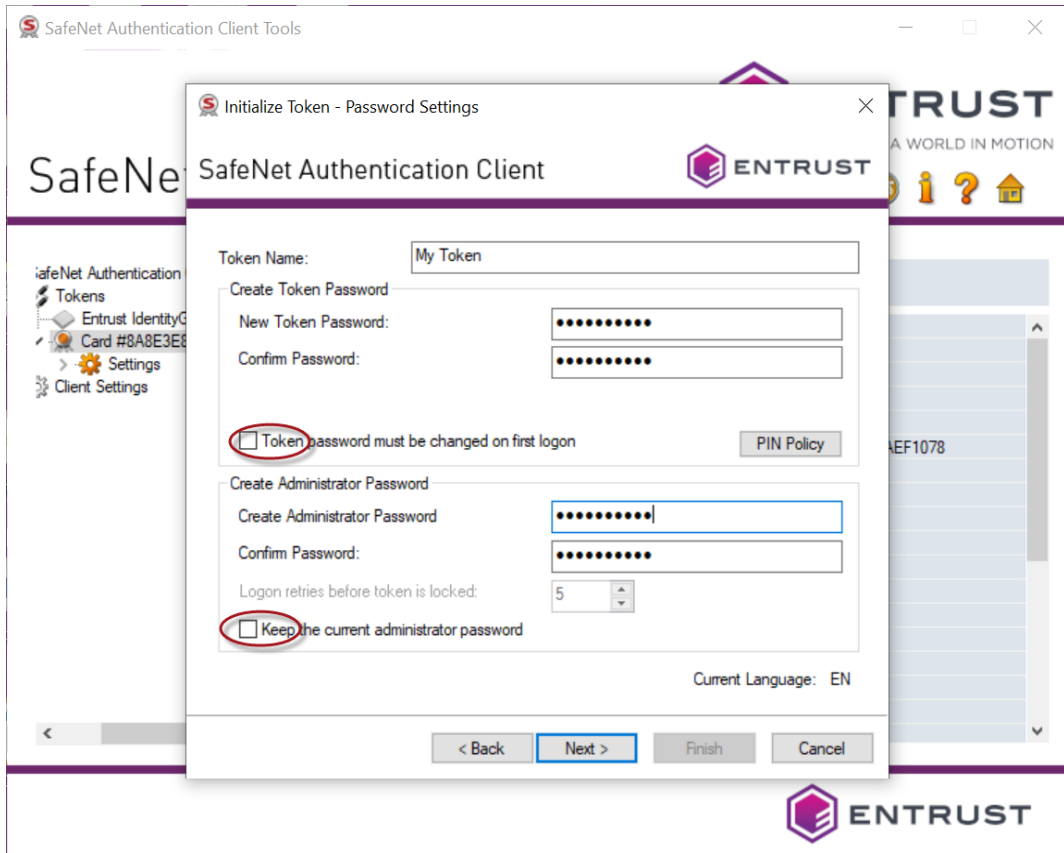


- 5 In the **Initialize Token - Initialization Options** window, select **Configure all initialization settings and policies**.



- 6 Click **Next**.

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



- 7** 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** Unselect **Token password must be changed on first logon**.
 - d** Create and confirm your Administrator password.
 - e** Unselect **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-up and cannot be unlocked.** You will need to buy a new token (Entrust will not replace it for free).

- 8** Click **Next**.

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

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



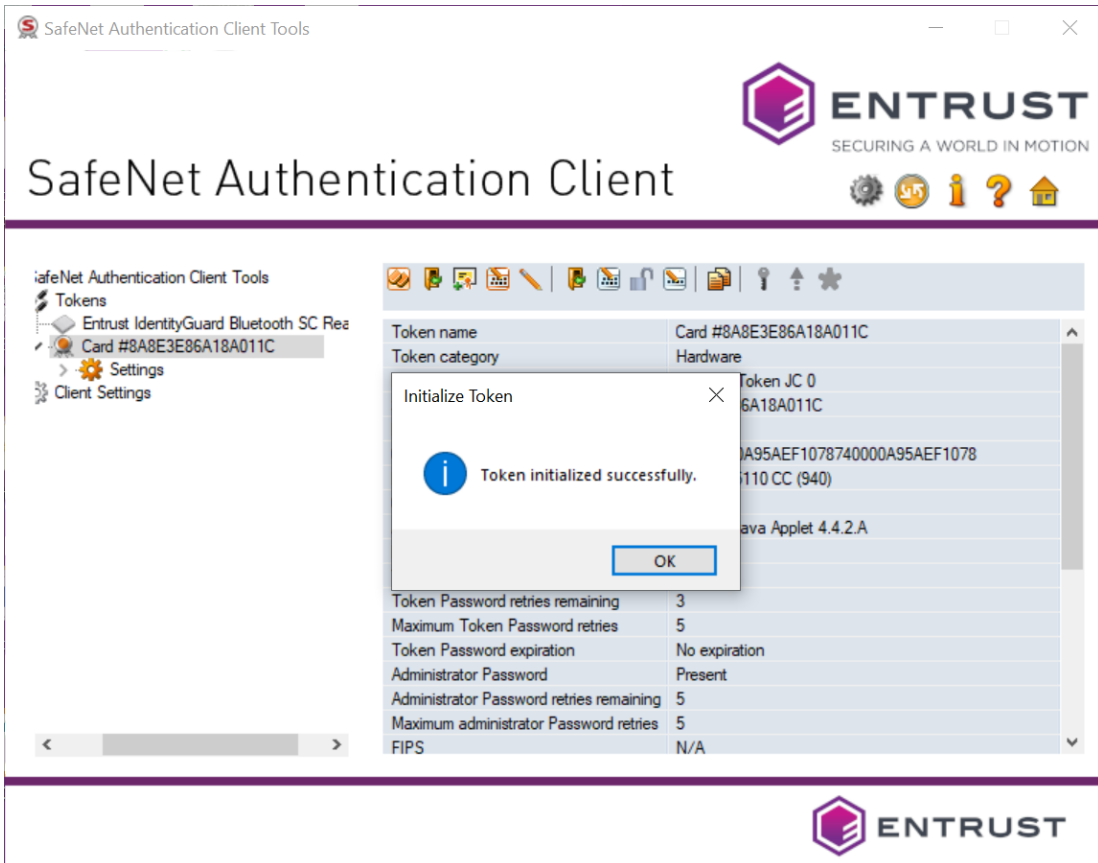
Attention:

Keep your passwords and PINs in a safe place (Token password, Administrator password, Digital Signature PIN and New Digital Signature PUK).

- 10** Click **Finish**.

- 11** A status bar opens, indicating the progress of the initialization, followed by a success message. Click **OK** to complete the initialization.

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



Picking up your Entrust certificate

Administrators using the Certificate Services interface can navigate to **Certificates > Managed Certificates > Pending User Pickup**. Select the certificate and click **Actions > Pickup** to access the certificate pickup pages. Other users will receive an email message containing a link to the pickup page.

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 9
- The Entrust USB token must be initialized. If that's not been done, follow the instructions in: "[Initializing an Entrust USB token](#)" on page 16

Installing certificate to 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 browser (legacy method).

- "[Install the certificate to Entrust USB token using PowerShell script](#)" on page 23
- "[To download a certificate to an Entrust USB token using Microsoft Internet Explorer](#)" on page 33

Install the certificate to Entrust USB token using PowerShell script

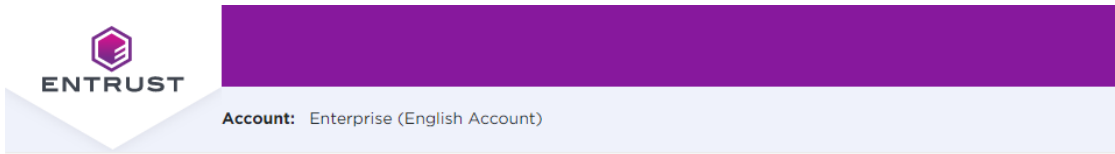
This is the recommended procedure for picking up your certificate to an Entrust USB token. It can be used with all supported browsers.

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

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

- 1 Click the link to the Entrust Certificate Retrieval Web pages in the notification email sent to you by Entrust.

The Entrust Certificate Pickup page appears.



Pick up certificate: Password

Enter the certificate pickup password.

Continue

[Use Internet Explorer to pick up to USB token \(legacy pickup process\).](#)

- 2** Enter the password that you entered when you created the certificate request or get it 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**.



Account: Enterprise (English Account)

Pick up certificate: Agreement

Certificate type: Document Signing Individual **Expiry date:** Friday, January 13, 2023

Certificate Subject: email=bruce.bateman@entrust.com, cn=Bruce Bateman, o=Additional Org of Primary Client, l=Ottawa, st=Ontario, c=CA

Please read the following Agreement. By declining this agreement, you are forfeiting your ability to create Document Signing certificates. You must accept the terms and conditions to proceed.

General Terms and Conditions

These general terms and conditions ("General Terms") are part of a legally binding agreement, which is confirmed or accepted when an Order (as defined in Section 1 below) is made or an "Accept" or similar button, and/or a check box presented with these General Terms (or a Schedule, defined below, incorporating these General Terms) is clicked and/or checked by you, for any one or more of the following Entrust products and services (each, an "Offering"): (a) one or more executable software modules and associated deployment tools in machine-readable form ("Software"); (b) managed or cloud services hosted by Entrust or its hosting providers ("Hosted Service"); (c) technical support, training and Software maintenance ("Support"); and (d) consulting and other professional services ("Professional Services").

You, as the individual clicking and/or checking the aforementioned buttons and/or boxes, represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS, USE, DOWNLOAD, AND/OR INSTALL THE ENTRUST OFFERING. THE CONTINUED RIGHT TO ACCESS AND USE THE ENTRUST OFFERING IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (AND BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Contract Structure and Parties.**

Decline

Accept

5 The Choose token setup screen appears.

The screenshot shows the 'Pick up certificate: Choose token setup' screen. At the top left is the Entrust logo. Below it, the account type is 'Enterprise (English Account)'. The main heading is 'Pick up certificate: Choose token setup'. Below this is a link for 'Instructions for installing the certificate on the token: Document Signing User Guide.pdf'. There are three sections, each with a 'No' toggle:

- Are you running a supported OS?** Select your operating system. A dropdown menu shows '--Operating system--'. The toggle is set to 'No'.
- Do you have the Entrust SafeNet Authentication Client installed?** Select the installer to download. A dropdown menu shows '64-bit installer' and a 'Download' button. The toggle is set to 'No'.
- Has your Entrust USB token been initialized?** Your token must be initialized before it is used for the first time. Follow the instructions in the [Document Signing User Guide.pdf](#). If there are certificates on the token, you don't need to initialize the token. **Important:** If you reinitialize a token, all existing certificates will be deleted. The toggle is set to 'No'.

Below these sections is a yellow warning box titled 'End User Key Storage Requirement' with an exclamation mark icon. The text reads: 'You must generate and store your private key on your Entrust USB token. Please agree before proceeding.' There is a checkbox labeled 'Yes, I agree' which is currently unchecked.

At the bottom of the form are two buttons: 'Previous' and 'Next'.

6 In **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, click to 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 9](#). 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 16](#). When the USB token is initialized, return to this browser page and this procedure to continue.
- 9** Select **Yes, I agree** to promise that your certificate will always be stored on a secure Entrust USB token.

Account: Enterprise (English Account)

Pick up certificate: Choose token setup

Instructions for installing the certificate on the token: [Document Signing User Guide.pdf](#)

Are you running a supported OS? Yes

Select your operating system

Microsoft Windows 10 (32-bit, 64-bit) up to 21H1

Do you have the Entrust SafeNet Authentication Client installed? Yes

If the client has not yet been installed, you must do that next.

Has your Entrust USB token been initialized? Yes

If your token is not initialized, you must do that next.

End User Key Storage Requirement

You must generate and store your private key on your Entrust USB token. Please agree before proceeding.

Yes, I agree

[Previous](#) [Next](#)

10 Click **Next** to proceed.

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



Account: Enterprise (English Account)

Pick up certificate: Confirm certificate details

Instructions for installing the certificate on the token: [Document Signing User Guide.pdf](#)

You are going to generate the following certificate:

Certificate type:

Document Signing Individual

Key Size:

2048

Expiry date:

Friday, January 13, 2023

Certificate Subject:

email=bruce.bateman@entrust.com, cn=Bruce Bateman, o=Additional Org of Primary Client, l=Ottawa, st=Ontario, c=CA

Key Storage:

Entrust USB Token

[Previous](#)

[Next](#)

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



Account: Enterprise (English Account)

Pick up certificate: Install certificate on token

Instructions for installing the certificate on the token: [Document Signing User Guide.pdf](#)

Steps to install the certificate:

1. Insert your Entrust USB token into your computer.

2. Download the certificate installer script: [token-cert-installer-1.0.ps1](#)

3. Run the certificate installer script:

a. In your Downloads folder, (or wherever the script was saved), right-click the script file, and select **Run with PowerShell**.

A PowerShell window opens and the script begins to run.

If Run with PowerShell is not an available option or you are having other difficulties, follow these [more detailed instructions](#).

b. When prompted, enter the following Pickup code and Pickup password.

Pickup code: 541439-86E8AF66 

Pickup password: (same as you entered earlier on this wizard)

c. Continue to follow the prompts as the script runs.

The SafeNet Authentication client will be launched. Use your token password to log on to the token client, and follow the prompts to install your certificate on the token.

4. Installation is complete when the script finishes successfully.

[Previous](#)

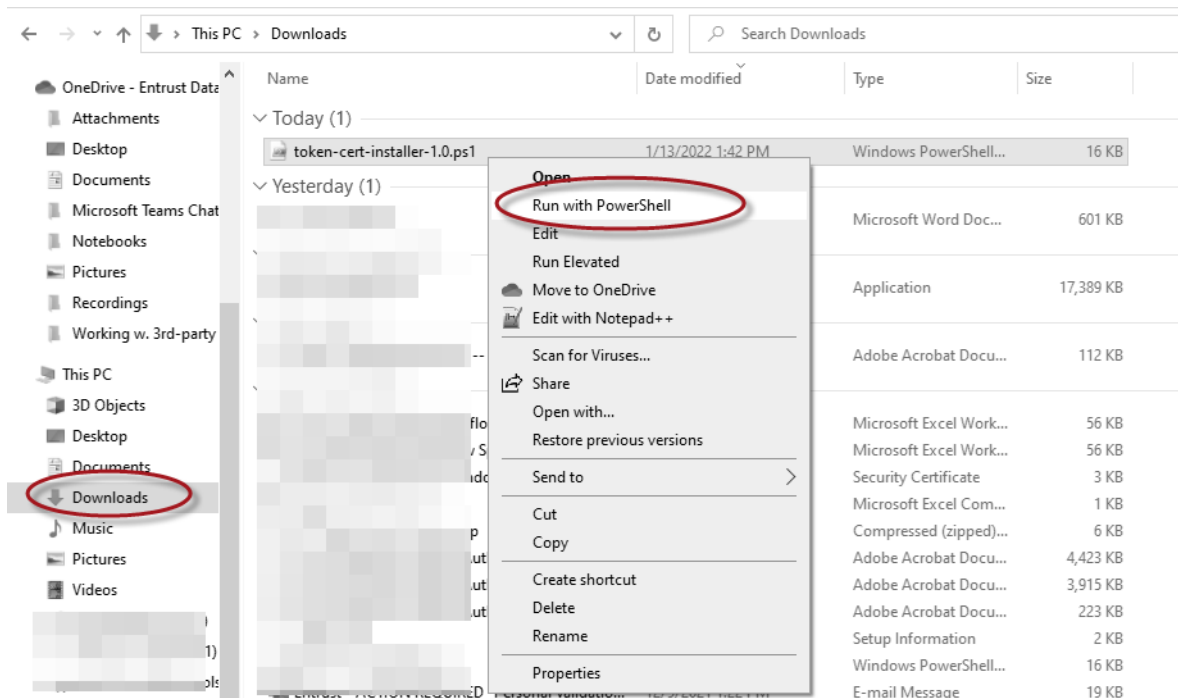
12 Insert your token into a USB port if it is not already there.

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.

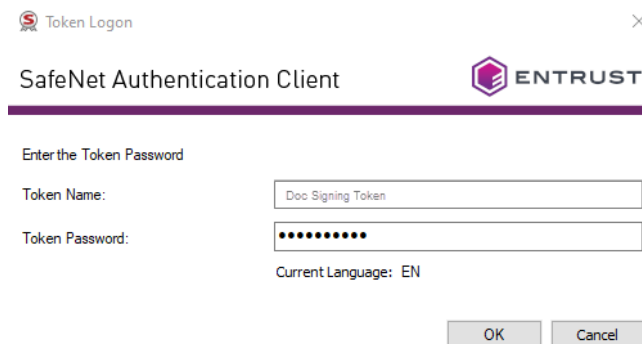
16 Locate the script in your **Downloads** (or other) folder, and right-click > **Run with PowerShell**.



- 17 The 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/Return key.

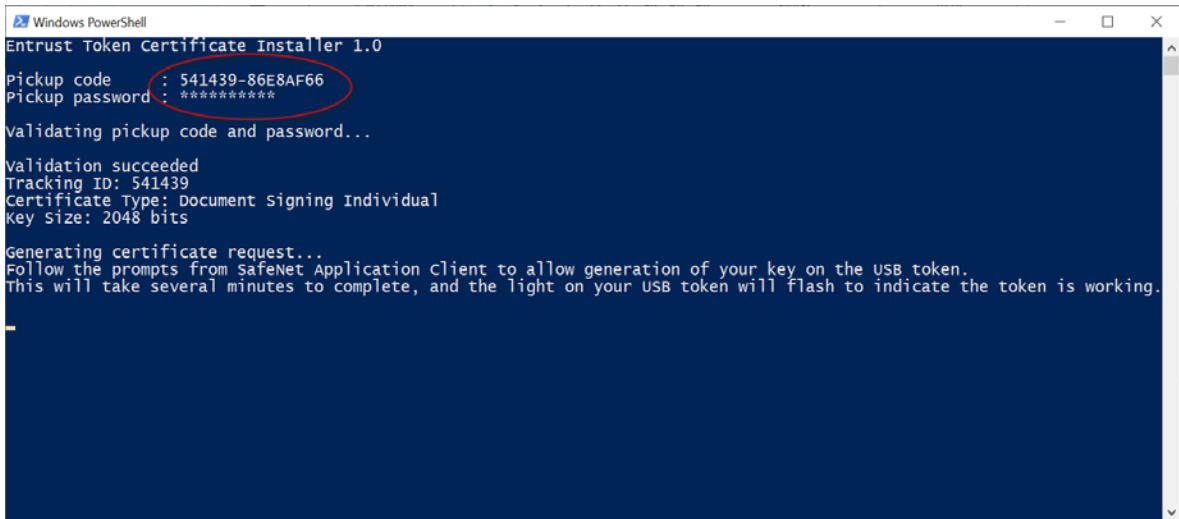
```
Windows PowerShell
Entrust Token Certificate Installer 1.0
Pickup code      : 541438-5B25DDE3
Pickup password  : *****
```

- 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/Return key.
The SafeNet client is started.



- 21 Log in to the token using the password you set during token initialization.
- 22 Click **OK**.

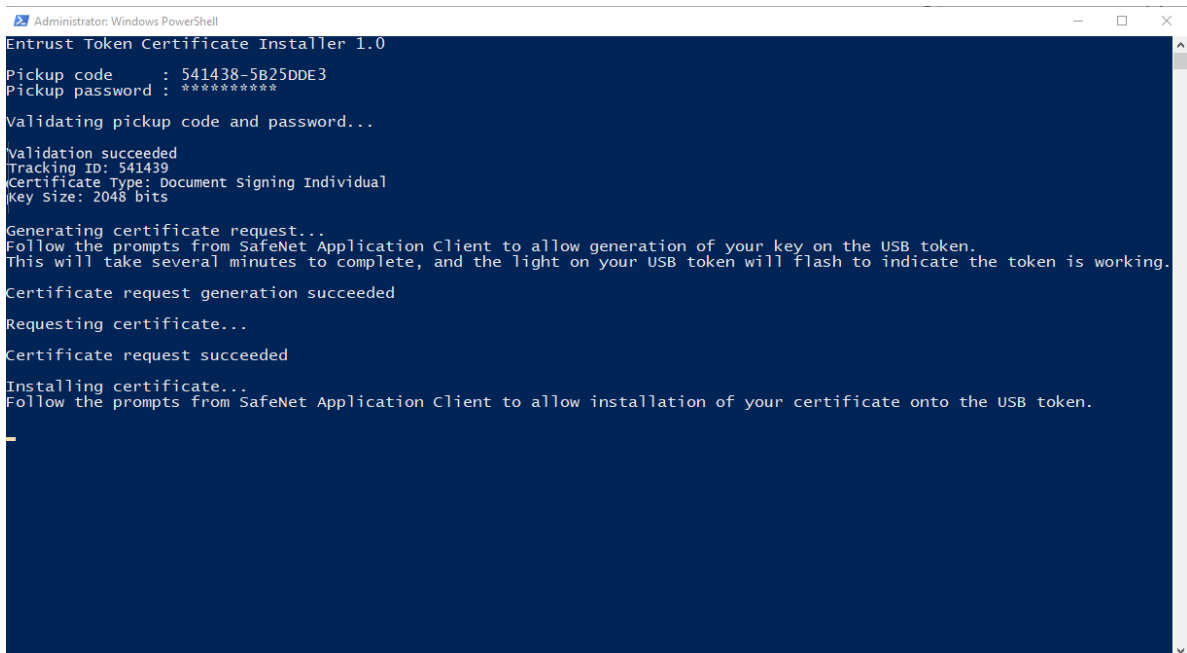
23 The PowerShell installation script continues to run.



```
Windows PowerShell
Entrust Token Certificate Installer 1.0
Pickup code : 541439-86E8AF66
Pickup password : *****
Validating pickup code and password...
Validation succeeded
Tracking ID: 541439
Certificate Type: Document Signing Individual
Key Size: 2048 bits
Generating certificate request...
Follow the prompts from SafeNet Application Client to allow generation of your key on the USB token.
This will take several minutes to complete, and the light on your USB token will flash to indicate the token is working.
```

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

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



```
Administrator: Windows PowerShell
Entrust Token Certificate Installer 1.0
Pickup code : 541438-5B25DDE3
Pickup password : *****
Validating pickup code and password..
Validation succeeded
Tracking ID: 541439
Certificate Type: Document Signing Individual
Key size: 2048 bits
Generating certificate request..
Certificate request generation succeeded
Requesting certificate...
Certificate request succeeded
Installing certificate...
Follow the prompts from SafeNet Application Client to allow installation of your certificate onto the USB token.
```

- 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

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

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

- 1 Insert your token into a USB port.
- 2 Click the link provided in the notification email from Entrust 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.

ENTRUST

Account: Enterprise (English Account)

Pick up certificate: Password

Enter the certificate pickup password.

[Use Internet Explorer to pick up to USB token \(legacy pickup process\).](#)

- 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 9 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.



Pick up certificate: Agreement

Certificate type: Document Signing Individual **Expiry date:** Friday, January 13, 2023

Certificate Subject: email=bruce.bateman@entrust.com, cn=Bruce Bateman, o=Additional Org of Primary Client, l=Ottawa, st=Ontario, c=CA

Please read the following Agreement. By declining this agreement, you are forfeiting your ability to create Document Signing certificates. You must accept the terms and conditions to proceed.

General Terms and Conditions

These general terms and conditions ("General Terms") are part of a legally binding agreement, which is confirmed or accepted when an Order (as defined in Section 1 below) is made or an "Accept" or similar button, and/or a check box presented with these General Terms (or a Schedule, defined below, incorporating these General Terms) is clicked and/or checked by you, for any one or more of the following Entrust products and services (each, an "Offering"): (a) one or more executable software modules and associated deployment tools in machine-readable form ("Software"); (b) managed or cloud services hosted by Entrust or its hosting providers ("Hosted Service"); (c) technical support, training and Software maintenance ("Support"); and (d) consulting and other professional services ("Professional Services").

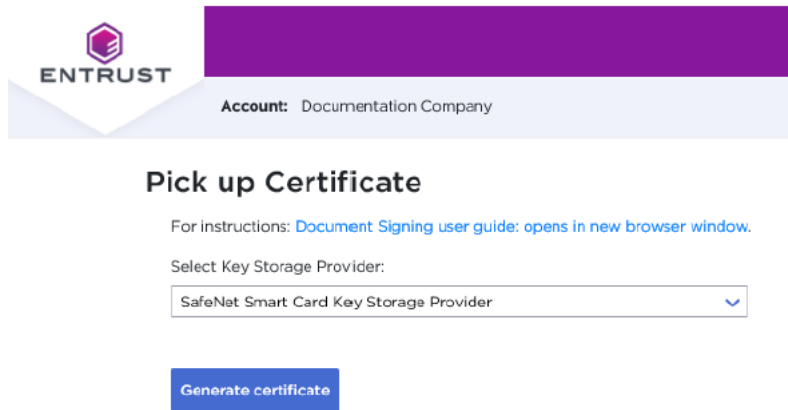
You, as the individual clicking and/or checking the aforementioned buttons and/or boxes, represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS, USE, DOWNLOAD, AND/OR INSTALL THE ENTRUST OFFERING. THE CONTINUED RIGHT TO ACCESS AND USE THE ENTRUST OFFERING IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (AND BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. Contract Structure and Parties.

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

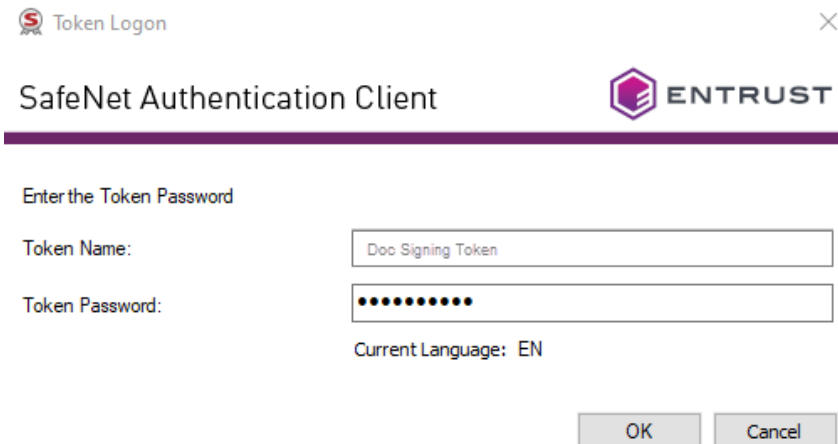
The **Pick up Certificate** page appears.



The screenshot shows the top of the Entrust web interface. On the left is the Entrust logo. To its right is a purple header bar. Below the header bar, the text "Account: Documentation Company" is displayed. The main heading is "Pick up Certificate". Below this heading, there is a link: "For instructions: [Document Signing user guide: opens in new browser window.](#)". Underneath is a label "Select Key Storage Provider:" followed by a dropdown menu showing "SafeNet Smart Card Key Storage Provider". At the bottom of the form is a blue button labeled "Generate certificate".

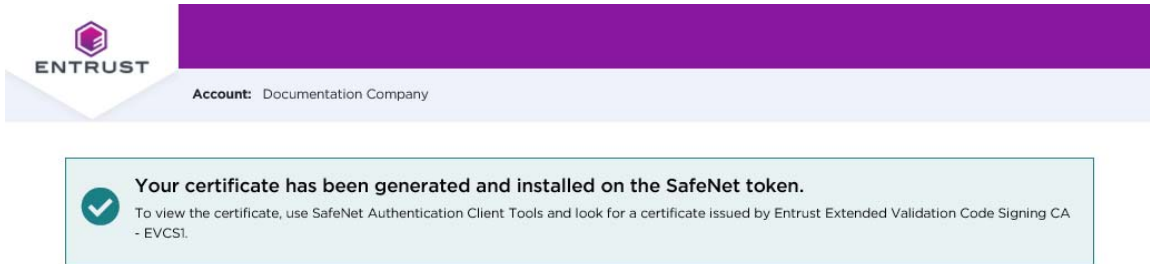
10 Click **Generate Certificate**.

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 screenshot shows a "Token Logon" dialog box. At the top left is a small icon and the text "Token Logon". At the top right is a close button (X). The main title is "SafeNet Authentication Client" and the Entrust logo is on the right. Below the title is a purple horizontal bar. The text "Enter the Token Password" is displayed. There are two input fields: "Token Name:" with the value "Doc Signing Token" and "Token Password:" with a masked password of ten dots. Below the input fields is the text "Current Language: EN". At the bottom right are two buttons: "OK" and "Cancel".

- 12** 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

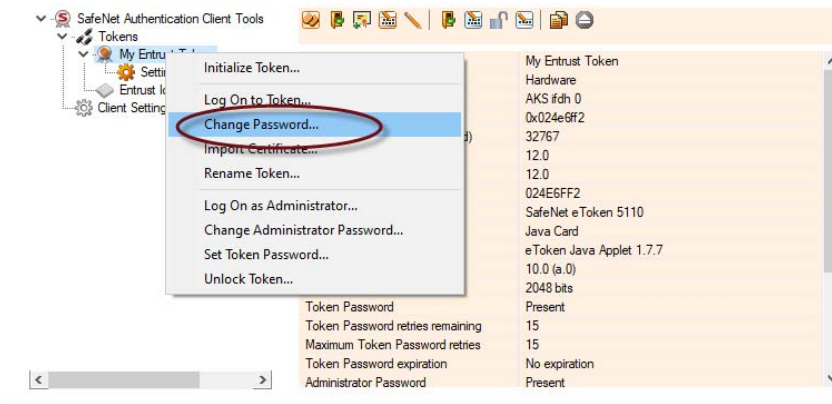
Use the following procedure when you need to change the password for your token.

To change your token password

- 1 Insert your token into a USB slot 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**.



SafeNet Authentication Client



- 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.

Change Password: My Entrust Token

SafeNet Authentication Client

ENTRUST

Current Token Password:

New Token Password:

Confirm Password: 100%

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: EN

OK Cancel

- 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.

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 through 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:

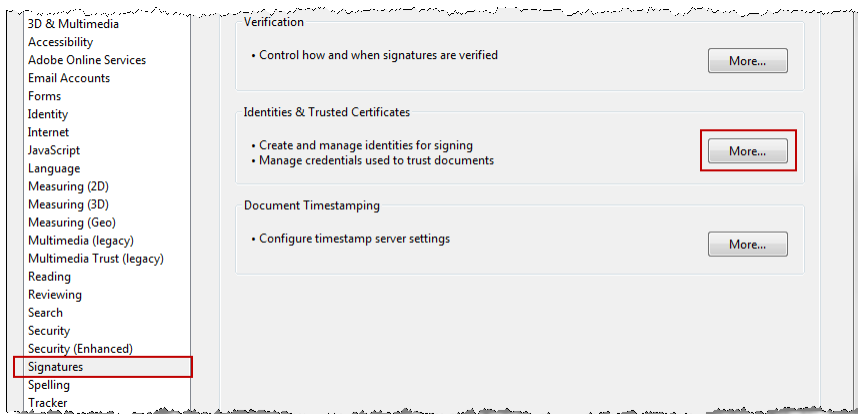
Procedures in this chapter are based on Adobe Acrobat Reader DC version 2015.010. The instructions may differ for other versions of Adobe Reader and Adobe Acrobat.

Complete the following procedures to sign a document:

- ["Select your certificate in Adobe Reader" on page 42](#)
- ["Sign the PDF document" on page 43](#)

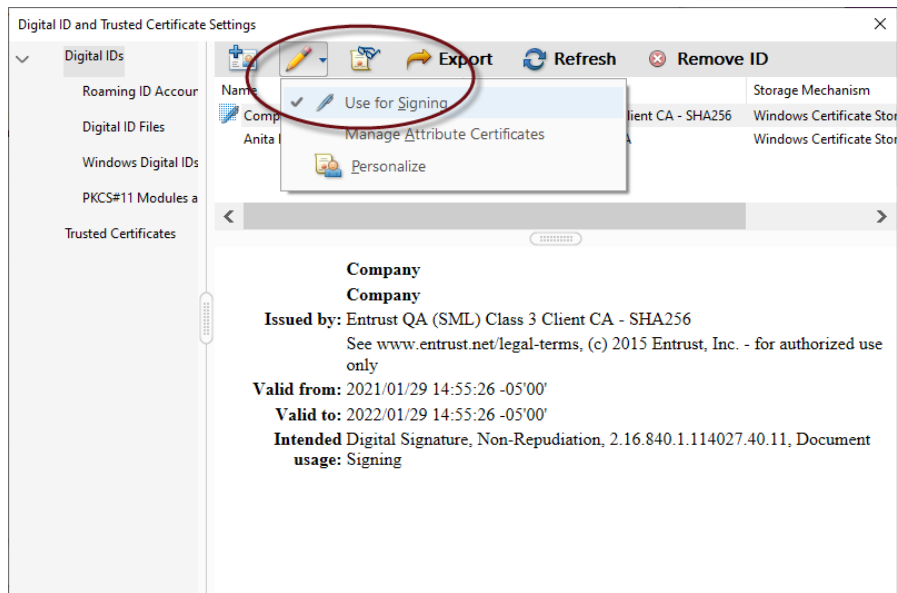
Select your certificate in Adobe Reader

- 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**.

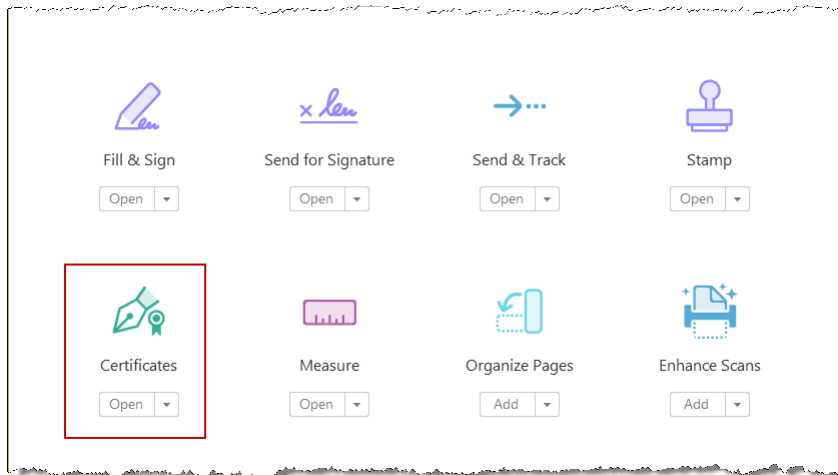


- 8 Close the Digital ID and Trusted Certificate Settings page and click **OK** in the Preferences page.

Sign the PDF document

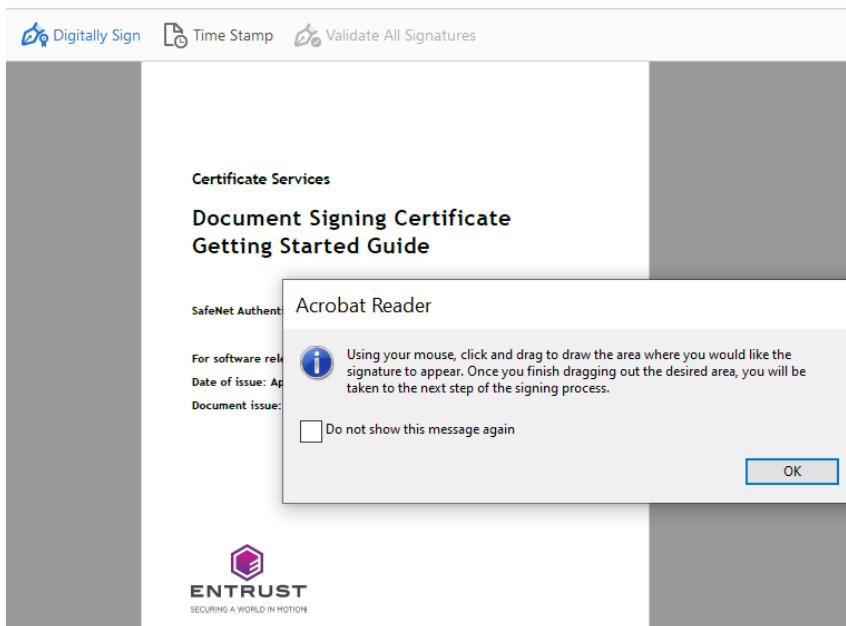
- 1 Be sure that your token is plugged in to a USB port on your computer.
- 2 In the Adobe Reader ribbon, select the **Tools tab**.

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

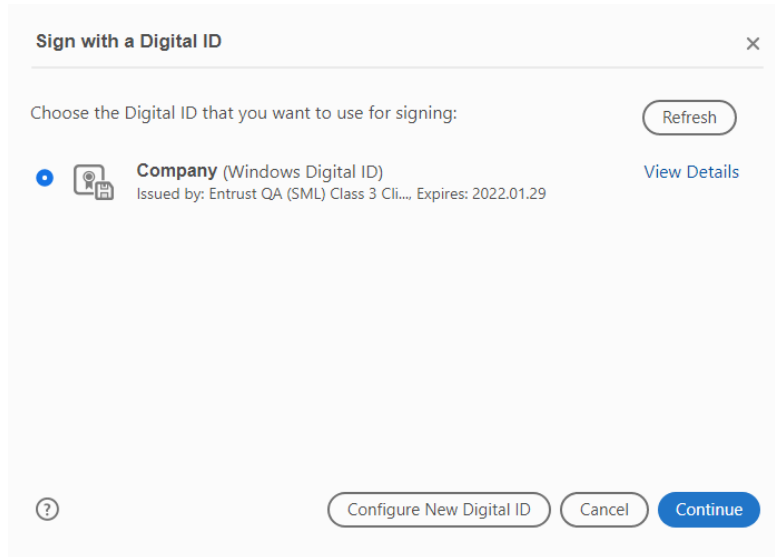


a Select **Digitally Sign** in the ribbon.

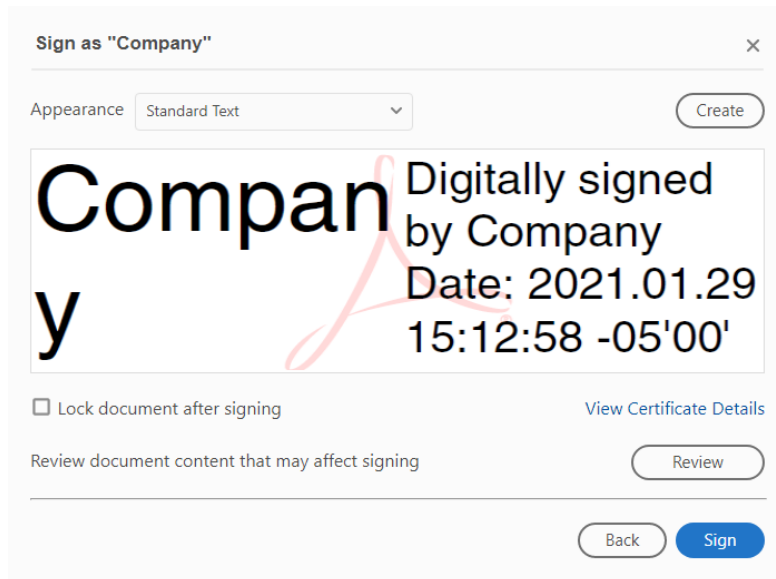
4 Read the information dialog and click **OK**.



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



- Make sure the correct certificate is selected, and click Continue.
- In the Sign Document dialog, edit the appearance of the signature if required. Help is provided for this dialog.



- 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.

Compa
ny

Digitally signed
by Company
Date: 2021.01.29
15:14:14 -05'00'



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.

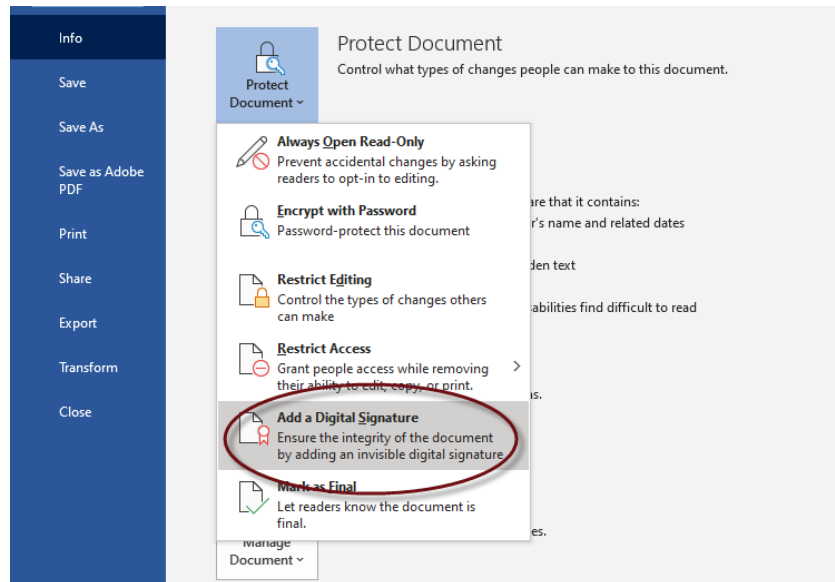


Note:

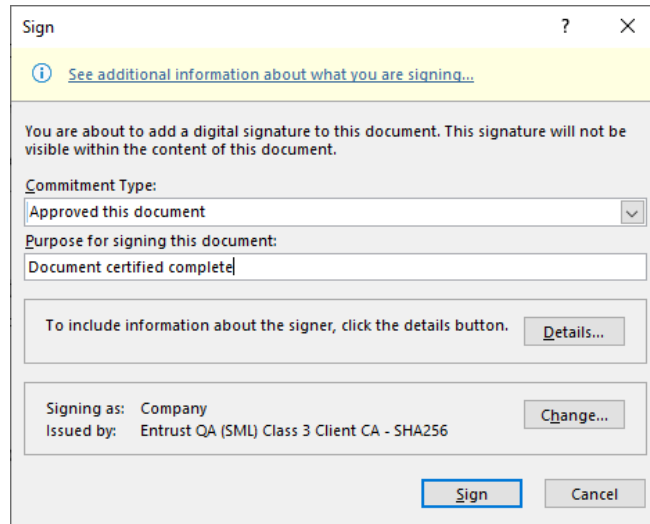
This procedure is based on Microsoft Office 2013. The procedure may differ for other Microsoft Office versions.

To sign a Word document

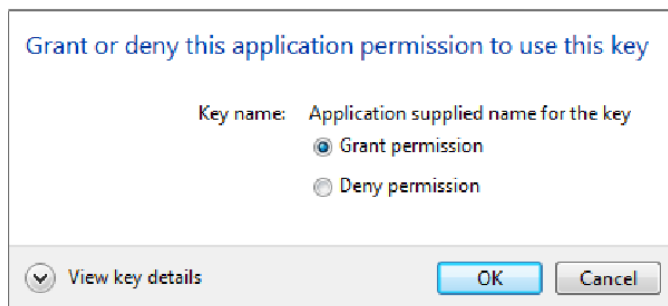
- 1 Plug the token with your Entrust Document Signing certificate into a USB port on your computer.
- 2 In your Word document, select **File > Info**.
- 3 Select **Protect Document > Add a Digital Signature**.



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**.