ENTRUST

Certificate Services
OV and EV Code Signing Guide

SafeNet Authentication Client, Version 10.8

For software release 13.8

Date of issue: January 2024

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.

© 2024 Entrust Corporation. All rights reserved.

TOC

About this guide

This guide describes how to store an Entrust certificate on an iKey 5100 token or Hardware Security Module (HSM). This includes:

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

Topics in this section:

Documentation feedback

You can rate and provide feedback about Entrust product documentation by completing the online feedback form. Suggestions and bug reports that you provide go directly to the documentation team and are used to improve and correct the information in Entrust guides. Access this form by:

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

Revision information

Document issue	Section	Revision
Issue 1.0	N/A	First release for 13.8.

Documentation conventions

The following documentation conventions are used in Entrust guides:

Table 1: Typographic conventions

Convention	Purpose	Example
Bold text (other than headings)	Indicates graphical user interface elements and wizards.	Click **Next**.
Italicized text	Used for book or document titles.	*Entrust Certificate Services Enrollment Guide*
Blue text	Used for hyperlinks to other sections in the document.	Entrust TruePass supports the use of many types of digital ID.
Underlined blue text	Used for Web links.	For more information, visit our website at www.entrust.net.
`Courier` type	Indicates installation paths, file names, Windows registry keys, commands, and text you must enter.	Use the `entrust-configuration.xml` file to change certain options for Verification Server.
Angle brackets < >	Indicates variables (text you must replace with your organization's correct values).	By default, the `entrust.ini` file is located in `<install_path>/conf/security/entrust.ini`.

Note and Attention text

Throughout this guide, paragraphs are set off by ruled lines above and below. They provide key information with two levels of importance, as shown below.

Note:
Information to help you maximize the benefits of your Entrust product.

Attention:
Issues that, if ignored, may seriously affect performance, security, or the operation of your Entrust product.

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 website 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 reading material that may be used in conjunction with this guide.

- Token software information (https://safenet.gemalto.com)

Documentation feedback

You can rate and provide feedback about Entrust product documentation by completing the online feedback form. Suggestions and bug reports that you provide go directly to the documentation team and are used to improve and correct the information in Entrust guides. Access this form by:

- clicking the *Report any errors or omissions* link located in the footer of Entrust PDF documents (see bottom of this page).
- 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:

- “Supported platforms” on page 12
- “Before you start” on page 13
- “Downloading and installing the token software (required for USB token pickup)” on page 14
- “Initializing an Entrust USB token” on page 21
- “Retrieving your Entrust certificate” on page 31
- “Changing the password for your token” on page 49
- “Installing the certificate to a Hardware Security Module (HSM)” on page 51
- “Recovering a certificate” on page 56
- “Downloading the certificate to Azure Key Vault or AWS CloudHSM” on page 57

Supported platforms

The following platforms and browsers are supported.

Supported operating systems

The following operating systems are supported:

- Microsoft Windows 11 update version 21H2
- Microsoft Windows 10 32-bit or 64-bit, version 21H1 or lower
- Microsoft Windows Server 2019. 64-bit
- Microsoft Windows Server 2016 64-bit

Supported browsers

The following browsers are supported:

- Microsoft Edge
- Mozilla Firefox 37 or higher
- Chrome 45 or higher
- Safari 5 or higher

Supported tokens

The following SafeNet eTokens are supported:

- 5110 CC
- 5110+ (also called 5110+ FIPS)

Tokens 510x (also called 5100) and 5110 are no longer supported for code signing.

Important changes

Entrust now offers ECS Enterprise customers the option of using Azure Cloud Key Vault or AWS CloudHSM as an alternative to a customer premises located HSM or a hardware Token.

Before you start

To download an Entrust certificate, you need:

- a supported browser with Internet access
- a supported operating system
- a supported token (provided by Entrust) or a Hardware Security Module (HSM)
- if you are using an HSM, you will need a certificate signing request (CSR) from the HSM to generate a certificate.

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

Installing to a token

This section discusses:

- how to configure a token to receive your certificate
- how to download the certificate from Entrust Certificate Services

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

The token software provided by Entrust must be installed before 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.

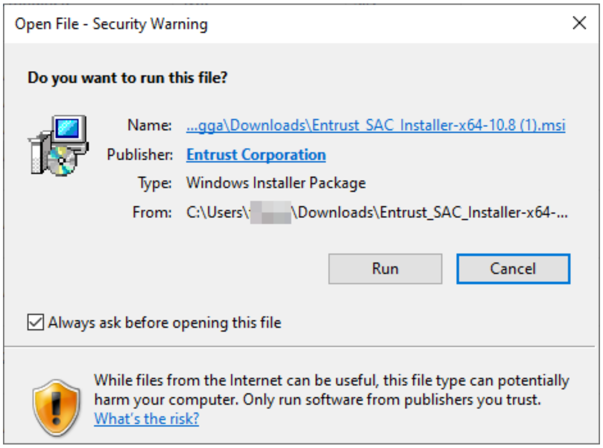
Attention:
Do not plug your token into your computer until you have completed this procedure.

Note:
For installing to HSM: This procedure is not needed. Proceed to: "Installing the certificate to a Hardware Security Module (HSM)" on page 51

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**.



Open File - Security Warning

Do you want to run this file?

Name: ...gga\Downloads\Entrust_SAC_Installer-x64-10.8 (1).msi

Publisher: **Entrust Corporation**

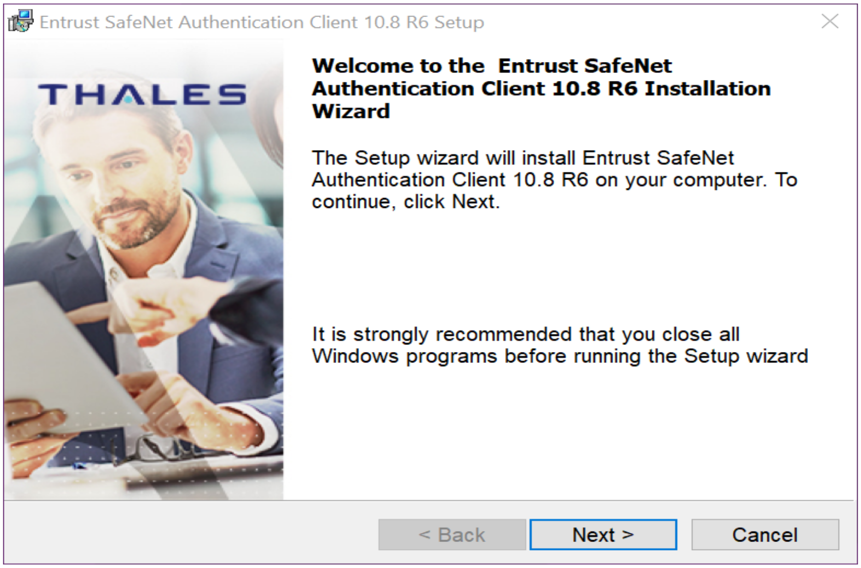
Type: Windows Installer Package

From: C:\Users\[redacted]\Downloads\Entrust_SAC_Installer-x64-...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

The installation wizard appears.



Entrust SafeNet Authentication Client 10.8 R6 Setup

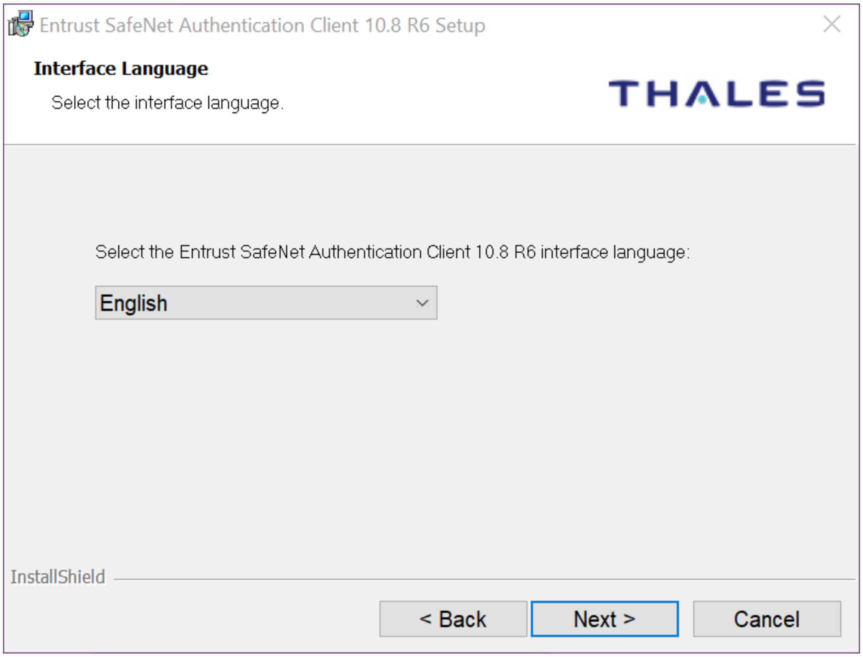
Welcome to the Entrust SafeNet Authentication Client 10.8 R6 Installation Wizard

The Setup wizard will install Entrust SafeNet Authentication Client 10.8 R6 on your computer. To continue, click Next.

It is strongly recommended that you close all Windows programs before running the Setup wizard

4 Click **Next**.

The **Interface language** page appears.



Entrust SafeNet Authentication Client 10.8 R6 Setup

Interface Language

Select the interface language.

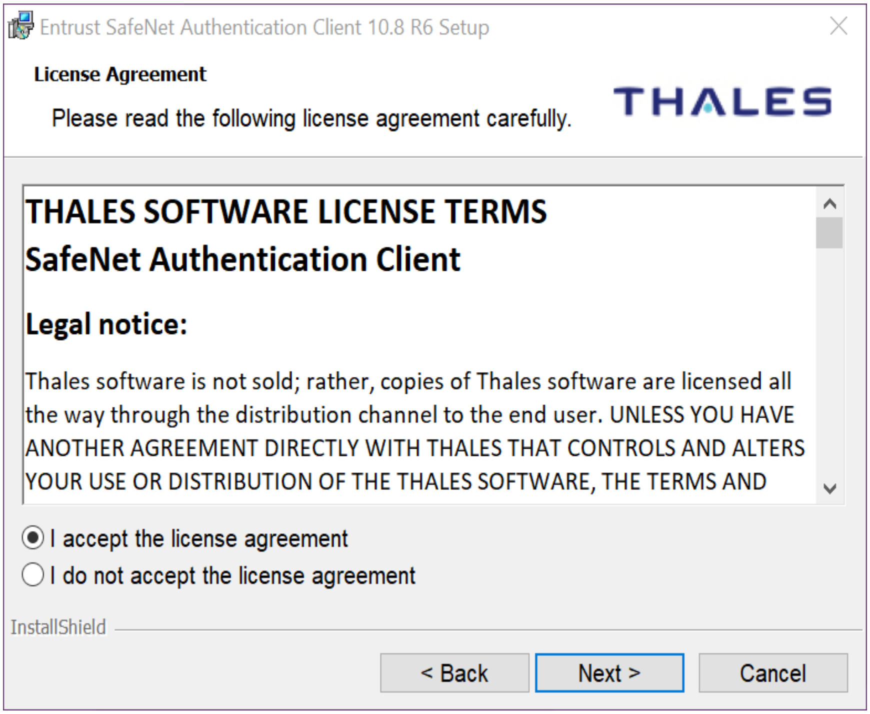
Select the Entrust SafeNet Authentication Client 10.8 R6 interface language:

English

5 Select the language to use for the installation.

6 Click **Next**.

The **License Agreement** screen appears.



Entrust SafeNet Authentication Client 10.8 R6 Setup

License Agreement

Please read the following license agreement carefully.

THALES SOFTWARE LICENSE TERMS

SafeNet Authentication Client

Legal notice:

Thales software is not sold; rather, copies of Thales software are licensed all the way through the distribution channel to the end user. UNLESS YOU HAVE ANOTHER AGREEMENT DIRECTLY WITH THALES THAT CONTROLS AND ALTERS YOUR USE OR DISTRIBUTION OF THE THALES SOFTWARE, THE TERMS AND

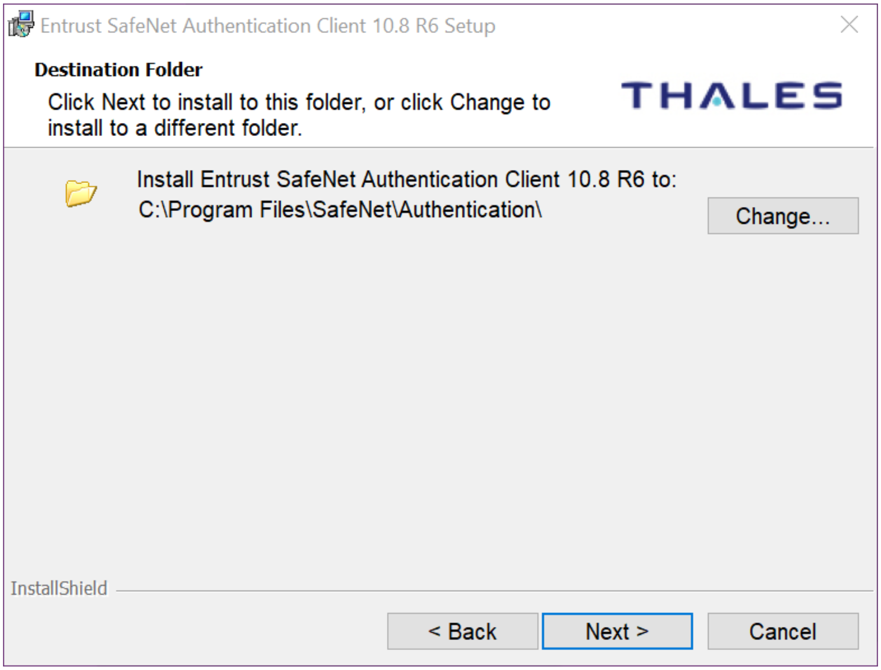
● I accept the license agreement

○ I do not accept the license agreement

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

8 Click **Next**.

The Destination Folder screen appears.



Entrust SafeNet Authentication Client 10.8 R6 Setup

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Entrust SafeNet Authentication Client 10.8 R6 to:
C:\Program Files\SafeNet\Authentication\

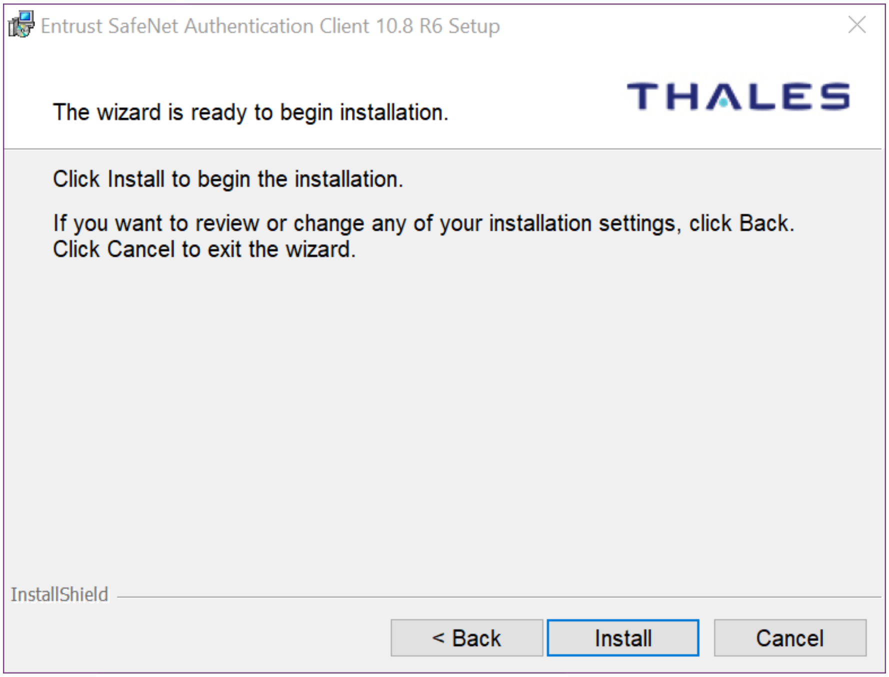
9 Accept the default folder or click **Change** to choose a new folder.

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.



Entrust SafeNet Authentication Client 10.8 R6 Setup

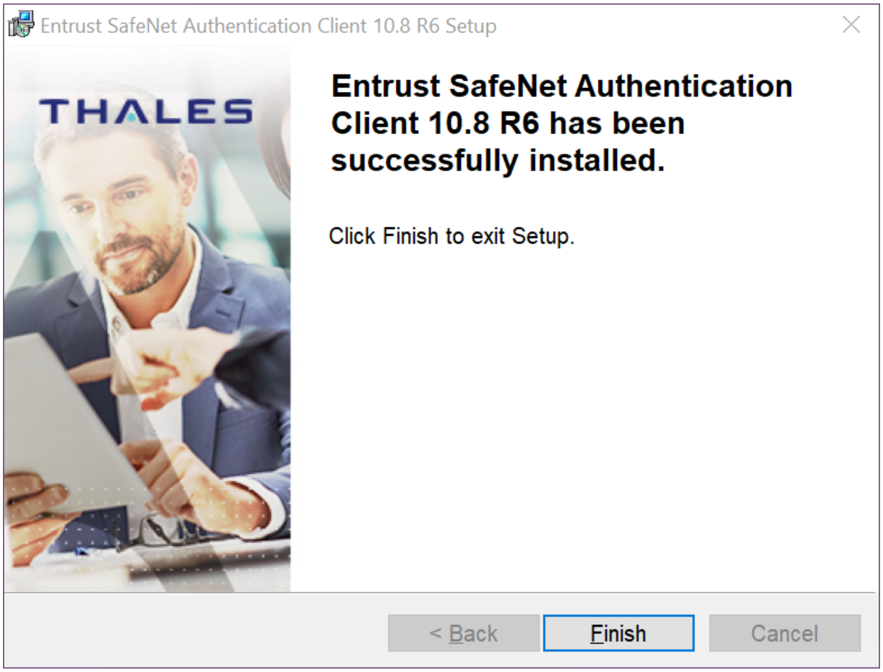
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

13 Click **Install**.

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



Entrust SafeNet Authentication Client 10.8 R6 Setup

Entrust SafeNet Authentication Client 10.8 R6 has been successfully installed.

Click Finish to exit Setup.

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: "Retrieving your Entrust certificate" on page 31.

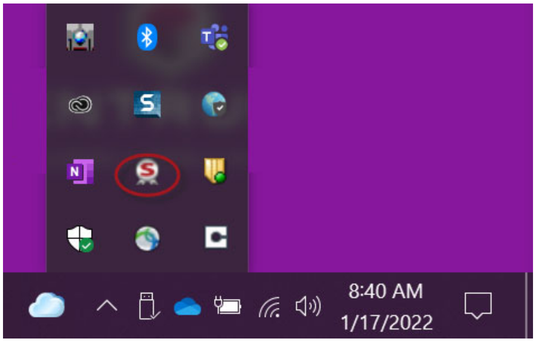
Attention:
This procedure is for new tokens. If this is not a new token, initializing the token will delete all certificates stored on the token.

Note:
For installing to HSM: This procedure is not needed. Proceed to: "Installing the certificate to a Hardware Security Module (HSM)" on page 51

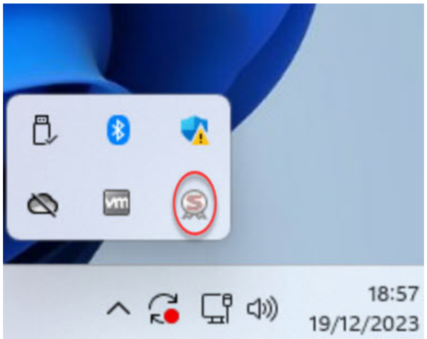
To initialize your token

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.

Windows 10 system tray

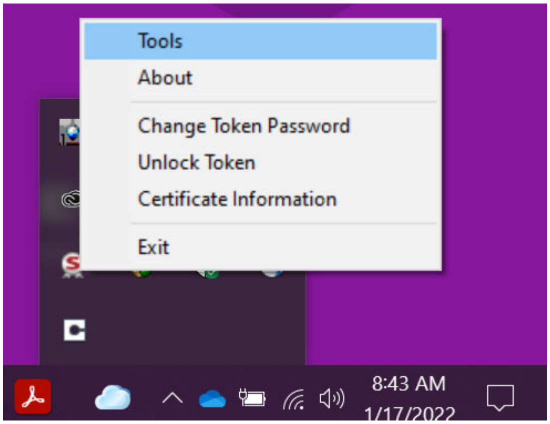


Windows 11 system tray

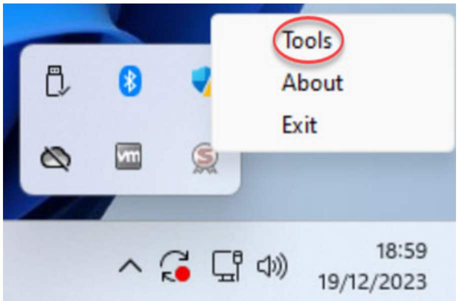


2. When the icon becomes active, right-click it to open the context menu. Select **Tools**.

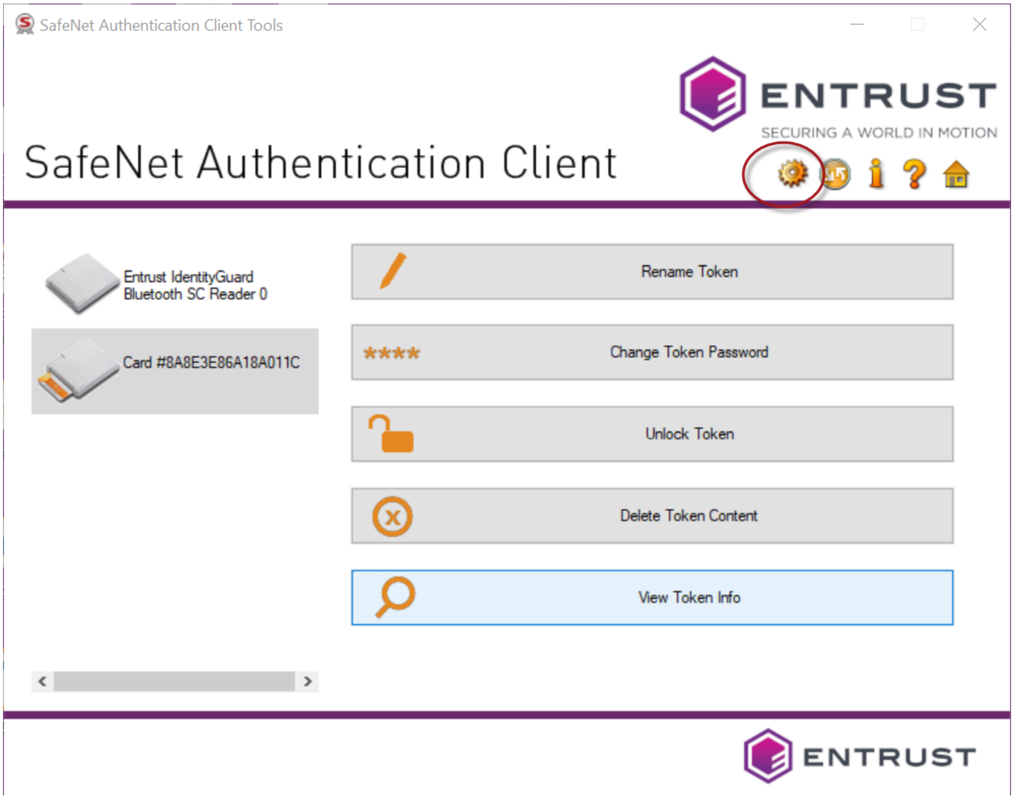
Windows 10 context menu



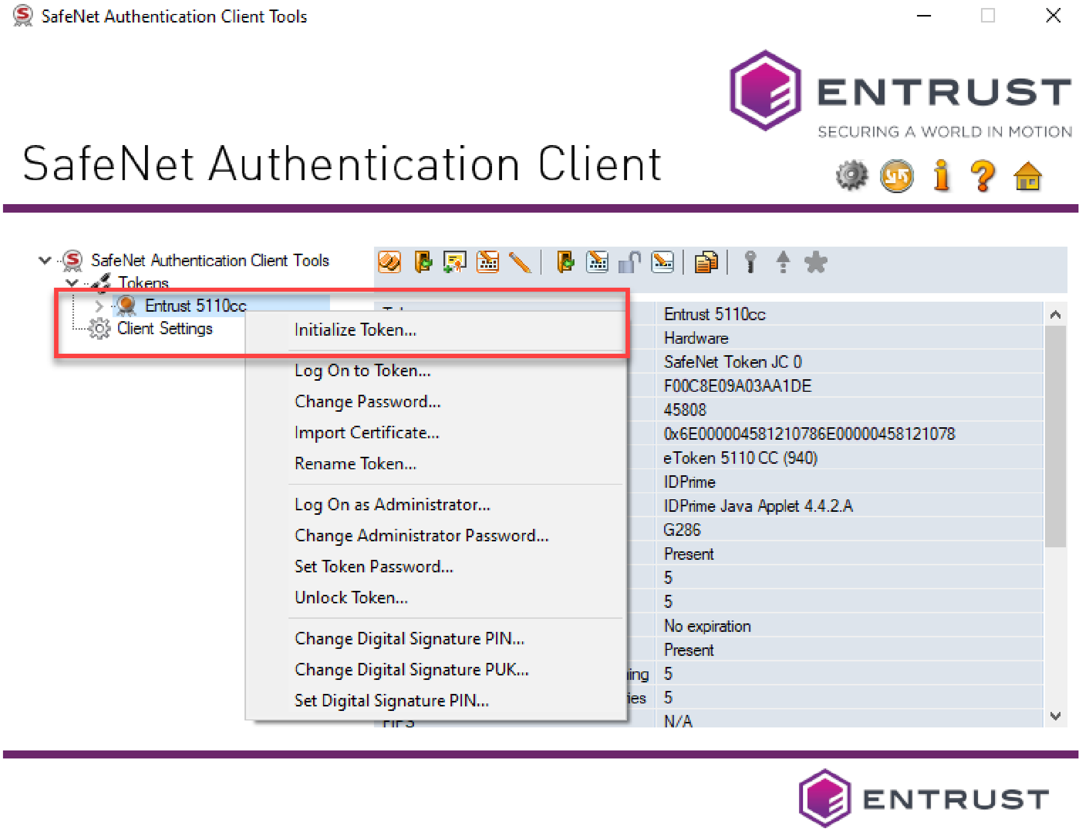
Windows 11 context menu



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

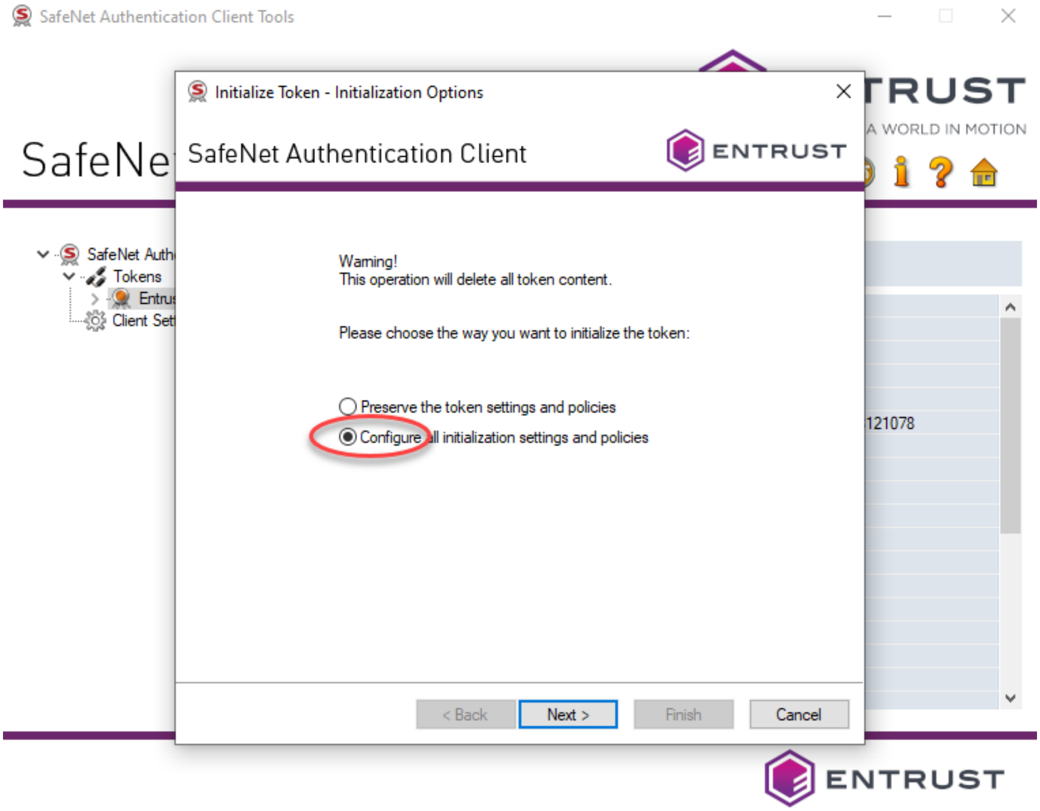

SafeNet Authentication Client Tools
ENTRUST
SECURING A WORLD IN MOTION
SafeNet Authentication Client
Entrust IdentityGuard Bluetooth SC Reader 0
Card #8A8E3E86A18A011C
Rename Token
Change Token Password
Unlock Token
Delete Token Content
View Token Info
ENTRUST

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


SafeNet Authentication Client Tools
ENTRUST
SECURING A WORLD IN MOTION
SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
Entrust 5110cc
Client Settings
Initialize Token...
Log On to Token...
Change Password...
Import Certificate...
Rename Token...
Log On as Administrator...
Change Administrator Password...
Set Token Password...
Unlock Token...
Change Digital Signature PIN...
Change Digital Signature PUK...
Set Digital Signature PIN...
ENTRUST

Entrust 5110cc
Hardware
SafeNet Token JC 0
F00C8E09A03AA1DE
45808
0x6E000004581210786E00000458121078
eToken 5110 CC (940)
IDPrime
IDPrime Java Applet 4.4.2.A
G286
Present
5
5
No expiration
Present
5
5
N/A

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



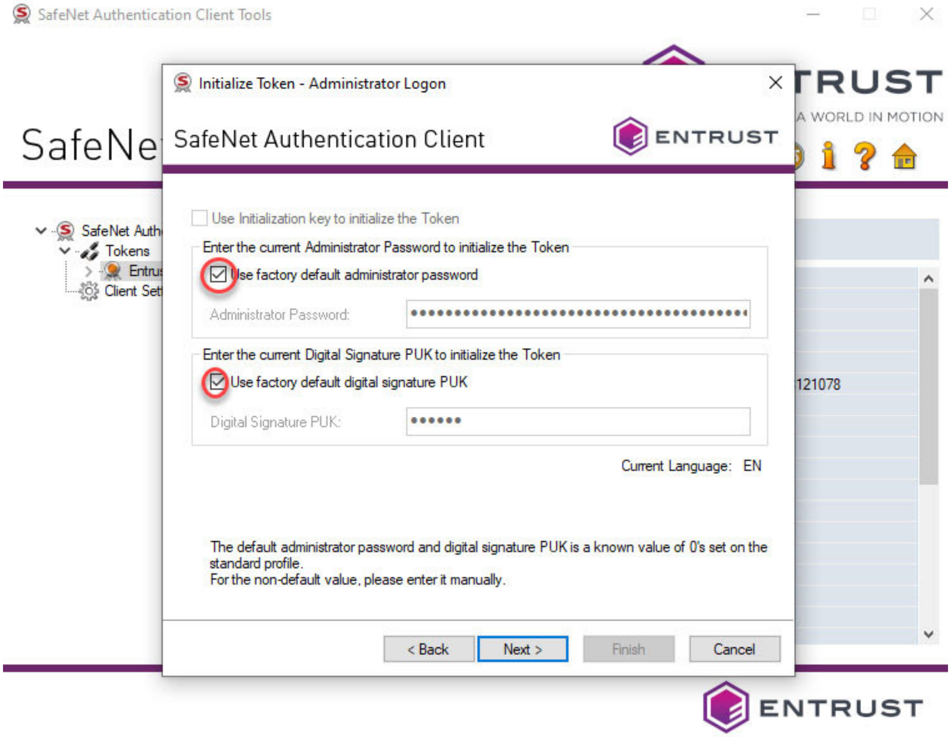
Warning!
This operation will delete all token content.

Please choose the way you want to initialize the token:

○ Preserve the token settings and policies
● Configure all initialization settings and policies

6 Click **Next**.

The *Administrator Logon* page appears.



SafeNet Authentication Client Tools

Initialize Token - Administrator Logon

SafeNet Authentication Client

☐ Use Initialization key to initialize the Token

Enter the current Administrator Password to initialize the Token

☑ Use factory default administrator password

Administrator Password: ••

Enter the current Digital Signature PUK to initialize the Token

☑ Use factory default digital signature PUK

Digital Signature PUK: ••••••

Current Language: EN

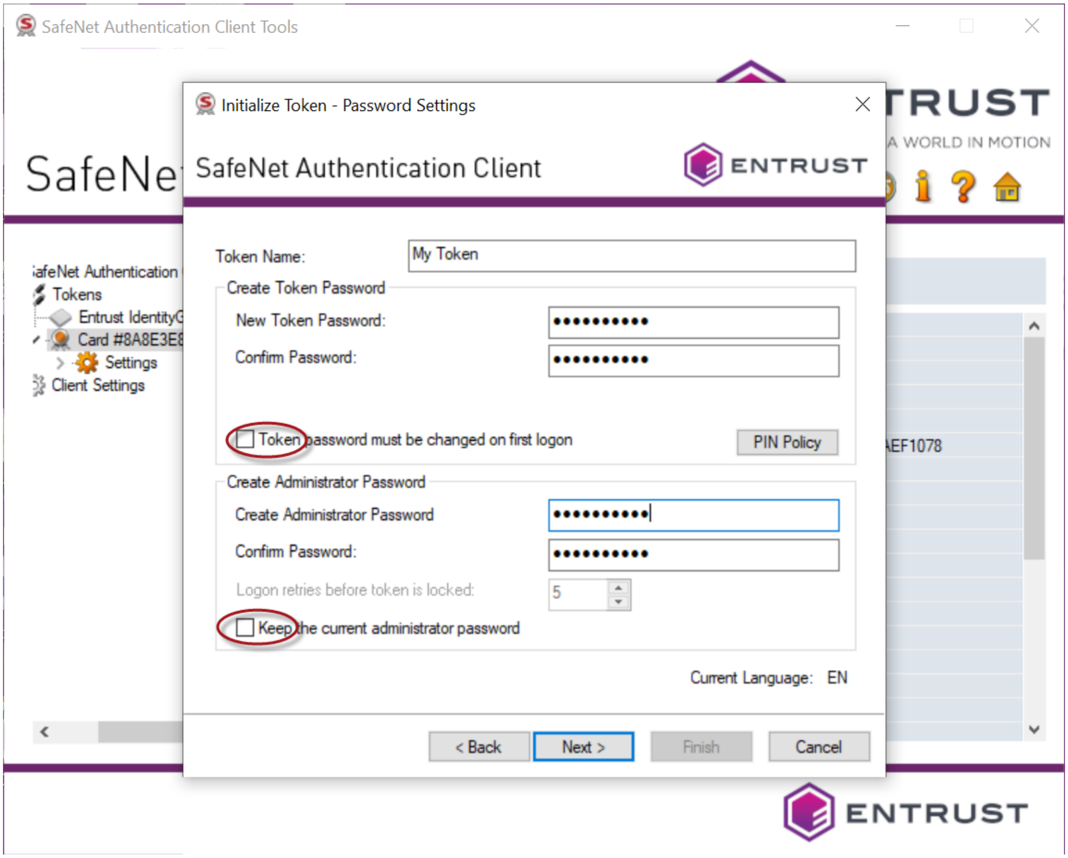
The default administrator password and digital signature PUK is a known value of 0's set on the standard profile.
For the non-default value, please enter it manually.

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

8 If applicable, select **Use the factory default signature PUK** and leave the default.

9 Click **Next**.

The *Initialize Token - Password Settings* page appears.



Initialize Token - Password Settings

SafeNet Authentication Client

Token Name: My Token

Create Token Password

New Token Password: ••••••••••

Confirm Password: ••••••••••

□ Token password must be changed on first logon

Create Administrator Password

Create Administrator Password ••••••••••

Confirm Password: ••••••••••

Logon retries before token is locked: 5

□ Keep the current administrator password

Current Language: EN

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**.

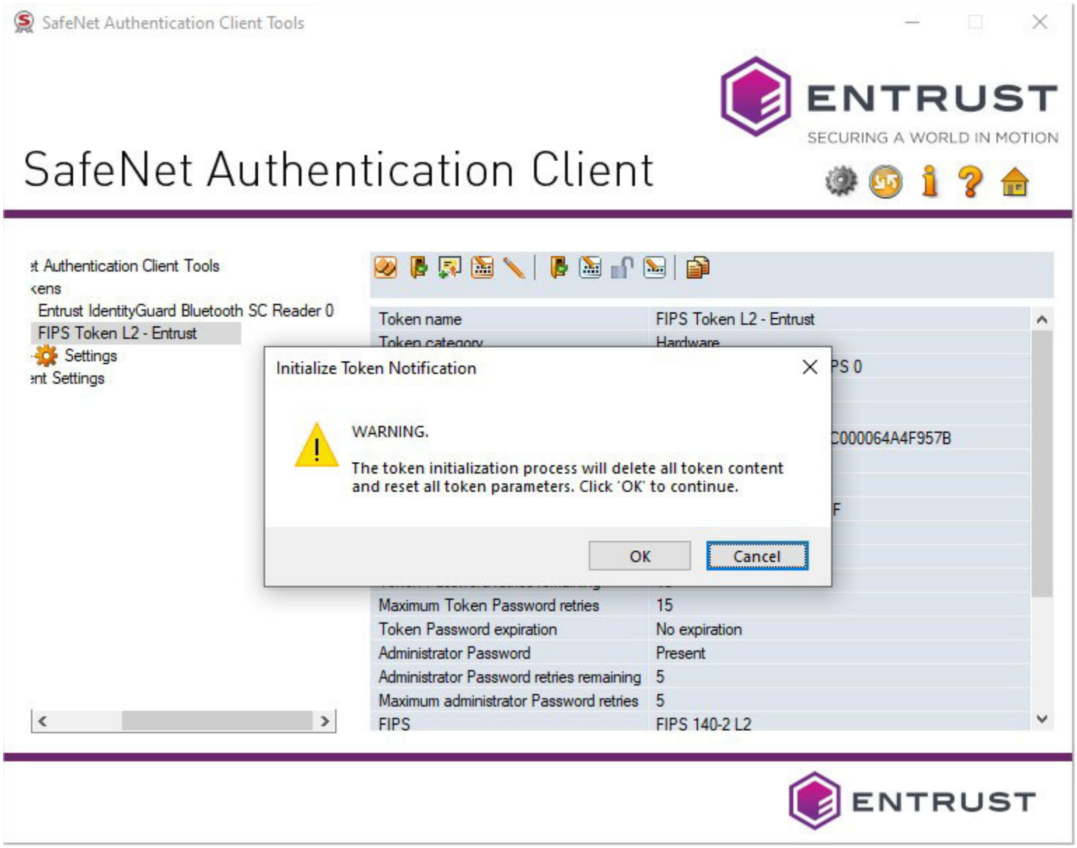
⚠ **Attention:**
You will be asked for this password when you use the certificate. It is important that you either remember this password or store it in a secure location. **If you enter the wrong password more than five times, the token will lock and cannot be unlocked**. You will need to buy a new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

11 Click **Next**.

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

12 Click **Finish**.

You may see a warning dialog box, “The token initialization process will delete all token content and reset all token parameters.”



SafeNet Authentication Client Tools

SafeNet Authentication Client

ENTRUST SECURING A WORLD IN MOTION

Initialize Token Notification

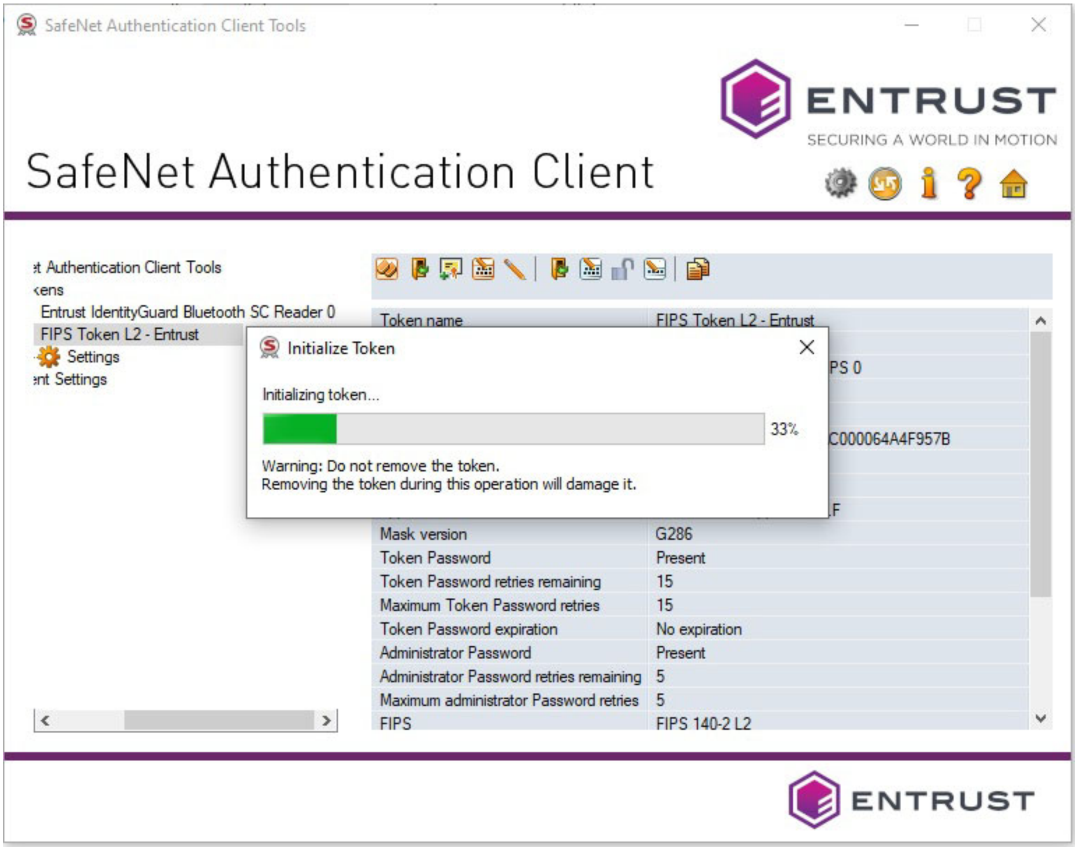
WARNING.

The token initialization process will delete all token content and reset all token parameters. Click 'OK' to continue.

Token name	FIPS Token L2 - Entrust
Token category	Hardware
Maximum Token Password retries	15
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	FIPS 140-2 L2

13 Click **OK** to complete the initialization if you see the warning dialog box.

A status bar opens, indicating the progress of the initialization.



SafeNet Authentication Client Tools

SafeNet Authentication Client

ENTRUST

SECURING A WORLD IN MOTION

ɛt Authentication Client Tools

‹ens

Entrust IdentityGuard Bluetooth SC Reader 0

FIPS Token L2 - Entrust

Settings

ɜnt Settings

Token name	FIPS Token L2 - Entrust
	PS 0
	C000064A4F957B
	F
Mask version	G286
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	FIPS 140-2 L2

Initialize Token

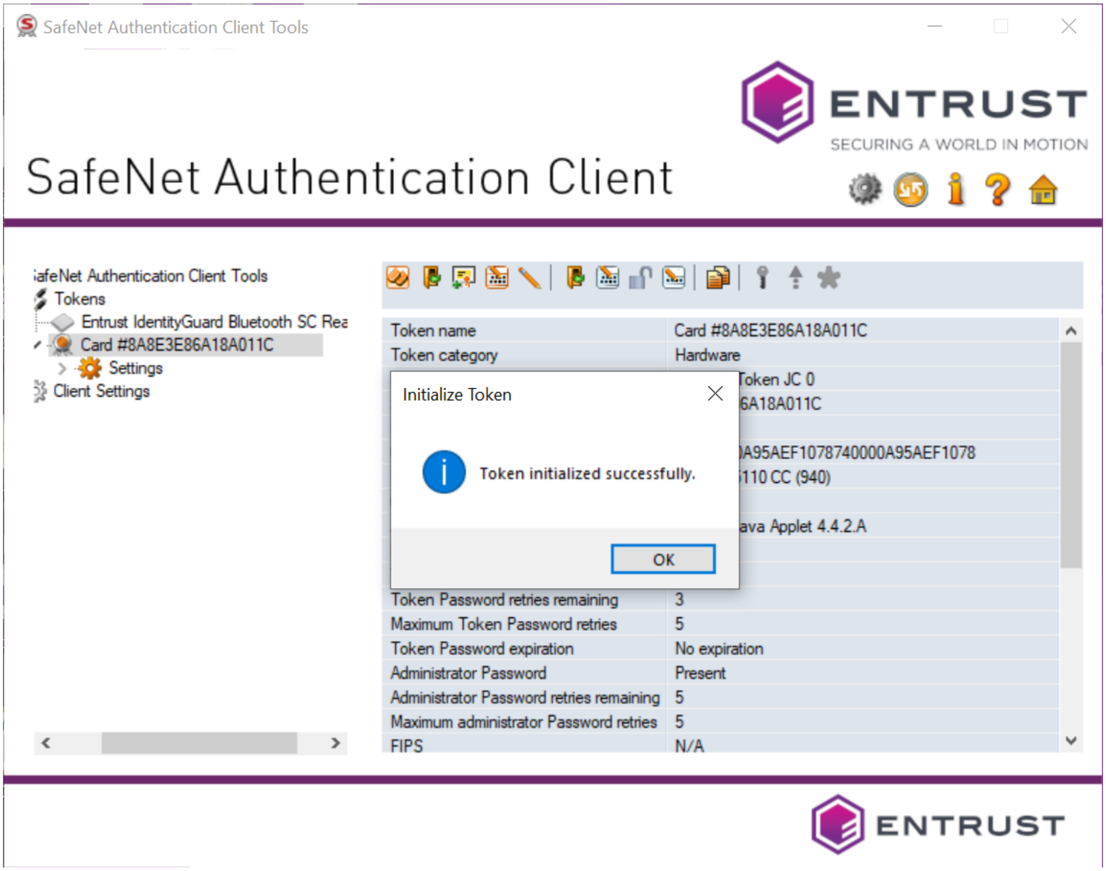
Initializing token...

33%

Warning: Do not remove the token.
Removing the token during this operation will damage it.

ENTRUST

14 A success message appears once the initialization is complete. Click **OK**.



SafeNet Authentication Client Tools

SafeNet Authentication Client

ENTRUST
SECURING A WORLD IN MOTION

- ɪafeNet Authentication Client Tools
  - Tokens
    - Entrust IdentityGuard Bluetooth SC Rea
    - Card #8A8E3E86A18A011C
      - Settings
  - Client Settings

Token name	Card #8A8E3E86A18A011C
Token category	Hardware
	Token JC 0
	6A18A011C
	A95AEF1078740000A95AEF1078
	110 CC (940)
	ava Applet 4.4.2.A
Token Password retries remaining	3
Maximum Token Password retries	5
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	N/A

Initialize Token

Token initialized successfully.

OK

ENTRUST

Retrieving your Entrust certificate

Code Signing certificates must be installed on secure hardware—either an Entrust USB token, or a Hardware Security Module (HSM). Procedures for both options are included in this section.

Prerequisites

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

- The SafeNet Authentication Client software must be installed on your Microsoft Windows machine. If that has not been done, follow the instructions in: “Downloading and installing the token software (required for USB token pickup)” on page 14
- The Entrust USB token must be initialized. If that has not been done, follow the instructions in: “Initializing an Entrust USB token” on page 21

To pick up and install a certificate to a Hardware Security Module, you need:

- a Hardware Security Module (HSM)
- a CSR that was generated on your HSM

Installing a certificate to secure hardware

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 32
- “To download a certificate to a hardware token using Microsoft Internet Explorer or Microsoft Edge” on page 43

To install the certificate on a Hardware Security Module (HSM), follow the procedure here. Note that you can use any supported browser.

- “Installing the certificate to a Hardware Security Module (HSM)” on page 51

Retrieving a certificate using the Certificate Services interface

This procedure explains how an Entrust Certificate Services administrator can pick up a certificate from the Certificate Services 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 to Entrust USB token using PowerShell script

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

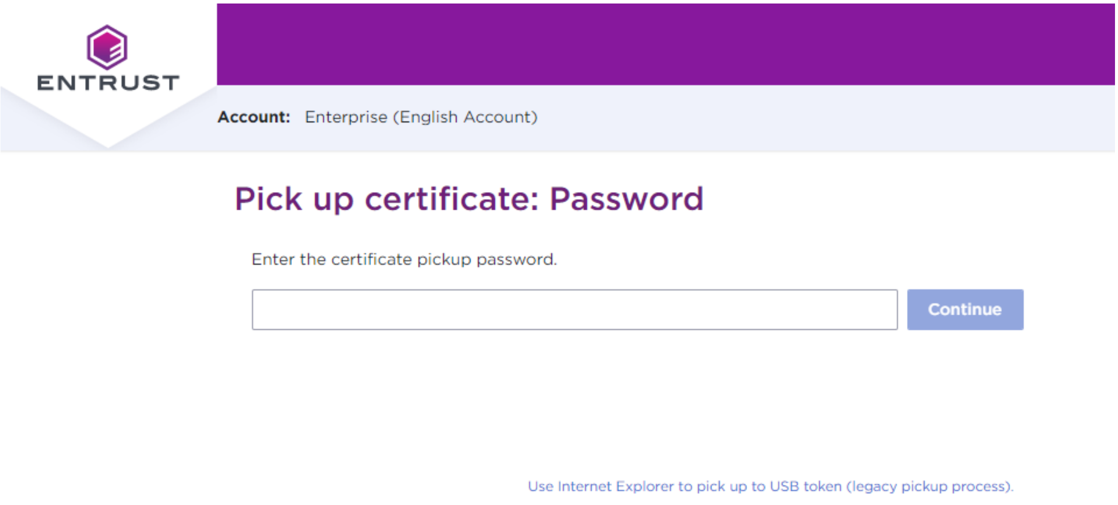
This procedure uses an Entrust-specific Microsoft Windows PowerShell script to install the certificate on your token. Follow the steps of the procedure below to download and run the `token-cert-installer` script in a PowerShell window.

Note:
Windows 11 differs from Windows 10 in its approach to PowerShell scripts. Windows 11 by default turns off the execution policy that enables PowerShell scripts to run. The issue cannot be addressed by making changes to the Entrust PowerShell script. Your IT department must address this issue before you can install tokens. For more details, see “Appendix: Microsoft PowerShell” on page 59.

To download a certificate to a hardware token using a PowerShell script

1. In the notification email from Entrust, click the link to the Entrust Certificate Retrieval Web pages.

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



ENTRUST

Account: Enterprise (English Account)

Pick up certificate: Password

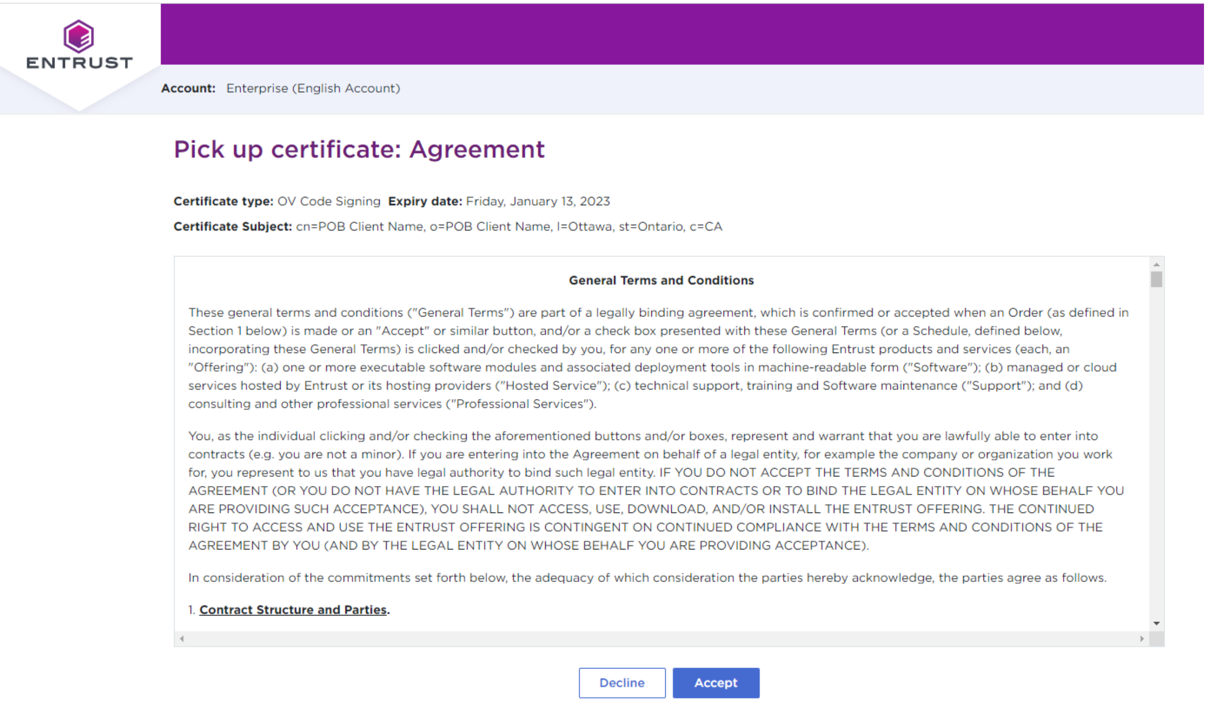
Enter the certificate pickup password.

Use Internet Explorer to pick up to USB token (legacy pickup process).

2 Enter the password that you used when you created the certificate request or the password provided by 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 the Entrust Certificate Services Agreement, then click **Accept**.



Account: Enterprise (English Account)

Pick up certificate: Agreement

Certificate type: OV Code Signing **Expiry date:** Friday, January 13, 2023

Certificate Subject: cn=POB Client Name, o=POB Client Name, l=Ottawa, st=Ontario, c=CA

General Terms and Conditions

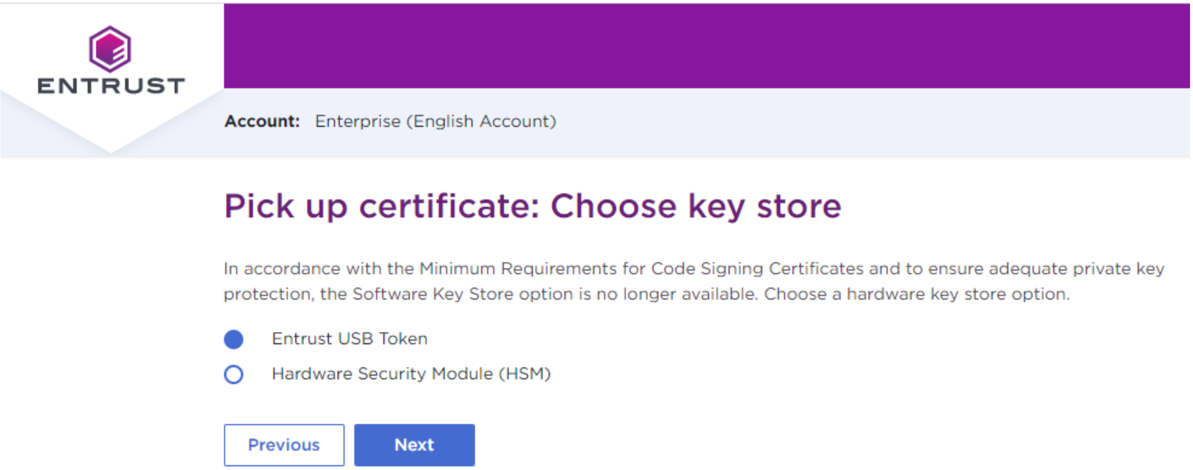
These general terms and conditions ("General Terms") are part of a legally binding agreement, which is confirmed or accepted when an Order (as defined in Section 1 below) is made or an "Accept" or similar button, and/or a check box presented with these General Terms (or a Schedule, defined below, incorporating 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**.

The *Choose key store* page appears.



Account: Enterprise (English Account)

Pick up certificate: Choose key store

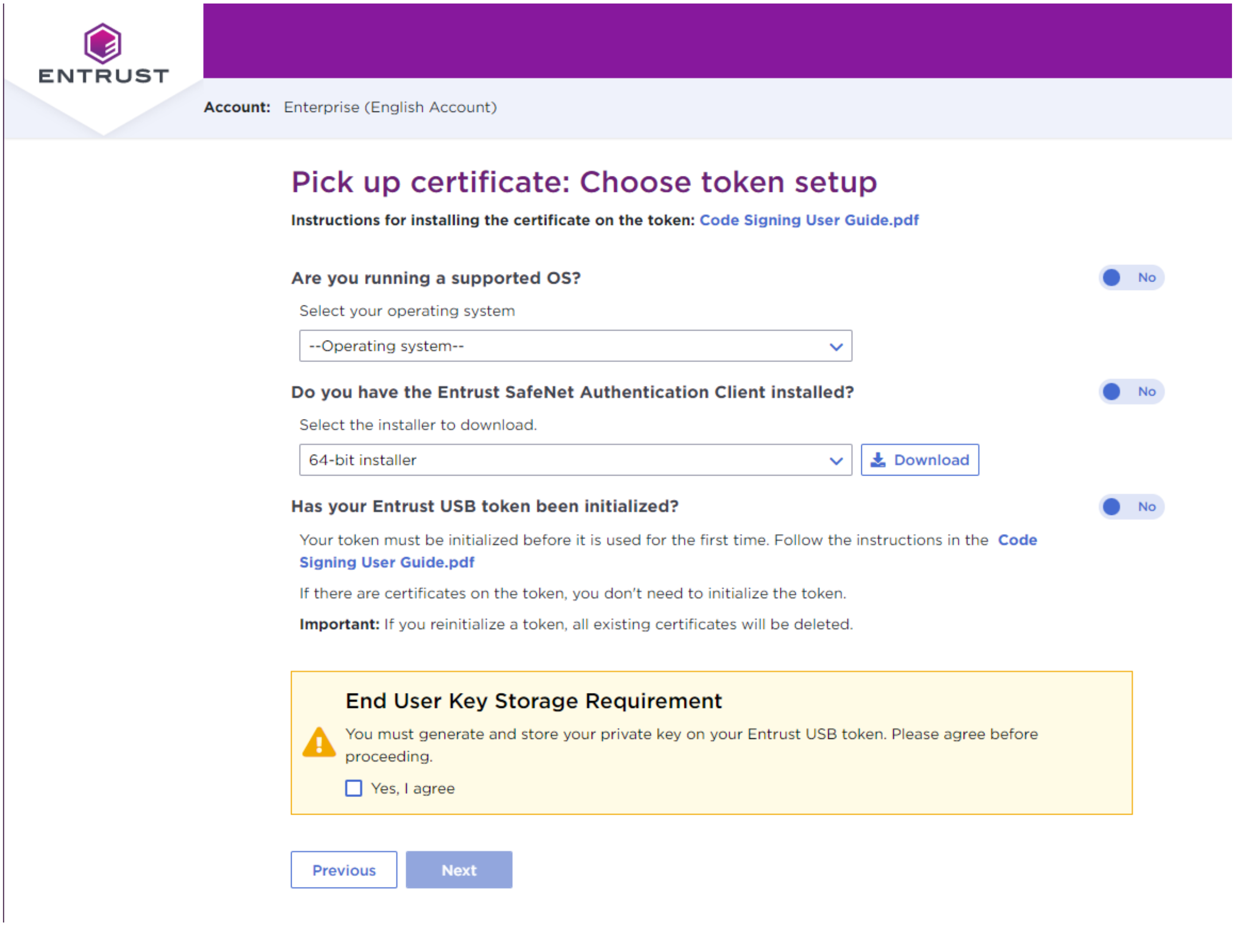
In accordance with the Minimum Requirements for Code Signing Certificates and to ensure adequate private key protection, the Software Key Store option is no longer available. Choose a hardware key store option.

● Entrust USB Token

○ Hardware Security Module (HSM)

5 Select **Entrust USB Token**, and click **Next**.

The *Choose token setup* screen appears.



Account: Enterprise (English Account)

Pick up certificate: Choose token setup

Instructions for installing the certificate on the token: Code Signing User Guide.pdf

Are you running a supported OS? No

Select your operating system

--Operating system--

Do you have the Entrust SafeNet Authentication Client installed? No

Select the installer to download.

64-bit installer

Download

Has your Entrust USB token been initialized? No

Your token must be initialized before it is used for the first time. Follow the instructions in the **Code 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.

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

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

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

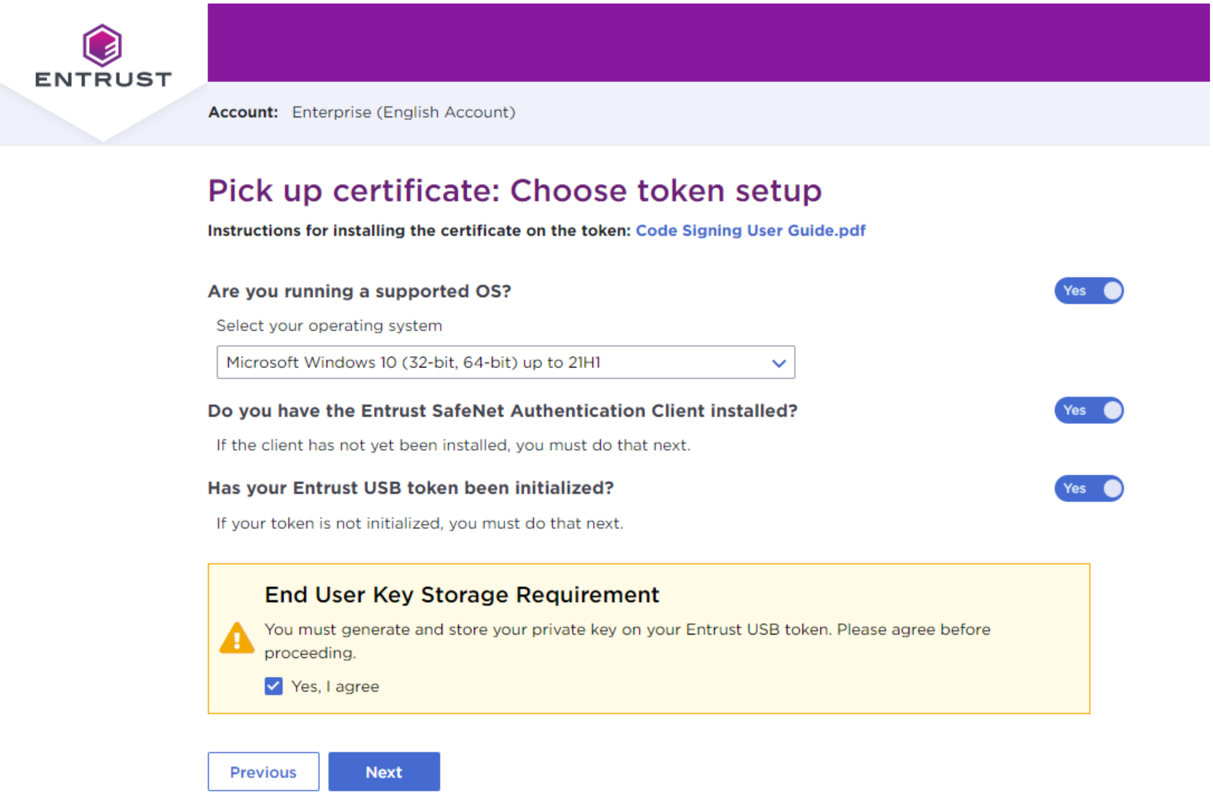
- If the SafeNet client is already installed, click to change the toggle to **Yes**, and continue with the next step.
- If the SafeNet client is not yet installed, follow the procedure in: "To obtain and install the token authentication client" on page 14. When the SafeNet software is installed, return to this browser page and this procedure to continue.

8 For **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 21. 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: Code 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.

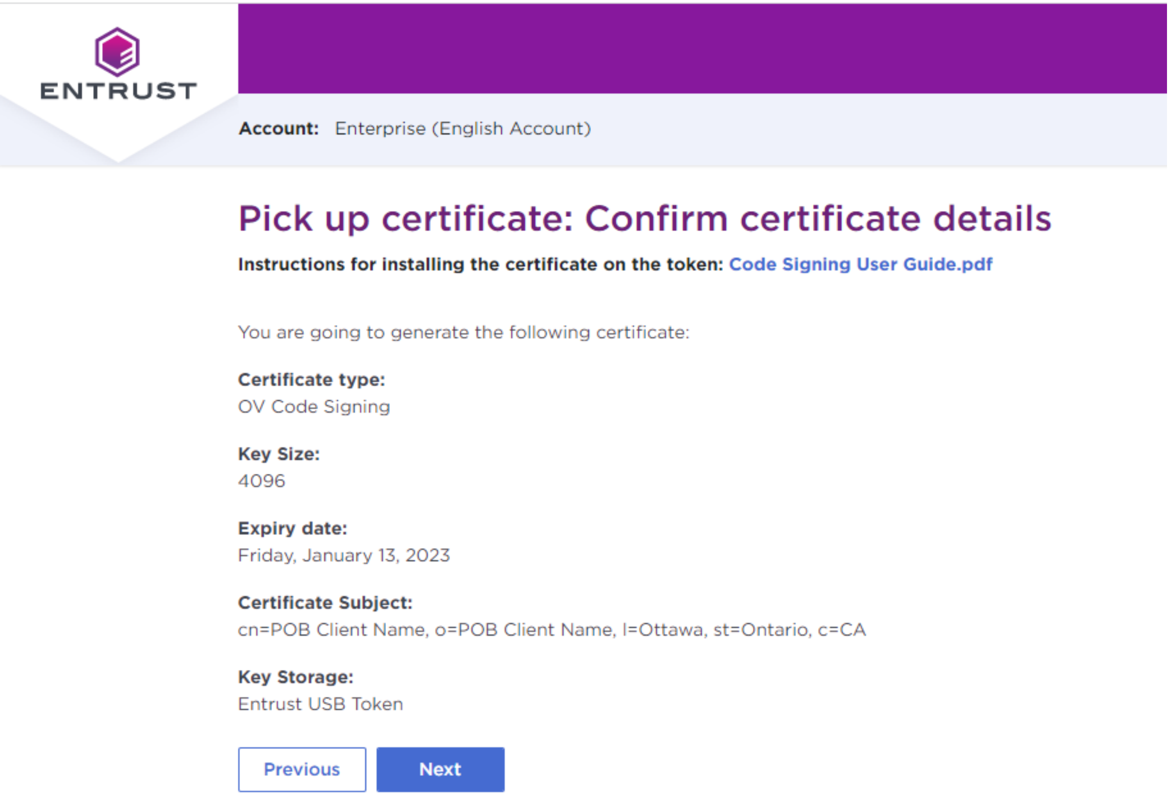
End User Key Storage Requirement

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

☑ Yes, I agree

10 Click **Next**.

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: Code Signing User Guide.pdf

You are going to generate the following certificate:

Certificate type:
OV Code Signing

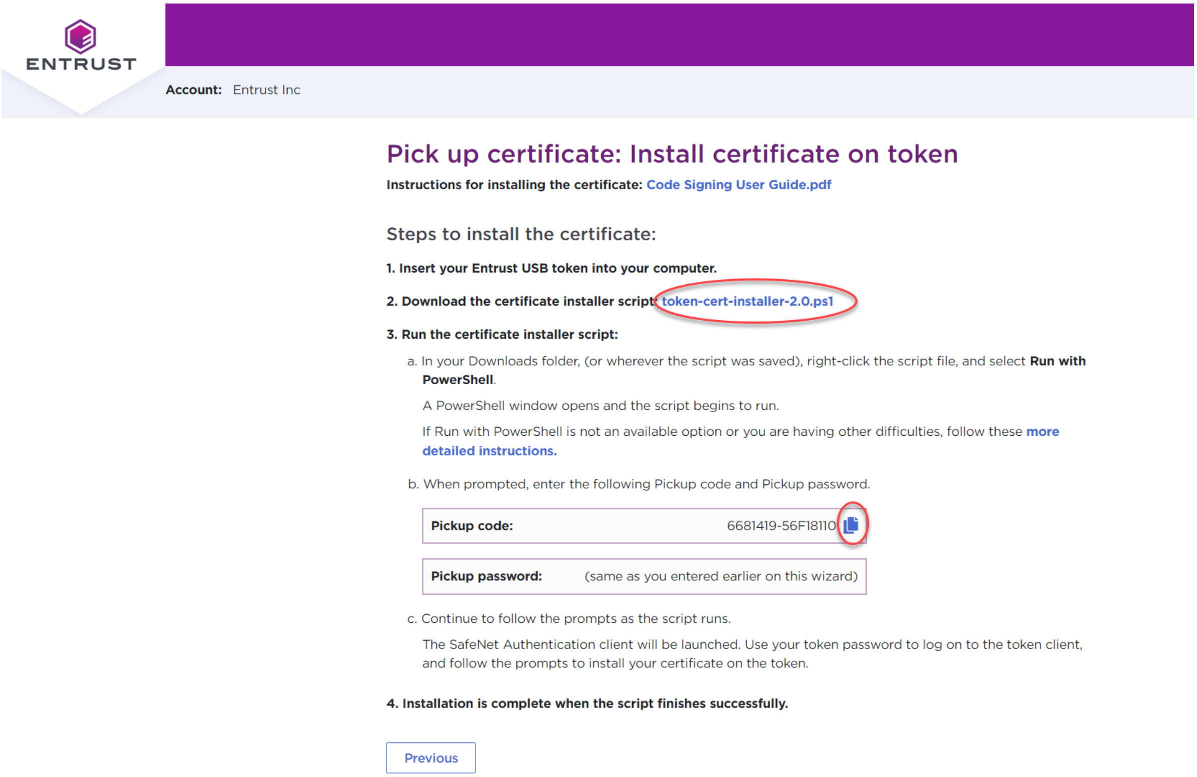
Key Size:
4096

Expiry date:
Friday, January 13, 2023

Certificate Subject:
cn=POB Client Name, o=POB Client Name, l=Ottawa, st=Ontario, c=CA

Key Storage:
Entrust USB Token

The *Install certificate on token* screen appears.



Account: Entrust Inc

Pick up certificate: Install certificate on token

Instructions for installing the certificate: Code 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-2.0.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:	6681419-56F18110
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.

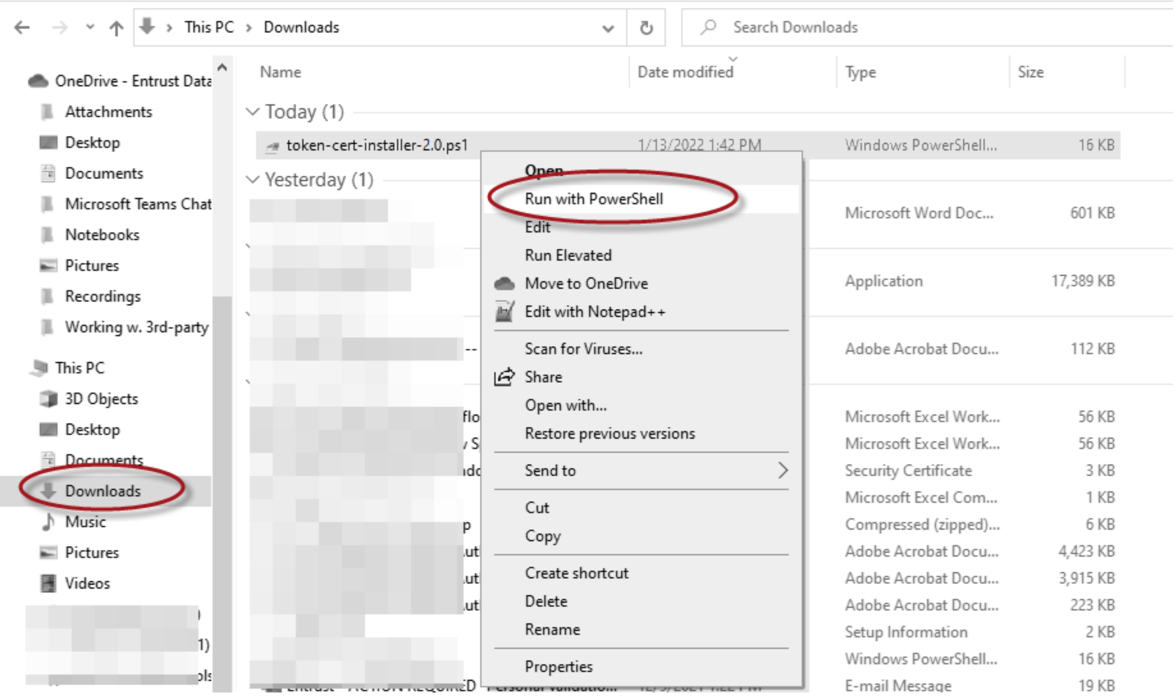
12 If necessary, insert your token into a USB port.

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.

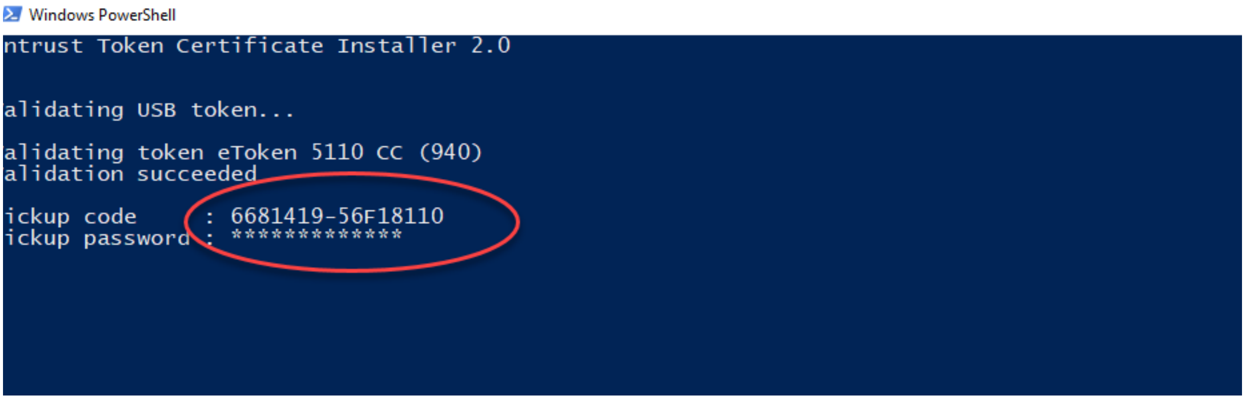
16 In your **Downloads** (or other) folder, locate and right-click the script, then select **Run with PowerShell**.



Name	Date modified	Type	Size
Today (1)			
token-cert-installer-2.0.ps1	1/13/2022 1:42 PM	Windows PowerShell...	16 KB
Yesterday (1)			
[redacted]		Microsoft Word Doc...	601 KB
[redacted]		Application	17,389 KB
[redacted]		Adobe Acrobat Docu...	112 KB
[redacted]		Microsoft Excel Work...	56 KB
[redacted]		Microsoft Excel Work...	56 KB
[redacted]		Security Certificate	3 KB
[redacted]		Microsoft Excel Com...	1 KB
[redacted]		Compressed (zipped)...	6 KB
[redacted]		Adobe Acrobat Docu...	4,423 KB
[redacted]		Adobe Acrobat Docu...	3,915 KB
[redacted]		Adobe Acrobat Docu...	223 KB
[redacted]		Setup Information	2 KB
[redacted]		Windows PowerShell...	16 KB
[redacted]		E-mail Message	19 KB

Note:
If, under Windows 11, you see the PowerShell window open briefly, then close, the issue likely is caused by the fact that Windows 11 by default turns off the execution policy that enables PowerShell scripts to run. Consult with your IT department to determine your best path forward. For more details, see "Appendix: Microsoft PowerShell" on page 59.

17 The PowerShell window 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.



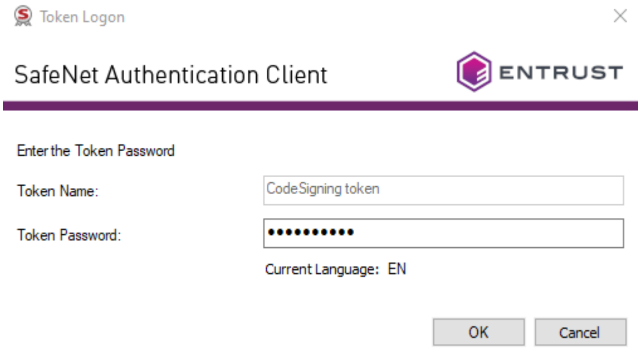
```
ntrust Token Certificate Installer 2.0

alidating USB token...

alidating token eToken 5110 CC (940)
alidation succeeded

ickup code     : 6681419-56F18110
ickup 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** key.

The SafeNet client is started.



Enter the Token Password

Token Name: CodeSigning token

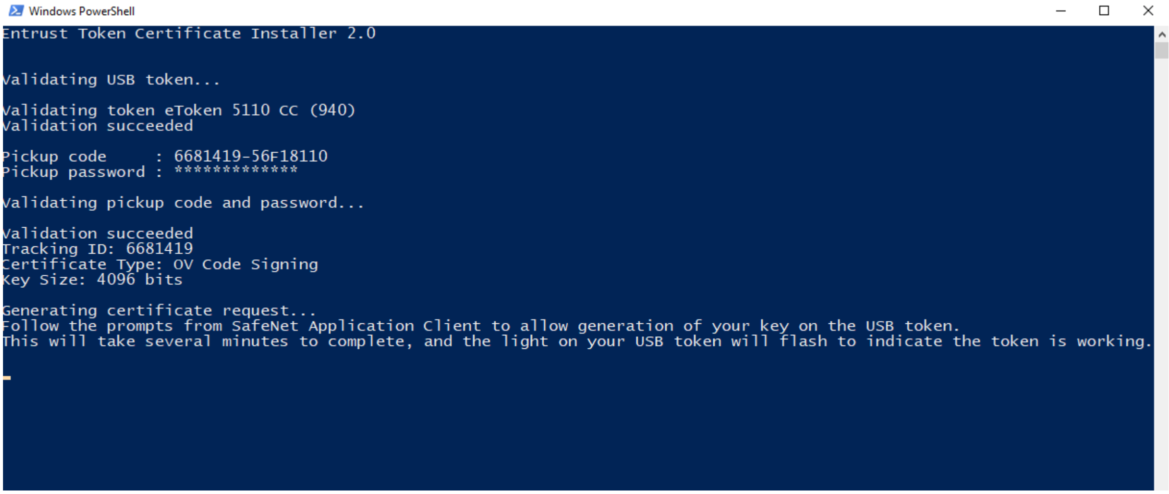
Token Password: ●●●●●●●●●●●

Current Language: EN

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

22 Click **OK**.

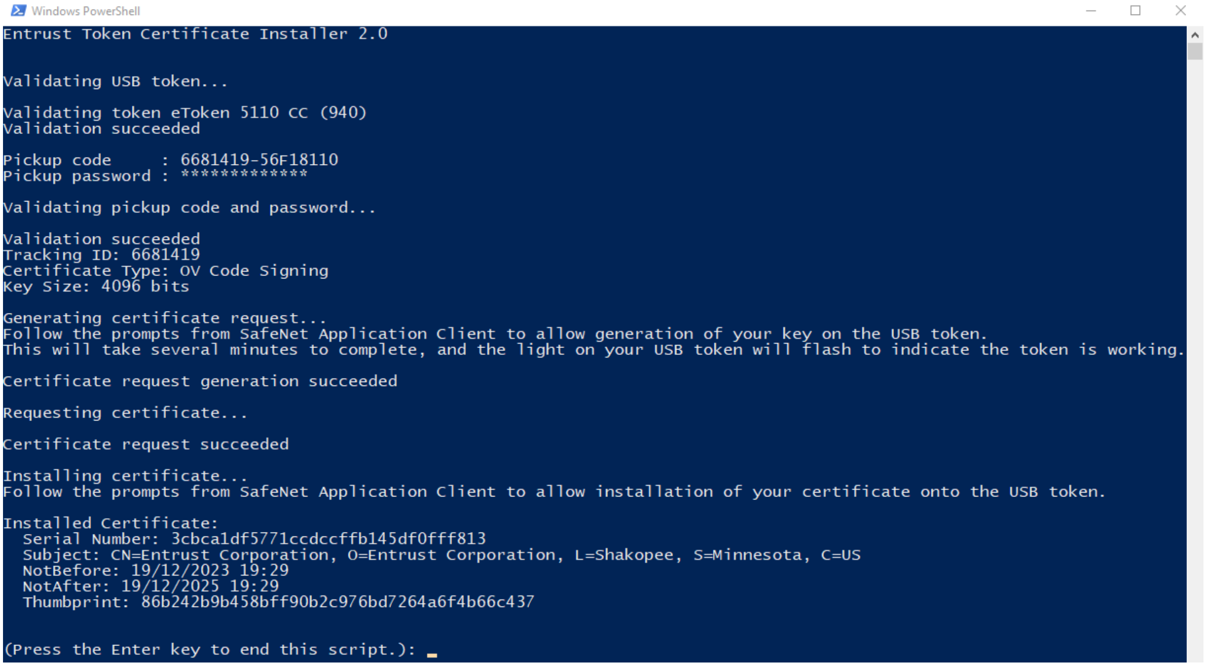
23 The PowerShell installation script continues to run.



```
Entrust Token Certificate Installer 2.0


Validating USB token...

Validating token eToken 5110 CC (940)
Validation succeeded

Pickup code     : 6681419-56F18110
Pickup password : *************

Validating pickup code and password...

Validation succeeded
Tracking ID: 6681419
Certificate Type: OV Code Signing
Key Size: 4096 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 light flashing through most of the process.

When this is done, the screen will display additional information:



```
Entrust Token Certificate Installer 2.0


Validating USB token...

Validating token eToken 5110 CC (940)
Validation succeeded

Pickup code     : 6681419-56F18110
Pickup password : *************

Validating pickup code and password...

Validation succeeded
Tracking ID: 6681419
Certificate Type: OV Code Signing
Key Size: 4096 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.

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.

Installed Certificate:
  Serial Number: 3cbca1df5771ccdccffb145df0fff813
  Subject: CN=Entrust Corporation, O=Entrust Corporation, L=Shakopee, S=Minnesota, C=US
  NotBefore: 19/12/2023 19:29
  NotAfter: 19/12/2025 19:29
  Thumbprint: 86b242b9b458bff90b2c976bd7264a6f4b66c437


(Press the Enter key to end this script.): _
```

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 only with the Microsoft Internet Explorer or Microsoft Edge browser.

Note:
Once Microsoft ends its support for Internet Explorer, this procedure will be deprecated.

To use Microsoft Edge to install the certificate, you must use Edge’s Microsoft Internet Explorer mode.

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

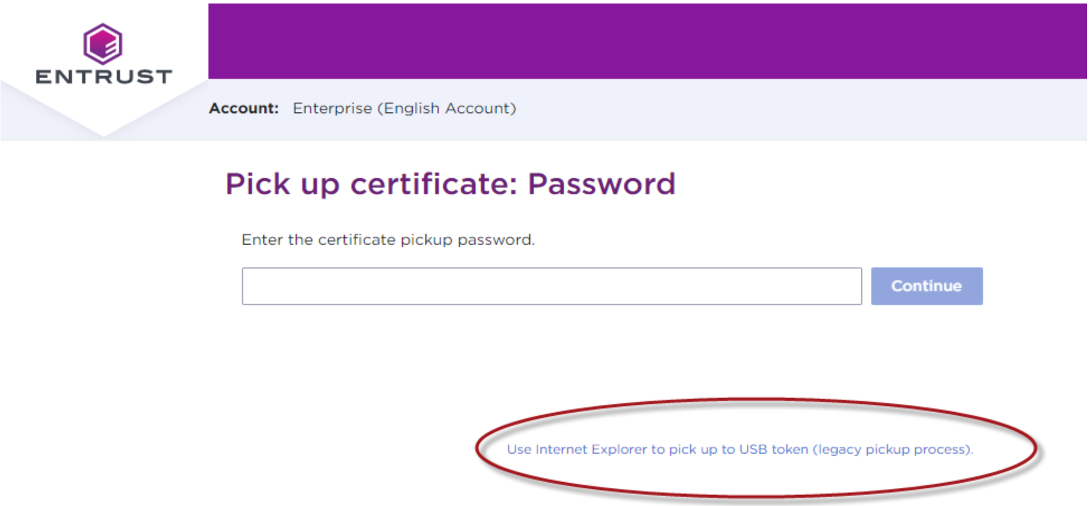
1. Open Microsoft Edge. In the upper right corner, click the three dots to open the menu.
2. Click **Settings**.
3. Click **Default browser**.
4. From *Allow Sites to be reloaded in Internet Explorer mode (IE mode),* select **Allow**.
5. From *Internet Explorer mode pages*, click **Add.**
6. Copy and 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 a hardware token using Microsoft Internet Explorer or Microsoft Edge

1. Insert your token into a USB port.

2 From Entrust’s notification email, click the link provided and 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.



Account: Enterprise (English Account)

Pick up certificate: Password

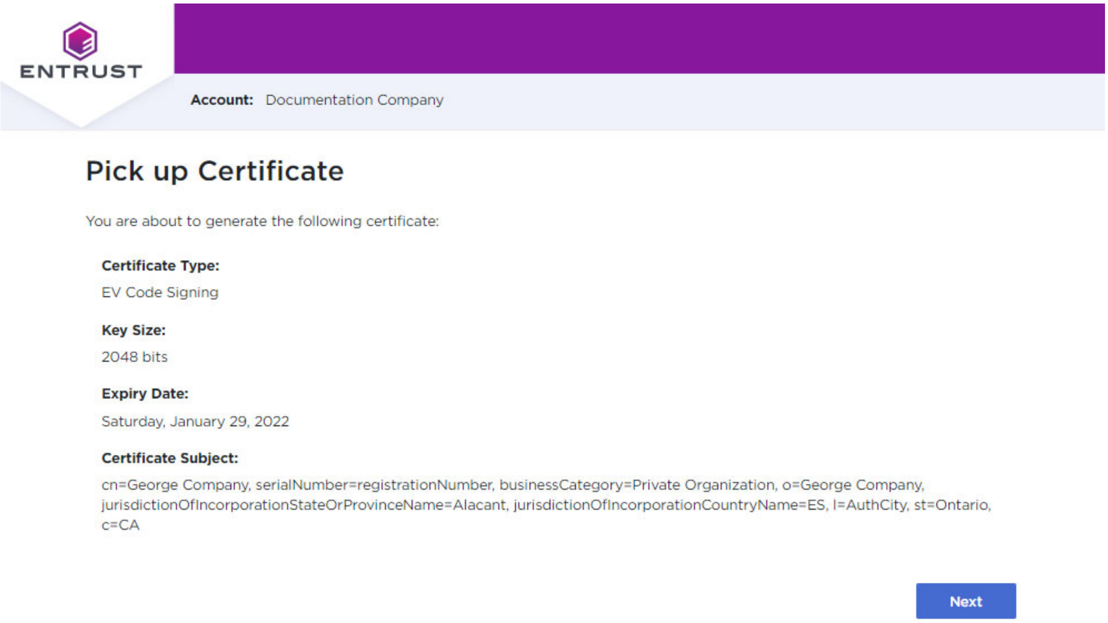
Enter the certificate pickup password.

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 Review your certificate information.



ENTRUST

Account: Documentation Company

Pick up Certificate

You are about to generate the following certificate:

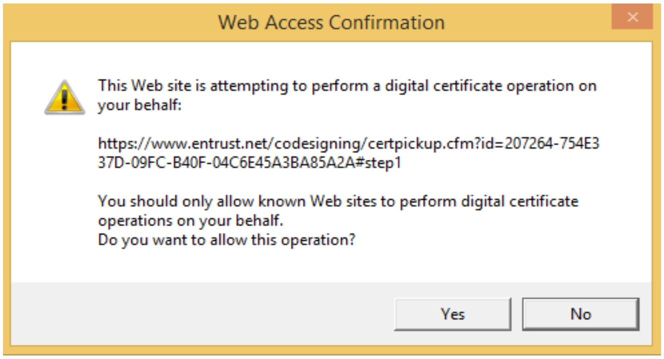
Certificate Type:
EV Code Signing

Key Size:
2048 bits

Expiry Date:
Saturday, January 29, 2022

Certificate Subject:
cn=George Company, serialNumber=registrationNumber, businessCategory=Private Organization, o=George Company, jurisdictionOfIncorporationStateOrProvinceName=Alacant, jurisdictionOfIncorporationCountryName=ES, l=AuthCity, st=Ontario, c=CA

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



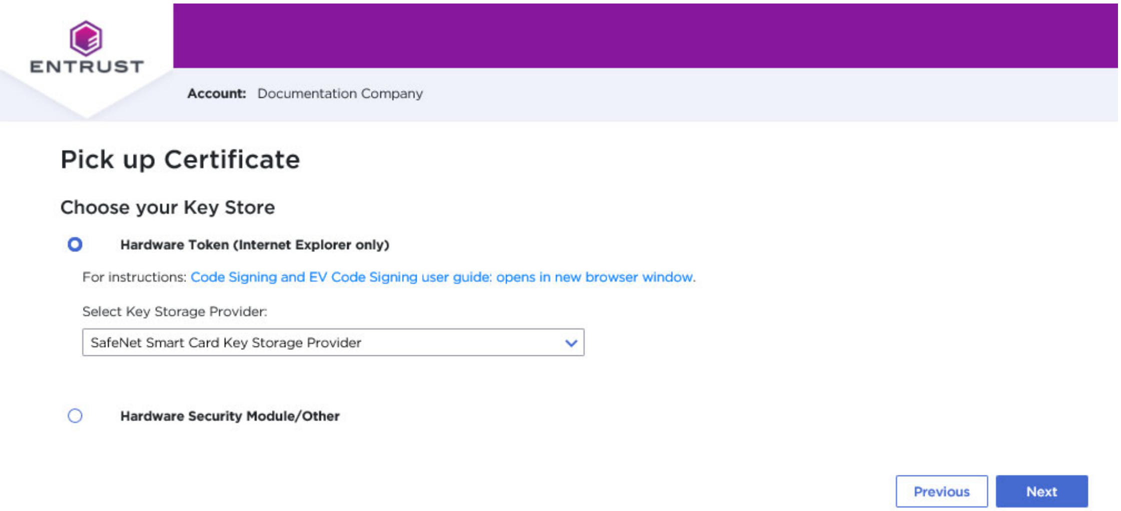
Web Access Confirmation

This Web site is attempting to perform a digital certificate operation on your behalf:

https://www.entrust.net/codesigning/certpickup.cfm?id=207264-754E3
37D-09FC-B40F-04C6E45A3BA85A2A#step1

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

7 On the screen that appears, select **Hardware Token**. Click **Next**.



Account: Documentation Company

Pick up Certificate

Choose your Key Store

● Hardware Token (Internet Explorer only)

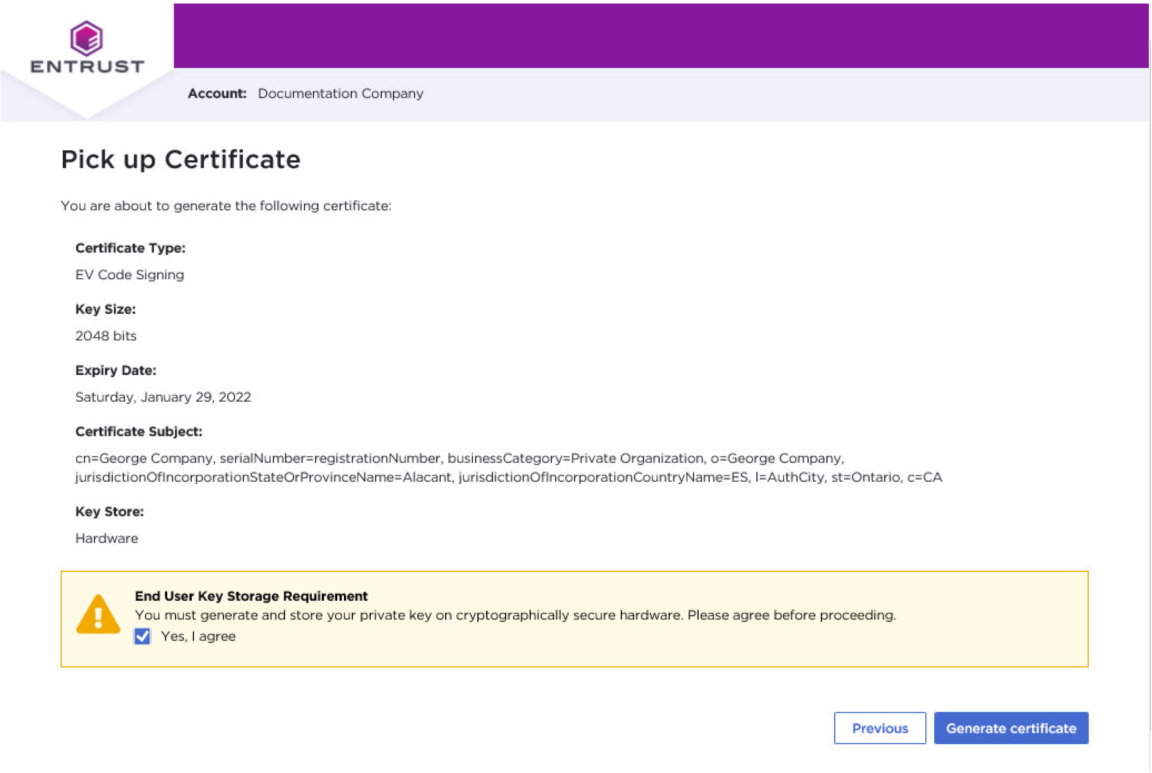
For instructions: Code Signing and EV Code Signing user guide: opens in new browser window.

Select Key Storage Provider:

SafeNet Smart Card Key Storage Provider

○ Hardware Security Module/Other

The *Pick up Certificate* page appears.



ENTRUST

Account: Documentation Company

Pick up Certificate

You are about to generate the following certificate:

Certificate Type:
EV Code Signing

Key Size:
2048 bits

Expiry Date:
Saturday, January 29, 2022

Certificate Subject:
cn=George Company, serialNumber=registrationNumber, businessCategory=Private Organization, o=George Company, jurisdictionOfIncorporationStateOrProvinceName=Alacant, jurisdictionOfIncorporationCountryName=ES, l=AuthCity, st=Ontario, c=CA

Key Store:
Hardware

End User Key Storage Requirement
You must generate and store your private key on cryptographically secure hardware. Please agree before proceeding.
☑ Yes, I agree

8 Click **Yes, I agree** to confirm that you are aware of the storage requirement (hardware-only) for Code Signing certificates.

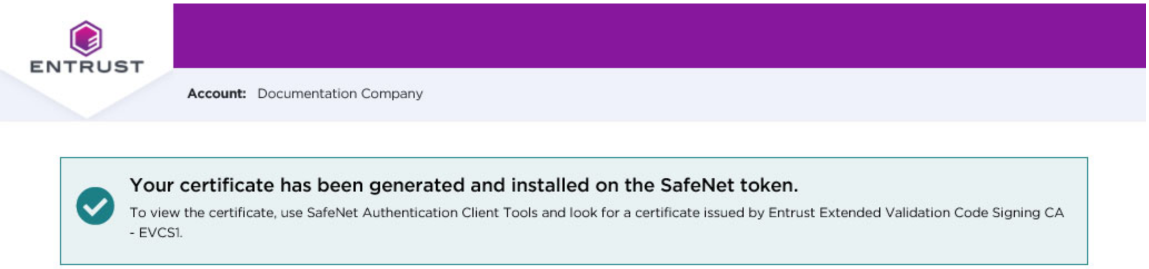
9 Click **Generate Certificate**.

10 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 website.

The website generates the certificate on your token. This will take a few minutes.

When the certificate has been created, you will see a success message.



Account: Documentation Company

Your certificate has been generated and installed on the SafeNet token.

To view the certificate, use SafeNet Authentication Client Tools and look for a certificate issued by Entrust Extended Validation Code Signing CA - EVCS1.

Changing the password for your token

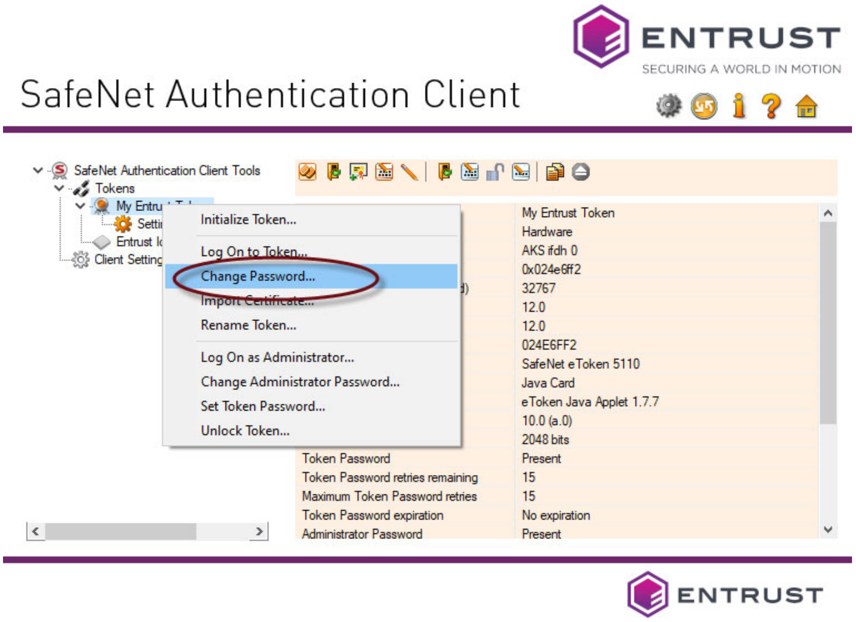
To change the password for your token

1 Insert your token into a USB slot on your PC.

2 Right-click the SafeNet icon in the Desktop tray and select **Tools**.

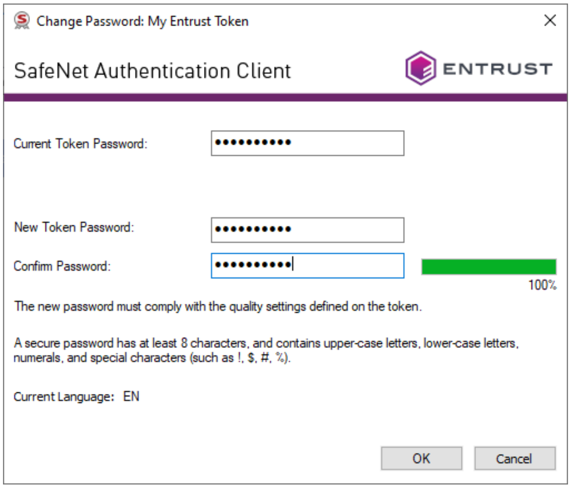
3 Click the Advanced View (gear) icon.

4 Right-click the entry for your token, and select **Change Password.**



	My Entrust Token
	Hardware
	AKS ifdh 0
	0x024e6ff2
d)	32767
	12.0
	12.0
	024E6FF2
	SafeNet eToken 5110
	Java Card
	eToken Java Applet 1.7.7
	10.0 (a.0)
	2048 bits
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration
Administrator Password	Present

5 Enter your current password and the new password, then 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

Current Token Password: ••••••••••

New Token Password: ••••••••••

Confirm Password: ••••••••••

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

6 Click **OK**.

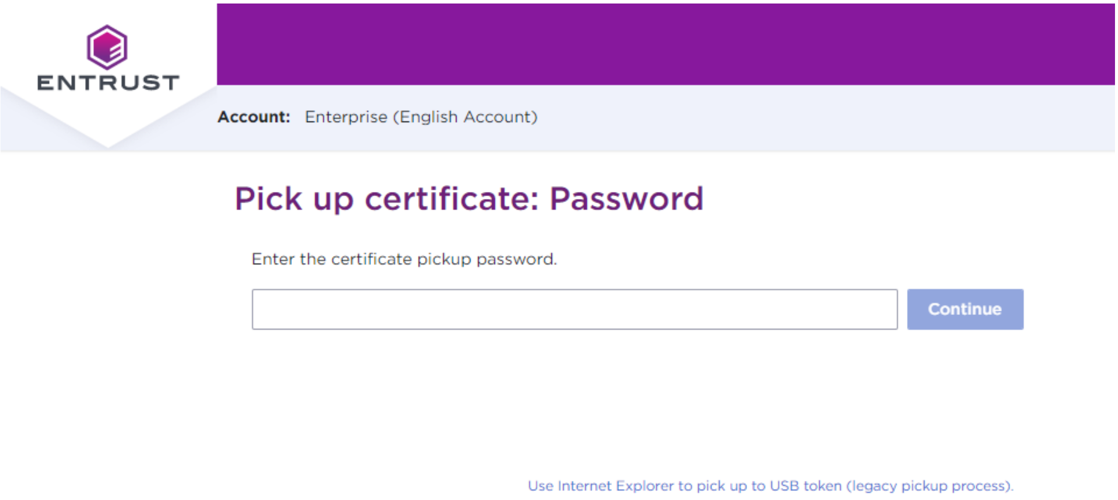
Installing the certificate to a Hardware Security Module (HSM)

Use this procedure to download your Code Signing certificate to an HSM. This procedure does not require the SafeNet Authentication Client, and can be run on any supported browser.

To install the certificate to a Hardware Security Module (HSM)

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.



Account: Enterprise (English Account)

Pick up certificate: Password

Enter the certificate pickup password.

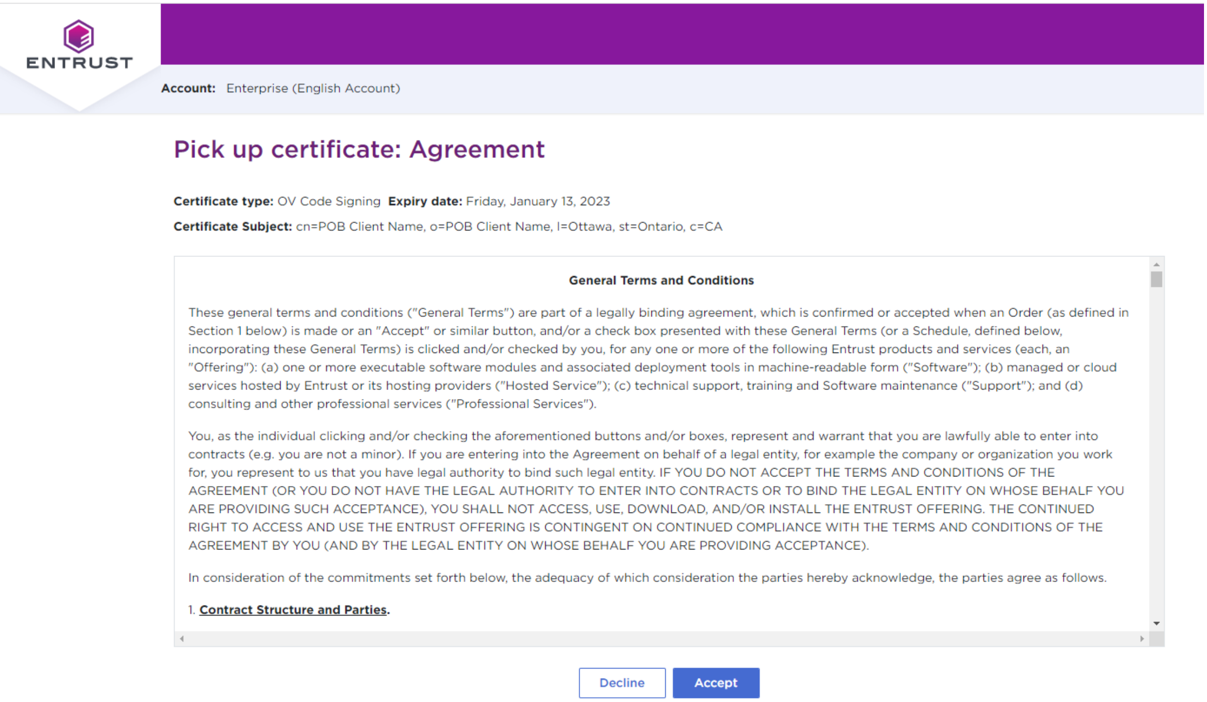
ENTRUST
Continue
Use Internet Explorer to pick up to USB token (legacy pickup process).

2 Enter the password that you entered when you created the certificate request or get it from your Certificate Administrator.

3 Click **Continue**.

4 You may see a warning that the browser is attempting to perform a certificate operation on your behalf. Allow the operation.

The *Agreement* screen appears.



Account: Enterprise (English Account)

Pick up certificate: Agreement

Certificate type: OV Code Signing **Expiry date:** Friday, January 13, 2023

Certificate Subject: cn=POB Client Name, o=POB Client Name, l=Ottawa, st=Ontario, c=CA

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).

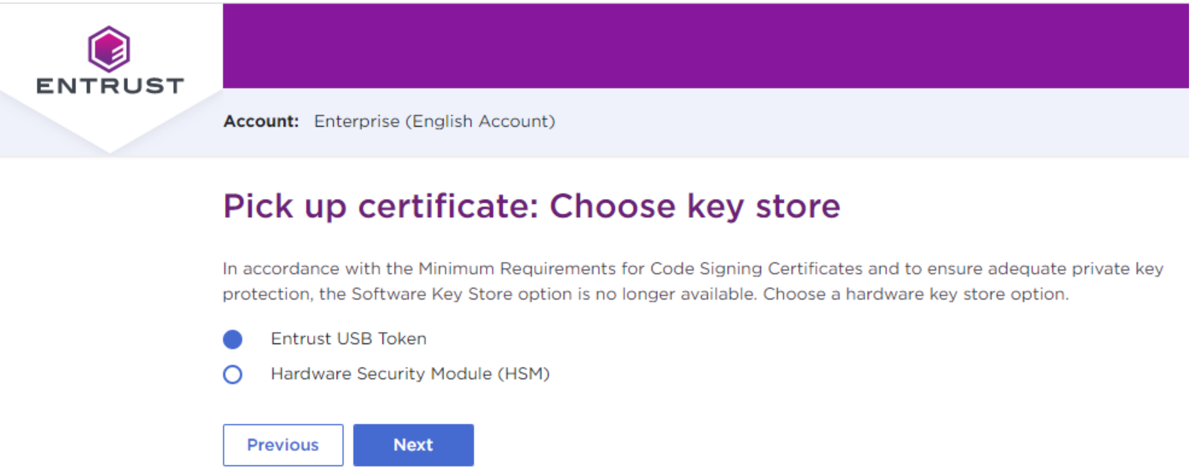
In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Contract Structure and Parties**.

5 Read and accept the Entrust Certificate Services Agreement.

6 Click **Accept**.

The *Choose key store* page appears.



Account: Enterprise (English Account)

Pick up certificate: Choose key store

In accordance with the Minimum Requirements for Code Signing Certificates and to ensure adequate private key protection, the Software Key Store option is no longer available. Choose a hardware key store option.

● Entrust USB Token

○ Hardware Security Module (HSM)

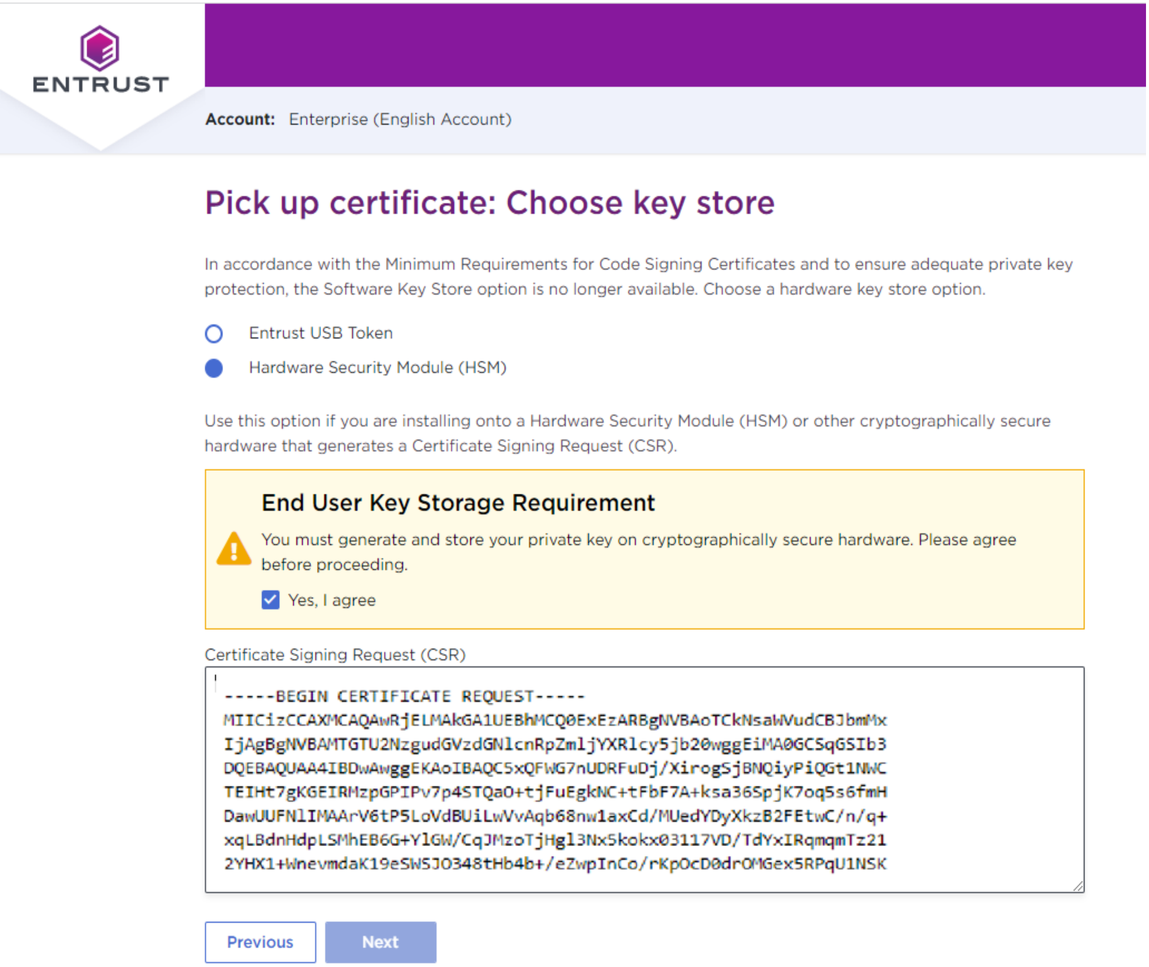
7 If the option for **Hardware Security Module (HSM)** is disabled, you must log in to Enterprise Certificate Services to complete the requirement for the use of HSM:

   a Select **Administration** > **Client Management** and click the row containing the relevant client.

   b Selected the **Extended Validation** tab. In the section Code Signing Verification, select **Enable and Select a representative**.

8 Select **Hardware Security Module (HSM)**.

9 Click **Next**.



Account: Enterprise (English Account)

Pick up certificate: Choose key store

In accordance with the Minimum Requirements for Code Signing Certificates and to ensure adequate private key protection, the Software Key Store option is no longer available. Choose a hardware key store option.

○ Entrust USB Token

● Hardware Security Module (HSM)

Use this option if you are installing onto a Hardware Security Module (HSM) or other cryptographically secure hardware that generates a Certificate Signing Request (CSR).

End User Key Storage Requirement

You must generate and store your private key on cryptographically secure hardware. Please agree before proceeding.

☑ Yes, I agree

Certificate Signing Request (CSR)

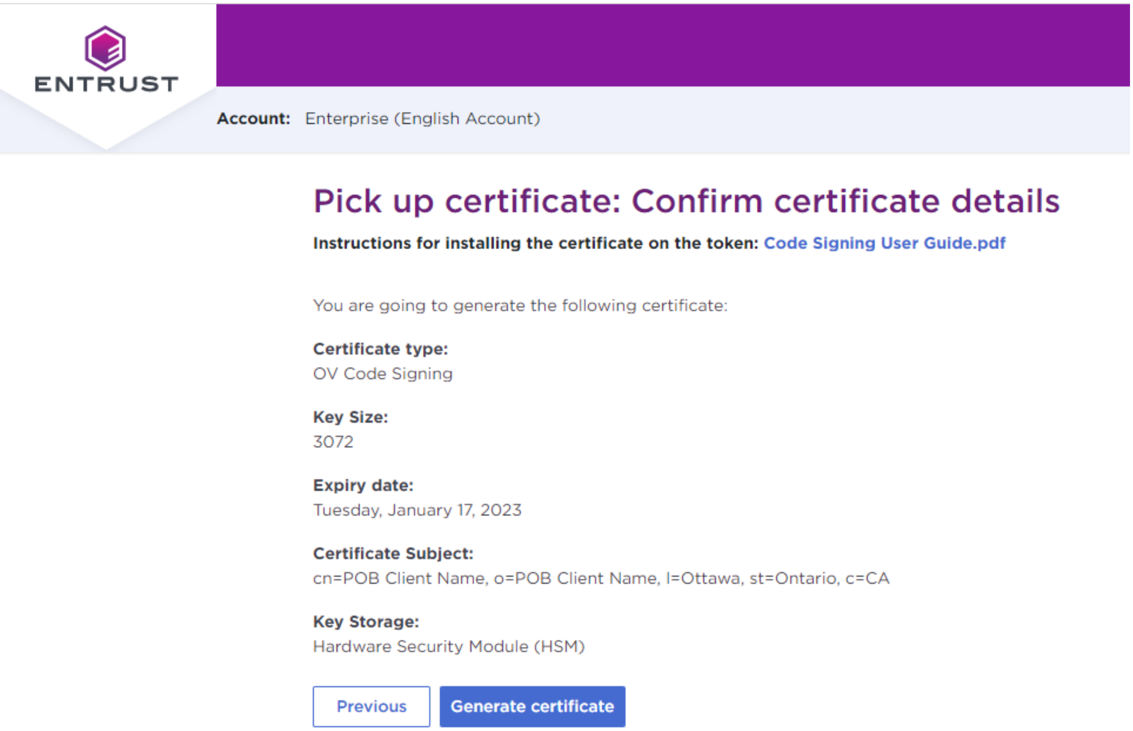
```
-----BEGIN CERTIFICATE REQUEST-----
MIICizCCAXMCAQAwRjELMAkGA1UEBhMCQ0ExEzARBgNVBAoTCkNsaWVudCBJbmMx
IjAgBgNVBAMTGTU2NzgudGVzdGNlcnRpZmljYXRlcy5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC5xQFWG7nUDRFuDj/XirogSjBNQiyPiQGt1NWC
TEIHt7gKGEIRMzpGPIPv7p4STQaO+tjFuEgkNC+tFbF7A+ksa36SpjK7oq5s6fmH
DawUUFNlIMAArV6tP5LoVdBUiLwVvAqb68nw1axCd/MUedYDyXkzB2FEtwC/n/q+
xqLBdnHdpLSMhEB6G+YlGW/CqJMzoTjHgl3Nx5kokx03117VD/TdYxIRqmqmTz21
2YHX1+WnevmdaK19eSW5JO348tHb4b+/eZwpInCo/rKpOcD0drOMGex5RPqU1NSK
```

10 Confirm that you will store the private key on the secure hardware by selecting **Yes, I agree**.

11 Paste in the CSR you generated on your HSM.

12 Click **Next**.

The *Confirm certificate details* screen appears.



ENTRUST

Account: Enterprise (English Account)

Pick up certificate: Confirm certificate details

Instructions for installing the certificate on the token: Code Signing User Guide.pdf

You are going to generate the following certificate:

Certificate type:
OV Code Signing

Key Size:
3072

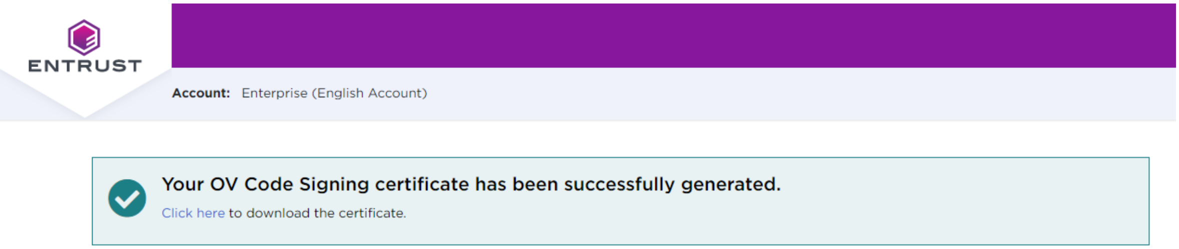
Expiry date:
Tuesday, January 17, 2023

Certificate Subject:
cn=POB Client Name, o=POB Client Name, l=Ottawa, st=Ontario, c=CA

Key Storage:
Hardware Security Module (HSM)

13 Check the certificate details, and click **Generate certificate**.

14 The *Success* screen appears.



ENTRUST

Account: Enterprise (English Account)

Your OV Code Signing certificate has been successfully generated.

Click here to download the certificate.

You can now install your certificate on your HSM.

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 without additional cost. 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, a Certificate Services Support Agent can help you to have the password reset.

Note:
The Token Utility cannot recover the certificate.

Downloading the certificate to Azure Key Vault or AWS CloudHSM

Entrust also offers the option of storing the certificate on Azure Key Vault or AWS CloudHSM. More information about this option is available from this link.

A

Appendix: Microsoft PowerShell

This appendix includes the following sections:

- "Running PowerShell" starting on page 60

Running PowerShell

Windows 11 differs from Windows 10 in its approach to PowerShell scripts. Windows 11 by default turns off the execution policy that enables PowerShell scripts to run. The issue *cannot* be addressed by making changes to the Entrust PowerShell script.

Whatever rules your company or organization enforces, your IT department must address this issue before you can install tokens.

Note:
We strongly recommend that you engage your IT department to resolve this issue by consulting official PowerShell documents written by Microsoft, for example:

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.4

Attention:
Entrust strongly recommends that you consult with your IT department before proceeding any further.

Running a specific PowerShell script to bypass execution policy

This procedure involves opening a PowerShell window and running the script from there. This is *different* from this guide's recommendation to locate the script and right-click the script to select "Run with PowerShell." The procedure requires that your account has administrator privileges

To run a script with a bypass

1. On the keyboard, press the Windows key + R, then type "powershell".
2. In the PowerShell window, navigate to the directory that contains the script.
3. To run the script with a bypass, enter the following command:

   ```
   ./script-name.ps1 -executionpolicy bypass
   ```

   Replace "script-name.ps1" with the name of the script you intend to run, such as "token-cert-installer-2.0.ps1".

Running all power PowerShell scripts as an administrator

The execution policy for your Windows account must be set to **`RemoteSigned`** or **`Unrestricted`**—preferably to **`RemoteSigned`**. The procedure requires that your account has administrator privileges.

To change the execution policy

1. In the Windows taskbar, in the search box (to the right of the Windows icon), type "PowerShell."
2. Right-click the search result **Windows PowerShell**, then select **Run as administrator**.
3. In the dialog box, if prompted, answer Yes to allow and, if prompted, enter your administrator credentials.
4. In the PowerShell window, enter the following command:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

5. At the prompt, type **Y** and press **Enter**.