Certificate Services
OV and EV Code 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

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 4
- "Before you start" on page 5
- "Downloading and installing the token software (required for USB token pickup)" on page 6
- "Initializing an Entrust USB token" on page 13
- "Picking up your Entrust certificate" on page 21

  There are three pickup methods:

  – "Install the certificate to Entrust USB token using PowerShell script" on page 22

  – "Install certificate to an Entrust USB token using Microsoft Internet Explorer" on page 32

  – "Install the certificate to a Hardware Security Module (HSM)" on page 37
- "Changing the password for your token" on page 43
- "Recovering a certificate" on page 45

Supported platforms

The following platforms and browsers are supported.

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

The following browsers are supported:

- Microsoft Internet Explorer 11 or higher
- Mozilla Firefox 37 or higher
- Chrome 45 or higher
- Safari 5 or higher

Important changes

Entrust has updated our Code Signing Certificate hierarchies and implemented the changes to enforce a minimum key size of 3072-bit RSA keys. These changes support the new CAB Forum guideline taking effect on 1st June 2021.

An upgraded token is required in the following scenarios:

- Where code signing inventory was ordered before the 18th January 2021 and is still unused as of 26th May 2021.
- Where an active code signing certificate is going to be renewed.
- Where an active code signing certificate is going to be reissued.

Please contact your Entrust sales representative or Entrust partner to discuss how you can upgrade your token(s).

In addition to enforcing the new minimum key sizes, a new Time Stamp Authority (TSA), which is compliant with the new CAB Forum Code Signing guidelines, been established at http://timestamp.entrust.net/rfc3161ts2. Customers performing Code Signing operations should update their configuration to begin using this new TSA.

Before you start

To download an Entrust certificate, you need:

- a supported browser with Internet access
- a supported operating system
- an iKey 5110 CC token (provided by Entrust) or a Hardware Security Module (HSM)
- if using an HSM, you need a certificate signing request (CSR) from the HSM.

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

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.

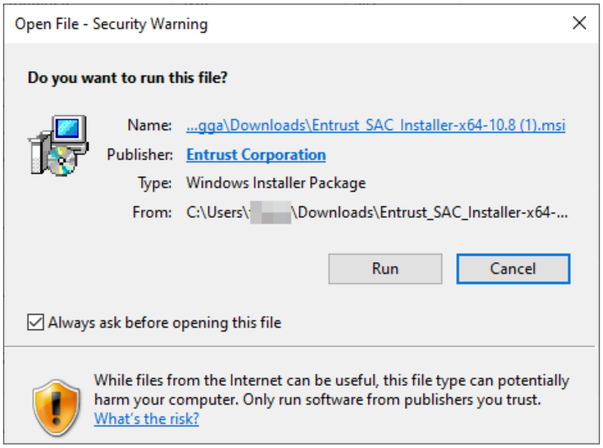
Attention:
Do not plug your token into your computer until you have completed this procedure.

Note:
For installing to HSM: This procedure is not needed. Proceed to: "Install the certificate to a Hardware Security Module (HSM)" on page 37

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

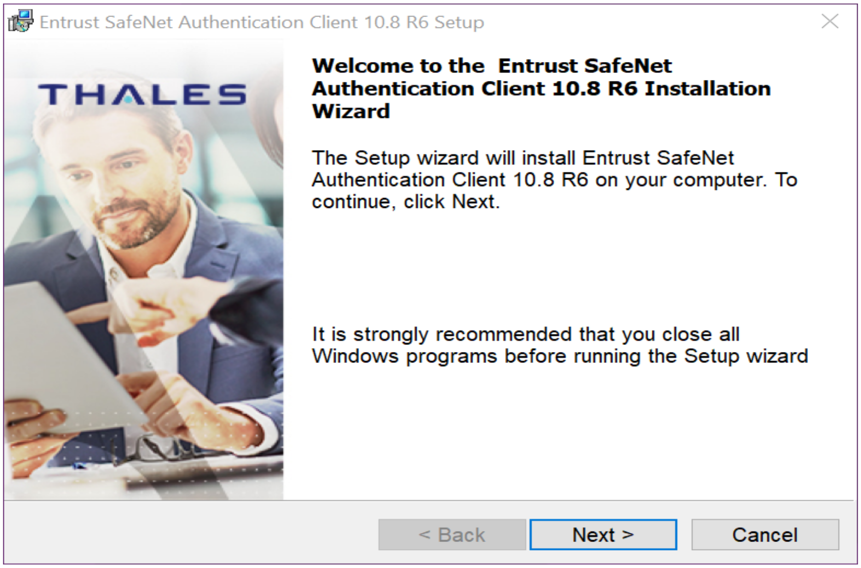
Type: Windows Installer Package

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

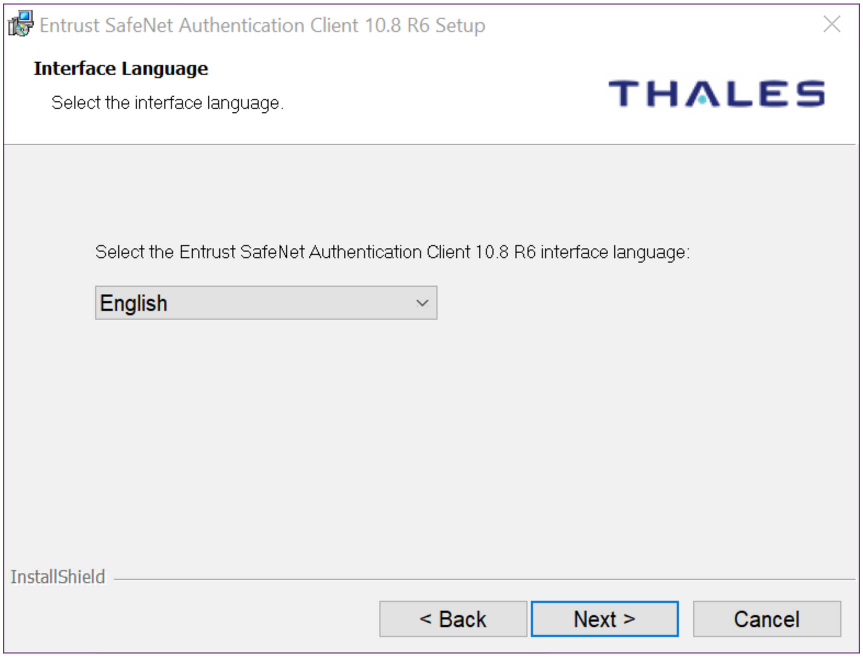
Welcome to the Entrust SafeNet Authentication Client 10.8 R6 Installation Wizard

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.

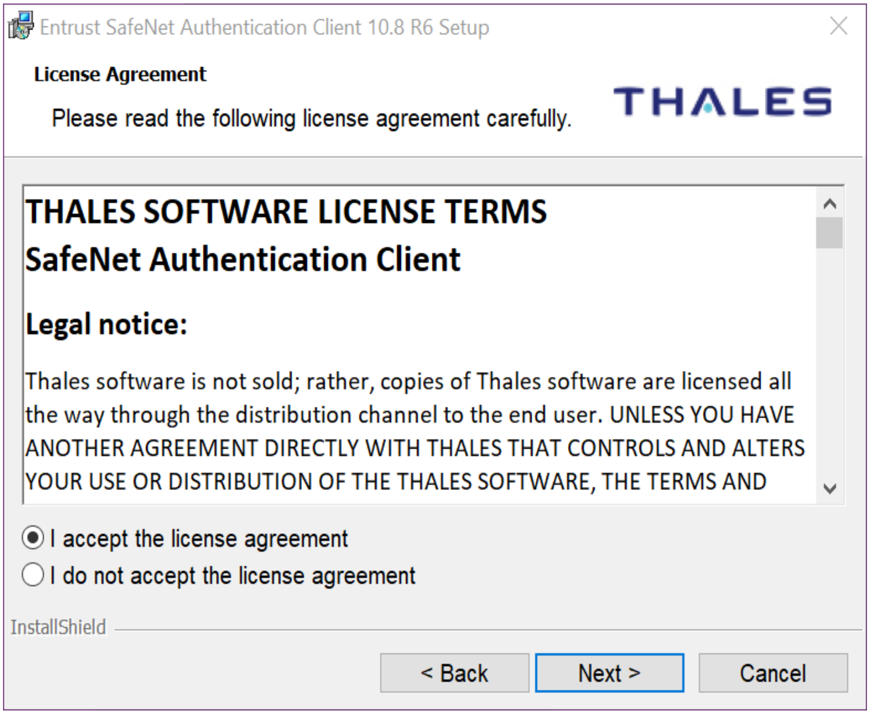
Select the Entrust SafeNet Authentication Client 10.8 R6 interface language:

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

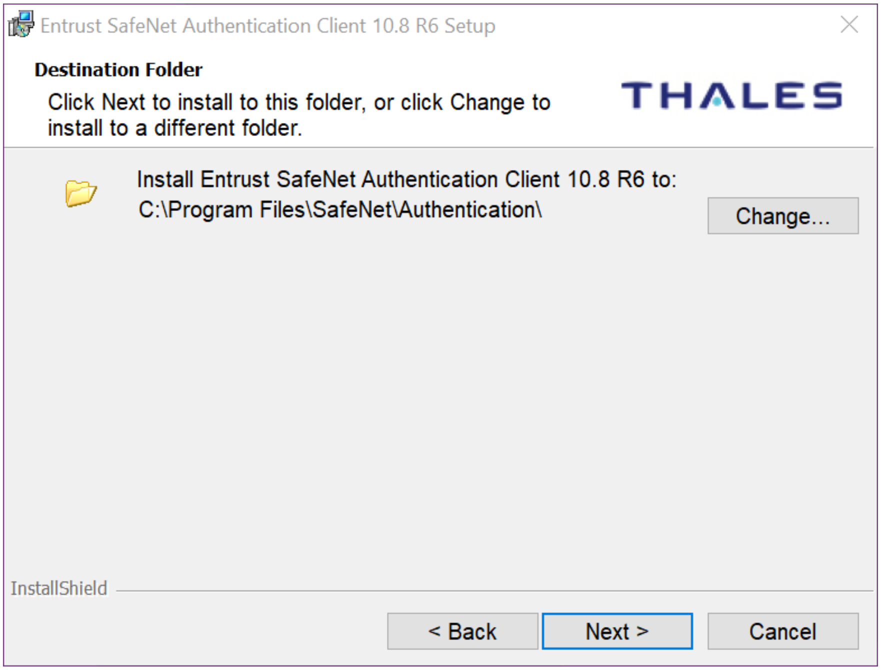
● I accept the license agreement

○ 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\

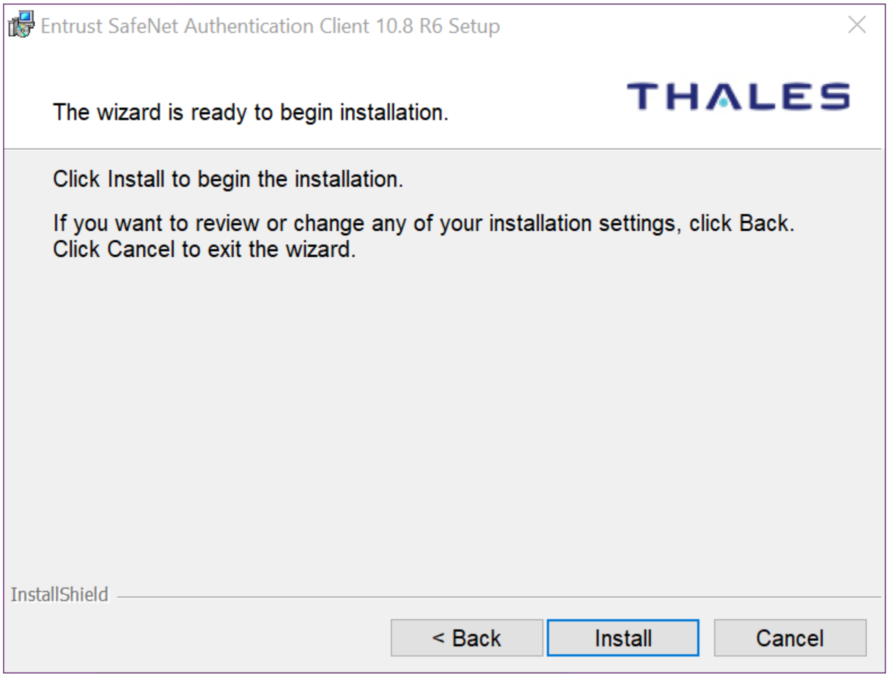
9 Accept the default folder or click **Change** to choose a new folder.

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

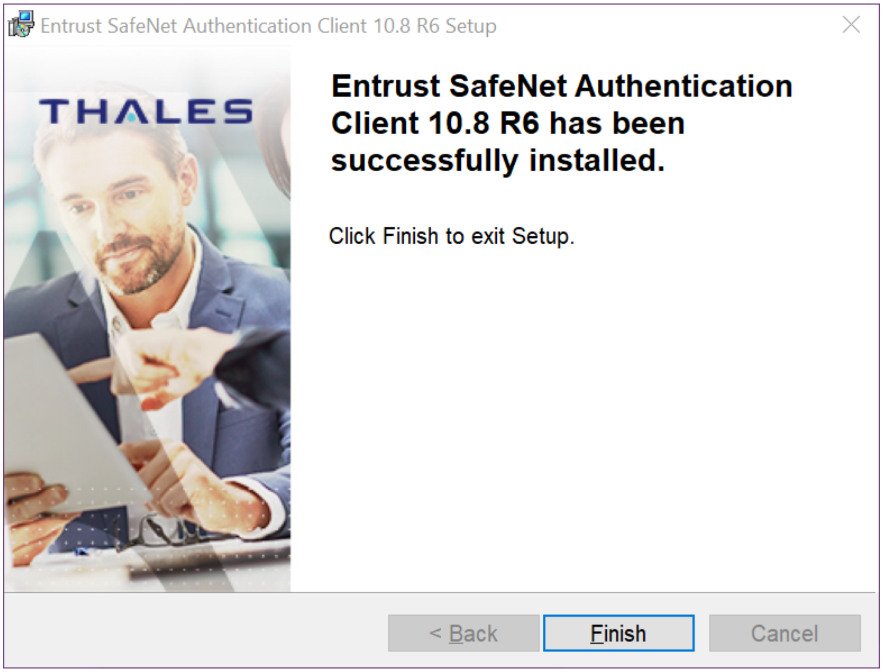
The wizard is ready to begin installation.

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

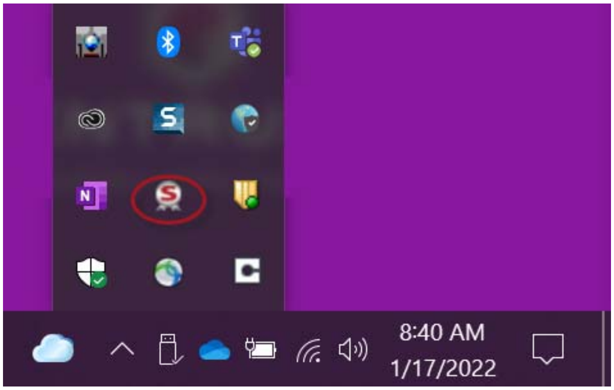
Initialize the new token so it can store your certificate. If your token is already initialized, skip to: "Picking up your Entrust certificate" on page 21.

Attention:
If this is not a new token, initializing the token deletes all certificates stored on it.

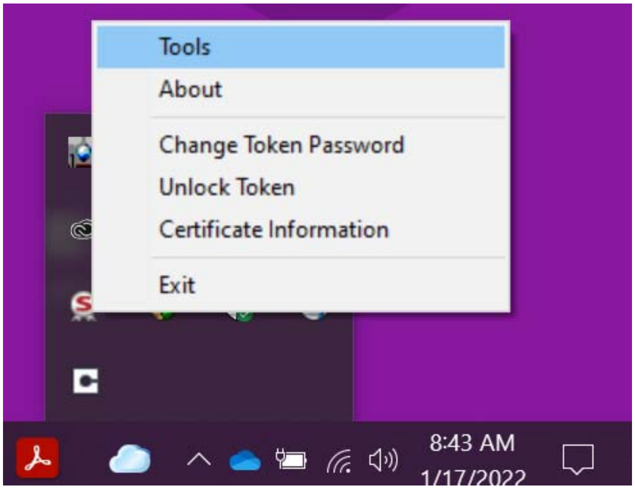
Note:
For installing to HSM: This procedure is not needed. Proceed to: "Install the certificate to a Hardware Security Module (HSM)" on page 37

To initialize your token

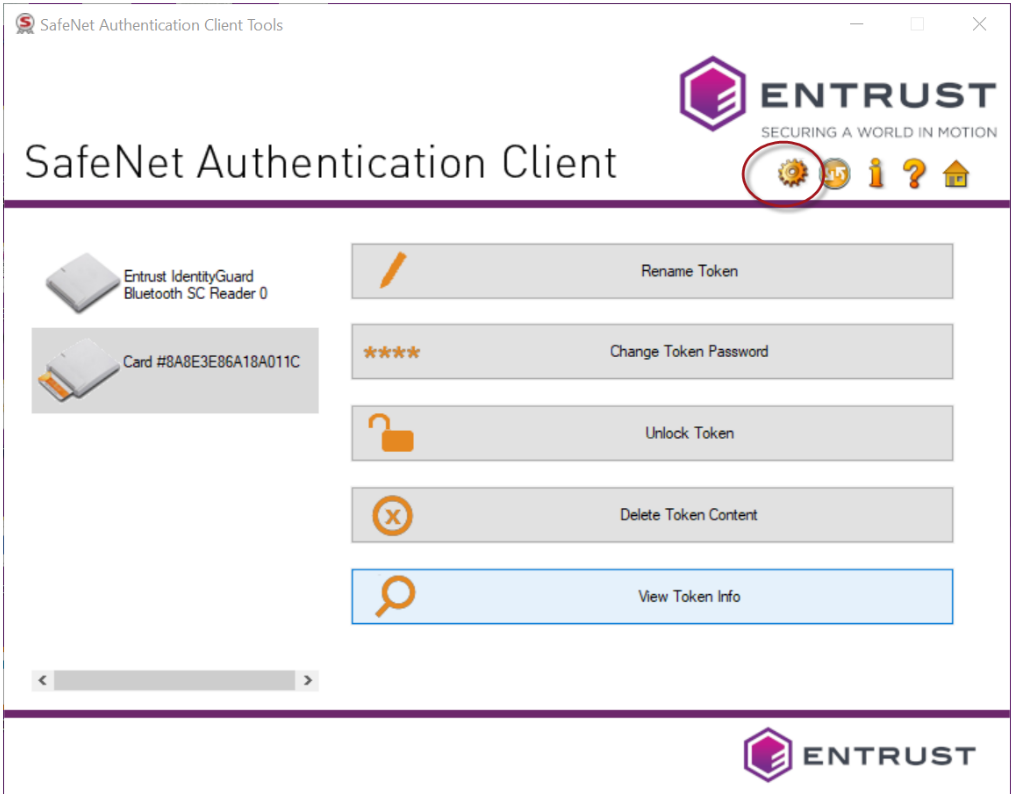
1 Insert your token into a USB slot on your computer. When the token has been recognized by the computer and the drivers have been installed, the Safenet icon in the system tray switches from grayed-out to active.



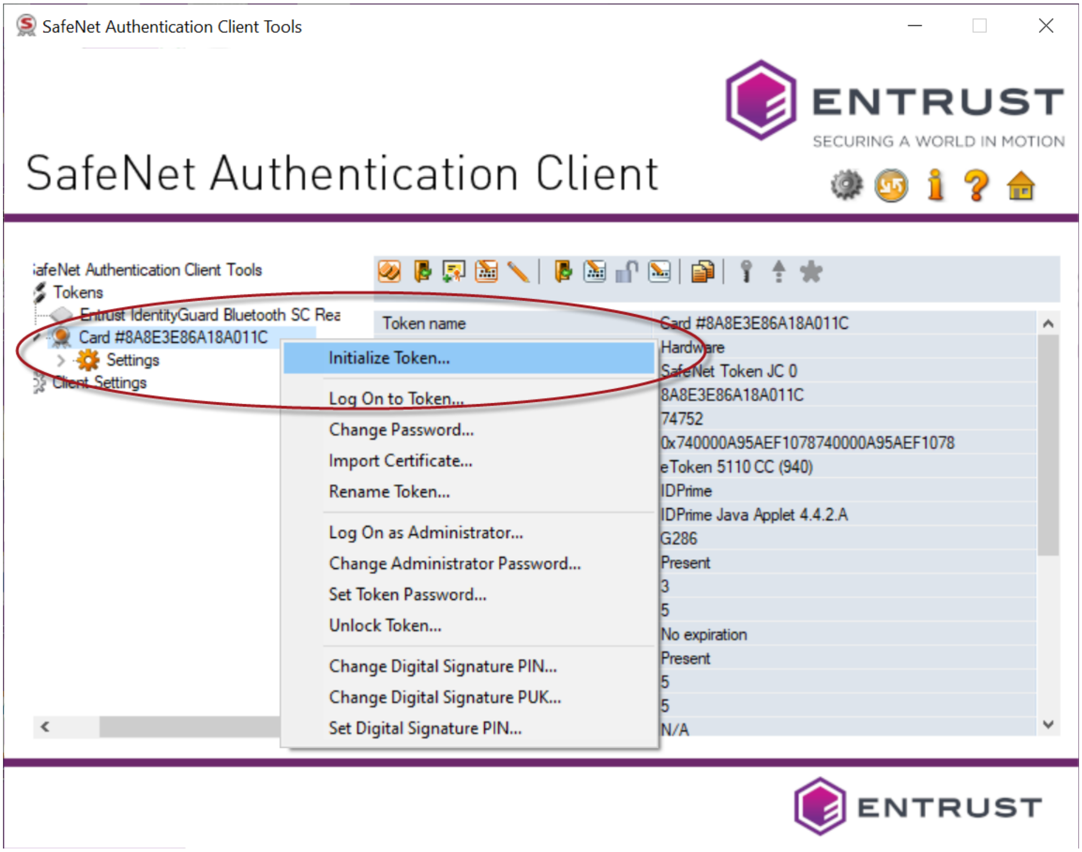
2 When the icon becomes active, right-click on it to open the menu. Select **Tools**.



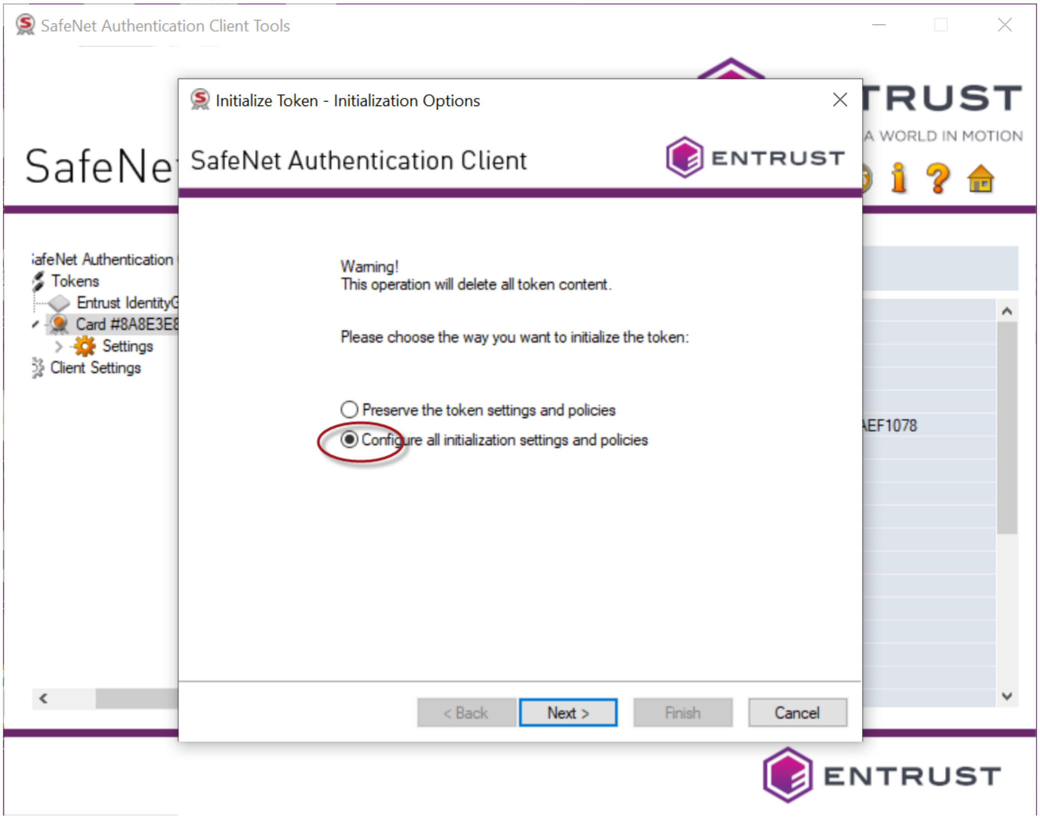
3 The SafeNet Authentication Client opens. Click the gear icon at the top right.


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 IdentityGuard Bluetooth SC Rea
Card #8A8E3E86A18A011C
Settings
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...
Token name
Card #8A8E3E86A18A011C
Hardware
SafeNet Token JC 0
8A8E3E86A18A011C
74752
0x740000A95AEF1078740000A95AEF1078
eToken 5110 CC (940)
IDPrime
IDPrime Java Applet 4.4.2.A
G286
Present
3
5
No expiration
Present
5
5
N/A
ENTRUST

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



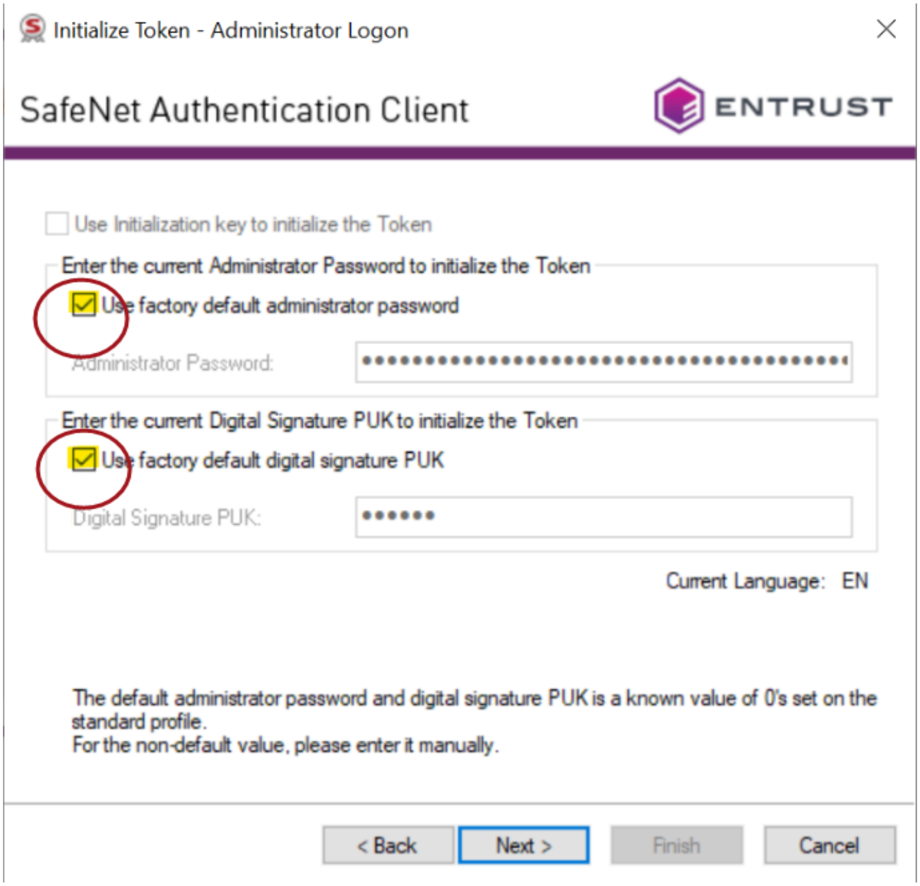
Warning!
This operation will delete all token content.

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.



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

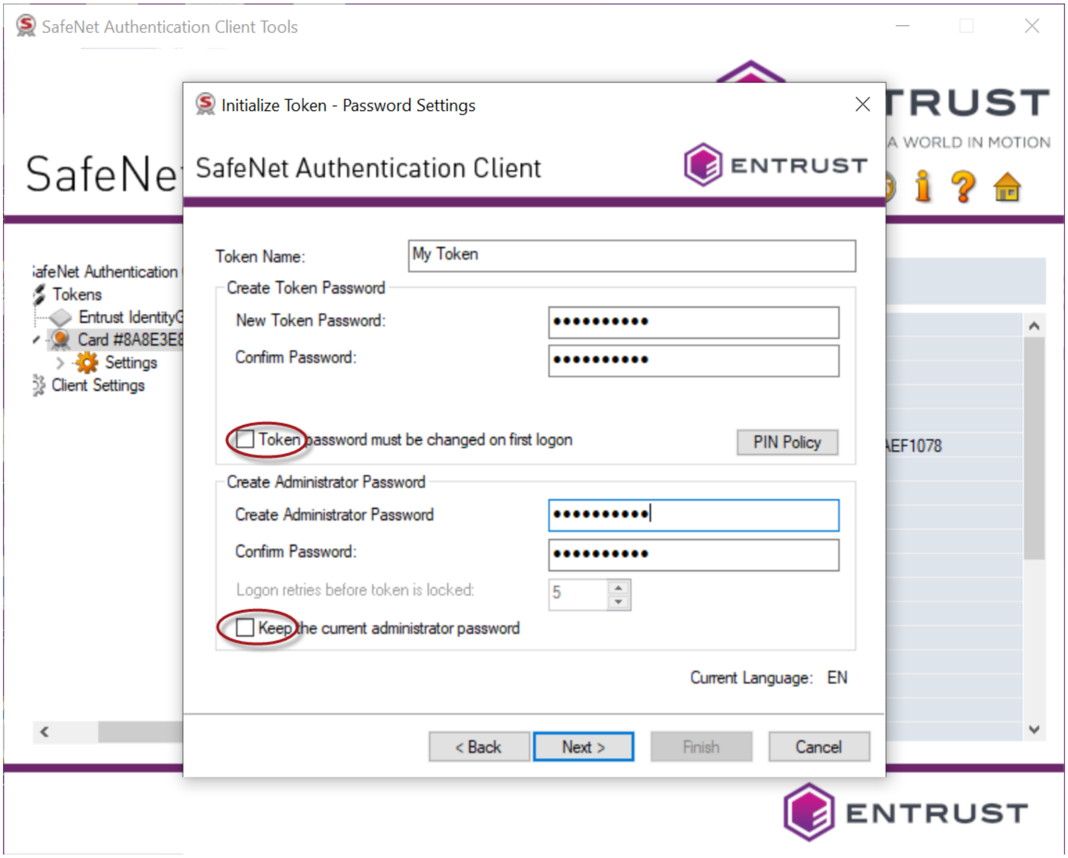
The default administrator password and digital signature PUK is a known value of 0's set on the standard profile.
For the non-default value, please enter it manually.

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

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

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 Unselect **Token password must be changed on first logon**.

d Create and confirm your Administrator password.

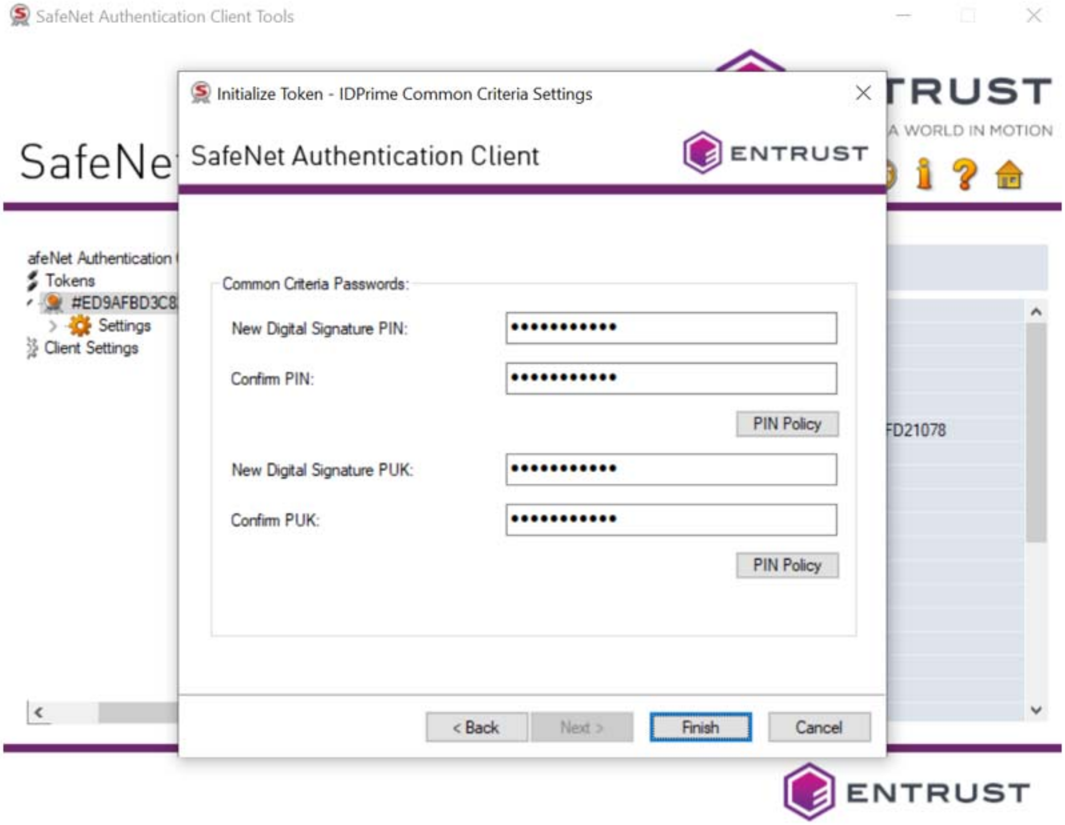
e Unselect **Keep the current administrator password**.

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).

11 Click **Next**.

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

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



Initialize Token - IDPrime Common Criteria Settings

SafeNet Authentication Client

Common Criteria Passwords:

New Digital Signature PIN: ••••••••••••

Confirm PIN: ••••••••••••

New Digital Signature PUK: ••••••••••••

Confirm PUK: ••••••••••••

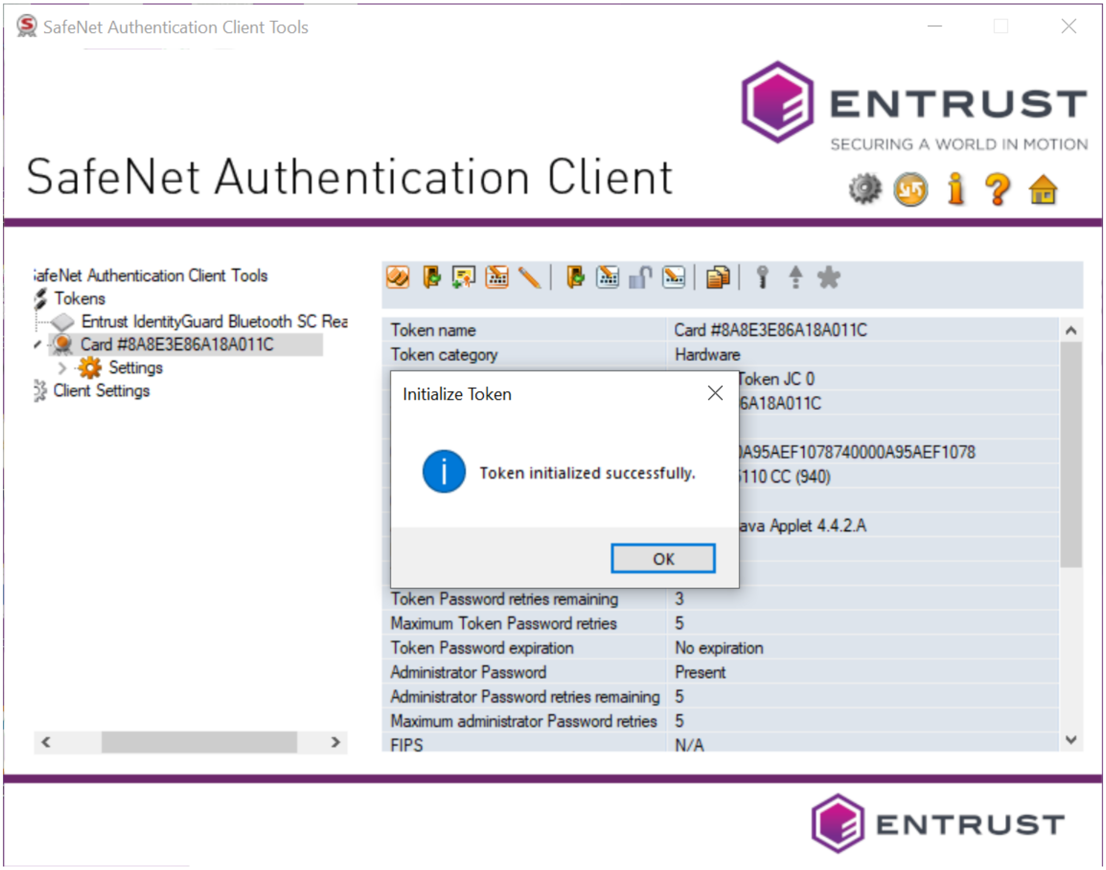
Attention:
Keep your passwords and PINs in a safe place (Token password, Administrator password, Digital Signature PIN and New Digital Signature PUK).

13 Click **Finish**.

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

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

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


SafeNet Authentication Client Tools
ENTRUST
SECURING A WORLD IN MOTION
SafeNet Authentication Client
iafeNet Authentication Client Tools
Tokens
Entrust IdentityGuard Bluetooth SC Rea
Card #8A8E3E86A18A011C
Settings
Client Settings
Initialize Token
OK
ENTRUST

Token initialized successfully.

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

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.

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 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 6
- The Entrust USB token must be initialized. If that's not been done, follow the instructions in: "Initializing an Entrust USB token" on page 13

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 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 22
- "To download a certificate to a hardware token using Microsoft Internet Explorer" on page 32

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

- "Install the certificate to a Hardware Security Module (HSM)" on page 37

Install the certificate to Entrust USB token using PowerShell script

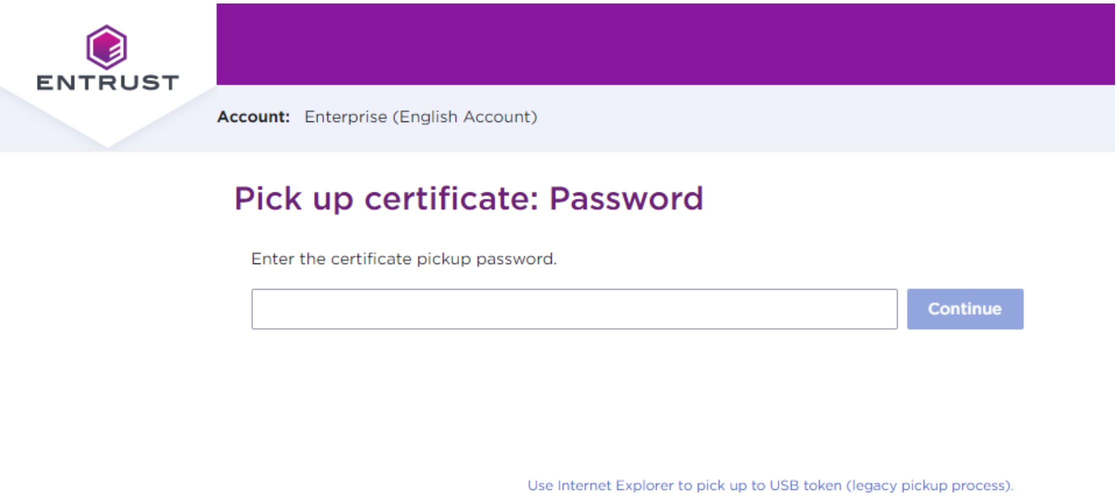
This is the recommended procedure for picking up your certificate to an Entrust USB token. It can be used with all supported browsers.

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 a hardware 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.



ENTRUST

Account: Enterprise (English Account)

Pick up certificate: Password

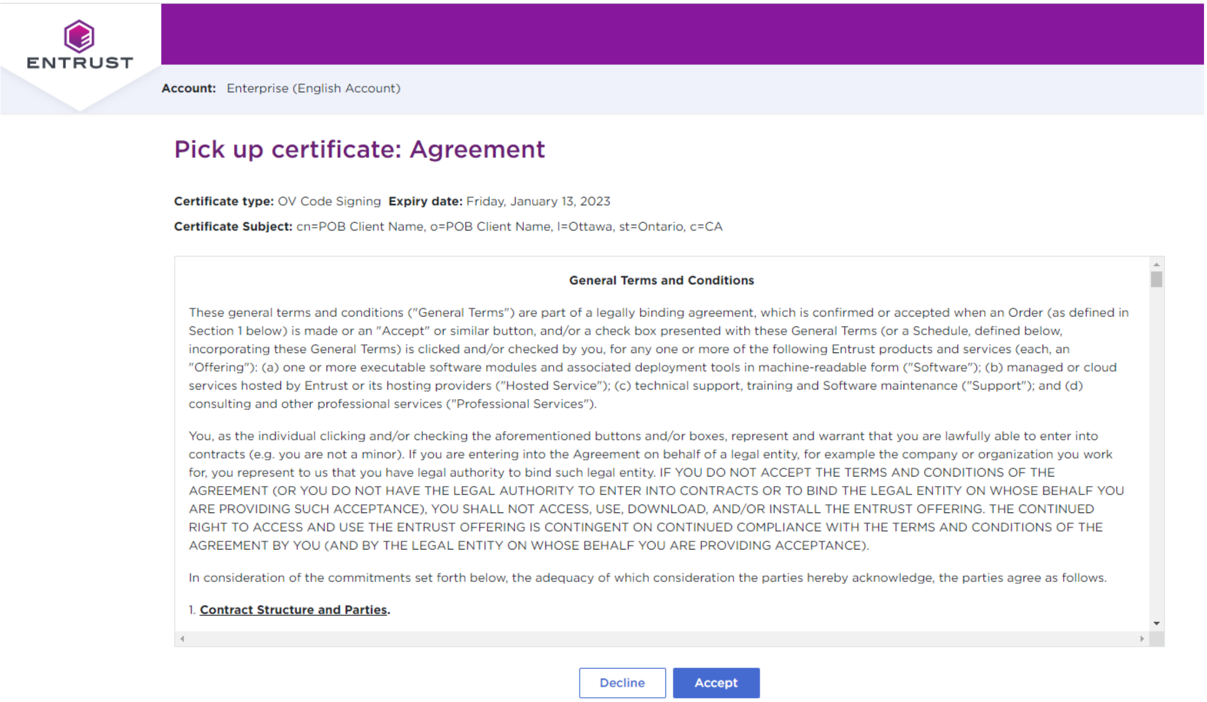
Enter the certificate pickup password.

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

2 Enter the password that you 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: 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

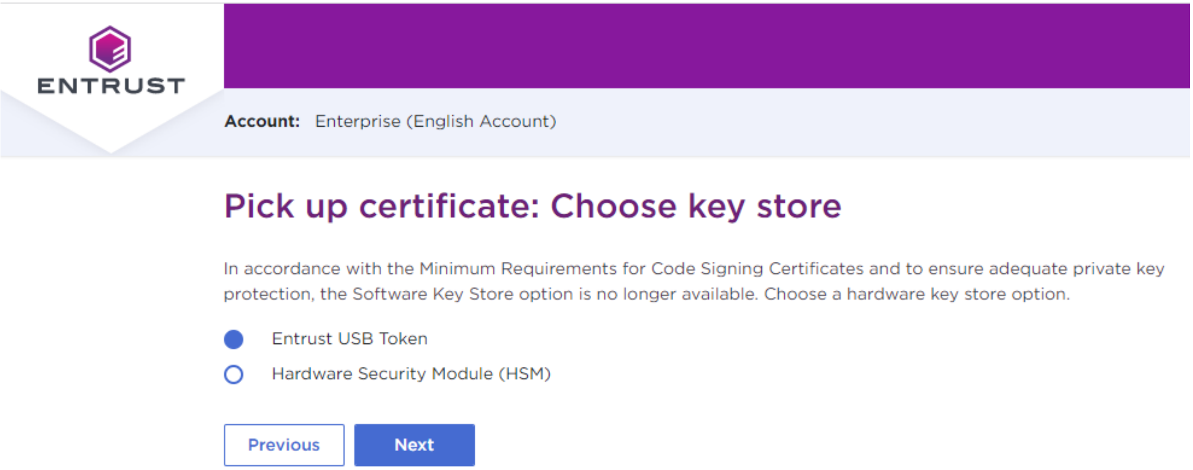
These general terms and conditions ("General Terms") are part of a legally binding agreement, which is confirmed or accepted when an Order (as defined in Section 1 below) is made or an "Accept" or similar button, and/or a check box presented with these General Terms (or a Schedule, defined below, incorporating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



Account: Enterprise (English Account)

Pick up certificate: Choose key store

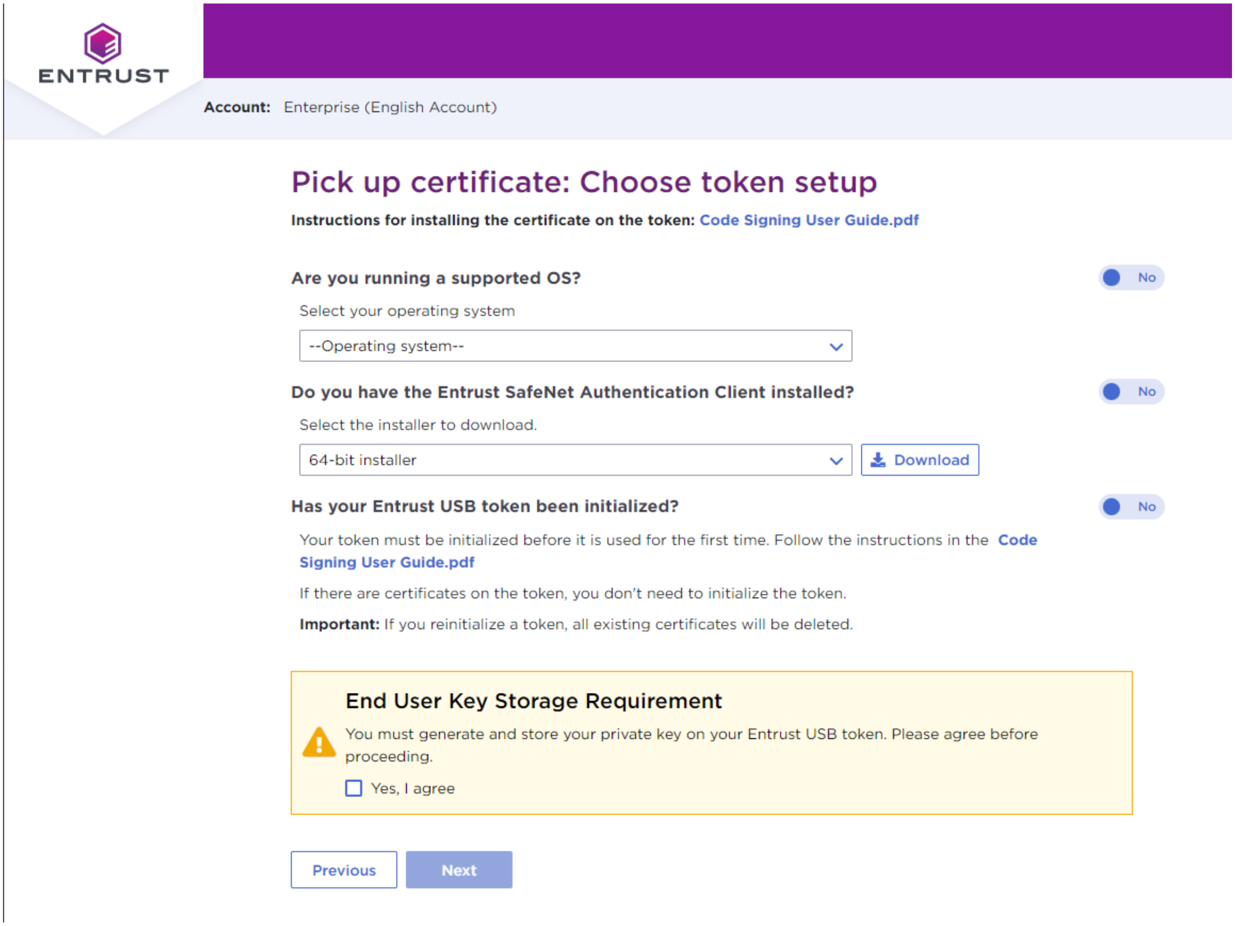
In accordance with the Minimum Requirements for Code Signing Certificates and to ensure adequate private key protection, the Software Key Store option is no longer available. Choose a hardware key store option.

● Entrust USB Token

○ Hardware Security Module (HSM)

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

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



ENTRUST

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

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

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

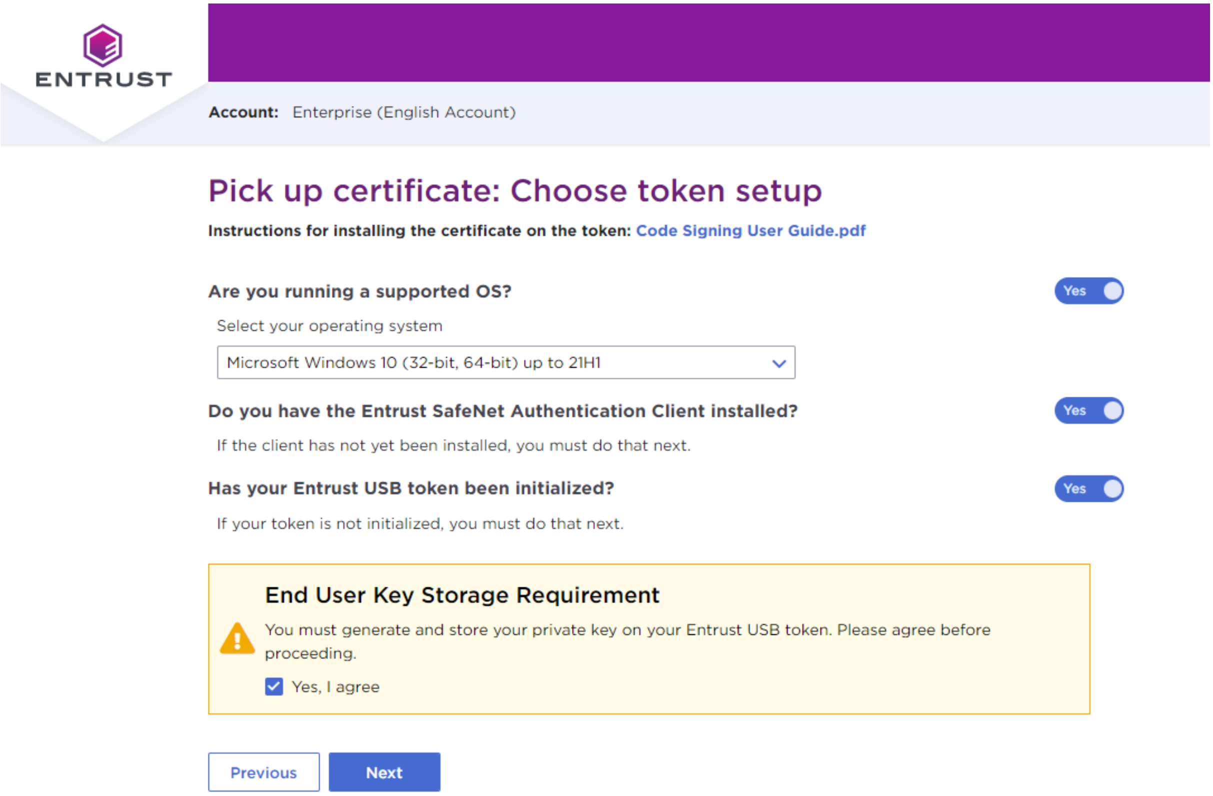
- If the SafeNet client is already installed, click to change the toggle to **Yes**, and continue with the next step.
- If the SafeNet client is not yet installed, follow the procedure in: "To obtain and install the token authentication client" on page 6. When the SafeNet software is installed, return to this browser page and this procedure to continue.

9 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 13. When the USB token is initialized, return to this browser page and this procedure to continue.

10 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.

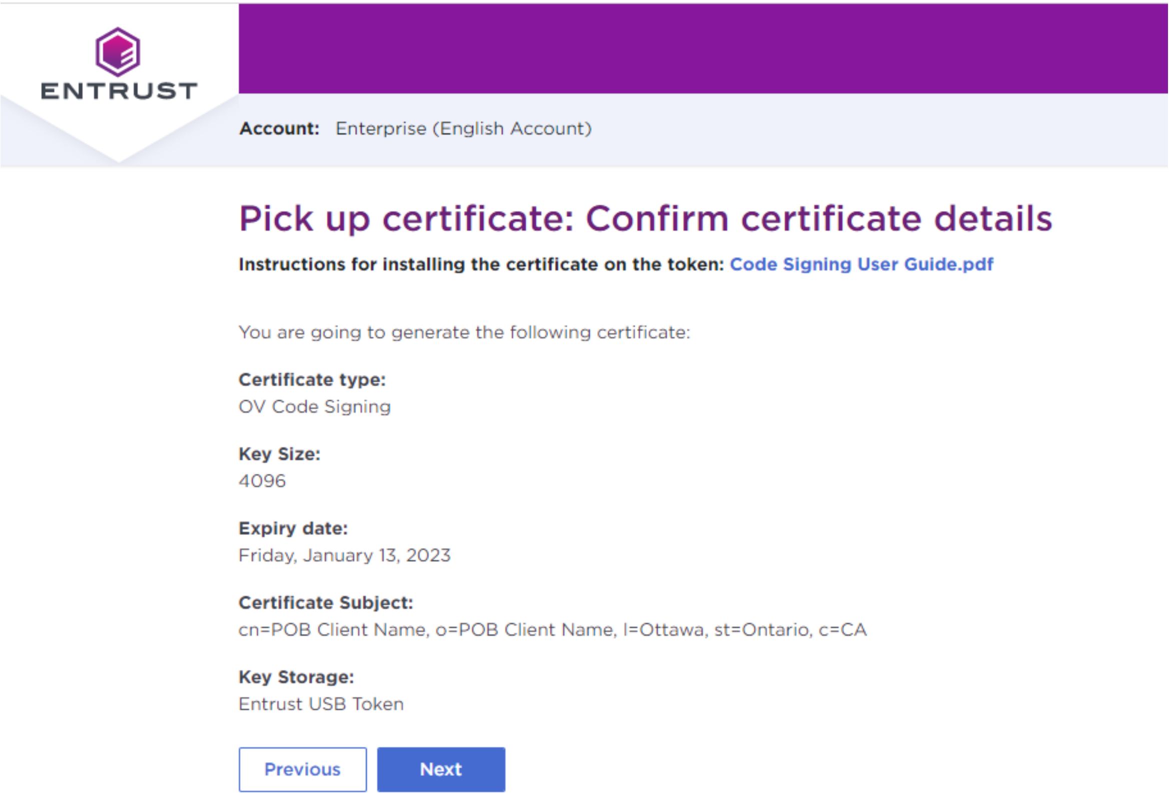
End User Key Storage Requirement

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

☑ Yes, I agree

11 Click **Next** to proceed.

12 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

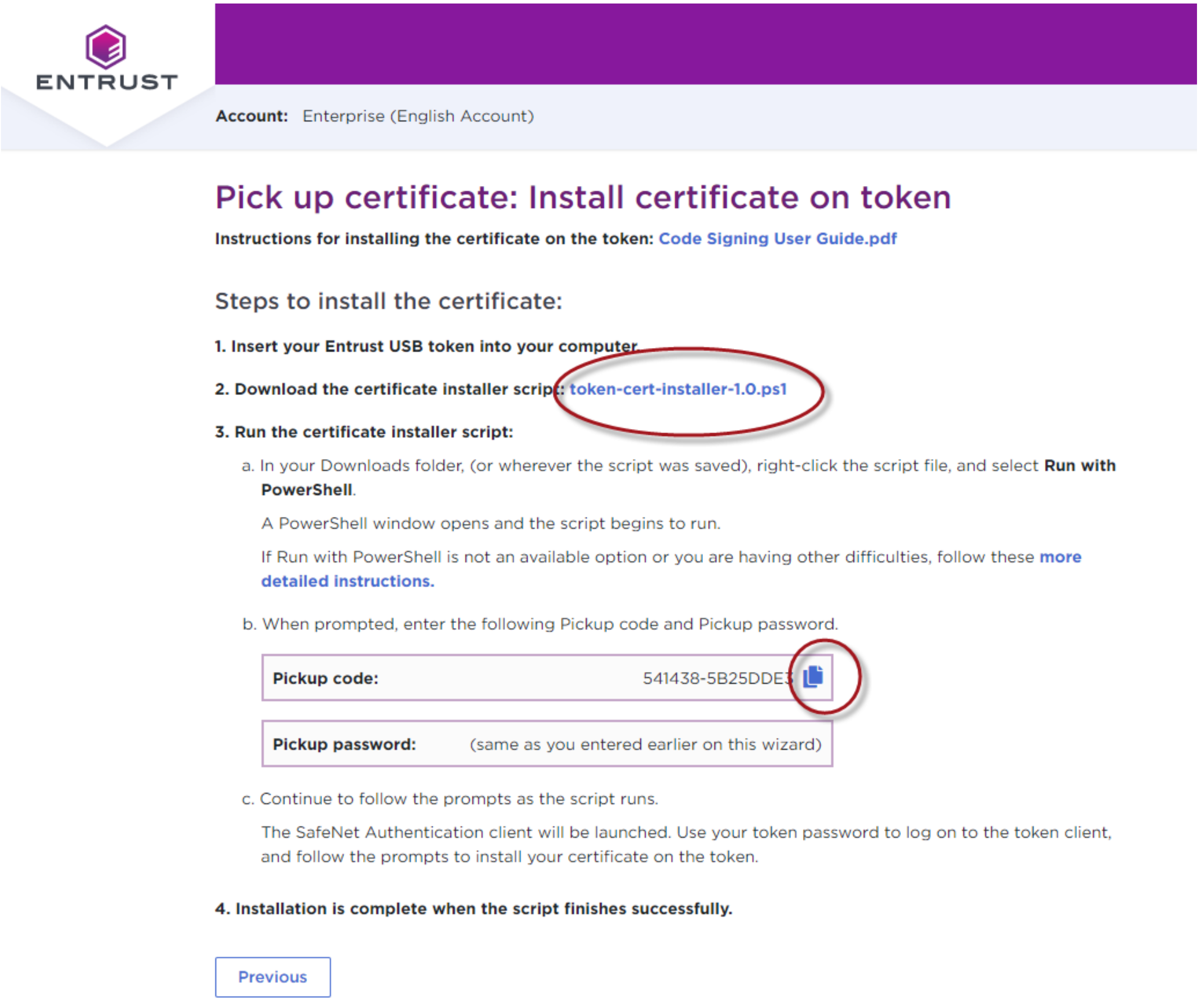
Key Size:
4096

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: Enterprise (English Account)

Pick up certificate: Install certificate on token

Instructions for installing the certificate on the token: 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-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:	541438-5B25DDE3
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.

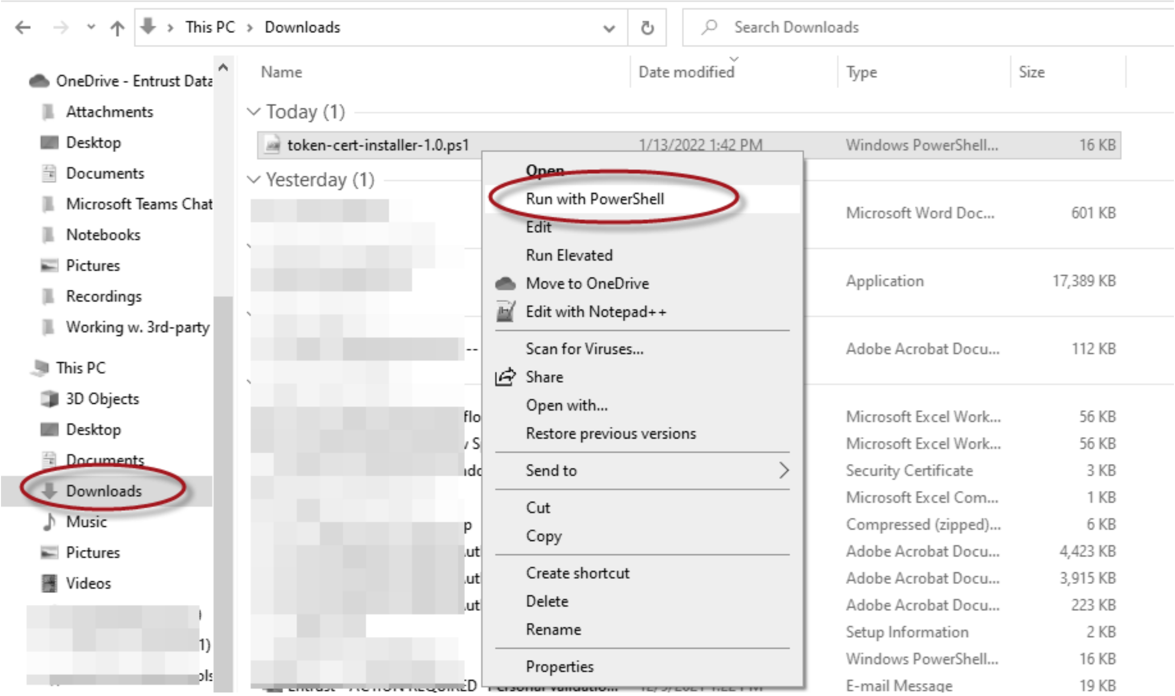
13 Insert your token into a USB port if it is not already there.

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

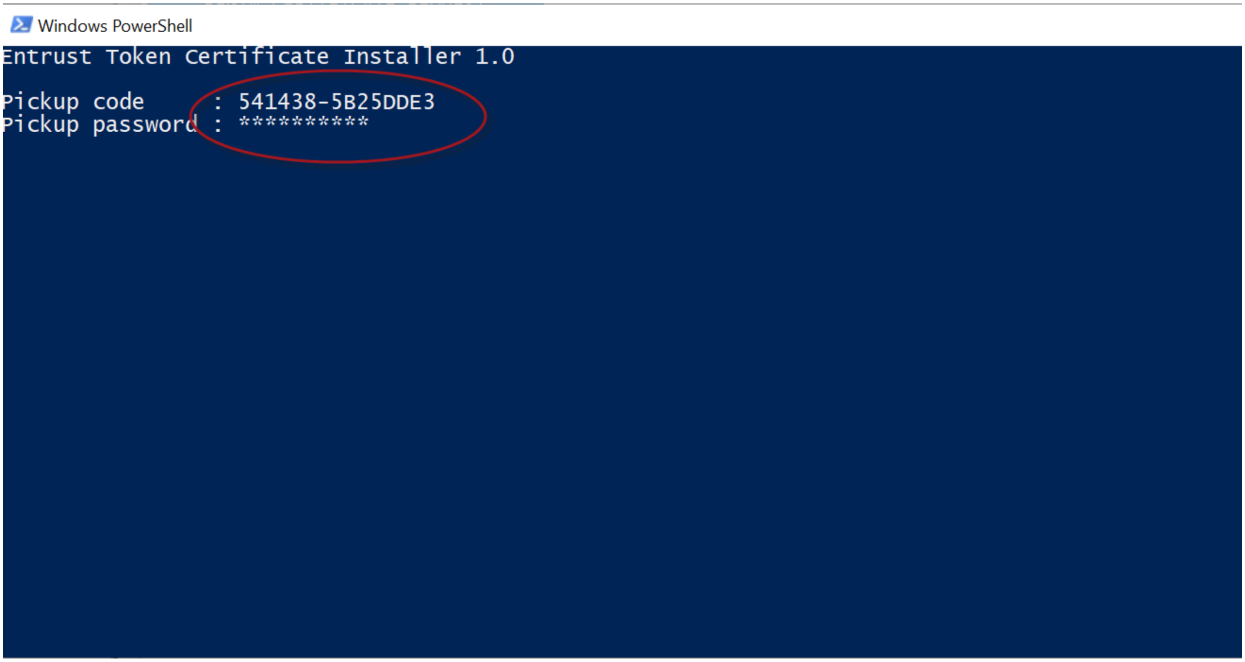
15 Download the token installer script by clicking the script name: `token-cert-installer-<version>.ps1`

16 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.

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



18 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

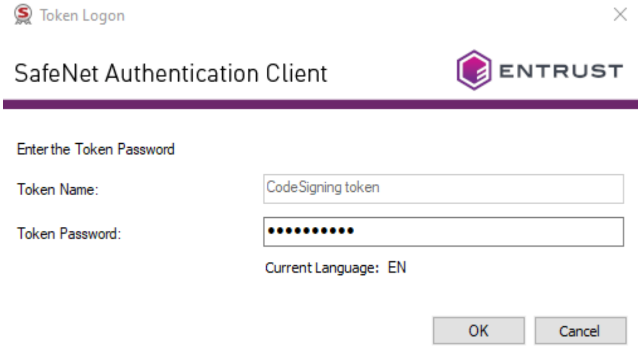
```
Entrust Token Certificate Installer 1.0

Pickup code     : 541438-5B25DDE3
Pickup password : **********
```

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

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

21 Press the Enter/Return key.

The SafeNet client is started.



Token Logon

SafeNet Authentication Client

Enter the Token Password

Token Name: CodeSigning token

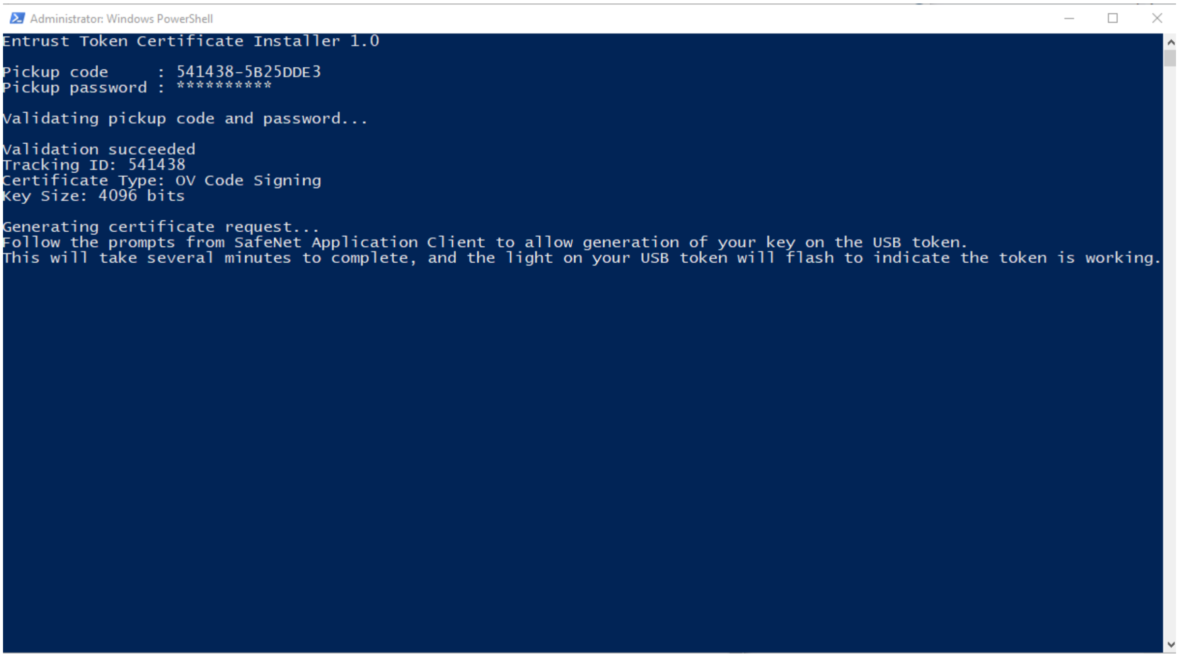
Token Password: ••••••••••

Current Language: EN

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

23 Click **OK**.

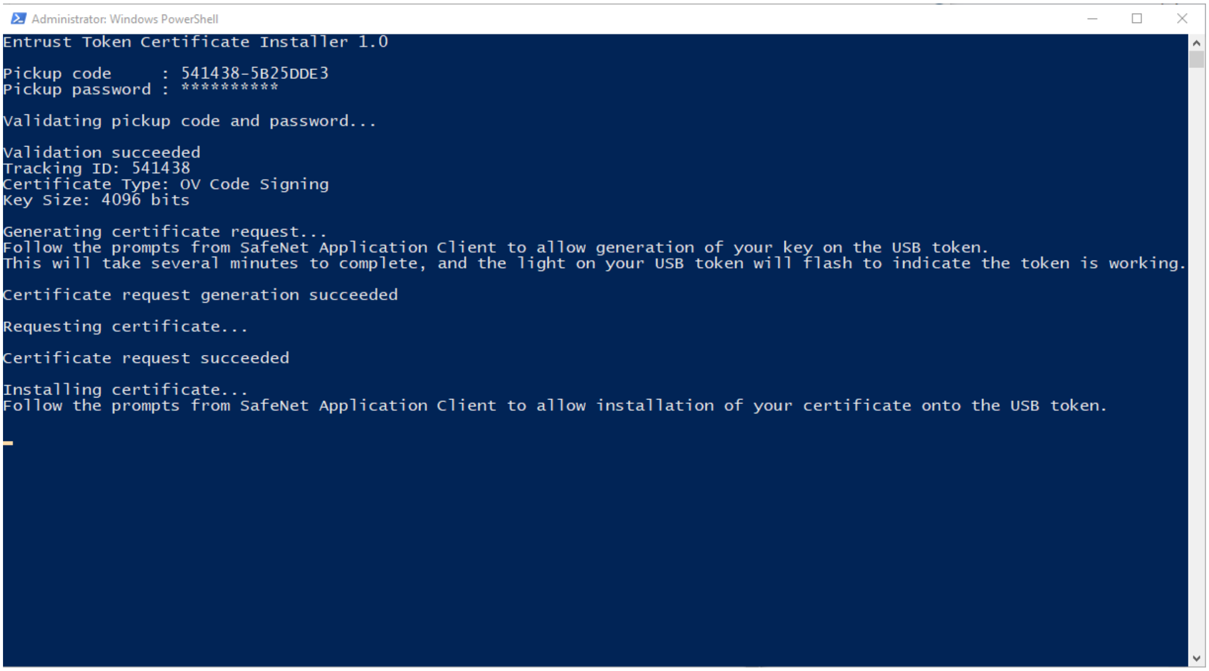
24 The PowerShell installation script continues to run.



```
Entrust Token Certificate Installer 1.0

Pickup code     : 541438-5B25DDE3
Pickup password : **********

Validating pickup code and password...

Validation succeeded
Tracking ID: 541438
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 flashing through most of the process.

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



```
Entrust Token Certificate Installer 1.0

Pickup code     : 541438-5B25DDE3
Pickup password : **********

Validating pickup code and password...

Validation succeeded
Tracking ID: 541438
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.

_
```

25 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

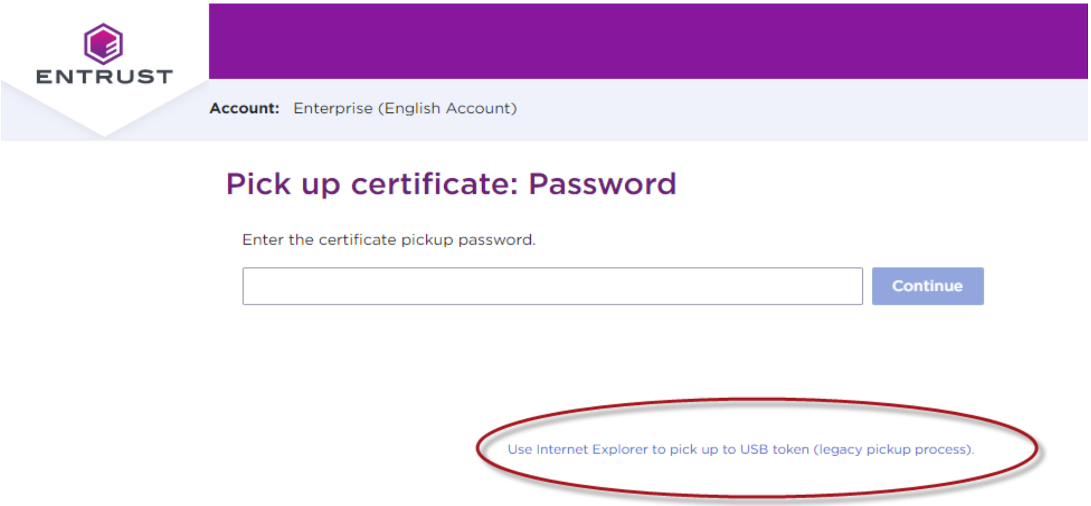
This pickup procedure is available only with the Microsoft Internet Explorer browser. This procedure will be deprecated when support for Internet Explorer is ended by Microsoft.

To download a certificate to a hardware 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.



Account: Enterprise (English Account)

Pick up certificate: Password

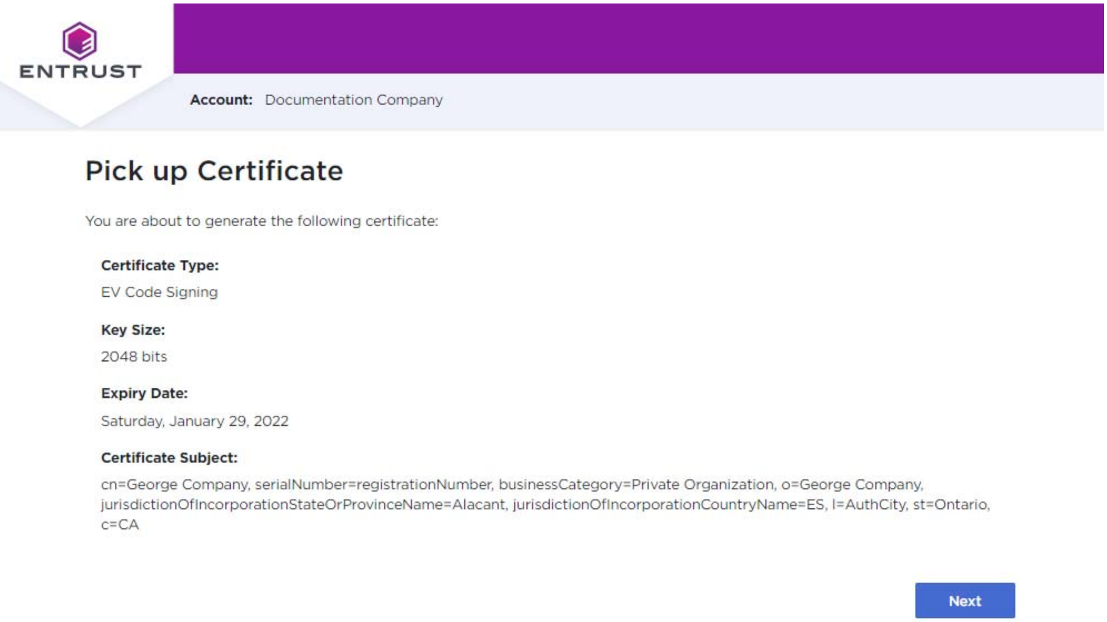
Enter the certificate pickup password.

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

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.



Account: Documentation Company

Pick up Certificate

You are about to generate the following certificate:

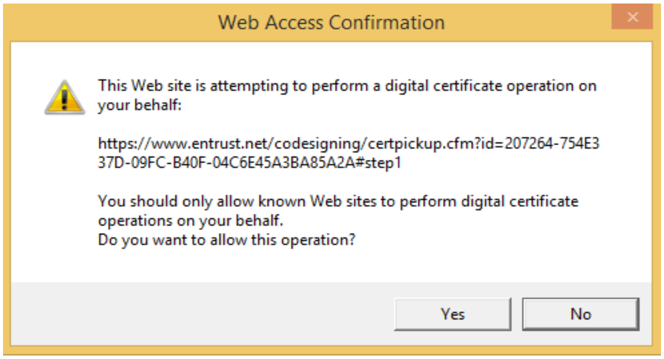
Certificate Type:
EV Code Signing

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.



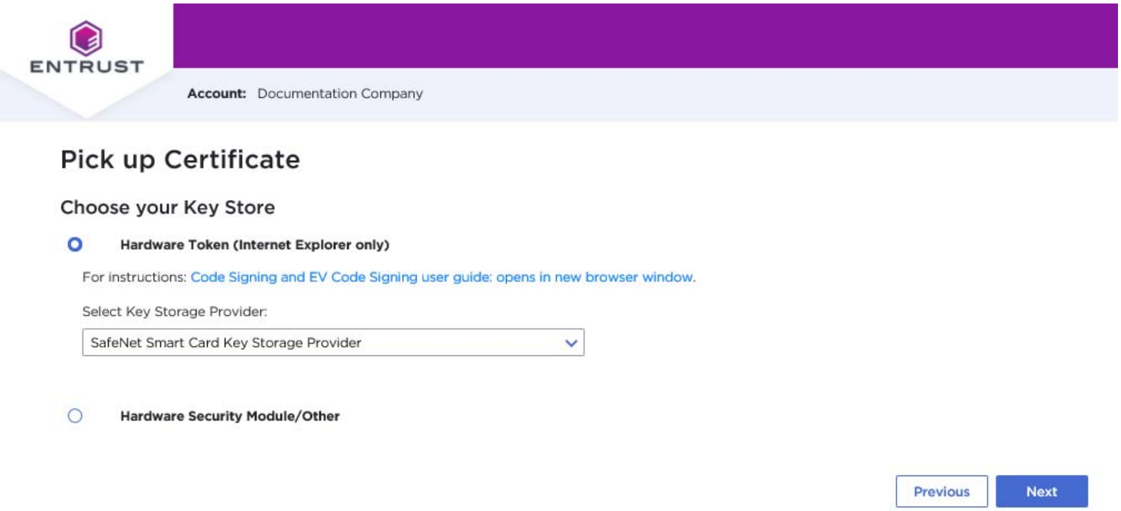
Web Access Confirmation

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

https://www.entrust.net/codesigning/certpickup.cfm?id=207264-754E337D-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)**

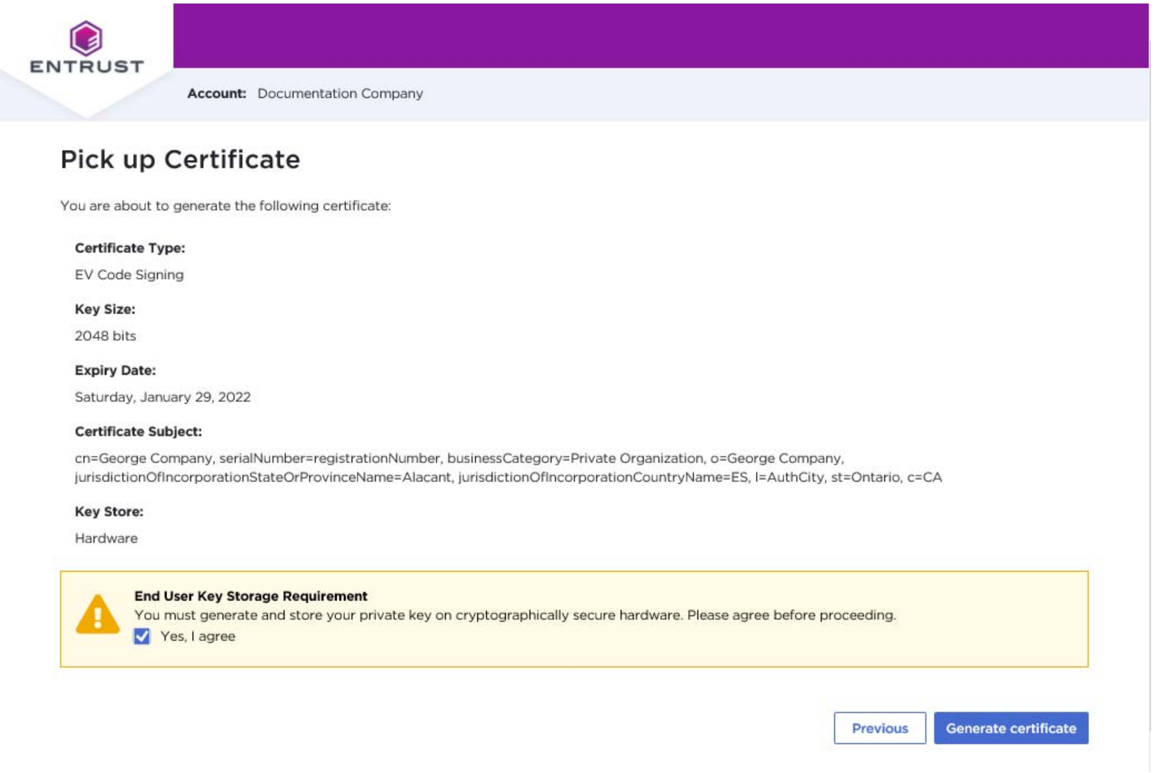
For instructions: Code Signing and EV Code Signing user guide: opens in new browser window.

Select Key Storage Provider:

SafeNet Smart Card Key Storage Provider

○ **Hardware Security Module/Other**

The **Pick up Certificate** page appears.



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

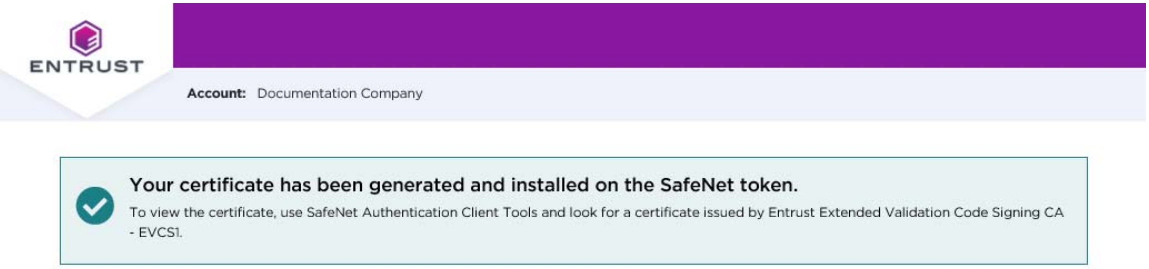
End User Key Storage Requirement
You must generate and store your private key on cryptographically secure hardware. Please agree before proceeding.
☑ Yes, I agree

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 Web site.

11 The Web site generates the certificate on your token. This will take a few minutes. When the certificate has been created, a success message is displayed.



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.

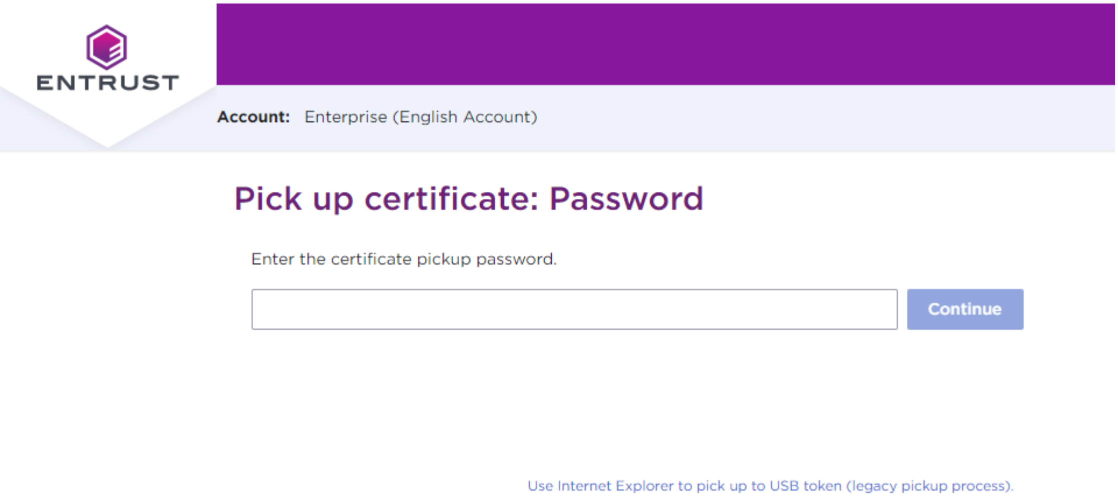
Install the certificate to a Hardware Security Module (HSM)

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.

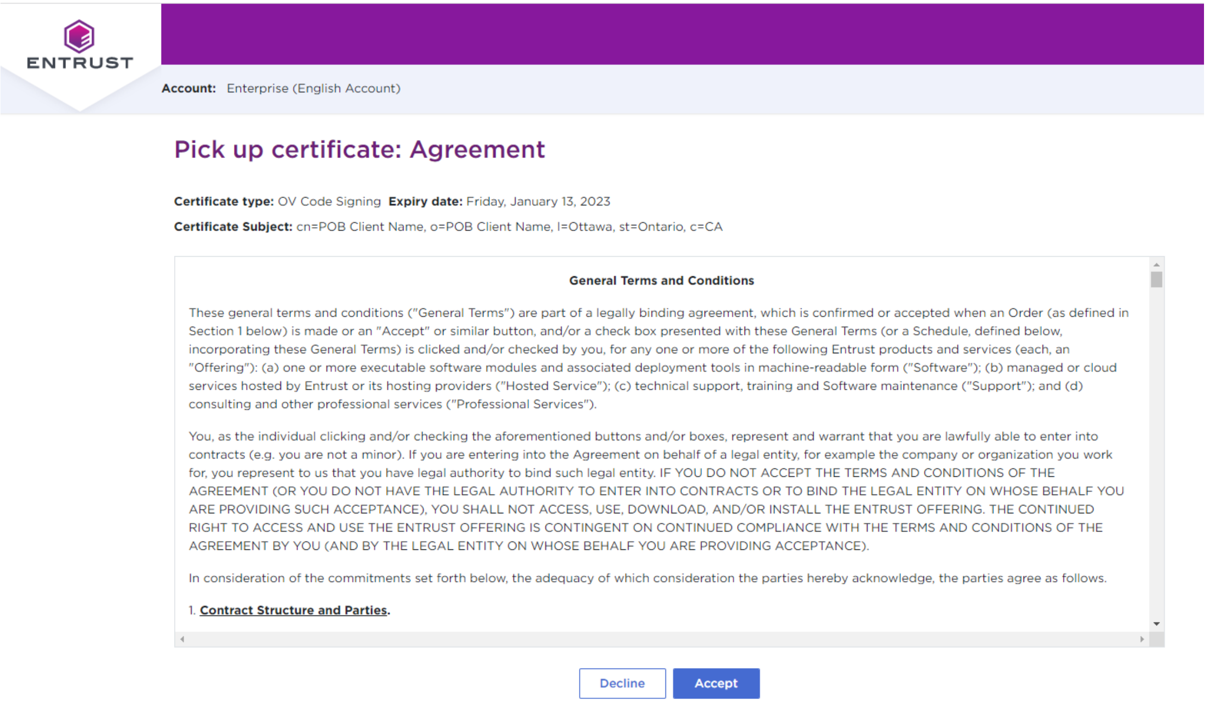
Use Internet Explorer to pick up to USB token (legacy pickup process).

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).

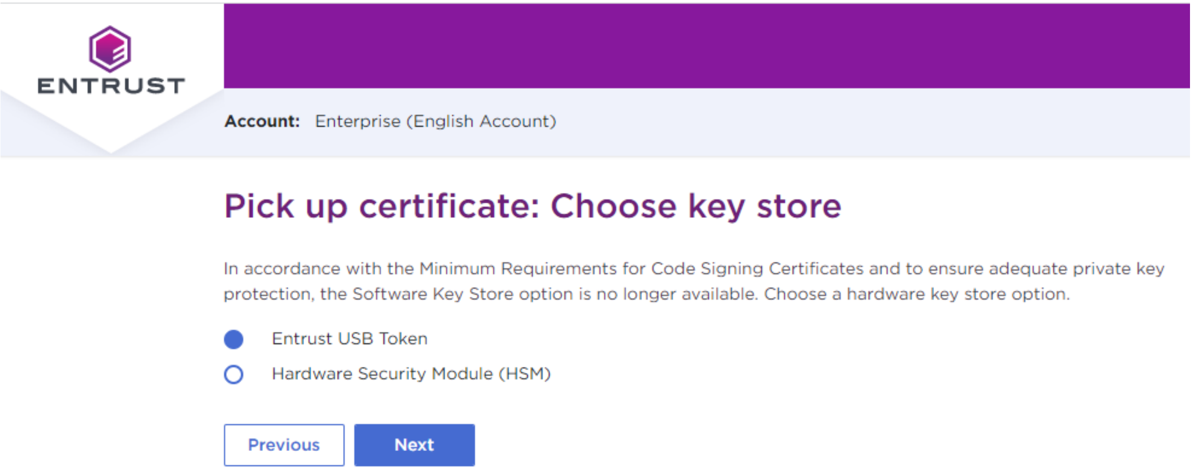
In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Contract Structure and Parties**.

5 Read and accept the Entrust Certificate Services Agreement.

6 Click **Accept**.

The **Choose your Key Store** page appears.



Account: Enterprise (English Account)

Pick up certificate: Choose key store

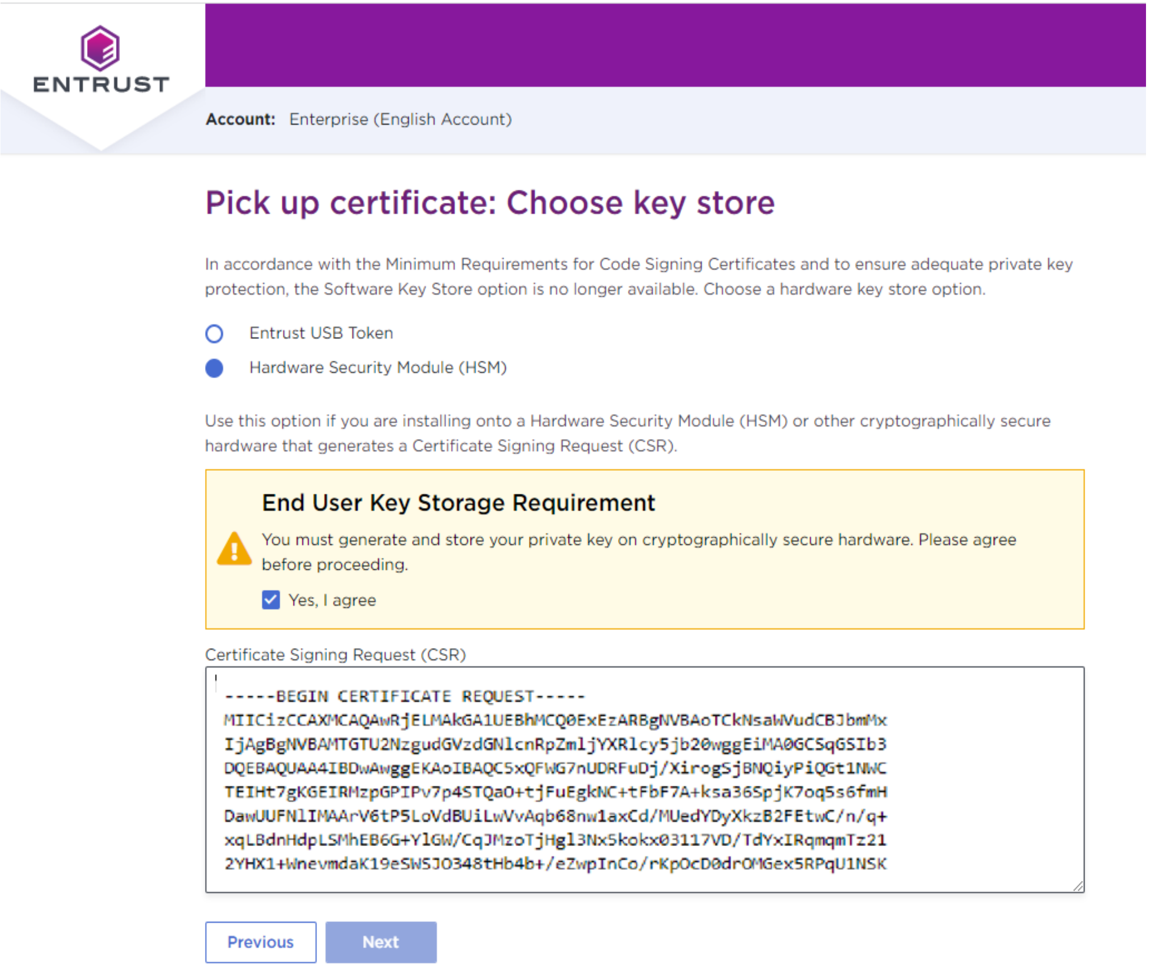
In accordance with the Minimum Requirements for Code Signing Certificates and to ensure adequate private key protection, the Software Key Store option is no longer available. Choose a hardware key store option.

● Entrust USB Token

○ Hardware Security Module (HSM)

7 Select **Hardware Security Module**.

8 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)

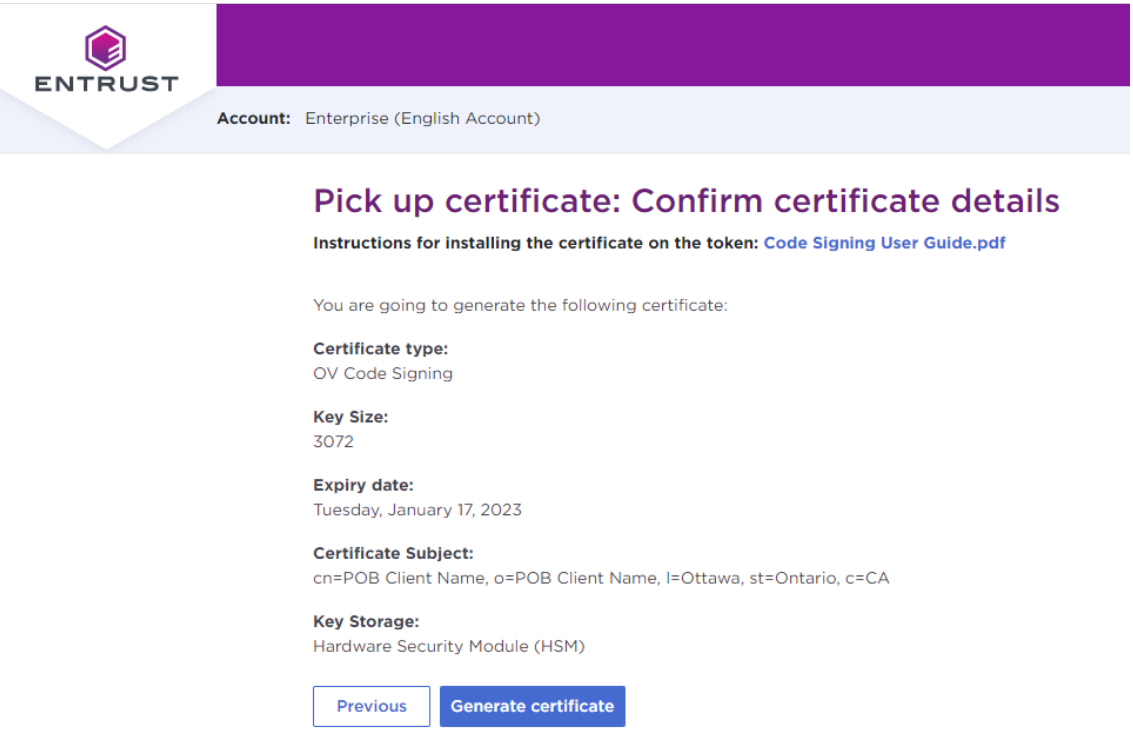
```
-----BEGIN CERTIFICATE REQUEST-----
MIICizCCAXMCAQAwRjELMAkGA1UEBhMCQ0ExEzARBgNVBAoTCkNsaWVudCBJbmMx
IjAgBgNVBAMTGTU2NzgudGVzdGNlcnRpZmljYXRlcy5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC5xQFWG7nUDRFuDj/XirogSjBNQiyPiQGt1NWC
TEIHt7gKGEIRMzpGPIPv7p4STQaO+tjFuEgkNC+tFbF7A+ksa36SpjK7oq5s6fmH
DawUUFNlIMAArV6tP5LoVdBUiLwVvAqb68nw1axCd/MUedYDyXkzB2FEtwC/n/q+
xqLBdnHdpLSMhEB6G+YlGW/CqJMzoTjHgl3Nx5kokx03117VD/TdYxIRqmqmTz21
2YHX1+WnevmdaK19eSWSJO348tHb4b+/eZwpInCo/rKpOcD0drOMGex5RPqU1NSK
```

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

10 Paste in the CSR you generated on your HSM.

11 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

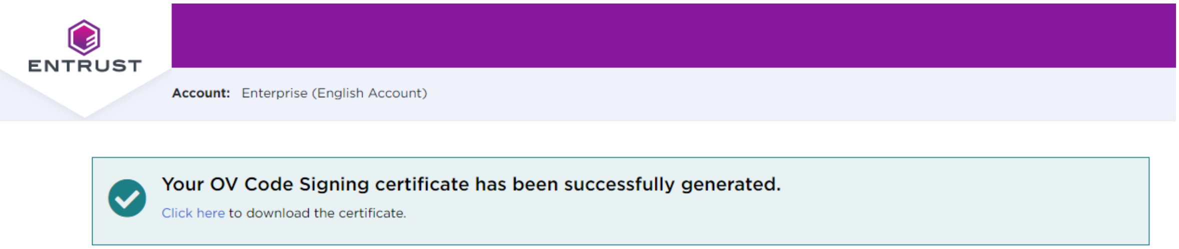
Expiry date:
Tuesday, January 17, 2023

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

Key Storage:
Hardware Security Module (HSM)

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

13 The **Success** screen appears.



ENTRUST

Account: Enterprise (English Account)

✓ Your OV Code Signing certificate has been successfully generated.

Click here to download the certificate.

14 You can now install your certificate on your HSM.

Changing the password for your token

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

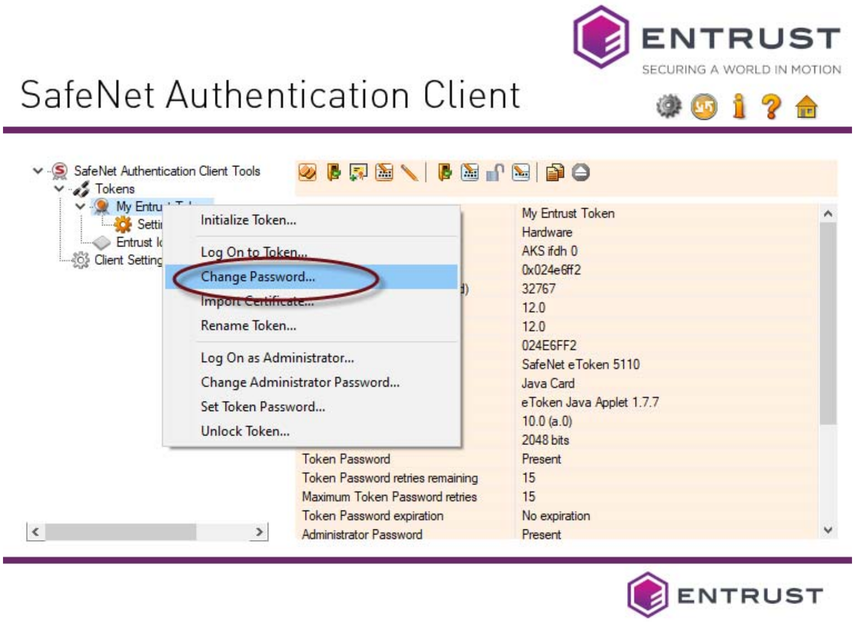
To change your token password

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

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

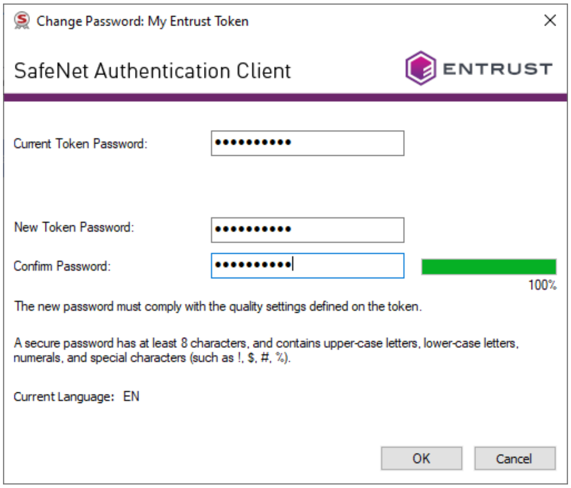
3 Click the **Advanced View** (gear) icon.

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



	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. 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

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

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.