SET UP YOUR DIGICERT PROVIDED ETOKEN

Solution ID : SO260521210823 **Last Modified : 11/01/2023**

Learn how to set up your code signing DigiCert-provided hardware token.

Before you begin

Before you begin, make sure you meet these prerequisites:

- DigiCert-provided hardware token: SafeNet 5110 CC, SafeNet 5110 FIPS, or SafeNet 5110+ FIPS.
- Access to your certificate's Order details page in CertCentral.
- Code Signing or EV Code Signing certificate order number.
- Verify whether the eToken is blank or comes with the certificate preinstalled.
- Administrator permissions on your computer.
- Secure password manager. See Passwords 101.

> Important:
>
> This process will require you to supply multiple passwords. If password, you can permanently disable your eToken. We rec manager to track the passwords used for initializing your eTo

How do I know if my eToken is blank or comes with the certificate installed?

In your CertCentral account, go to your certificate's Order

details page. In the Certificate actions dropdown menu, what option do you see? The menu option lets you know if the eToken is blank or has the certificate preinstalled.

Menu options:

- Install certificate
  This option means the eToken is blank, and you must install the certificate on the eToken. See Install your code signing certificate on your hardware eToken below.

- Initialize token
  This option means the certificate comes preinstalled on your eToken. You need to unlock the eToken to access your certificate. See Initialize your eToken below.

Install your code signing certificate on your eToken

1. In your CertCentral account, in the left main menu, go to Certificates > Orders.

2. On the Orders page, select the certificate's order number.

3. On the certificate's Order details page, in the Certificate detail section, in the Certificate actions dropdown, select Install certificate.

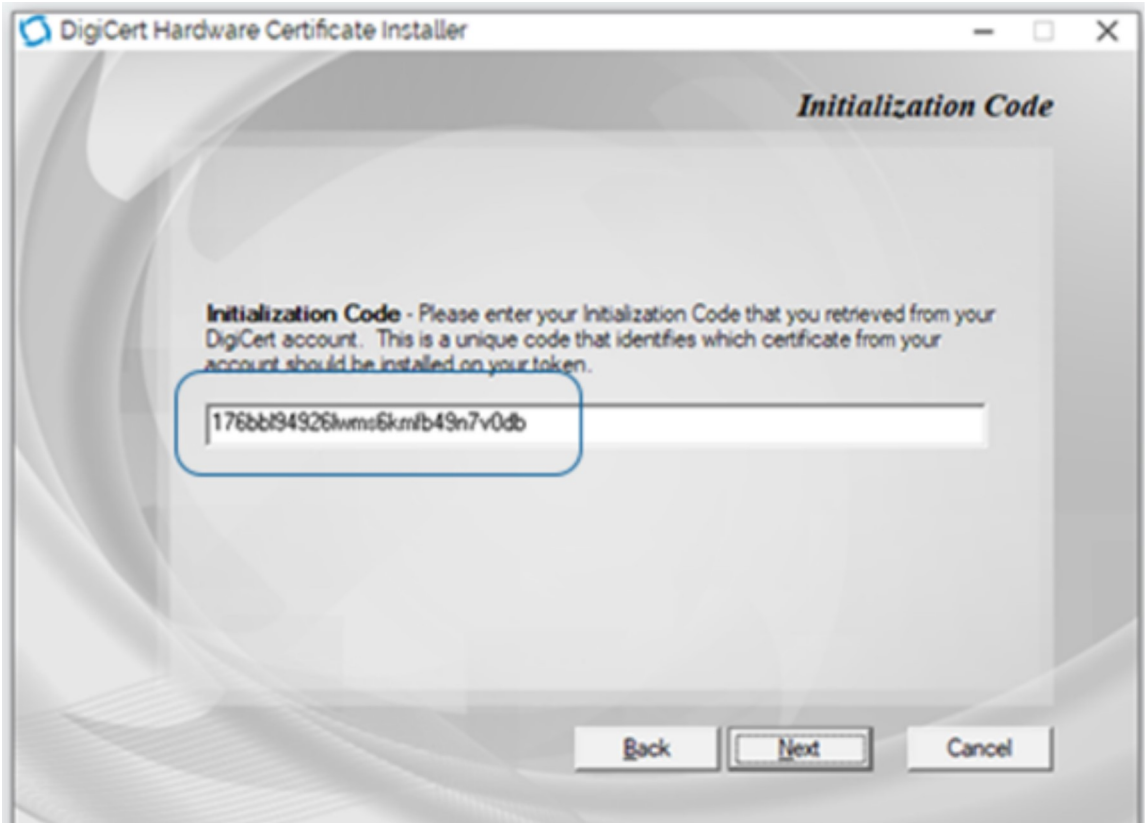
4. On the install certificate page, use the link to download and install the DigiCert Hardware Certificate Installer.

   1. You must install the SafeNet Authentication Client on any system you plug the eToken in to sign code.
   2. Learn how to install the SafeNet Drivers.

5. Copy the initialization code for your order.

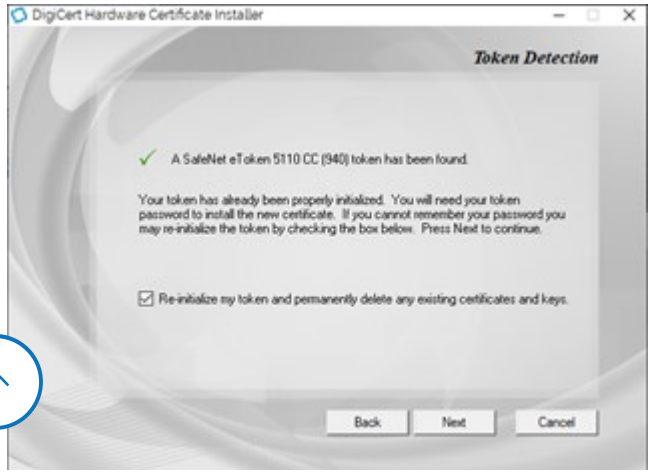
6. Open the DigiCert Hardware Certificate Installer.

7. In the DigiCert Hardware Certificate Installer on the Initialization Code page, in the Initialization Code box, enter the initialization code from your CertCentral account and then select Next.



8. Plug in your eToken.

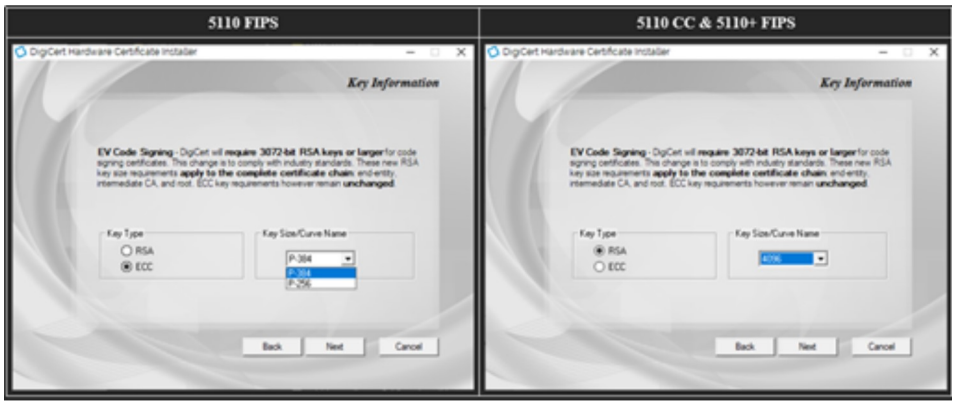
9. On the Token Detection page, check Re-initialize my token and permanently delete any existing certificates and keys and then select Next.
If you are installing an alternate chain or key type and need to keep your current certificate on the eToken intact, leave the Re-initialize option unchecked.



10. On the Key information page, do one of the following tasks and then select Next:

- RSA
    1. Under Key Type, select RSA.
    2. Under Key Size/Curve Name, select 4096.

- ECC Key Types
    1. Under Key Type, select ECC
    2. Under Key Size/Curve Name, select p-256 or p-384.



11. On the Token Setup page, do the following tasks:

1. Add a Token Name.
   The token name is used to identify the eToken. This name is helpful when you have multiple eTokens.
2. Create a Token Password.
   This password (sometimes called a token PIN) is required to access the certificates saved on the eToken.

12. READ THIS BEFORE YOU CONTINUE

On the Administrator Password page, do one of the following tasks:

1. If you have NOT changed the Administrator Password since receiving your eToken, leave Use factory default Administrator password checked and select Finish.
2. If you have set a new Administrator Password (done outside of DigiCert Support using the SafeNet client), uncheck Use factory default Administrator password, enter the current Administrator Password, and select Finish.

13. On the Certificate Installation page, be patient and wait. Some of the steps may take several minutes to complete. Wait to remove the eToken until the whole process is completed. Generating an RSA 4096-bit key will take time. Let the process complete.

14. When the process finishes, select Close.

15. You can now use the code signing certificate on your eToken to sign code.

Initialize your eToken

1. In your CertCentral account, in the left main menu, go to Cert

2. On the Orders page, select the certificate's order number.

3. On the certificate's Order details page, in the Certificate detai dropdown, select Initialize Token.

> **Important: Do not proceed without your DigiCert-provided ha to complete these steps. Additionally, some information is c**

4. On the initialization page, confirm you have your eToken. If you have not received your DigiCert-provided hardware token, check your tracking information. However, come back once you

1. Now that you have your DigiCert-provided hardware toke token.

2. When ready, select Submit.

5. On the confirmation page, copy your preassigned eToken pas

> **Warning: Your preassigned password will only be visible onc password. You need it to access your certificate on your Dig** See Password 101.

6. Use the link to download and install the DigiCert Hardware C

1. You must install the SafeNet Authentication Client on an code.
2. Learn how to install the SafeNet Drivers.

7. Change the eToken password.
The eToken password is used to access the eToken certificate

1. Open the SafeNet Authentication Client and then connec
2. In the SafeNet Authentication Client, on the top of the pa button).
   You should now see the eToken listed in the tree menu o
3. Right-click on the eToken name and select Change Pass
4. On the change password page, enter your Current Token CertCentral.
5. Next, create a new password.
6. Save the New Token Password in your secure password
7. When ready, select OK.

8. You can use the certificate on your eToken to sign code.

Password 101

> **Warning: The SafeNet eToken uses multiple passwords for Password is entered incorrectly five times, the eToken is per**

The SafeNet eToken uses the following passwords:

- Administrator Password:

  The default Administrator Password is "0" 48 times as provided by the manufacturer. If "this" password is lost, you are permanently locked out of the eToken and must purchase a new one. DigiCert does not set up this password.

- Token Password:

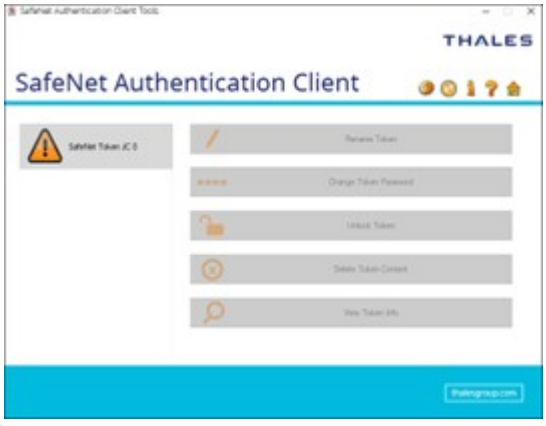
  This password is used to access the eToken certificate store. If lost, you can reset the eToken and reinstall the certificate.

- Personal Unlocking Key (PUK): Default PUK is 000000.

  DigiCert does not use the PUK in our process.

Troubleshooting

1. My token appears as "SafeNet Token JC 0."
Your eToken has been permanently disabled due to incorrect password attempts. Please contact DigiCert Support to order a new eToken.



2. I lost my Administrator password

2. I lost my Administrator password.
The administrator password is required to reset the device and is unrecoverable. Please contact DigiCert Support to order a new eToken.
Note: The manufacturer sets this password, not DigiCert.

3. I lost my Token password.
The Token Password is used to access the eToken certificate store. Use the Administrator Password to reset the eToken password if lost.
If you have lost your Token Password, you can reinitialize the eToken and create a new Token store when you reissue/rekey your certificate.

1. Reissue your certificate.
   - Reissue or re-key a Code Signing certificate
   - Reissue or re-key an EV Code Signing certificate
   - Rekeying Your DigiCert Document Signing Certificate

2. Re-initialize your eToken.
   After DigiCert reissues your certificate, install it on your eToken. See Install your code signing certificate on your hardware token.

Support

Products

Solutions

Cookie Settings