



PRECISION
BIOMETRIC

User Manual for InnaIT DSC

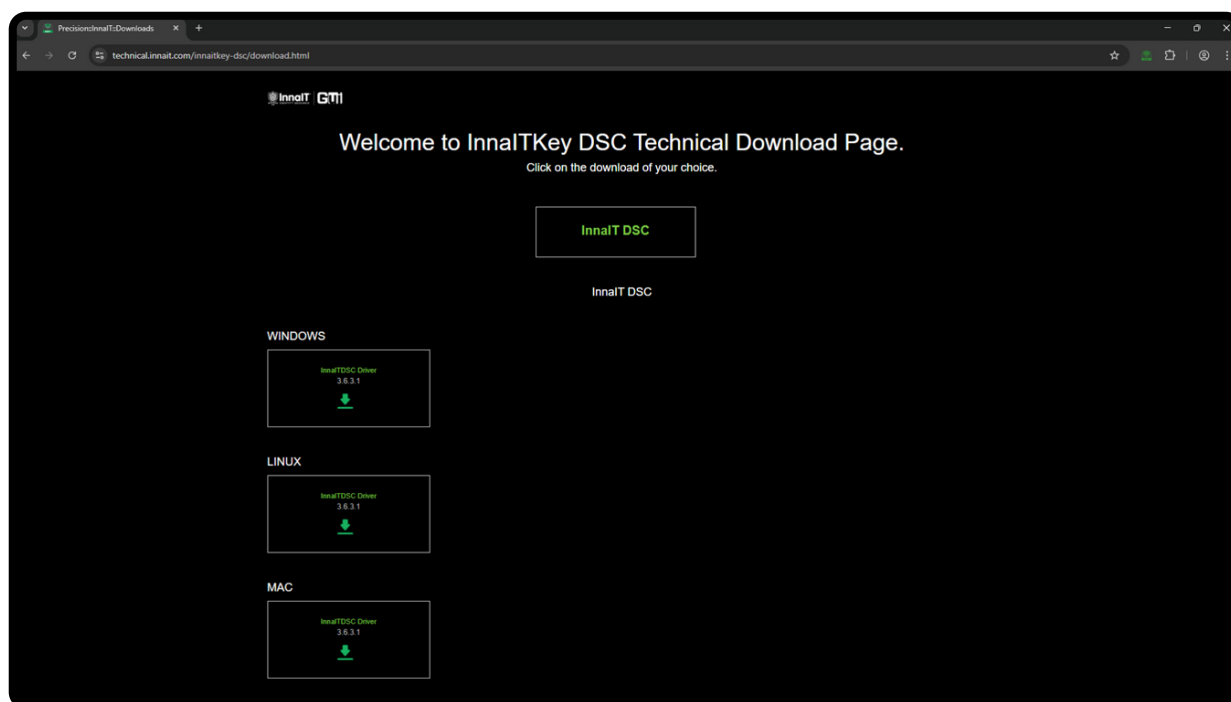
Contents

A. Download DSC Application	4 - 5
B. Software Installation (Windows)	6 - 7
C. Software Installation (Linux)	8 - 9
D. Software Installation (MacOS)	10
E. First Login (Non-Touch Token)	11 - 14
F. First Login (Biometric Token)	15 - 18
G. Fingerprint Enrollment	19 - 23
H. Fingerprint Management	24 - 27
I. Enable Single Sign On	28 - 32
J. Import Certificate (.cer)	33 - 36
K. Import PFX (.pfx)	37 - 40
L. View Certificate	41 - 42
M. View Key Details	43 - 44
N. Export Certificate	45 - 46

Contents

O. Delete Certificate	47 - 49
P. Update Software	50 - 52
Q. Renaming Token	53 - 54
R. Zeroize Key	55 - 57
S. Resetting Locked Token	58 - 60
T. Setting up Document Sign (Linux)	61 - 66
U. Signing a Document (Linux)	67 - 70
V. Setting up Document Sign (MacOS)	71 - 80
W. Signing a Document (MacOS)	81 - 85

A. Download DSC Application



Step 1 – Please go to “<https://technical.innait.com/innaitkey-dsc/download.html>” to download the InnaIT DSC Token Manager application.

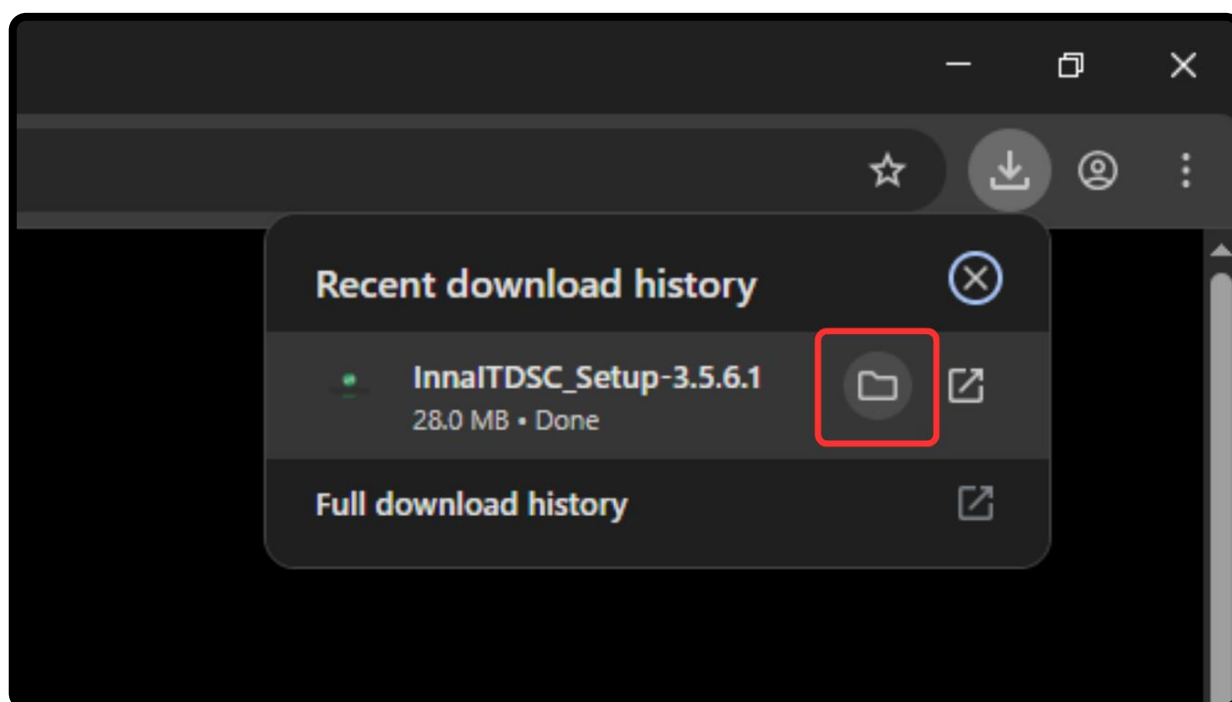


Step 2 – Here, find the appropriate variant of the Token Manager, based on the Operating System running on your PC.

A. Download DSC Application

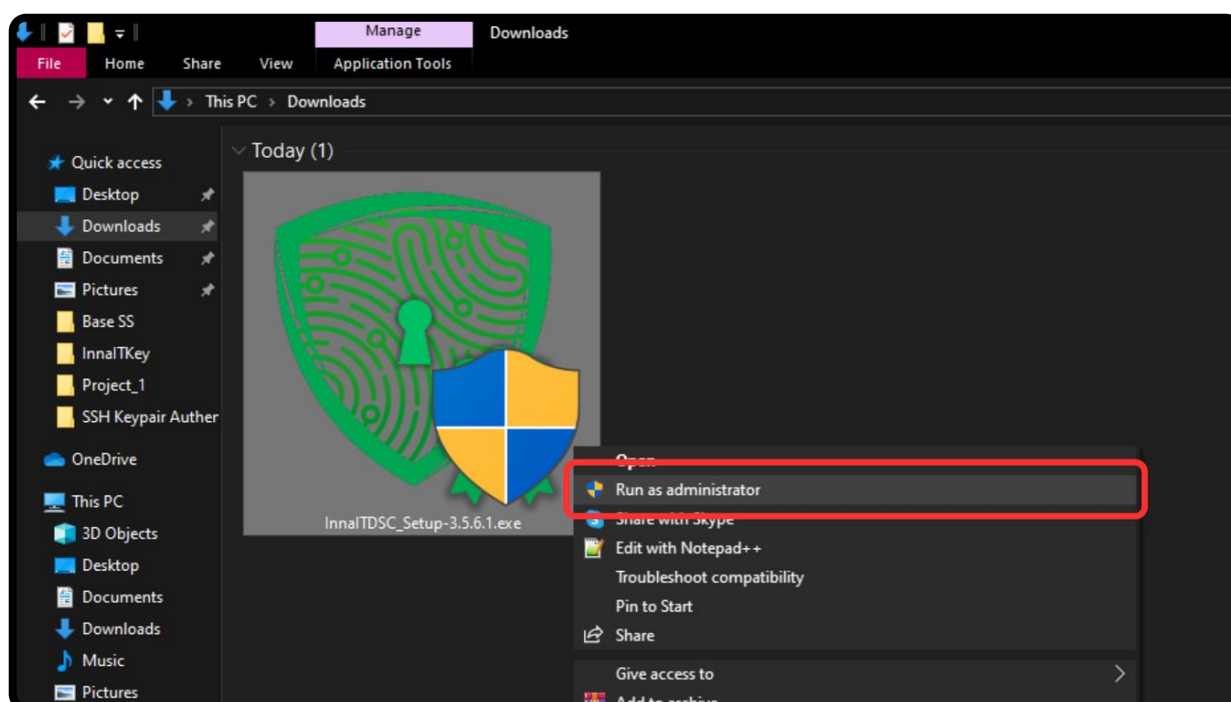


Step 3 – Click on the download button.

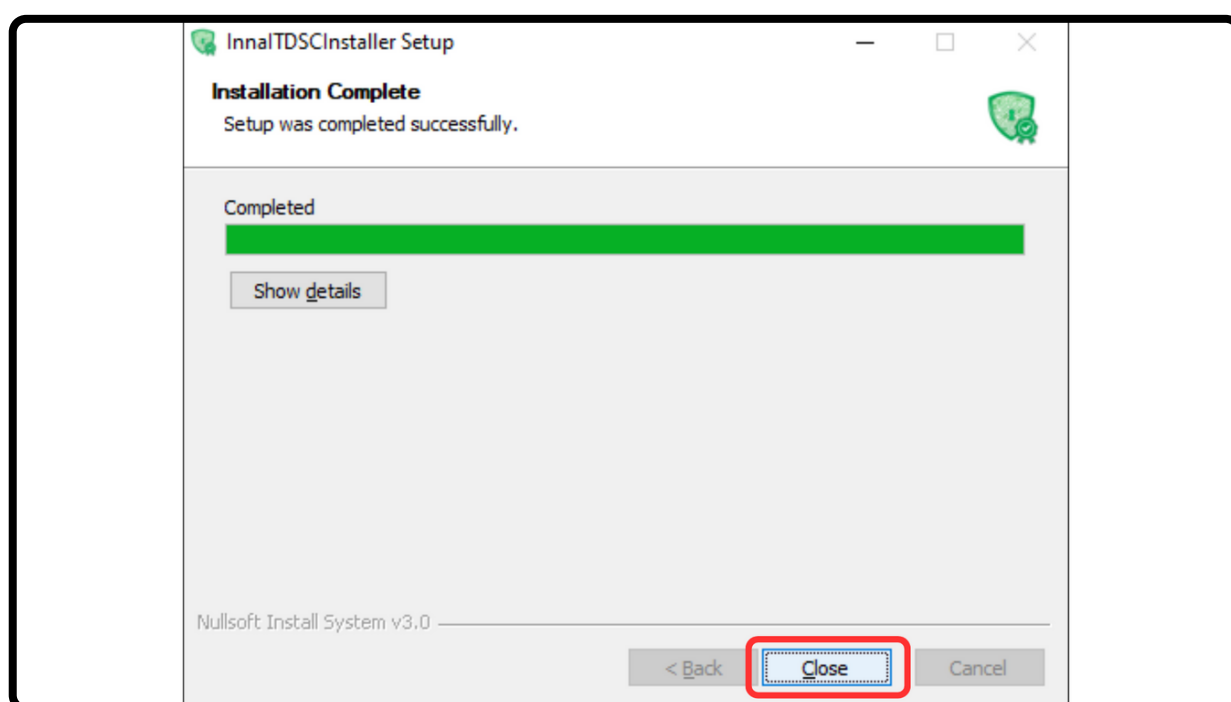


Step 4 – Once the download is complete, go to the location where it was saved.

B. Software Installation (Windows)

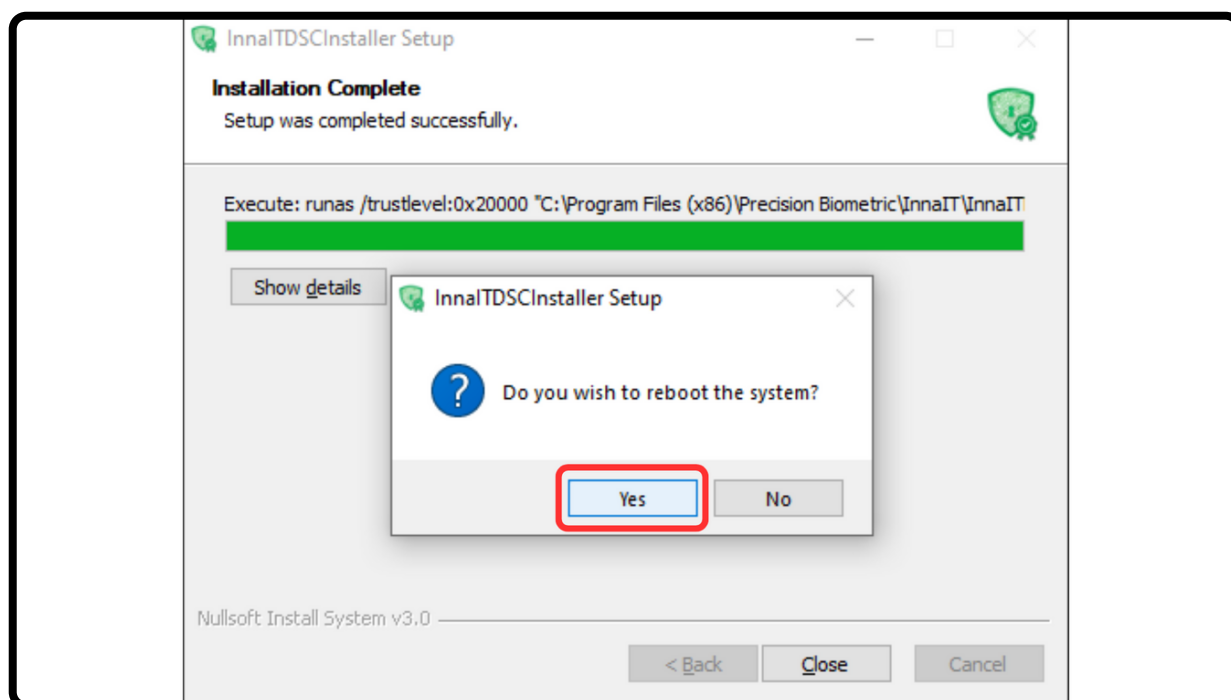


Step 1 – Right-click on the application and choose the “Run as administrator” option.

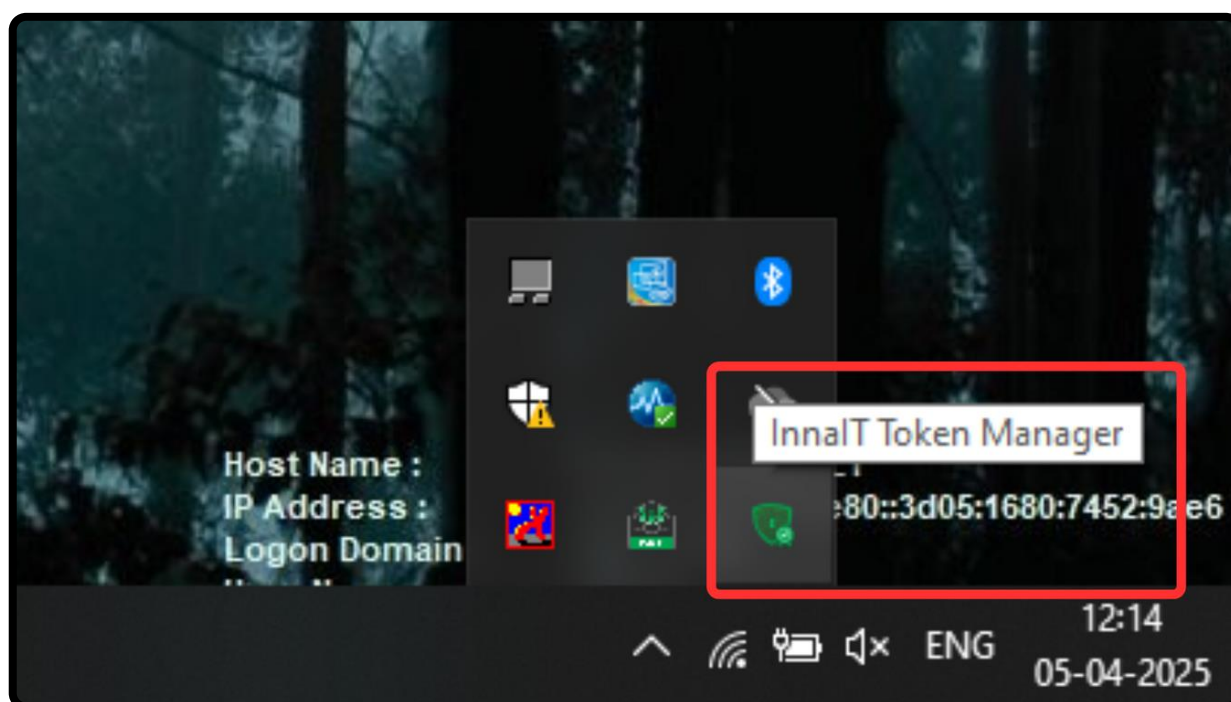


Step 2 – After the installation is complete, click on “Close”.

B. Software Installation (Windows)



Step 3 – You will now be asked to reboot your PC. Click on “Yes” to do so.



Info – After the restart is complete, you can start using the InnalT DSC Token Manager. You can find the icon to open the application in the system tray.

C. Software Installation (Linux)

Step 1 - Please go to "<https://technical.innait.com/innaitkey-dsc/download.html>" to download the InnaIT DSC Token Manager Package for Linux.

Step 2 - Now, open the terminal and go to the path where the package was downloaded, using the "cd" command.

Step 3 - Now, unzip the downloaded package using the following command.

```
tar -xvzf InnaITDSC-ubuntu22.tar.xz
```

Step 4 - Once the extraction is complete, go to the path using the following command.

```
cd InnaITDSC-ubuntu22
```

Step 5 - Use the following command to add execute permission to the shell script in the package.

```
chmod +x InnaITDSCSetup.sh
```

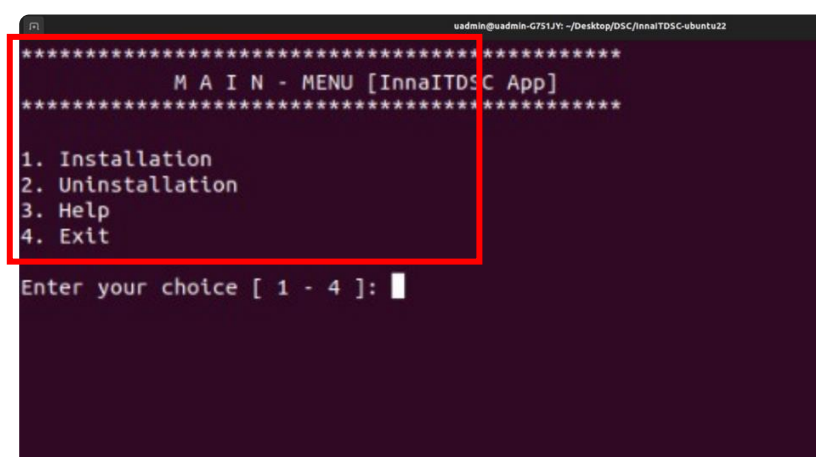
Step 6 - Now, run the shell (.sh) file.

```
./InnaITDSCSetup.sh
```

Note - Since some of the commands executed by the shell script (.sh) need "sudo" privileges, you need to enter the "sudo" password, when prompted. Alternatively, you can also directly run the shell script with "sudo" privileges by using the following command.

```
sudo ./InnaITDSCSetup.sh
```

Step 7 - You will see 4 options as shown in the below image



```
uadmin@uadmin-G751JY: ~/Desktop/DSC/innaitdsc-ubuntu22
*****
M A I N - M E N U [InnaITDSC App]
*****
1. Installation
2. Uninstallation
3. Help
4. Exit
Enter your choice [ 1 - 4 ]: █
```

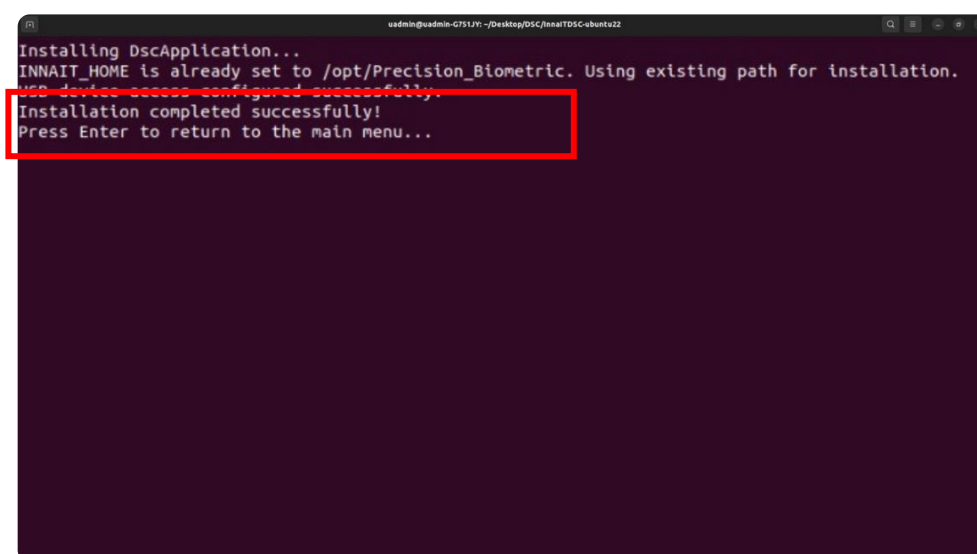
C. Software Installation (Linux)

Note - The function of these 4 options are explained below.

- 1.Installation - Begins the installation of the InnaIT DSC Token Manager on your Linux PC.
- 2.Uninstallation - Uninstalls any version of the InnaIT DSC Token Manager that is already installed on your Linux PC.
- 3.Help - Shows the details of the InnaIT DSC Token Manager.
- 4.Exit - Stops the execution of the shell script (.sh) and exits the current terminal session.

Step 8 - Now, press the "1" key and press the "Enter" key to begin the installation.

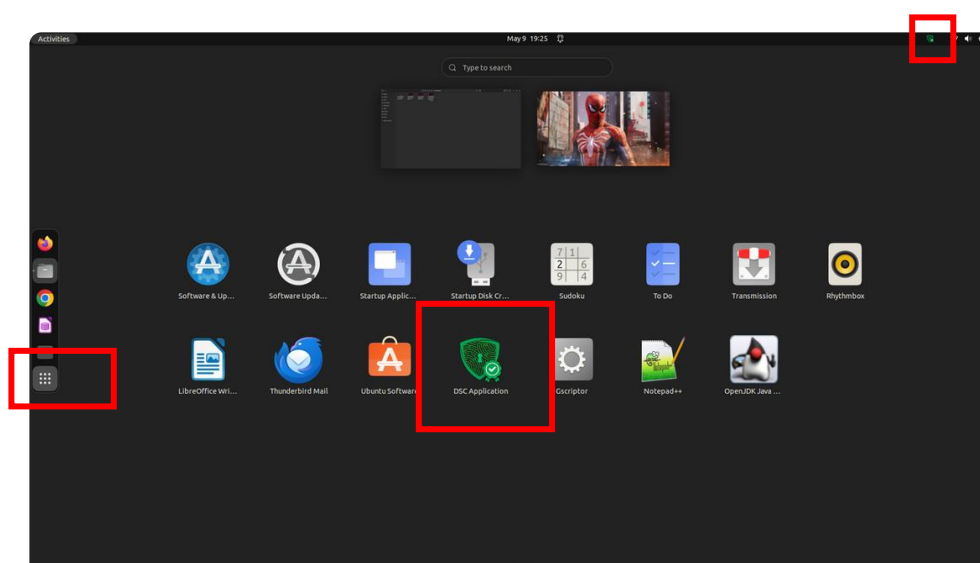
Step 9 - Once it is complete, you will get the "Installation Completed Successfully!" message.



```
Installing DscApplication...  
INNAIT_HOME is already set to /opt/Precision_Biometric. Using existing path for installation.  
USB device access configured successfully.  
Installation completed successfully!  
Press Enter to return to the main menu...
```

Step 10 - Hit the "Enter" key to return to the main menu and then press the "4" key and "Enter" again, to exit the installer.

Step 11 - You can find the InnaIT DSC Token Manager icon in the Applications List and on the Activities Bar of your Linux PC, as shown below. Click on it to start the application.



D. Software Installation (MacOS)

Step 1 - Please go to "<https://technical.innait.com/innaitkey-dsc/download.html>" to download the InnaIT DSC Token Manager Package for MacOS.

Step 2 - Extract the package to a folder of your choosing.

Step 3 - Now, open the terminal and go to the folder where the package was extracted to, using the "cd" command.

Step 4 - Using the following command, allow execution permission for the InnaITDSCSetup.sh file within the package.

```
chmod 755 InnaITDSCSetup.sh
```

Step 5 - Now, we can begin the installation. Run the following command to do so. You will be prompted to enter your "sudo" password as this command requires elevated permissions.

```
./InnaITDSCSetup.sh
```

Note - Once the execution begins, you will see 4 options as shown in the below image.

```
*****
M A I N - MENU [InnaITDSC App]
*****
1. Installation
2. Uninstallation
3. Help
4. Exit
Enter your choice [ 1 - 4 ]: █
```

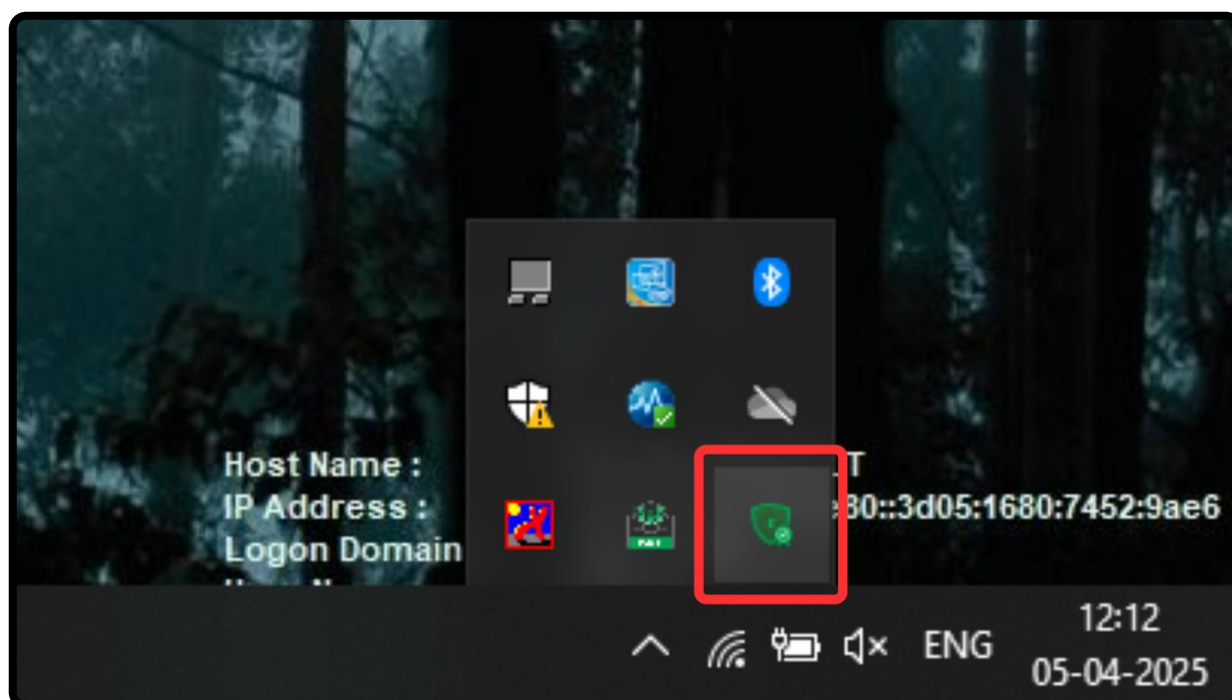
Note - The function of these 4 options are as follows.

- 1.Installation - Begins the installation of the InnaIT DSC Token Manager on your Mac.
- 2.Uninstallation - Uninstalls any version of the InnaIT DSC Token Manager that is already installed on your Mac.
- 3.Help - Shows the details of the InnaIT DSC Token Manager.
- 4.Exit - Stops the execution of the installer and exits the current terminal session.

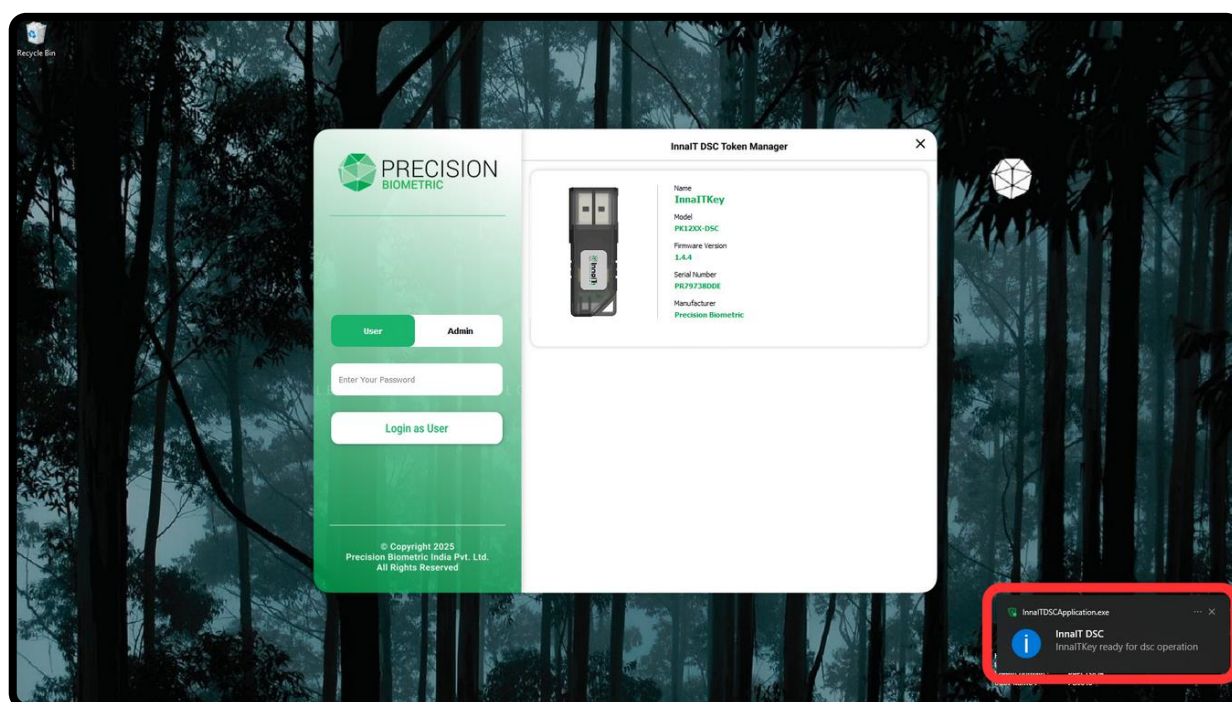
Step 6 - Now, press the "1" key and press the "Enter" key to begin the installation.

Step 7 - Once it is complete, you will get the "Installation Completed Successfully!" message. Hit the "Enter" to return to the main menu and then press the "4" key and "Enter" again, to exit the installer.

E. First Login (Non-Touch Token)

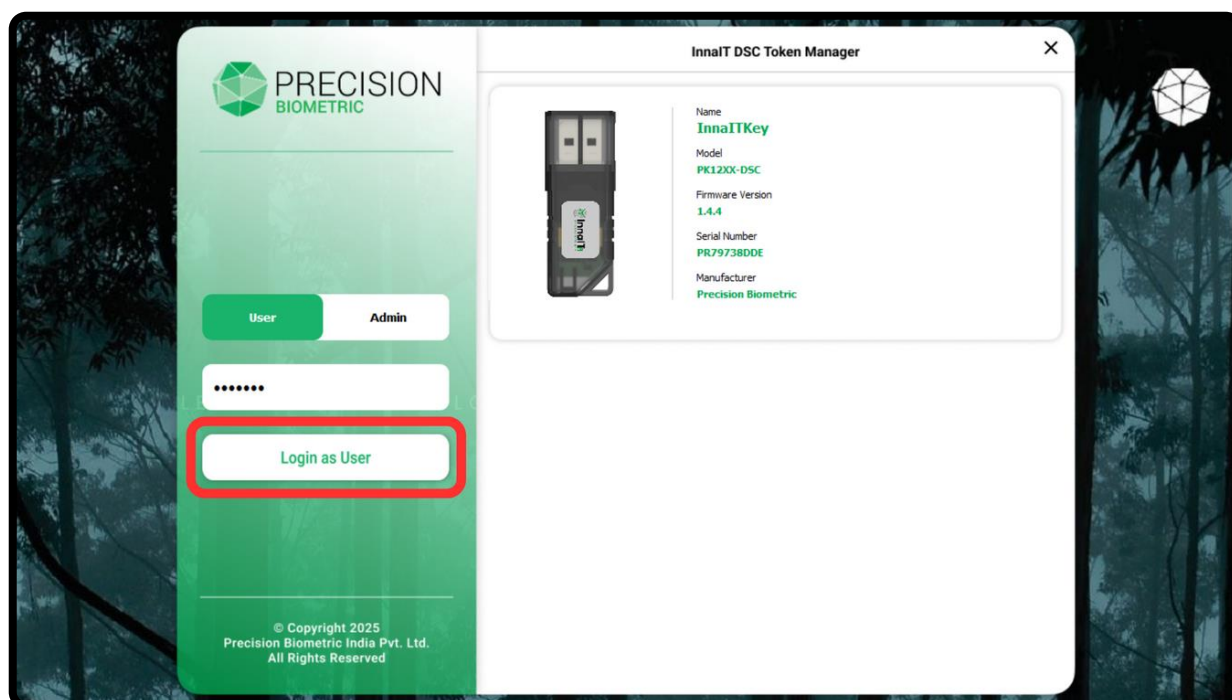


Step 1 – Click on the InnaIT DSC Token Manager app icon on your system tray and connect the InnaIT DSC token to your PC.



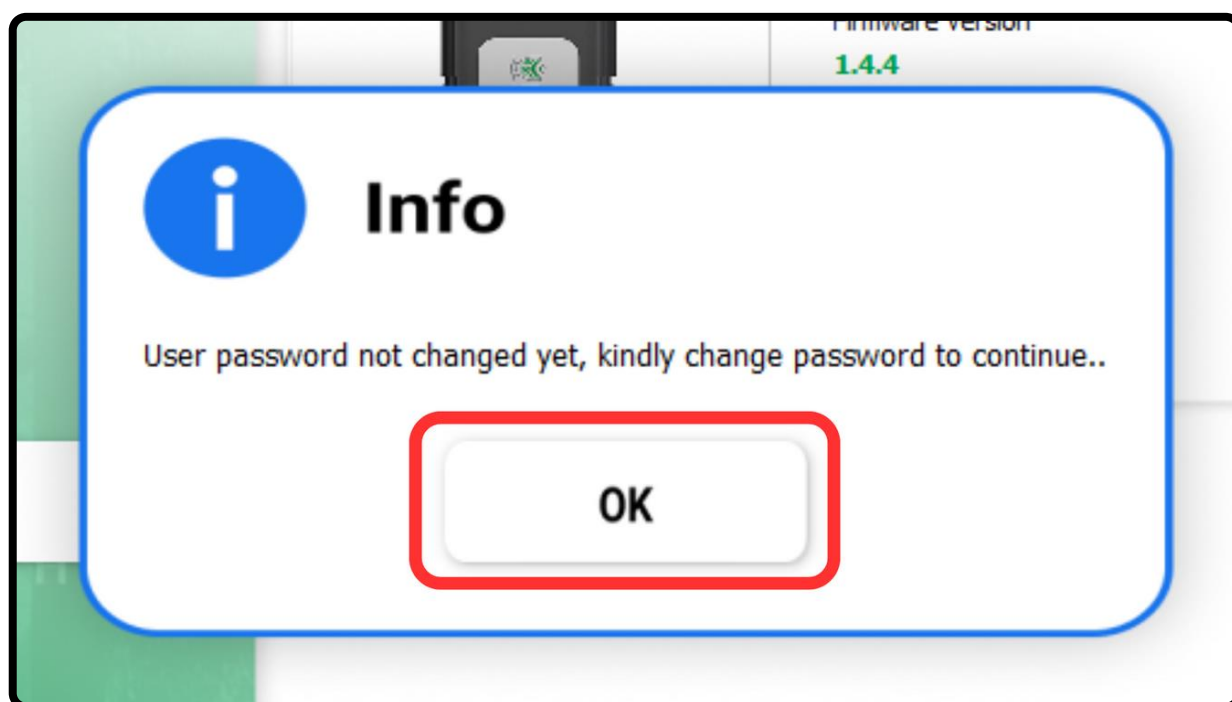
Info – You will get a notification on the bottom right which says “InnaITKey is ready for DSC Operation” once the token is detected. The token’s details will also appear in the application window.

E. First Login (Non-Touch Token)



Step 2 – With your token connected, enter the default password in the “Password” field and click on “Login as User”

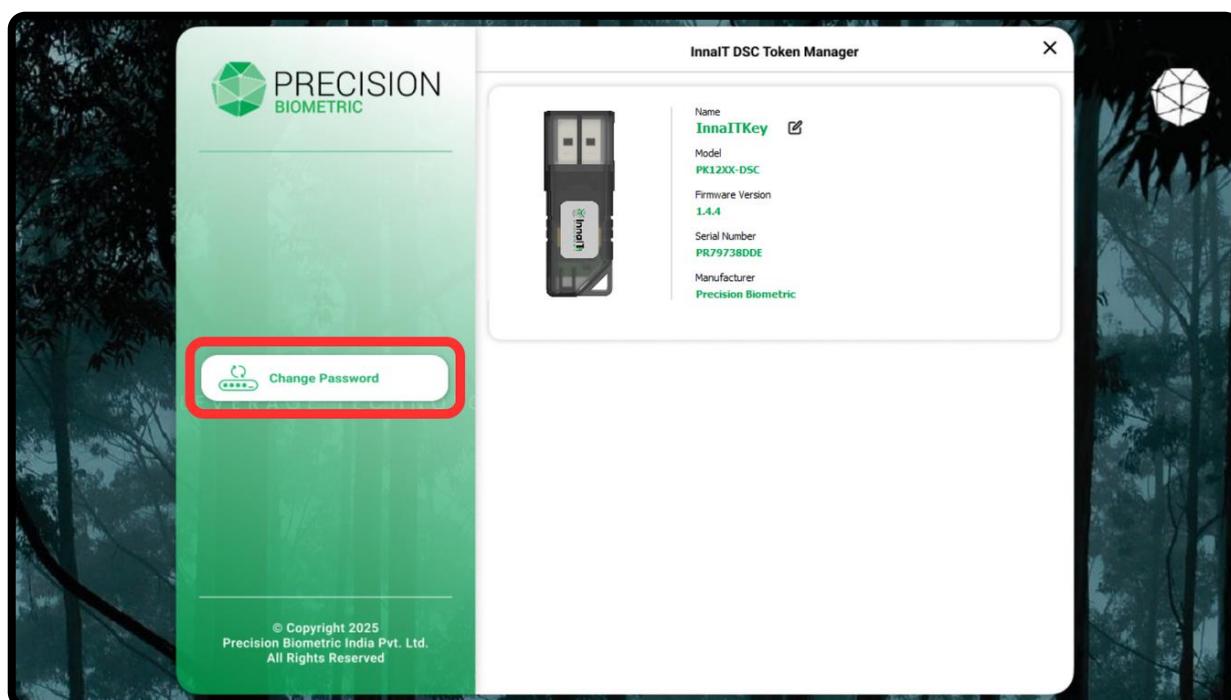
Note: The default password is **123456**.



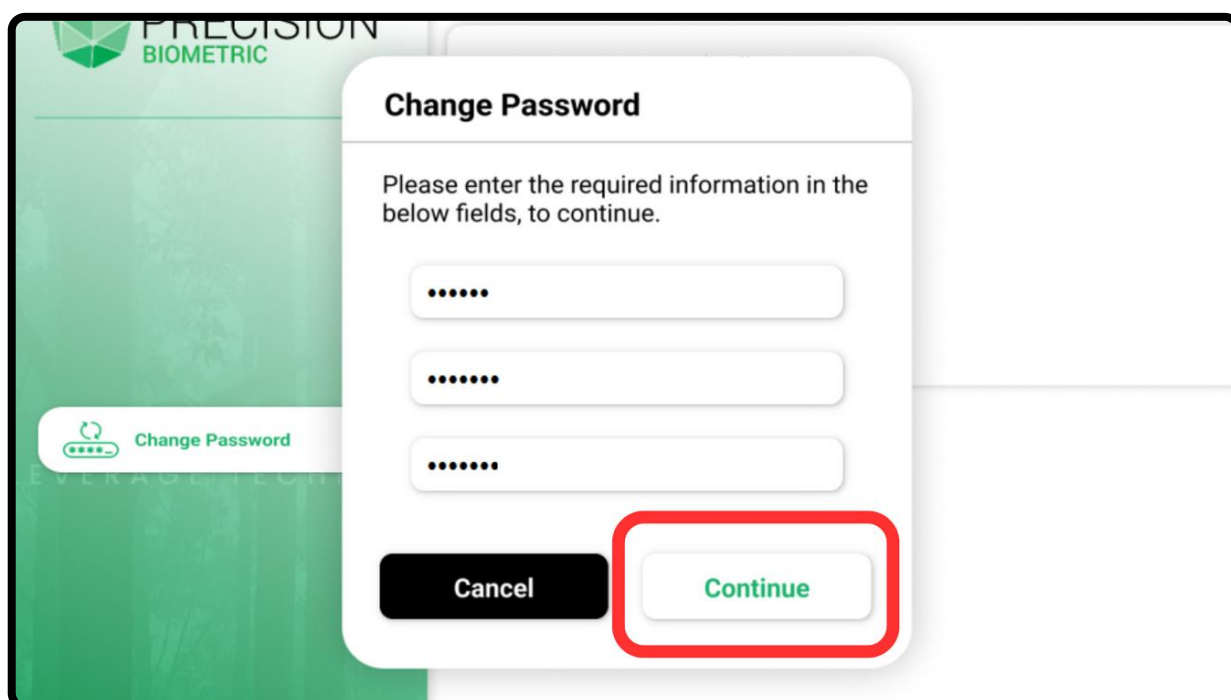
Step 3 – After logging in, you will be prompted to change your password. Click on “OK” to continue.

Note: You will not be able to perform any functions until your password is changed.

E. First Login (Non-Touch Token)

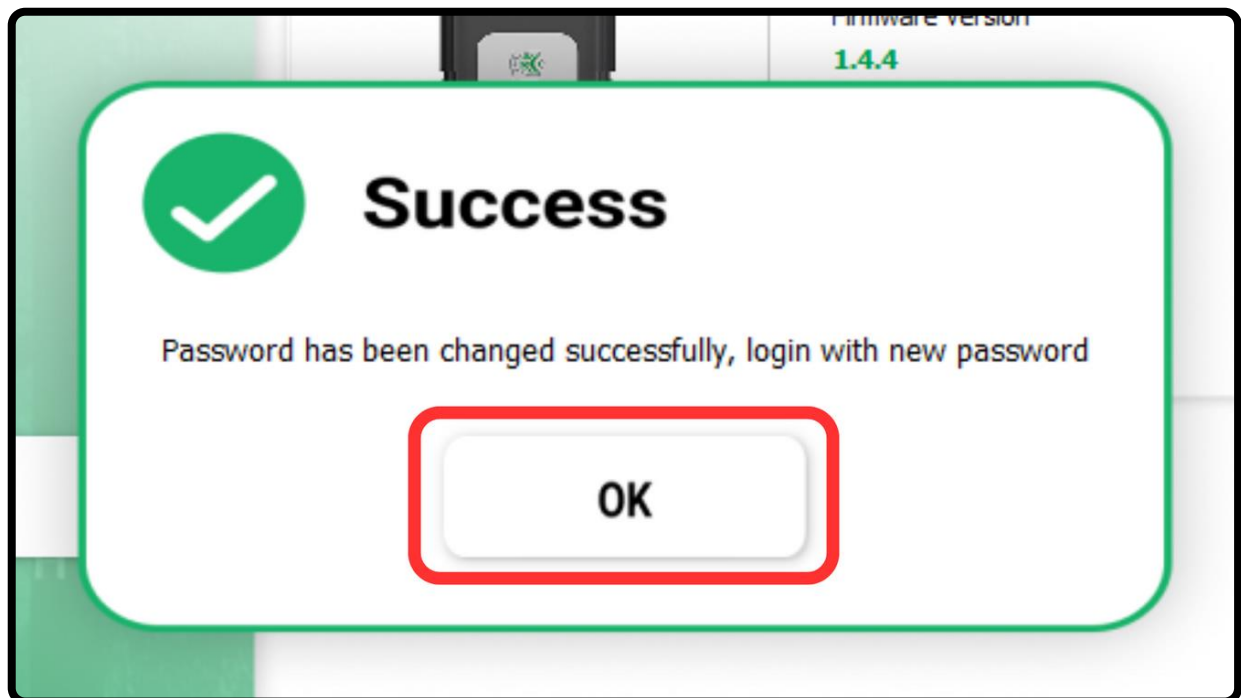


Step 4 – Now, click on the “Change Password” button.

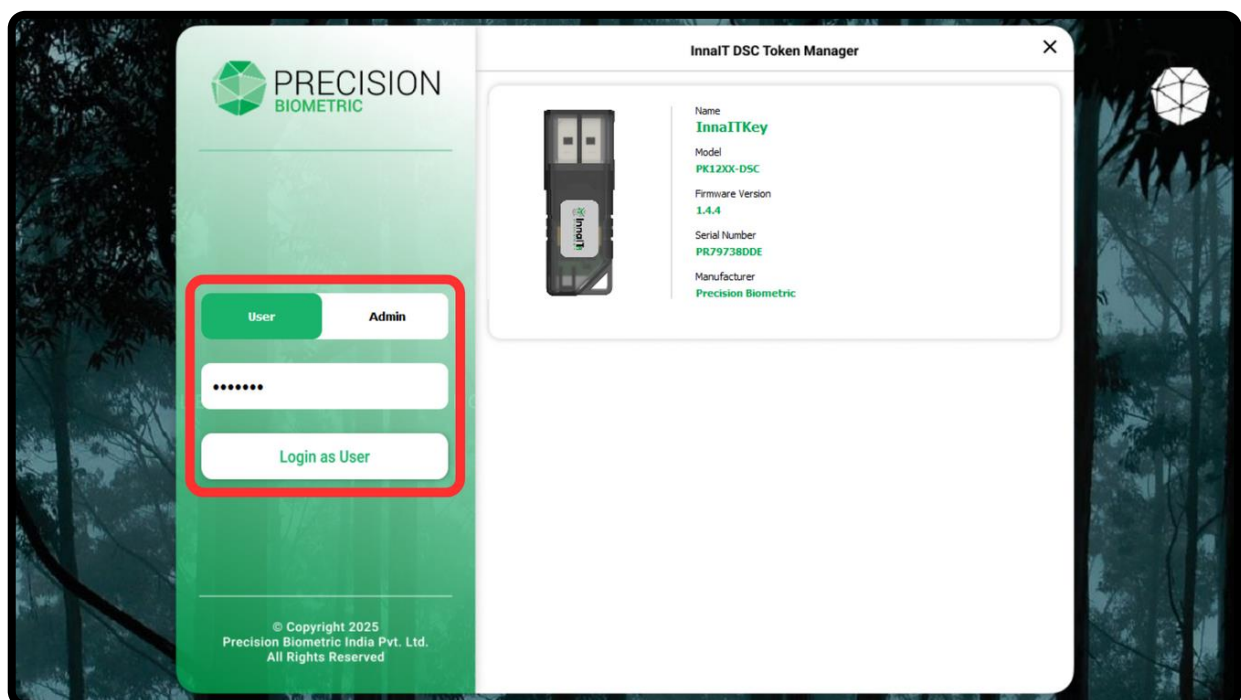


Step 5 – In this pop-up, enter your old password, new password and confirm your new password. Click on “Continue” to confirm the change.

E. First Login (Non-Touch Token)

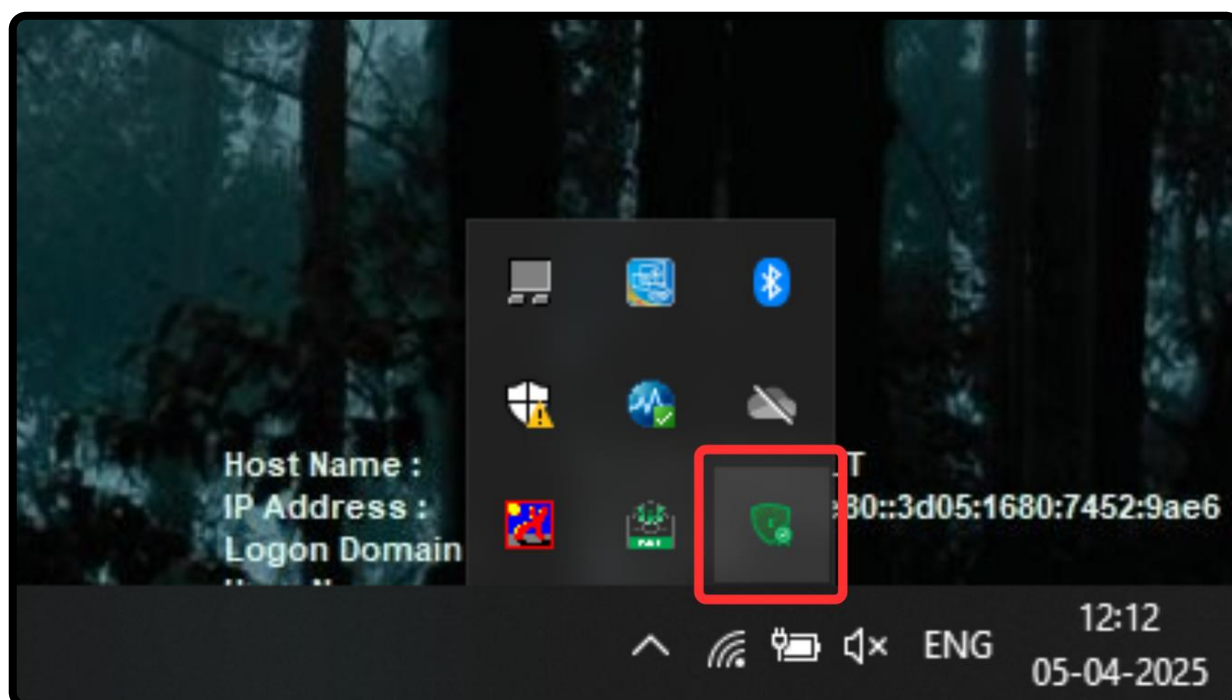


Step 6 – You will get a “Success” dialogue box. Once you click on “OK” you will be logged out.

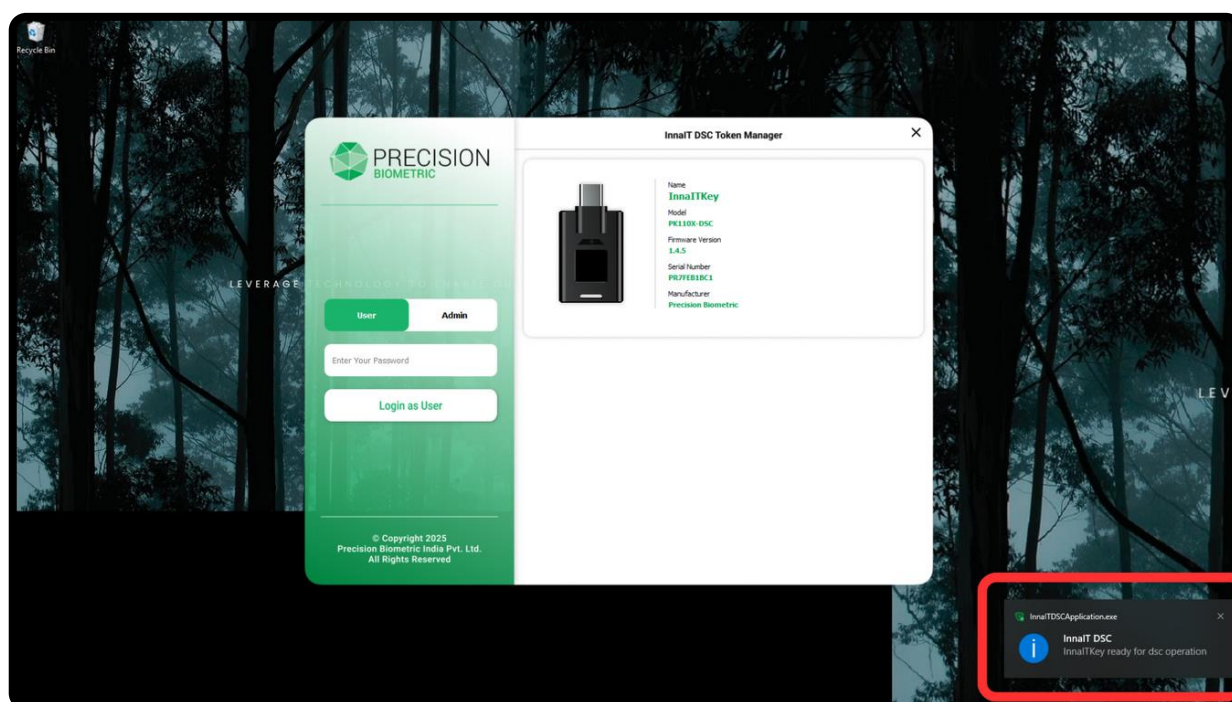


Step 7 – Please login now using your new user password to access other token functions.

F. First Login (Biometric Token)

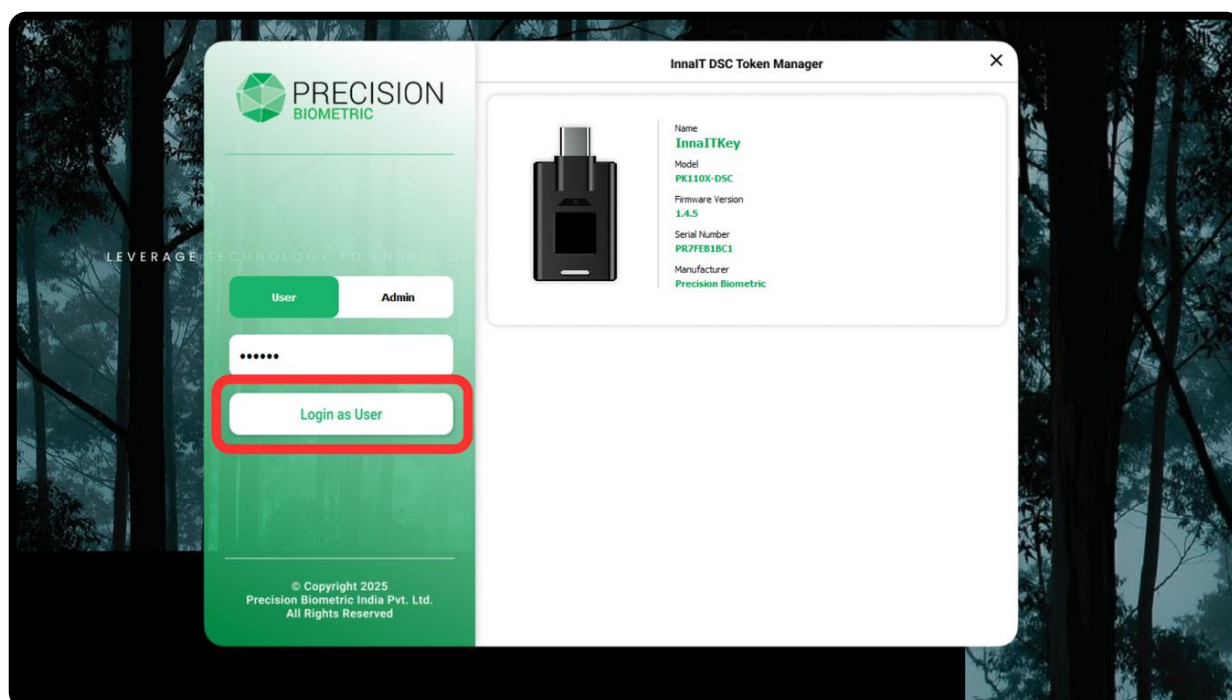


Step 1 – Click on the InnaIT DSC Token Manager app icon on your system tray and connect the InnaIT DSC token to your PC.



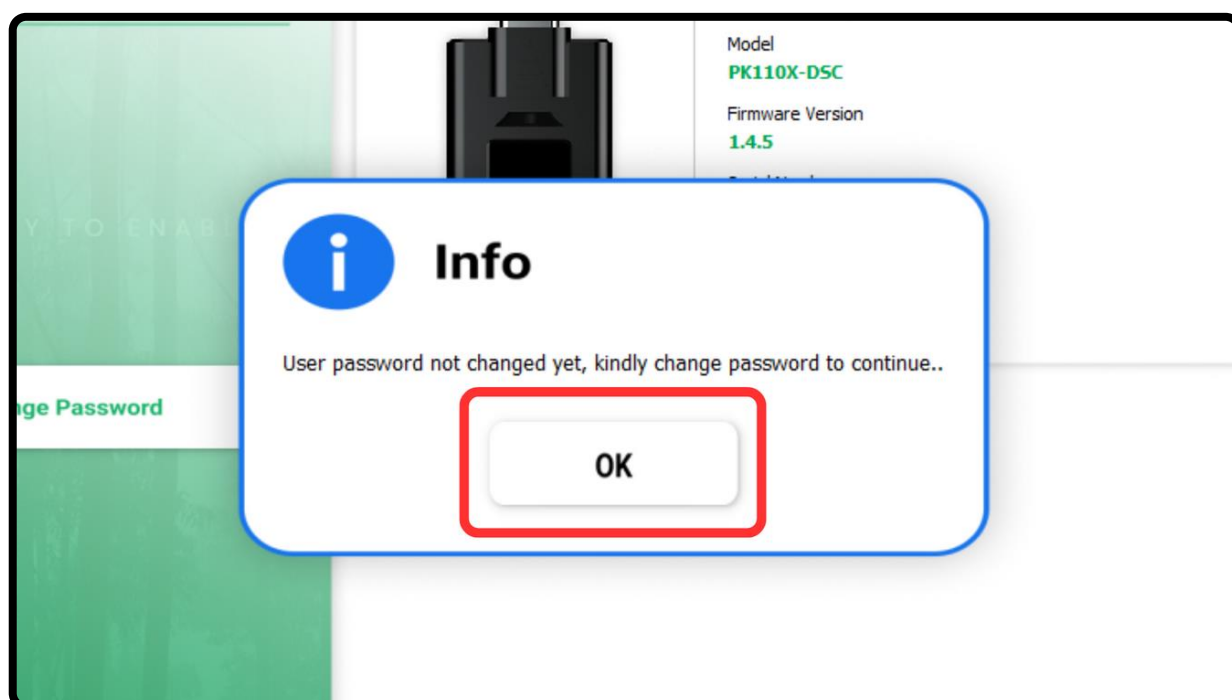
Info – You will get a notification on the bottom right which says “InnaITKey is ready for DSC Operation” once the token is detected. The token’s details will also appear in the application window.

F. First Login (Biometric Token)



Step 2 – With your token connected, enter the default password in the “Password” field and click on “Login as User”

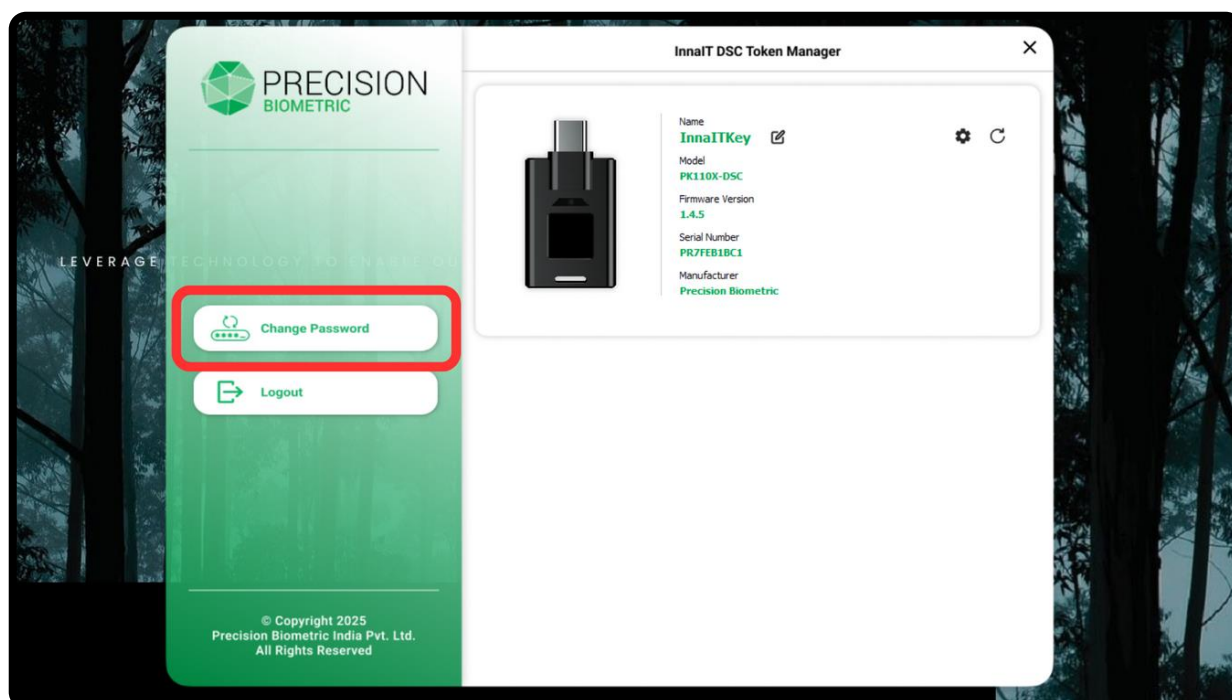
Note: The default password is **123456**.



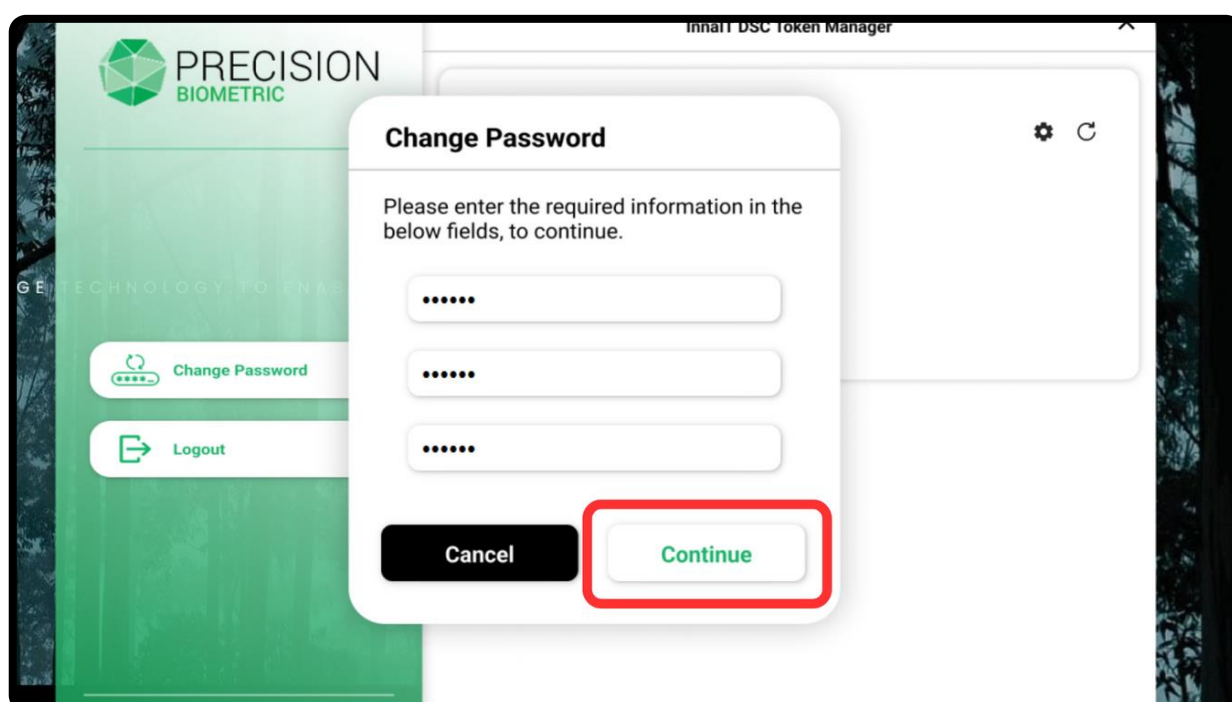
Step 3 – After logging in, you will be prompted to change your password. Click on “OK” to continue.

Note: You will not be able to perform any functions until your password is changed.

F. First Login (Biometric Token)

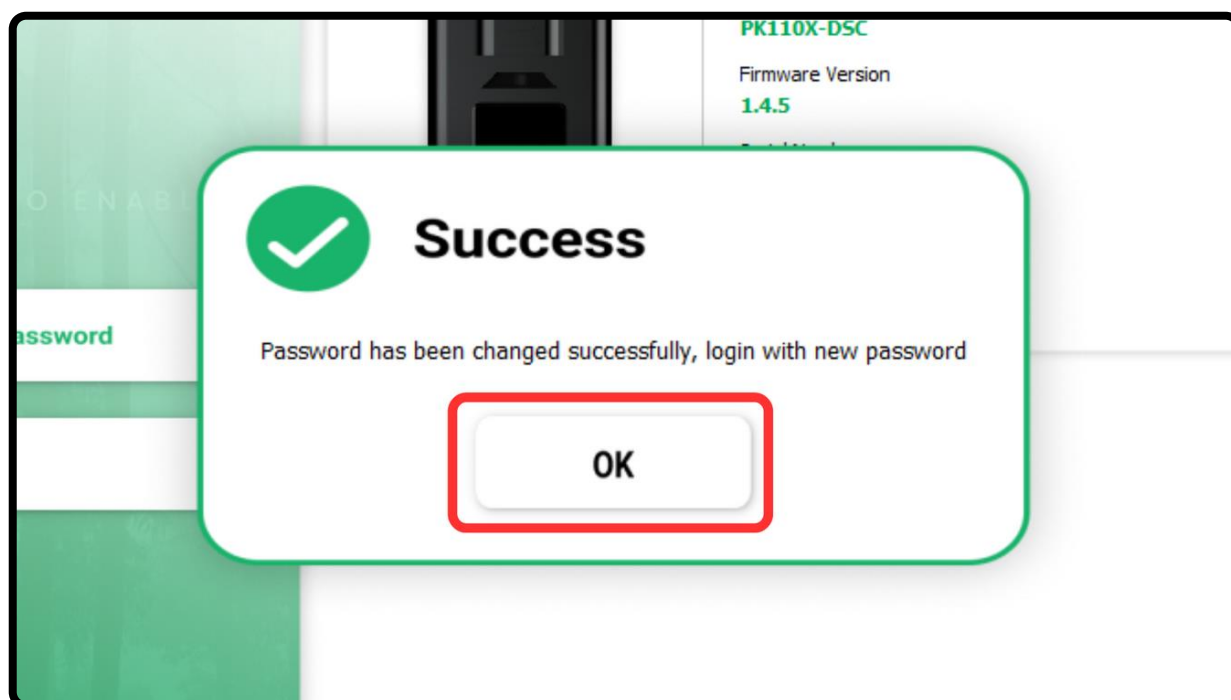


Step 4 – Now, click on the “Change Password” button.

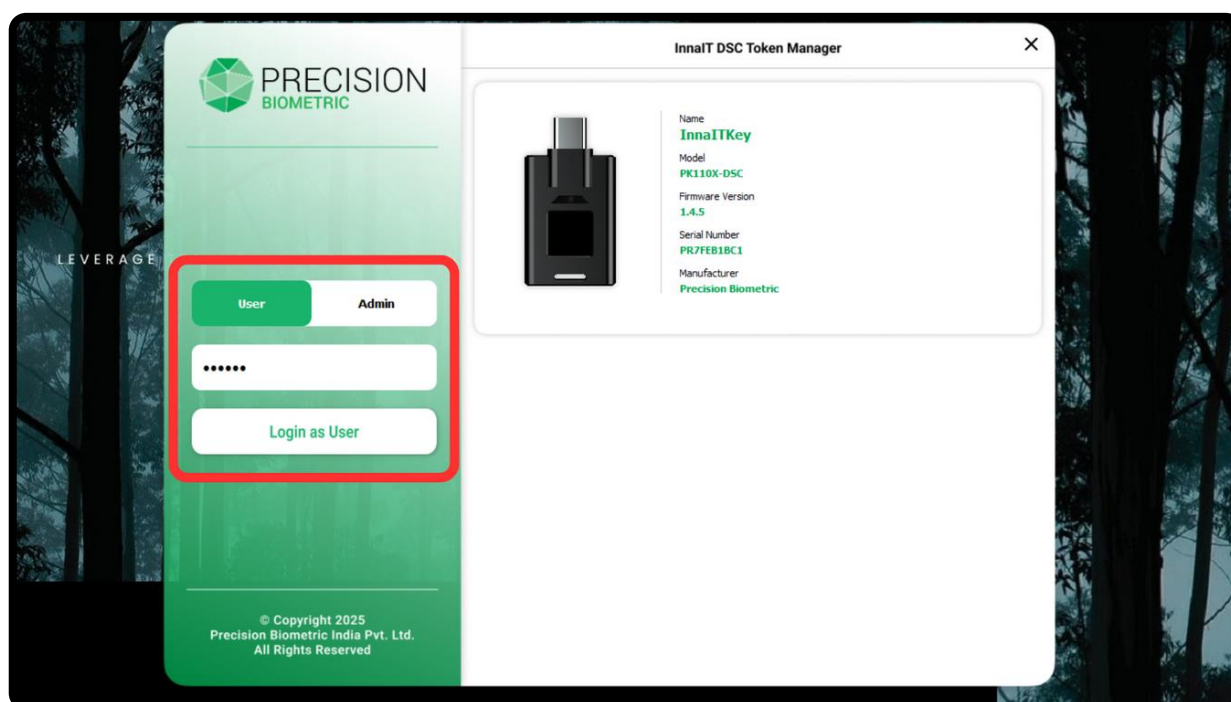


Step 5 – In this pop-up, enter your old password, new password and confirm your new password. Click on “Continue” to confirm the change.

F. First Login (Biometric Token)

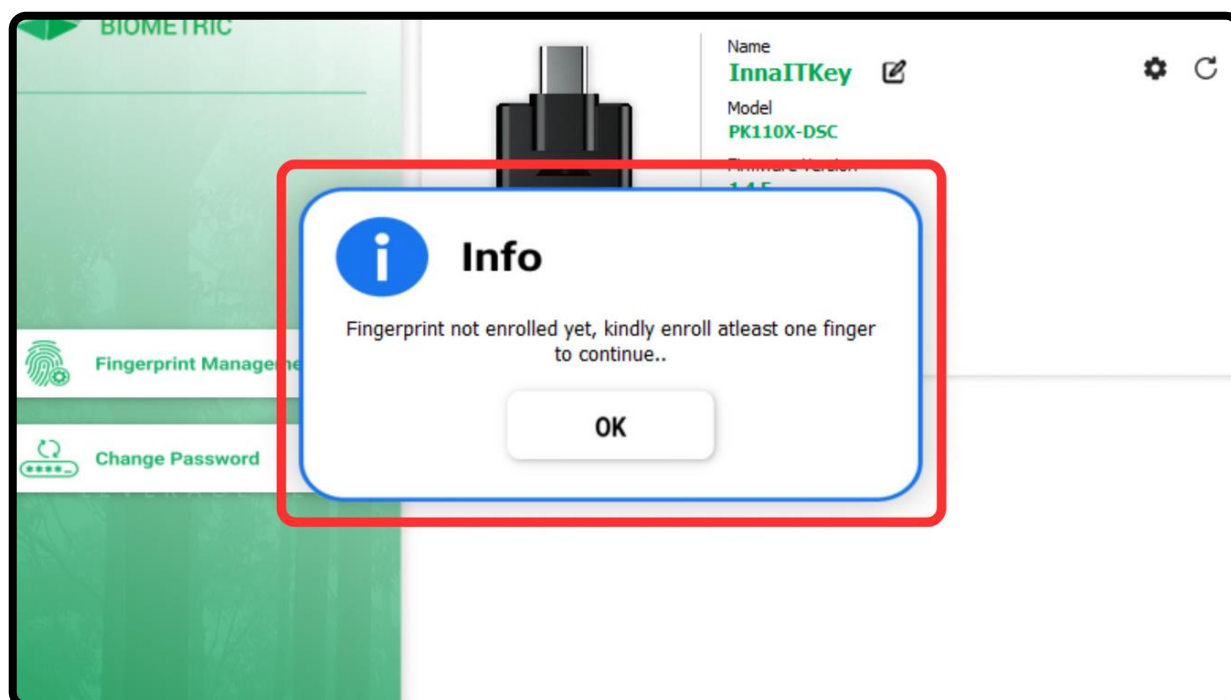


Step 6 – You will get a “Success” dialogue box. Once you click on “OK” you will be logged out.

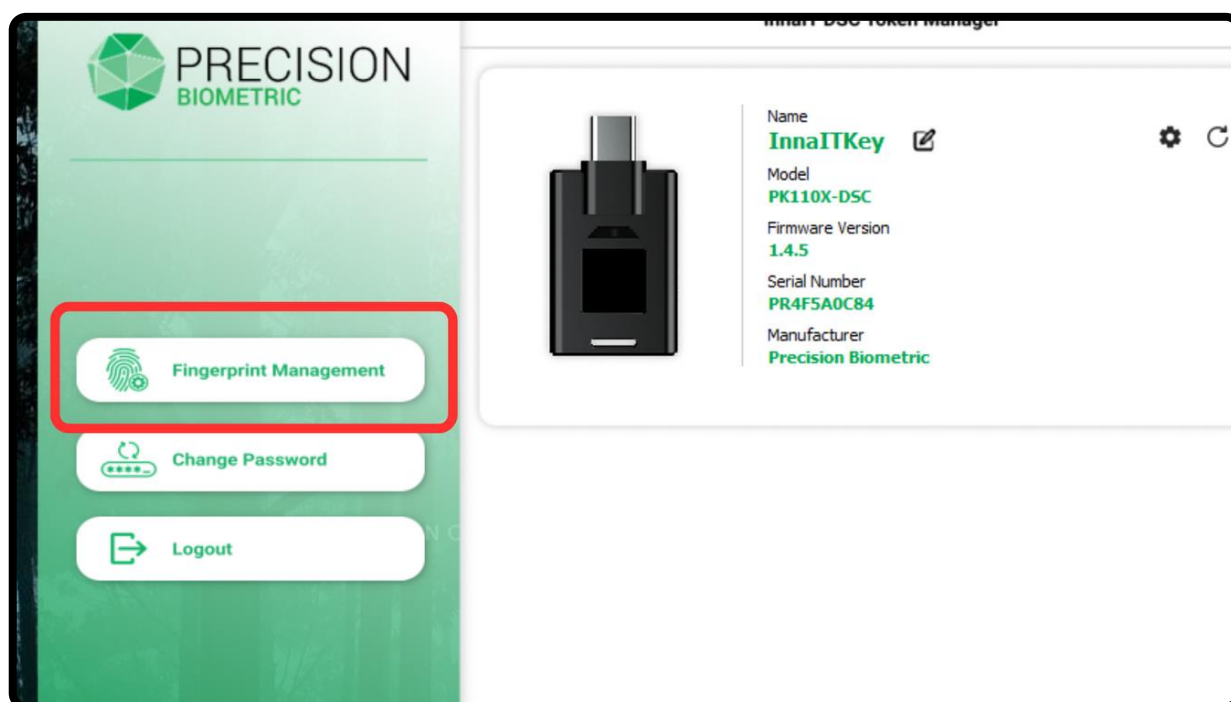


Step 7 – Please login now using your new user password to access other token functions.

G. Fingerprint Enrollment

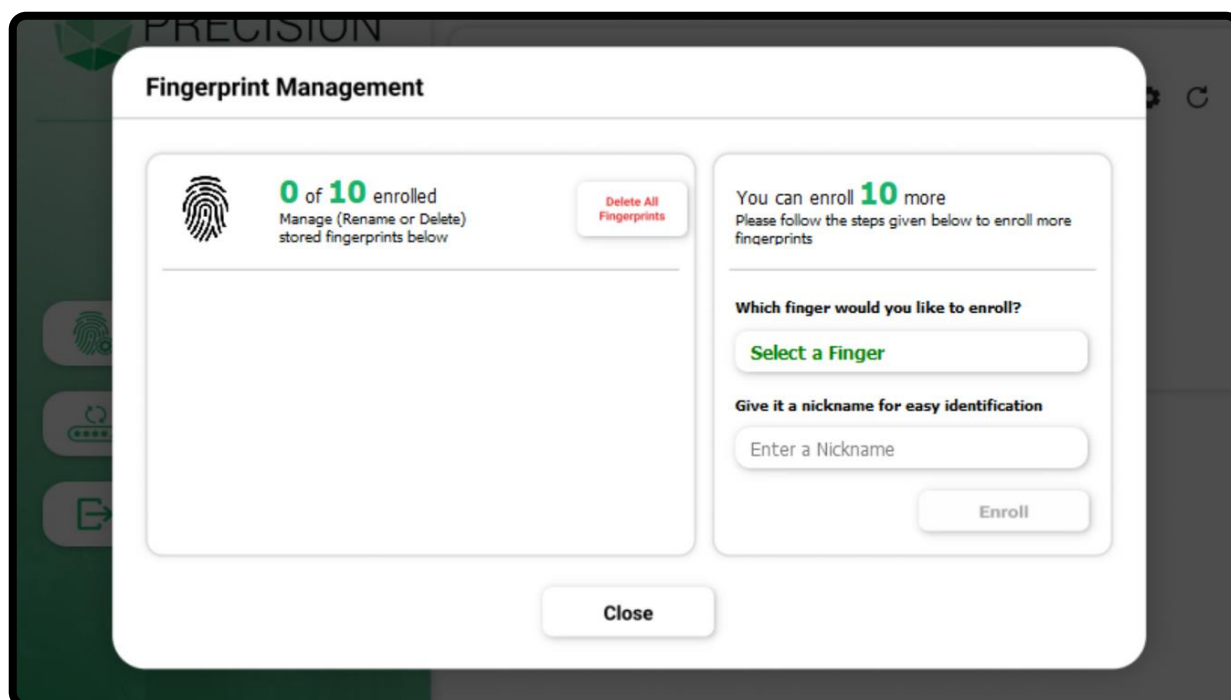


Step 1 – When logging in for the first time after changing your user password, you will be prompted to enroll at least one fingerprint. Click on “OK” to continue.

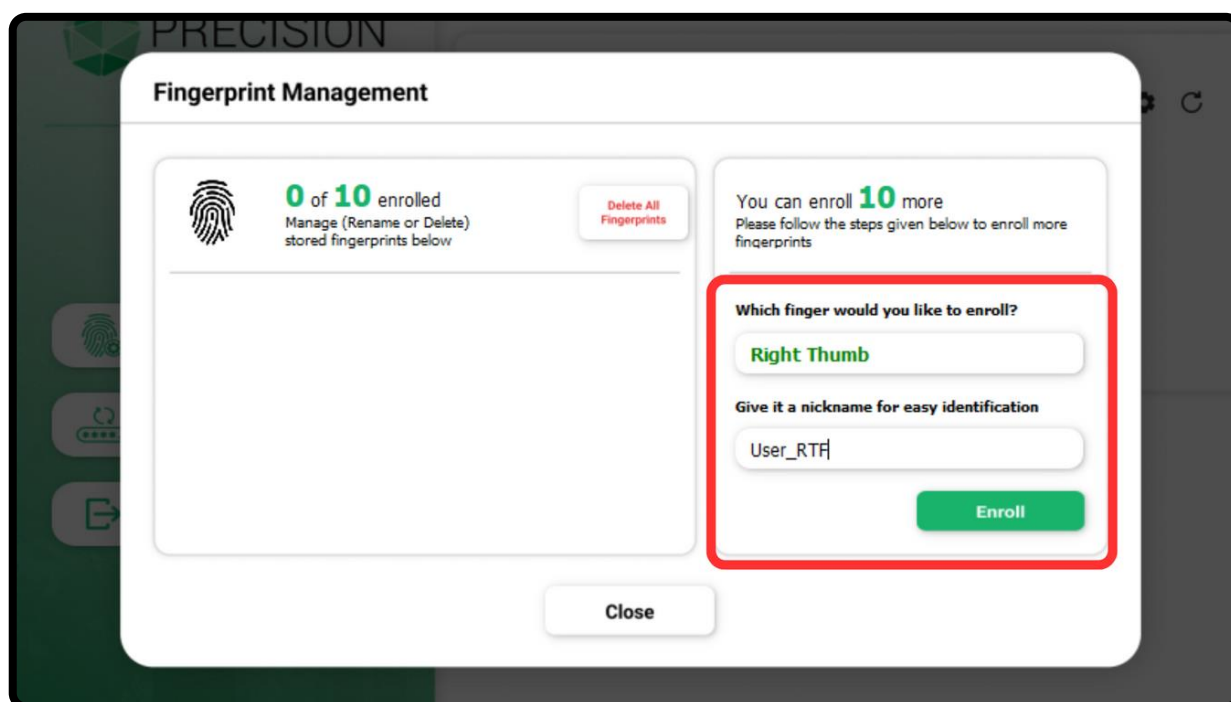


Step 2 – Now, click on to the “Fingerprint Management” button.

G. Fingerprint Enrollment

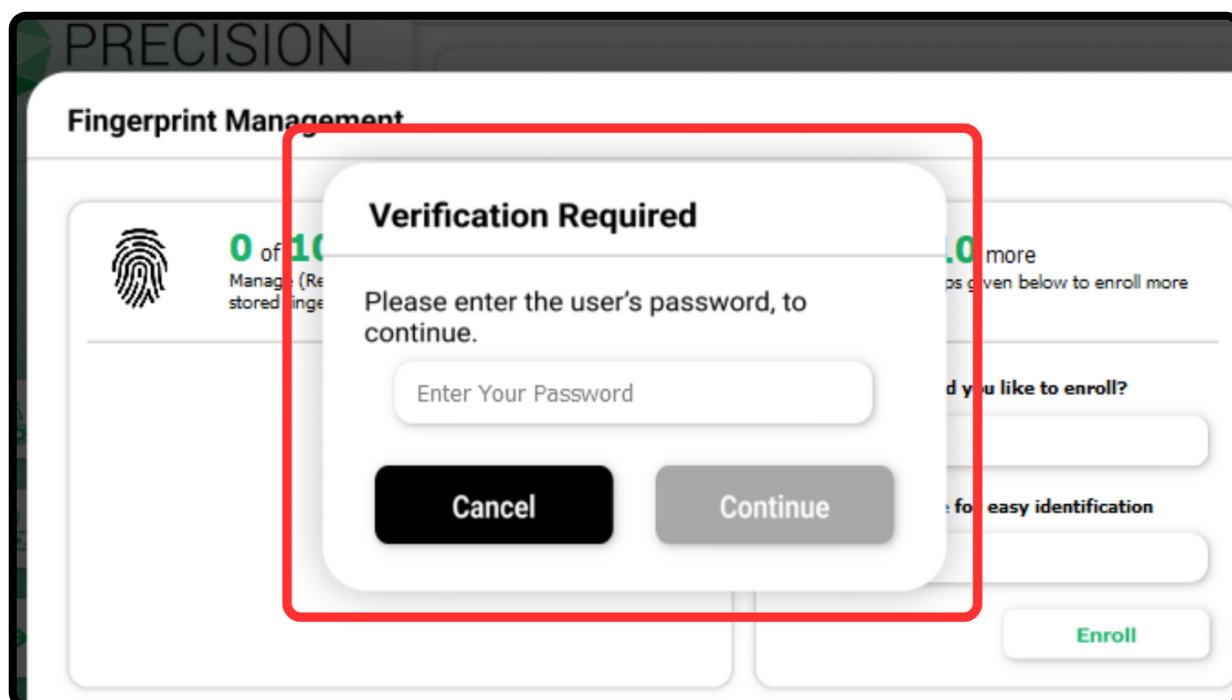


Step 3 – In the “Fingerprint Management” window, you can see a list of enrolled fingerprints and how many more can be enrolled.

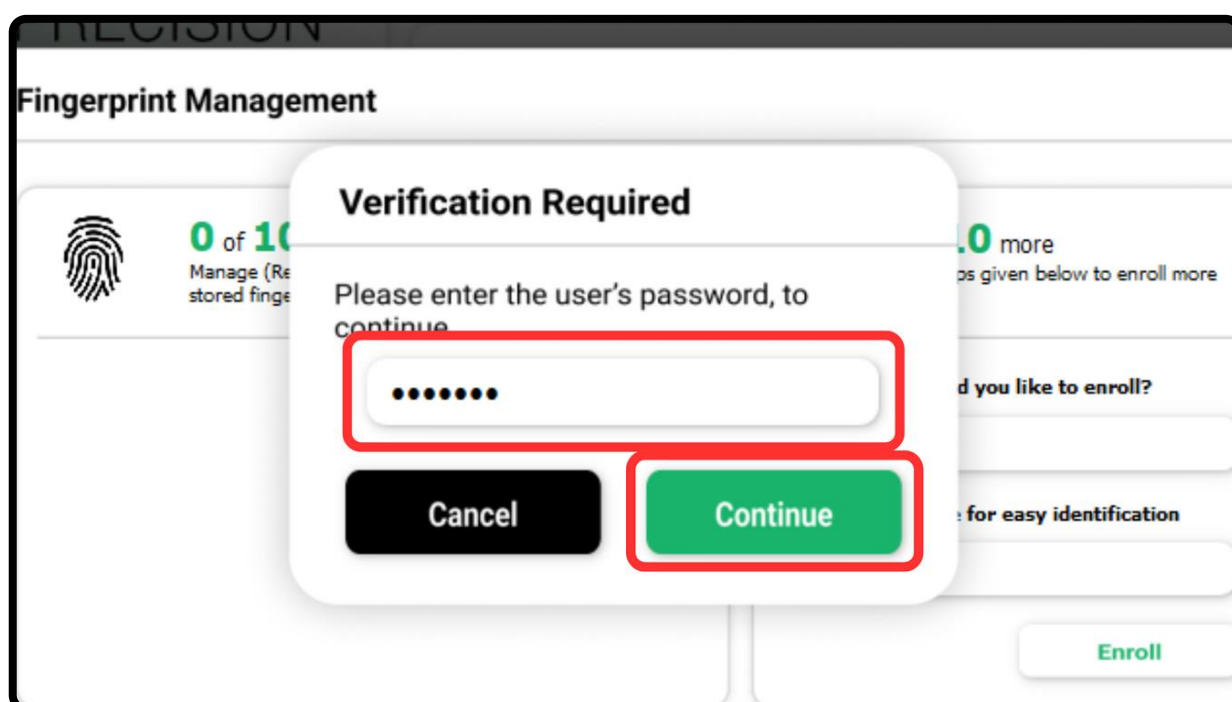


Step 4 – Now, select a finger that you would like to enroll, and give it a nickname. Click on the “Enroll” button to begin enrollment.

G. Fingerprint Enrollment

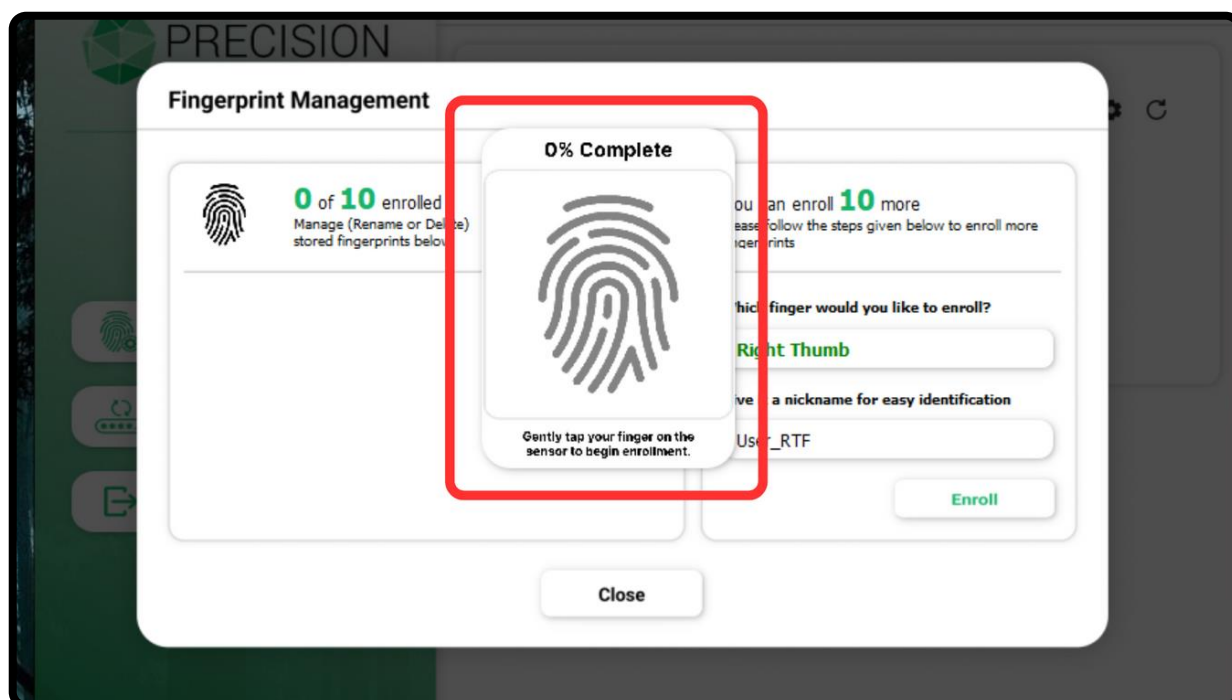


Step 5 – After clicking the “Enroll” button you will be prompted to enter your user password for verification.

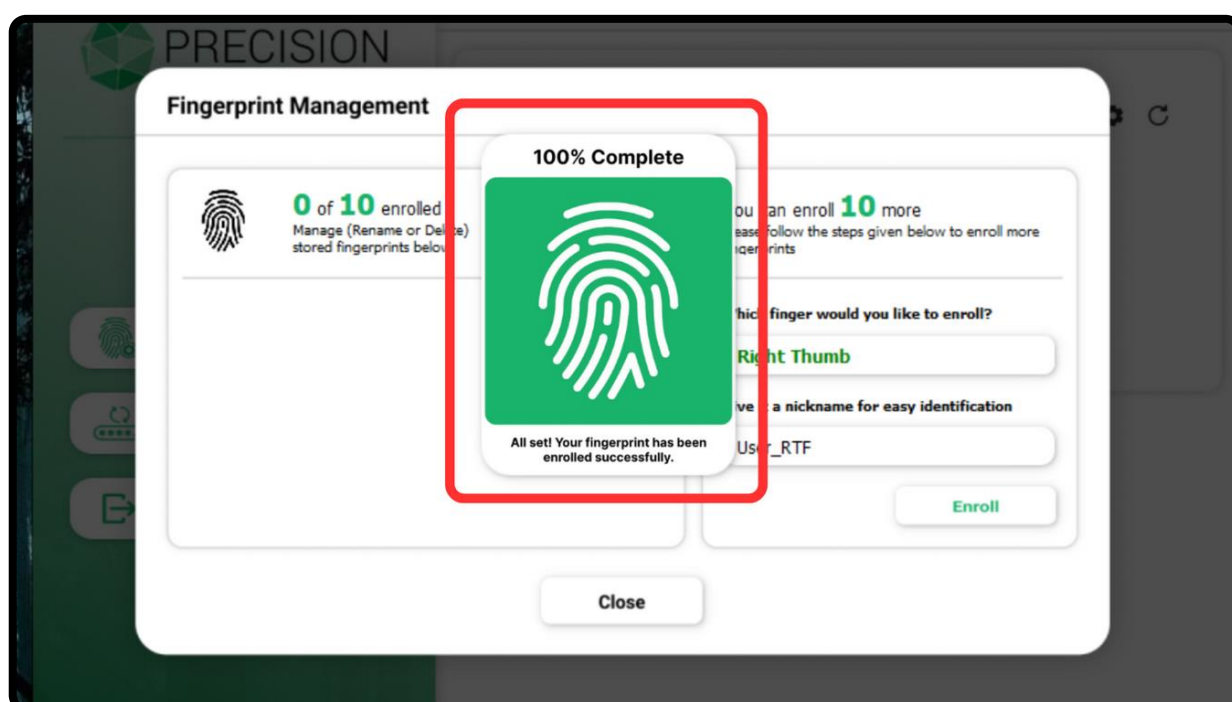


Step 6 – Enter your user password in the given field and click on “Continue” to proceed.

G. Fingerprint Enrollment

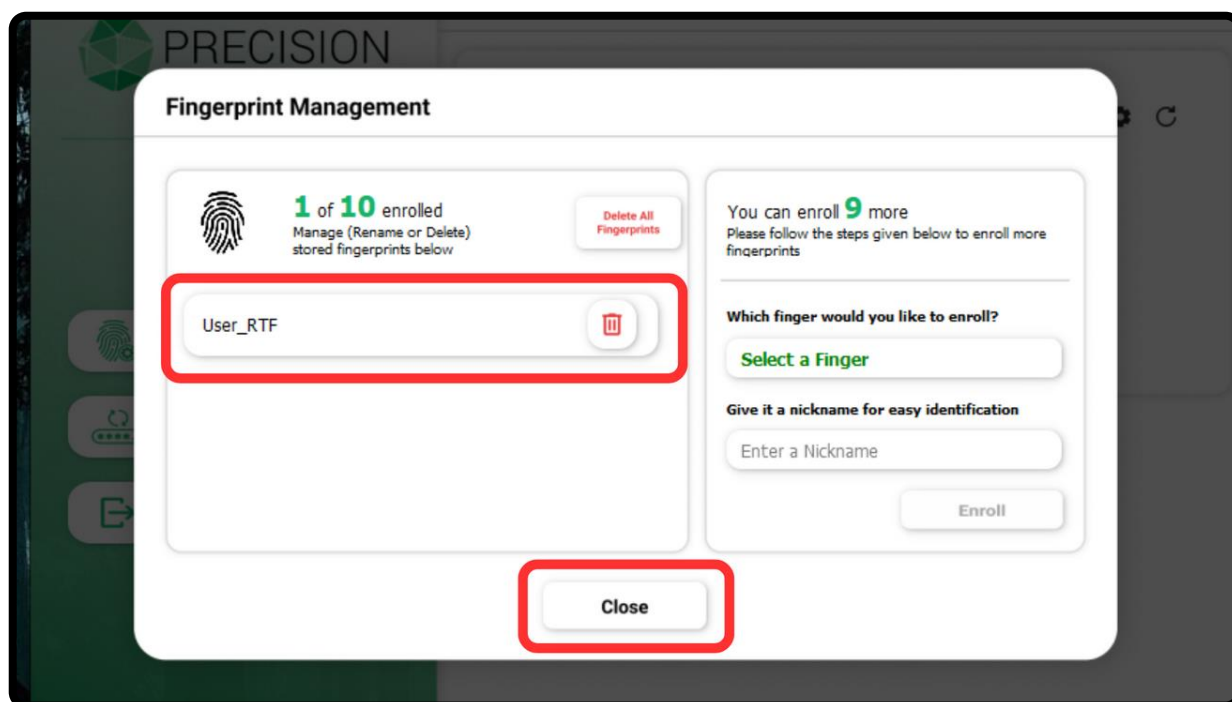


Step 7 – Once the light on the token starts flashing in blue, gently place your finger on the token's sensor multiple times, in multiple orientations to enroll your fingerprint.



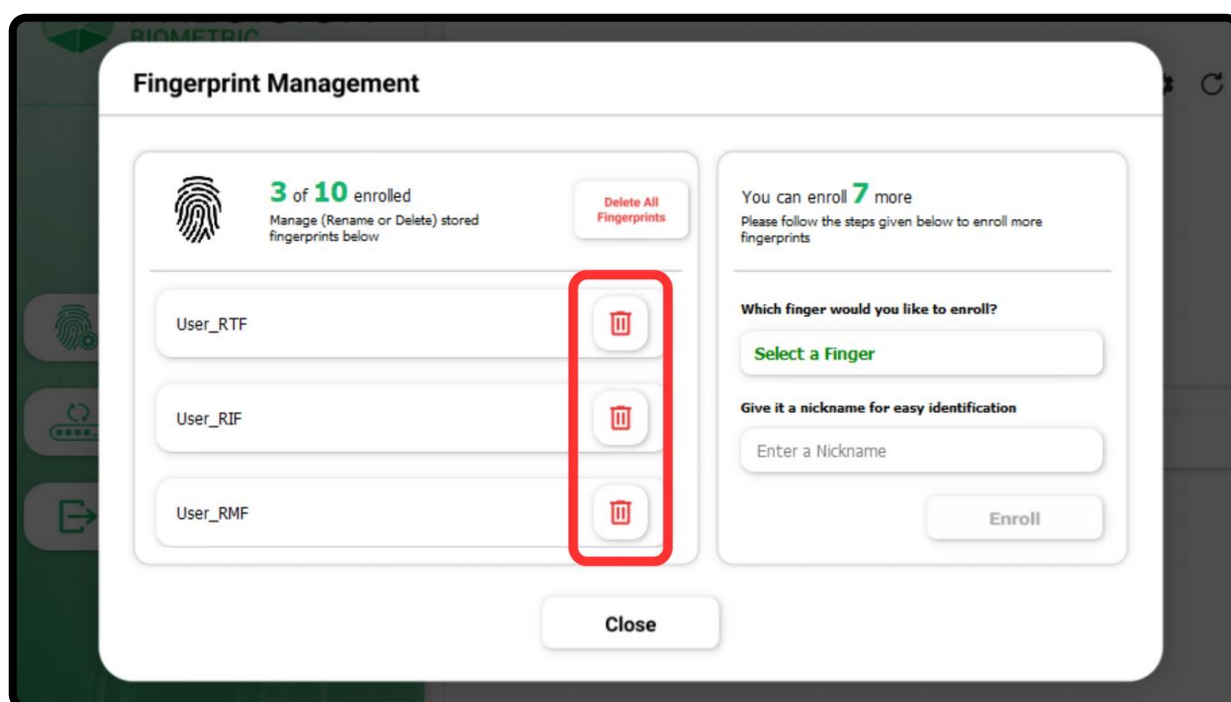
Step 8 – Once the progress bar reaches 100%, your fingerprint has been successfully enrolled.

G. Fingerprint Enrollment

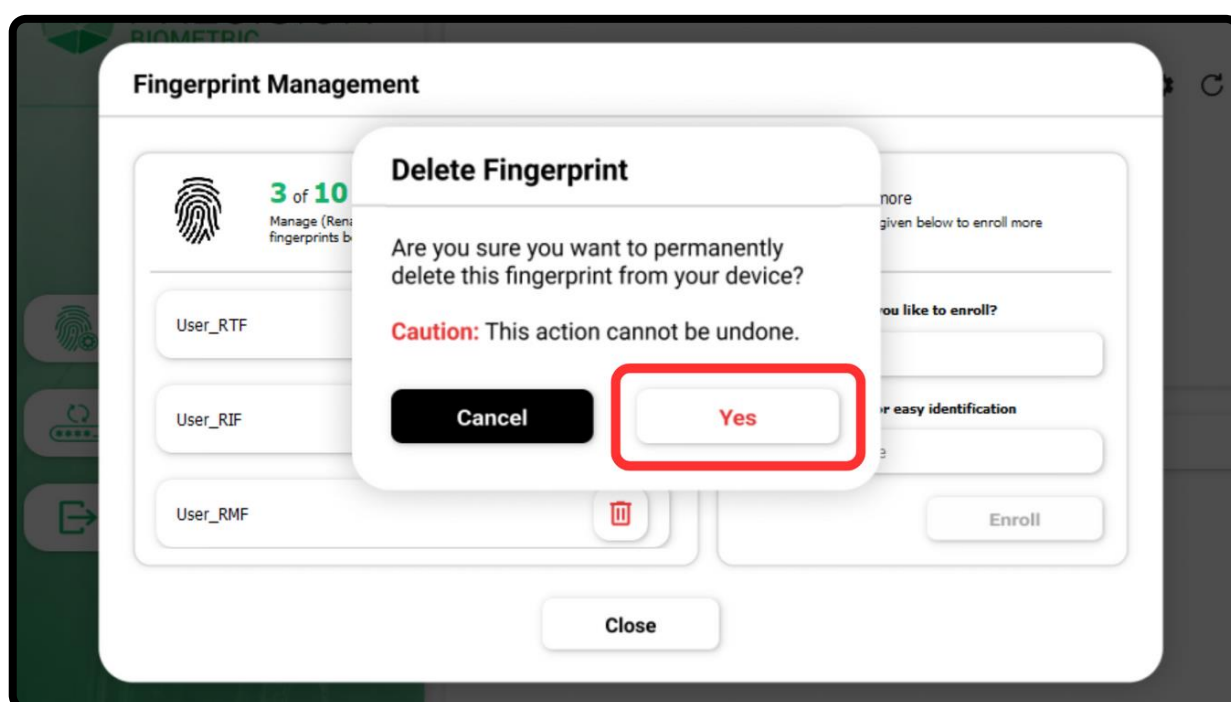


Step 9 – Enrolled fingerprints will be listed in the “Fingerprint Management” page. Click on “Close” to go back to the home page. You can come back to this page to enroll more fingerprints later.

H. Fingerprint Management

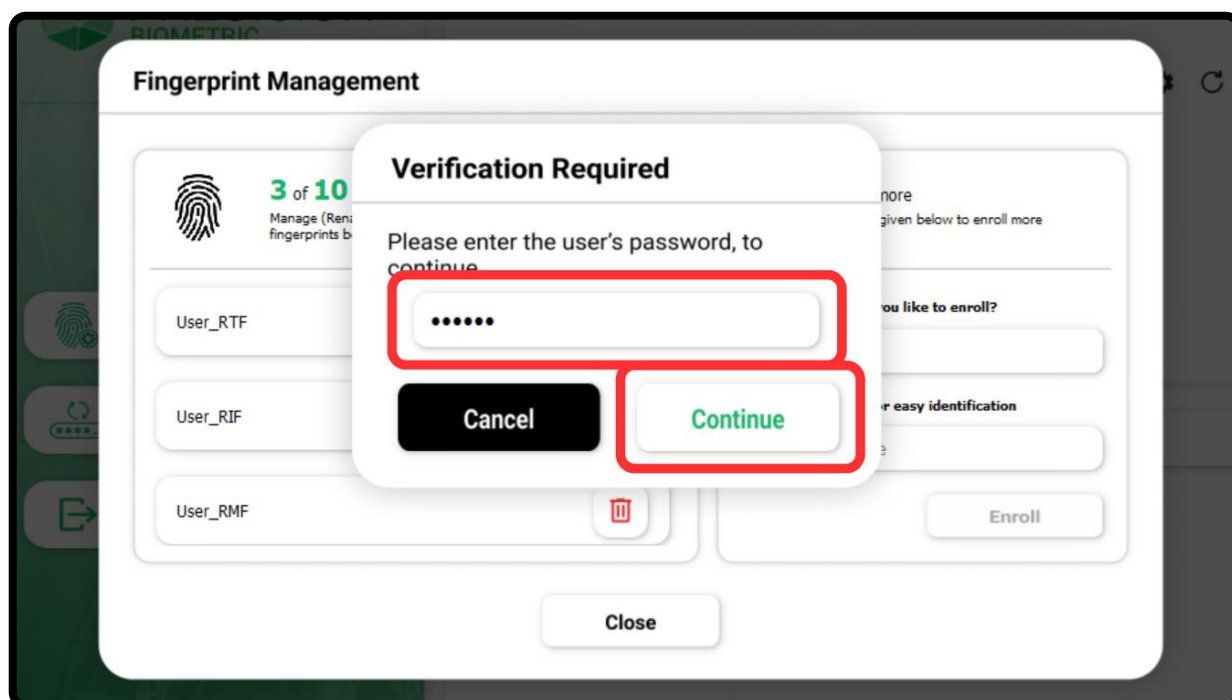


Step 1A – You can delete individual fingerprints from your biometric token from the “Fingerprint Management” window. Click on the “Delete” icon next to the fingerprint that you would like to delete, to get started.

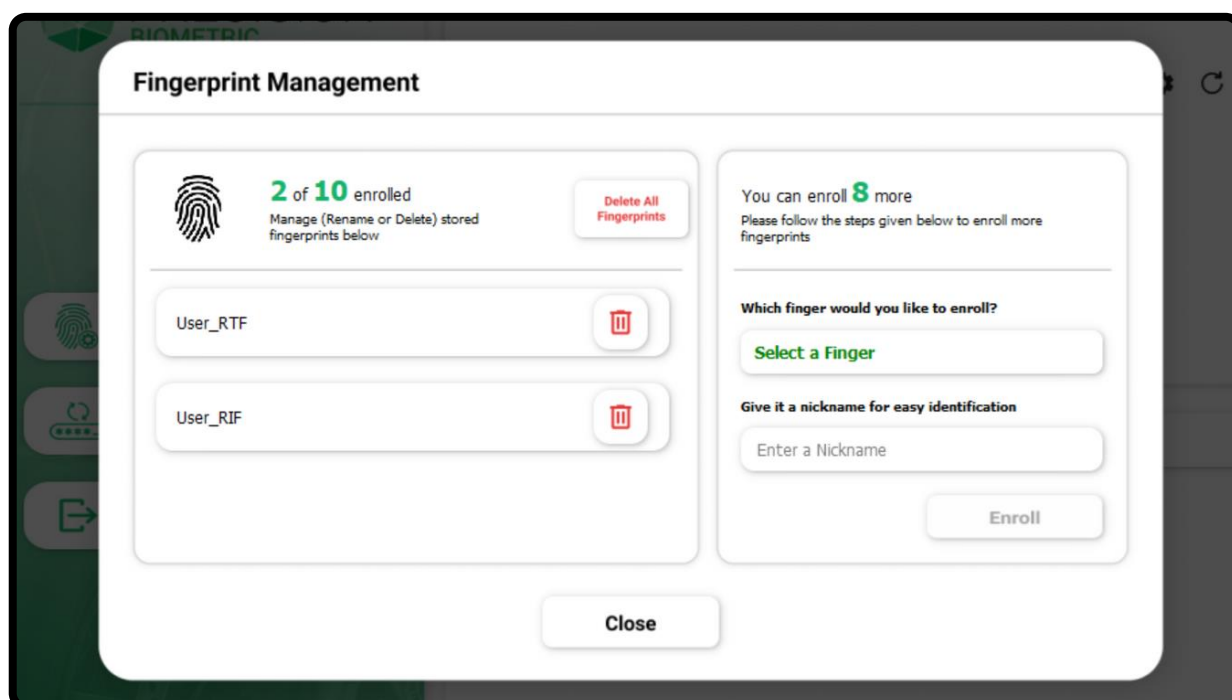


Step 2A – Please provide confirmation by clicking on “Yes”, as this action is not reversible.

H. Fingerprint Management

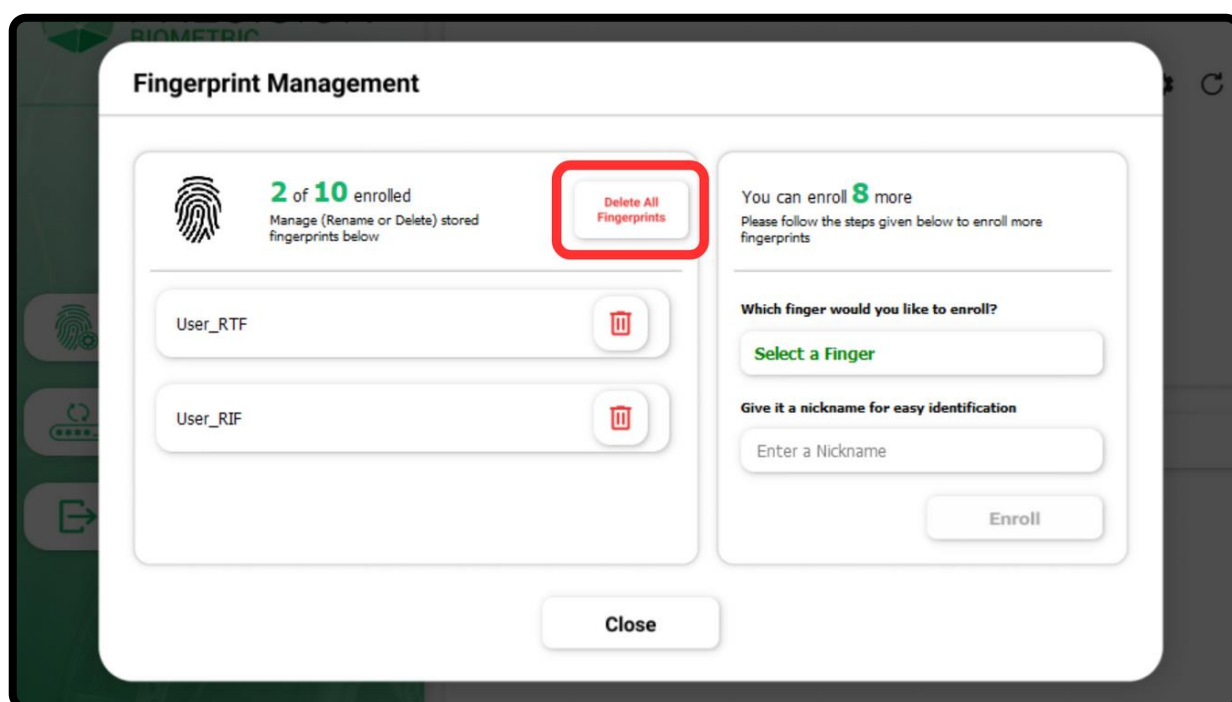


Step 3A – Now, enter your user password for verification, and click on “Continue” to proceed with the deletion.

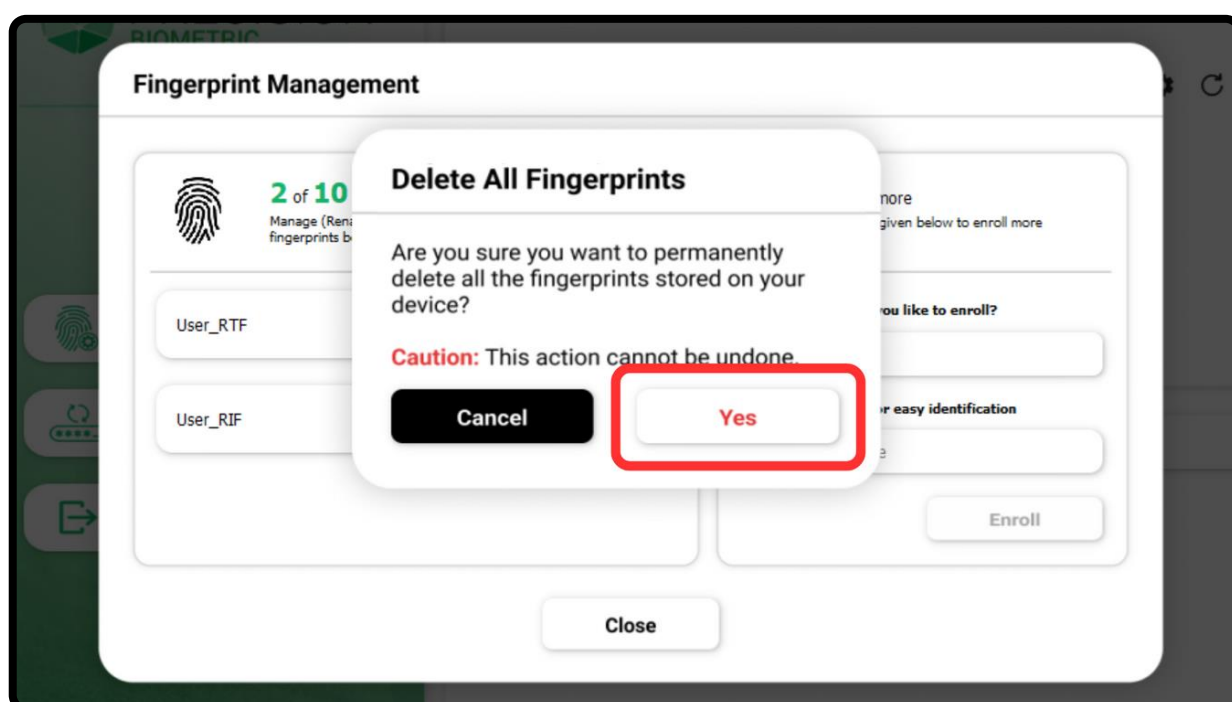


Step 4A – Once it has been deleted, you will be returned to the “Fingerprint Management” window.

H. Fingerprint Management

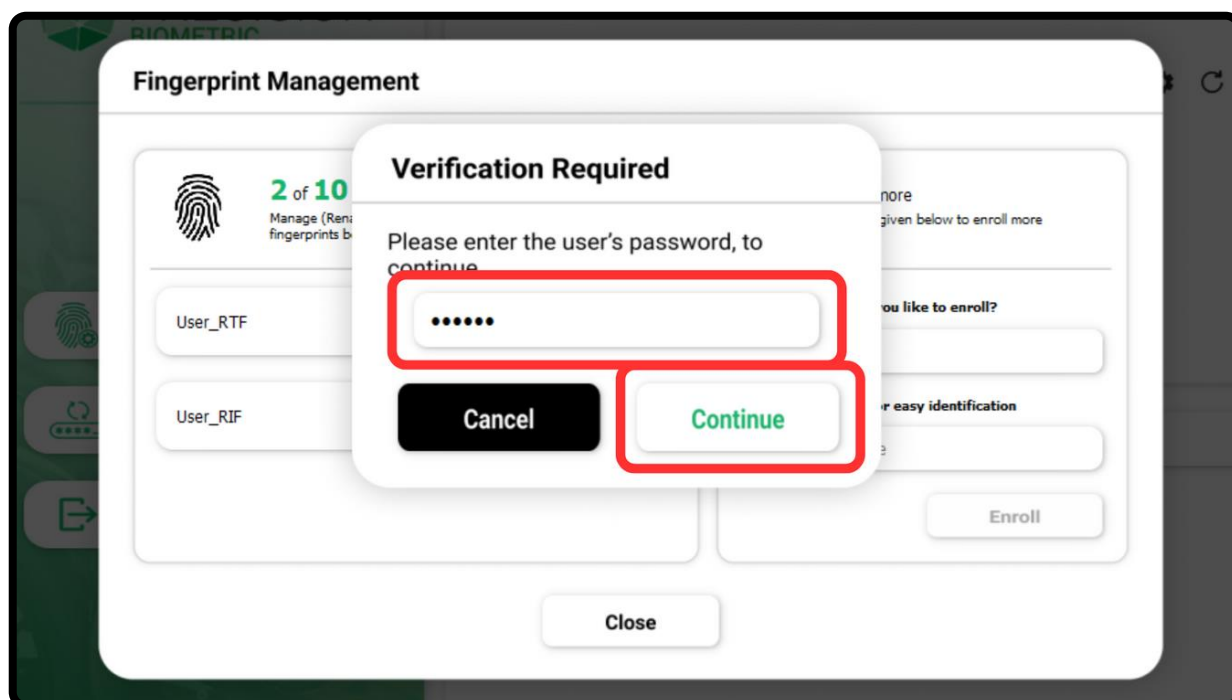


Step 1B – You can also delete all enrolled fingerprints from your biometric token from the “Fingerprint Management” window. Click on the “Delete All Fingerprints” button, to do so.

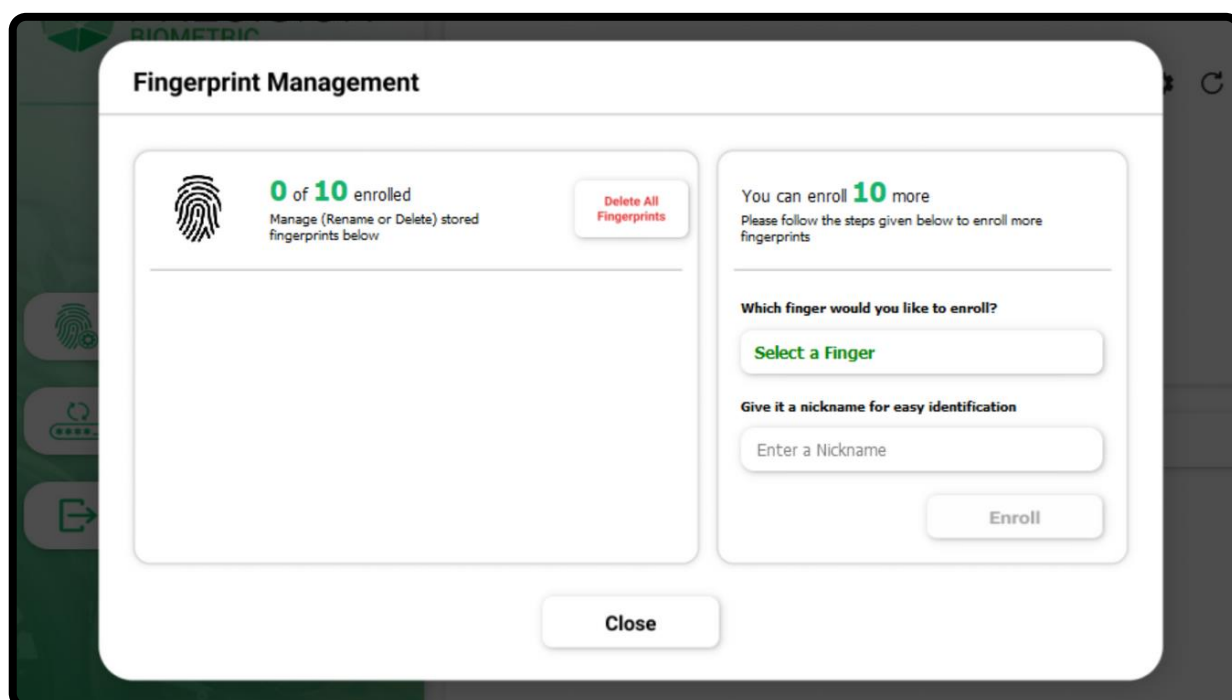


Step 2B – Please provide confirmation by clicking on “Yes”, as this action is not reversible.

H. Fingerprint Management

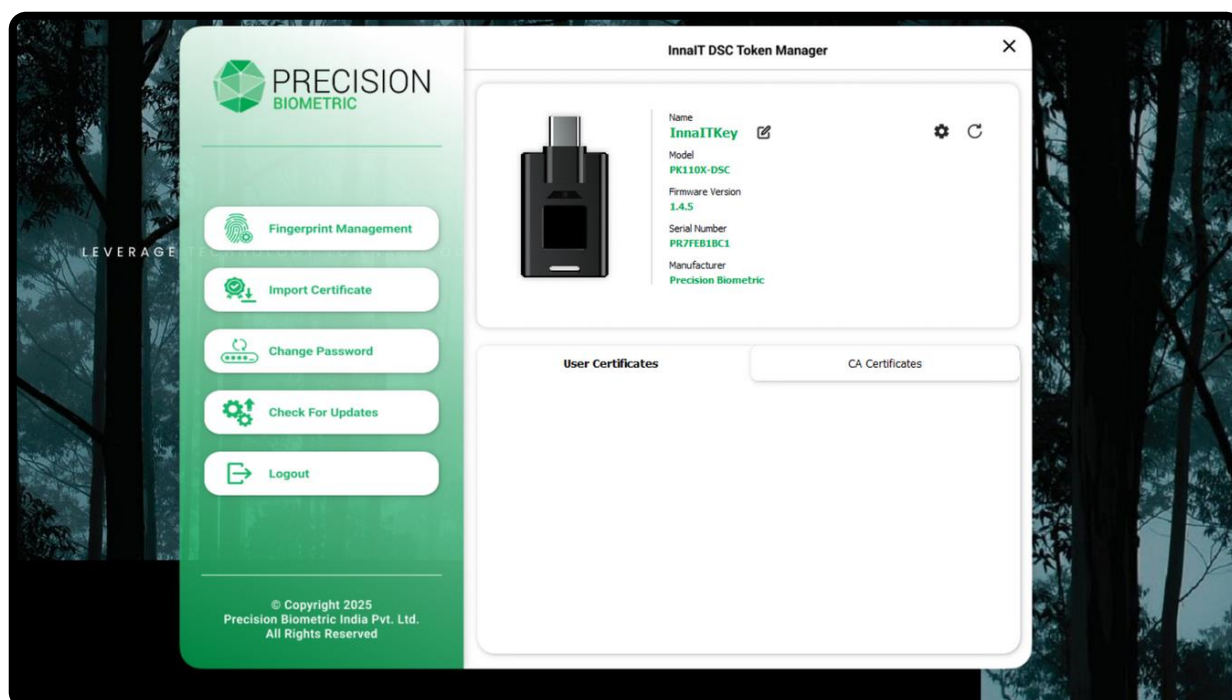


Step 3B – Now, enter your user password for verification, and click on “Continue” to proceed with the deletion.

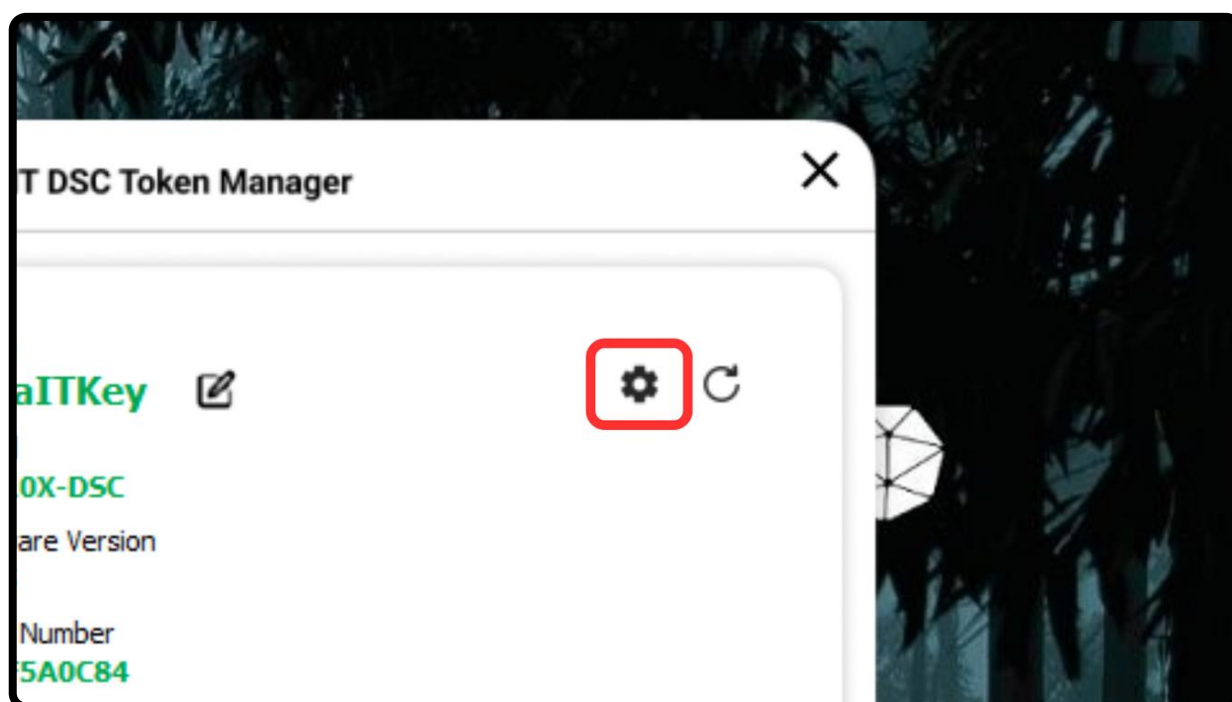


Step 4B – Once the deletion is complete, you will be returned to the “Fingerprint Management” window.

I. Enable Single Sign On

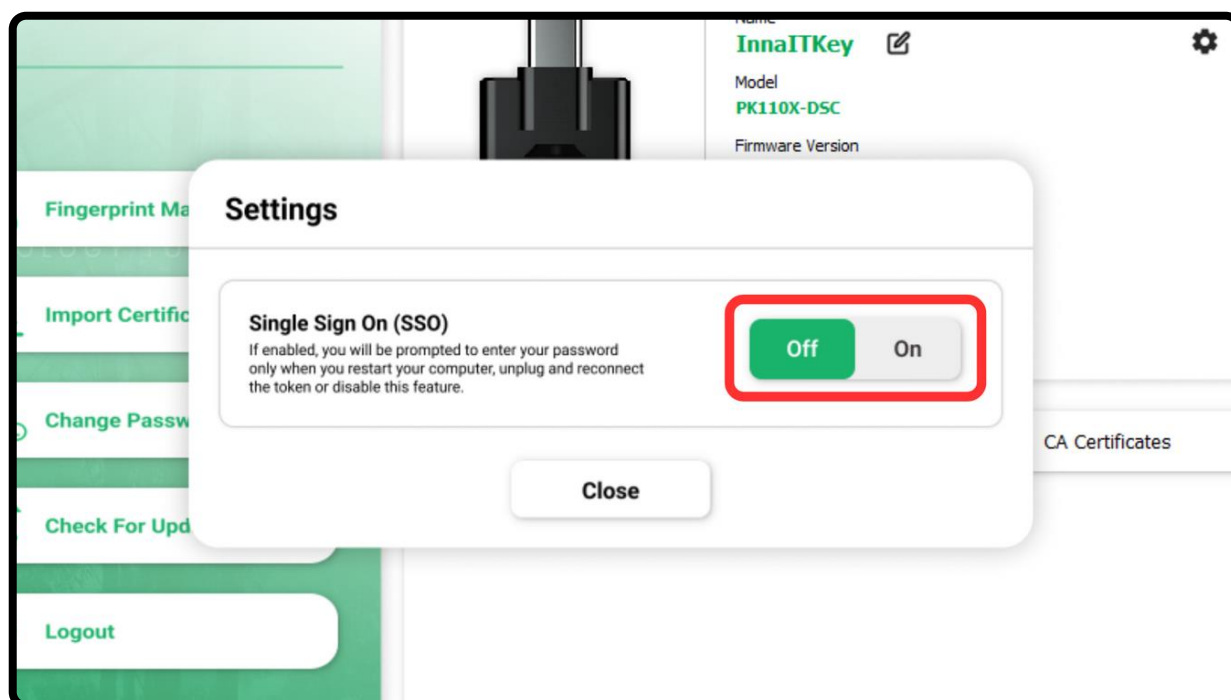


Note – If the Single Sign On feature is enabled, the user will be asked to verify their identity only once, while signing a document within a single session. A session will end when the PC is restarted or token is unplugged. Other functions within the token manager will still require verification.

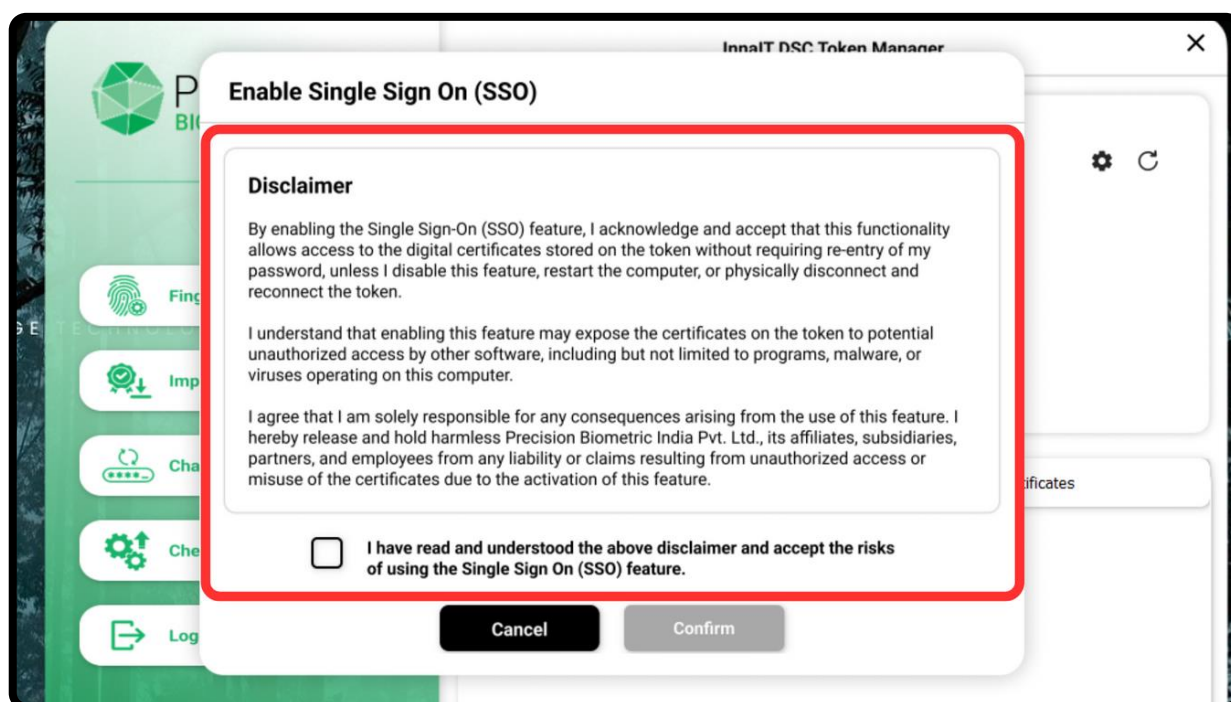


Step 1 - To enable this feature, click on the settings icon in the home page.

I. Enable Single Sign On

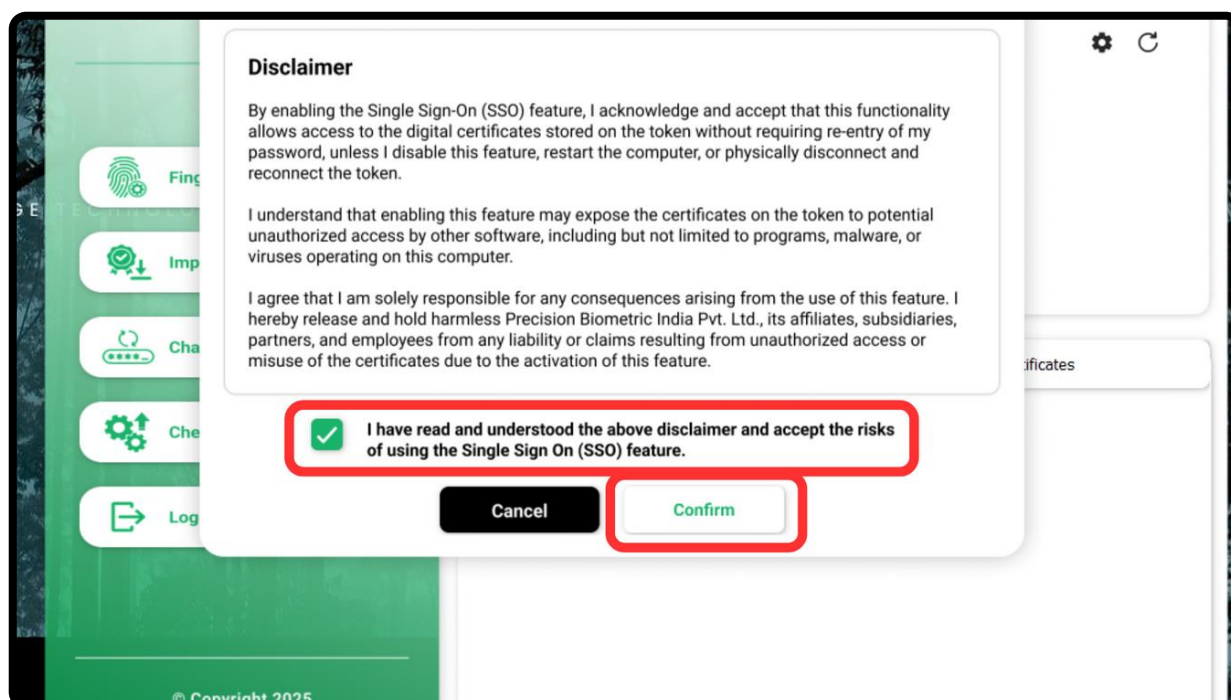


Step 2 – Here, click on the toggle button next to “Single Sign On” to change it to the “On” position.

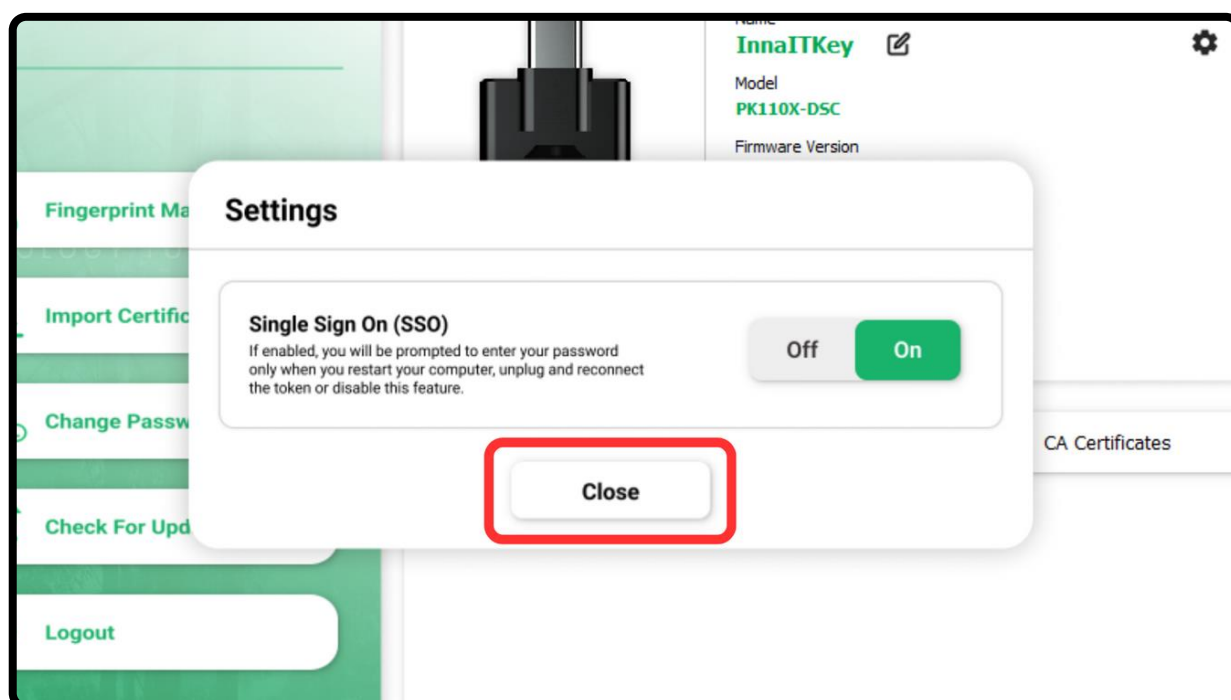


Note - A disclaimer will appear, stating the risks associated with using the Single Sign On feature. Please read the disclaimer thoroughly before proceeding.

I. Enable Single Sign On

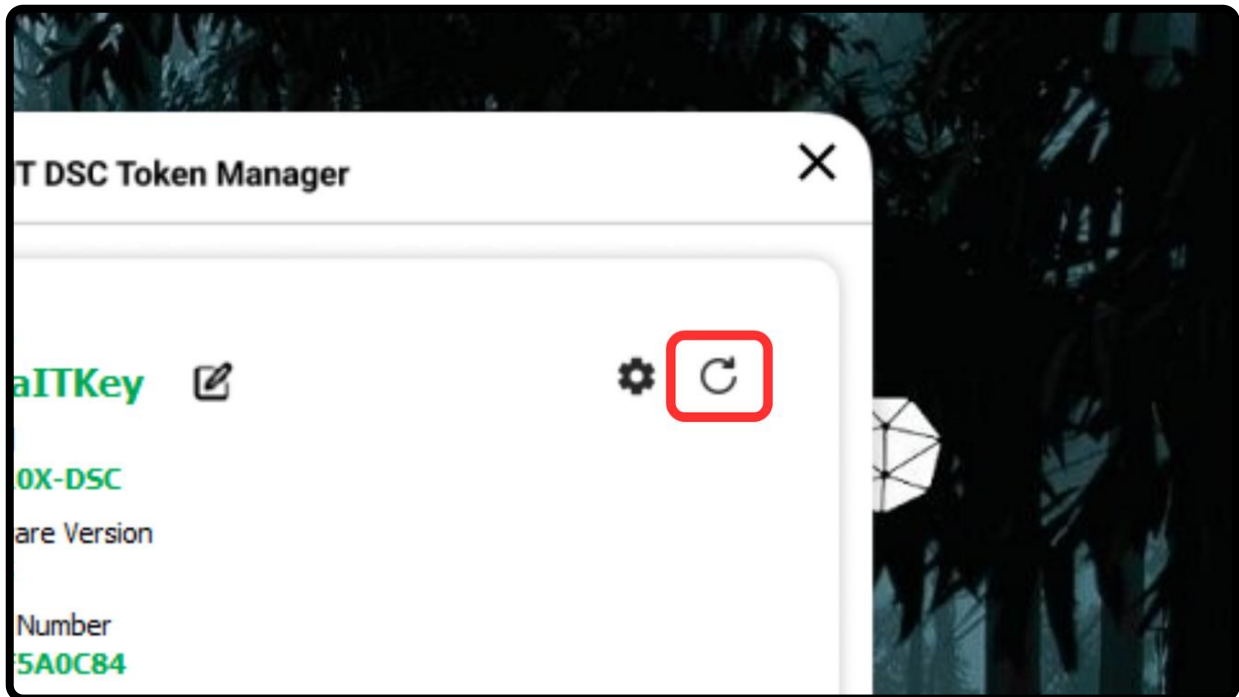


Step 3 – Click on the check box to acknowledge the disclaimer and then click on “Confirm” to enable the SSO feature.

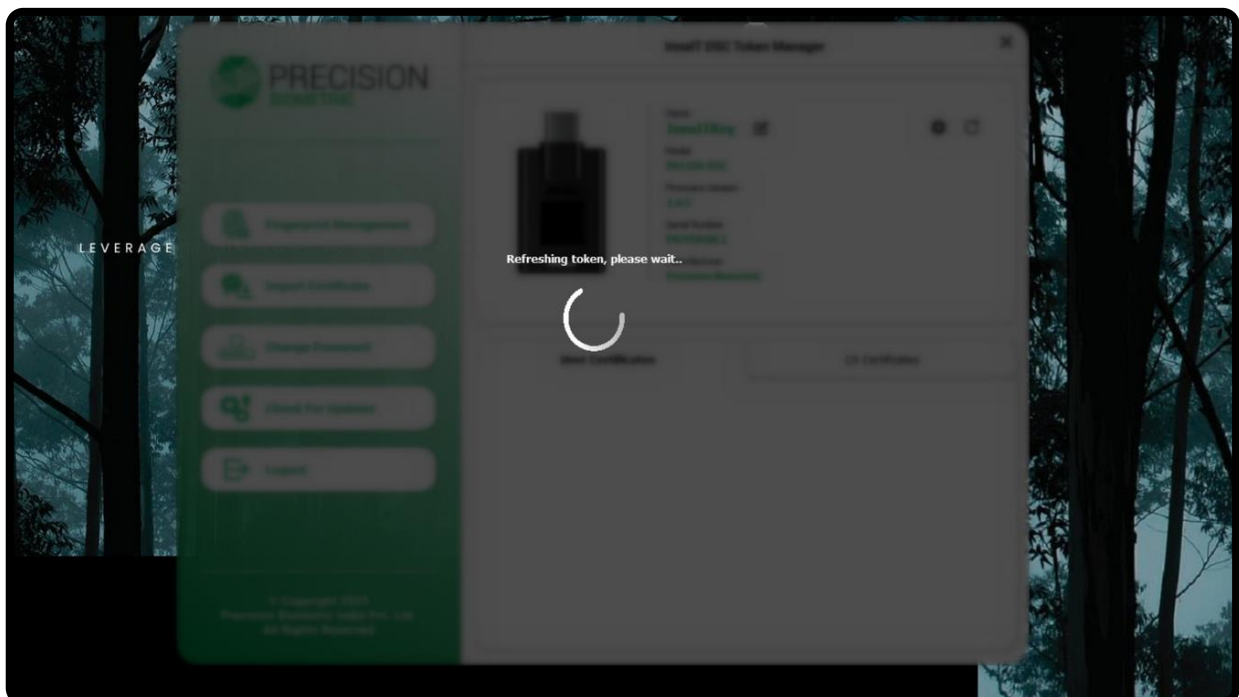


Step 4 – Now, click on the “Close” button on the “Settings” window, to go back to the home page.

I. Enable Single Sign On

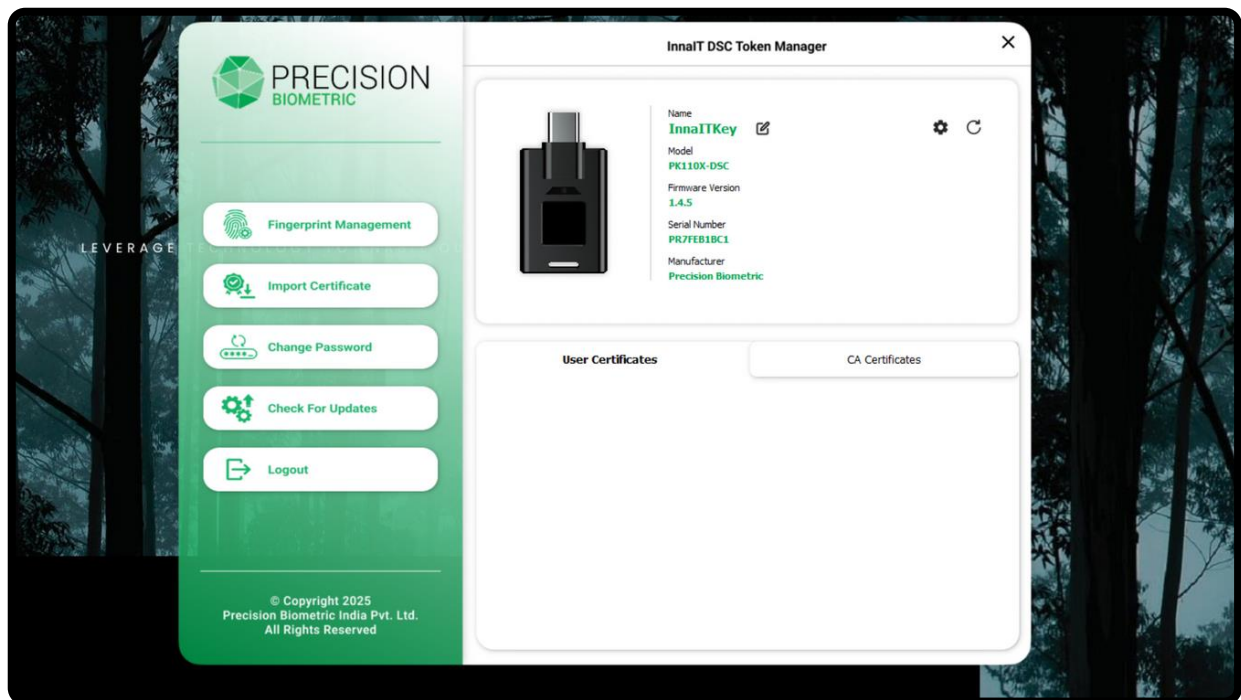


Step 5 – Click on the “Refresh” button in the home page.



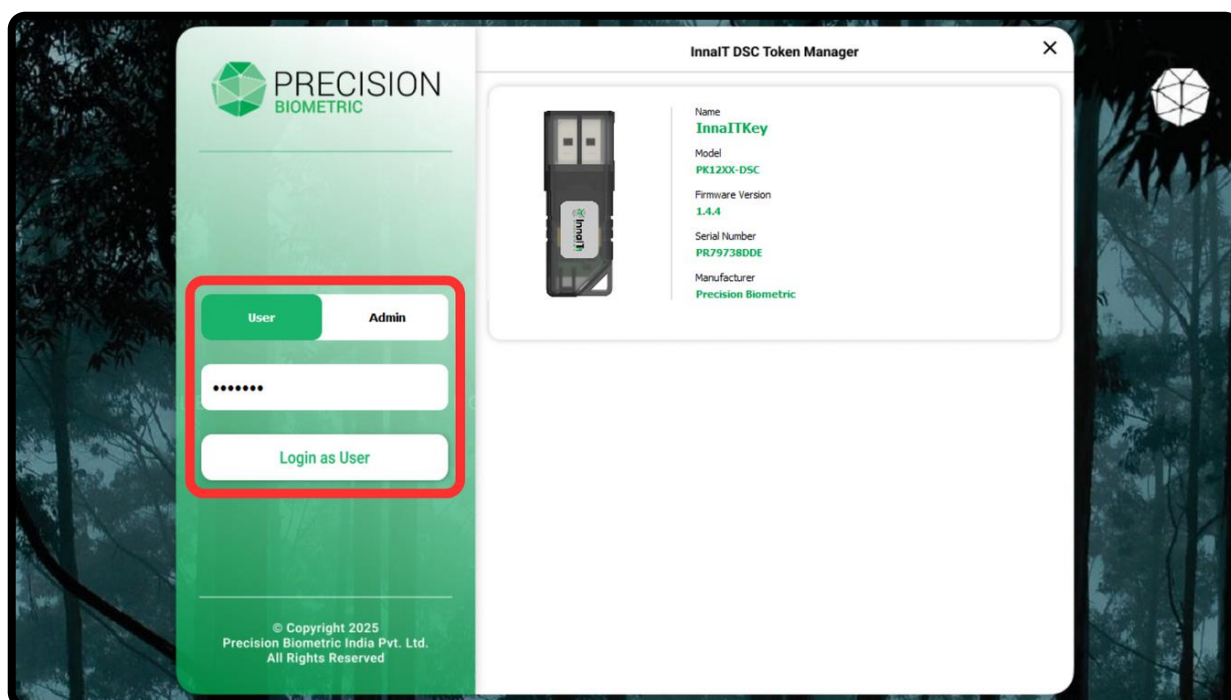
Step 6 – Please wait for the device settings to get refreshed.

I. Enable Single Sign On

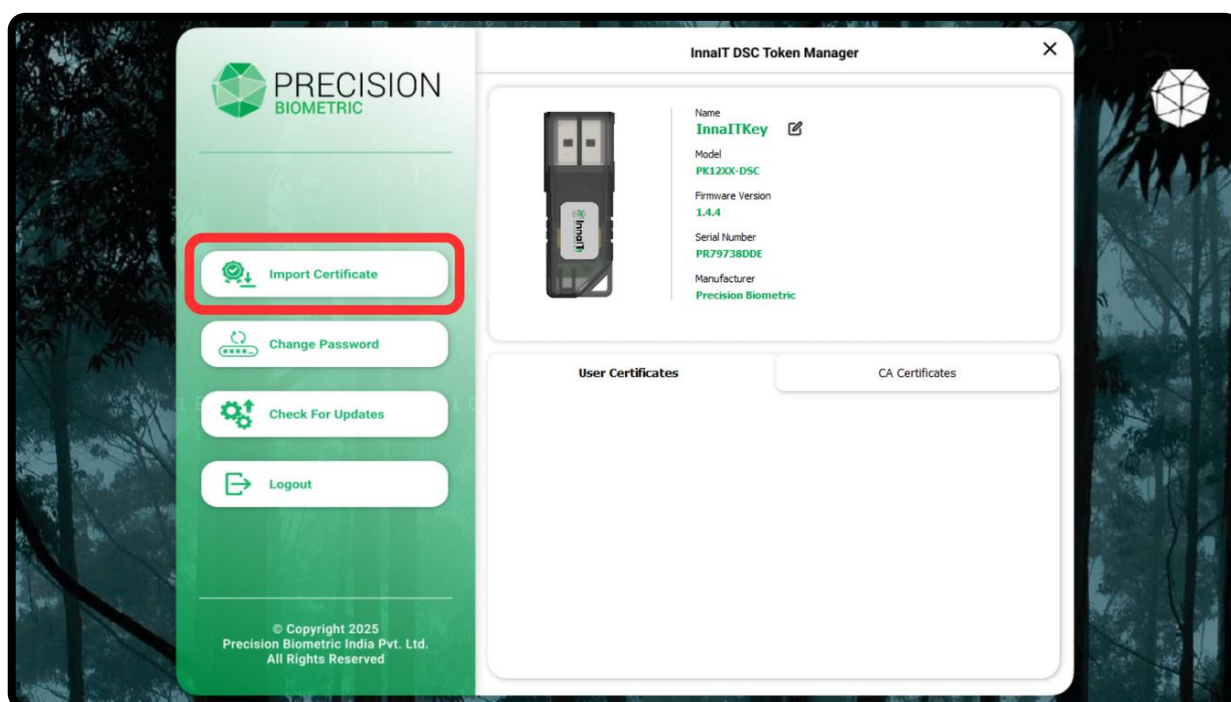


Step 7 – Now, you can continue using your token.

J. Import Certificate (.cer)

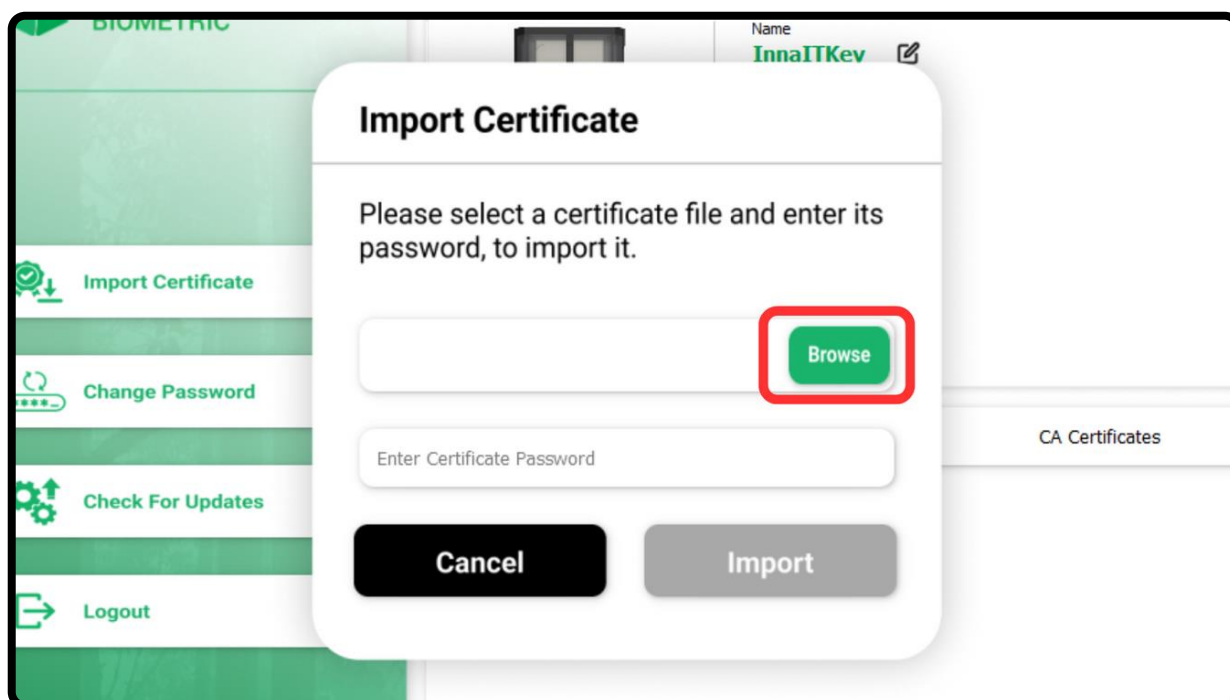


Step 1 – Login as a user.

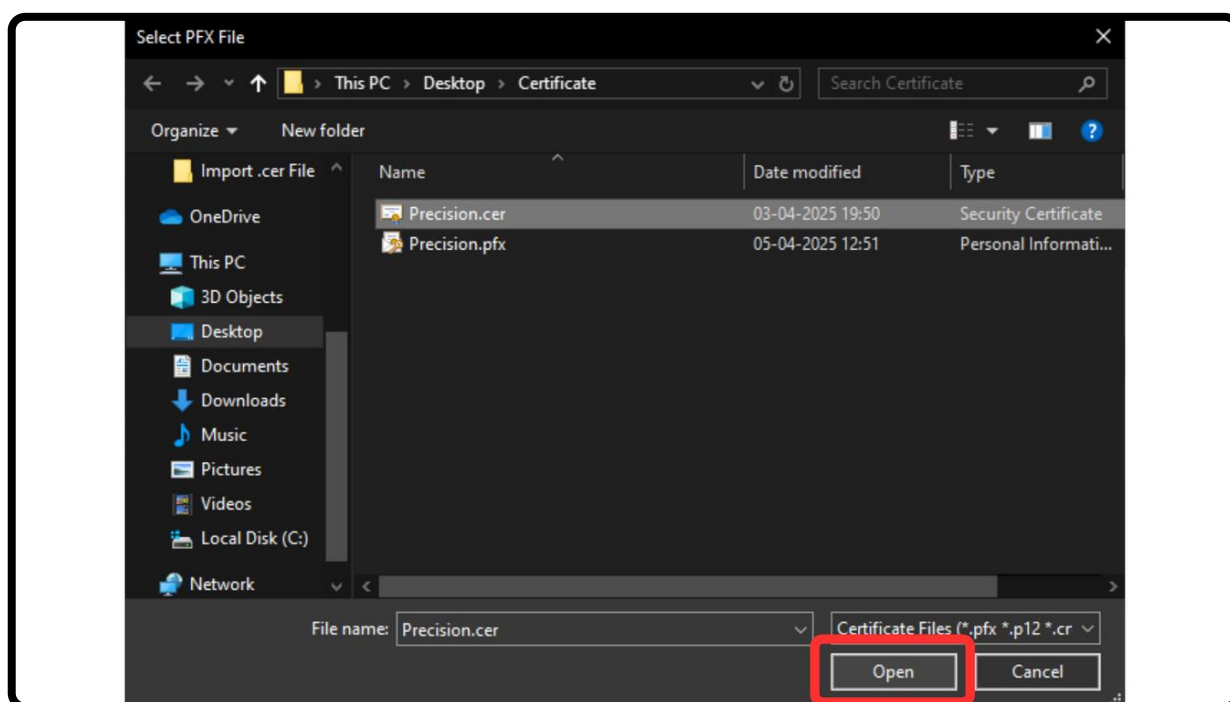


Step 2 – Click on the “Import Certificate” button.

J. Import Certificate (.cer)

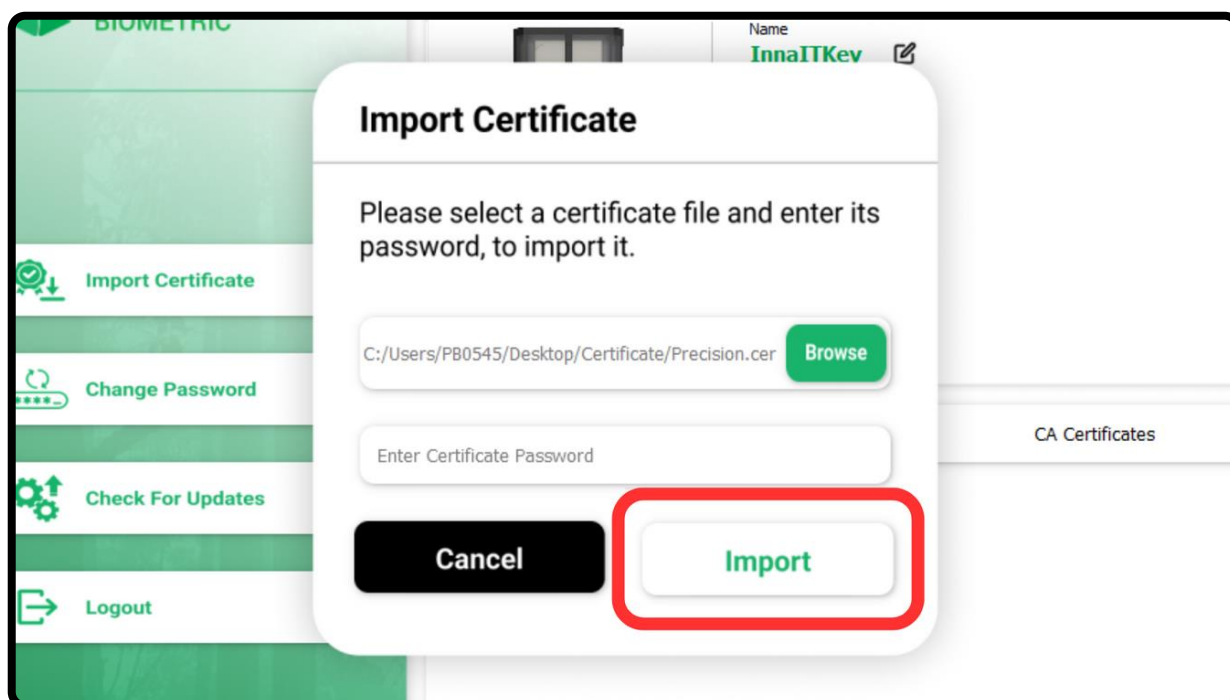


Step 3 – In this window, click on “Browse” to select a certificate to import.



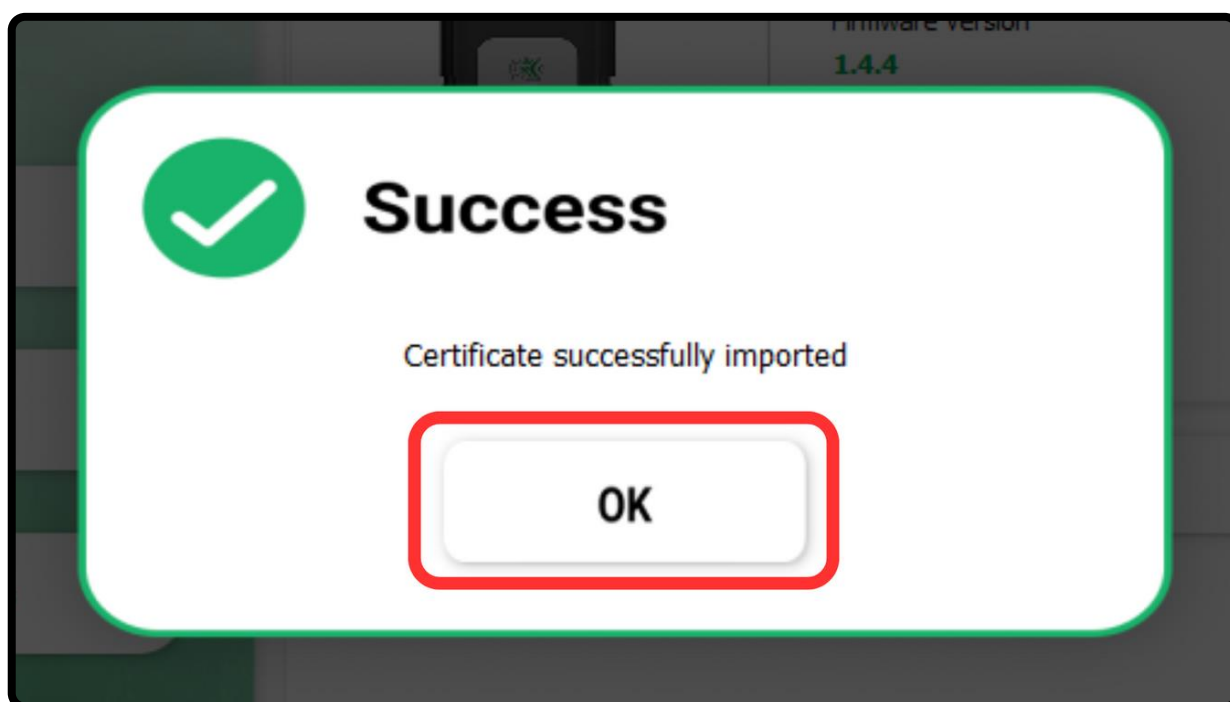
Step 4 – Choose the certificate file and then click on “Open”, to continue.

J. Import Certificate (.cer)



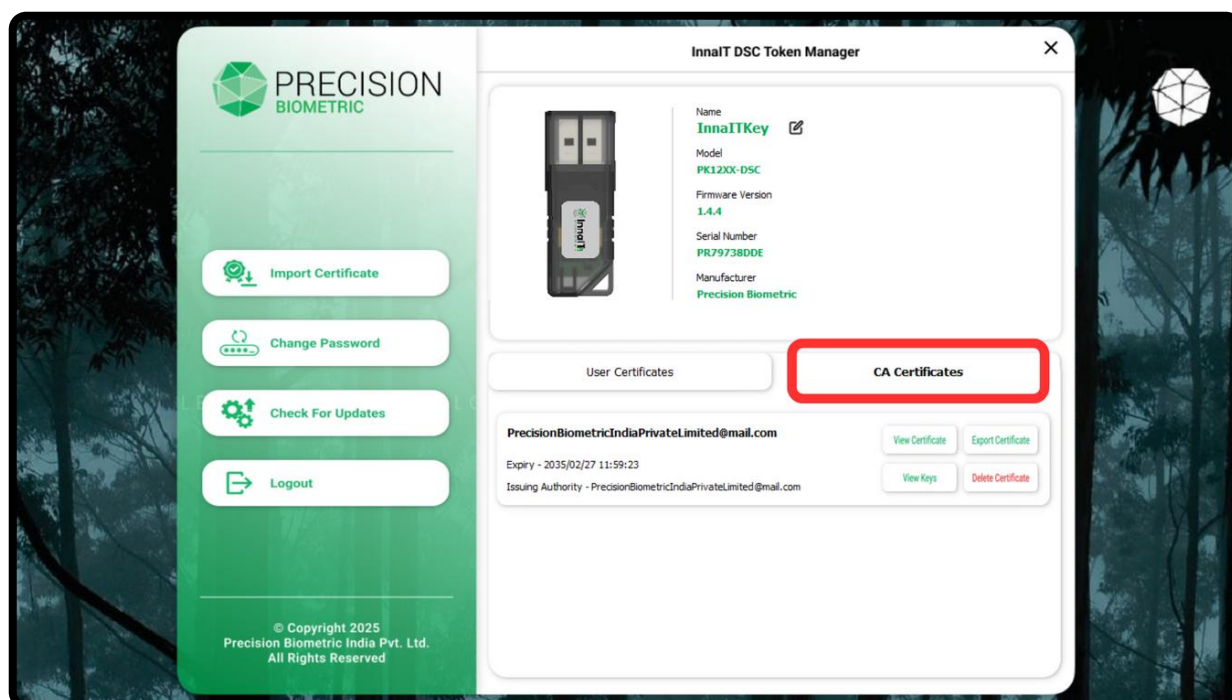
Step 5 – Now, click on “Import” to import the certificate to your token.

Note: Since you are importing a .cer file, you do not have to enter a certificate password.



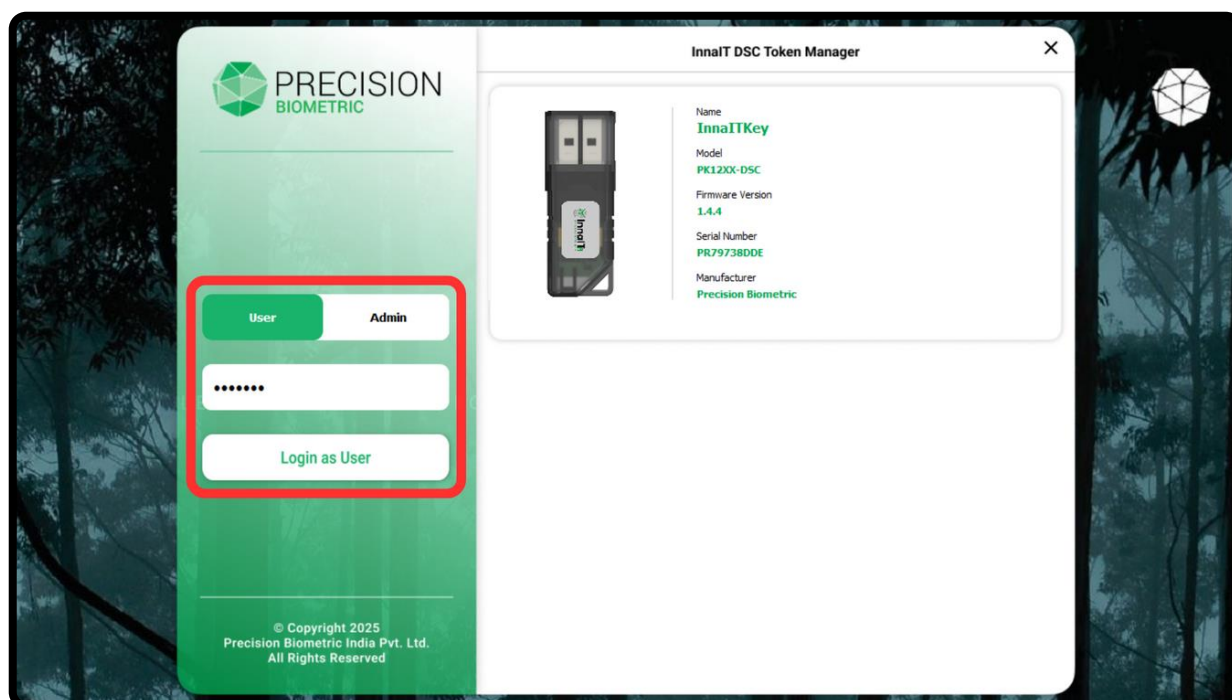
Step 6 – Once the file is imported, click “OK” on the “Success” dialogue box, to continue.

J. Import Certificate (.cer)

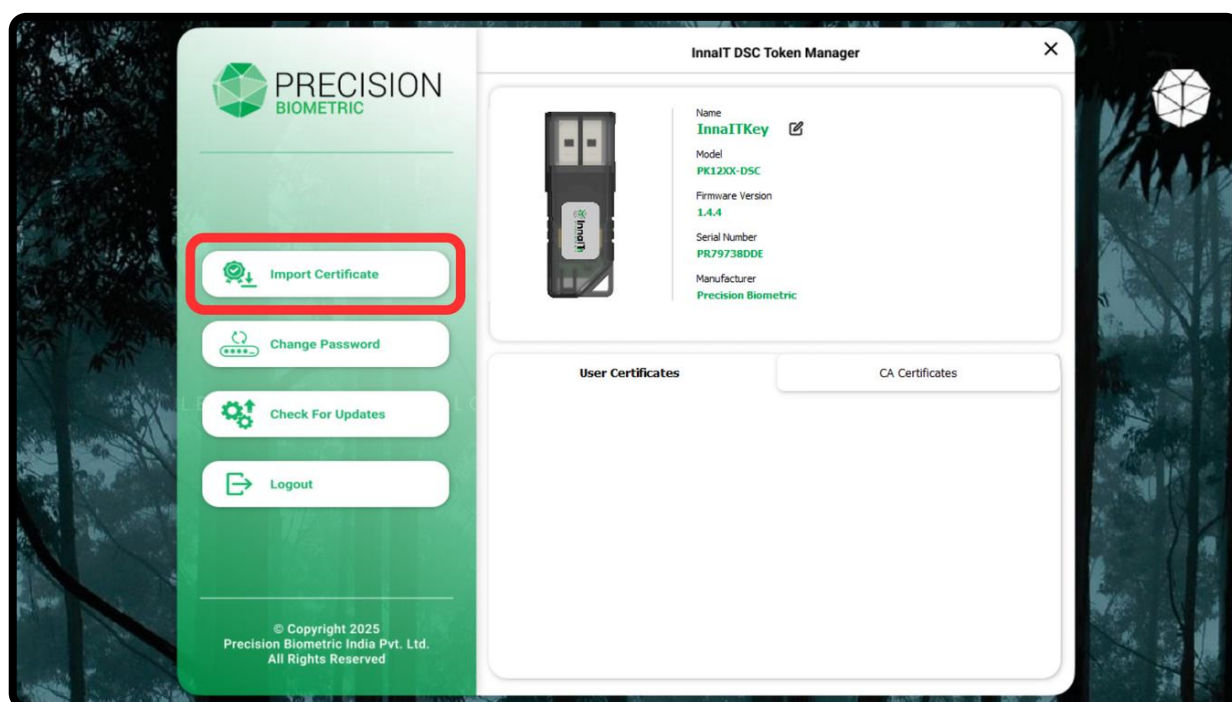


Step 7 – You can find the newly imported certificate (.cer) by clicking on the “CA Certificates” tab.

K. Import PFX (.pfx)

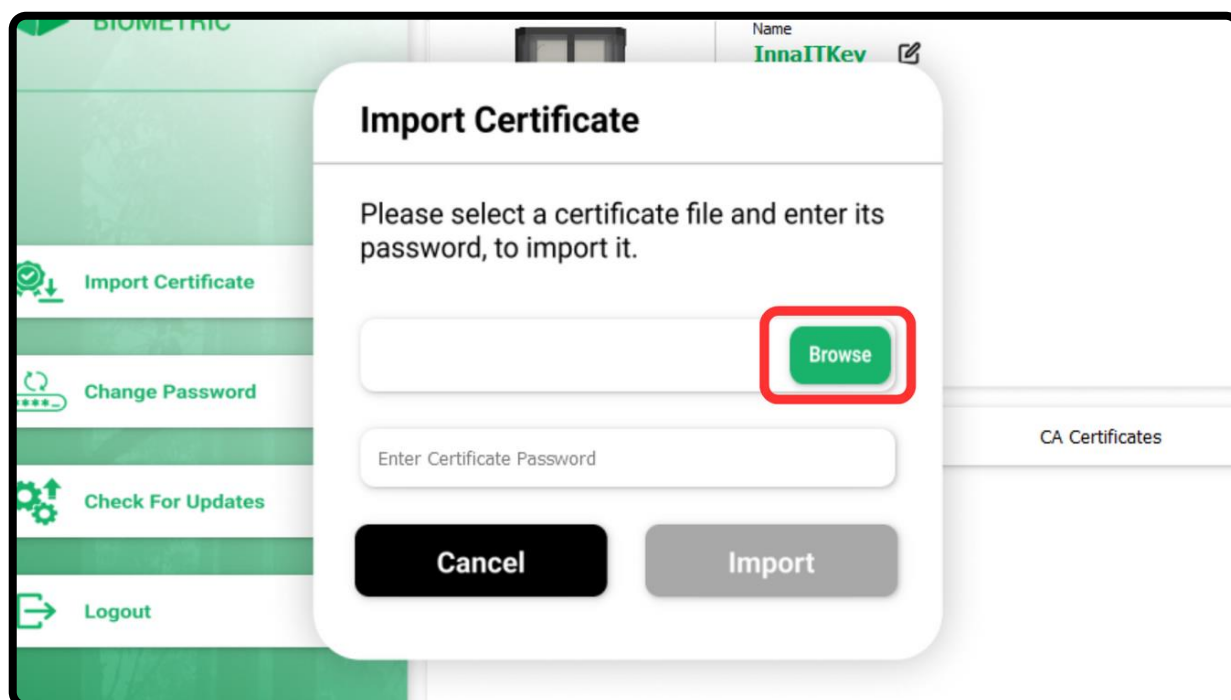


Step 1 – Login as a user.

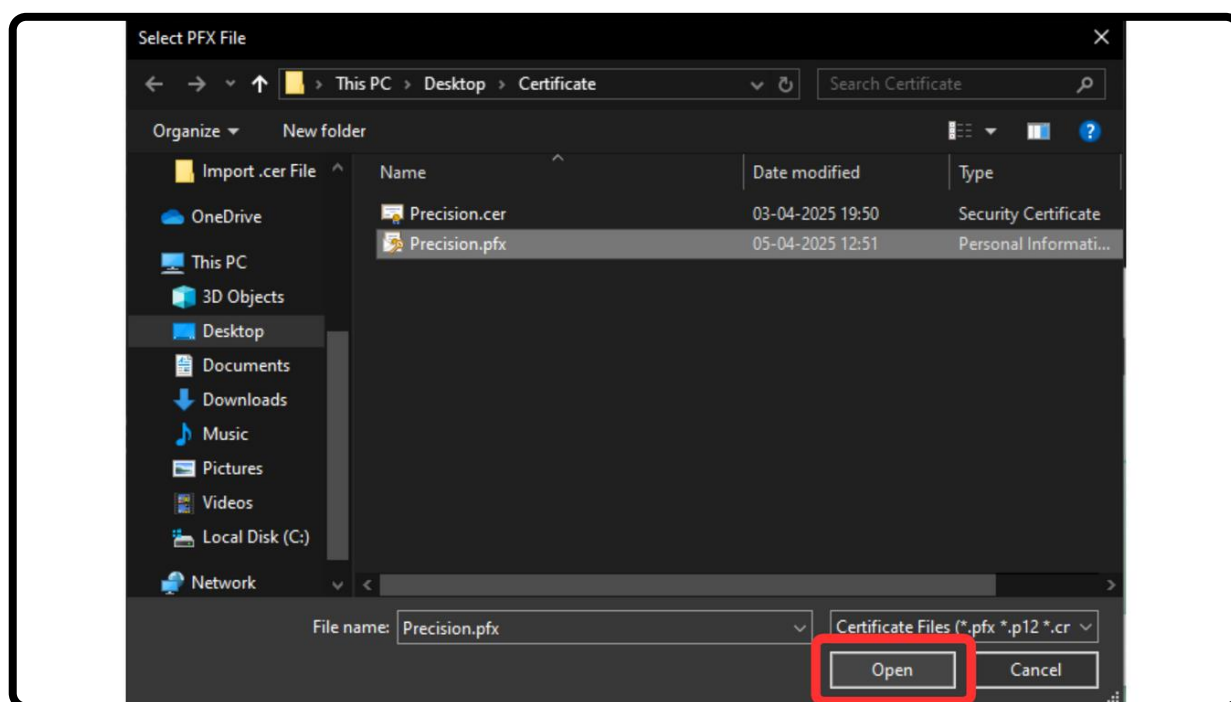


Step 2 – Click on the “Import Certificate” button.

K. Import PFX (.pfx)

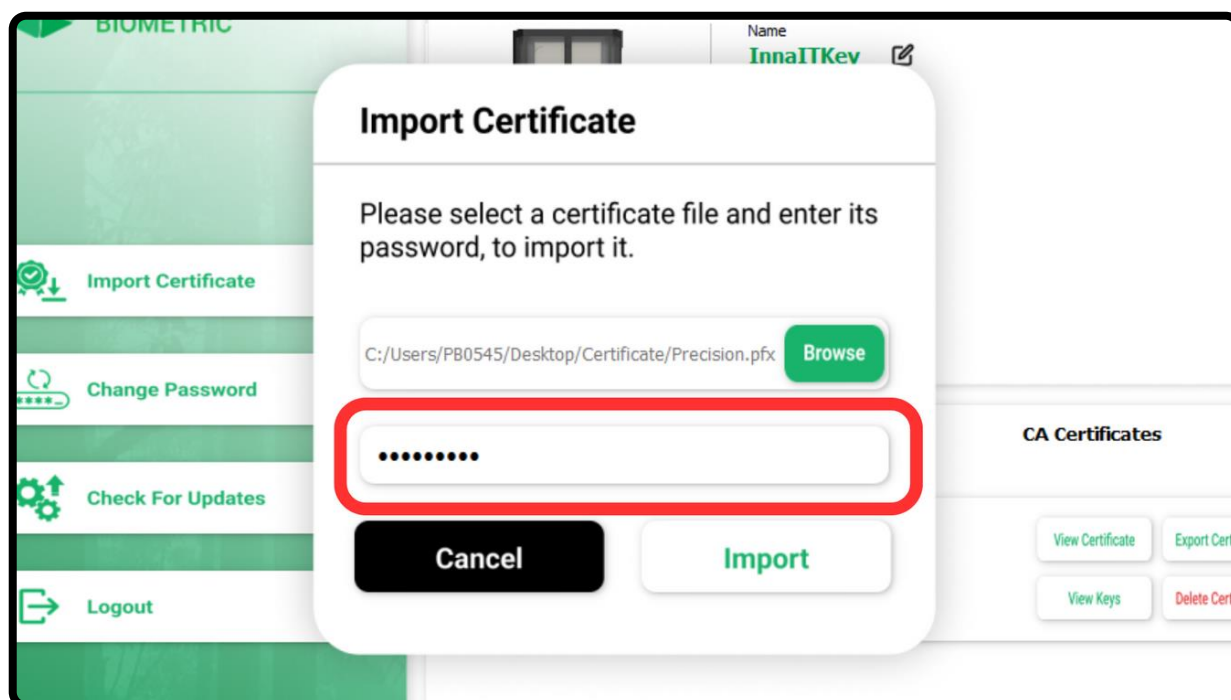


Step 3 – In this window, click on “Browse” to select a PFX file to import.

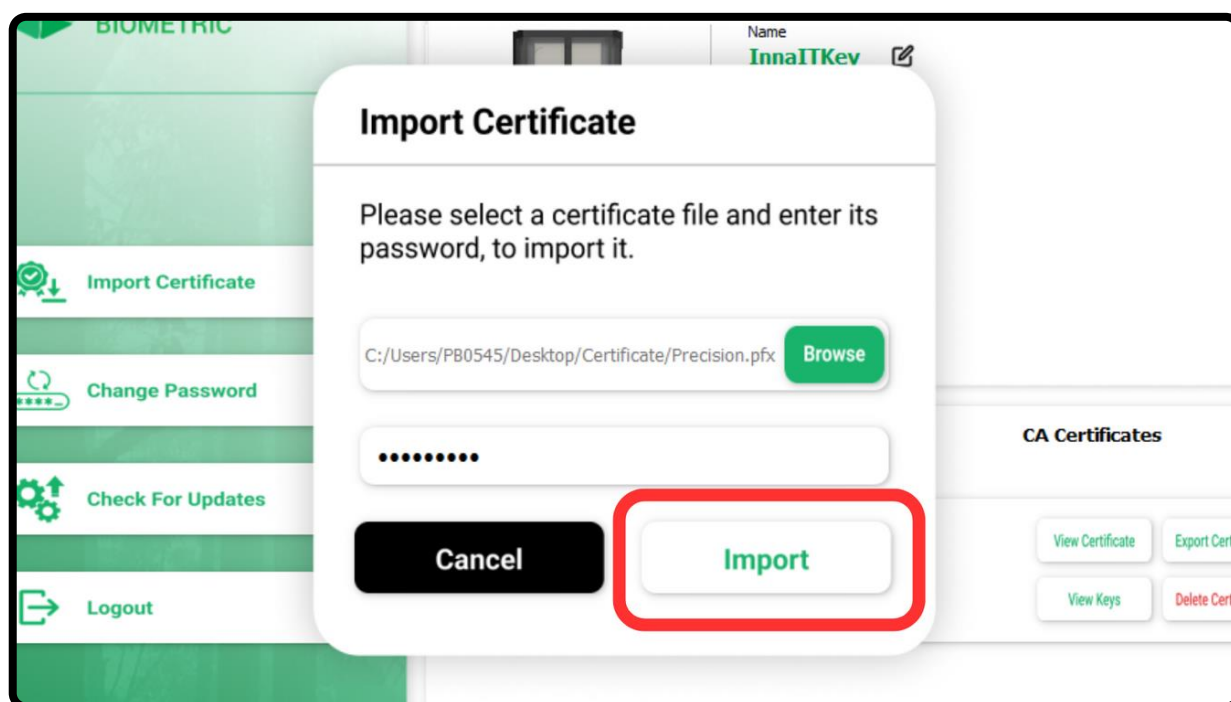


Step 4 – Choose the file and then click on “Open”, to continue.

K. Import PFX (.pfx)

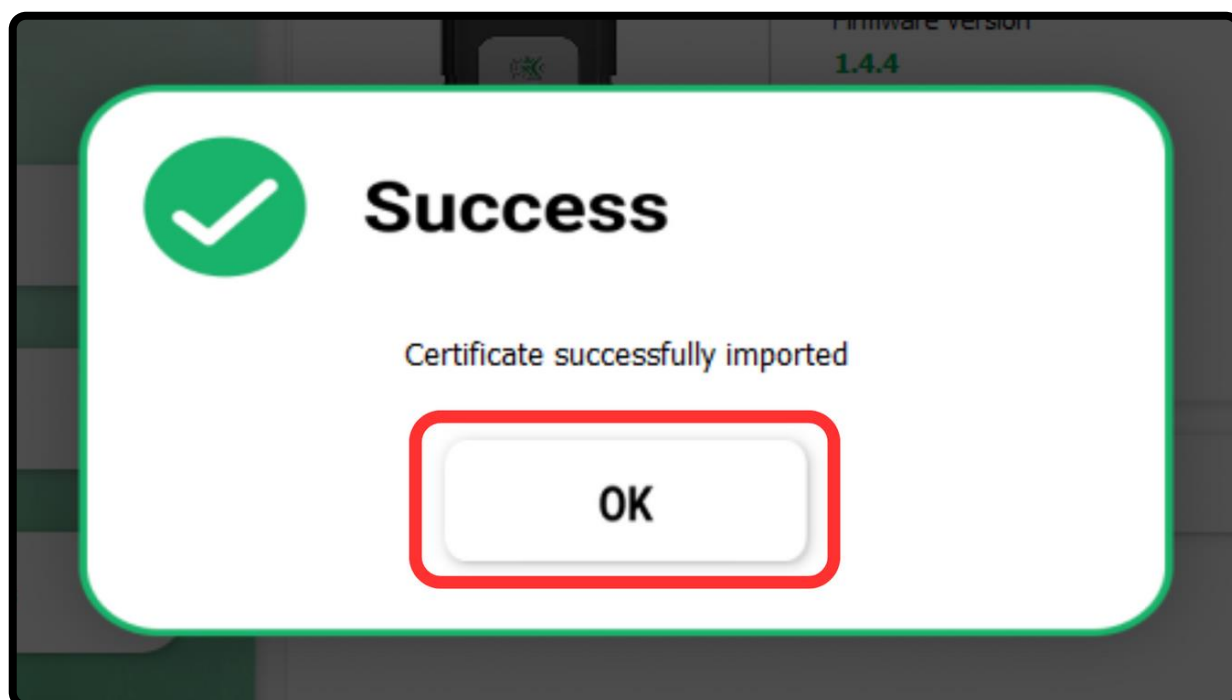


Step 5 – Now, you need to enter the password for your PFX file in the given field.

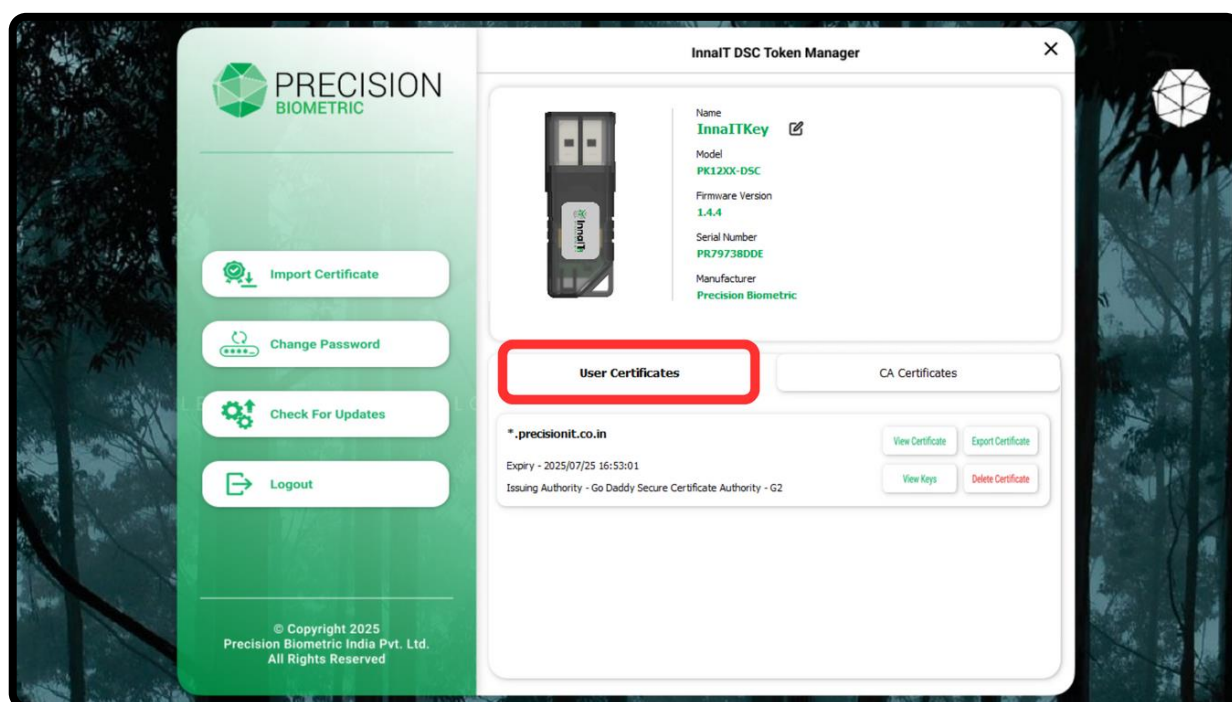


Step 6 – Finally, click on “Import” to import the PFX file to your token.

K. Import PFX (.pfx)

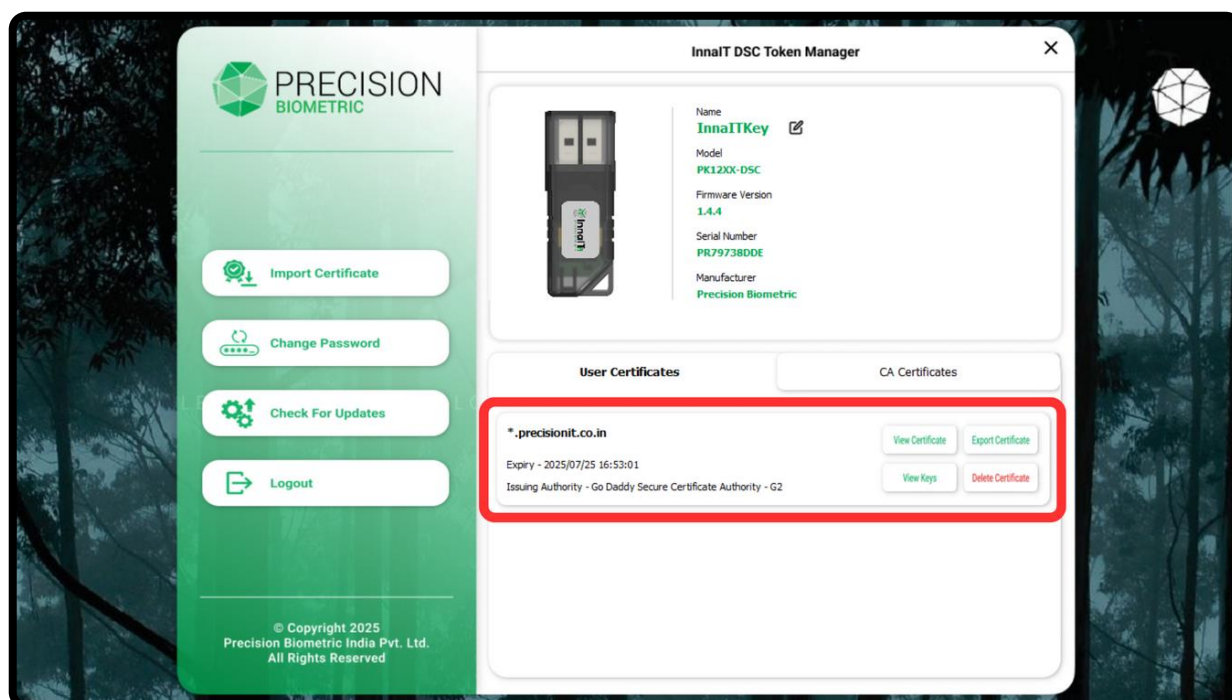


Step 7 – Once the file has been imported, click “OK” in the “Success” dialogue box, to continue.

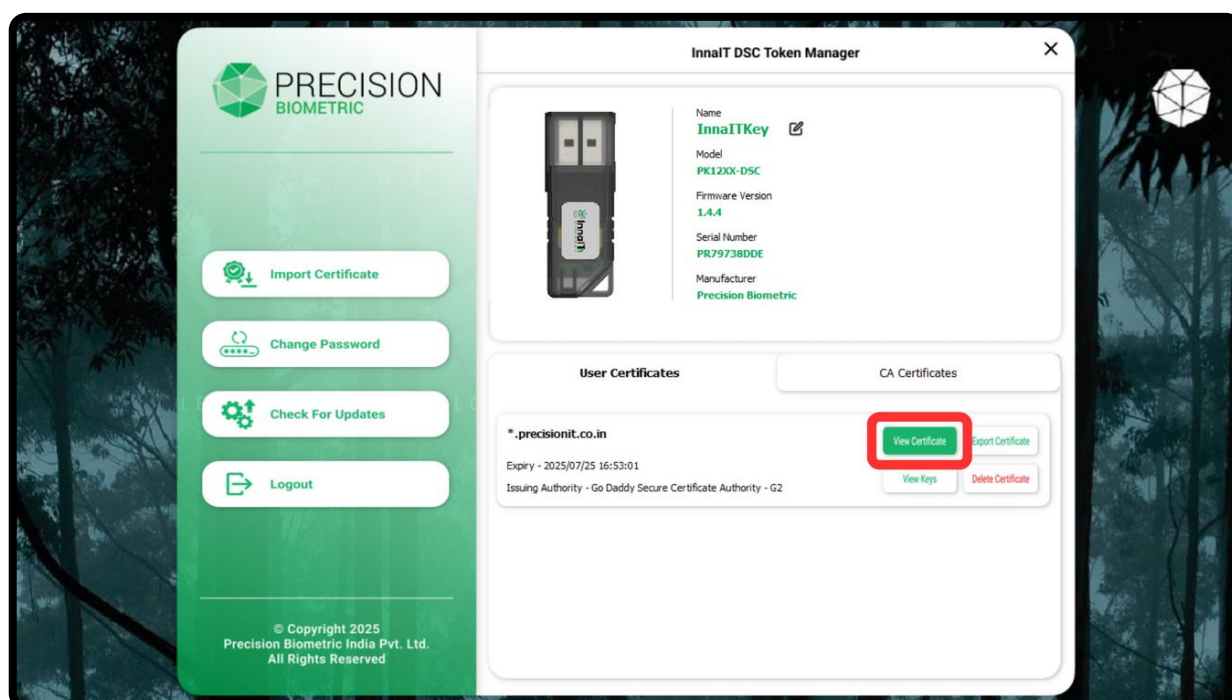


Step 8 – Your newly imported PFX (.pfx) will appear under the “User Certificates” tab.

L. View Certificate

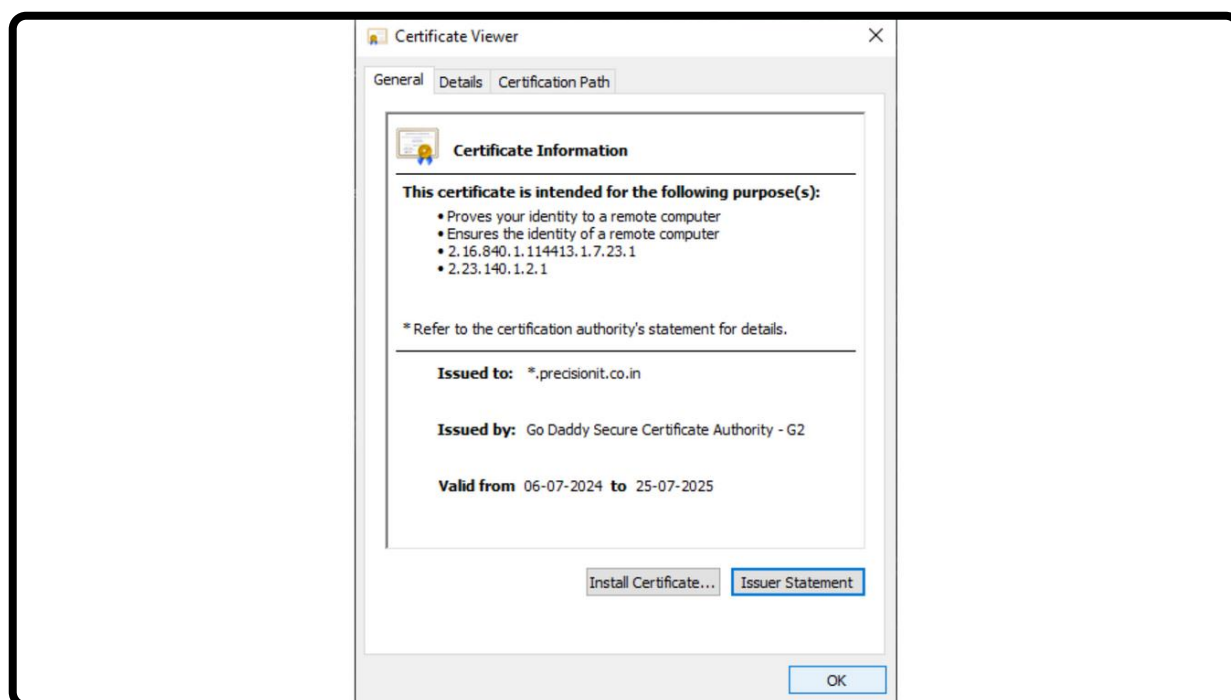


Step 1 – Login as a user and find the file that you would like to view the certificate for, under either the “User Certificates” or “CA Certificates” tab.

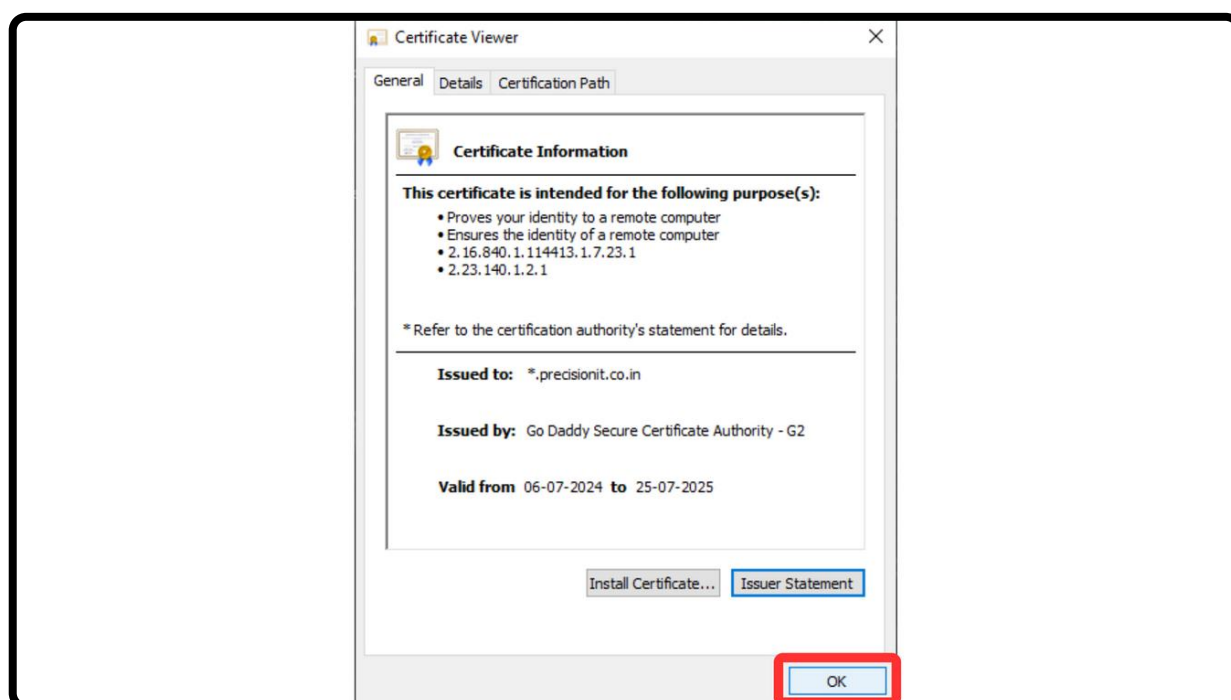


Step 2 – Now, click on the “View Certificate” button next to the listing.

L. View Certificate

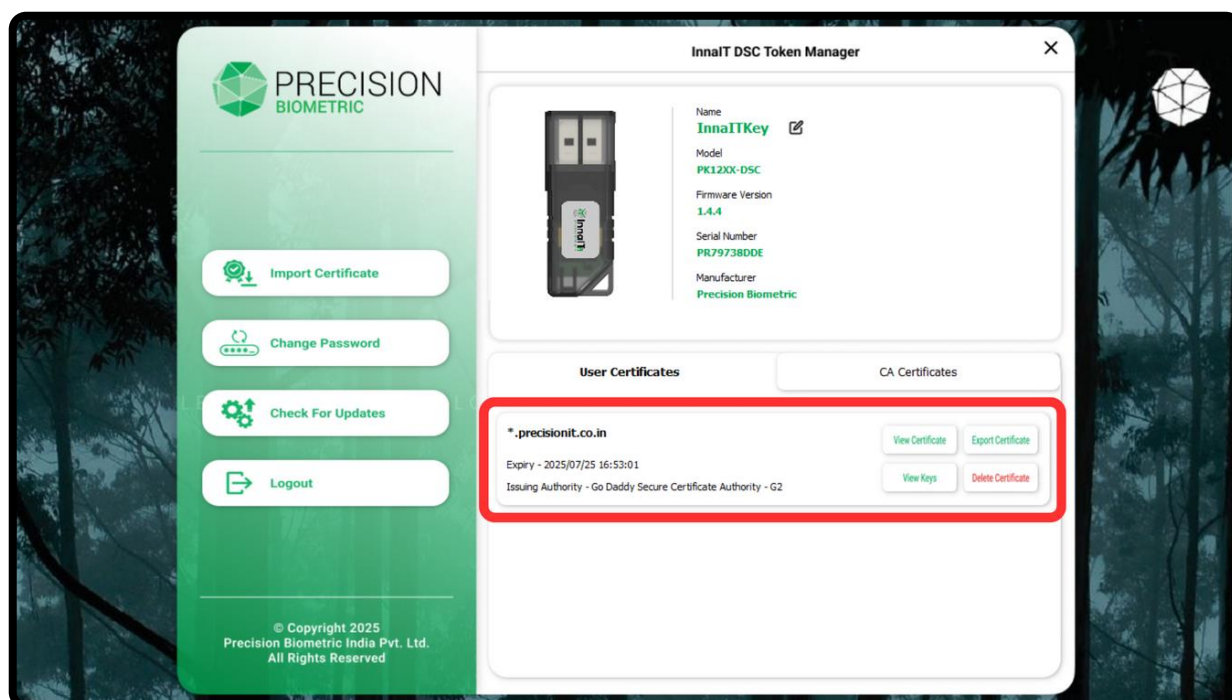


Step 3 – The Windows “Certificate Viewer” window will open, showing you details about the certificate (Such as the validity of the certificate, the issuer, etc.)

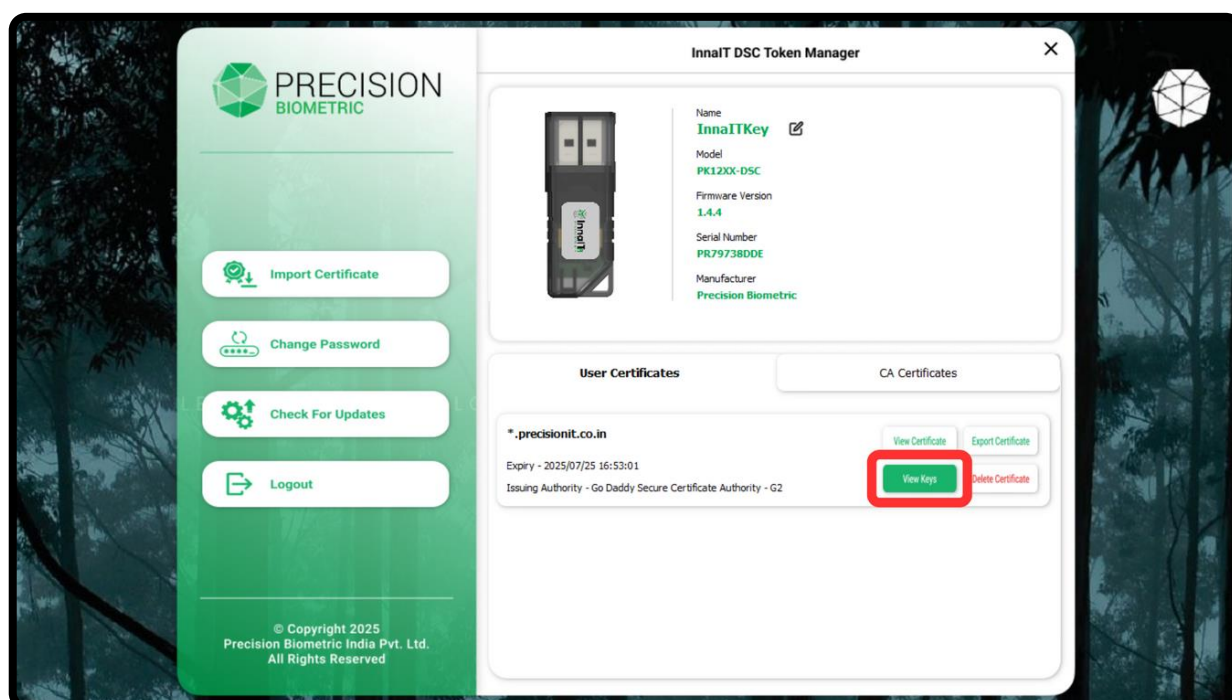


Step 4 – Click on “OK” or the close icon once you are finished viewing the certificate.

M. View Key Details

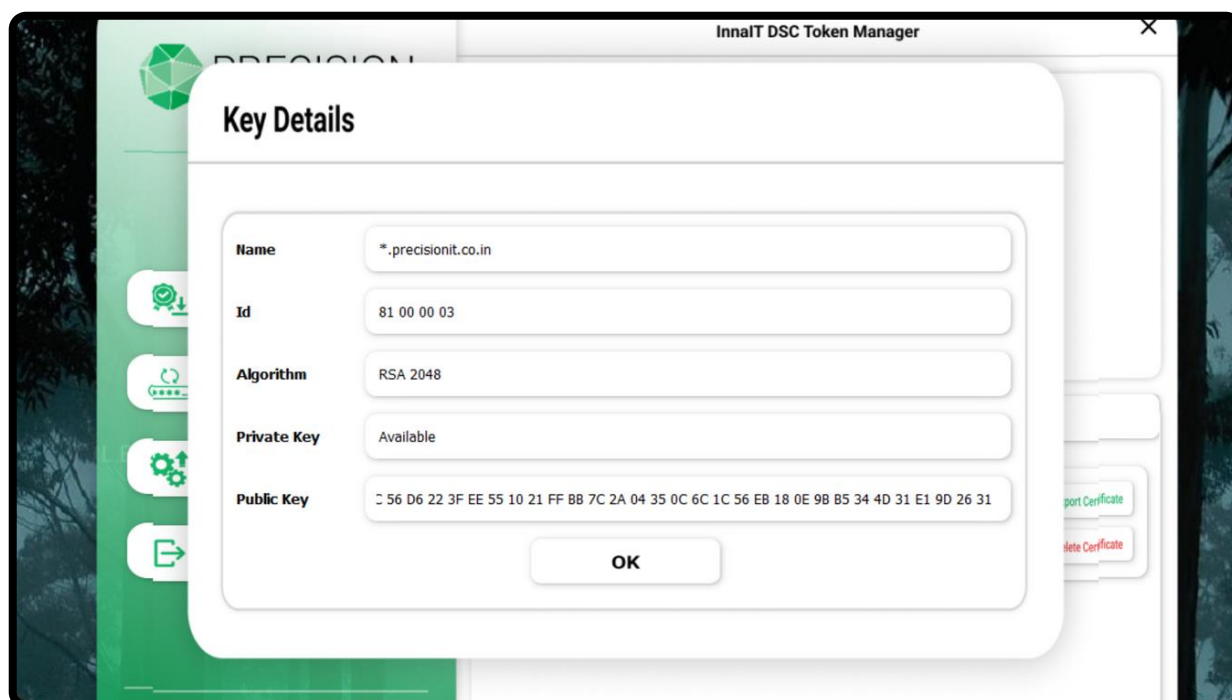


Step 1 – Login as a user and find the file that you would like to view the key details for, under either the “User Certificates” or “CA Certificates” tab.

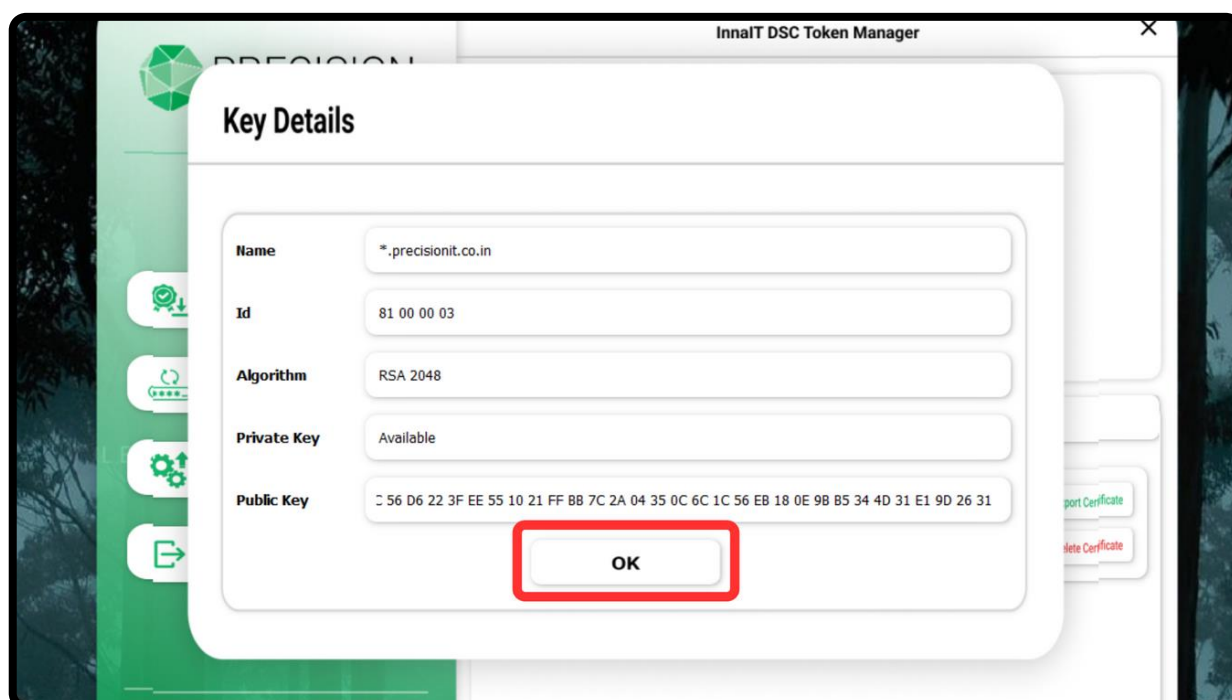


Step 2 – Now, click on the “View Keys” button next to the listing.

M. View Key Details

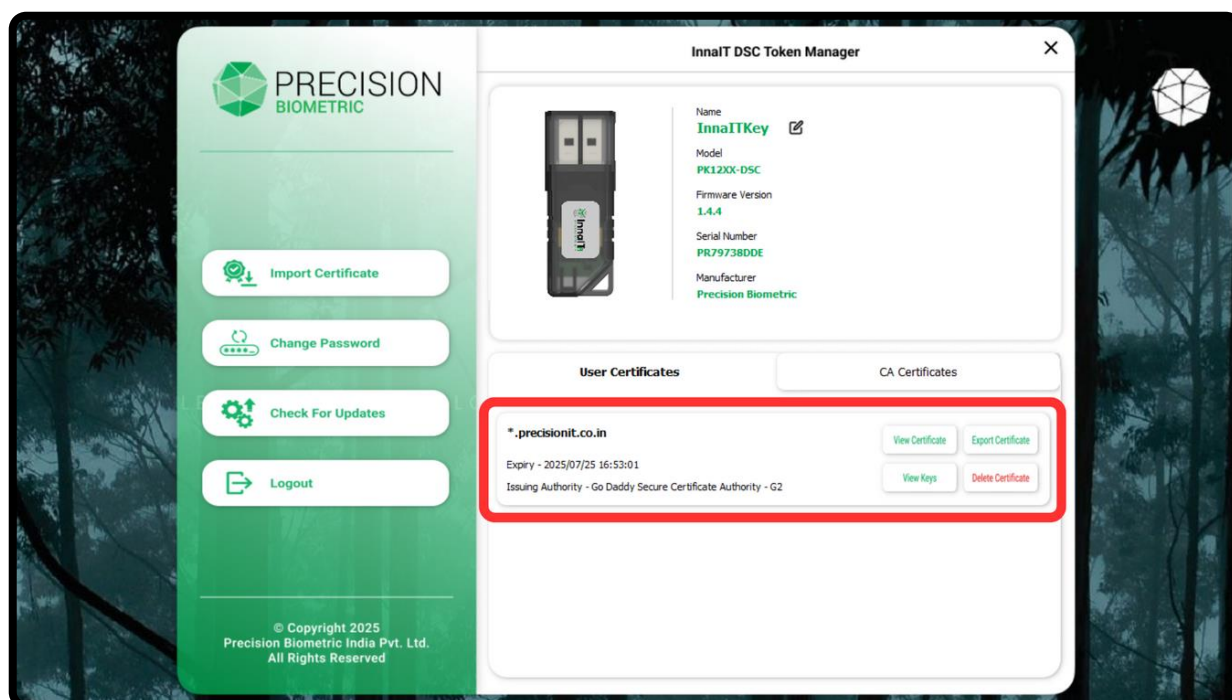


Step 3 – This will open a window which will display the key details of the file.

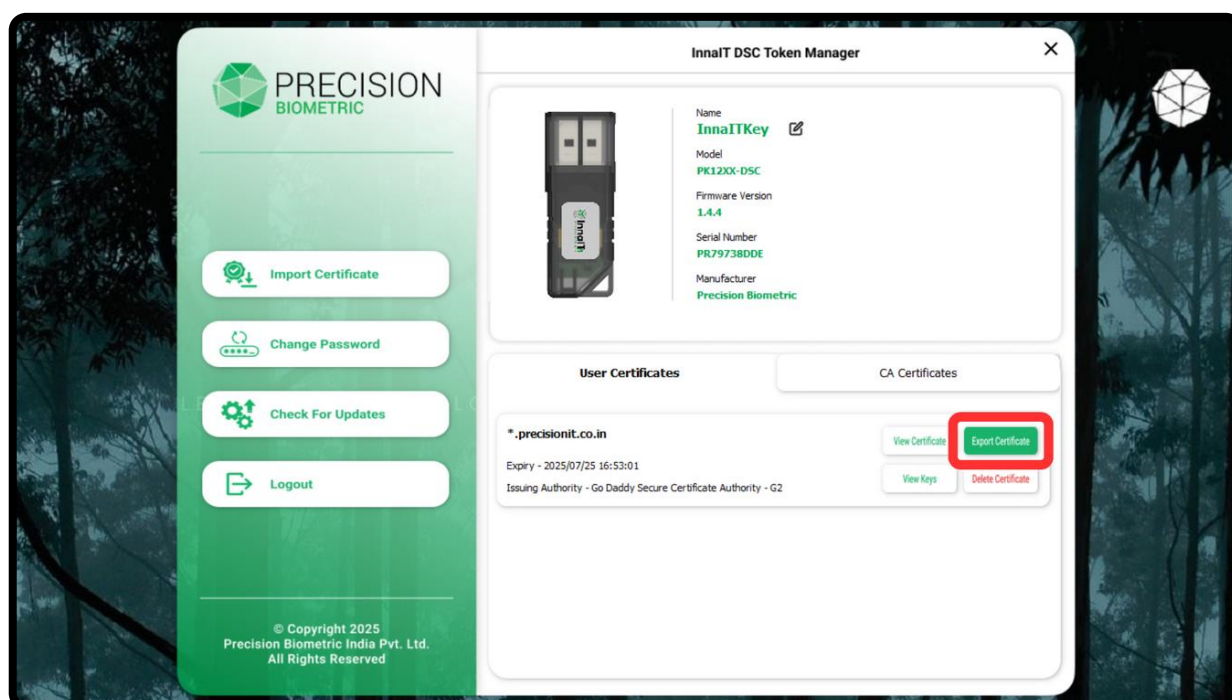


Step 4 – Click on "OK" once you are finished viewing the key details.

N. Export Certificate

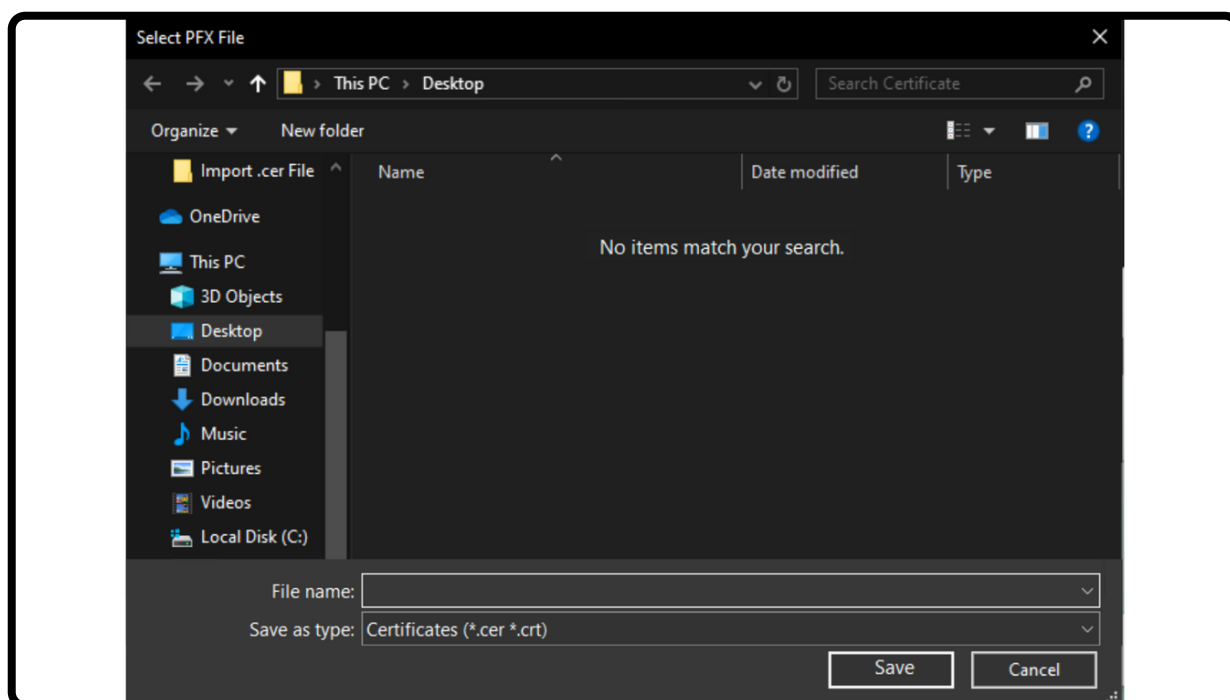


Step 1 – Login as a user and find the file that you would like to export, under either the “User Certificates” or “CA Certificates” tab.

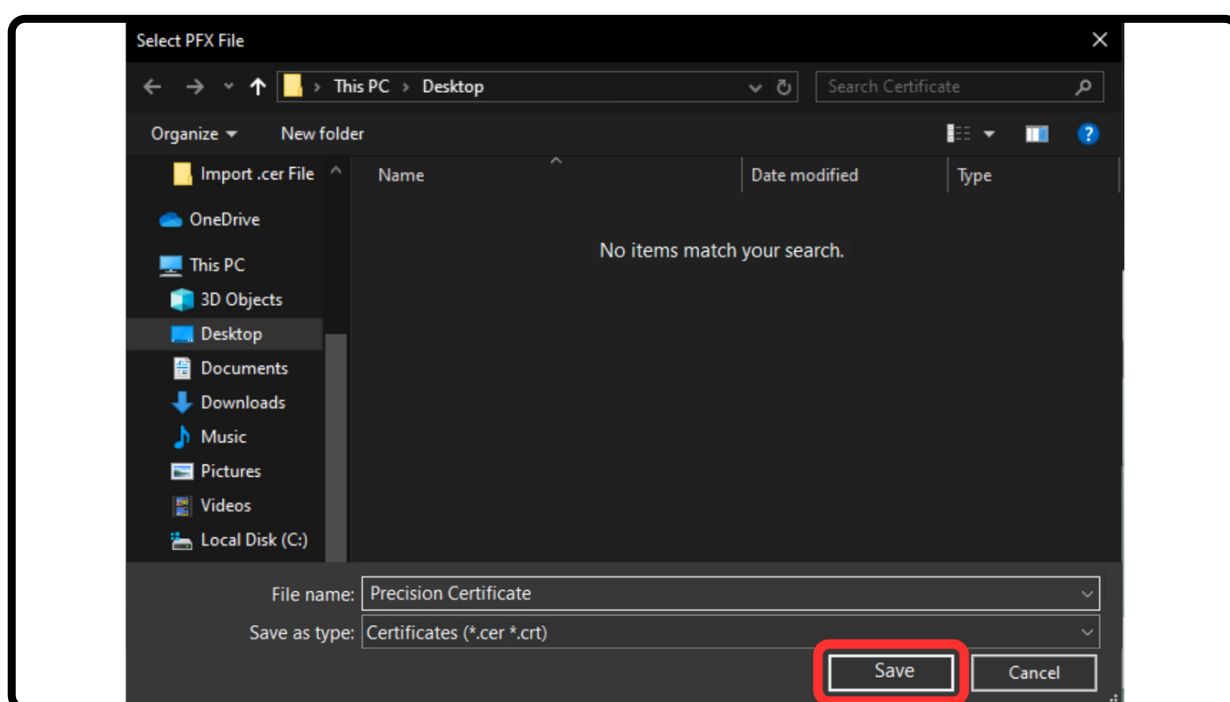


Step 2 – Now, click on the “Export Certificate” button next to the listing.

N. Export Certificate

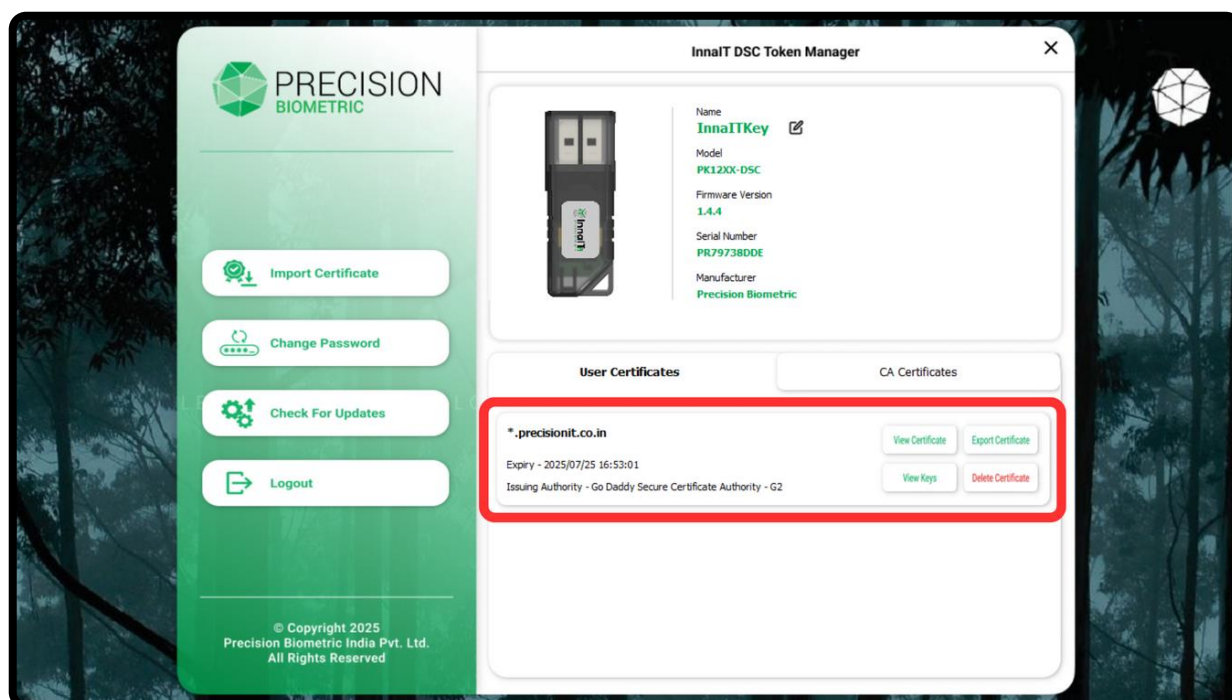


Step 3 – This will open a window where you will have to select the location where you would like to export the file to.

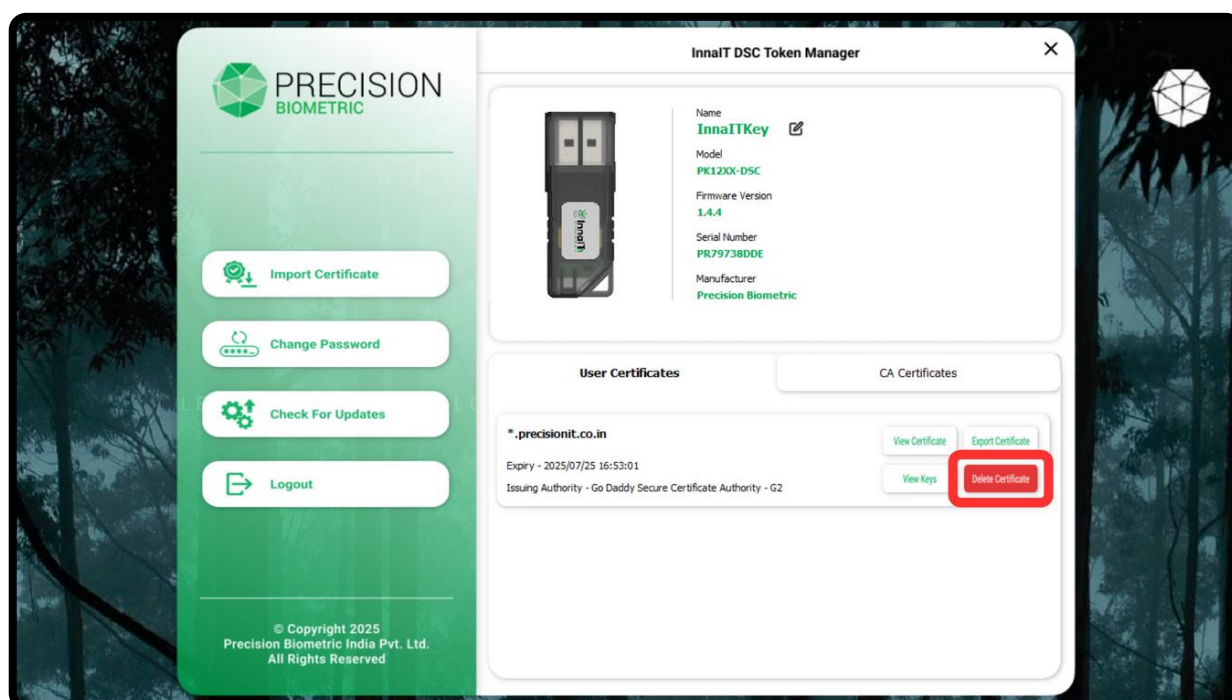


Step 4 – After this, enter a name for the exported file and click on “Save” to export the certificate

O. Delete Certificate

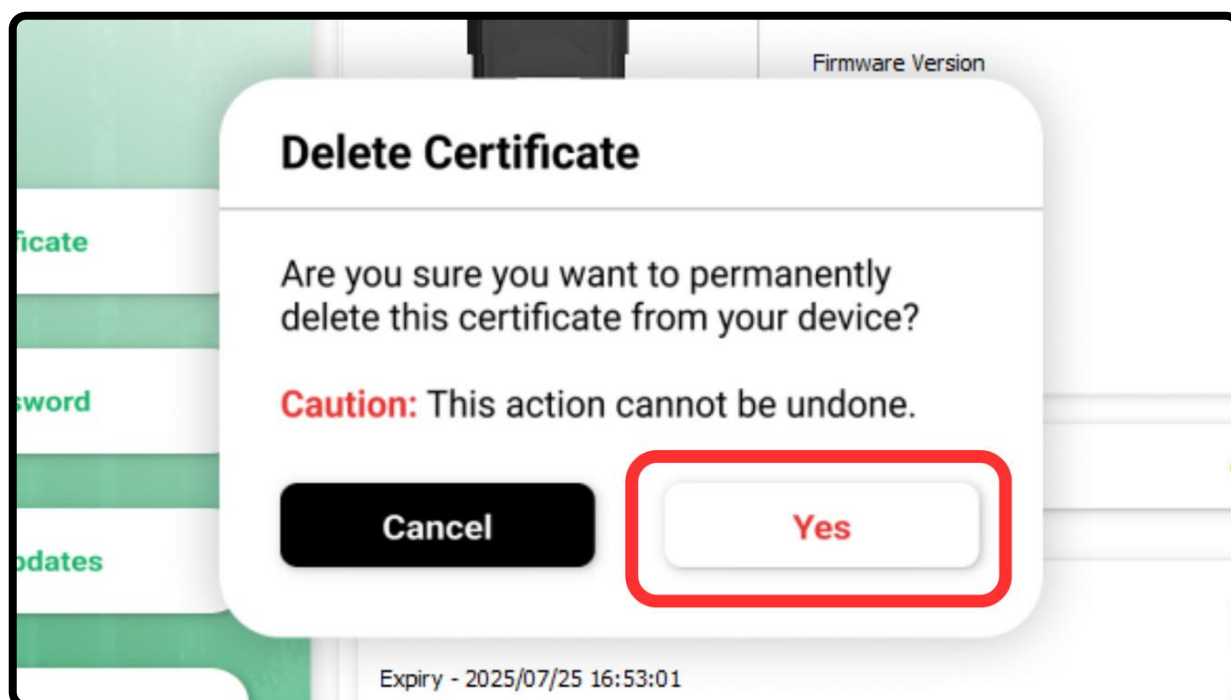


Step 1 – Login as a user and find the file that you would like to delete, under either the “User Certificates” or “CA Certificates” tab.

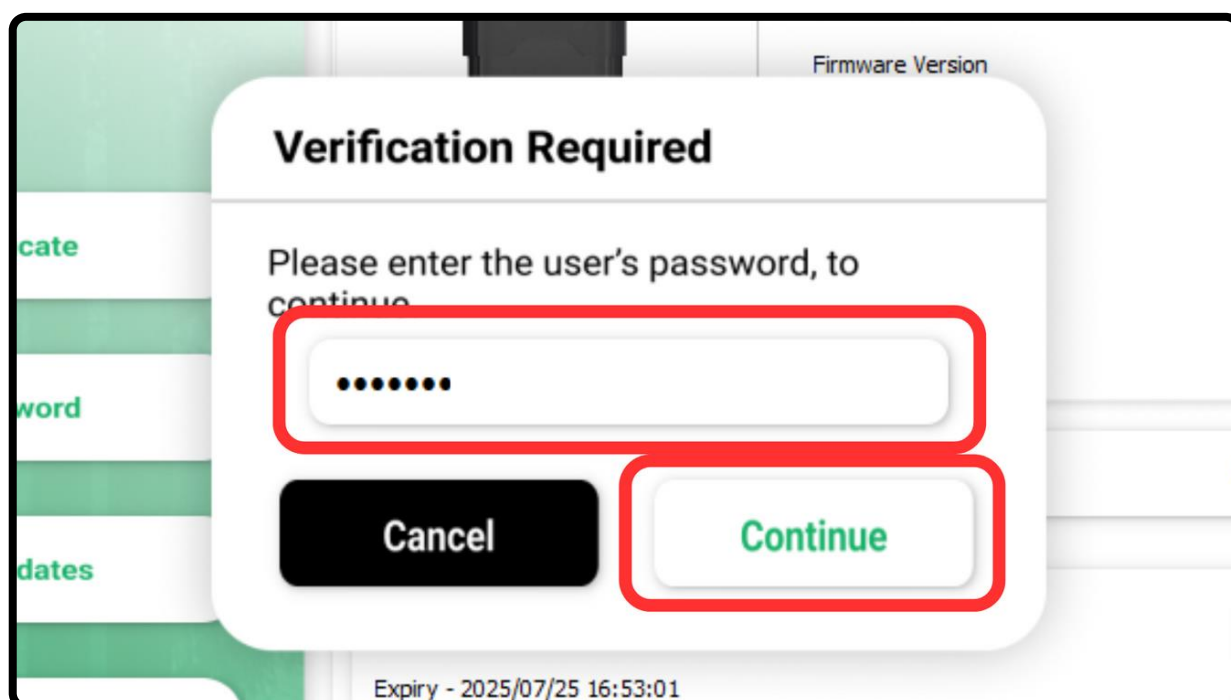


Step 2 – Now, click on the “Delete Certificate” button next to the listing.

0. Delete Certificate

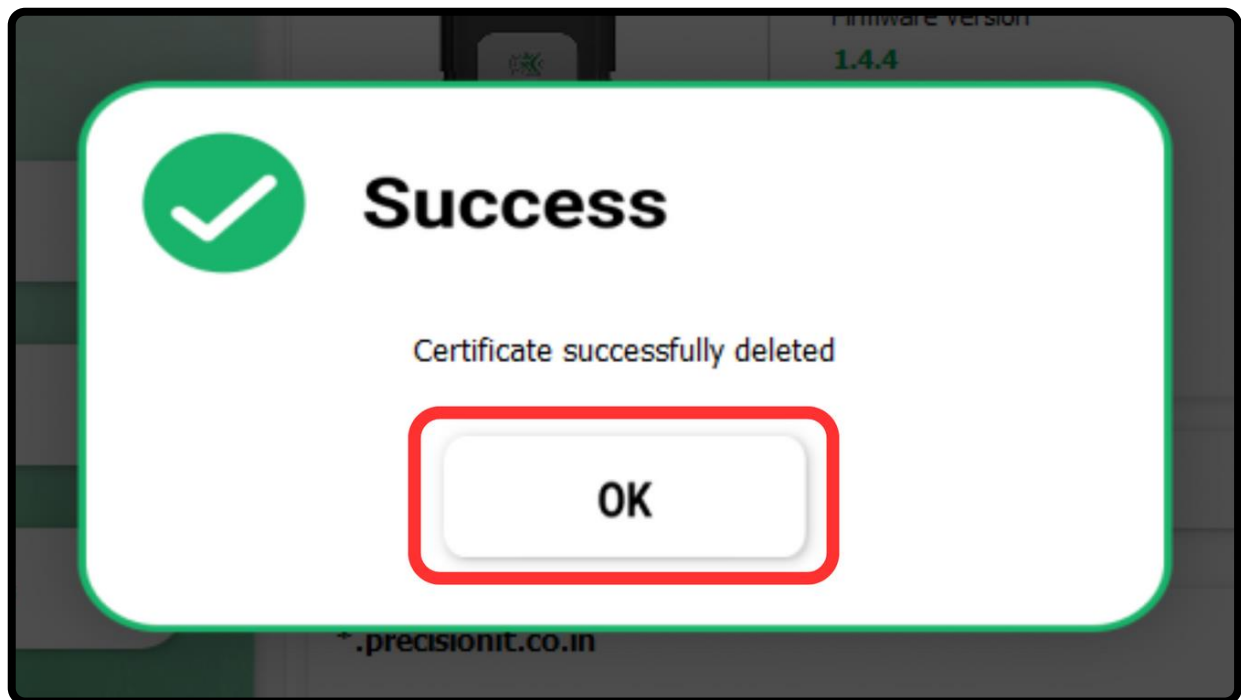


Step 3 – You will be asked to confirm your action since it is not reversible. Click on “Yes” to do so.



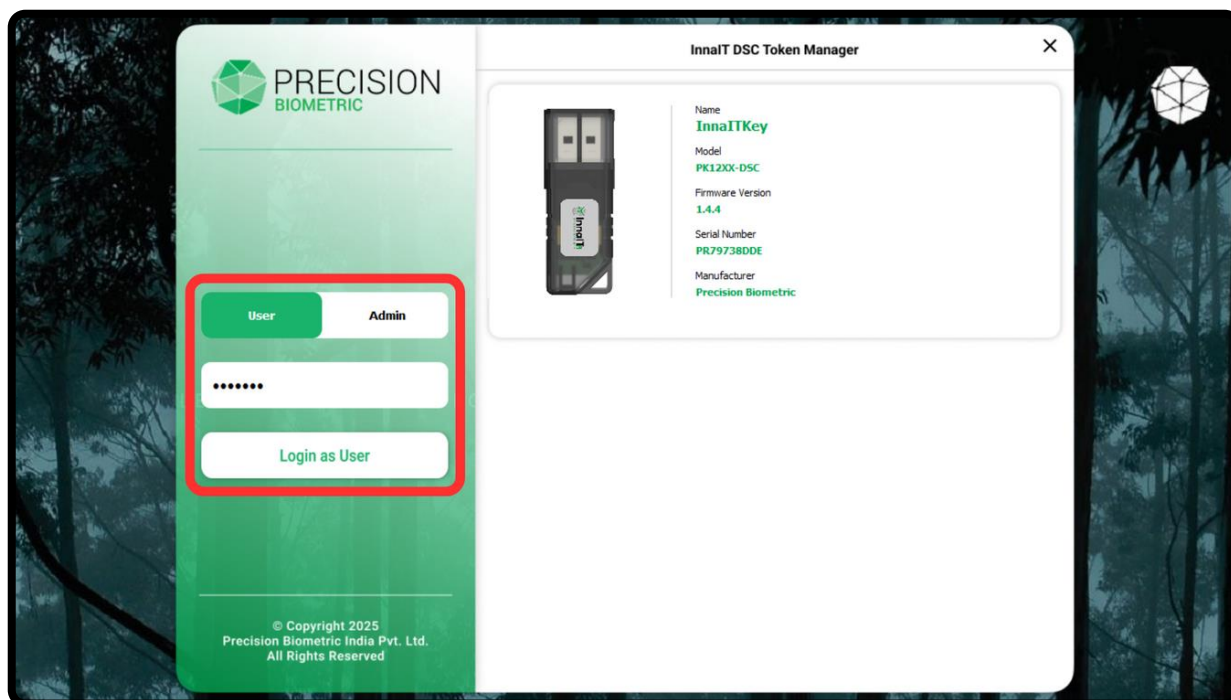
Step 4 – Now, you must enter your **User Password** and then click on “Continue”, to proceed.

O. Delete Certificate

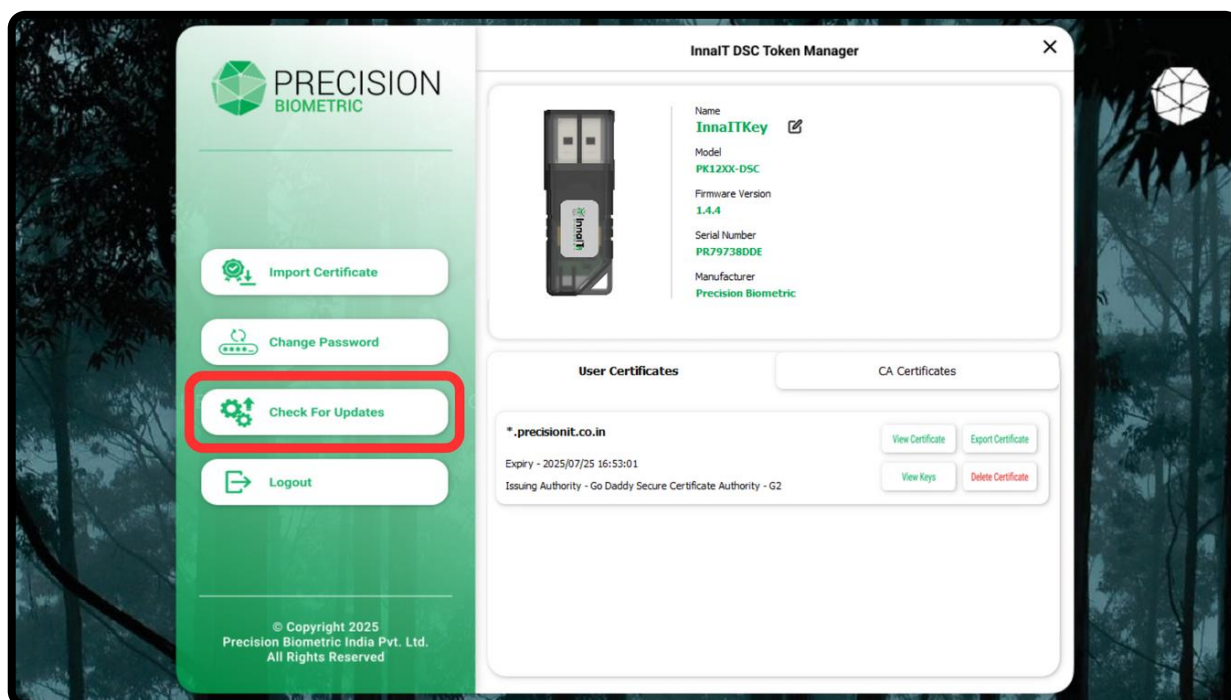


Step 5 – Once it is deleted, you will get a “Success” dialogue box. Click on “OK” to continue.

P. Update Software

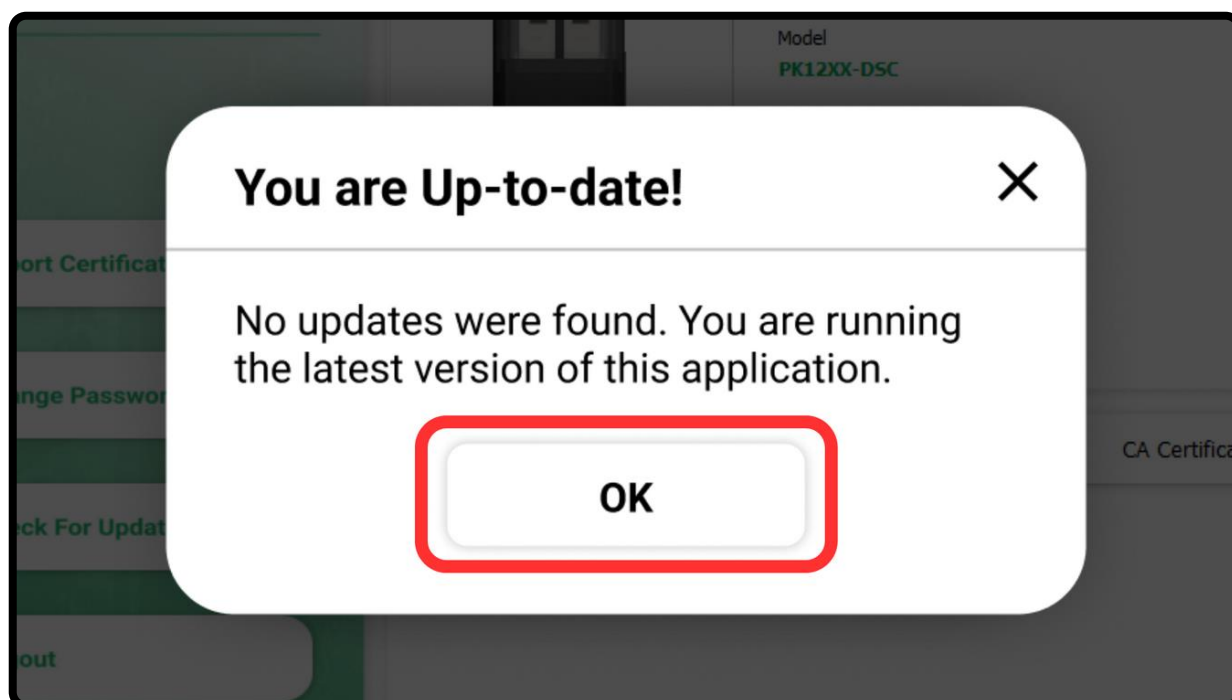


Step 1 – Login as a user.

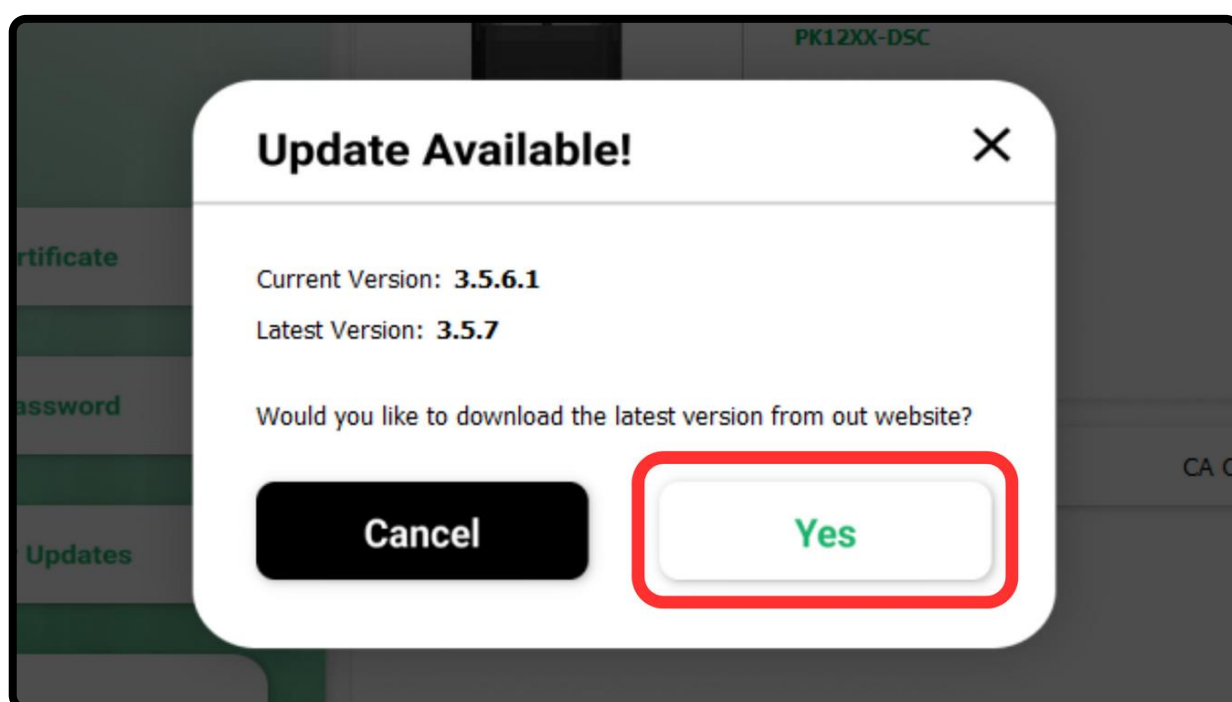


Step 2 – Click on the “Check for Updates” button.

P. Update Software

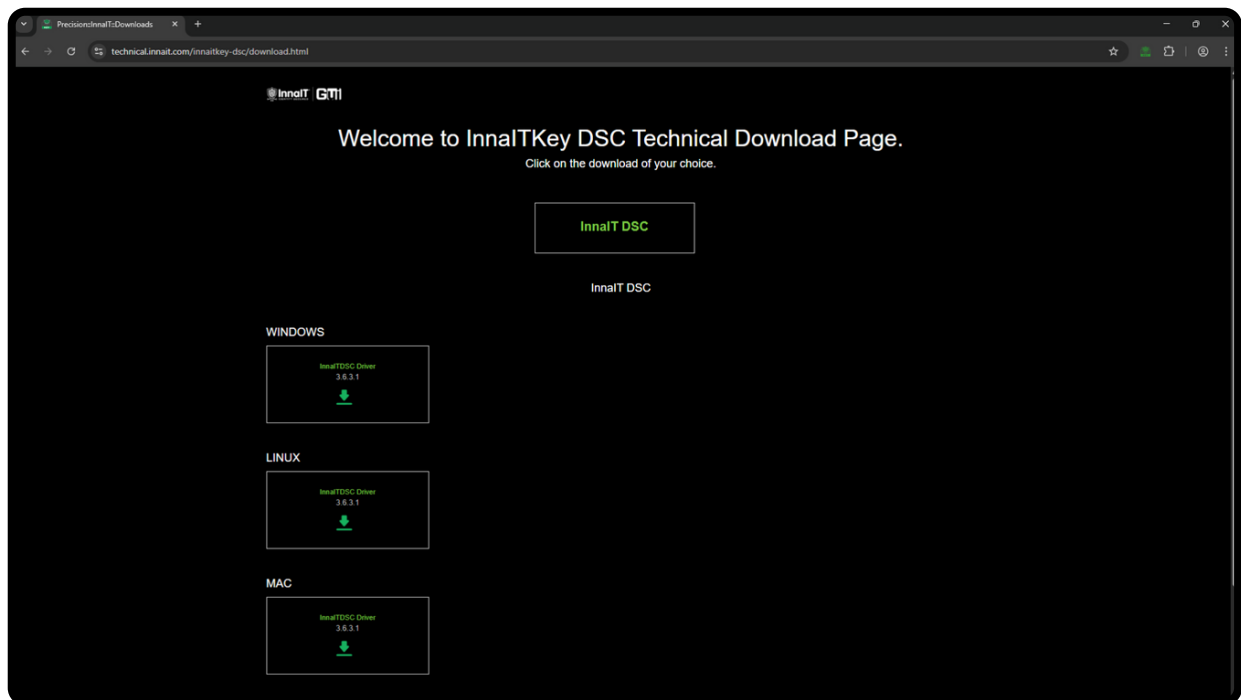


Step 3 – If you are on the latest version, you will get a pop-up saying that you are up to date. Click on “OK” to go back.



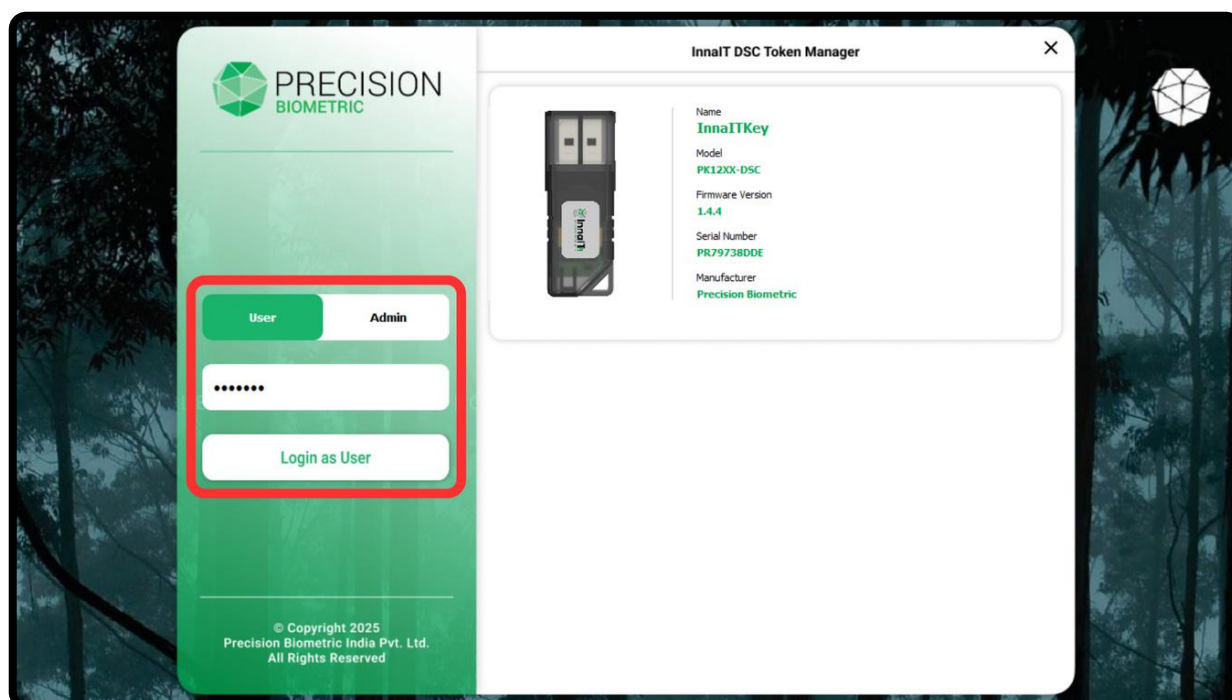
Step 4 – If there is an update, you will get a pop-up showing information about the new version. Click on “Yes” to go to our downloads page.

P. Update Software



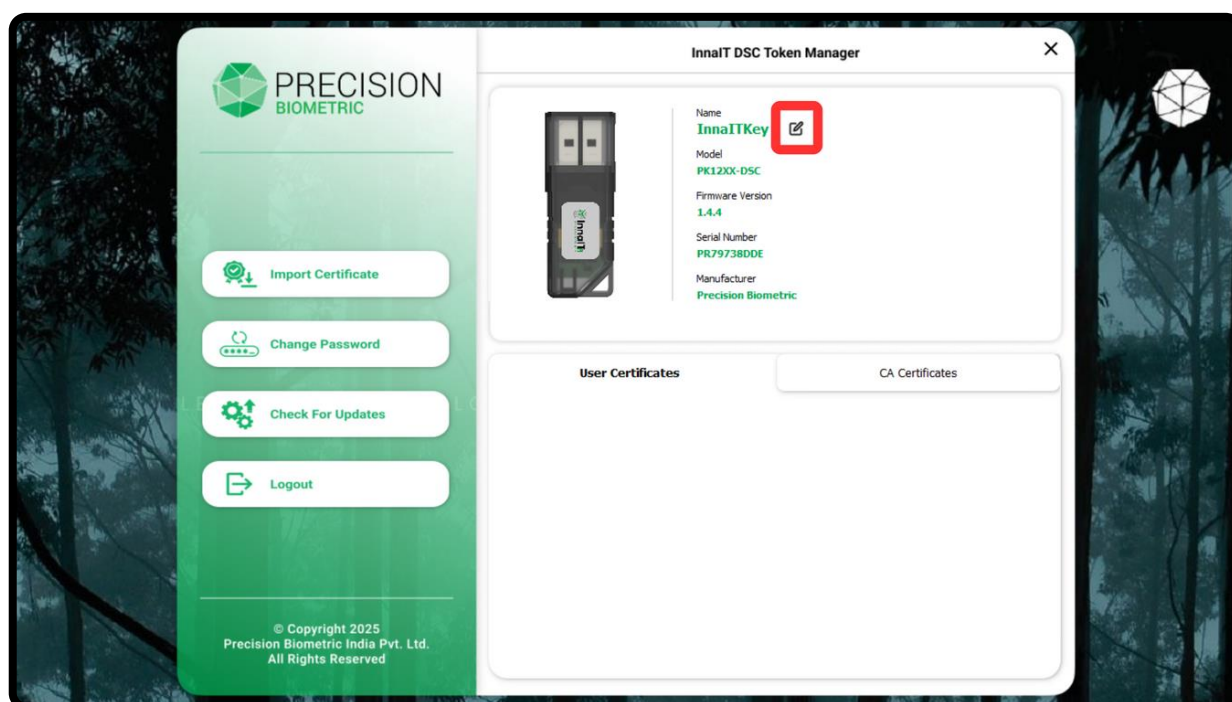
Step 5 – From here, you can download and install the latest version of the application.

Q. Renaming Token



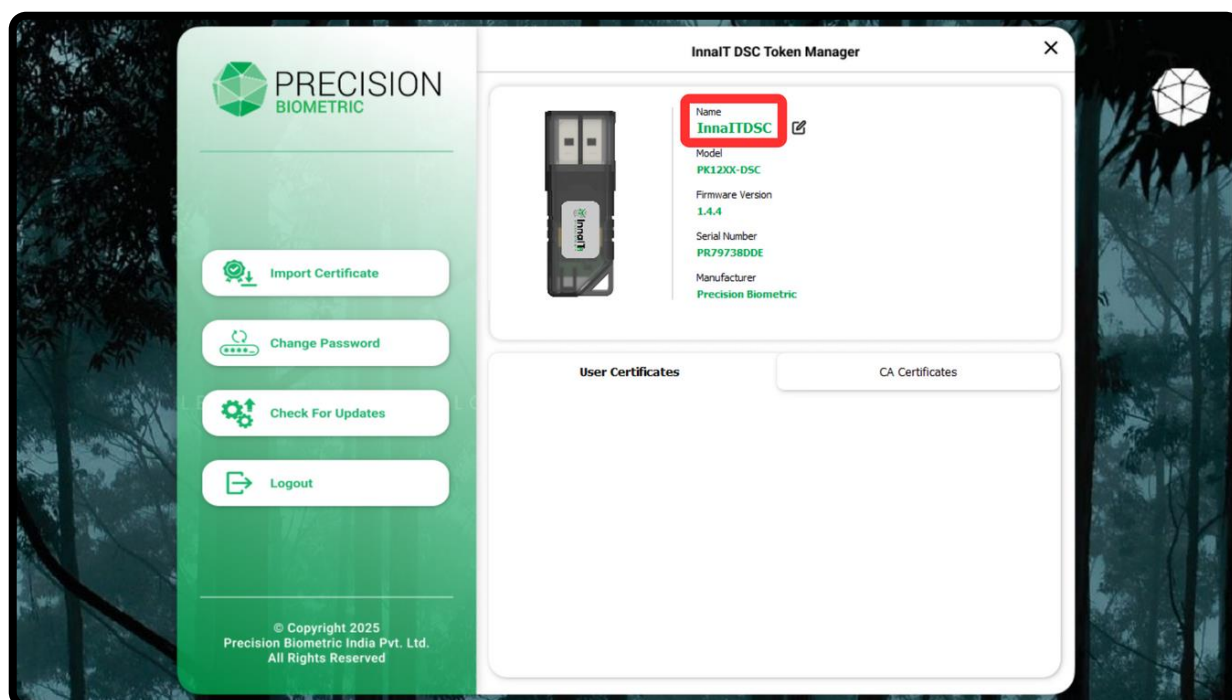
Step 1 – Login as a user.

Note: Only users can rename the token.

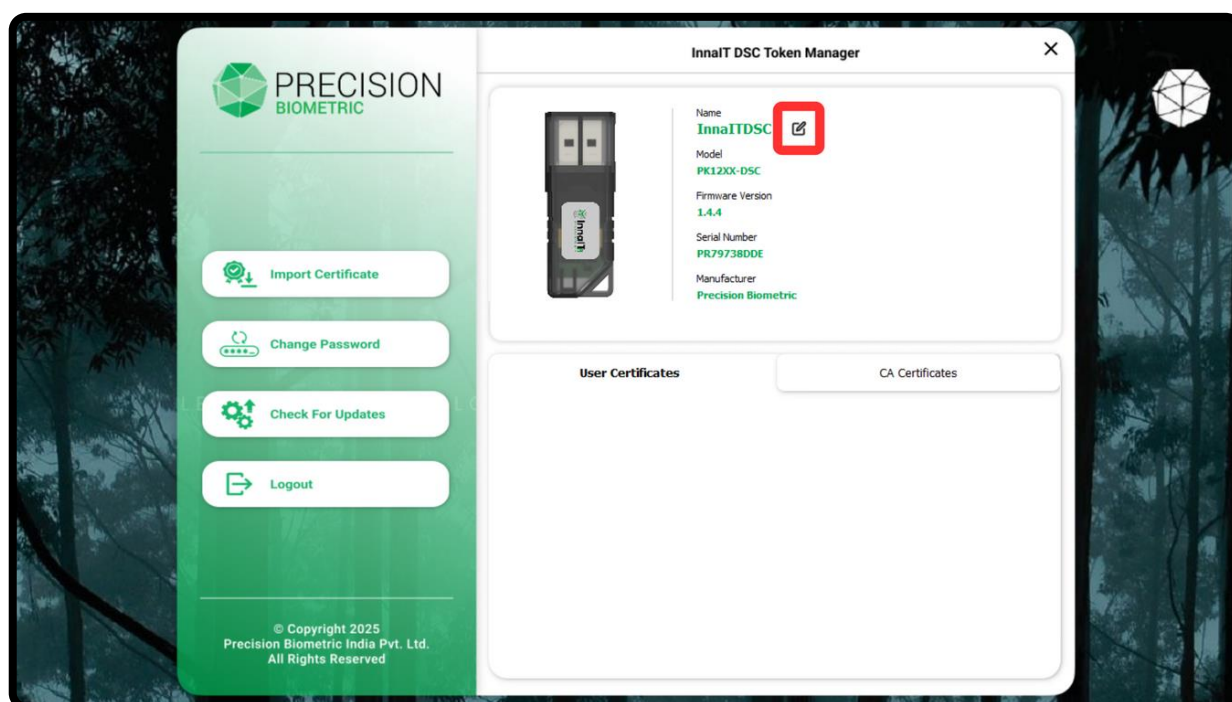


Step 2 – Click on the edit icon next to the “Name” field in the device information section.

Q. Renaming Token

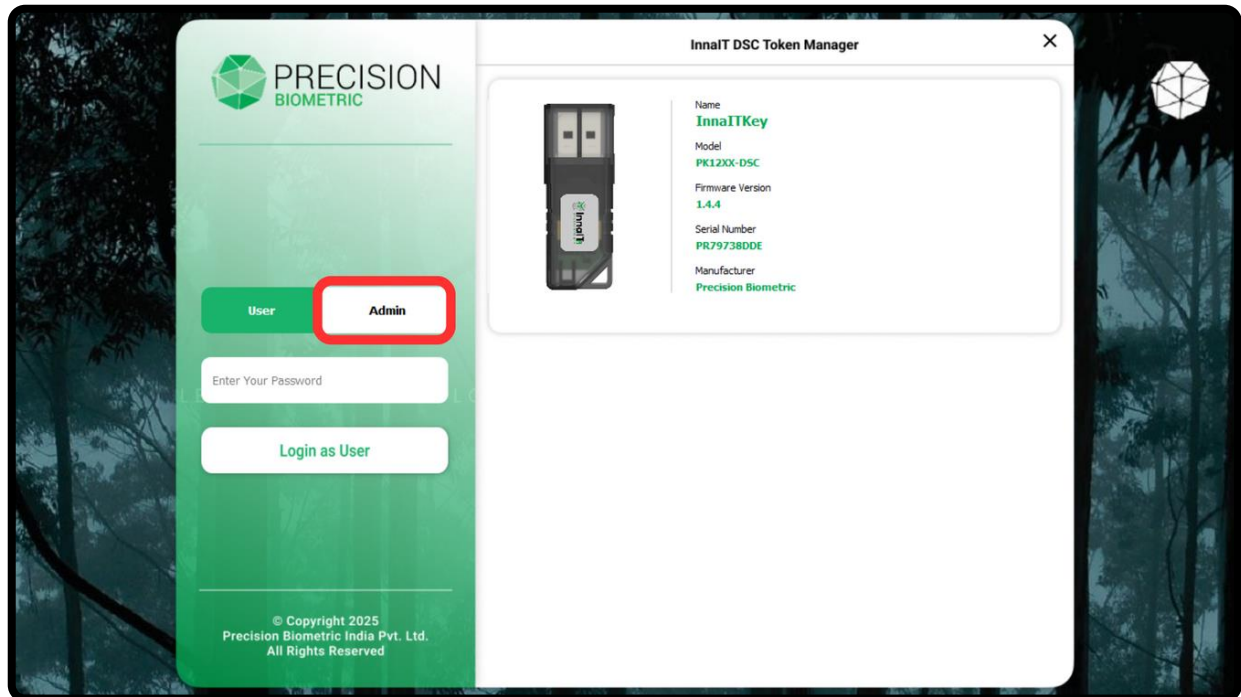


Step 3 – You can now edit the name of the token by clicking on the current name and changing it.



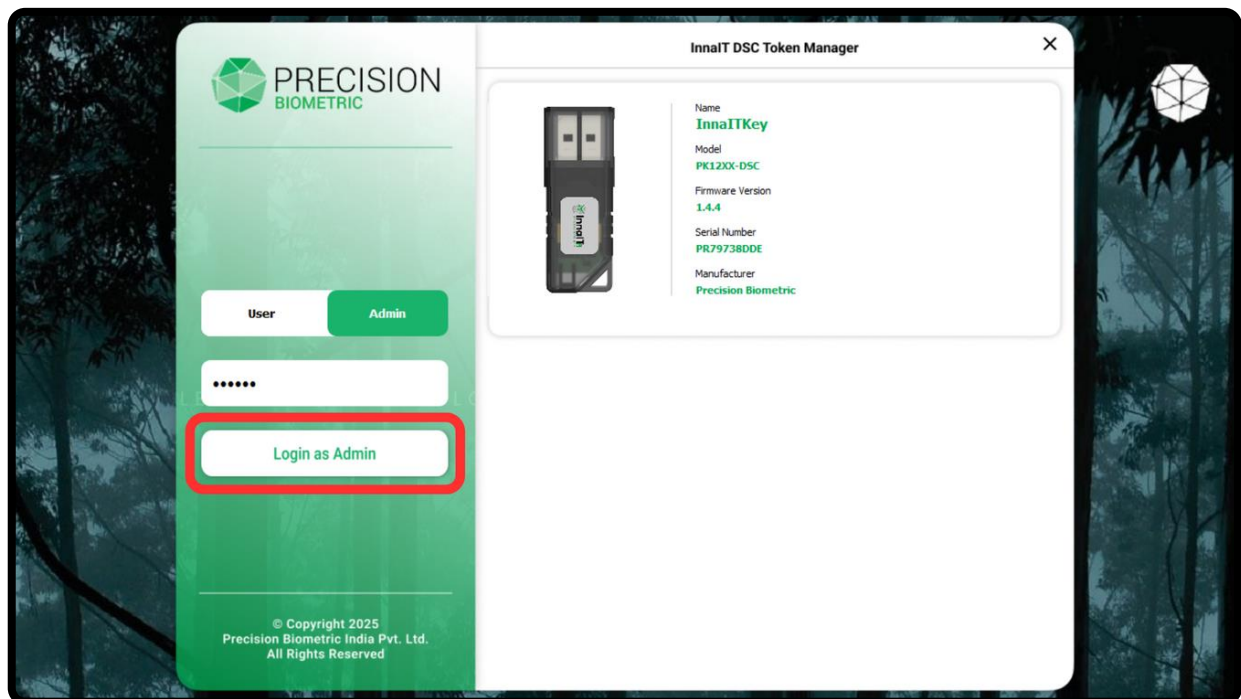
Step 4 – After editing the name, click on the edit button again to confirm the change.

R. Zeroize Key



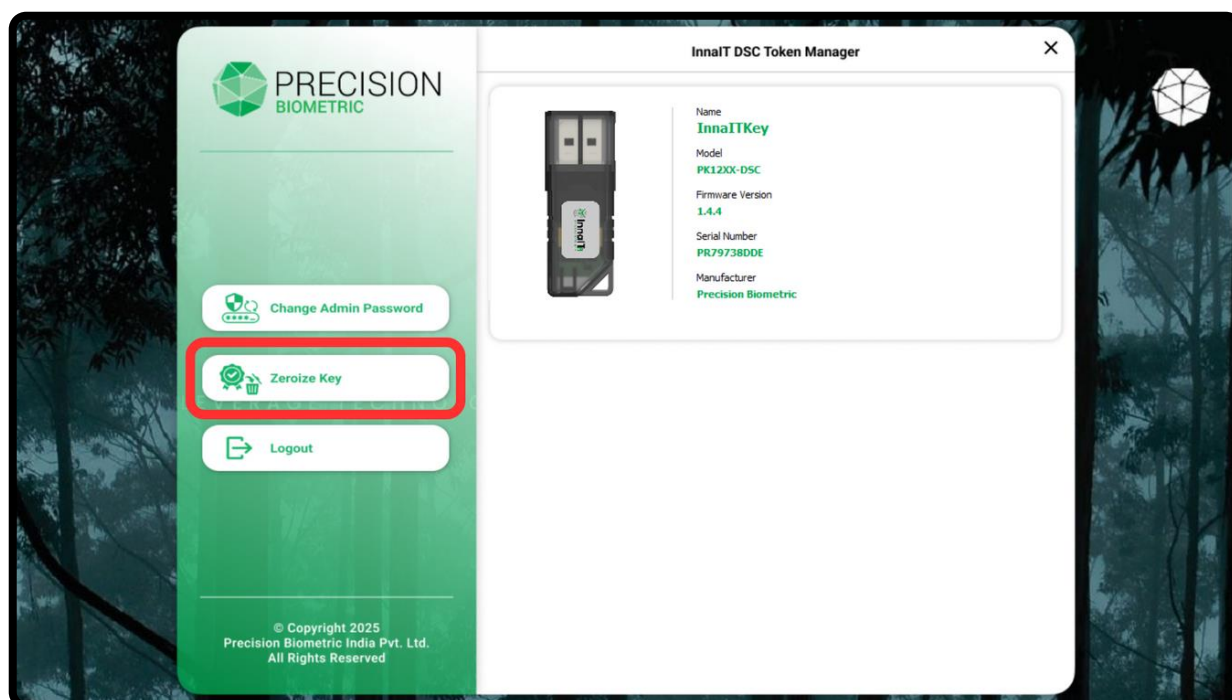
Step 1 – In the login page, click on “Admin” to login as an administrator.

Note: If this is your first time logging in as an administrator, you can use the default admin password, which is **123456**.



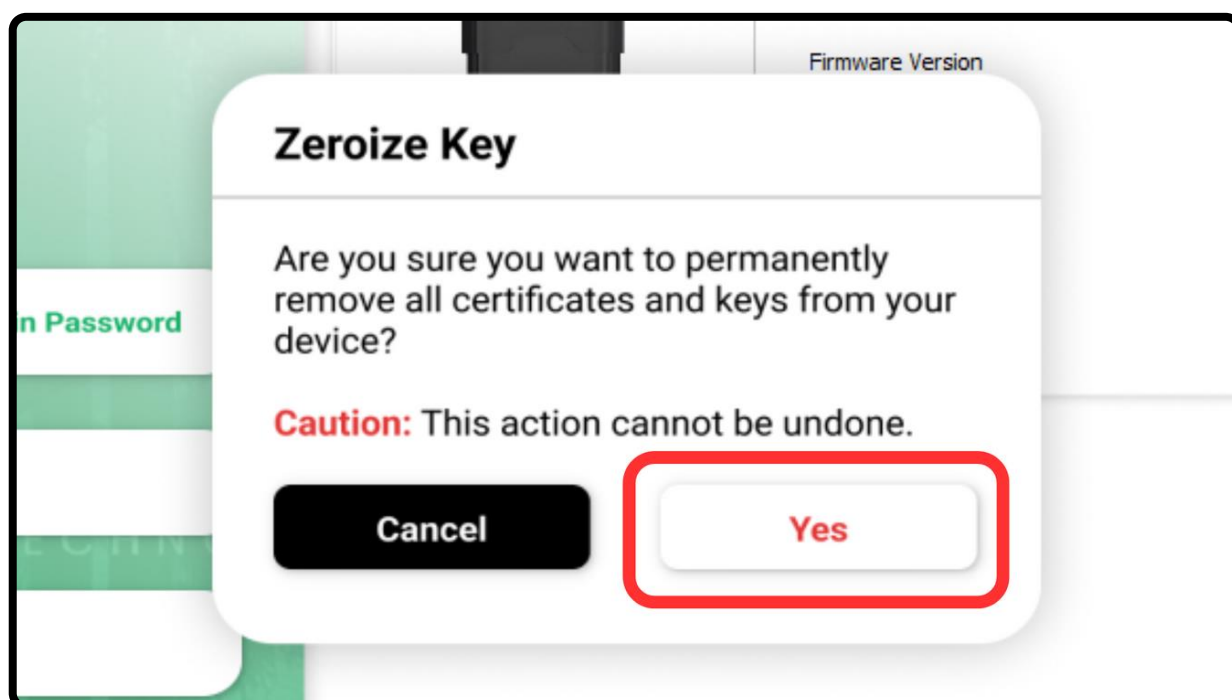
Step 2 – Enter the admin password and then click on “Login as Admin”.

R. Zeroize Key



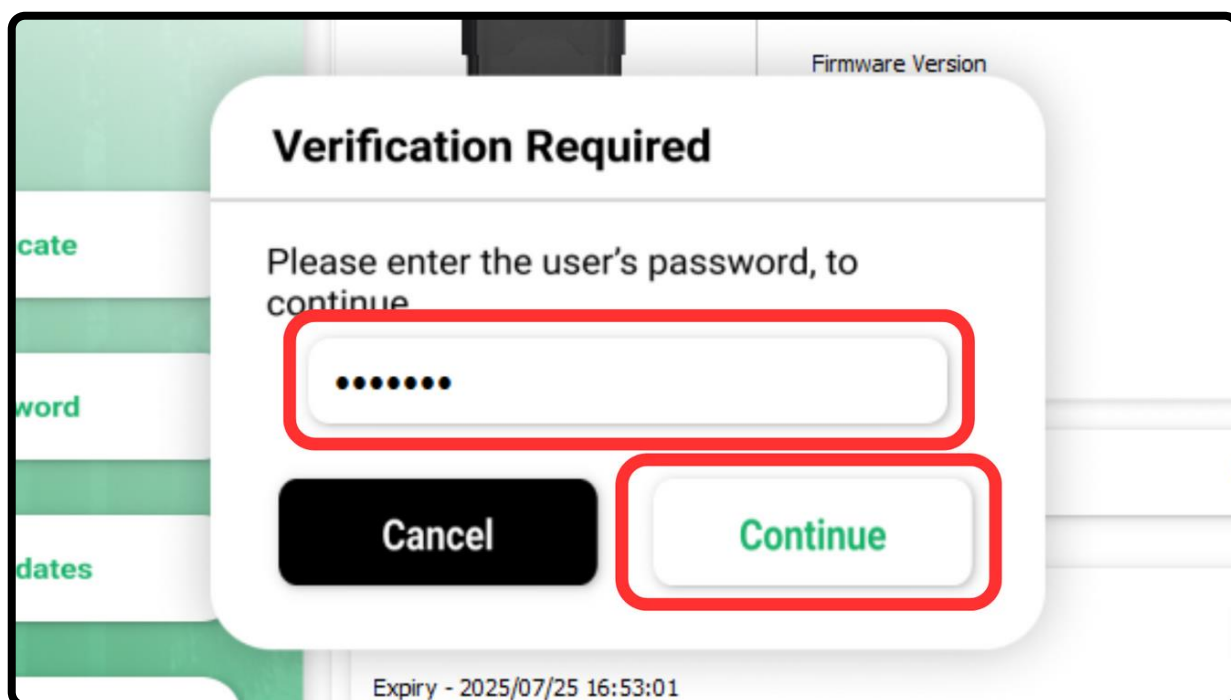
Step 3 – To Zeroize your keys, you can click on the “Zeroize Key” button.

Note: Zeroization is the process by which all the Keys and Certificates stored on the token can be permanently removed.

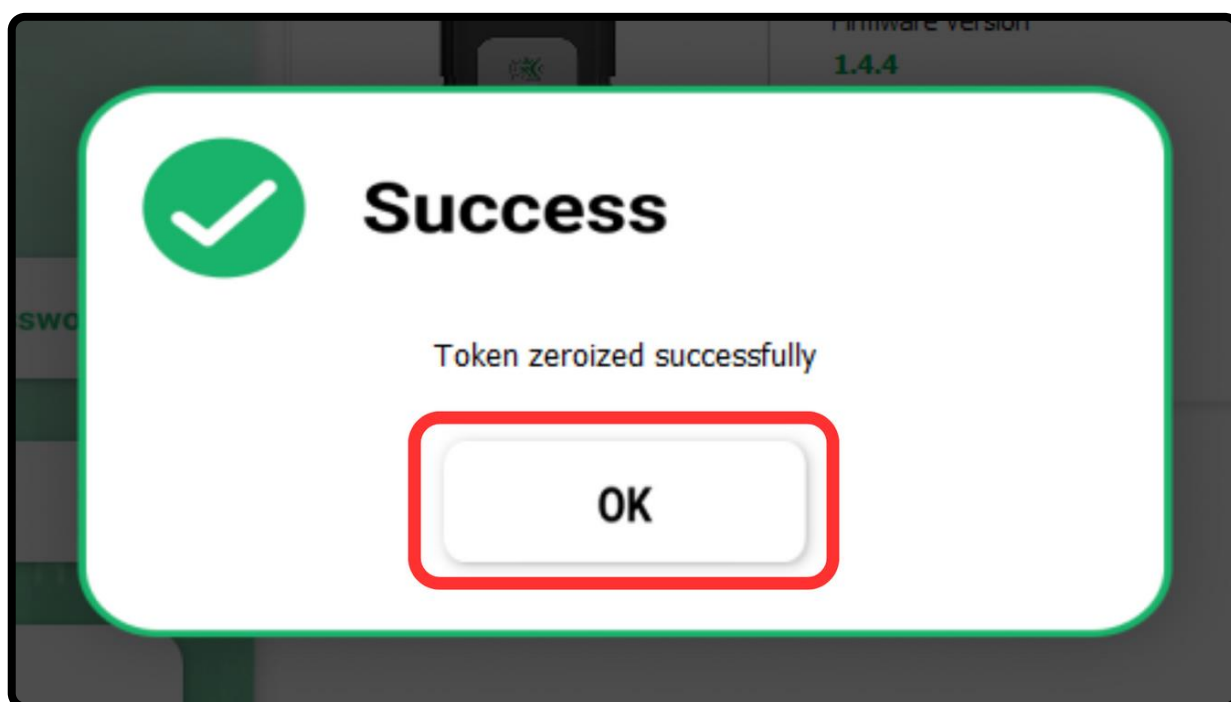


Step 4 – You will be asked for confirmation as this action is not reversible. Click “Yes” to proceed.

R. Zeroize Key

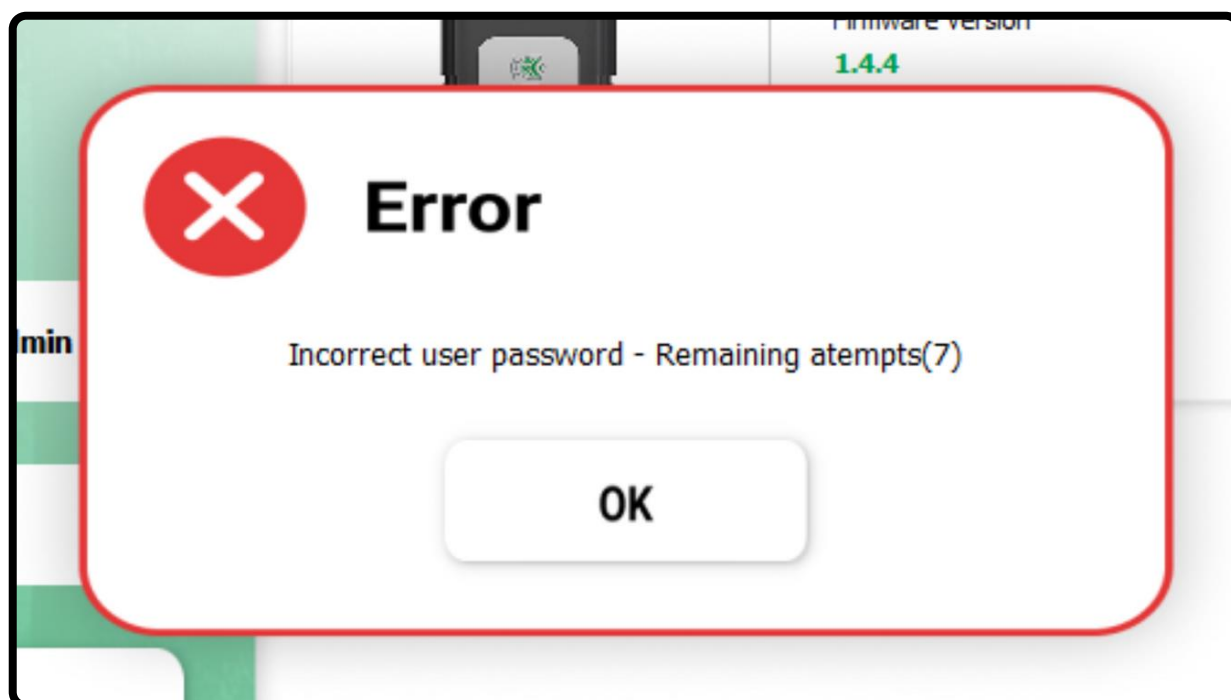


Step 5 – Finally, enter your **User Password** and click on “Continue”.

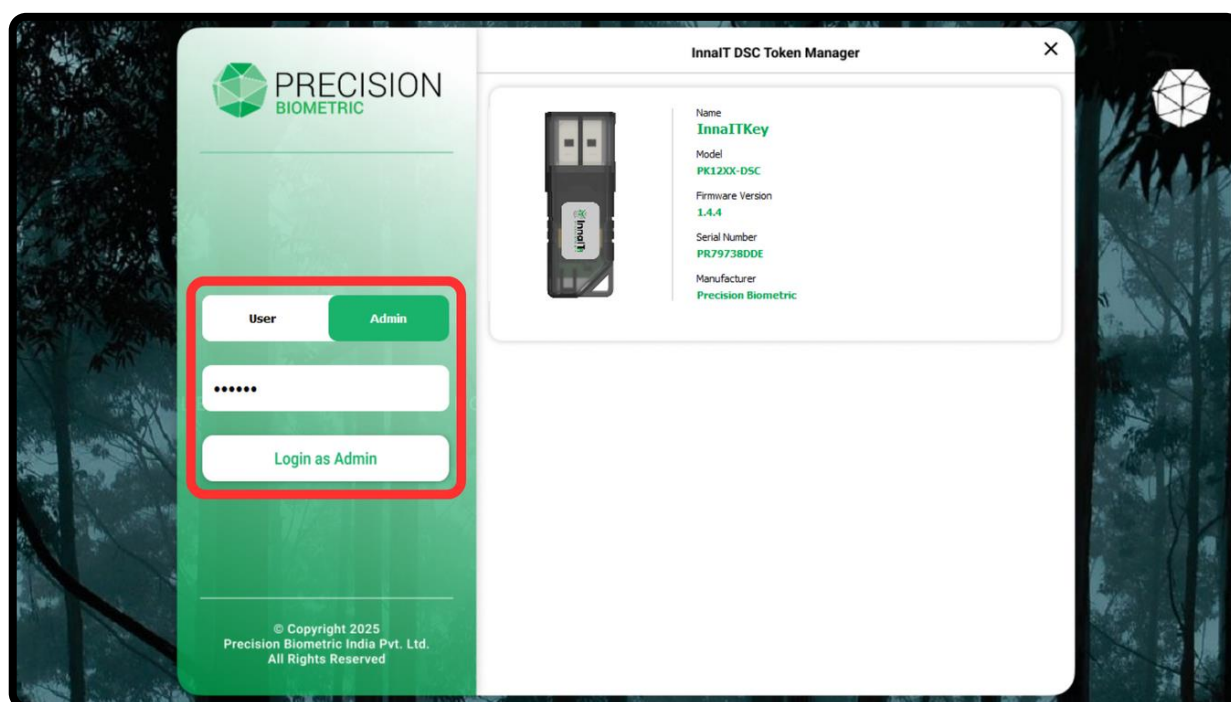


Step 6 – Once the Zeroization is complete, you will get a “Success” dialogue box. Click “OK” to continue.

S. Resetting Locked Token

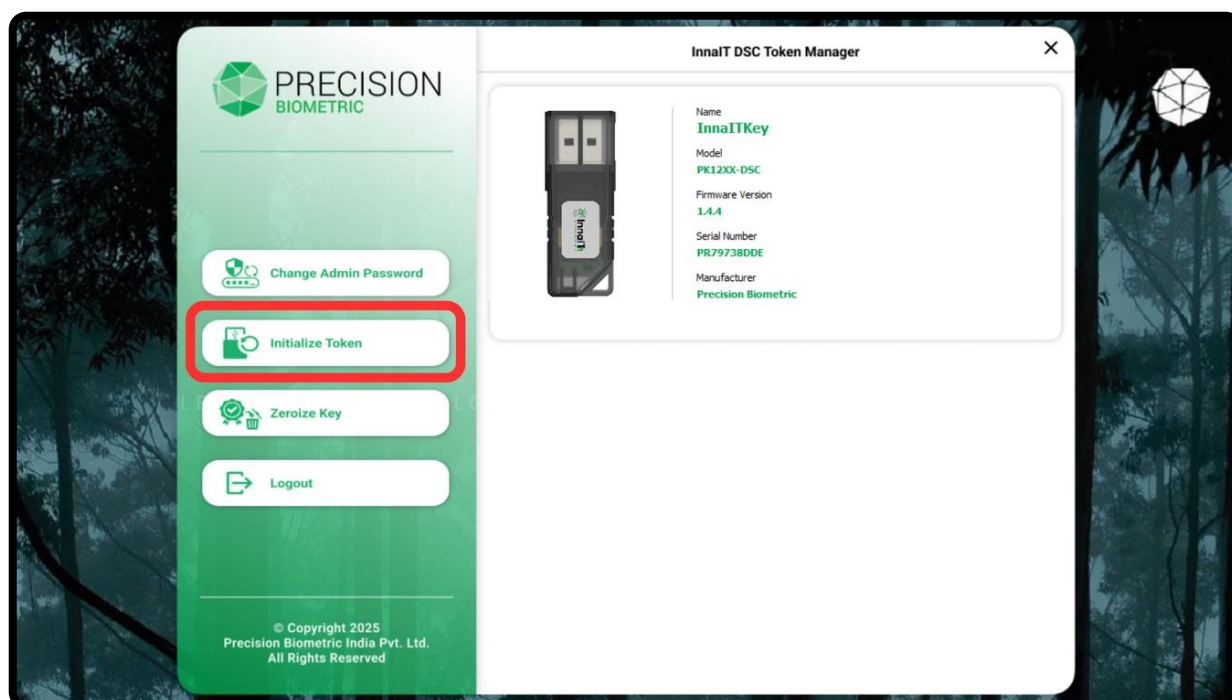


Info – The InnaIT DSC Token will get locked after 8 incorrect login attempts (Incorrect Password). The only way to unlock a token after this, is to initialize it again. This will reset the user and admin passwords to the default and remove all stored keys and certificates.

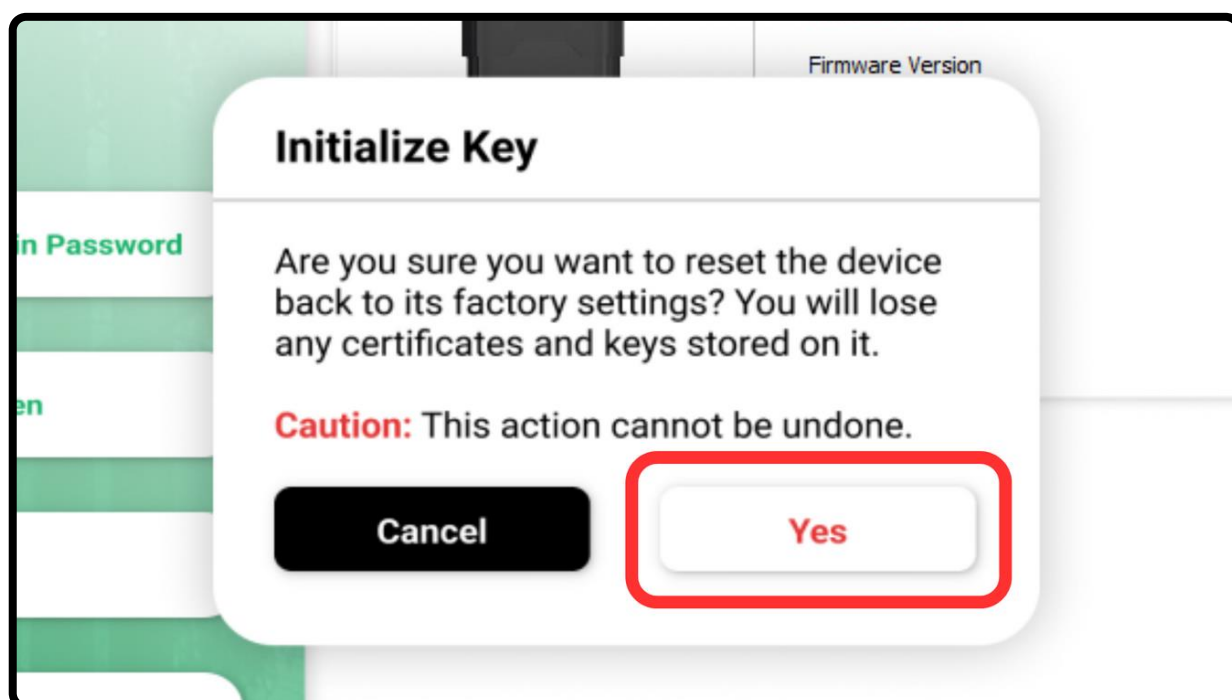


Step 1 – If your token is locked, you need to reset it by logging in as an administrator.

S. Resetting Locked Token

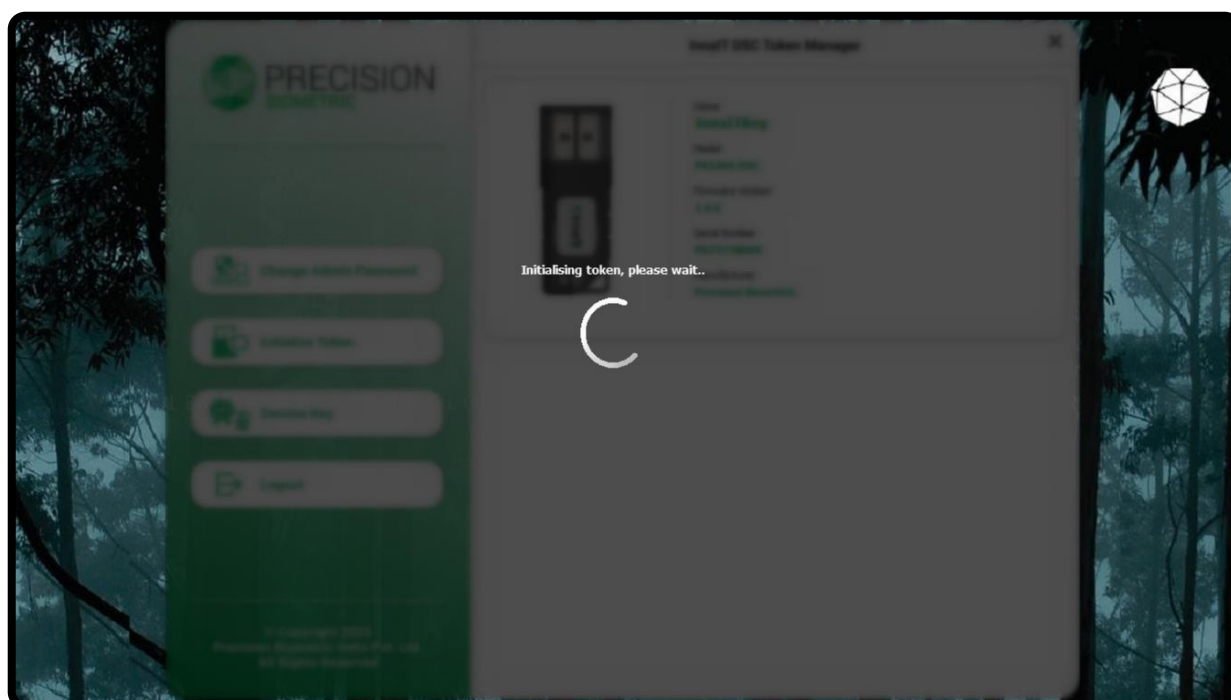


Step 2 – After logging in, click on the “Initialize Token” button.



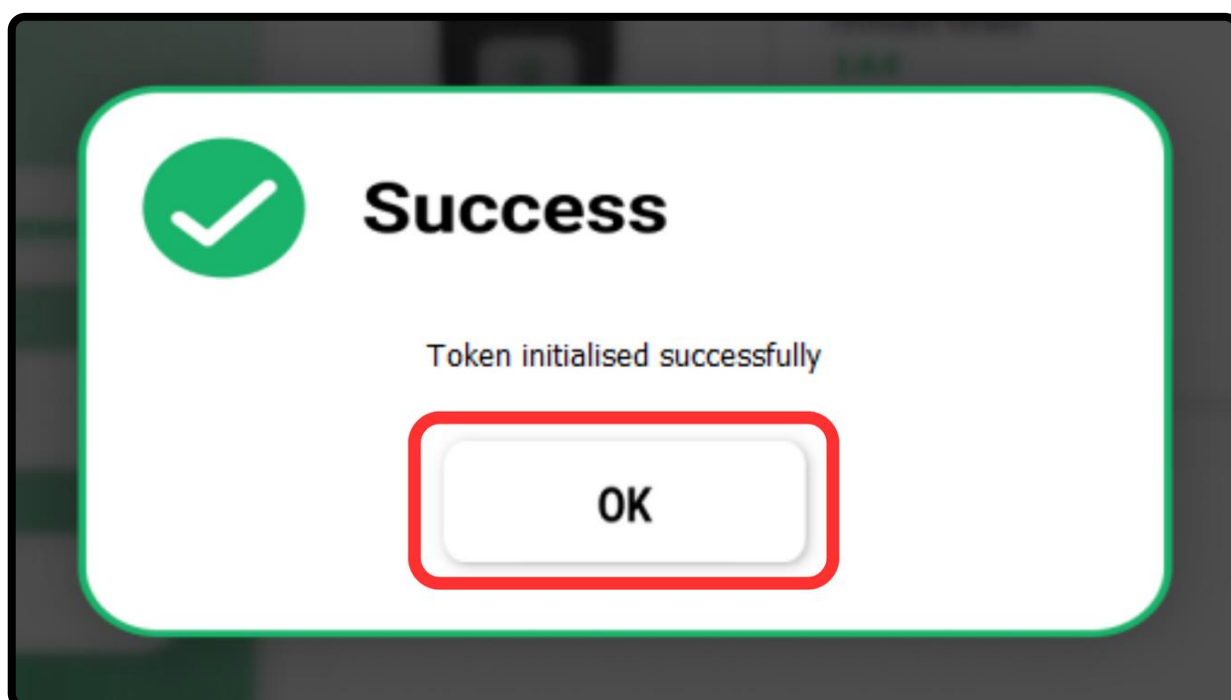
Step 3 – You will be asked to confirm your action as it is not reversible. Click “Yes” to do so.

S. Resetting Locked Token



Step 4 – Please wait for the initialization to get completed.

Note: Please DO NOT unplug your token while it is being initialized.



Step 5 – You will get a “Success” dialogue box once it is done. Click “OK” to continue.

Note: You will now have to setup the token as a fresh device, as shown in the “B. First Login (Token)” section

T. Setting up Document Sign (Linux)

Note - After installing the InnaIT DSC Token Manager application on your Linux PC, you can set it up to sign documents. Following are the steps to do so.

Step 1 - Open the terminal and execute the following commands to reset and remove any existing Firefox database. You can skip this step if you are using a freshly installed instance of Linux on your PC.

```
pkill -f firefox
```

```
rm -rf ~/.mozilla/
```

Step 2 - Now, give the InnaIT PKCS11 driver execution permissions using the following command. You will be prompted to enter your “sudo” password at this step.

```
sudo chmod 644  
/opt/Precision_Biometric/InnaITDSC/  
libraries/libInnaITPKCS11Driver.so
```

Step 3 - Create a directory for the Firefox database using the following command.

```
mkdir -p  
~/.mozilla/firefox/profile.default
```

Step 4 - Once the installation is complete, or if you already have the “certutil” tool installed, use the following command to set an empty password for your database profile.

```
certutil -N -d  
~/.mozilla/firefox/profile.default  
--empty-password
```

Note - To proceed, the “certutil” tool must be installed on your PC. Use the following command to install it, if you do not already have it. You will be prompted to enter your “sudo” password at this step.

```
sudo apt install libnss3-tools
```

T. Setting up Document Sign (Linux)

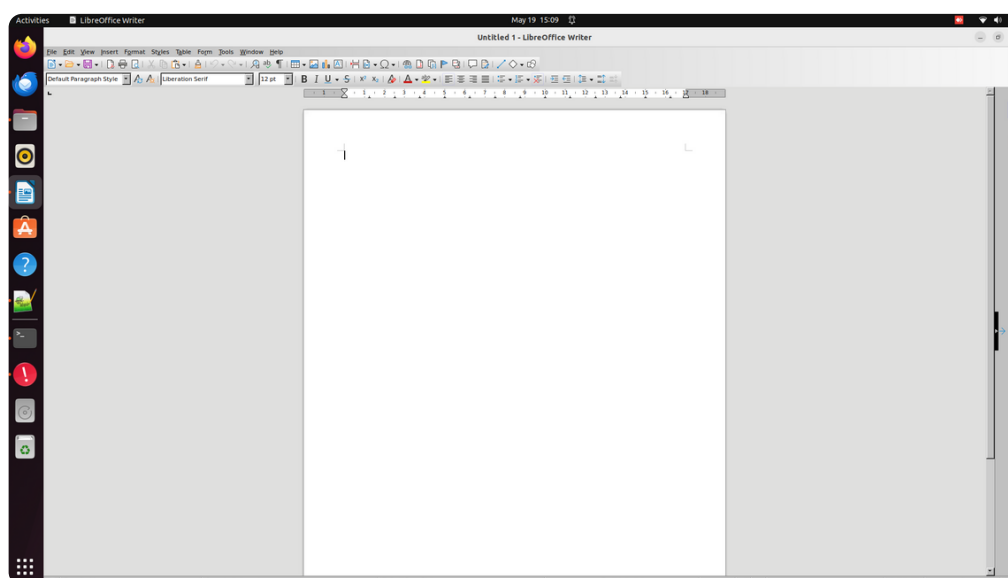
Step 5 - Now, add the InnaITKey to your Firefox database using the following command.

```
modutil -add "InnaITKey" -libfile  
/opt/Precision_Biometric/InnaITDSC/  
libraries/libInnaITPKCS11Driver.so  
-dbdir  
~/.mozilla/firefox/profile.default
```

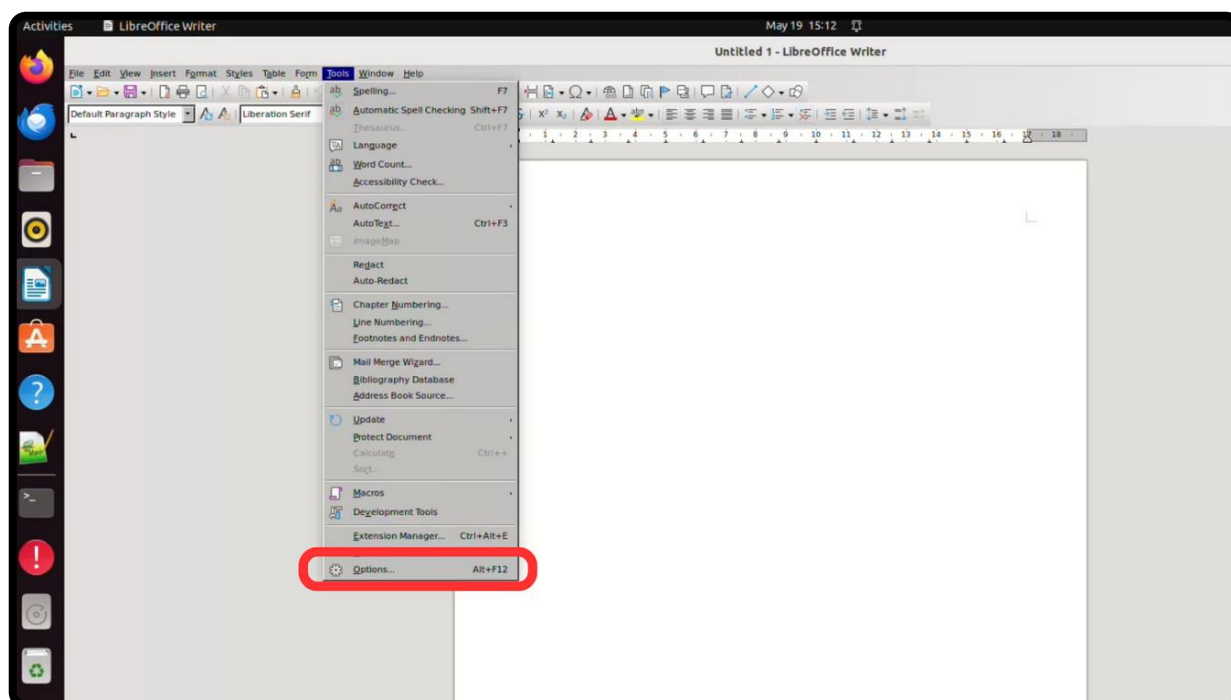
Step 6 - You will be asked for confirmation before this command is executed. Hit the "Enter" key, as prompted, to provide confirmation.

```
ubuntu@ubuntu-G751JY:~$ modutil -add "InnaITKey" -libfile /opt/Precision_Biometric/InnaITDSC/libraries/libInnaITPKCS11Driver.so -dbdir ~/.mozilla/firefox/profile.default  
  
WARNING: Performing this operation while the browser is running could cause corruption of your security databases. If the browser is currently running, you should exit browser before continuing this operation. Type 'q <enter>' to abort, or <enter> to continue: 
```

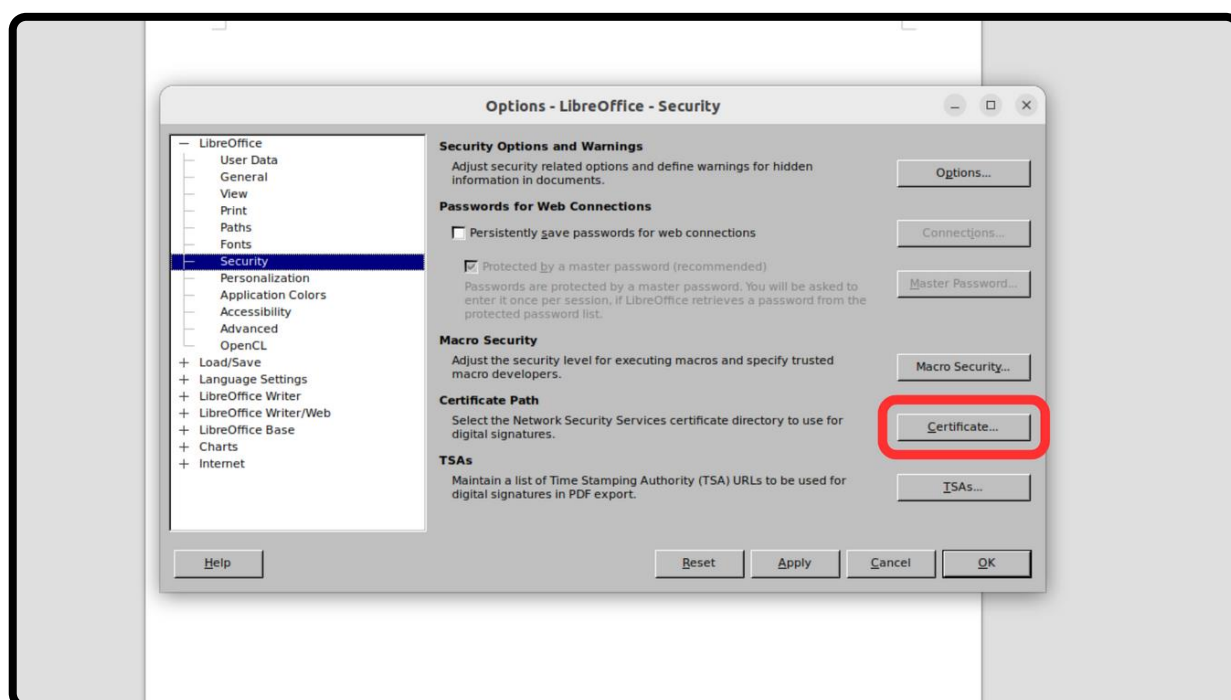
Step 7 - Once the InnaITKey has been added, you can close the terminal and open Libre Office.



T. Setting up Document Sign (Linux)

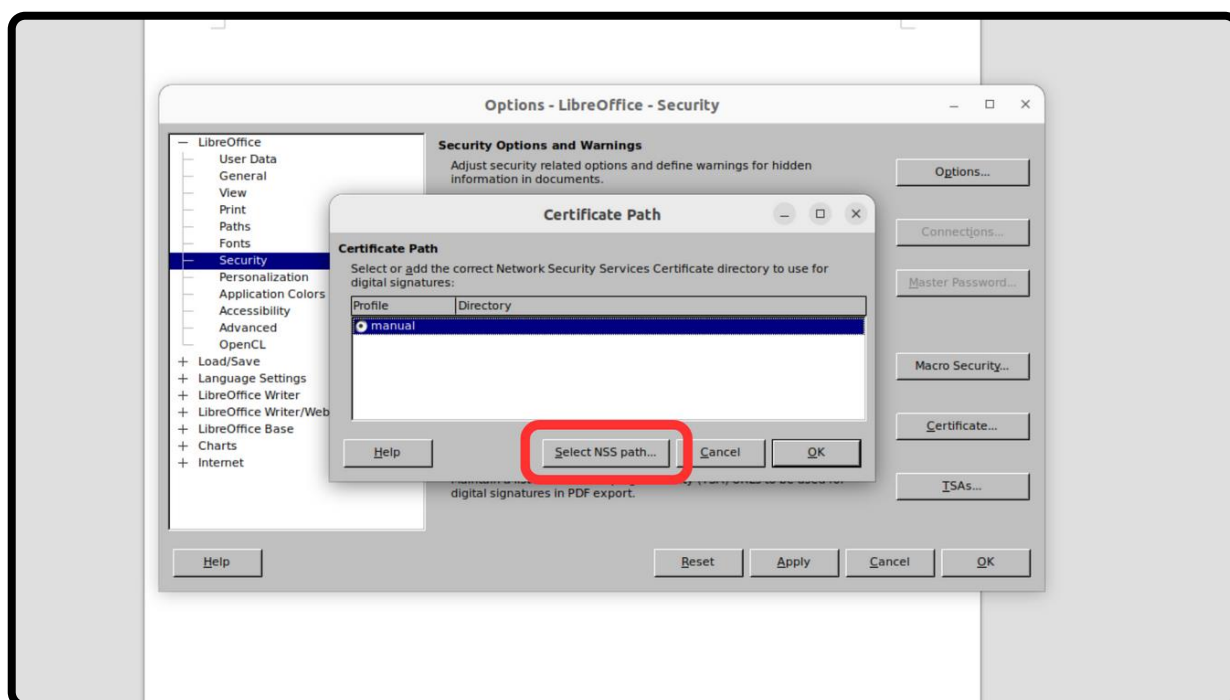


Step 8 – In the toolbar, under “Tools”, click on the “Options” button.

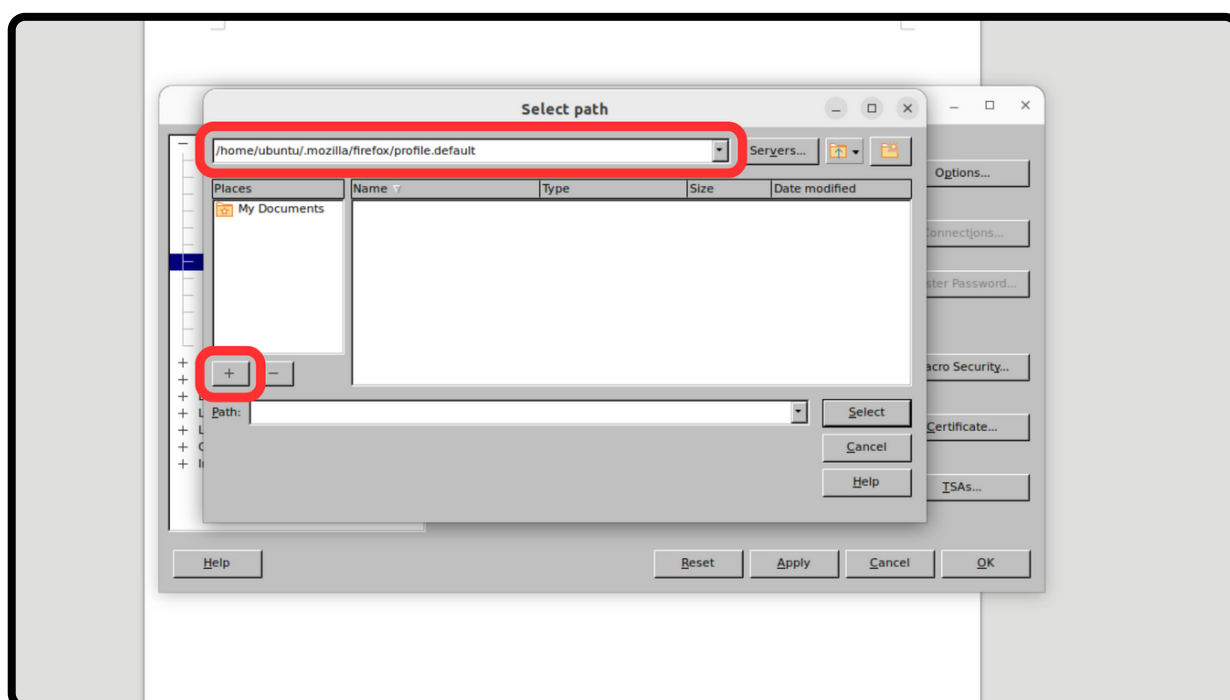


Step 9 – In this window, click on the “Certificate...” button under “LibreOffice > Security”.

T. Setting up Document Sign (Linux)

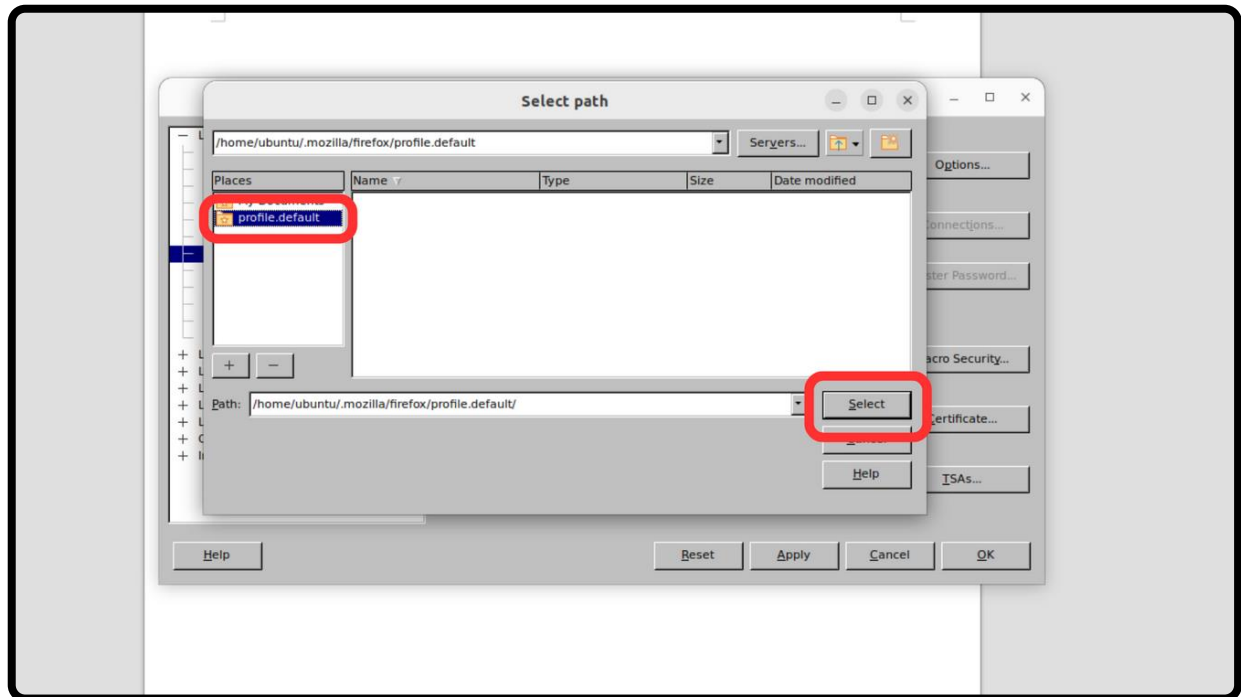


Step 10 – Now, click on the “Select NSS Path...” button.

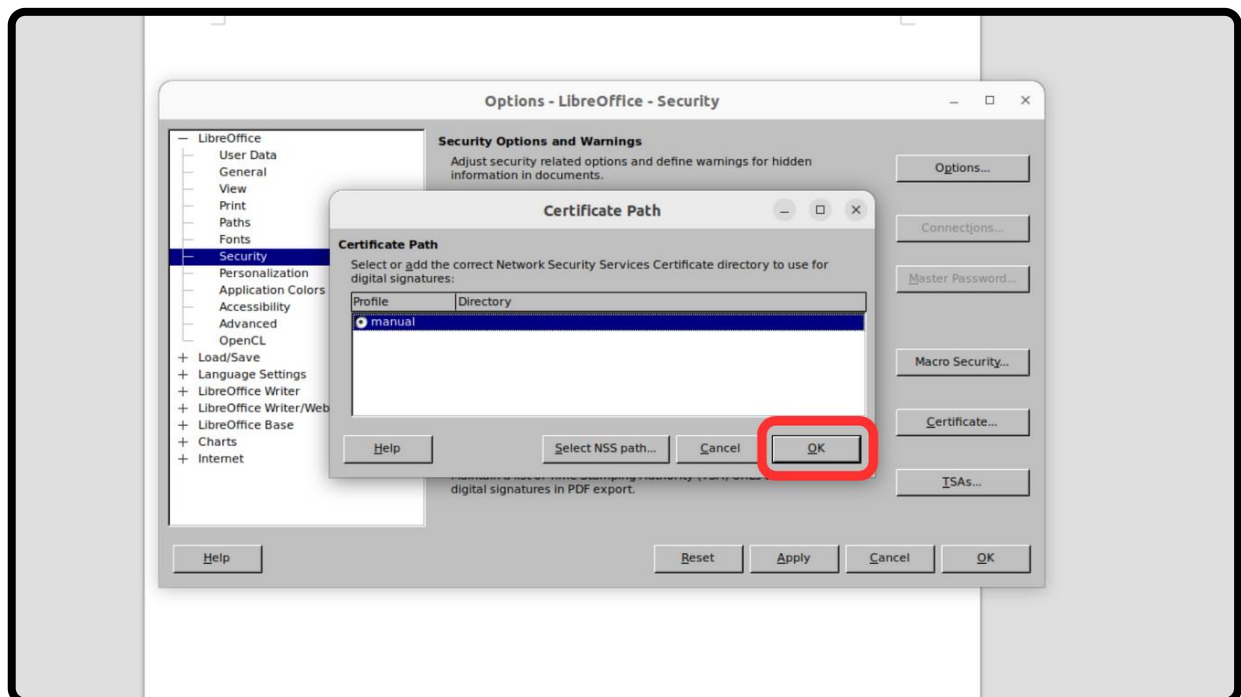


Step 11 – Enter the path of the directory that was created in step 3, in the indicated field, and then click on the “+” icon.

T. Setting up Document Sign (Linux)

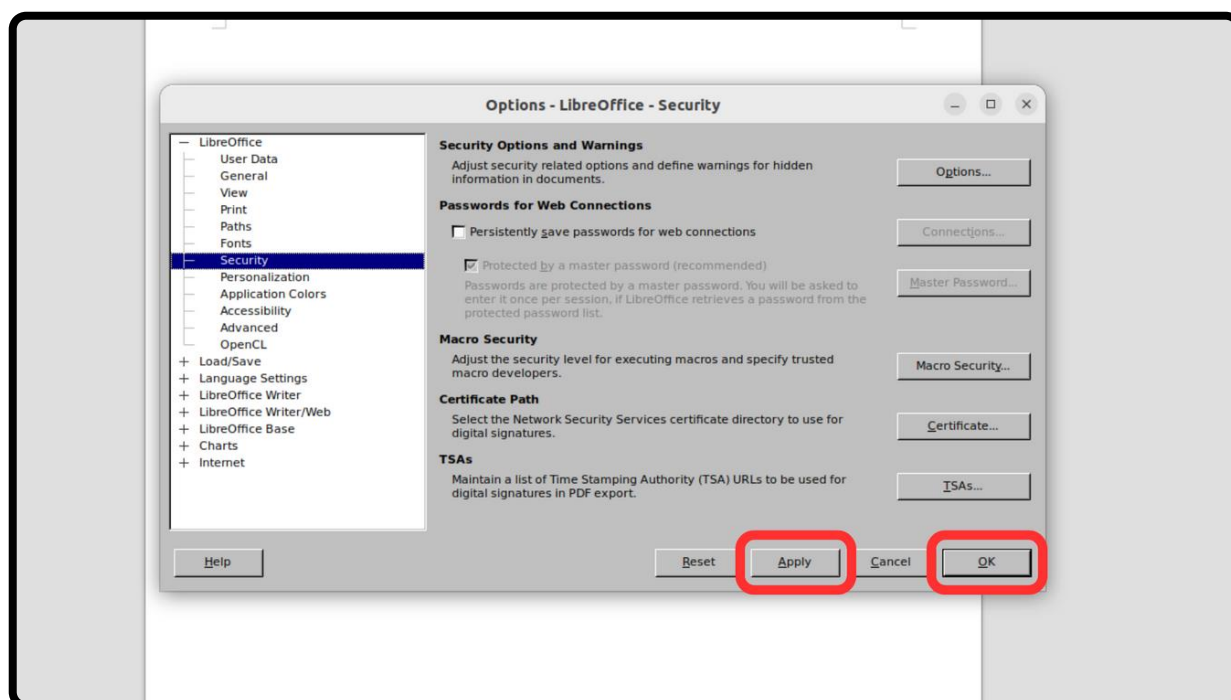


Step 12 – Click on the newly added path under “Places” and then click on the “Select” button. This will close the current window automatically.



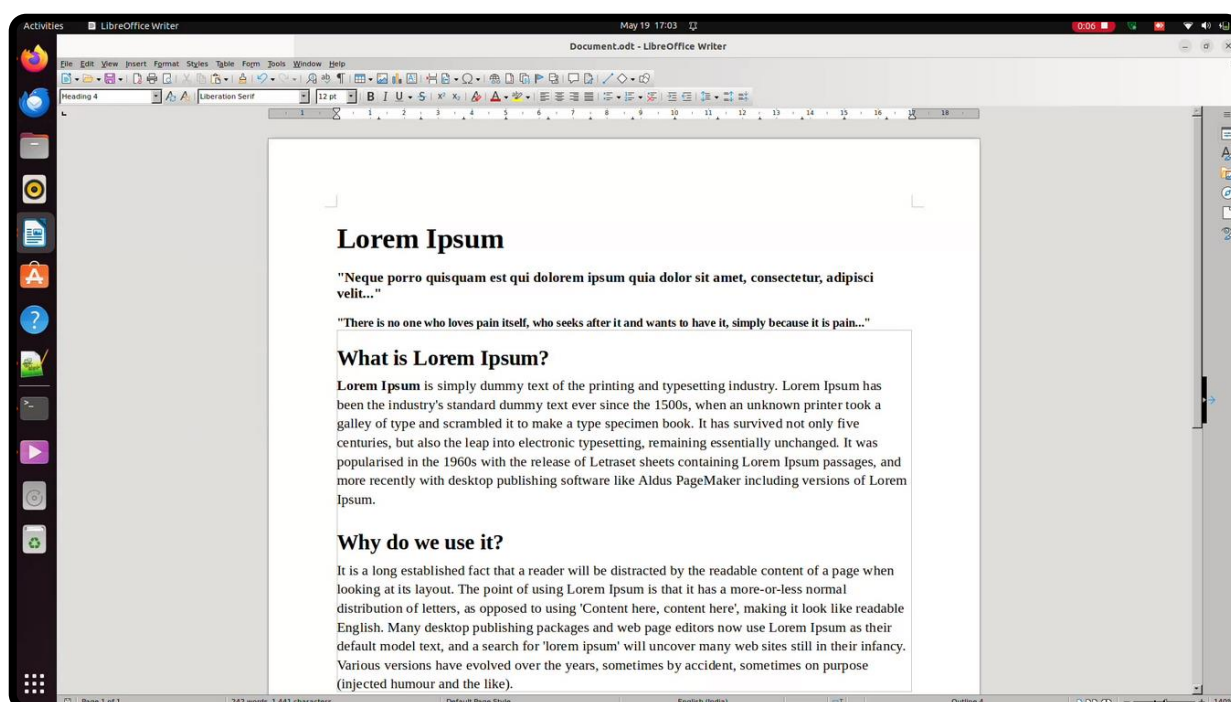
Step 13 – In this window, click on “OK”.

T. Setting up Document Sign (Linux)

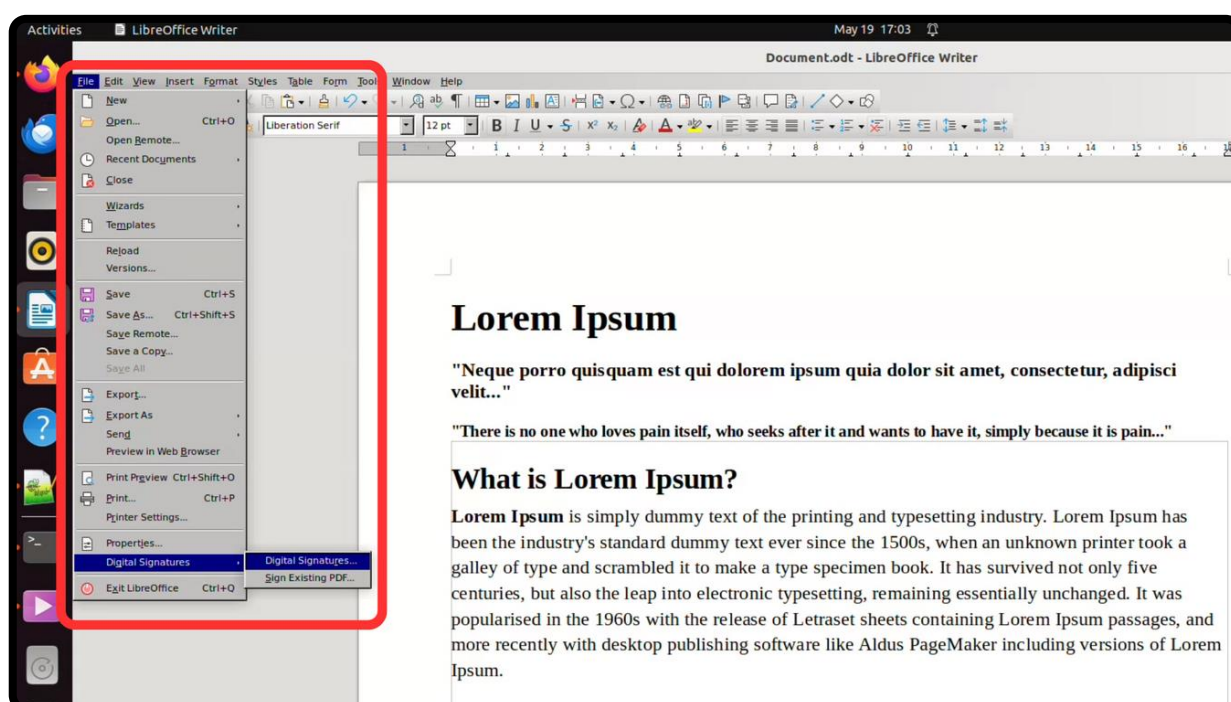


Step 14 – Finally, click on “Apply” and then “OK” to apply the settings and then close the window, respectively.

U. Signing a Document (Linux)

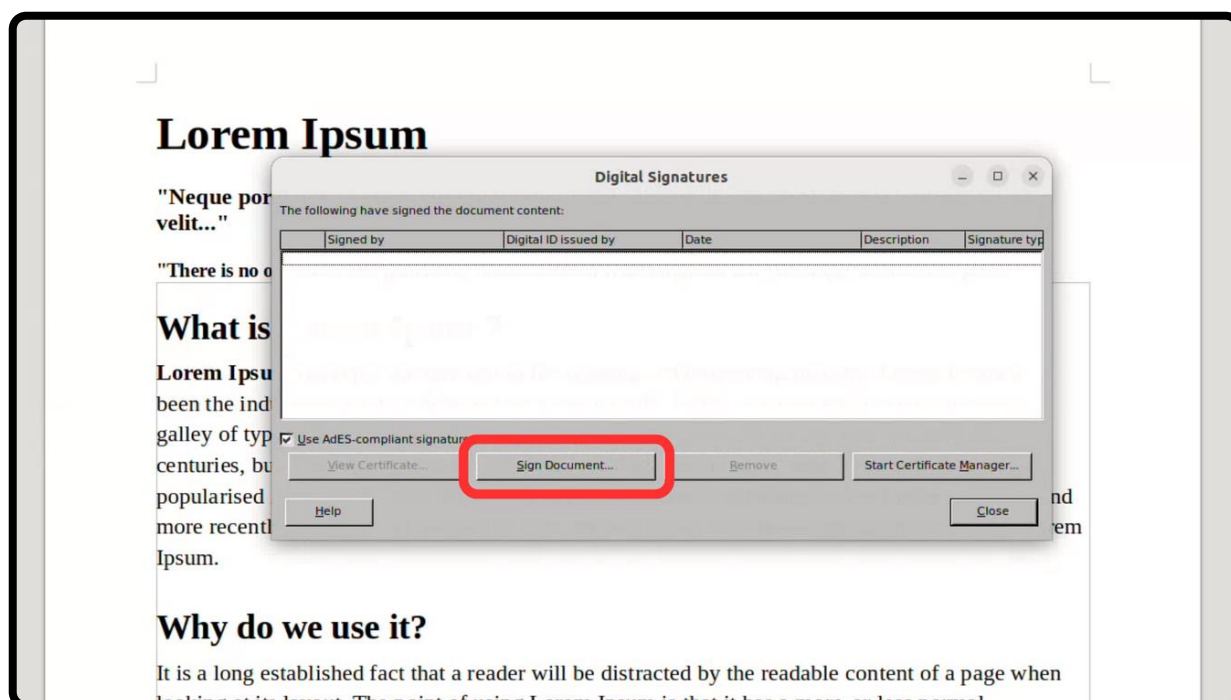


Step 1 – Please open the document that you would like to sign, using LibreOffice.

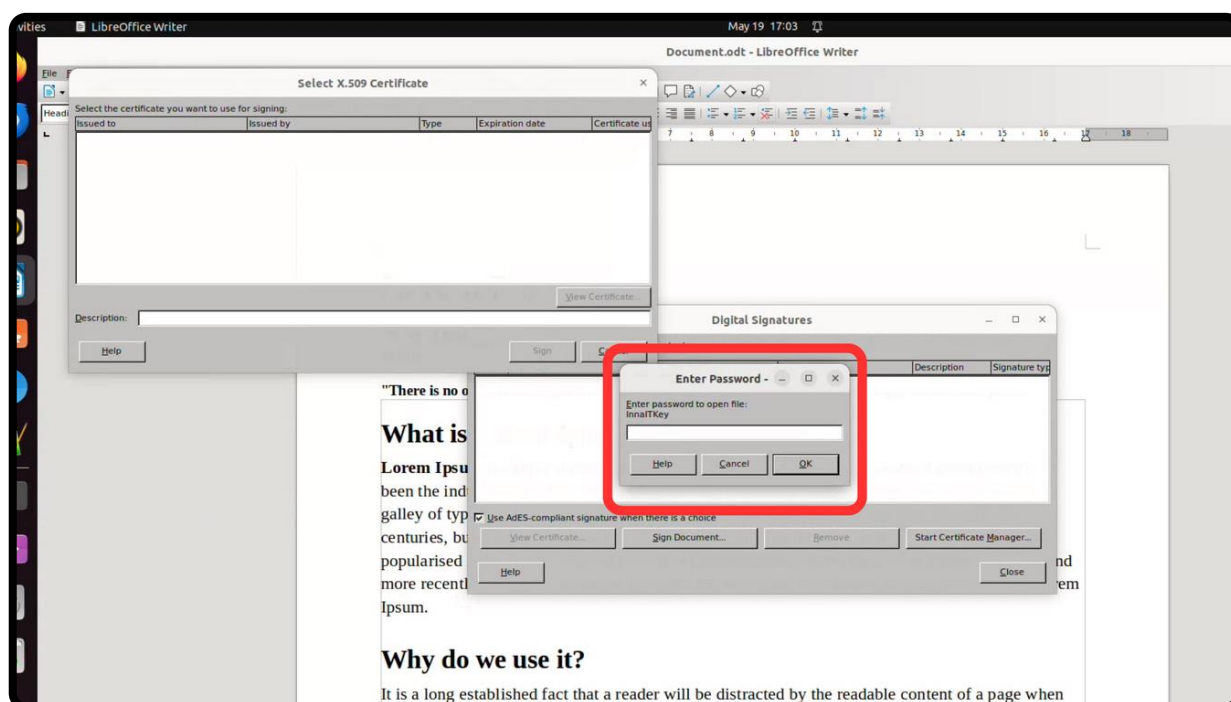


Step 2 – In the toolbar, under “File” and then “Digital Signatures”, select the “Digital Signatures...” option

U. Signing a Document (Linux)

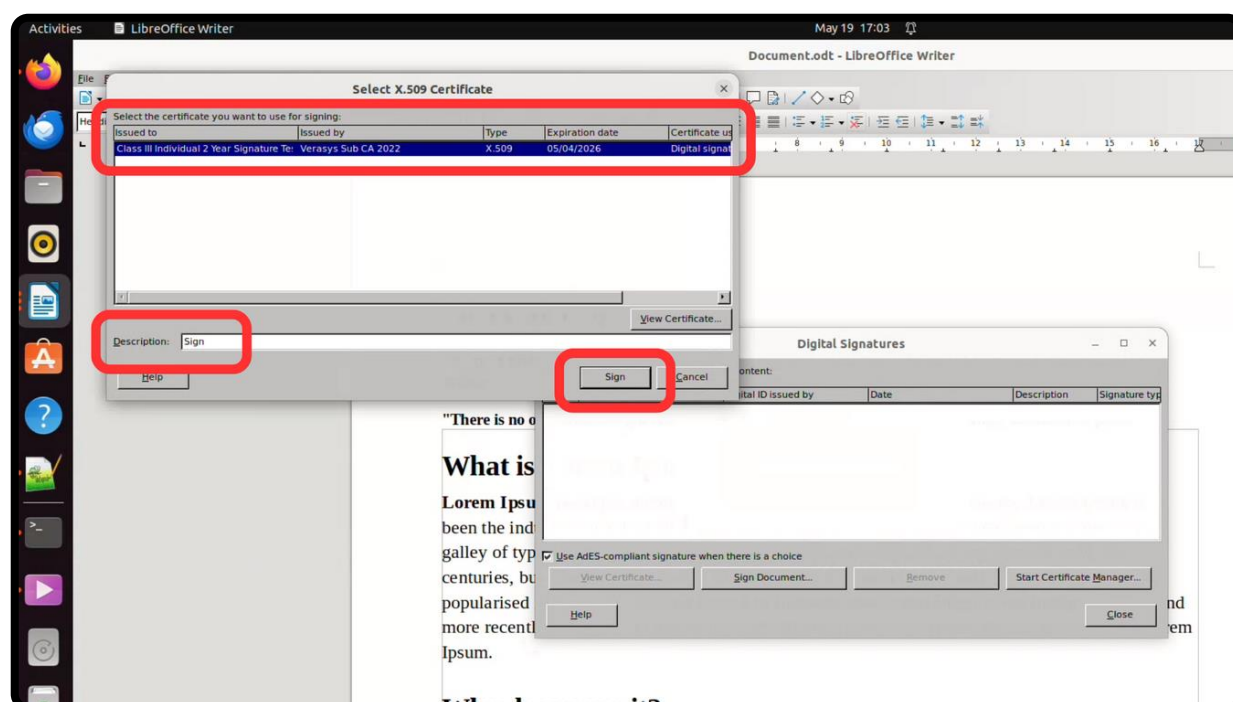


Step 3 – Here, click on the “Sign Document...” button, to begin.

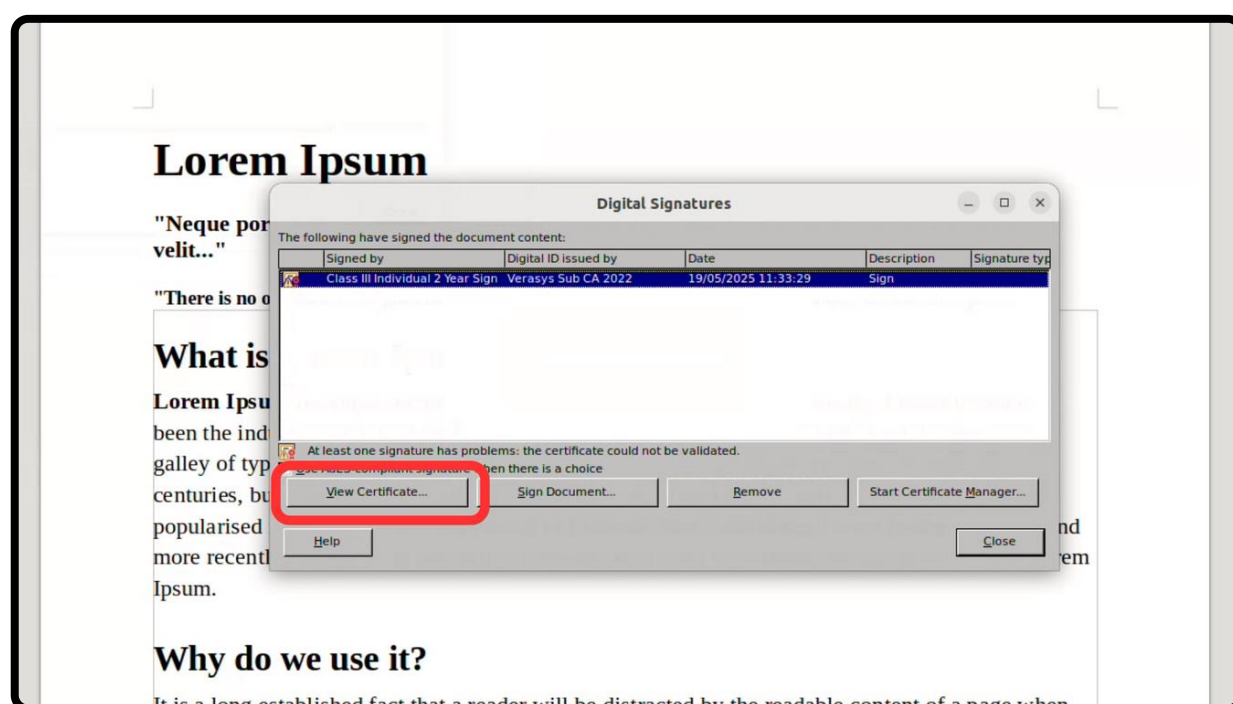


Step 4 – You will now be prompted to verify your identity.

U. Signing a Document (Linux)

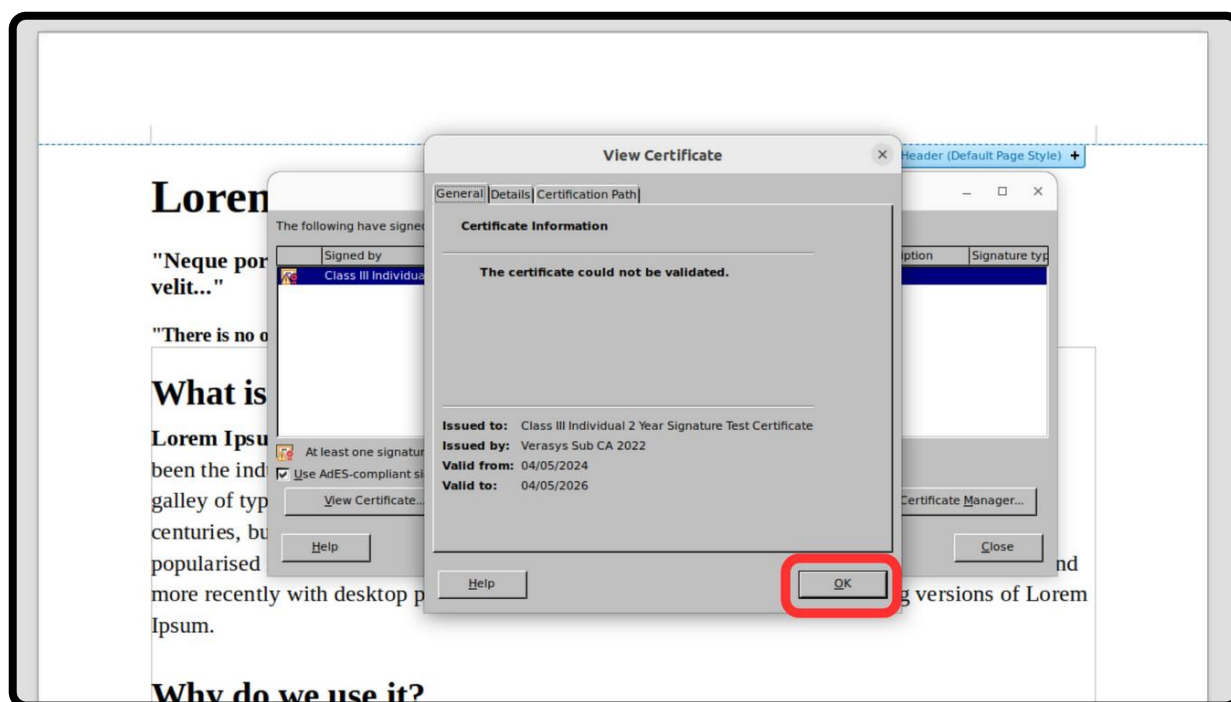


Step 5 – The certificates stored on your token will now be displayed. You must select the certificate that you would like to use to sign this document, enter a description in the given field, and then click on “Sign”.

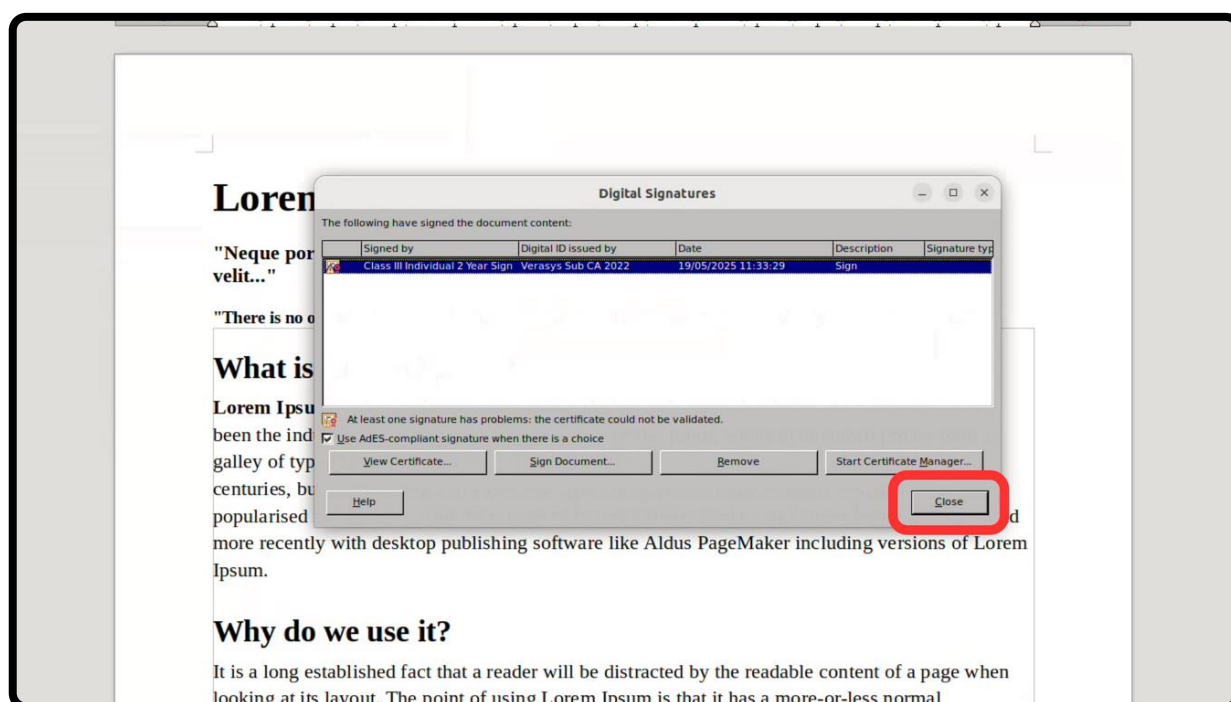


Step 6 – After the signing is complete, the “Digital Signatures” window will contain information about the certificate used to sign the document. You can view the certificate as well, by clicking on the “View Certificate...” button.

U. Signing a Document (Linux)

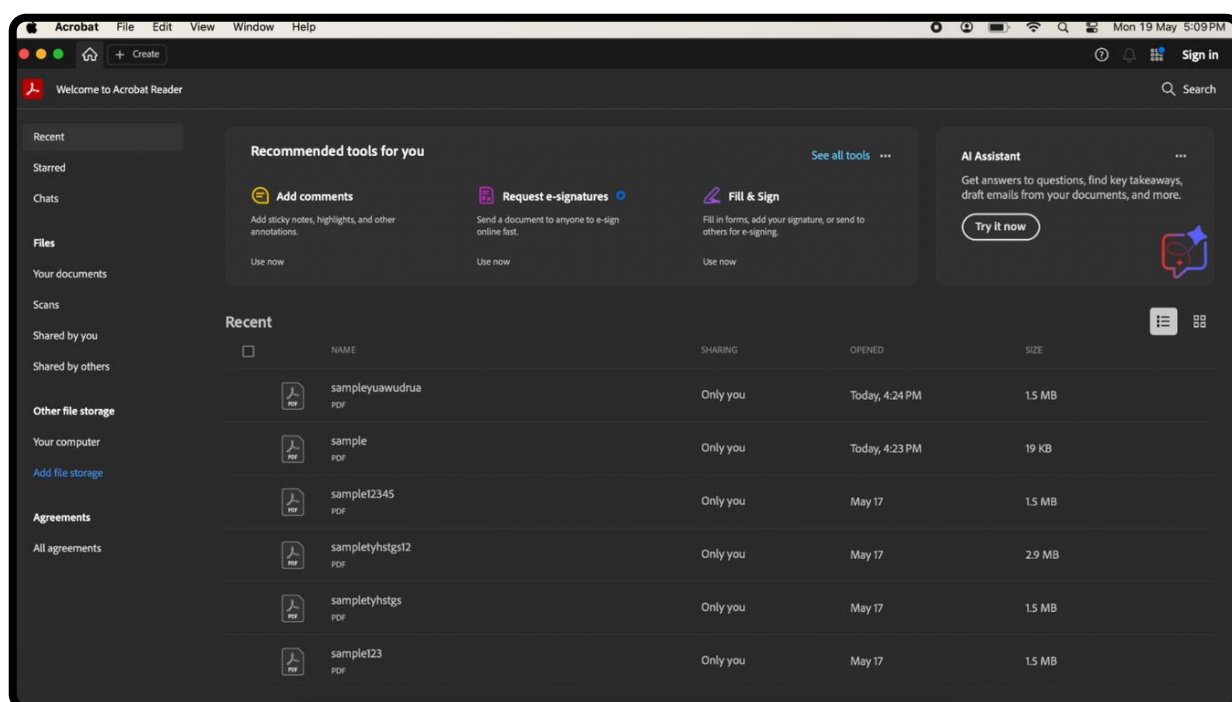


Step 7 – You can view the details of the certificate in this window. Click on “OK” to close this window.

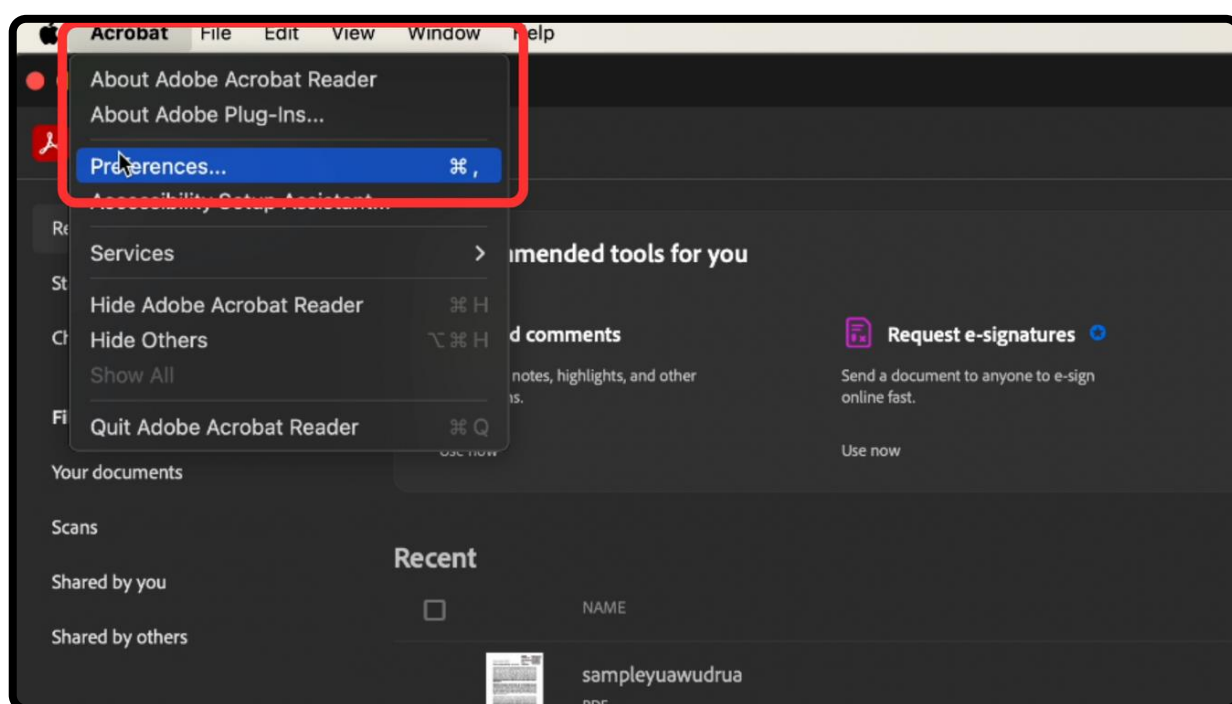


Step 8 – Click on “Close” in this window, to go back to your document. You have successfully signed a document.

V. Setting up Document Sign (MacOS)

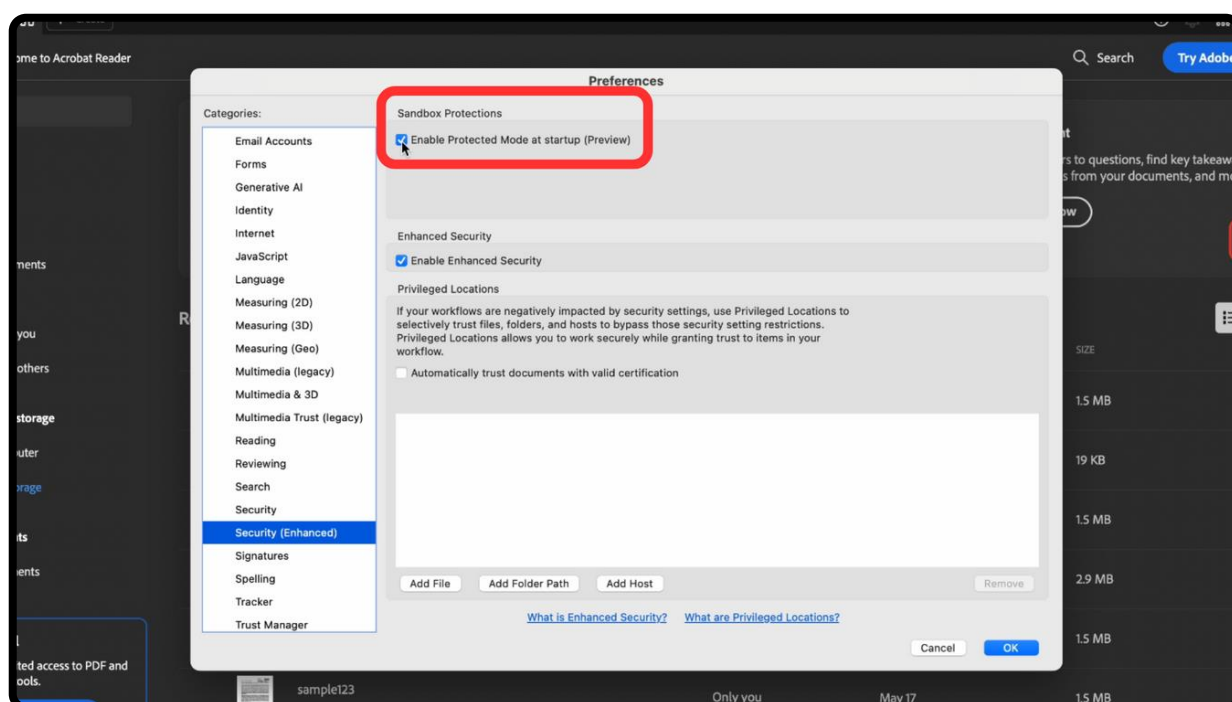


Step 1 – Please open Adobe Acrobat on your Mac to begin the setup.

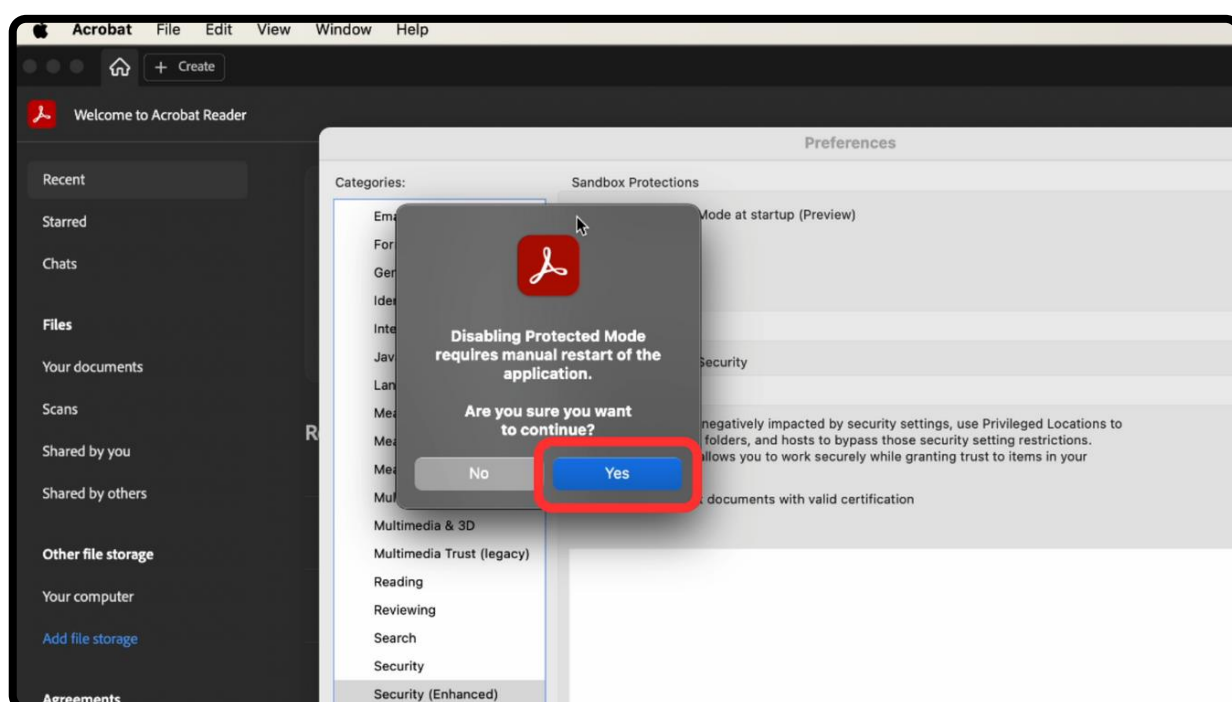


Step 2 – Click on “Acrobat” in the Toolbar, and then on “Preferences”.

V. Setting up Document Sign (MacOS)

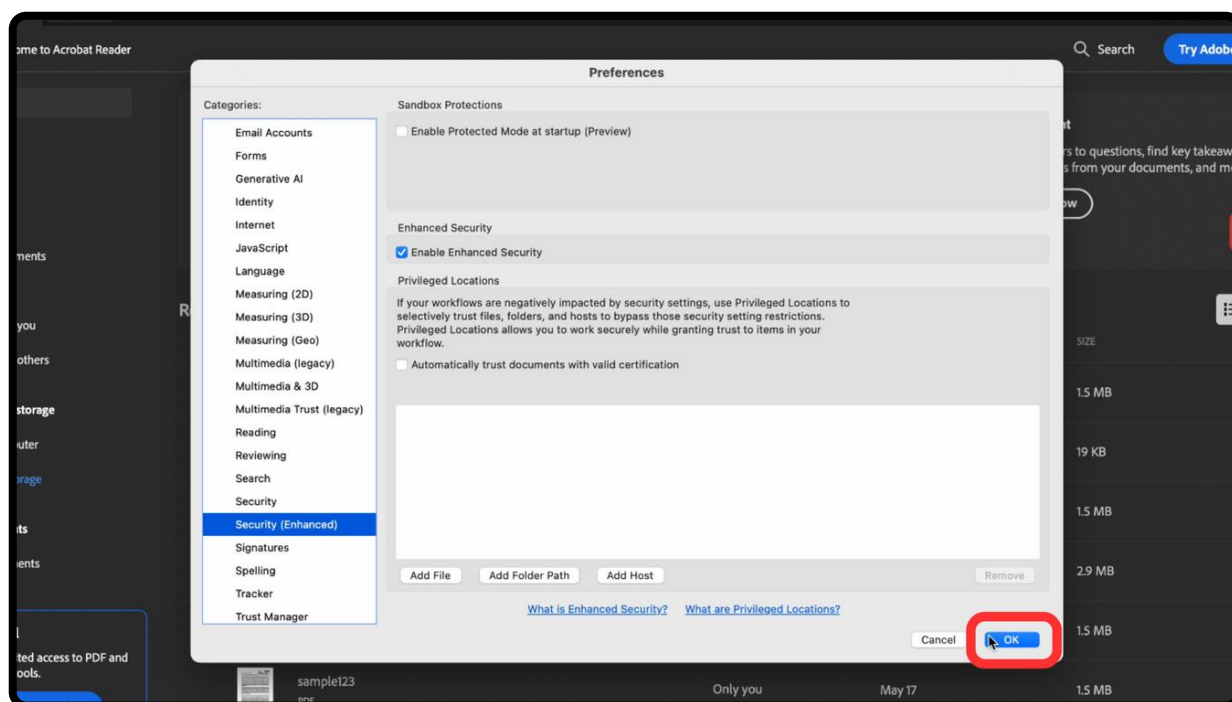


Step 3 – In this window, select “Security (Enhanced)” and then uncheck the “Enable Protected Mode at startup” option under “Sandbox Protections”.

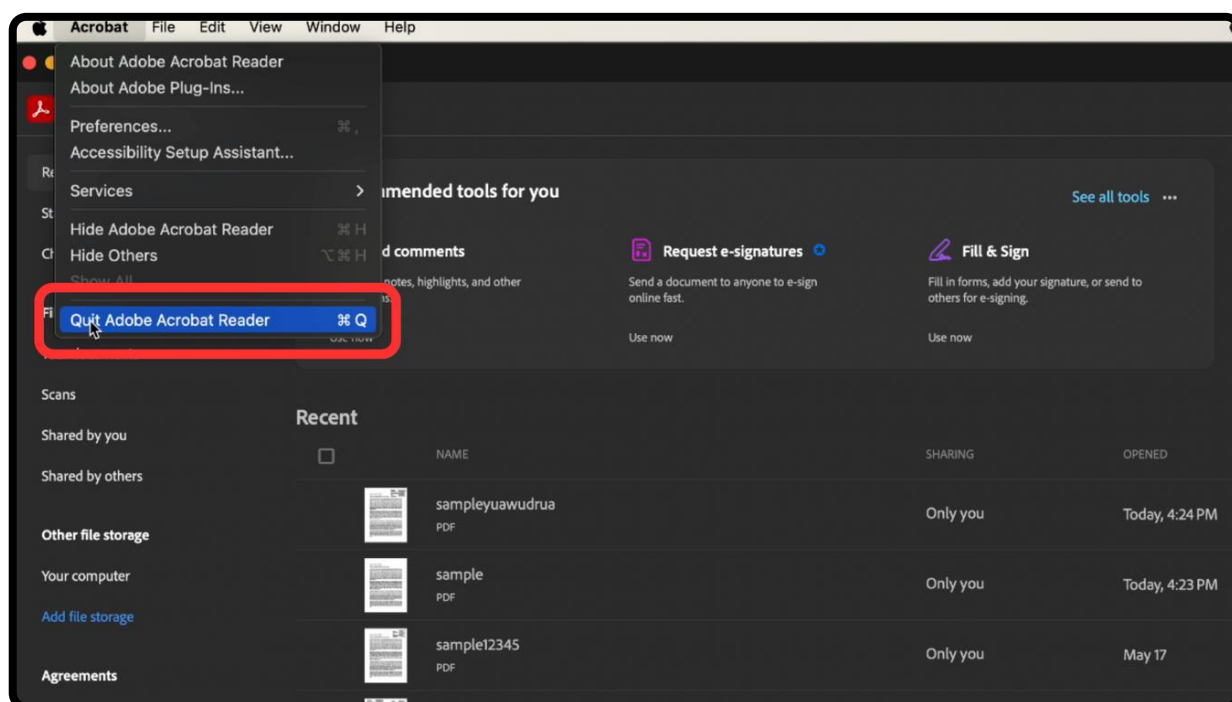


Step 4 – You will now be asked for confirmation. Click “Yes” to proceed.

V. Setting up Document Sign (MacOS)

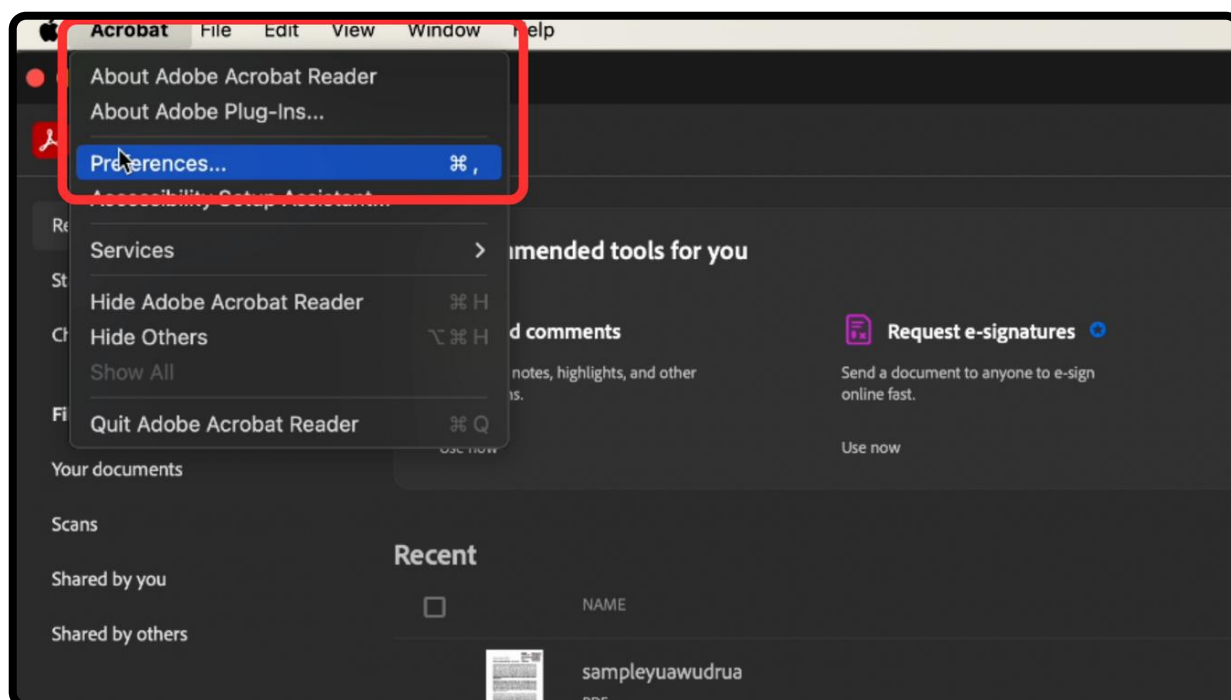


Step 5 – Please click on “OK” to exit this window.

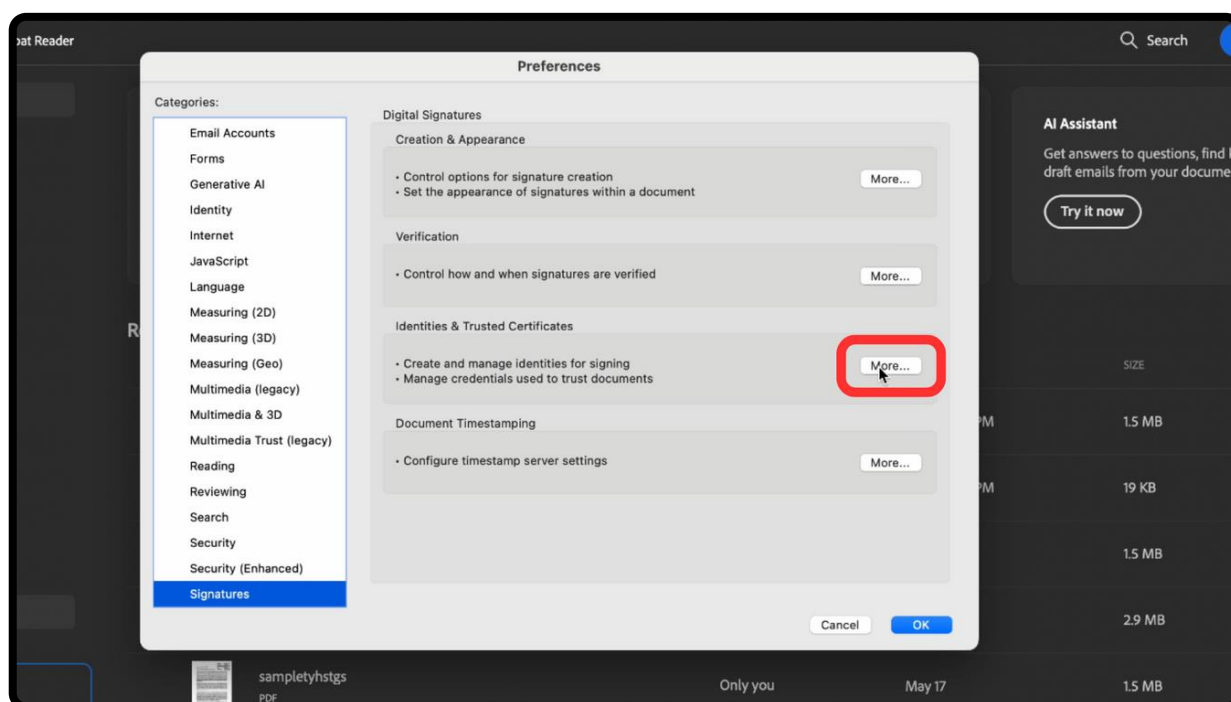


Step 6 – Quit Adobe Acrobat manually and then open it again for the changes to take effect.

V. Setting up Document Sign (MacOS)

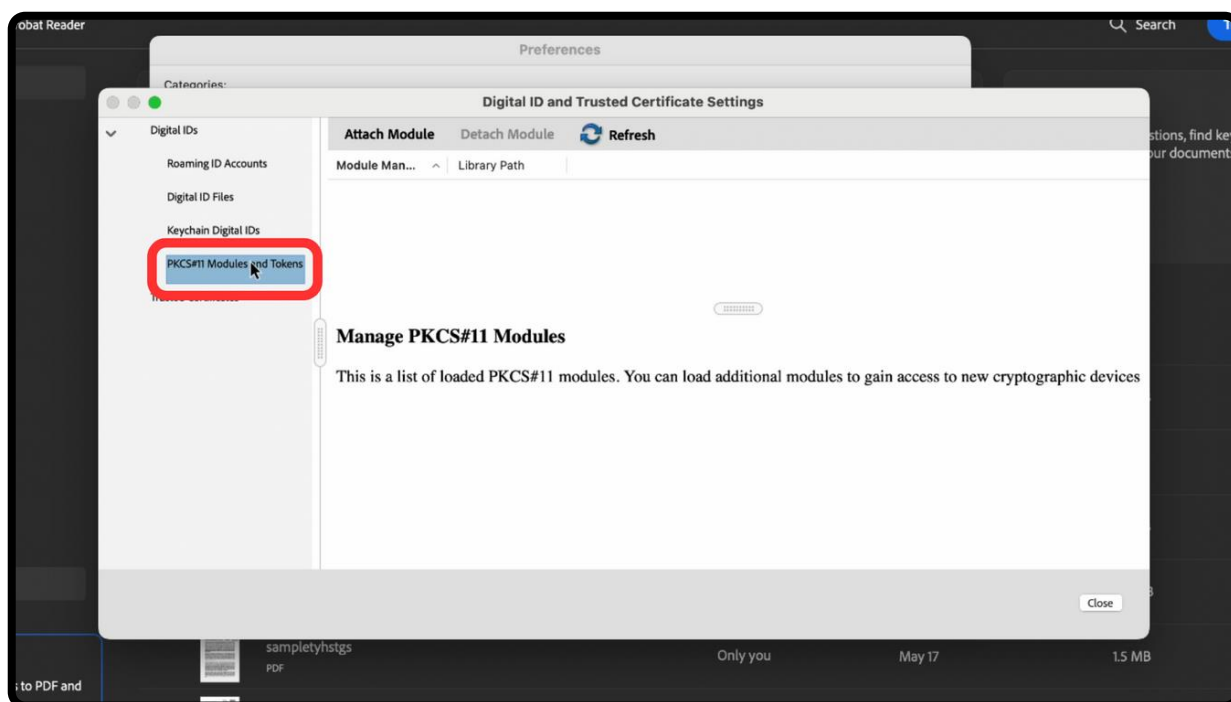


Step 7 – Start Adobe Acrobat again and then go back to the “Preferences” window.

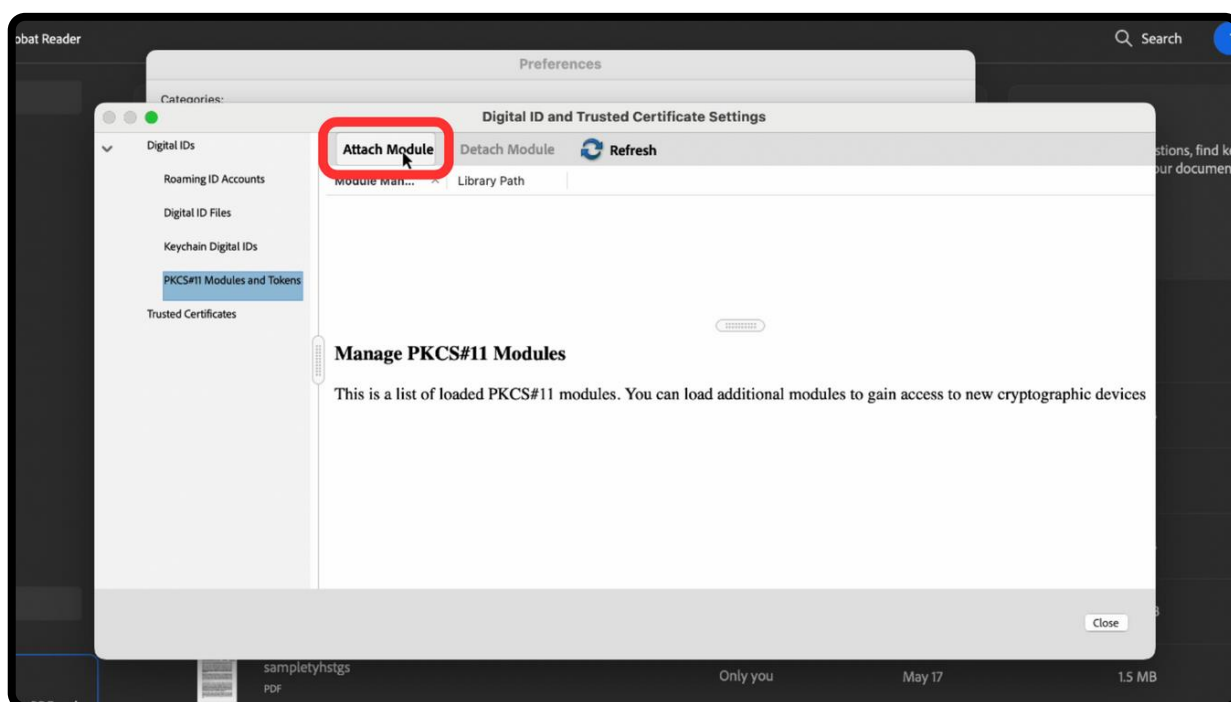


Step 8 – Here, navigate to the “Signatures” tab and then click on “More...” under “Identities & Trusted Certificates”.

V. Setting up Document Sign (MacOS)

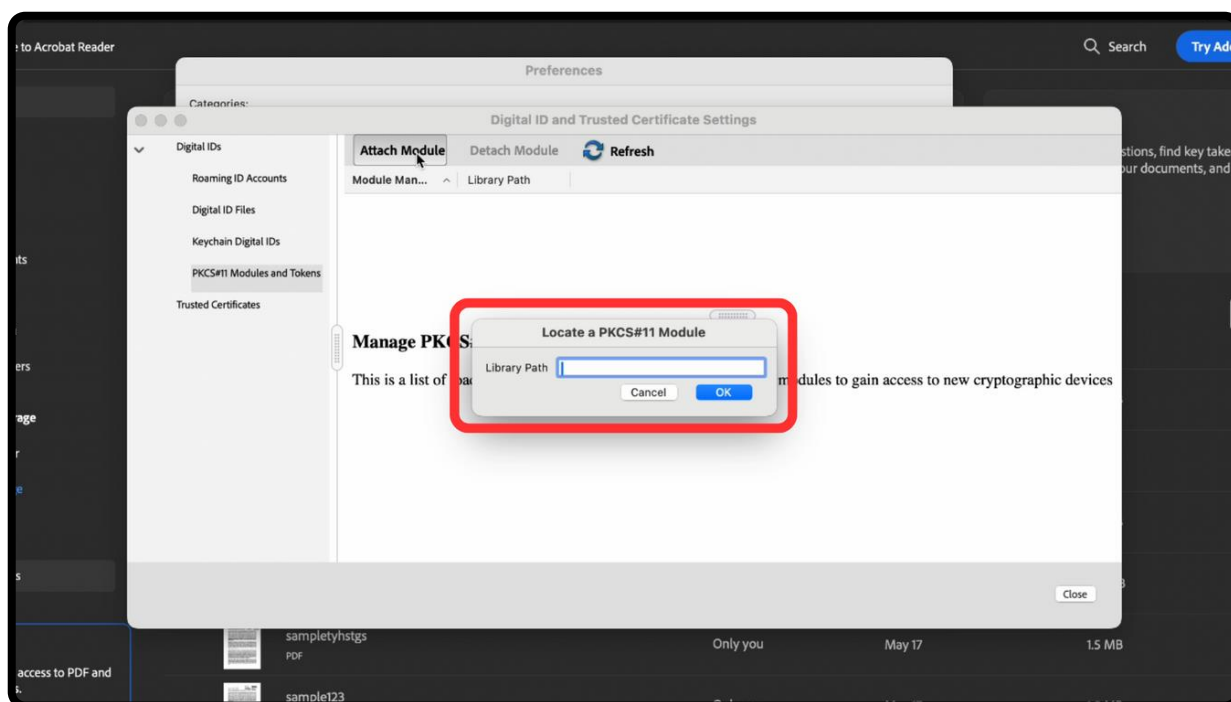


Step 9 – In this window, navigate to “PKCS#11 Modules and Tokens” under “Digital IDs”.



Step 10 – Click on “Attach Module” to continue.

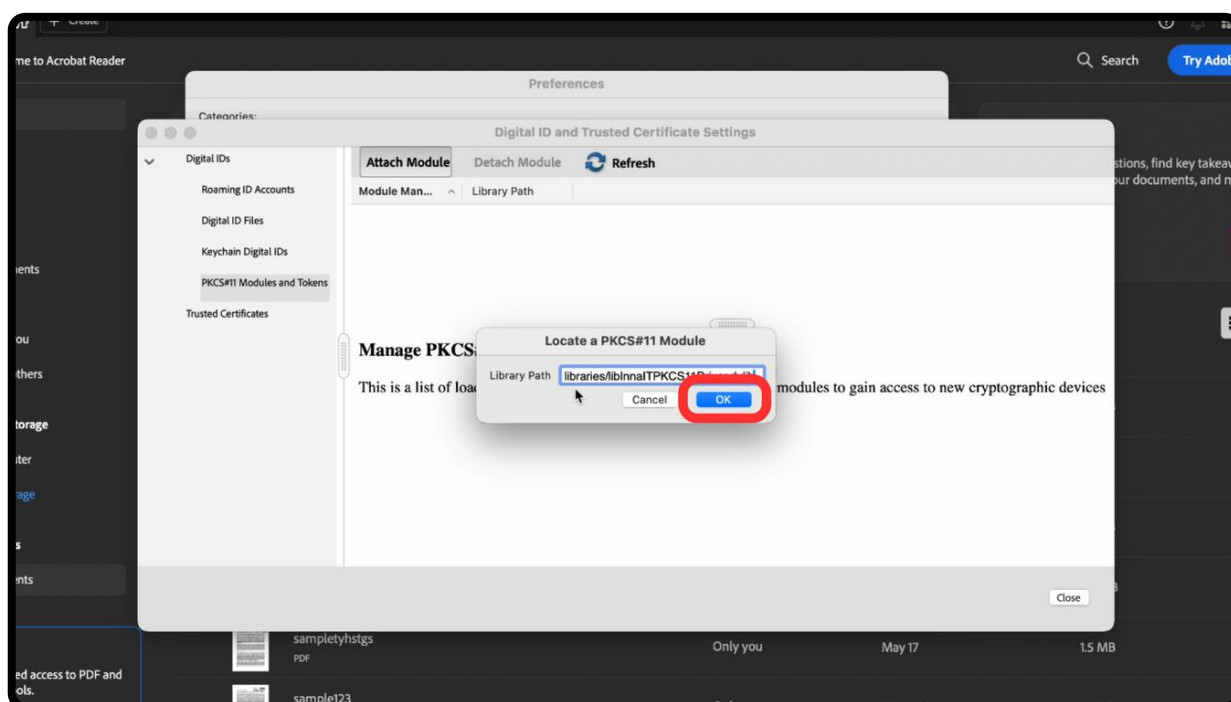
V. Setting up Document Sign (MacOS)



Step 11 – Please enter the path for the PKCS11 Module in the given field.

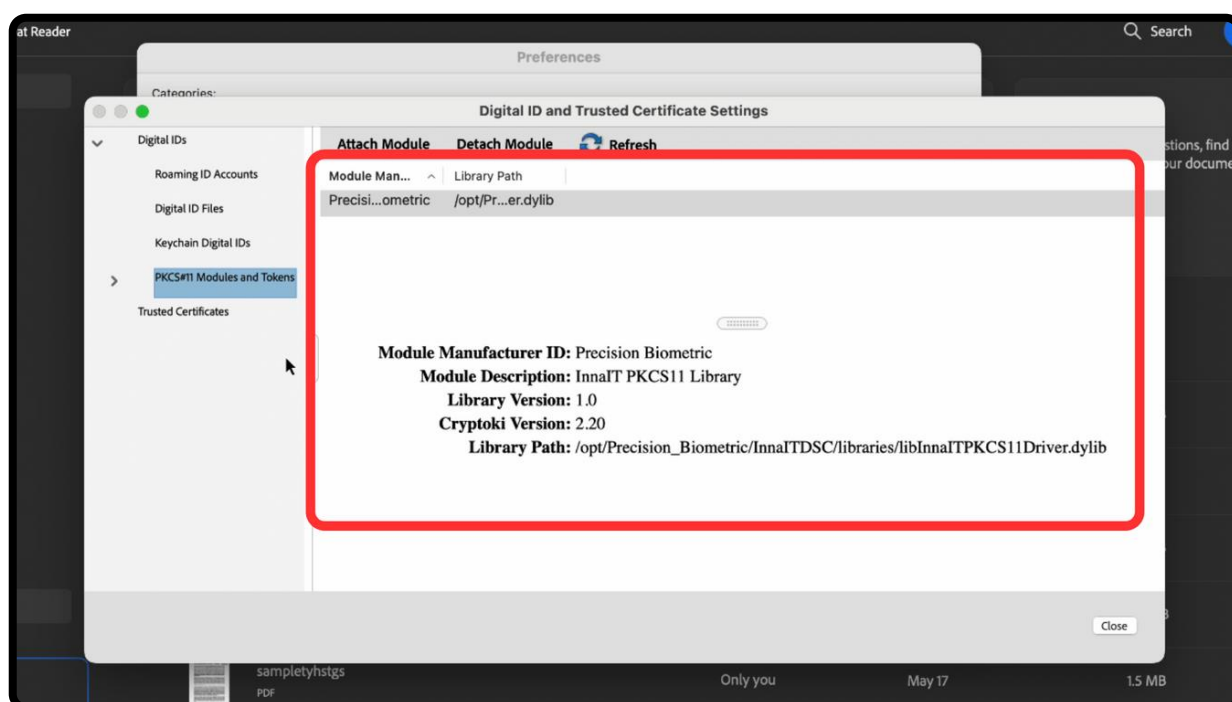
Note - The default path is

“/opt/Precision_Biometric/InnaITDSC/libraries/libInnaITPKCS11Driver.dylib”

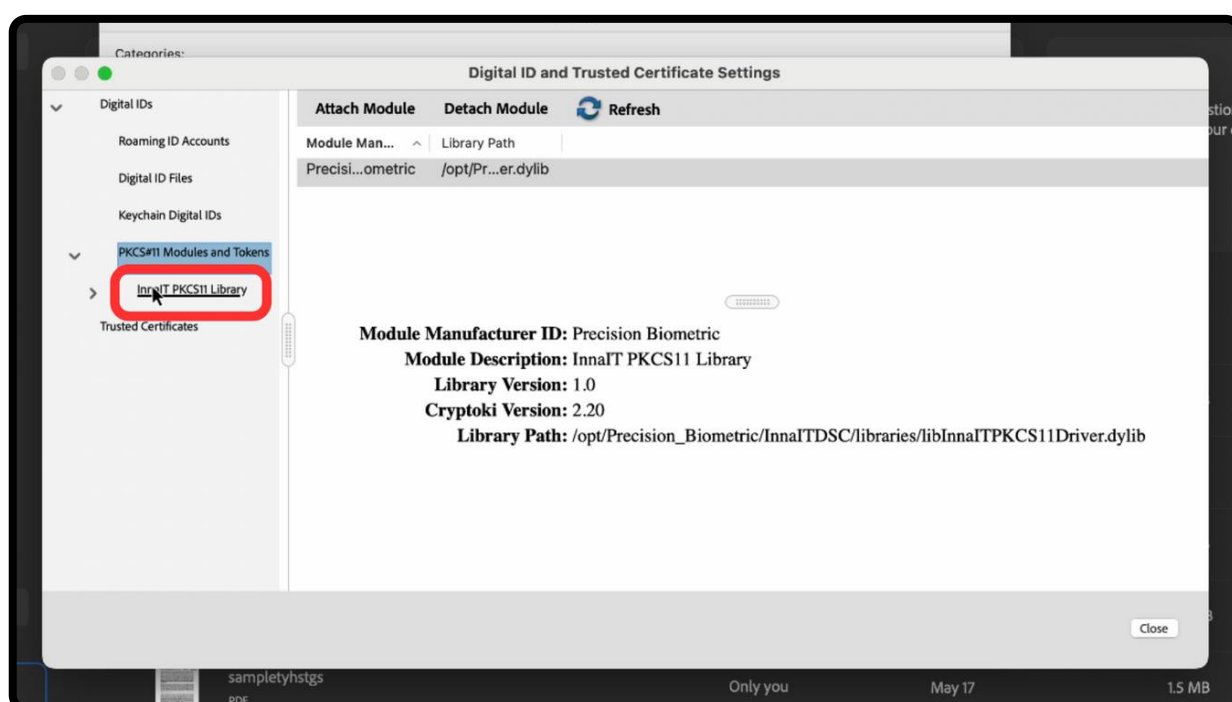


Step 12 – Click on “OK”.

V. Setting up Document Sign (MacOS)

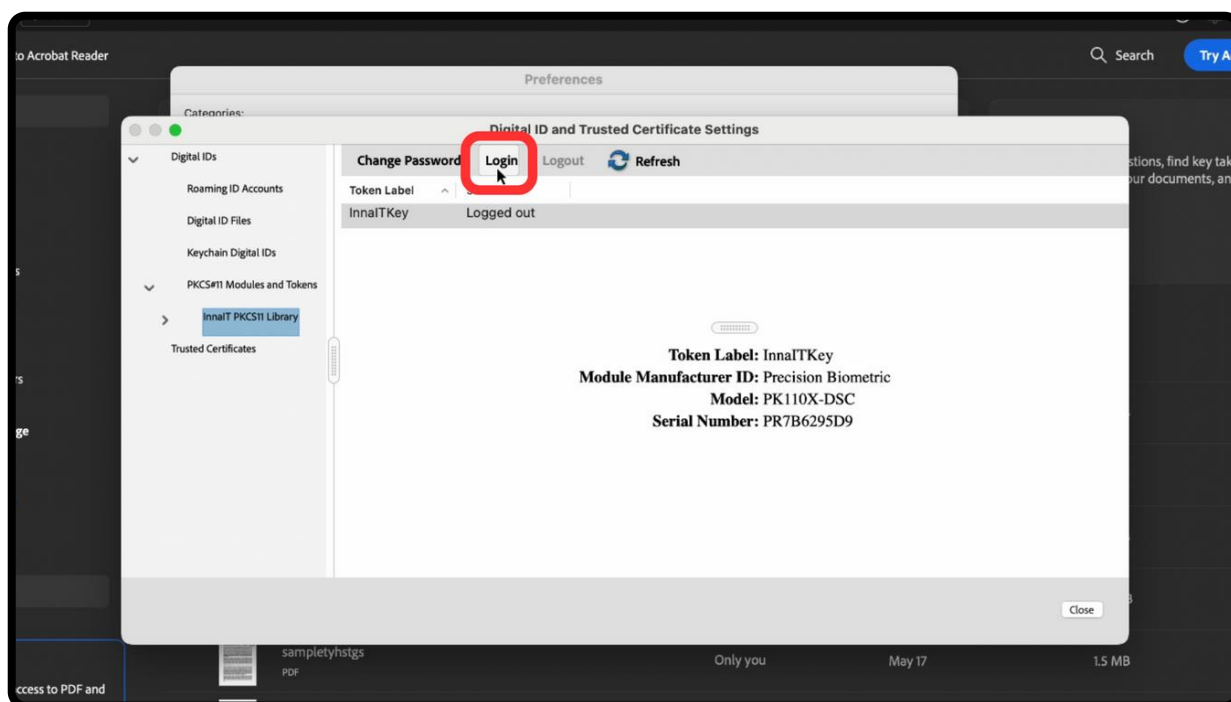


Step 13 – Please wait for the information of the module to appear in the “Digital ID and Trusted Certificate Settings” window.

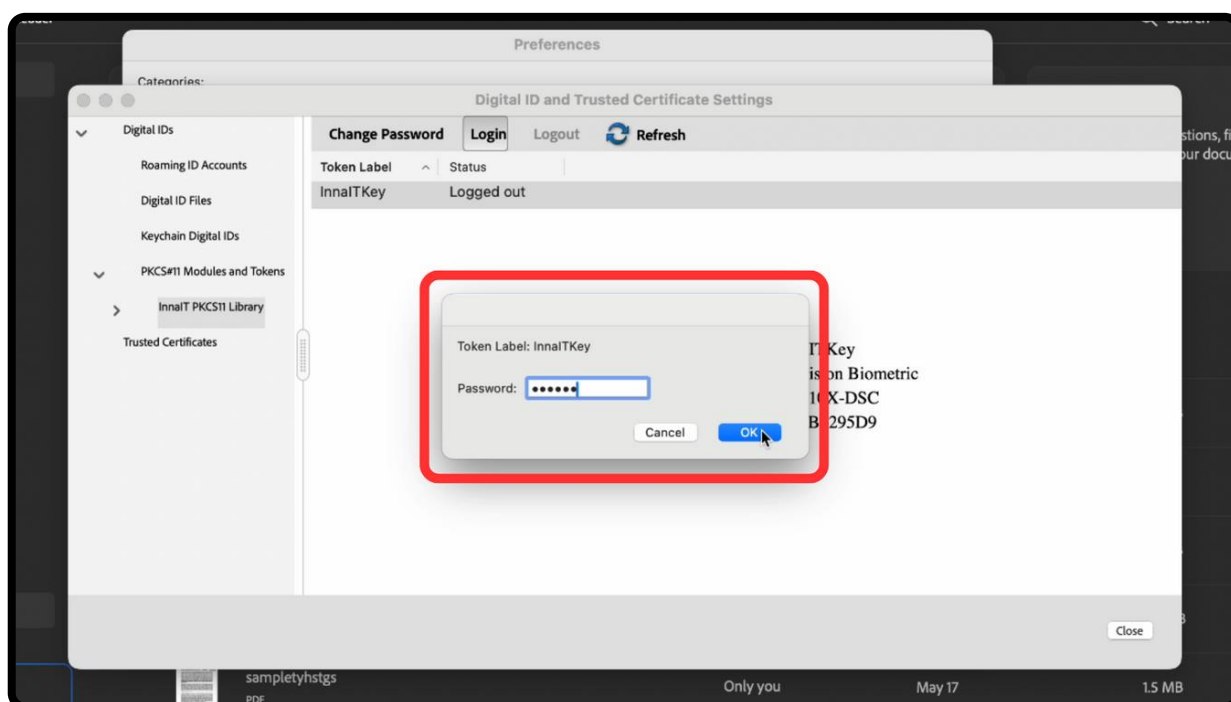


Step 14 – Once the information appears, navigate to “InnalT PKCS11 Library” under “PKCS#11 Modules and Tokens”.

V. Setting up Document Sign (MacOS)

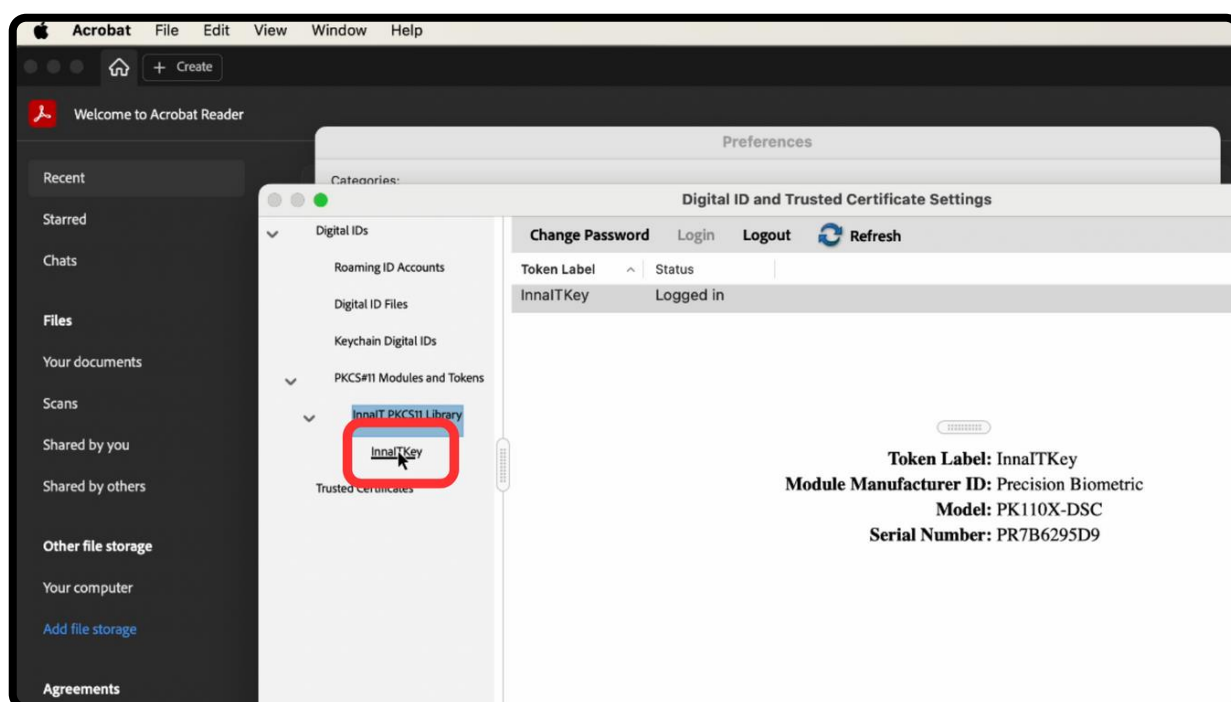


Step 15 – Here, click on the “Login” button.

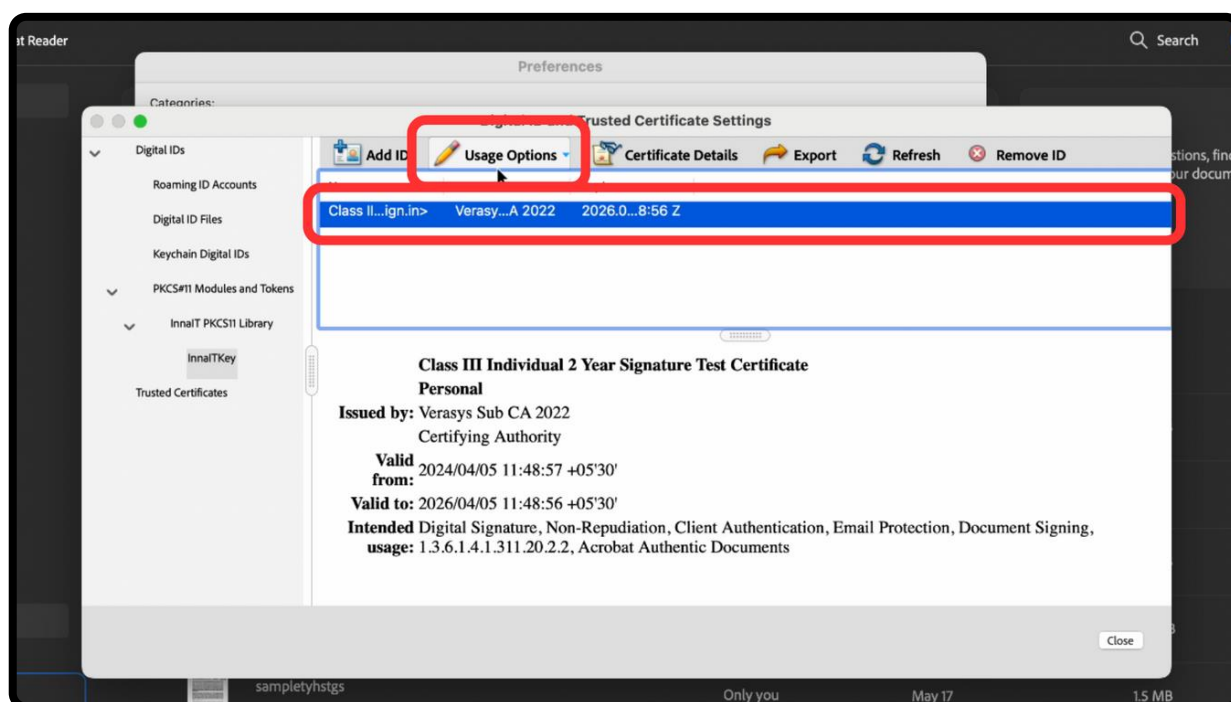


Step 16 – You will now be prompted to verify your identity. Enter your token’s password in the given field and click “OK”.

V. Setting up Document Sign (MacOS)

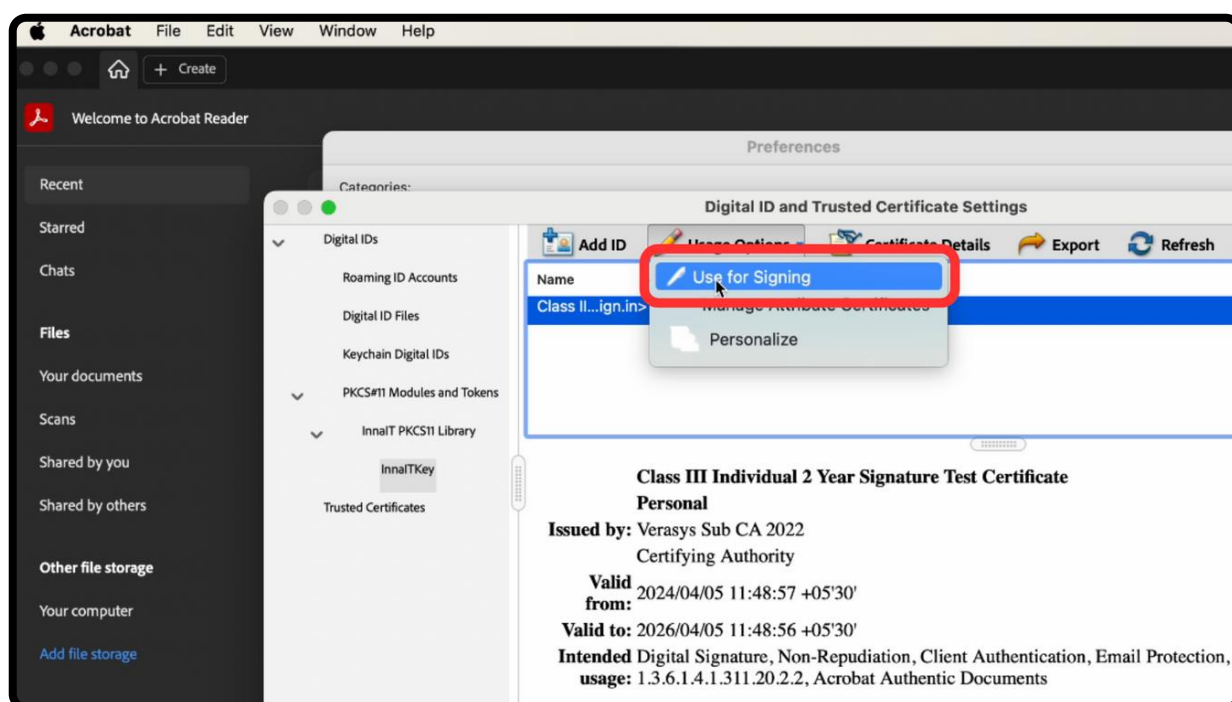


Step 17 – After logging in, navigate to “InnaITKey” under “InnaIT PKCS11 Library”.

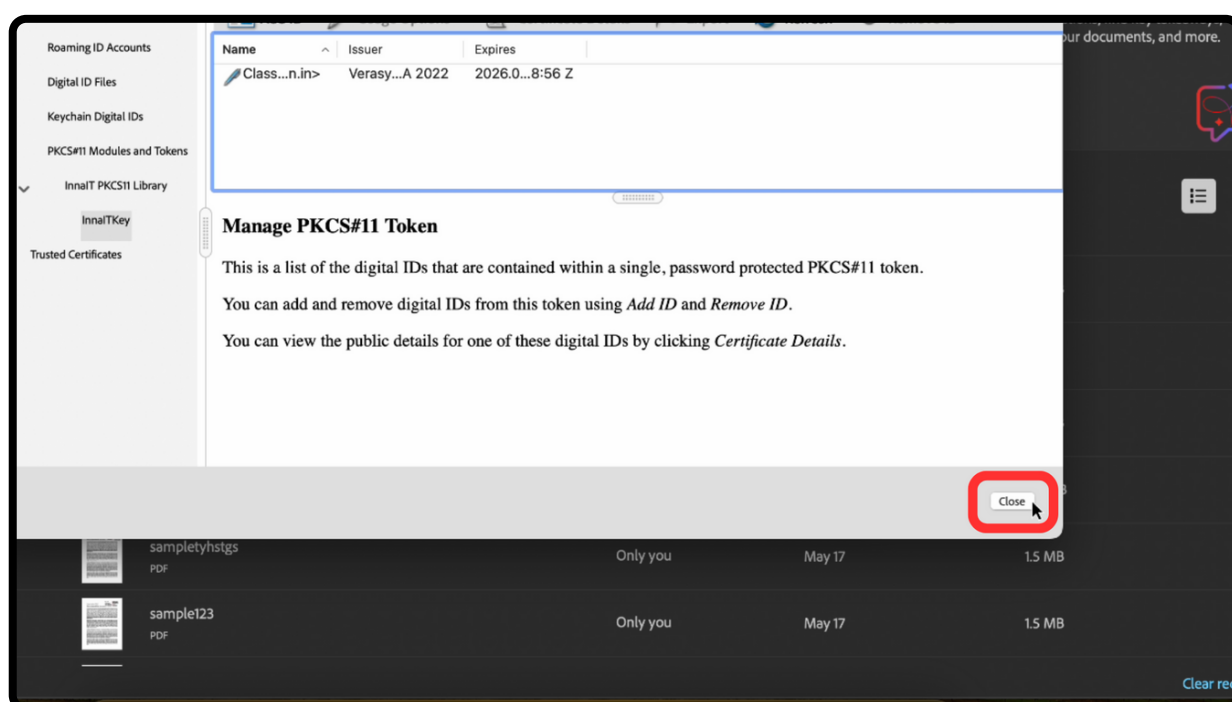


Step 18 – Here, click on the certificate that you would like to use and then on “Usage Options”.

V. Setting up Document Sign (MacOS)

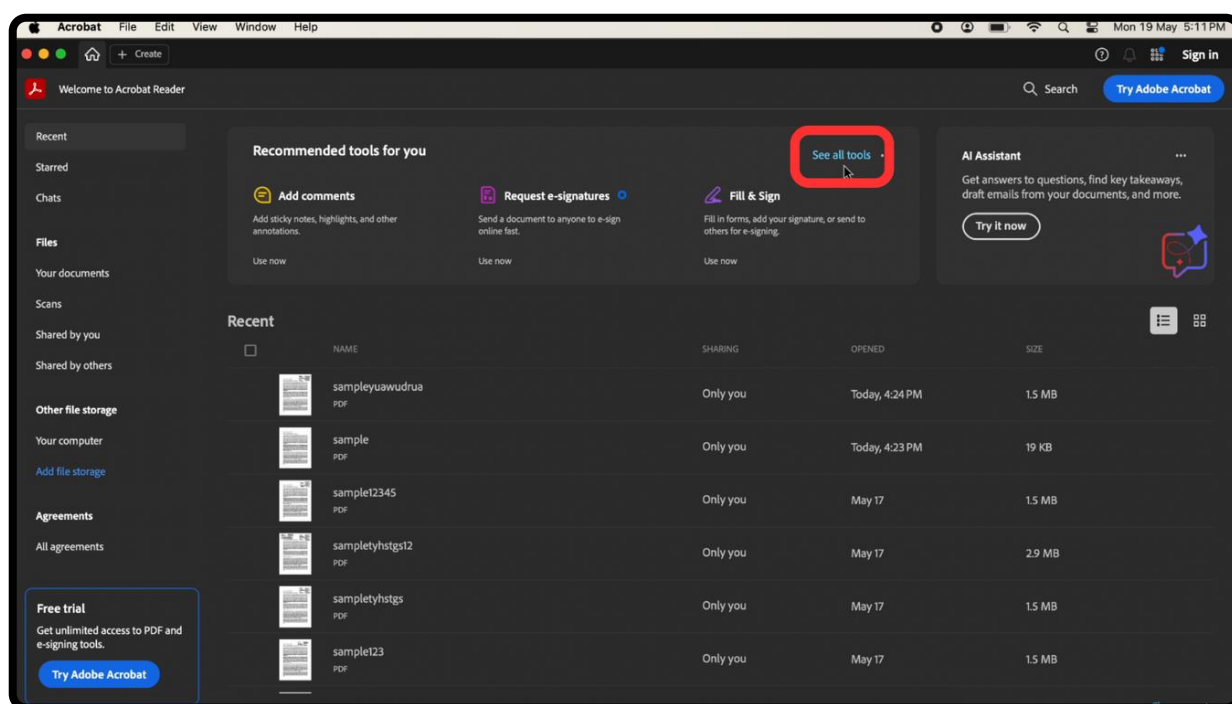


Step 19 – Select the “Use for Signing” option from the drop-down menu.

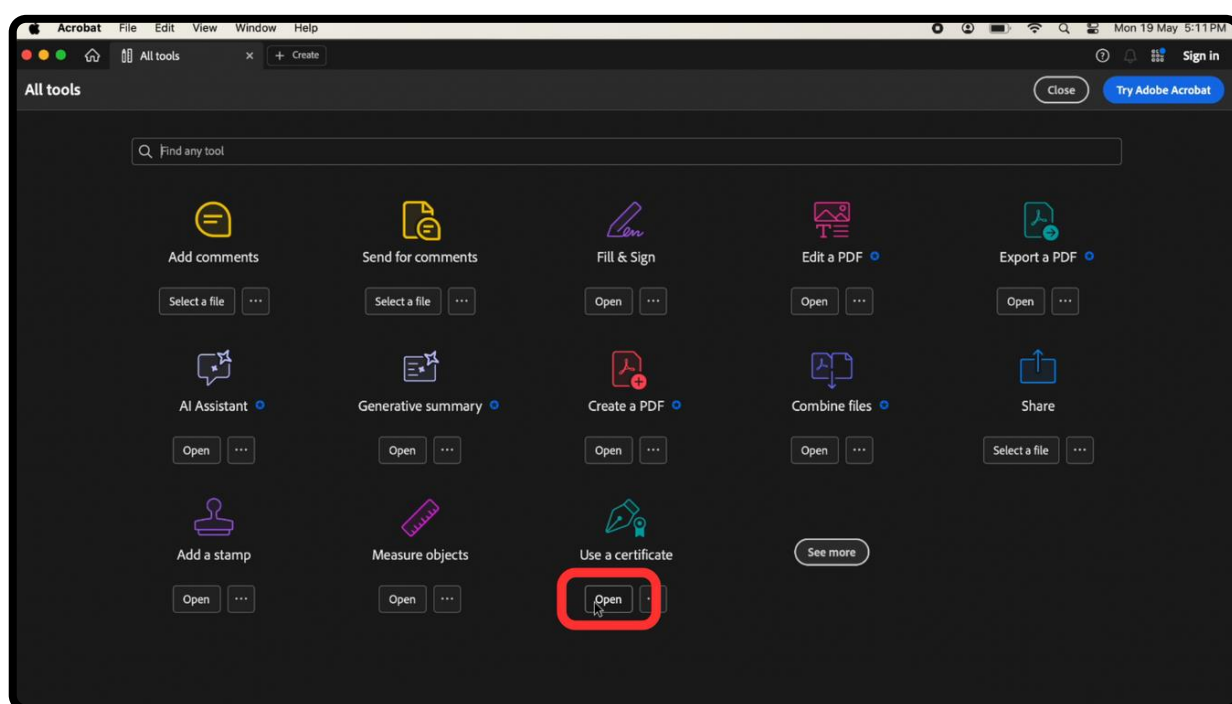


Step 20 – This certificate can now be used for signing. Click on “Close” to exit this window.

W. Signing a Document (MacOS)

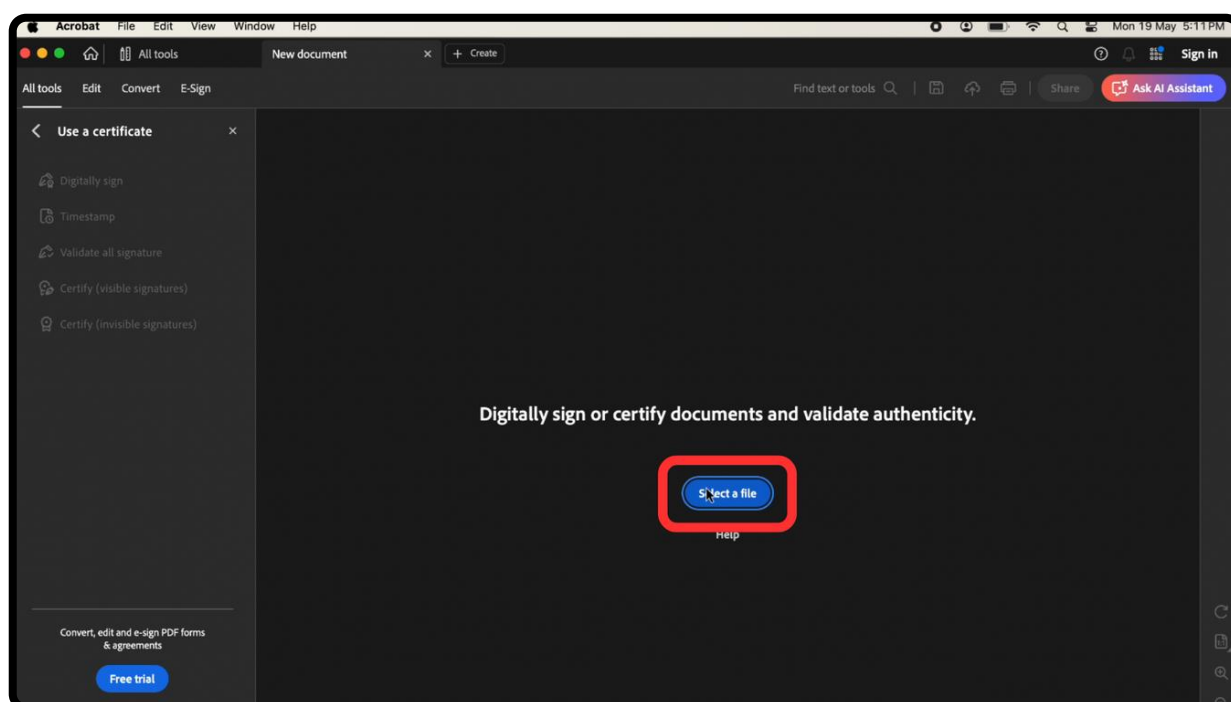


Step 1 – To sign a document on your Mac, start Adobe Acrobat and click on the “See All Tools” button on the home page.

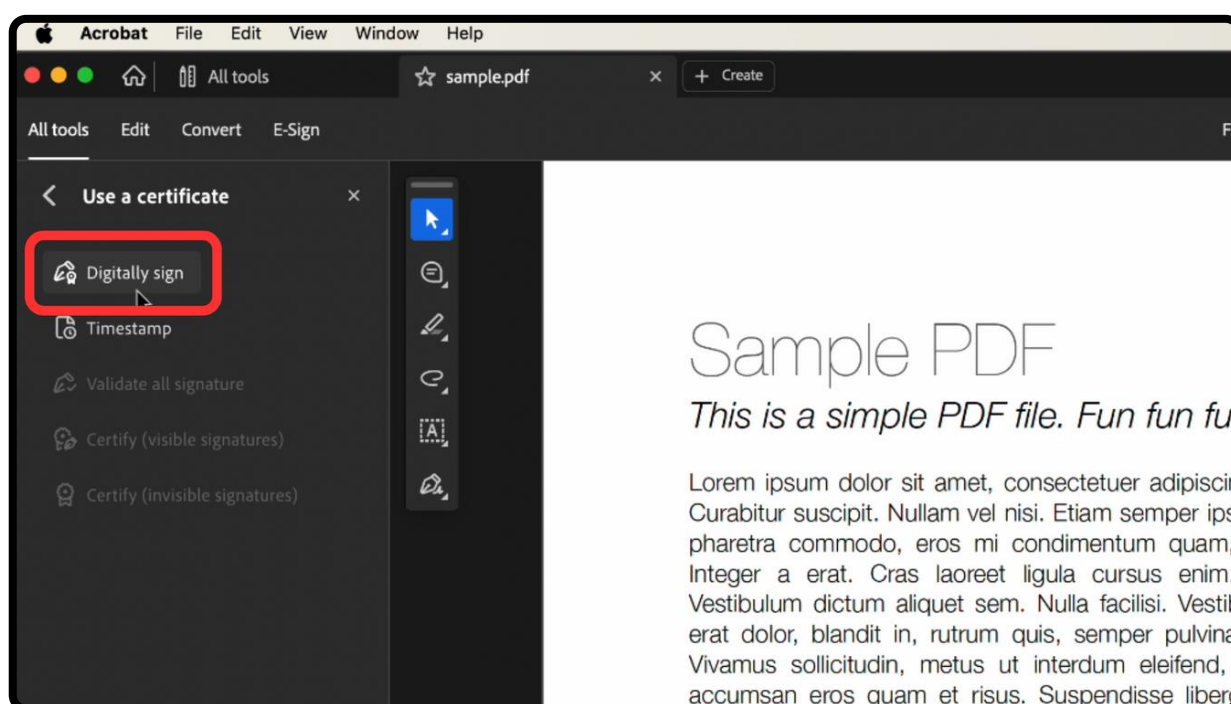


Step 2 – Now, click on “Open” under the “Use a Certificate” option.

W. Signing a Document (MacOS)



Step 3 – Please click on the “Select a File” button and use the browse feature to select the file that you would like to sign.

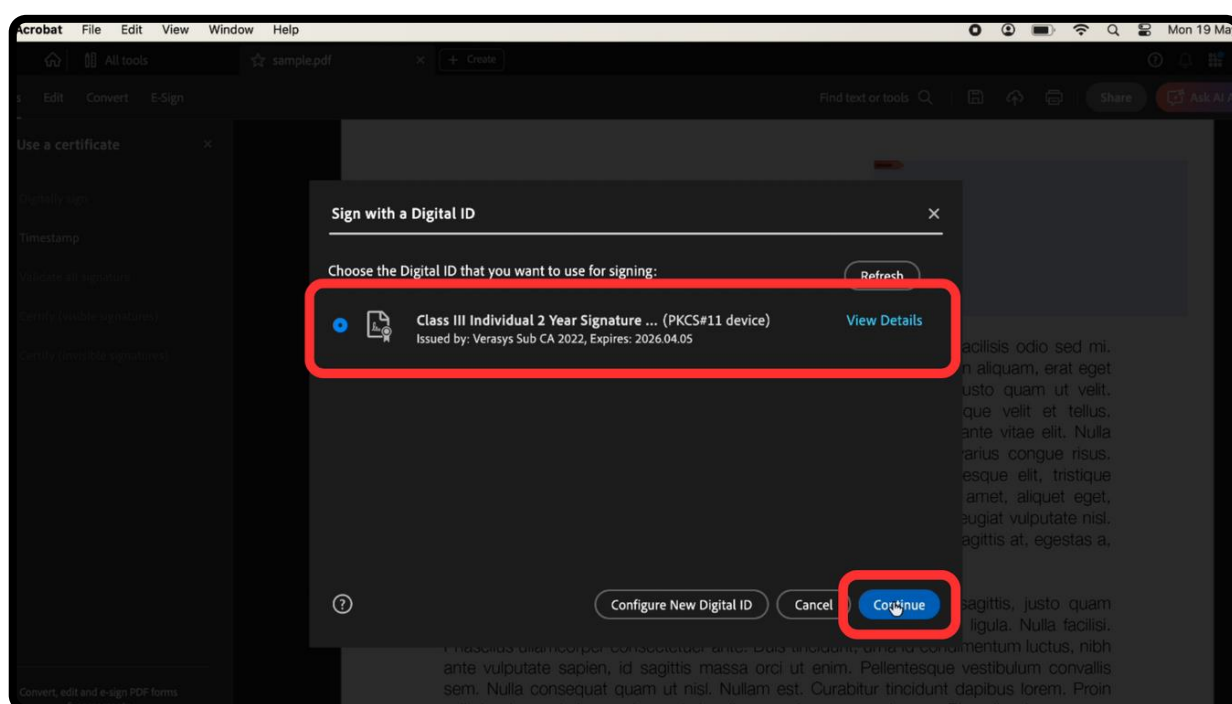


Step 4 – Once the file opens, click on the “Digitally Sign” option on the left pane.

W. Signing a Document (MacOS)

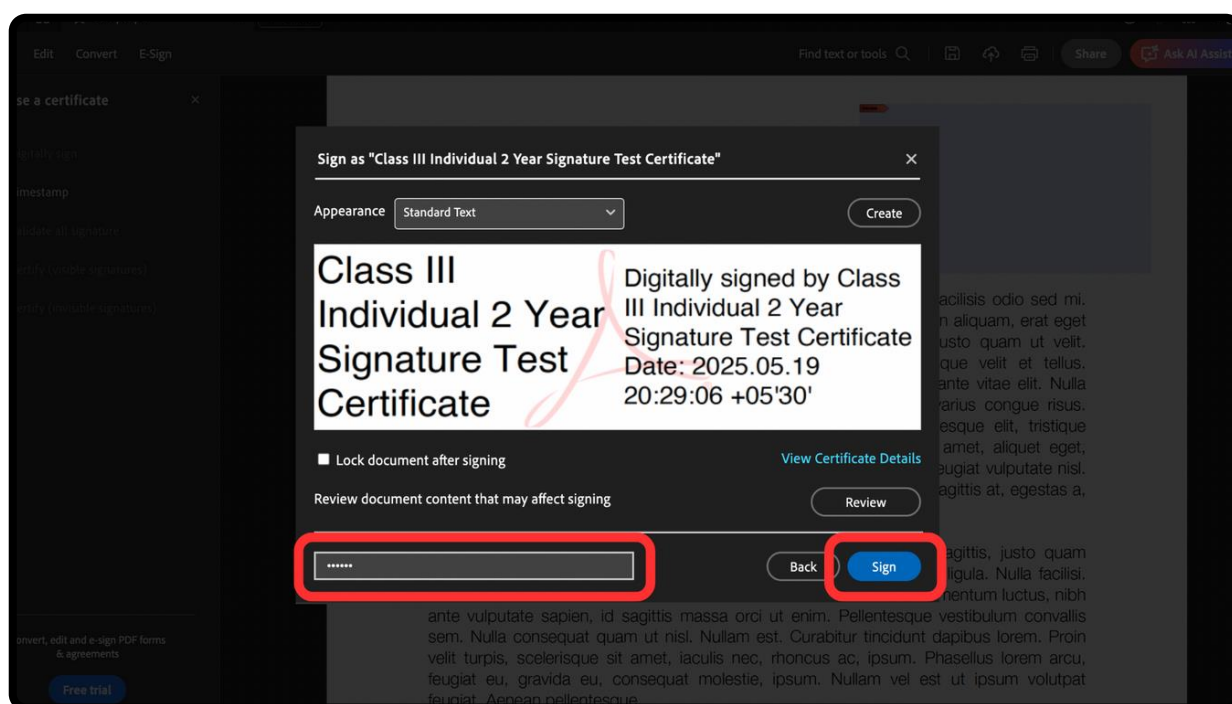


Step 5 – Select the place within your document, where you would like the sign to appear.

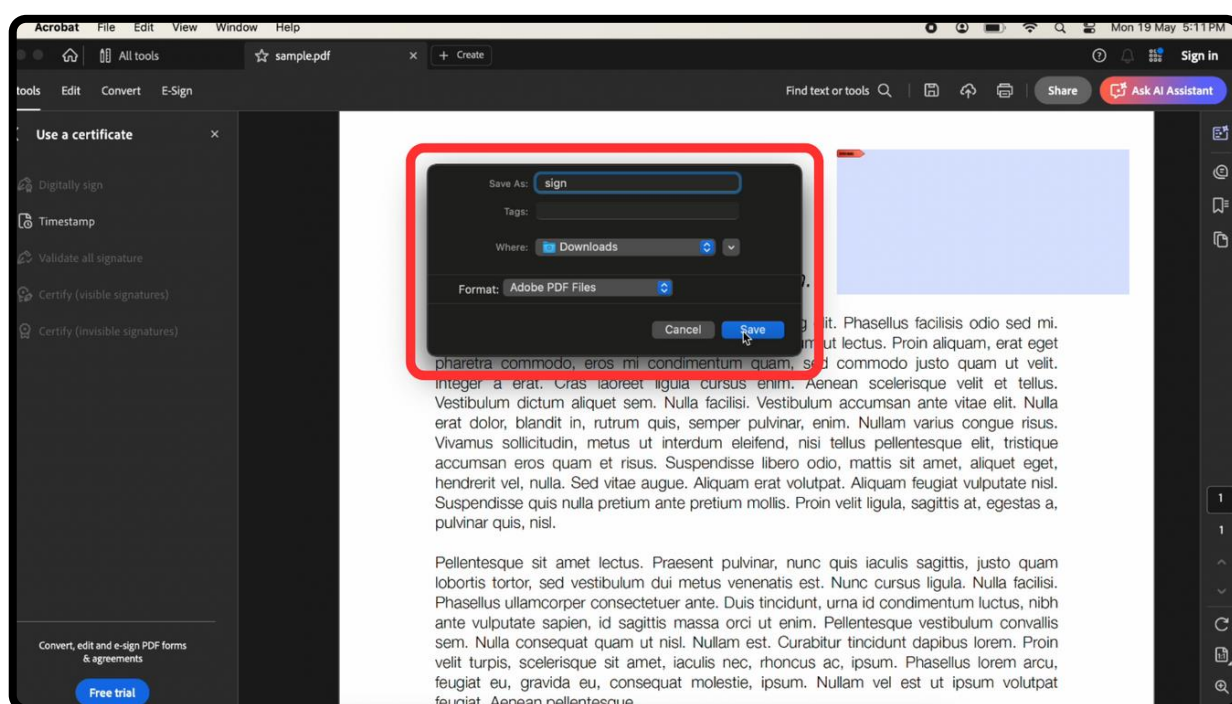


Step 6 – A pop-up will appear asking you to select the certificate that you would like to use. Click on "Continue" after selecting the same.

W. Signing a Document (MacOS)

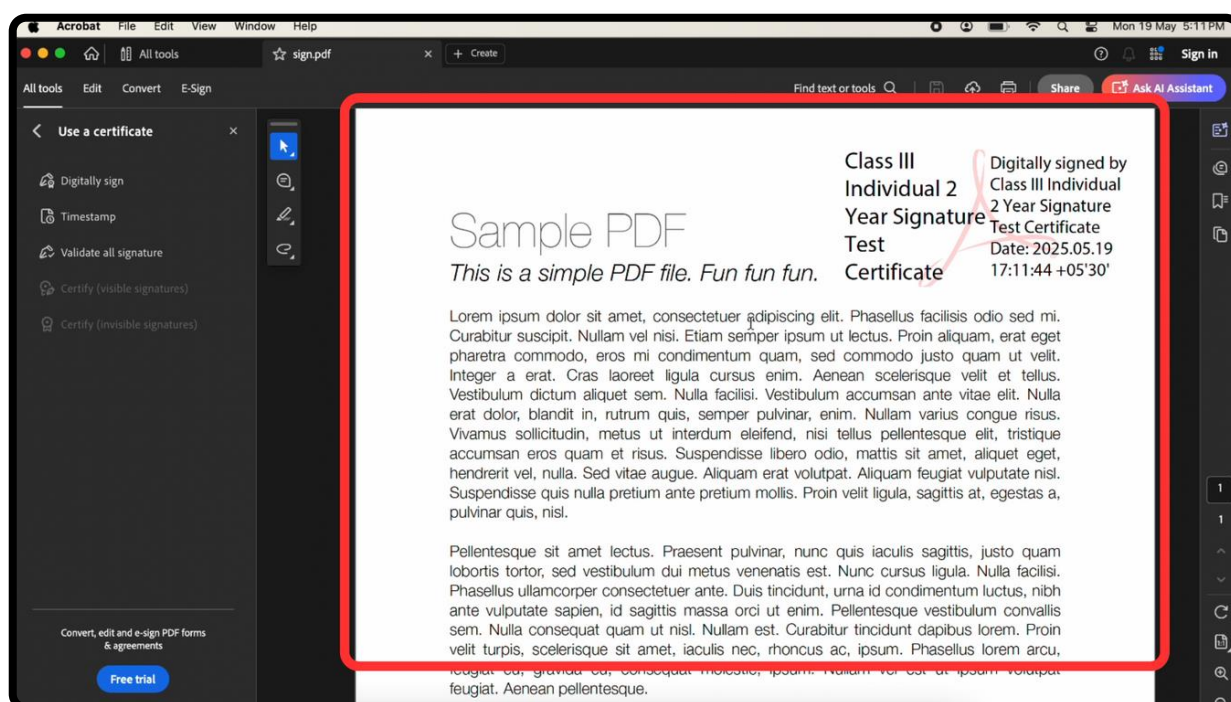


Step 7 – Enter your token's password and then click on the "Sign" button, to proceed.



Step 8 – You will also be prompted to save the signed PDF as a separate file. Please enter the necessary details to do so.

W. Signing a Document (MacOS)



Step 9 – Your document has been signed successfully.



PRECISION
BIOMETRIC

Thank You!