DerivID
User Guide

Table of Contents

DerivID User Manual

Sept 2019

DerivID

DerivID is a patent pending, first-of-its-kind derived PIV/CAC credentials solution that validates the identity of mobile users seamlessly, simply and securely. It exceeds NIST and DISA security standards and eliminates the need for an external card reader. Our credential issuance process guarantees the highest level of assurance.

DerivID credentials provide a convenient replacement for your CAC or PIV card. The need for a physical card reader is eliminated. With DerivID credentials you will have the same secure access to your government resources but without the inconvenience of having to use your CAC or PIV each time you access a familiar device. The DerivID solution consists of multiple apps on any mobile device.

DerivID Applications

DerivID Enrollment

This is a Windows application used to authenticate the user with their CAC or PIV. Enrollment will grant an activation code which can be used in the DerivID application for iOS or Android.

DerivID

This is an application for iOS and Android. After enrolling, the activation code which is granted can be used in this app. Using the granted activation code will generate the certificates.

DerivID CP

This is an application for iOS and Android. DerivID CP (CryptoPath) allows for the creation of a secure tunnel from your public network to your corporate network, allowing for access to internal resources. If your organization chooses to deploy the CryptoPath solution to enhance the security of accessing your enterprise resources, then you need to download this app.

DerivID Secure Browser

This is a sample application for iOS and Android. It functions as a secure Internet Browser. When installed, this sample browser has the ability to communicate with the certificates stored in the DerivID app. When using this app, secure sites requiring certificate-based authentication can be accessed.

Pre-Enrollment Phase (Registration)

In order for the DerivID App to be used, the CAC or PIV must be registered in MobiNET. The CAC or PIV can then have its certificates derived.

Installing the Certificate and Credentials

In order to register your certificate and credentials, you need to:

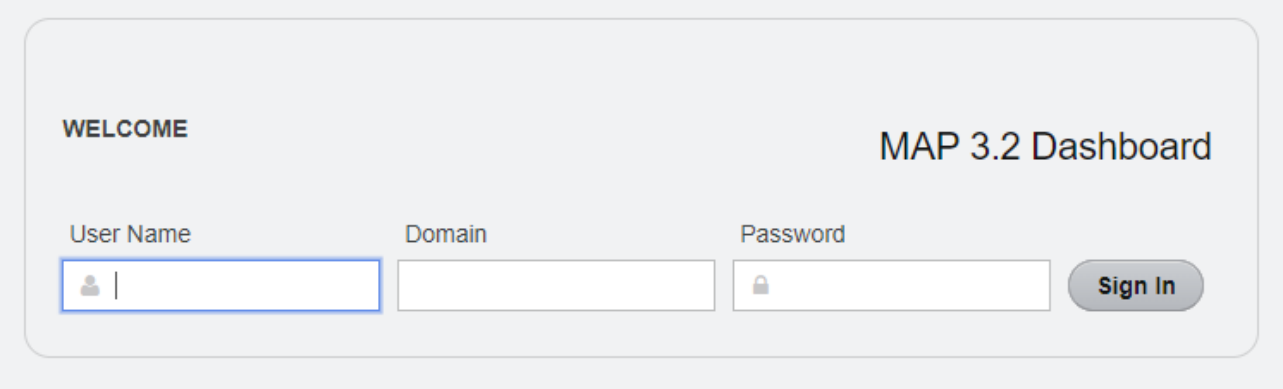
1. Send an email to support@route1.com to request a unique PKI (Public Key Infrastructure) certificate to enable Multi-Factor authentication into the MobiNET Administration and Provisioning (MAP) website
2. After you've received the certificate (usually in a .pfx format), install it (a password will be required which is usually provided by phone)

Internet Explorer	Edge *	Firefox	Chrome
1. Double click on the certificate file **2.** Click **"Next"** to accept all default configurations 3. When prompted for the password, enter the password as provided to you by Route1 4. Continue with the default configuration until you have received an **"Install Successful"** message 5. Launch IE	1. Double click on the certificate file **2.** Click **"Next"** to accept all default configurations 3. When prompted for the password, enter the password as provided to you by Route1 4. Continue with the default configuration until you have received an **"Install Successful"** message 5. Launch Edge ** browser not officially tested*	1. Launch Firefox **2.** Click **"Tools" | "Options"** 3. Click **"Advanced" | "Certificates" | "View Certificates"** 4. From the **"Your Certificates"** tab, choose **"Import..."** 5. Browse to the saved certificate and select **"Open"** 6. When prompted for the password, enter the password as provided to you by Route1 7. Click **"OK"** to exit the installation window	1. Double click on the certificate file **2.** Click **"Next"** to accept all default configurations 3. When prompted for the password, enter the password as provided to you by Route1 4. Continue with the default configuration until you have received an **"Install Successful"** message 5. Launch Chrome

3. Access the MobiNET Administration and Provisioning (MAP) website and select the newly installed certificate when prompted

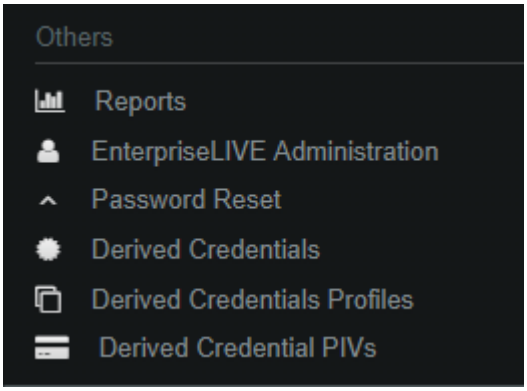
Accessing the MobiNET Administration and Provisioning (MAP) Website

1. Once you've provided a valid certificate to authenticate into MAP, additional credentials will be required
2. Enter the username, password and domain to login



Pre-Enrolling the Smart Card – PIV / CAC Creation

1. On the left-hand side is a navigational menu. Scroll all the way down until "Derived Credential PIVs" can be found (under the "Others" category)

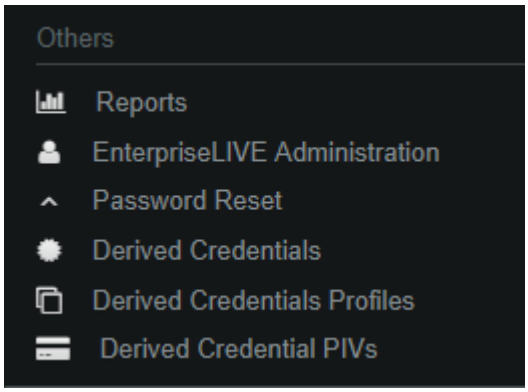


2. After clicking on "Derived Credential PIVs," click on the "+" button to add a new PIV/CAC

3. Enter the UPN of the PIV or CAC (from the Authentication Certificate), then click "Save"

Pre-Enrolling the Smart Card – Profile Creation

1. On the left hand side is a navigational menu. Scroll all the way down until “Derived Credential Profiles” can be found (under the “Others” category)

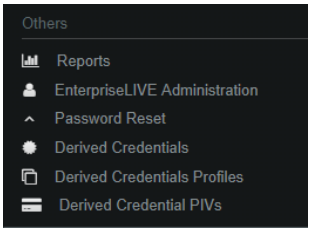


2. After clicking on “Derived Credential Profiles,” click on the “+” button to add a new Profile

3. Give the Profile a name
4. Under “Settings,” you will find entries such as “domainName” and “domainKey” under “defimnetDomain” and “tunnelConfig” under “vpnTunnel”
5. These values will need to change – if you are not sure which values to choose, our support team can be contacted (see “Route1 Support” for details)
6. Change “domainName” to accurately reflect which domain you reside in
7. Change the “domainKey” to the appropriate license key
8. Change the IP address seen in “tunnelConfig” to the appropriate tunnel IP address
9. Click on “Save”

Pre-Enrolling the Smart Card – Assigning a Profile

1. On the left hand side is a navigational menu. Scroll all the way down until “Derived Credential PIVs” can be found (under the “Others” category)



2. Click on the PIV or CAC that was created earlier

3. Under the card's details, click on "Edit"
4. Click on "Pick" next to "Profile Group"
5. Click on the Profile Group that was created earlier when the "Derived Credential Profile Groups" dialog pops up
6. Click on "Save"

Enrollment Phase

NOTE: Enrollment can be done in two different ways. If you have a MobiKEY A2T card reader, you may skip to the "Enrolling Through the DerivID App (iOS or Android) - Alternative Usage of the DerivID App (on iOS or Android)" step. Otherwise, continue to "Enrolling Through Windows"

Enrolling Through Windows

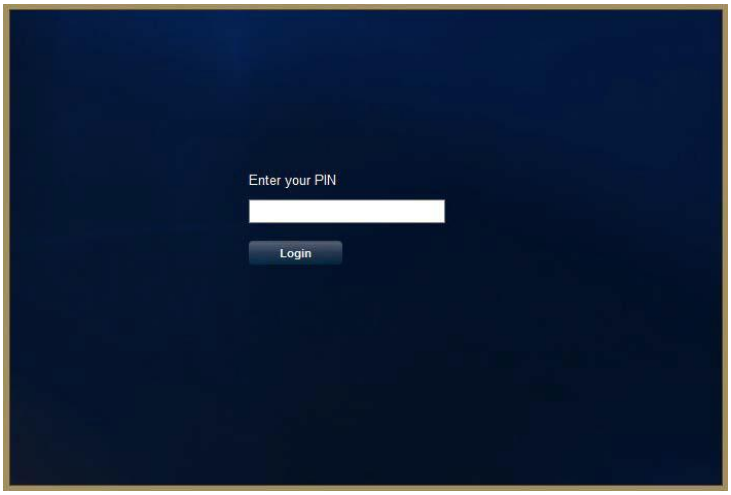
Installation of the DerivID Enrollment Application

1. Send an email to Route1 support to receive steps on how to get the DerivID Enrollment Setup package for Windows
2. Double click on the provided "Setup.exe"
3. If there is a UAC (User Account Control) prompt, administrative rights may be required to proceed with the installation. Contact your Administrator to continue the installation
4. Click on "Next >"
5. Ensure that the END USER LICENSE AGREEMENT FOR ROUTE1 SOFTWARE is read
6. Click on "I accept the terms in the license agreement"
7. Click on "Next >"
8. Optional: Uncheck "Create Desktop shortcuts" if you do not want a DerivID Icon on your desktop
9. Click on "Install"
10. Click on "Finish"

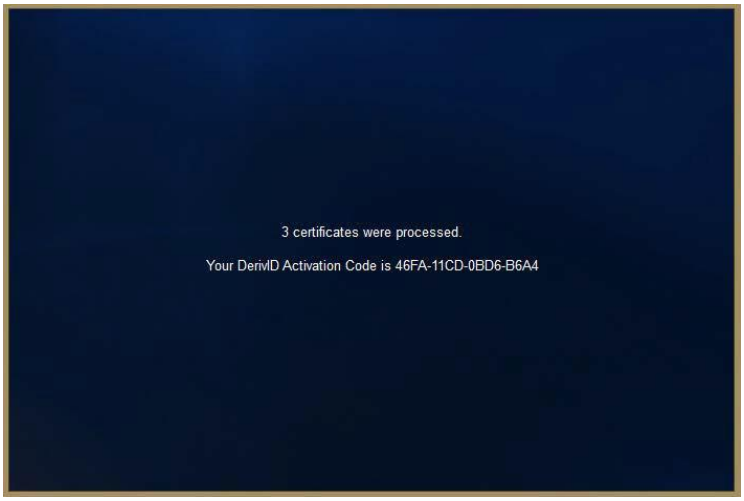
Usage of the DerivID Enrollment Application

1. Launch the DerivID Enrollment app on your desktop
2. Insert your CAC or PIV into the reader at your computer

3. You will be prompted to authenticate. Enter the PIN for your card



4. After entering your PIN, an Activation Code will be generated. Record the Activation Code as this will be required later in the DerivID App (for iOS or Android)



Enrolling Through the DerivID App (iOS or Android)

Installation of the DerivID App (on iOS or Android)

1. Download the DerivID app from the iOS App Store or Google Play Store

Using the DerivID App (on iOS or Android)

1. Launch the DerivID App
2. The App will ask you to set a PIN (6 – 20 digits in length)

3. Enter and confirm the PIN

4. After you've set your PIN, jump to the "Generating Certificates: Using the Activation Code in the iOS or Android application" step

Alternative Usage of the DerivID App (on iOS or Android)

If you have an A2T or Thursby card reader, you will not need to use the Windows DerivID Enrollment Application to generate an activation code. All of this is done through the card reader.

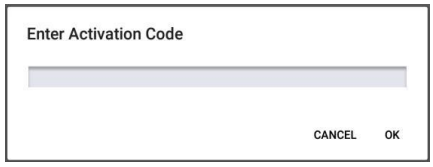
1. Plug your MobiKEY A2T or Thursby card reading device into your Mobile Device
2. Insert your CAC or PIV
3. Launch the DerivID App
4. The App will ask for the PIN associated with the inserted CAC or PIV
5. Enter the PIN of the PIV or CAC that was inserted

After Step 5, the DerivID App will generate an activation code behind the scenes and subsequently generate the certificates (see the next section). This is a much faster method than generating an Activation Code via Windows then redeeming it on the DerivID App. If you've chosen to generate your certificates using the alternative method outlined in these steps, skip to "Generating the Certificates: Automatic Certificate Generation." Otherwise, continue to "Generating the Certificates: Using the Activation Code in the DerivID iOS or Android App."

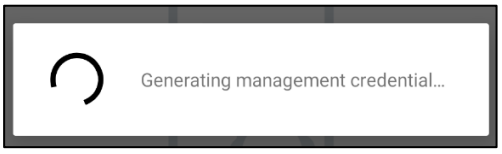
Generating the Certificates

Using the Activation Code in the DerivID iOS or Android App

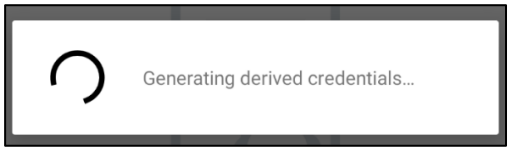
1. When prompted for the Activation Code, enter it (the code that was previously generated)



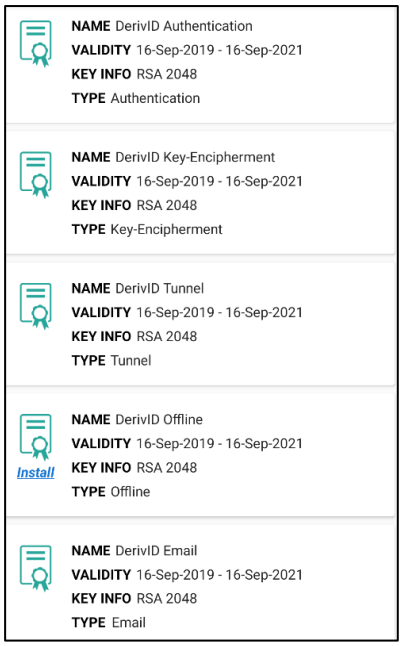
2. The app will now generate the credentials. The first part of the process is the management credential



3. The card's certificates then subsequently get derived

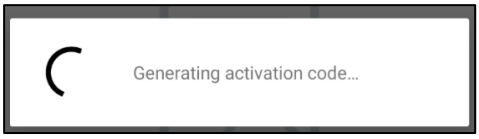


4. All certificates are now generated

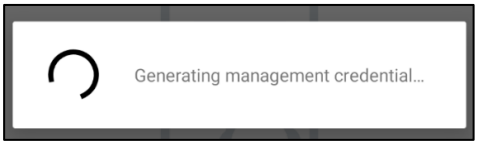


Automatic Certificate Generation

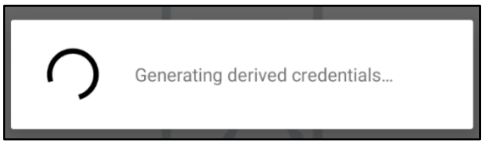
1. After entering the PIN, the DerivID app will perform enrollment and certificate generation automatically. It starts with the creation of an activation code



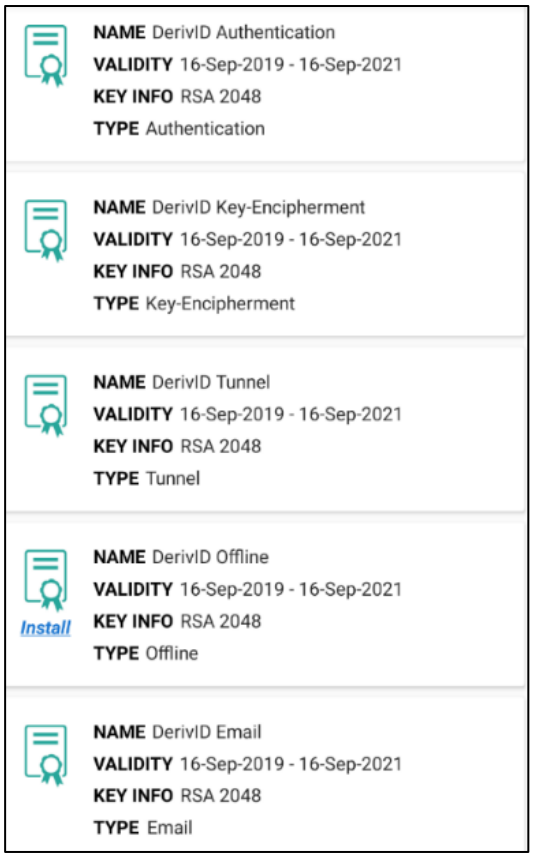
2. It then generates the Management Credential



3. It then generates the Derived Credentials



4. The process is now complete and all Certificates have been derived



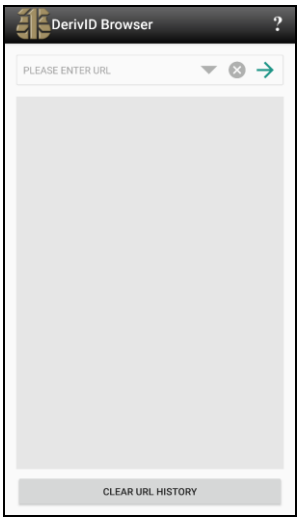
Using the Certificates

Using the Certificates Contained in the DerivID App

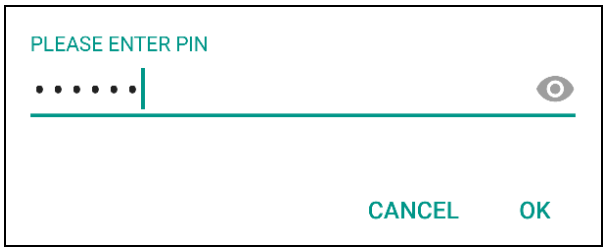
The certificates that are derived are held within the DerivID App, and **only** usable by other DerivID Apps (except for the Offline cert which is covered in the subsequent section). In the example below, a sample app will be demonstrated which makes use of the DerivID App's derived certificates.

Demonstration using the Derived Certificates within the DerivID App on the DerivID Secure Browser Sample App

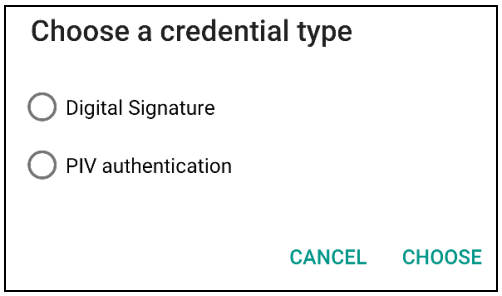
1. Download the DerivID Browser App from the Google Play Store or Apple App Store
2. Launch the DerivID Secure Browser App



3. When launched, click on the empty address bar and enter a website you're familiar with which requires a certificate to access. If this website is accessible only within your corporate network, check the section "Accessing Corporate Entities which make use of your Derived Certificates" before proceeding with the DerivID Browser Sample App
4. After entering the website, tap on the green arrow next to the URL to load the website.
5. There will be a PIN prompt. Enter the same PIN that you're using in the DerivID App (where your certificates are stored) then tap "OK"



6. An additional prompt will ask you to choose a certificate. Choose the certificate that you're familiar with then tap "CHOOSE"



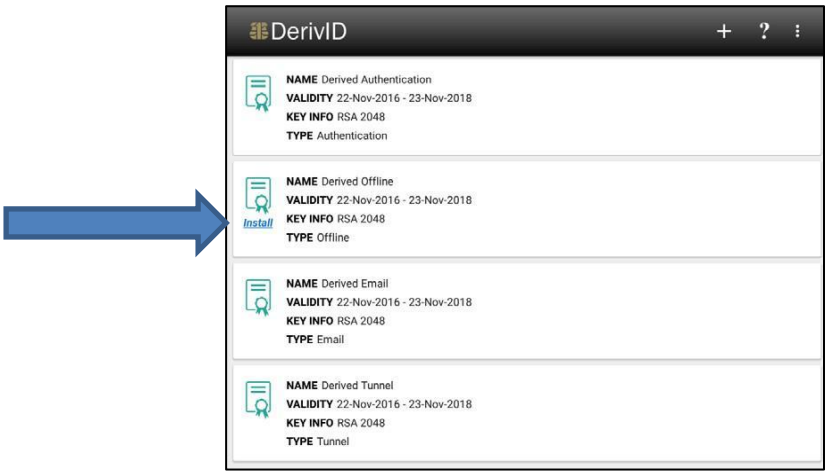
7. At this point, you should have successfully accessed the website

Using the Offline Certificate

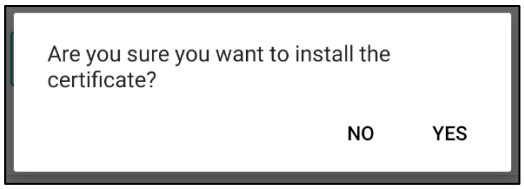
The “Offline” credential type can be installed into the device’s local certificate storage. By doing so, the credentials will be available when you are not connected to a carrier or Wi-Fi network. The ability to use an “Offline” certificate may be required by certain government applications. Below you will find steps on how to install the Offline cert for Android and iOS.

DerivID Android App

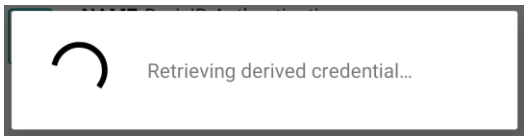
1. Tap the **"Install"** below as noted by the blue arrow



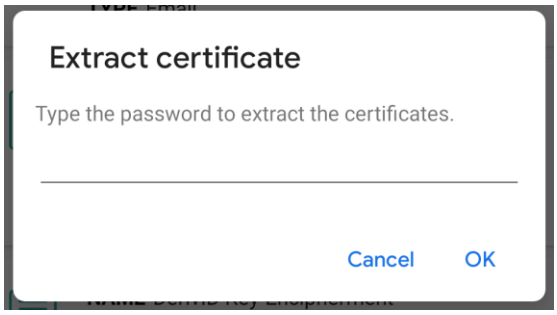
2. After **tapping** "Install," there will be a prompt to install the certificate



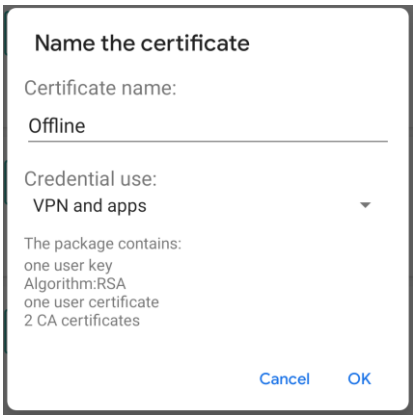
3. Tapping "Yes" will retrieve the offline certificate



4. A password prompt will appear. To continue, enter the PIN of your CAC / PIV (or the PIN that was manually set)



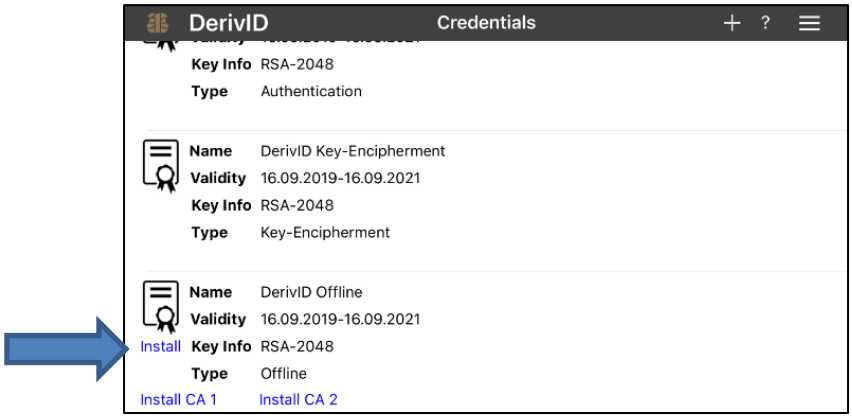
5. If you've entered the correct PIN, you'll arrive at the final step. Give the certificate a name (it defaults to "Offline"), then tap "OK." You will then receive a brief prompt indicating that the certificate was installed



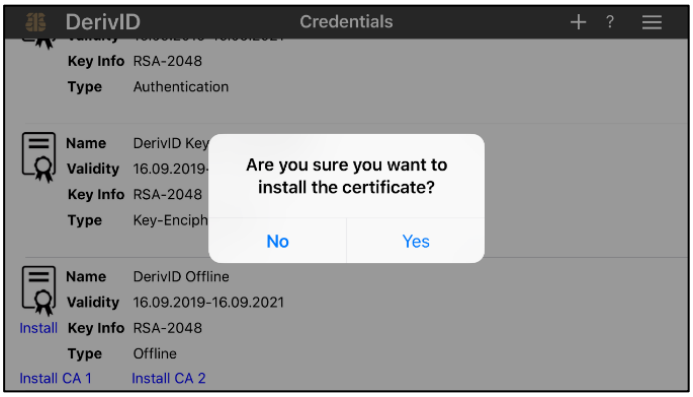
6. With the Offline certificate installed, through Android's Google Chrome app, you may now access websites requiring certificate-based authentication

DerivID iOS App

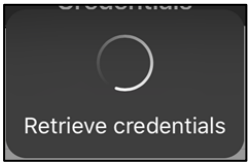
1. Tap the **"Install"** below as noted by the blue arrow

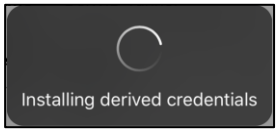


2. After tapping "Install," there will be a prompt to install the certificate

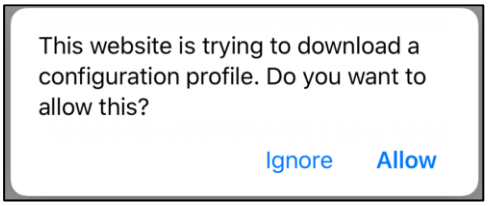


3. Tapping “Yes” will begin the credential retrieval process

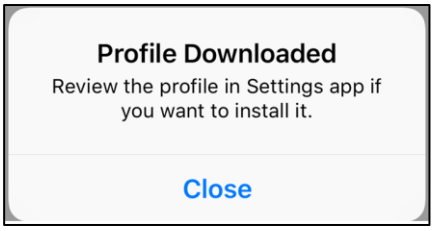




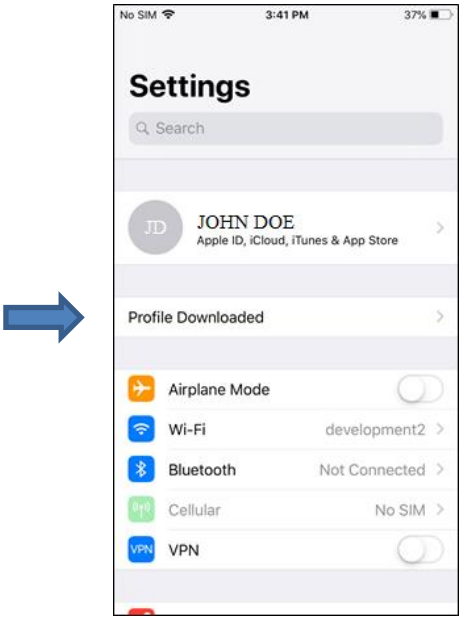
4. You will be redirected to the Safari Browser and asked to download a configuration profile. Tap “Allow”



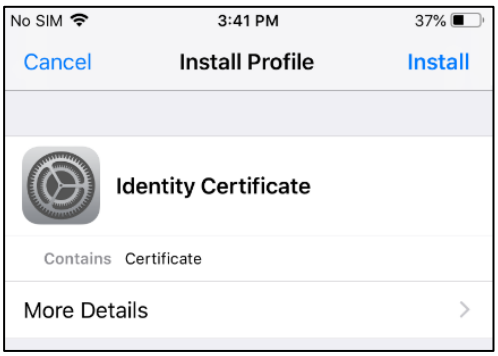
5. After tapping “Allow,” you will be told to review the profile in the Settings app if you want to install it



6. Navigate to the “Settings” app and tap on “Profile Downloaded” (as shown below). An alternative way to get to the profile view is by finding “General” in the Settings app and tapping on it. After tapping on General, scroll all the way down until “Profiles & Device Management” can be found. Tap on it



7. When prompted with the Identity Certificate, tap on “Install”



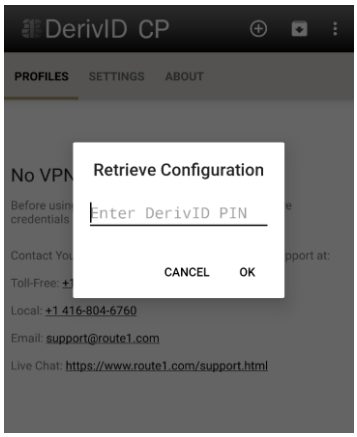
8. You will be asked to first enter your “passcode.” This is the passcode that is used to unlock your iPhone or iPad
9. It will ask you once again to install. Tap “Install”
10. The final step in this process is to enter the password for the certificate. This will be the PIN of your CAC or PIV, or the PIN that was manually set in the DerivID App
11. To install the CAs (these are needed to make use of the Identity Certificate), repeat steps 1 – 10 for each CA
12. After you’ve completed these steps, you will have the Offline certificate installed along with its CAs. Through the Safari app, you may now access websites requiring certificate-based authentication

DerivID CP App

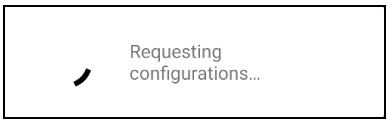
Accessing Corporate Entities (Which Make Use of Your Derived Certificates)

The Crypto Path application can be downloaded from the Google Play Store or Apple App Store. Crypto Path allows for enhanced security when accessing your enterprise resources.

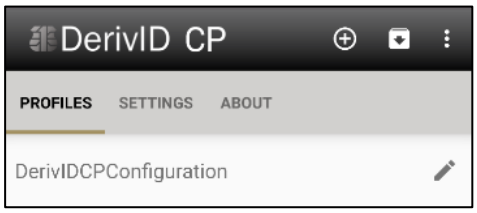
1. After installing the DerivID CP application, open it by tapping on it
2. You will be asked to type a PIN
3. Type your PIN (which is used in the DerivID App that holds the certificates)



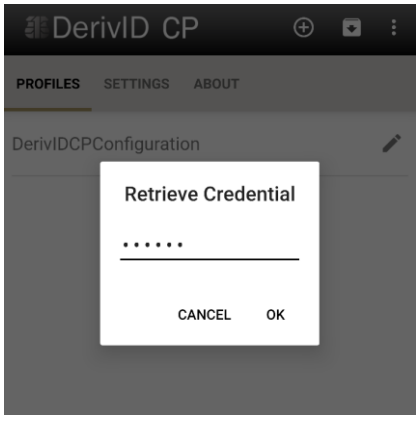
4. After entering the PIN, DerivID CP will communicate with the "Tunnel" credential type in the DerivID App to save a configuration into the DerivID CP app. This configuration contains VPN settings that allow for secure access to enterprise resources. The VPN settings are typically defined by your Administrator



5. After the configuration has been pulled into the DerivID CP app, it will be added into the list of VPNs with the name "DerivIDCPConfiguration"

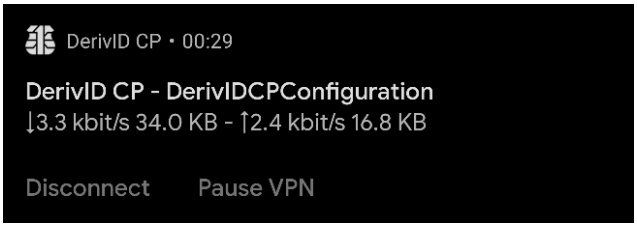


6. To activate the VPN within the DerivID CP application, tap on "DerivIDCPConfiguration" and enter your PIN (the same PIN used in the DerivID App where your certificates are stored)



7. Tap on "OK" to confirm the PIN
8. The VPN will now activate (noted by the Route1 logo on the top left and key icon on the top right in the Notification Bar)

9. Expanding the Notification Bar by swiping your finger down from the top will give you expanded details on the activated VPN. If you wish to turn off the VPN, "Disconnect" can be tapped



Route1 Support

For assistance with installation, the below contact information can be used to communicate with our Route1 support team.

Network Operations Support

support@route1.com

Telephone: +1 416-848-8391
Toll Free: +1 866-286-7330
Support: +1 866-371-1781 (Available from 12 am on Monday to 11 pm on Friday, and 8 am to 8 pm on each of Saturday and Sunday. All times are Eastern)

Office Locations

Arizona
5590 W. Chandler Boulevard, Suite 3
Chandler, Arizona. 85226

Colorado
1200 W. Mississippi Ave.
Denver, CO 80223

Florida
951 Broken Sound Parkway, Suite 108
Boca Raton, Florida. 33487

Tennessee
6031 Century Oak Drive
Chattanooga, Tennessee. 37416

Virginia
9962 Brook Road, Suite 607
Glen Allen, Virginia. 23059

Canada
Corporate Head Office
8 King St. East, Suite 600
Toronto, Ontario. M5C 1B5

Sales Enquiries

sales@route1.com
+1 866-371-1780
+1 416-814-2608