

DerivID User Manual



Table of Contents

1. DerivID	3
2. DerivID and AirWatch	3
3. DerivID Credential Generation	4
4. Minimum System Requirements	4
5. DerivID Enrollment	5
6. DerivID App	6
7. DerivID CP App	8
8. Using DerivID	9
9. Reference	10
10. Contact Us	13

© 2017 Route1 Inc. All rights reserved. Route1 Inc. is the owner of, or licensed user of, all copyright in this document, including all photographs, product descriptions, designs and images. No part of this document may be reproduced, transmitted or otherwise used in whole or in part or by any means without prior written consent of Route1 Inc. Route1, Route 1, the Route1 and shield design Logo, MobiDESK, Mobi, Route1 MobiVDI, Route1 MobiDESK, Route1 MobiBOOK, Route1 MobiKEY, Route1 MobiNET, IBAD, MobiVDI, MobiNET, DEFIMNET, Powered by MobiNET, Route1 Mobi, Route1 MobiLINK, TruOFFICE, MobiLINK, EnterpriseLIVE, PurLINK, TruCOMMAND, MobiMICRO, DerivID, MobiENCRYPT and MobiKEY are either registered trademarks or trademarks of Route1 Inc. in the United States and/or Canada. All other trademarks and trade names are the property of their respective owners. The DEFIMNET and MobiNET platforms, the MobiKEY, MobiKEY Classic, MobiKEY Classic 2, MobiKEY Classic 3, MobiKEY Fusion, MobiKEY Fusion2, MobiKEY Fusion3 devices, and MobiLINK are protected by U.S. Patents 7,814,216, 7,739,726, 9,059,962, 9,059,997 and 9,319,385, Canadian Patent 2,578,053, and other patents pending. The MobiKEY Classic 2 and MobiKEY Classic 3 devices are also protected by U.S. Patents 6,748,541 and 6,763,399, and European Patent 1001329 of Aladdin Knowledge Systems Ltd. and used under license. Other patents are registered or pending in various countries around the world.

DerivID User Manual

January 2017

DerivID

A New Era in Secure Mobile User Identity Validation
Derived Credentials for PIV and CAC

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.

1. DerivID

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.

The DerivID solution consists of two Apps on your mobile device and an enrollment application:



DerivID: The first App enables you to initially generate credentials for your device.

DerivID CP: The second App permits the establishment of a highly secure Crypto Path™ tunnel for accessing the government network.

DerivID Enrollment: A Windows application that is used to initially authenticate you based on your CAC or PIV card. It issues an Activation Code that permits you to generate the DerivID Credentials for your mobile device.

2 DerivID and AirWatch

DerivID is fully integrated with the AirWatch Enterprise Mobility Management Solution, providing a seamless process for the issuance of your new identification.

Typically, either your administrator will perform initial provisioning of your mobile device or you will be sent an email instructing you to download the AirWatch App from

the Google Play Store or the Apple App Store. You need to follow these instructions, as they are a prerequisite to generating your DerivID credentials.

3. DerivID Credential Generation

The process consists of a series of steps that will be explained in detail in the subsequent sections.

1. DerivID Enrollment.

The DerivID Enrollment program authenticates your identity against the credentials on your CAC or PIV Card. The DerivID enrollment program creates an activation code used to authenticate your credentials on a mobile device through the DerivID App.

2. DerivID Credential Generation using the DerivID App.

The DerivID App creates a set of soft credentials once an activation code from the DerivID Enrollment program is entered. These soft credentials are based off of the credentials on your CAC or PIV card and can be used in all of the same applications.

3. Profile configuration with the DerivID CP App.

Upon opening the DerivID App you will be prompted for a PIN number. Once the PIN is entered a DerivID CP configuration profile will be created based on your organization's Airwatch settings. You also have the option to create your own profiles and change the settings as needed.

4. Minimum System Requirements

Minimum System Requirements for the DerivID Enrollment Application

- Windows 7 x32/x64, Windows 8.1 x32/x64 and Windows 10 x32/x64
CAC or PIV Card Reader: any CCID-capable smart card reader

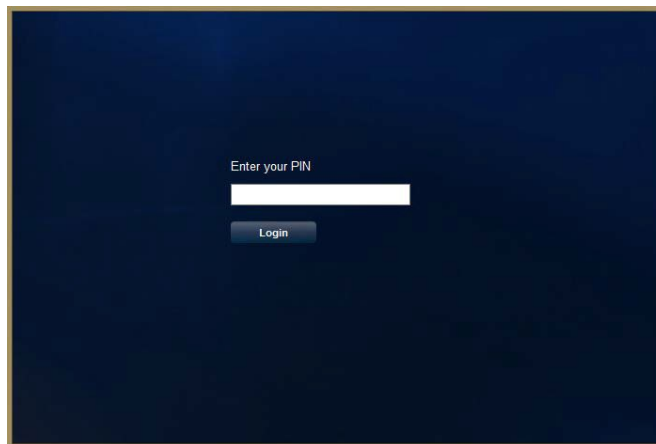
Minimum System Requirements for DerivID and DerivID CP Applications

- Android version Kitkat (4.4), Lollipop (5.1.1) and marshmallow (6.0-6.0.1)

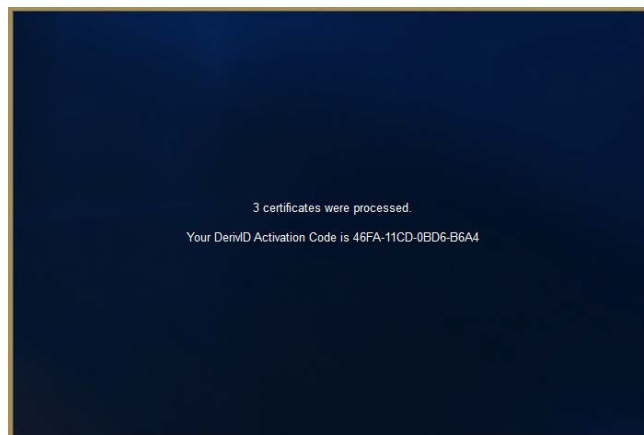
5. DerivID Enrollment

This is a windows application used to authenticate you with your CAC or PIV Card and provide an activation code to enroll the DerivID App.

1. Launch the DerivID Enrollment application on your desktop.
2. Insert your CAC or PIV Card into the reader at your computer.
3. You will be prompted to authenticate. Enter the PIN for your CAC or PIV Card.



4. Record the Activation Code you are given from the DerivID Enrollment Application. We will use this to register the DerivID Mobile Application.



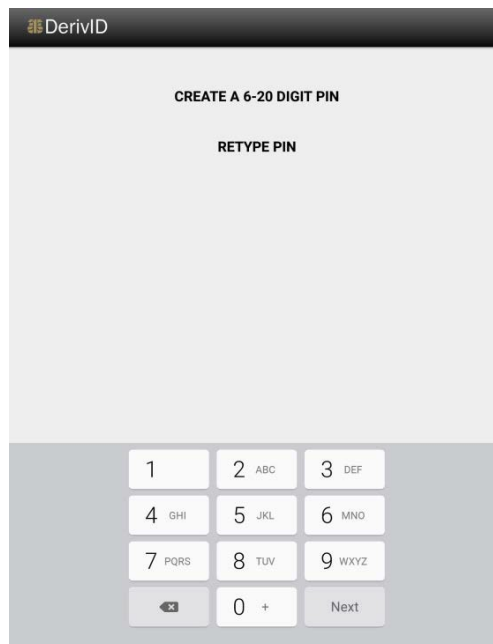
6. DerivID App

Typically the DerivID App will be automatically installed on your mobile device as part of the AirWatch EMM enrollment process. If it has not been installed on your device, you should download it from the Google Play Store or the Apple App Store.

1. Launch the app on your Mobile Device.



2. You will be prompted to create a PIN number.
3. Create a 6 to 20 Digit PIN and remember it. This will be the PIN you use to unlock your Derived Credentials going forward.

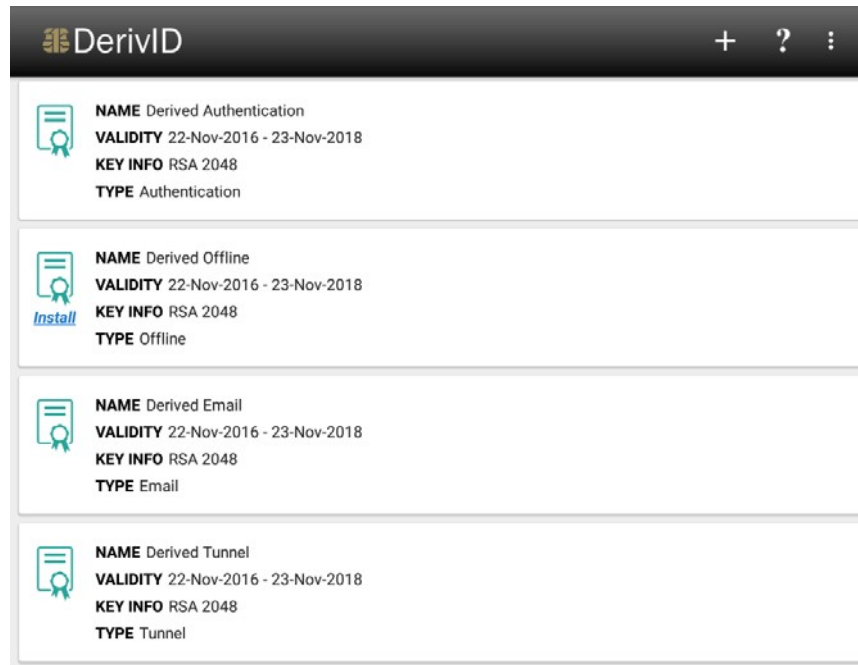


4. Then enter the Activation Code from the windows DerivID Enrollment when prompted with the window below.

Enter Activation Code

CANCEL OK

5. All credentials should now be present and automatically installed.
6. The credential of type **“Offline”** can be installed into the local system keychain. By doing so the credentials will be available when you are not connected to a carrier or Wi-Fi network. This may be required by certain government applications. To do this, click the **“Install”** button under the cert icon pictured below.



7. The type, number, name and quantity of certificates will depend on the requirements of your organization.
8. The Process with the DerivID app is now completed. To safely exit the app please perform one of the following options.
 - a. For Android KitKat and Lollipop: Minimize the DerivID app by pressing the menu or home button. Do not force close the application.
 - b. For Marshmallow: Double click the back or home button and return to the home screen.

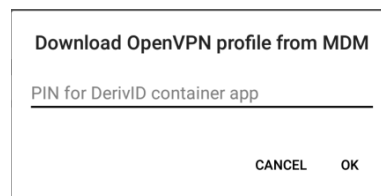
7. DerivID CP App

If your organization chose to deploy the Crypto Path solution to enhance the security of accessing your enterprise resources, then typically, the DerivID CP App will be automatically installed on your mobile device as part of the AirWatch EMM enrollment process. If it has not been installed on your device, you should download it from the Google Play Store or the Apple App Store.

1. Open the DerivID CP app



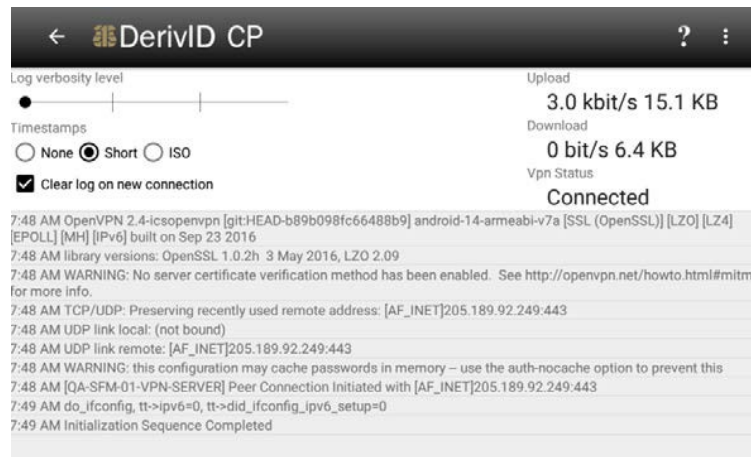
2. Enter your DerivID PIN when presented with the dialogue box below and Select "OK".



3. This will automatically retrieve a profile configuration for the DerivID CP app.



4. Click on the newly created profile. This will open up a new page and establish a secure connection.



5. Once the connection is established and the VPN status changes to **“Connected”**.



8. Using DerivID

Based on your organization’s configuration the DerivID credentials should now be available to all the applications that require them.

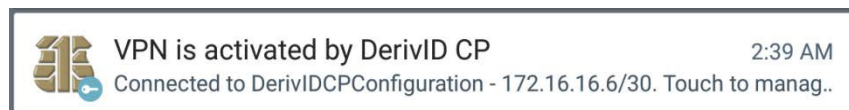
If your organization requires you to connect through the Crypto path please complete the following steps:

1. Ensure that both the DerivID and DerivID CP apps are running.
2. Open the DerivID CP app.
3. Select the **“DerivDCPConfiguration”** profile.



4. Minimize the application and confirm it is running in the background.

You can check notifications by pulling down on the top center of the touch screen.



You will now be able to digitally sign documents and emails as well as log into secured websites using your government credentials all from this mobile device.

9. Reference

DerivID Enrollment

About Button

Clicking the **"About"** button will bring up the DerivID IP notice, copyright information and support team contact information.

Login Button

Clicking the **"Login"** button will authenticate the entered PIN against the CAC or PIV card inserted in the computer.

Help Button

Selecting the **"help"** button will give the option to use Chrome or Internet to view the www.route1.com/support.html page.

Exit Button

Clicking the **"Exit"** button closes the application.

DerivID

Plus Button (+)

Clicking the **"+"** symbol displays the Activation code text box.

Entering a random value into Activation code displays **"Activation code invalid"**.

Adding the correct activation code displays **"generating management credential"** followed by the **"generating derived credential"** message.

Pressing **"+"** after credentials are already present displays **"Credentials exist"**.

Question Mark Button (?)

Pressing the **"?"** Button brings you to the Route1 support website.

Logout Button

Selecting the **"Logout"** button brings the device back to the DerivID pin prompt.

Delete all credentials Button

Pressing the **"Delete all credentials"** button when no certificates are present will display the message **"Nothing to delete"**. With certificates present, the message **"Are you sure you want to delete all credentials"** is displayed.

Pressing **"ok"** immediately deletes all Credentials in DerivID.

Canceling exits dialogue box and no certificates are deleted.

Three Dots Button (...)

Pressing the **"..."** button and selecting **"About"** displays the EULA

DerivID CP

Profile tab

The VPN Profile is downloaded and listed under the **"Profiles"** tab.

When the profile is clicked **"Retrieve Credential"** is displayed and you must enter the pin you set in DerivID. A connection through the VPN should then be initiated and established.

Clicking the icon to the right of the name of the profile and then clicking the three dots in the top right will display 2 options **"Remove VPN"** and **"Duplicate VPN"**.

Settings Tab

Allows you to change the application and VPN behavior.

About tab

Clicking the about tab displays the DerivID CP version and copyright information. The source code license information for programs used with DerivID CP is also listed.

Full Licenses Button

Pressing the **"Full Licenses"** button will display all the license information for all programs being used.

Three Dots Button (...)

When the **"..."** button is clicked the buttons **"log window"** and **"Help"** will appear.

Help Button

Selecting the **"help"** button will give the option to use Chrome or internet to view the www.route1.com/support.html page.

Show log window Button

Selecting the **"Show log window"** button will display the log information for the VPN connection that was made. Clicking the **"..."** again will display the options **"Clear log"**, **"Send log file"** and **"Disconnect VPN"**.

Clear Log Button

Selecting the **"Clear Log"** button will erase the contents of the specified log file.

Send Log File Button

Selecting the **"Send Log File"** button will display an application selection window for the file to be sent with. This can include messaging and emailing applications, as an example.

Disconnect VPN Button

Selecting the **"Disconnect VPN"** button will bring a disconnect confirmation window, where you will be asked if you would like to disconnect from the VPN or cancel the connection attempt.

10. Contact Us

Canada:

8 King St. East, Suite 600
Toronto, Ontario
M5C 1B5

Telephone: +1 416-848-8391
Toll Free: +1 866-286-7330
Fax: +1 416-848-8394

Sales Inquiries:

sales@route1.com

+1 866-371-1780
+1 416-814-2608

USA:

1 South Ocean Blvd., Suite 201
Boca Raton, Florida
33432

Telephone: +1 866-286-7330
9962 Brook Road, Suite 607
Glen Allen, Virginia
23059

Telephone: +1 703-919-1353

Network Operations Support:

support@route1.com

+1 866-371-1781
+1 416-804-6760