ROUTE1
DRIVING DATA FORWARD

Security Officer Configuration Guide

DerivID with AirWatch EMM

Table of Contents

© 2019 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.   See https://www.route1.com/terms-of-use/ for notice of Route1's intellectual property.

Security Officer Configuration Guide

July 2019

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

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.

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 end-user portion of the DerivID solution consists of two Apps on your mobile device and an enrollment application:

DerivID DerivID CP

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.

The capabilities of the DerivID technology are enabled through the **DEFIMNET** infrastructure. DEFIMNET is Route1's fully accredited universal identity management and service delivery platform that is deployed within government facilities.

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.
As part of the initial enrollment of a mobile device into AirWatch, it is recommended that the DerivID and DerivID CP Apps be installed on the mobile device. That can be accomplished by providing the links to the Apps within Google Play Store or the Apple App Store, or alternatively, Route1 can provide the required APK or IPA files.
The configuration of the DerivID Credentials that will be issued to the users is performed through the AirWatch console. DEFIMNET communicates with the AirWatch Mobile-Cloud Architecture in order to orchestrate the DerivID Credential generation.

3. DerivID Credential Issuance Process

DEFIMNET Provisioning and Integration
To enable the Issuance of DerivID Credentials, DEFIMNET requires interconnectivity with:

- Pertinent Agency or Federal Bridge Certificate Authorities
- Pertinent IDMS and ICAM systems
- LDAP/ActivDirectory Services (to update user account with issued certificates)
- MDM/EMM Systems

The integration and provisioning process is coordinated by the Route1 Customer Support Team.

One component of the provisioning involves associating your EMM system or systems with your one or more UPN-suffixes. The UPN is extracted from the User’s CAC or PIV Authentication certificate during the enrolments process. The suffix is used to locate the user’s mobile device (identified by a UDID) in a set of associated MDM/EMM systems.

Depending on the desired topology, you will be issued a DEFIMNET Domain Key that is required to authenticate the configuration settings.

DerivID Custom Settings Record

A Configuration Settings record is created and placed within a baseline Profile that needs to be installed on the user's device as part of the initial Mobile Device enrolment. The Configuration Settings record defines, amongst other things, what credentials will be generated for the user.

SCEP Server Configuration

Leveraging the AirWatch Certificate Authority Integration capabilities, the DEFIMNET SCEP Proxy Service must be configured.

Certificate Authority Request Template Configuration

One element of the credential generation process involves the MDM/EMM system, as a consequence of installing certain profiles that request credentials, providing data to the mobile device that must be part of the Certificate Signing Request. Specific syntax and attributes are required – the configuration is done through a Certificate Authority Request Template.

The AirWatch administrator executes the following steps:

1. Copy the script in Section 8 we will need to use it later.
2. Open the AirWatch Console.
3. Go to the Devices Tab.
4. Go to the Profiles and Resources Tab.
5. Go to the Profiles Tab.
6. Select add Profile or edit on an existing profile.
7. Fill in the General Section.
8. Go to Custom Settings.
9. Select Configure.
10. Paste the script from step 1 into the Custom settings field.
11. Select Save and Publish to save the changes.

4. User Applications Explained

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

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.

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.

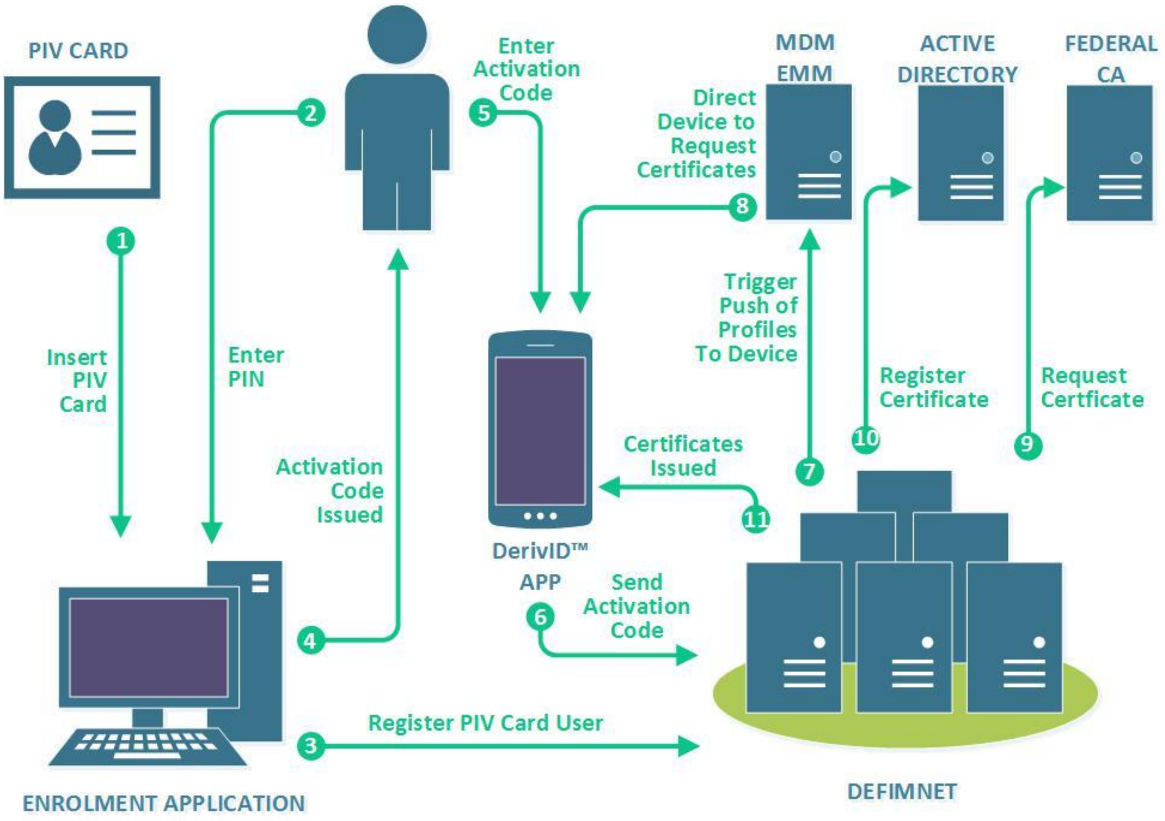
Profile configuration with the DerivID CP App

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.

5. Crypto Path: DerivID CP

DerivID CP is an enhanced VPN Client that leverages the DerivID Virtual Smart Card technology of the DerivID to provide a secure connection to the services provided by your organization.

6. DerivID Credential Generation Process



1. The user launches the DerivID Enrollment Application.
2. The user inserts their CAC or PIV Card.
3. The user enters their PIN associated with their CAC or PIV Card.
4. The CAC or PIV Card is registered to the DEFIMNET.
5. An activation Code is issued by the enrollment application.
6. The user enters Activation Code in the DerivID App.
7. The DerivID App authenticates the Activation Code with DEFIMNET.
8. Once authenticated this triggers a push of profiles to the device through the EMM.

9. The device makes a direct to request for Certificates to the MDM.
10. The DEFIMNET registers a certificate from the Federal Certificate Authority.
11. The DEFIMNET registers Certificate in Active Directory.
12. Certificates are issued by the DEFIMNET to the DerivID App.

7. Configuration Settings Record

One or more Configuration Settings Records needs to be installed within the AirWatch MDM/EMM system. The Configuration Settings Record provides authentication of the configuration, associates the user devices with a DEFIMNET Domain, defines what DerivID Credentials will or may be issued, and provides additional settings. Multiple Configuration Settings Records can be created and associated with different baseline Profiles that are installed at the time of user device enrollment. Such approach enables granular control over the configurations required for different groups of users or mobile devices.

The instructions for installing the Configuration Settings Records are as follows:

1. **Copy** the below script, we will need to use it later.

```
CN={UDID} OU=UPN.smith@abc.gov
OU=DerivID.Route1 (constant)
OU=MDM.AirWatch {MDM.MaaS360}
OU=Type.Email {Type.Authentication | Type.Offline | Type.Email-Offline
|
Type:Key-Encipherment }
```

2. Open the AirWatch Console.
3. Go to the **Devices** Tab.
4. Go to the **Certificates** Tab.
5. Go to the **Certificate Authority** Tab.

6. Select **Request Templates.**
7. Select **add (+)** at the top of the window or **edit** on an existing template.
8. Go to the **Subject Name** field.
9. **Paste** the script from step 1 into the **Subject Name** field.
10. Select **Save** to save your changes.

The Configuration Settings Record Consists of a set of elements represented using JSON, as follows:

Credential Deployment
Credential Deployment is assigned as a either the DerivID-Container or the AirWatch-SCEP this determines how the credentials will be managed.

Credential Deployment: DerivID-Container

Credentials of this type will be managed by the DerivID app. These credentials will be accessible to any custom apps developed using the DerivID SDK. In addition, two types of credentials are treated specially. The credential of type Tunnel is used to establish the crypto path between the DerivID apps and the credential of type offline can be saved in to the system keychain. Please refer to the DerivID User Manual for more detail.

Credential Deployment: AirWatch-SCEP

Credentials of this type are managed by AirWatch EMM.

defimnetDomain

The defimnetDomain establishes the parameters of the domain through the domainName and domainKey variables.

defimnetDomain: domainName

The domainName determines the name of the domain. This is abc.gov in the example configuration script.

defimnetDomain: domainKey

The domainKey will be generated and provided by a Route1 administrator. This creates a unique Identifier for the domain.

vpnTunnel

The vpnTunnel establishes the parameters of the VPN connection through the tunnelConfig variable.

vpnTunnel : tunnelConfig

The tunnelConfig variable establishes a path for the VPN connection.

credentialProfiles

The credentialProfiles establish the parameters of the VPN Connection Profile through the profileName variable.

credentialProfiles : profileName

The profileName variable can be set to either DerivID-Credentials or ActivSync- Boxer.

derivedCredentials

derivedCredentials establishes the parameters of the credentials through the credentialType variable.

derivedCredentials : credentialType

The credential type variable will be different based on the requirements of your organization but can include the types of Authentication, Offline, and Email

credentialDeployment

The credentialDeployment variable can be either set to either DerivID or AirWatch- SCEP depending on the requirements of your organization.

issuingCA

This refers to the issuing certificate authority of the credentials, which in the case of the example configuration file, is Route1 Inc.

addToAD

The addToAD is a Boolean that stands for add to Active Directory, it can be true or false.

aDDomain

The aDDomain variable will change based on the requirements of your organization. aDDomain stands for active directory domain, this will be the domain in which the CAC or PIV card will be registered.

addCnPrefix

The addCnPrefix variable will add the specified prefix to the common name. Your common name is based on your credentials.

addCnSufffix

The addCnSuffix variable will add the specified suffix to the common name. Your common name is based on your credentials.

addUpnPrefix

The addUpnPrefix variable will add the specified prefix to your Universal Principal Name before the email address. For example if addUpnPrefix was set to “LT.” the UPN would appear as LT.johndoe@mail.com

addUpnSufffix

The addUpnSufffix variable will add the specified suffix to your Universal Principal Name before the @ sign. For example if addUpnSufffix was set to “.CTR” the UPN would appear as johndoe.ctr@mail.com .

Credential Types

Credential Type: Authentication

The authentication certificate is used during the log in process to verify your identity.

Credential Type: Email

The email certificate is used to digitally sign emails on your mobile device.

Credential Type: Offline

The offline certificate can be installed locally for use on your mobile device, even when not connected to a carrier or Wi-Fi network.

Credential Type: Tunnel

The tunnel certificate is used to create the secured Crypto Path between DerivID applications.

Credential Type: Storage

The storage certificate is used for the encryption of data at rest.

Credential Type: Email-Offline

The email-offline certificate is used during to digitally sign emails on your mobile device, even when not connected to a carrier or Wi-Fi network.

Credential Type: Key-Encipherment

The key-encipherment Certificate is primarily used to for task such as email encryption.

8. DerivID Example Configuration Record

The following is an example of an AirWatch configuration script:

```
<DerivIDCustomConfig>
{
  "testDomain":{
    "domainName":"abc.com",
    "domainKey":"XXXX-XXXX-XXXX-XXXX"
  },
  "vpnTunnel":  {
    "tunnelConfig":"client\ndev tun\nfloat\nproto udp\nremote
123.678.12.456.123\nresolv-retry infinite\nkey-direction
1\nnobind\npersist-
key\npersist-tun\nca \"trust.pem\"\ntls-auth \"ta.key\" 1\nauth-user-
pass\nauth-nocache\ncipher AES-256-CBC\nverb 3\nRoute1DCType
Tunnel\nabcProfileEditable 0"
  },
  "credentialProfiles":
  [
    {"profileName":"QA - Others"},
    {"profileName":"QA - Airwatch Inbox"}
  ],
  "derivedCredentials": [
  {
    "credentialType":"Authentication",
    "credentialDeployment":"AirWatch-SCEP",
    "issuingCA":"ABCCO",
    "addToAD": "T",
    "aDDomain":"abc.com",
    "addCnPrefix":".",
    "addCnSufffix":".",
    "addUpnPrefix":"",
    "addUpnSufffix":".offline"
    },
    { "credentialType":"Email",
    "credentialDeployment":"AirWatch-SCEP",
    "issuingCA":"ABCco",
    "addToAD": "T",
    "aDDomain":"abc.com",
    "addCnPrefix":".",
    "addCnSufffix":".",
    "addUpnPrefix":"",
    "addUpnSufffix":".offline"
    },
    { "credentialType":"Authentication",
    "credentialDeployment":"DerivID-Container",
    "issuingCA":"ABCCO",
    "addToAD": "T",
    "aDDomain":"abc.com"
    },
    { "credentialType":"Offline",
    "credentialDeployment":"DerivID-Container",
    "issuingCA":"ABCCO",
    "addToAD": "T",
    "aDDomain":"abc.com"
    },
    {
        "credentialType":"Email",
        "credentialDeployment":"DerivID-Container",
        "issuingCA":"ABCCO",
        "addToAD": "T",
        "aDDomain":"abc.com",
        "addCnPrefix":"",
        "addCnSufffix":"",
        "addUpnPrefix":"",
        "addUpnSufffix":""
    },
    {
        "credentialType":"Tunnel",
        "credentialDeployment":"DerivID-Container",
        "issuingCA":"ABCCO",
        "addToAD": "T",
        "aDDomain":"abc.com",
        "addCnPrefix":"",
        "addCnSufffix":"",
        "addUpnPrefix":"",
        "addUpnSufffix":""
    }
  ]
}
</DerivIDCustomConfig>
```

9. Application 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. Route1 Support

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