# VMware PIV-D Manager Deployment Guide

AirWatch v9.3

**Have documentation feedback?** Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

# Table of Contents

# Chapter 1:
## Overview

# Introduction to VMware PIV-D Manager

## Derived Credentials

A Derived Credential is a client certificate generated on a mobile device (or issued) after an end user proves their identity by using their existing smart card (CAC or PIV) during an enrollment process.

Derived Credentials provides government agencies and contractors with a solution for replacing Smart Card Authentication on mobile devices to meet high security requirements in the government sector. Both the Department of Defense (DoD) and all Federal civilian agencies must use smart cards for physical and network access. It is easy to integrate Smart cards with laptops and desktops because laptops have built-in smart card readers, and desktops use USB-based smart card readers. Also, desktops and laptops support smart cards at the operating system level so any application that runs on the operating system use the smart card. With the vast use of mobile devices as the primary method of access to internal resources, federally controlled information systems and applications changed how authentication is done.

To meet this need, NIST updated FIPS 201 standards to include "Guidelines for Derived Personal Identification Verification (PIV) Credentials." Instead of using the CAC or PIV Card like laptop and desktops, this new standard provides guidelines for how to generate and use an alternative token, which can be implemented and deployed directly with mobile devices. This newly derived PIV credential is called a derived credential or PIV-D.

## VMware PIV-D Manager

VMware PIV-D Manager is a mobile application that integrates with various Derived Credential solution providers enabling the use of Derived Credentials with VMware AirWatch.

## Derived Credentials Solutions Supported by VMware AirWatch

There are multiple government off the shelf (GOTS) and commercially off the shelf (COTS) providers in the market today to use for Derived Credentials. The available vendors currently supported with the PIV-D Manager app are DISA Purebred, Entrust IdentityGuard, Intercede MyID, XTec, and VMware AirWatch. Once the app is configured in the AirWatch Console, the user follows the steps for the corresponding vendor configured for their device.

# Requirements for Using VMware PIV-D Manager

Meet the following prerequisites related to the AirWatch Console and device operating system to configure the VMware PIV-D Manager application with your Derived Credentials implementation.

- AirWatch Console v9.2+

- iOS 9+ mobile device

- VMware PIV-D Manager v1.1 for iOS

# Chapter 2:
## Application Configuration

# Configure VMware PIV-D Manager for iOS in the AirWatch Console

Configuring the VMware PIV-D Manager for iOS involves adding the PIV-D Manager as a public application, determining how end-users receive it, and configuring PIV-D settings for each vendor.

1. Navigate to **Apps & Books > Applications > Native > Public** and select **Add Application**.

2. Select the desired **Platform**.

3. Select **Search App Store** from the **Source** field to find the application.

4. Enter "VMware PIV-D Manager" as the keyword in the **Name** text box to find the application in the app store.

5. Select **Next** and use **Select** to pick the application from the app store result page. The **Edit Application** window displays.

6. Select **SDK Tab** and either select the default SDK Profile or a custom SDK Profile.

7. Select **Save & Assign** and then **Add Assignment**.

8. Add your assignment groups and enable **Send Application Configuration** and configure the following Configuration Keys and Values. Use the Add button to insert additional lines.

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| **PIVDProvider** | Integer | 1 = Entrust<br>2 = Intercede<br>3 = Purebred<br>4 = XTec<br>5 = AirWatch | This numeric value corresponds to a given provider. AirWatch sends the value to the app to pre-configure the provider for the assigned end users. |
| **PIVDInstructions** | String | The instructional text for the end user. | A brief single string instruction for the end user to prepare them for using the app to Activate/Provision/Import Derived Credentials from the provider. |
| **PIVDConfig**<br><br>9. | Array | 0 = Off<br>1 = On (Default) | PIV-D Manager prompts the end user for an App Token from AW SSP before letting them proceed with fetching an SDK Profile and certificate. This only works when the PIVDProvide configuration key value is 5 (AirWatch). |

10. (Optional) Deploy VMware PIV-D Manager as a managed application automatically. .

# Configure VMware PIV-D Manager for Android in the AirWatch Console

Configuring the VMware PIV-D Manager for Android involves adding the PIV-D Manager as a public application, determining how end-users receive it, and configuring PIV-D settings for each vendor.

1. Navigate to **Apps & Books > Applications > Native > Internal**.

2. Select **Add Application** from the **Internal** tab.

3. Select **Upload > Choose File** to browse for the application file on the system.

4. Select the PIV-D Manager APK you downloaded from the Resource Portal and click **Save**.

5. Select **Continue** and configure the **Details** tab options.

6. Select **More > SDK** and choose either the Default SDK Profile or a custom SDK Profile you have setup for the PIV-D manager.

7. Select **SDK Tab** and either select the default SDK Profile or a custom SDK Profile.

8. Select **Save & Assign** and then **Add Assignment**.

9. Add your assignment groups and enable **Send Application Configuration** and configure the following Configuration Keys and Values. Use the Add button to insert additional lines.

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| **PIVDProvider** | Integer | 1 = Entrust<br>2 = Intercede<br>3 = Purebred<br>4 = XTec<br>5 = AirWatch | This numeric value corresponds to a given provider. AirWatch sends the value to the app to pre-configure the provider for the assigned end users. |
| **PIVDInstructions** | String | The instructional text for the end user. | A brief single string instruction for the end user to prepare them for using the app to Activate/Provision/Import Derived Credentials from the provider. |
| **PIVDConfig** | Array | 0 = Off<br>1 = On (Default) | PIV-D Manager prompts the end user for an App Token from AW SSP before letting them proceed with fetching an SDK Profile and certificate. This only works when the PIVDProvide configuration key value is 5 (AirWatch). |

10.

11. (Optional) Deploy VMware PIV-D Manager as a managed application automatically. .

## Configure Device Profiles for VMware PIV-D Manager Deployment

Device profiles ensure proper use of devices, protection of sensitive data, and workplace functionality. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing devices for how they are used.

Credentials profiles deploy corporate certificates for user authentication to managed devices.

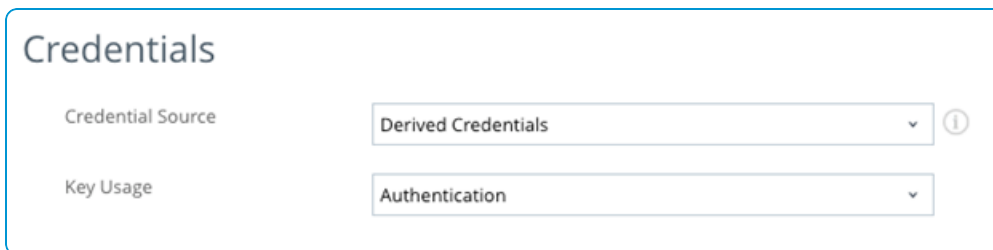Configure the following options to apply credentials:

1. Navigate to Devices > Profiles & Resources > Profiles > Add > Add Profile . Select either iOS or Android (Device or Container).

2. Configure the profile **General** settings as appropriate.

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

3.  Select the **Credentials** profile and select **Configure**.

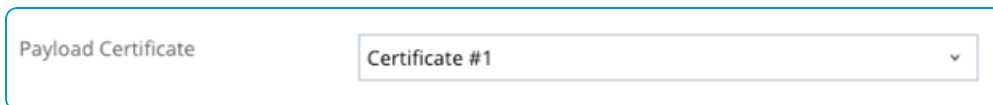4.  Set the **Credentials Source** to **Derived Credentials**.

> **Important**: If you have at least one Credential Source set to Derived Credential, you cannot add credential sources other than Derived Credentials to the Credentials profile.

5.  Select the **Key Usage** based on how the certificate is used. Choose **Authentication**, **Signing**, or **Encryption**. To add additional certificates, use the plus sign at the bottom of the profile window.

### Credentials

| | |
|---|---|
| Credential Source | Derived Credentials |
| Key Usage | Authentication |

6.  Add a Wi-Fi, VPN, Email, or other payload with which you want to associate the Derived Credential. Select the appropriate certificate just like with other credential sources.

| | |
|---|---|
| Payload Certificate | Certificate #1 |

If you are configuring multiple payloads, create additional profiles instead of one profile containing multiple payloads and multiple Derived Credentials.

7.  Select **Save and Publish**. The profile displays as pending in the Profiles List View.

At this point, end users will install and configure the VMware PIV-D Manager on their iOS device and the device profile are pushed down and installed on the managed iOS device. For more information, see Application Management on page 9

# Chapter 3:
## Application Management

# VMware AirWatch PIV-D Manager Overview

The VMware PIV-D Manager can be pushed to devices as a managed app or users can download it from the app catalog. The app can be pre-configured to immediately show a specific PIV-D Provider and custom instructions by setting the appropriate Key Value Pairs. For more information on configuring the PIVDProvider settings, see Configure VMware PIV-D Manager for iOS in the AirWatch Console on page 6.

If no Key Value Pair (KVP) is set for the PIVDProvider, then the end user will see the following screen once the app is launched.
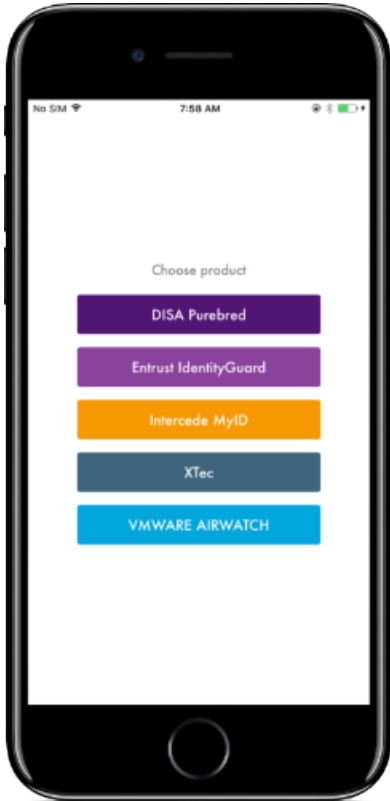


The available vendors currently supported with the VMware PIV-D Manager are DISA Purebred, Entrust IdentityGuard, Intercede MyID, XTec, and VMware AirWatch.

# Install VMware PIV-D Manager

After you configure and publish device profiles with Derived Credentials as the Credential Source, end users install and configure the VMware PIV-D app on their iOS or Android devices. This ensures the device profiles are pushed and installed on the managed devices.

End users follow these steps on their iOS device to install the VMware PIV-D Manager.

To install application, do the following:

1. Enroll the device using the AirWatch Agent.

2. After the device is enrolled, tap the prompt to install the VMware PIV-D Manager. You can also download the app through the app catalog.

3. Follow the instructions provided by your administrator which requires you to smart card authenticate to the PIV-D

provider Self-Service Portal (SSP).

If you did not pre-select a Derived Credentials Provider from the AirWatch Console, your end users must select the provider and follow the steps for the selected provider:

- DISA Purebred - For steps, see Configure DISA Purebred on page 11.

- Entrust IdentityGuard - For steps, see Configure Entrust IdentityGuard on page 13.

- Intercede MyID - For steps, see Configure Intercede MyID on page 13

- XTec - For steps, see Configure XTec on page 14

- VMware AirWatch - For steps, see Configure VMware AirWatch on page 15

4. After authentication from the PIV-D provider SSP, complete the enrollment process in the VMware PIV-D Manager.

Once enrollment is complete, the application shows the Derived Credentials and trigger the installation of any device profiles that use a Derived Credential. Anytime a device profile is updated or a new one is created, the user needs to launch the VMware PIV-D Manager for the new profile to get pushed down to the mobile device.

Navigate to **Settings > General> Device Management** to view the profile and the certificates on the device as a managed profile on the device.

## Configure DISA Purebred

Purebred is a Derived Credentials solution developed by the Department of Defense (DoD) Public Key Enablement (PKE) office. You can learn more about Purebred by going to http://iase.disa.mil/pki-pke/Pages/purebred.aspx.

To configure the VMware PIV-D Manager using Disa Purebred, complete the following:

1. Complete the Derived Credentials enrollment through the Purebred Self Service Portal (SSP).

2. Tap the VMware PIV-D Manager from the device and tap **DISA Purebred**.

3. Tap **Add certificate > Purebred Key Chain**.
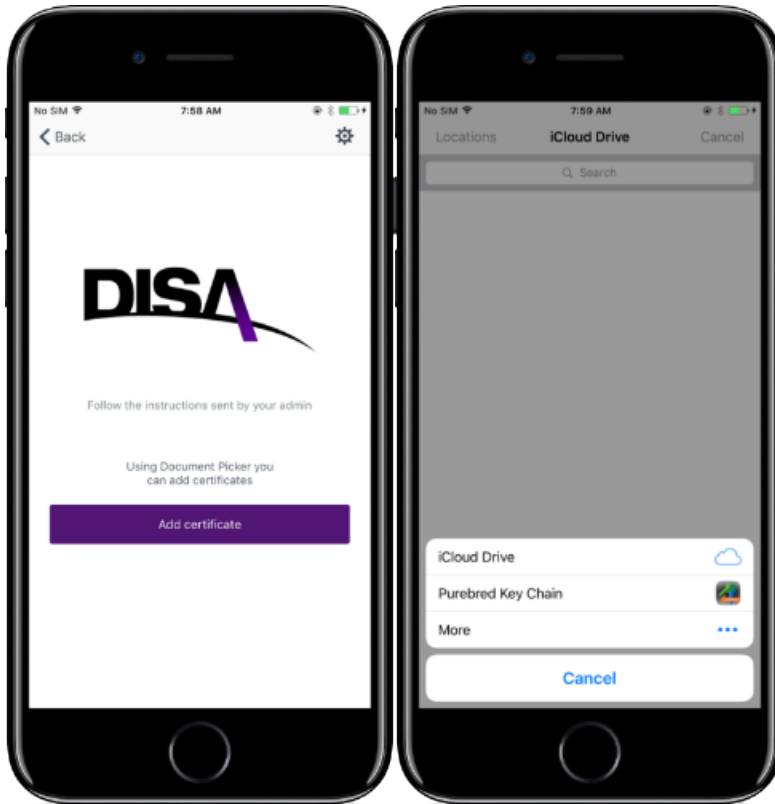
4. Select your Authentication Certificate and tap **Import Key**. Repeat to import Signing and Encryption Certificates.

5. Once you import all three, view the certificates from the **Certificate** list view.
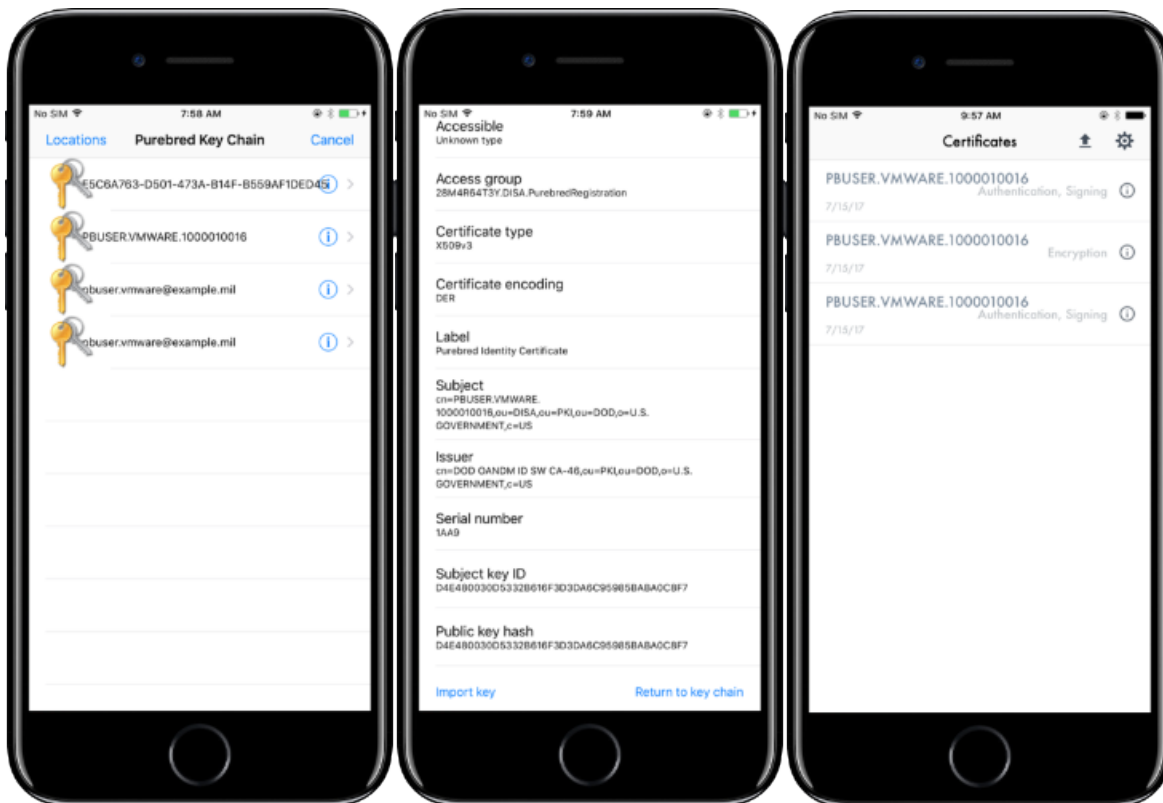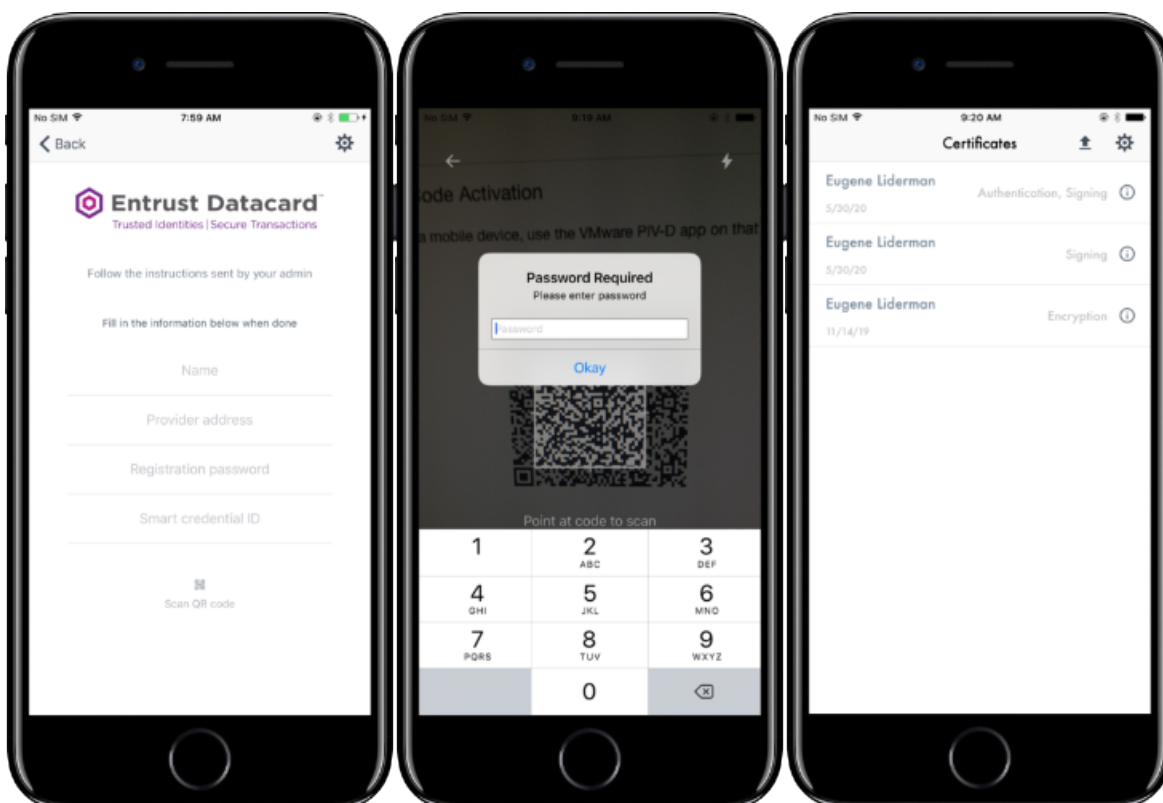
## Configure Entrust IdentityGuard

Entrust IdentityGuard is a commercially off the shelf (COTS) Derived Credentials solution. You can learn more about it by going to https://www.entrust.com/products/entrust-identityguard/.

To configure the VMware PIV-D Manager using Entrust IdentityGuard, complete the following:

1. Start the enrollment process by logging in to the Entrust IdentityGuard Self-Service Portal from your laptop/desktop computer with your existing smart card.

2. Once logged in, select on " I'd like to enroll for a derived mobile smart credential".

3. Select "I've successfully downloaded and installed the Entrust IdentityGuard Mobile Smart Credential application" and click Next.

4. Enter a name under Identity Name, then select VMware PIV-D under the Derived Mobile Smart Credential App field.

5. Click OK A QR Code and a one-time password displays.

6. Launch the VMware PIV-D Application on your iOS Device and tap Scan QR code and then enter the one-time password.

7. Once the process is complete, you will be taken to the Certificate list view



## Configure Intercede MyID

Intercede MyID is a commercially off the shelf (COTS) Derived Credentials solution. You can learn more about it by going to https://www.intercede.com/myid.

**vm**ware airwatch

To configure the VMware PIV-D Manager using Intercede MyID, complete the following:

1.  Start the enrollment process by logging in to the Intercede MyID Self-Service Portal from your laptop/desktop computer with your existing smart card

2.  Once logged in, select **Request My ID**.

3.  Select the appropriate profile and click on **Continue**.

4.  Select **QR Code**.

5.  Launch the VMware PIV-D Application on your iOS Device and tap **Scan QR code**.

6.  Once the process is complete, you will be taken to the **Certificate** list view.

## Configure XTec

Xtec in partnership with the Department of Homeland Security developed a Derived Credentials solution for use within DHS. You can learn more about it by going to http://www.xtec.com/.

To configure the VMware PIV-D Manager using Xtec, complete the following:

1.  Start the enrollment process by logging in to the XTec AuthentX Self-Service Portal from your laptop/desktop computer with your existing smart card.

2.  Once you have completed step one, return to the VMware PIV-D Manager application on your iOS device and tap **Next**.

3. Once the process is complete, you will be taken to the **Certificate** list view.
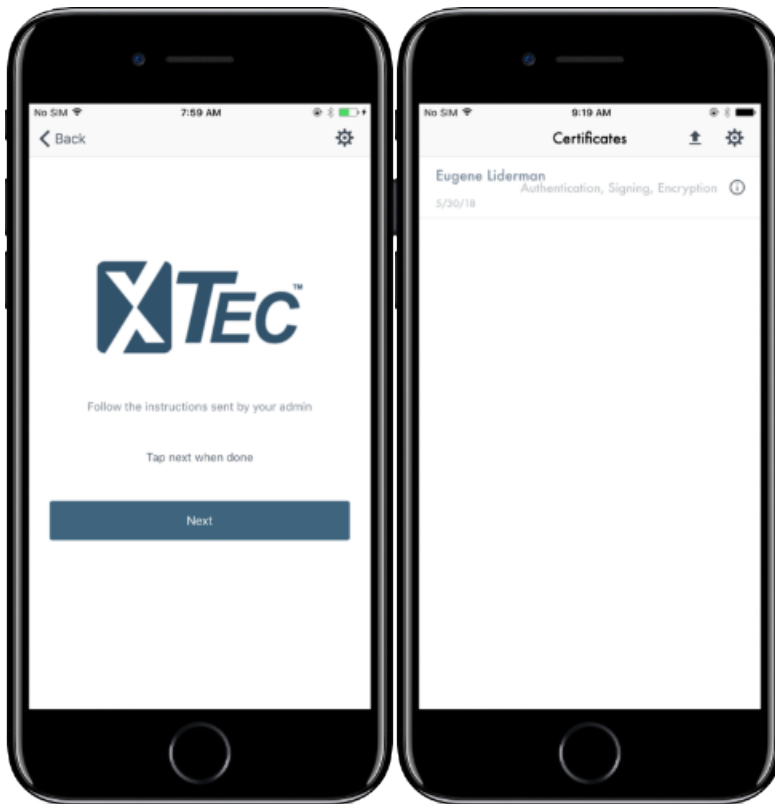


## Configure VMware AirWatch

VMware AirWatch allows customers to use their existing Certificate Authority configuration within AirWatch to issue Derived Credentials in compliance with NIST SP 800-157.

To configure the VMware PIV-D Manager using VMware Airwatch, complete the following:

1. On your iOS device tap the VMware PIV-D Manager application and tap **Next**



2. If you are prompted for a One-time token, login in to the AirWatch Self-Service Portal from your laptop/desktop computer with your existing smart card.

3. Once logged in, select the option to generate an app token.

4. Go back to the VMware PIV-D Manager application on your iOS device, enter your App Token and tap on **Activate.**

5. Once the process is complete, you will be taken to the **Certificate** list view.
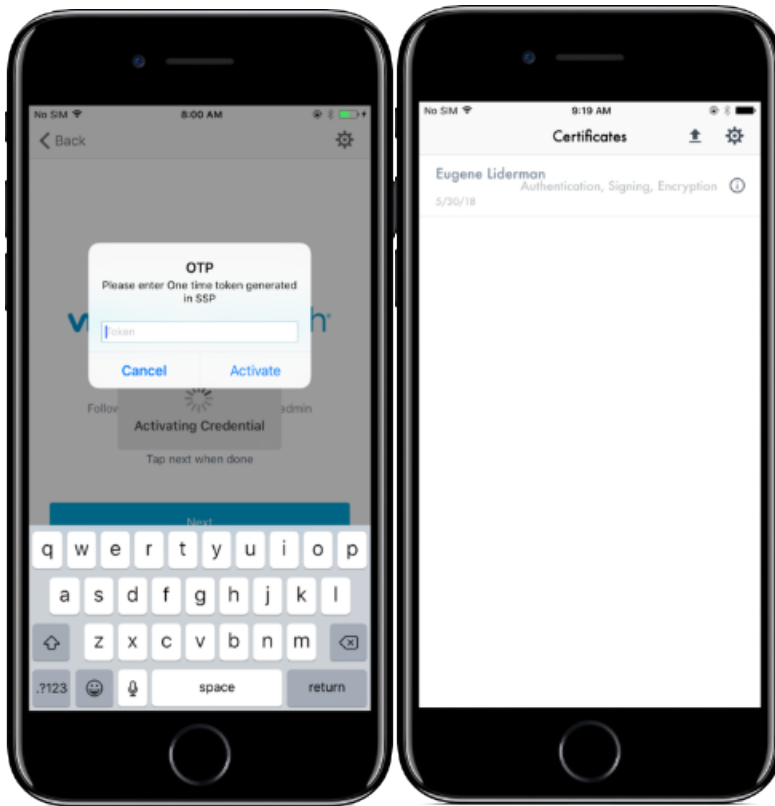
# Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.