Using VMware PIV-D Manager

VMware Workspace ONE UEM
VMware Workspace ONE PIV-D Manager

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction to VMware PIV-D Manager 1

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 Workspace ONE UEM.

Derived Credentials Solutions Supported by Workspace ONE UEM

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 Workspace ONE UEM. Once the app is configured in the Workspace ONE™ UEM 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 Workspace ONE UEM console and device operating system to configure the VMware PIV-D Manager application with your Derived Credentials implementation.

- Workspace ONE UEM console v9.2
- iOS 9+ devices
- Android 6.0+ (7.0+ for Samsung KNOX) devices
- VMware PIV-D Manager v1.4 for iOS and v.1.3 for Android

How to Configure VMware PIV-D Manager in the Workspace ONE UEM Console

2

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

Procedure

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

The **Managed By** field displays the organization group where the app is uploaded.

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 (Optional) Select the **Assignment** tab and scroll to the section labeled **Application Configuration**.

7 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 2 = Intercede 3 = Purebred 4 = XTec 5 = Workspace ONE UEM	This numeric value corresponds to a given provider. Workspace ONE UEM 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		0 = Off 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 (Workspace ONE UEM).

Configuration Key	Value Type	Configuration Value	Description
EnableEntrustBluetoothLogin	Boolean	true = on false = off	

Table 2-1. iOS App Config key-value pairs

Key	Value Type	Description
PinLengthMinimum	Integer	The minimum character length for the pin protecting the Certificate Store.
PinUppercaseMinimum	Integer	The minimum number of uppercase characters for the pin protecting the Certificate Store.
PinLowercaseMinimum	Integer	The minimum number of lowercase characters for the pin protecting the Certificate Store.
PinSpecialCharMinimum	Integer	The minimum number of special characters for the pin protecting the Certificate Store. Supported characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
PinNumbersMinimum	Integer	The minimum number of number characters for the pin protecting the Certificate Store.
PinDisallowDuplicate	Boolean	Setting this to "True" checks for duplicate characters next to each other in the pin protecting the Certificate Store.
PinDisallowSequential	Boolean	Setting this to "True" checks for a sequence of characters going up or down in value (123, 321, abc) in the pin protecting the Certificate Store.

Note If Entrust Bluetooth Login is enabled, the pin policy defined in the Entrust system will be honored instead of what's defined here.

8 Deploy VMware PIV-D Manager as a managed application.

This chapter includes the following topics:

Configure VMware PIV-D Manager for Android in the Workspace ONE UEM 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.

Procedure

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

2 Select **Add Application**.

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 2 = Intercede 3 = Purebred 4 = XTec 5 = AirWatch	This numeric value corresponds to a given provider. Workspace ONE UEM 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		0 = Off 1 = On (Default)	PIV-D Manager prompts the end user for an App Token from SSP before letting them proceed with fetching an SDK Profile and certificate. This only works when the PIVDProvide configuration key value is 5 (Workspace ONE UEM).

10 Deploy VMware PIV-D Manager as a managed application.

Configure Device Profiles on iOS 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.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Apple iOS**.

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

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.

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.

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.

What to do next

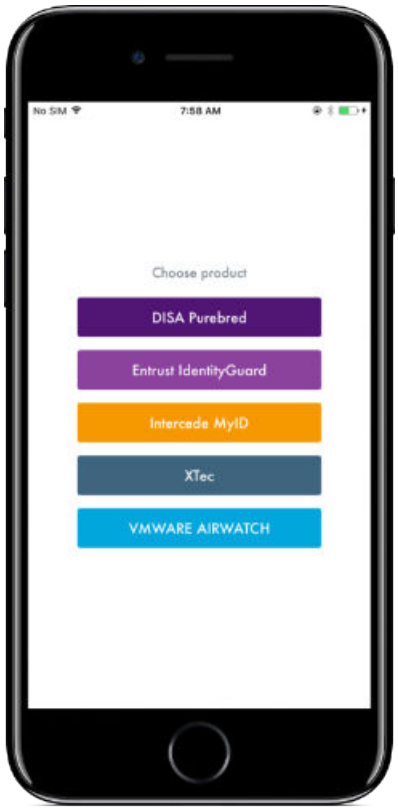
At this point, end users will install and configure the VMware PIV-D Manager on their iOS device and the device profile are pushed down and installed on the managed iOS device. For more information, see Chapter 3 Workspace ONE UEM PIV-D Manager Installation and Configuration.

Workspace ONE UEM PIV-D Manager Installation and Configuration

3

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 Chapter 2 How to Configure VMware PIV-D Manager in the Workspace ONE UEM Console.

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 Workspace ONE UEM.

This chapter includes the following topics:

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 device. This ensures the device profile are pushed and installed on the managed iOS device.

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

Procedure

1. Enroll the device using the Workspace ONE Intelligent Hub.
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 Workspace ONE UEM console, your end users must select the provider and follow the steps for the selected provider:

   - DISA Purebred - For steps, see Configure DISA Purebred.
   - Entrust IdentityGuard - For steps, see Configure Entrust IdentityGuard.
   - Intercede MyID - For steps, see Configure Intercede MyID.
   - XTec - For steps, see Configure XTec.
   - Workspace ONE UEM - For steps, see Configure Workspace ONE UEM.
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.

What to do next

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

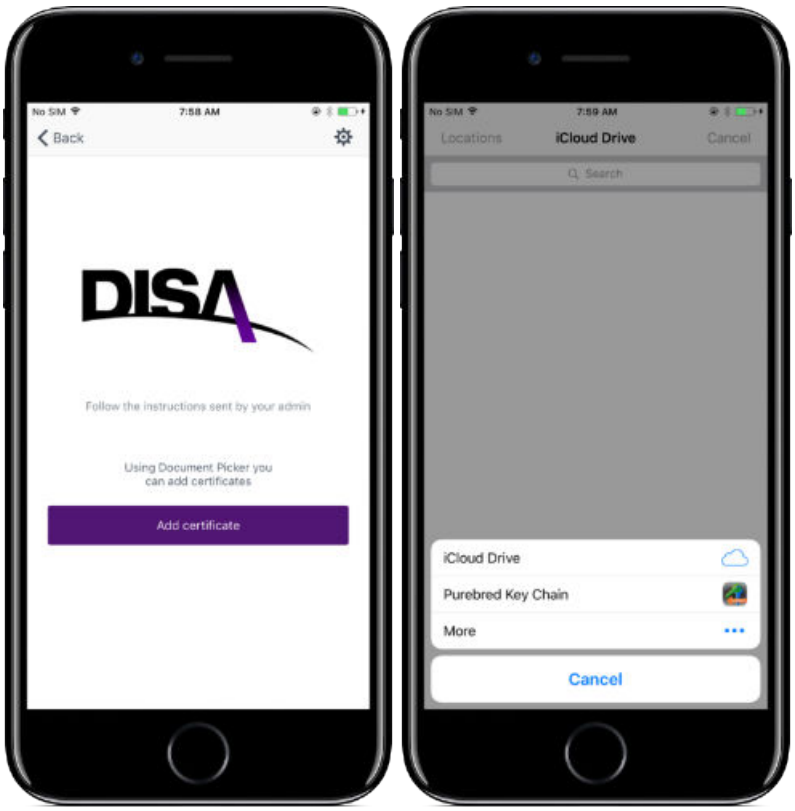
Purebred is a Derived Credentials solution developed by the Department of Defense (DoD) Public Key Enablement (PKE) office. You can learn more about Purebred by going to http://iase.disa.mil/pki-pke/Pages/purebred.aspx.

Procedure

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

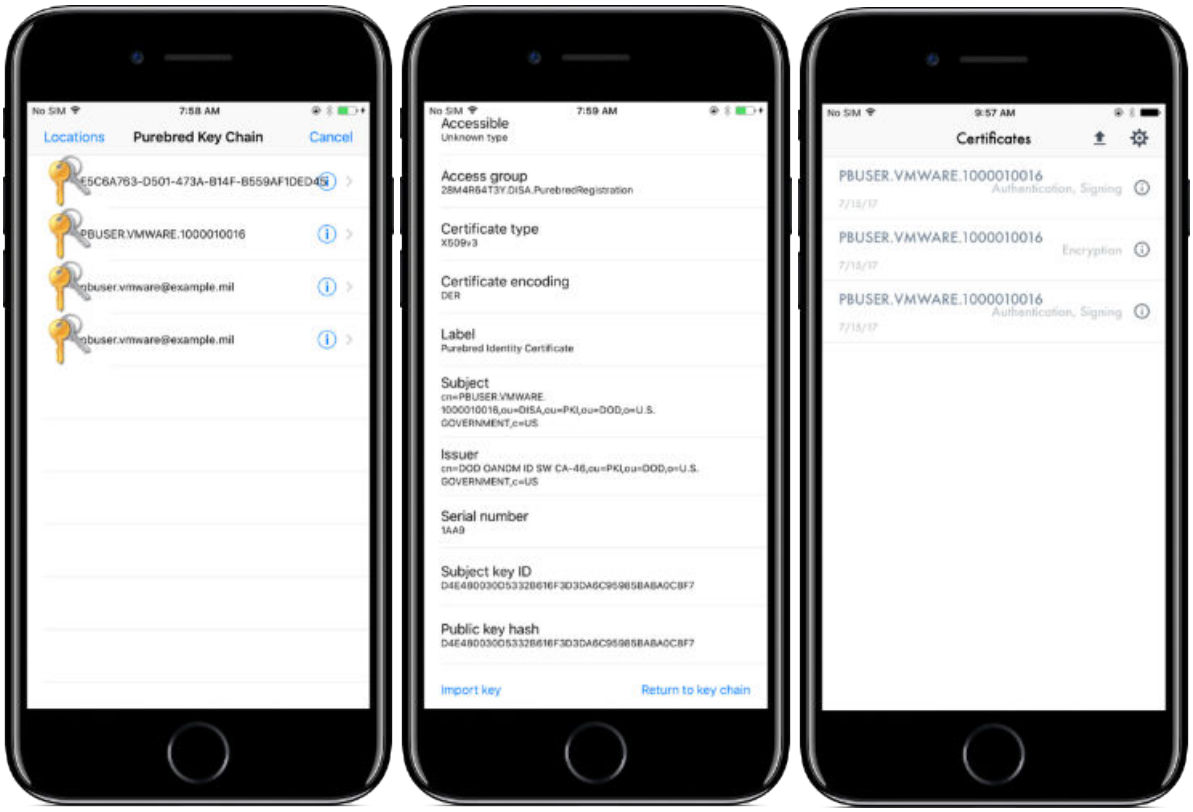
2 Tap the VMware PIV-D Manager from the device and tap **DISA Purebred**.

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/.

Procedure

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 **" 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.

Once the process is complete, you are taken to the **Certificate** list view.

Configure Intercede MyID

Configure the VMware PIV-D Manager using 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.

Procedure

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**.

What to do next

Once the process is complete, You are 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/.

Procedure

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. Return to the VMware PIV-D Manager application on your iOS device and tap **Next**.

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

Configure Workspace ONE UEM

Workspace ONE UEM allows customers to use their existing Certificate Authority configuration to issue Derived Credentials in compliance with NIST SP 800-157.

Procedure

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, log in in to the **Workspace ONE UEM 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**.

Once the process is complete, you are taken to the **Certificate** list view.

Configure Bluetooth Login

The Bluetooth login feature allows users to use the PIV-D app as a virtual smartcard to log in to Windows or Mac desktops and websites that would normally require a physical smartcard for authentication.

Prerequisites

The Bluetooth Login configuration is only available when the following conditions are met:

1 The PIV-D app is enrolled using Entrust as the derived credential provider

2 The admin has set the **EnableEntrustBluetoothLogin** configuration key with a value type of **Boolean** to **true** in the Workspace ONE UEM console when the PIV-D application is assigned.

3 If a user is already using PIV-D with Entrust-activated derived credentials, iOS requires the user to re-activate their credentials before they can use bluetooth login. If the user does not re-activate their credentials, the bluetooth settings will not appear in the app UI.

   a Users can re-issue a derived credential in the PIV-D app by navigating to**Settings > Account Re-Issue > Derived Credential**

Procedure

1 Enable Bluetooth login on your mobile device.

   a Under **Device Settings**, enable Bluetooth.

   b Launch the PIV-D app and tap the settings gear icon.

   c Enable **Bluetooth Login**.

2 Pair PIV-D with a Desktop.

   a Once Bluetooth login is enabled in the PIV-D settings, the PIV-D app home page will have an option for bluetooth login. Press the bluetooth login option to begin scanning for nearby devices to pair with or connect to.

   b Select the desktop to connect to.

   c Once the connection is made, the desktop will prompt for the PIV-D pin if applicable (this is the pin created at the time of derived credential enrollment in PIV-D) and request selection of the certificate to use for authentication.

3 Log in to a desktop computer or website using PIV-D.

   a Once Bluetooth login is enabled in the PIV-D settings, the PIV-D app's home page will have an option for bluetooth login. Press the bluetooth login option to begin scanning for nearby devices to pair with or connect to.

   b Select the desktop to connect to.

   c Once the connection is made, the desktop will prompt for the PIV-D pin if applicable (this is the pin created at the time of derived credential enrollment in PIV-D).

d Upon successful connection and pin entry (if applicable), the user will be logged in to the desktop.

e Additionally, if the user browses to a website expecting smart card auth on the desktop, the same PIV-D connection can be used to authenticate to the website as well.

4 Enable a device to auto-connect by selecting the autoconnect option next to the device name.

Attempting to auto-connect to another device will cause the existing auto-connect to be disabled. Once auto-connect is enabled, the PIV-D application automatically connects to desktops when the device enters Bluetooth range.