# Workspace ONE 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/

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

# Contents

# Workspace ONE PIV-D Manager and Supported Derived Credentials

1

VMware Workspace ONE® PIV-D Manager is a mobile application that integrates with various derived credential providers for use with devices managed by Workspace ONE UEM powered by AirWatch. Find out what a derived credential is and which solutions Workspace ONE PIV-D Manager supports.

## What are 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 provide 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. This standard does not use the CAC or PIV Card like laptop and desktops. It provides guidelines for how to generate and use an alternative token. You can then implement and deploy the alternative token directly to mobile devices. This newly derived PIV credential is called a derived credential or PIV-D.

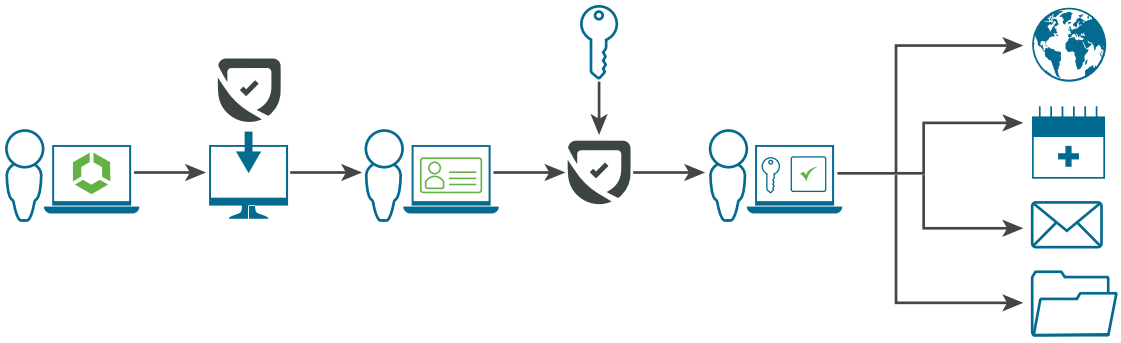
## Supported Derived Credentials Solutions

Workspace ONE PIV-D Manager supports the listed PIV-D providers.

- DISA Purebred
- Entrust Identity Enterprise
- Intercede MyID

- XTec
- Workspace ONE UEM

## How does Workspace ONE PIV-D Manager work with DC Providers?



Workspace ONE PIV-D Manager interacts with derived credential (DC) providers and Workspace ONE UEM components to make mobile derived credentials available for use in profiles and productivity apps.

1. Users enroll with Workspace ONE UEM through the Workspace ONE Intelligent Hub on devices.
2. Users get the Workspace ONE PIV-D Manager app from the Workspace ONE Intelligent Hub and install it on devices.
3. Users authenticate with a Smartcard to a DC provider. The DC provider issues mobile derived credentials to users.
4. Certificates for mobile derived credentials get added to the Workspace ONE PIV-D Manager app on devices. This process varies depending on the DC provider.
   - Android - The system encrypts the certificates and stores them in the Workspace ONE PIV-D Manager app.
   - iOS - The system encrypts the certificates and stores them in the iOS Keychain.
5. Users can access apps and services on the device using the mobile derived credential.

This chapter includes the following topics:

# Requirements for Using Workspace ONE PIV-D Manager

Meet the prerequisites for the Workspace ONE UEM console and device operating systems to deploy and use theWorkspace ONE PIV-D Manager app with your derived credentials implementation.

## Minimum Software Requirements

- Workspace ONE UEM console v9.7 or later
- Workspace ONE PIV-D Manager
  - iOS - v1.5.1
  - Android - v1.5

## End-User Device Operating System Minimums

- iOS 11 or later
- Android
  - Android (Enterprise) - 6.0 or later
  - Android (Legacy) - 6.0 or later
  - Android (for Samsung KNOX) - 7.0 or later

## Required Tasks

Perform multiple tasks to use Workspace ONE PIV-D Manager to integrate your derived credential solution with Workspace ONE UEM.

1 Admins add, assign, and publish the Workspace ONE PIV-D Manager app to devices. The app receives the derived credential certificates on the device from the Workspace ONE UEM console.

  When you assign the Workspace ONE PIV-D Manager app, you can enter app config values to pre-configured and show a specific PIV-D provider and to show custom instructions.

2 Admins add, assign, and deploy a device profile with a credentials payload. The device profile gets the certificates from the Workspace ONE PIV-D Manager app so that the device uses the derived credential solution for authentication, signing, and encryption as configured.

3 Device users install and configure Workspace ONE PIV-D Manager for the desired PIV-D provider. The amount of manual configuration depends on the use of app config parameters.

# PIV-D Feature Matrix

The VMware Workspace ONE PIV-D Manager frees you from carrying a smart card reader to access your PIV or CAC credentials. VMware Workspace ONE PIV-D Manager integrates with various derived credential providers or a YubiKey accessory. Learn more about the supported

configurations for Workspace ONE PIV-D Manager when using third-party providers and the differences between Android, iOS, iPadOS, and Samsung Knox.

## PIV-D Feature Matrix

The PIV-D Feature Matrix shows the availability of certificate-based authentication (CBA) and S/MIME based on the credential source and the mobile device type. The credential source is one of the following:

- **Issuance** - Credentials are issued to the PIV-D Manager app and then stored securely on the device. The following are supported issuance sources:
  - DISA Purebred
  - Entrust
  - Intercede
  - Workspace ONE UEM
  - XTec
- **Accessory** - Credentials are stored on an accessory connected through NFC or by being plugged in. The following is the only supported accessory:
  - YubiKey by Yubico

**Feature/Device Availability**

In some instances, there are dependencies for feature availability on certain devices. The following shows when a feature is available on a device.

- CTK - Availability depends on the Apple Persistent Device Token extension, also known as CryptoTokenKit (CTK) provider.
- DI - Availability depends on the direct installation of certificates to the Android device key store by the PIV-D Manager app.
- MDM - Availability depends on the mobile device management (MDM) capability of the operating system.
- CTK/MDM - Availability depends on either CTK provider or MDM.
- * - Availabilty on a device.

**Credential Source: Issuance**

| Feature | Registered iOS or iPadOS | Registered Android | Managed iOS or iPadOS | Managed Android | Managed Knox |
|---|---|---|---|---|---|
| Workspace ONE Boxer email CBA | * | * | * | * | * |
| Workspace ONE Boxer email S/MIME | * | * | * | * | * |

| Feature | Registered iOS or iPadOS | Registered Android | Managed iOS or iPadOS | Managed Android | Managed Knox |
|---|---|---|---|---|---|
| Microsoft Outlook CBA | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Microsoft Outlook S/MIME | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Native mail client CBA | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Native mail client S/MIME | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Workspace ONE Web website CBA | * | * | * | * | * |
| Native browser website CBA | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Wi-Fi connection CBA | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Third party VPN CBA | CTK* | DI* | CTK/MDM* | MDM* | MDM* |
| Digitally sign PDFs | * | * | * | * | * |

## Credential Source: Accessory

| Feature | Registered iOS or iPadOS | Registered Android | Managed iOS or iPadOS | Managed Android | Managed Knox |
|---|---|---|---|---|---|
| Workspace ONE Boxer email CBA | CTK* | | CTK* | | |
| Workspace ONE Boxer email S/MIME | CTK* | | CTK* | | |
| Microsoft Outlook CBA | CTK* | | CTK* | | |
| Microsoft Outlook S/MIME | CTK* | | CTK* | | |
| Native mail client CBA | CTK* | | CTK* | | |
| Native mail client S/MIME | CTK* | | CTK* | | |
| Workspace ONE Web website CBA | CTK* | | CTK* | | |
| Native browser website CBA | CTK* | | CTK* | | |

| Feature | Registered iOS or iPadOS | Registered Android | Managed iOS or iPadOS | Managed Android | Managed Knox |
|---|---|---|---|---|---|
| Wi-Fi connection CBA | CTK* | | CTK* | | |
| Third party VPN CBA | CTK* | | CTK* | | |
| Digitally sign PDFs | * | * | * | * | * |

# Send Derived Credentials from the Console to iOS Devices

2

Add and publish the Workspace ONE PIV-D Manager to devices as a public app. The app receives the derived credential certificates from the console so that the device can use them.

For details on how to use Workspace ONE PIV-D Manager to sign PDFs with derived credentials, see Sign PDFs with Workspace ONE PIV-D Manager for iOS.

Procedure

1 Navigate to **Resources > Apps > Native > Public** and select **Add Application**.

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

2 Select the desired platform.

3 To find the application, select Search App Store from the Source field.

4 To find the application in the app store, enter "VMware PIV-D Manager" as the keyword in the Name text box.

5 **Select** the application from the app store result page.

   The **Add Application** window displays. It is not necessary to add further information.

6 To move to the deployment section, select **Save & Assign**.

   You assign the app to devices and add optional app config parameters in the deployment section.

7 Select the **Assignment** tab and **Add Assignement**.

8 Enter a group that includes the devices that use your derived credential solution for **Select Assignment Groups**.

9 Optional: Under the Application Configuration tab, enable **Application Configuration** and enter the listed **Configuration Key** and **Value** pairs. To insert lines, click the **Add** button.

   App config values parameters some manual configurations for the user on the device but they are not required for Workspace ONE PIV-D Manager to work.

Table 2-1. Common App Config Key-Value Pairs

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| `CertificateExpiryWarning` | String | Your custom warning message for when a certificate is about to expire. | The default warning message is displayed there is no custom warning message. |
| `CertificateExpiryWarningPeriod` | Integer | Enable = Any numerical value greater than 0<br>Disable = 0 | The default value is 30 days when nothing is manually set. |
| `ConnectorAppName` | String | | Select an application name that can be used by a back end connector to Workspace ONE UEM.<br>To select a lookup value from the list or enter fixed text such as "VMware PIV-D", click **+**.<br>This configuration key is only supported by the Intercede provider. |
| `ConnectorDeviceIdentifier` | String | | Select a device identifier that can be used by a back end connector to Workspace ONE UEM.<br>To select a lookup value, such as {DeviceUid}, from the list, click **+**.<br>This configuration key is only supported by Entrust and Intercede providers. |
| `EnableEntrustBluetoothLogin` | Boolean | True = On<br>False = Off | When you enable this value, the PIN policy defined in the Entrust system is honored instead of the key defined here. |
| `EnableManualCertificateImport` | Boolean | True = On<br>False = Off | Enables integrations with XTec to import the certificates from web browser downloads using the download portal website for customers. |
| `EnablePDFSigning` | Boolean | True = On<br>False = Off | Enable apps like Mail, Workspace ONE Boxer, or Adobe Acrobat Reader, to sign a PDF document using the derived credential in Workspace ONE PIV-D Manager. |

Table 2-1. Common App Config Key-Value Pairs (continued)

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

Table 2-1. Common App Config Key-Value Pairs (continued)

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| `PIVDConfig` | Array | 0 = Off<br>1 = On | Workspace ONE PIV-D Manager prompts the end user for an app token from the Self Service Portal before letting them proceed with fetching an SDK profile and certificate. This feature only works when the `PIVDProvider` configuration key value is 5 (Workspace ONE UEM). |
| `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. |
| `PIVDPromptForPIN` | Boolean | True = On<br>False = Off | Workspace ONE PIV-D Manager prompts the end user for the PIN even if you enable SSO. |
| `PIVDProvider` | Integer | 1 = Entrust<br>2 = Intercede<br>3 = Purebred<br>4 = XTec<br>5 = Workspace ONE UEM<br>6 = YubiKey | 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. |

Table 2-2. iOS App Config Key-Value Pairs

| Key | Value Type | Description |
|---|---|---|
| `PersistentTokenExtensionAllowed` | Boolean | Settings to **`True`** enables the Persistent token extension and PIV-D Manager acts as a CTK Provider, by default the Persistent Token Extension is not allowed. |
| `PersistentTokenExtensionTimeOutSeconds` | Integer | Checking to maintain an up-to-date policy setting in case the enterprise changes policy. The default is 86400 (24 hours, in seconds). |
| `UserPresenceProtection` | Boolean | The default setting is **`True`**.<br>Setting to **`False`** does not require the user to authenticate using the Device Passcode or Biometrics (Touch ID / Face ID) to access the CTK tokens.<br>All providers support this configuration key except YubiKey. |

10 Select **Add** to assign the app to the devices in the assignment group and then save and publish Workspace ONE PIV-D Manager as a managed application.

# Use Profiles to Control How iOS Devices use Derived Credentials Certificates

Deploy a device profile with a credentials payload to iOS devices. The profile gets the certificates from Workspace ONE PIV-D Manager app so the device can use the certificates to securely access resources.

Procedure

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

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

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** payload.

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**.

#### Results

The profile displays as pending in the **Profiles List View**.

#### What to do next

At this point, end users install and configure Workspace ONE PIV-D Manager on their iOS device. The console pushes down and installs the device profile on the managed iOS device. For more information, see Chapter 4 Configure Workspace ONE PIV-D Manager on Devices.

# SSO and Keychain PIN Use for iOS

Control the use of the keychain PIN when users log in to apps with derived credentials by configuring Single Sign-On (SSO). Then, deploy the SSO configuration to Workspace ONE PIV-D Manager for iOS.

**Note** You deploy this SDK profile at the app level. It is different from the **Credentials** profile that you use to set devices to use derived credentials in the console.

## SSO Configurations Control PIN Use

If you do not use the default SDK profile at all, users must set a PIN with a six character minimum length.

If you deploy Workspace ONE PIV-D Manager with **Single Sign-On > Enabled**, the Workspace ONE PIV-D Manager app does not prompt users for their PINs when using derived credentials.

If you set the default SDK profile as **Single Sign-On > Disabled**, the Workspace ONE PIV-D Manager app prompts users for their PINs when using derived credentials.

## Force PIN Use in Application Configuration

If you configured your default SDK profile as **Single Sign-On > Enabled**, you can still require PIN use. In Application Configuration, select **`True`** as the Configuration Value for `PIVDPromptForPIN`.

## Configure Complexity with KVPs

To configure the complexity of the PIN, use several available KVPs. For a list of available KVPs and how to configure them, access Chapter 2 Send Derived Credentials from the Console to iOS Devices.

## How to Deploy SSO

Configure the default SDK profile with the PIN behavior you want and then assign the default SDK profile to Workspace ONE PIV-D Manager.

1 Configure SSO in the default SDK profile.

   a In the Workspace ONE UEM console, go to the applicable organization group where your Workspace ONE PIV-D Manager app resides.

   b Go to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies > Single Sign-On**.

   c Select **Enabled** or **Disabled** depending on the desired experience and save the default SDK profile.

   d Optional: To force PIN use, in Application Configuration for PIV-D Manager, select **`True`** as the Configuration Value for `PIVDPromptForPIN`.

2 Assign the SDK profile to Workspace ONE PIV-D Manager.

   a Go to **Resources > Apps > Native > Public** and edit the Workspace ONE PIV-D Manager app.

   b Select **SDK** and select **iOS Default Settings @ Global** for **SDK Profile**.

   c Save your changes.

# PIV-D Manager and YubiKey for iOS

VMware Workspace ONE® PIV-D Manager works with YubiKey. Use the PIV-D Manager mobile app to authenticate end users with YubiKey credentials and sign PDF documents on a mobile device with credentials from a YubiKey accessory.

## Prerequisites

Before you begin, you need the following:

- An enrolled device

  Enroll the Workspace ONE Intelligent Hub and PIV-D Manager apps in the usual way, or by following instructions from your enterprise administrator.

- An accessory with installed credentials

  Your enterprise administrator might issue you with an accessory with an installed credential, or provide you with enrollment instructions. Otherwise, you can install an electronic certificate yourself.

  To install a certificate yourself, you need the following:

  - Suitable management software that can downloaded from the Yubico website.

- Accessory management keys. YubiKey accessories come configured with default keys. Use those keys unless the accessory has been reconfigured.
- Electronic certificate. The certificate must have the key usages: Digital Signature and Non-Repudiation.

To verify that the certificate is suitable for PDF signing, use the PIV-D Manager app.

You can register your YubiKey accessory for use with the PIV-D Manager app on your device by following these instructions.

The Persistent Device Token Extension supports YubiKey. For information, see Persistent Device Token Extension.

## Register Your YubiKey Accessory

Complete these steps to authenticate credentials and electronically sign PDFs on a mobile device.

1 Open the PIV-D app. Opening the app might require you to enter a passcode or authenticate another way.

2 Open the product selection screen. The first screen shown by PIV-D might be the product selection screen.

3 Select Product: YubiKey.

4 Follow the on-screen instructions for connecting the accessory, either by USB or NFC. PIV-D only accesses the public details of the certificate at this stage and you won't need to enter the accessory PIN. When the accessory has been accessed, the Certificates screen opens in the PIV-D app. The certificate from the accessory should be listed there.

**Note** Be careful not to trigger Yubico OTP (One-Time Passcode) entry. Triggering the OTP might cause the browser app to open. If the browser app opens, then return to the PIV-D app. To avoid triggering the OTP, try holding the accessory in a different way.

5 Select the certificate name and verify the attributes are as required. The Subject must show the common name (CN) that you want to appear on signed documents. The Key Usage line must show both Digital Signature and Non-Repudiation.

If any attributes are not as required, then a different certificate must be loaded on the accessory. Return to your administrator or generate and install an amended certificate of your own.

## Sign a Document With a YubiKey Accessory

Complete these steps to electronically sign a document.

1 Ensure that your YubiKey device is registered.

2 Share a signable PDF file with PIV-D.

3 Tap the sign button and confirm if prompted.

4 Follow the on-screen instructions for connecting the accessory, either by USB or NFC. PIV-D accesses the private key of the certificate at this stage and you are prompted to enter the accessory PIN.

**Note** Be careful not to trigger Yubico OTP (One-Time Passcode) entry. Triggering the OTP might cause the browser app to open. If the browser app opens, then return to the PIV-D app. To avoid triggering the OTP, try holding the accessory in a different way.

5 Ensure that the signature is entered correctly.

# Sign PDFs with Workspace ONE PIV-D Manager for iOS

You can sign PDFs with a PIN, facial recognition, or fingerprint using Workspace ONE PIV-D Manager.

Signing PDFs with Workspace ONE PIV-D Manager has some limitations.

- PIV-D records that PDFs are signed, but it does not validate the signatures.
- Workspace ONE PIV-D Manager uses a single signing certificate that can be used for multiple signatures. It does not support the use of multiple signing certificates for PDF signing.

### Prerequisites

- The PDF must have a signature element (allows digital signing).
- Your deployment must use Workspace ONE PIV-D Manager for iOS v1.5 or later.
- The corresponding certificate in Workspace ONE PIV-D Manager for iOS must have the `keyUsage` attribute for signing and non-repudiation.
- Device users need a keystore PIN. Users configure their keystore PINs when they activate and import their derived credential certificates. The keystore PIN is different from the Workspace ONE PIV-D Manager passcode.
- **Important** Users get six attempts to enter their PINs. On the sixth incorrect PIN entry, the Workspace ONE PIV-D Manager app wipes all data.
- Facial recognition or fingerprint scanning must be configured on the device to utilize biometric signing.
- Biometric Authentication for keystore also requires SSO to be ON.

Procedure

1 Admins configure the Workspace ONE PIV-D Manager app in the Workspace ONE UEM console.

   a Navigate to **Resources > Apps > Native > Public** and edit the Workspace ONE PIV-D Manager app in the view list.

   b Add the key value pair, `EnablePDFSigning` as a Boolean data type with the value of `true`.

   c (optional) Add the key value pair, `EnableBiometricAuthentication` as a Boolean data type with the value of *true* to allow for biometric signing.

   Adding this value pair gives you the option to enable biometric signing within PIV-D Application Settings.

   a Push the Workspace ONE PIV-D Manager to deploy the PDF signing feature.

2 Users copy the applicable PDF file into the Workspace ONE PIV-D Manager app for signing on their devices.

   a On their devices, users open the applicable PDF file in the app that usually renders PDFs (Workspace ONE Boxer, Mail, or Adobe Acrobat Reader).

   b Copy the PDF file from the usual app using the app's **Share** capability to Workspace ONE PIV-D Manager.

   The PDF opens in the Workspace ONE PIV-D Manager app.

   c In the PDF that opens in Workspace ONE PIV-D Manager, choose where you want your signature, and select **Sign**.

   Workspace ONE PIV-D Manager prompts users for the keystore PIN or biometric scan based on settings. Users configured this PIN when they activated and imported their derived credential certificates.

   If users enter an incorrect PIN, Workspace ONE PIV-D Manager does not sign the PDF. Users must enter their PIN again. The maximum number of failed attempts is 6.

   d Users have several options to store their signed PDFs.

   - Users can import the signed PDF to another app for saving on their devices.
   - Users can save the signed PDF in Workspace ONE PIV-D Manager for 30 days.

     This option enables users to open another app and import the signed file from Workspace ONE PIV-D Manager during those 30 days.

# Persistent Device Token Extension

The Persistent Device Token Extension, available through the CryptoTokenKit (CTK) framework, is a way to provide credentials for apps that are not a part of the Workspace ONE UEM platform. The Persistent Device Token Extension makes certificates accessible without depending on mobile device management or the managed certificate store.

## Supported iOS and iPadOS versions

The Persistent Device Token Extension is supported on the following versions:

- iOS 14 or later
- iPadOS 14 or later

## Persistent Device Token Extension Overview

The CTK framework includes support for always-available tokens, referred to as persistent tokens. The Persistent Device Token Extension provides responses based on requests from consumer apps. A consumer app might send a request for authentication, signing, encryption, or decryption. The Persistent Device Token Extension processes the request and sends a response without revealing the certificate information. For details on the CryptoTokenKit, see the Apple Developer website.

**Note** Private key material is not exposed to the consumer app when using the Persistent Device Token Extension. Apps might have access to the private key. However, the apps do not have access to private key material.

The Persistent Device Token Extension can be used on managed and unmanaged devices to provide credentials for apps on that device. The Persistent Device Token Extension is available to any app on a device to use for any purpose. For example, a device has Workspace ONE UEM and Safari installed (outside of the Workspace ONE UEM platform). Although Safari is not integrated in Workspace ONE UEM, it can authenticate a website using a credential issued to PIV-D through the Persistent Device Token Extension.

The Persistent Device Token Extension supports YubiKey. For PIV-D Manager and YubiKey information, see PIV-D Manager and YubiKey for iOS.

## Enable the Persistent Device Token Extension

The Persistent Device Token Extension is deactivated by default. Enable or deactivate the token extension on the Application Configuration tab in the PIV-D Manager.

For information on configuring the Persistent Token Extension, see the iOS App Config Key-Value Pairs section of Chapter 2 Send Derived Credentials from the Console to iOS Devices.

## Persistent Device Token Extension Time Out

The Persistent Device Token Extension times out when the PIV-D Manager is not running in the foreground of the device for an amount of time. The default duration of the time out is 24 hours. The duration is configured on the Application Configuration tab in the PIV-D Manager.

PIV-D Manager only receives configuration updates when the app UI is open in the foreground. Persistent Device Token Extension requests can be processed in the background. However, PIV-D Manager does not receive configuration updates (such as enabling or deactivating the token extension) in the background. For example, when the Persistent Device Token Extension is deactivated, the change does not update in the PIV-D manager while it runs in the background. To process configuration updates, run PIV-D manager in the foreground.

## Persistent Device Token Extension Local Notifications

PIV-D Manager uses local notifications to prompt you to open the app when a Persistent Device Token Extension request cannot be processed in the background. For example, a notification with details shows when the Persistent Device Token Extension time out expires. If PIV-D Manager notifications are blocked on a device, then notification details are not shown.

When requests fail in the consumer app, the app might show an error message that does not identify the cause of failure relating to the Persistent Device Token Extension. For example, a browser might show a network connection lost error without referring to the Persistent Device Token Extension failure.

To receive detailed notifications, enable notifications from PIV-D Manager on the device.

# Send Derived Credentials from the Console to Android Devices

3

Add and publish the Workspace ONE PIV-D Manager for Android app to devices as a public app. The app receives the derived credential certificates from the console so that the device can use them.

Procedure

1 Navigate to **Resources > Apps > Native > Public** and select **Add Application**.

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

2 Select **Android** for the **Platform**.

3 To find the application, select **Search App Store** from the **Source** text box.

4 To find the application in the app store, enter **`VMware PIV-D Manager`** in the **Name** text box.

5 **Select** the application from the app store result page.

The **Add Application** window displays. Adding information is optional.

6 To move to the deployment section, select **Save & Assign**.

You assign the app to devices and add optional app config parameters in the deployment section.

7 Select the **Assignment** tab and **Add Assignment**.

8 Enter a group that includes the devices that use your derived credential solution for **Select Assignment Groups**.

9 Optional: Enable **Application Configuration** and enter the listed **Configuration Key** and the **Value** pairs. To insert lines, use the **Add** button.

App config parameters perform some manual configurations for the user on the device but they are not required for Workspace ONE PIV-D Manager to work.

Table 3-1. Common App Config Key-Value Pairs

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| `CertificateExpiryWarning` | String | Your custom warning message for when a certificate is about to expire. | If nothing is manually set, then our default warning message is displayed. |
| `CertificateExpiryWarningPeriod` | Integer | Enable = Any numerical value greater than 0<br>Disable = 0 | The default value is 30 days when nothing is manually set. |
| `ConnectorAppName` | String | | Select an application name that can be used by a back end connector to Workspace ONE UEM.<br>To select a lookup value from the list or enter fixed text such as "VMware PIV-D", click **+**.<br>This configuration key is only supported by the Intercede provider. |
| `ConnectorDeviceIdentifier` | String | | Select a device identifier that can be used by a back end connector to Workspace ONE UEM.<br>To select a lookup value, such as {DeviceUid}, from the list, click **+**.<br>This configuration key is only supported by Entrust and Intercede providers. |
| `EnableEntrustBluetoothLogin` | Boolean | True = On<br>False = Off | When you enable this value, the PIN policy defined in the Entrust system is honored instead of what is defined here. |
| `EnableManualCertificateImport` | Boolean | True = On<br>False = Off | Enables integrations with XTec to import certificates from web browser downloads using the download portal website for customers. |
| `EnablePDF Signing` | Boolean | True = On<br>False = Off | Enables apps like Workspace ONE Boxer or Adobe Acrobat Reader to sign a PDF document using the derived credential in Workspace ONE PIV-D Manager. |

Table 3-1. Common App Config Key-Value Pairs (continued)

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| `PinDisallowDuplicate` | Boolean | True = On<br>False = Off | Setting to **`True`** checks for duplicate characters next to each other in the pin protecting the certificate store. |
| `PinDisallowSequential` | Boolean | True = On<br>False = Off | Setting to **`True`** checks for a sequence of characters going up or down in value (123, 321, abc) in the pin protecting the certificate store. |
| `PinLengthMinimum` | Integer | | The minimum character length for the PIN protecting the certificate store. |
| `PinLowercaseMinimum` | Integer | | The minimum number of lowercase characters for the PIN protecting the certificate store. |
| `PinNumbersMinimum` | Integer | | The minimum number of number characters for the PIN protecting the certificate store. |
| `PinSpecialCharMinimum` | Integer | | The minimum number of special characters for the PIN protecting the certificate store.<br>Supported characters: **`~!@#$%^&*_-+=`\|\(){}[]:;"'<>,.?/`** |
| `PinUppercaseMinimum` | Integer | | The minimum number of uppercase characters for the PIN protecting the certificate store. |
| `PIVDConfig` | Array | 0 = Off<br>1 = On | Workspace ONE PIV-D Manager prompts the end user for an app token from Self Service Portal before letting them proceed with fetching an SDK profile and certificate. This feature only works when the `PIVDProvider` configuration key value is 5 (Workspace ONE UEM). |

Table 3-1. Common App Config Key-Value Pairs (continued)

| Configuration Key | Value Type | Configuration Value | Description |
|---|---|---|---|
| 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. |
| PIVDPromptForPIN | Boolean | True = On<br>False = Off | Workspace ONE PIV-D Manager prompts the end user for the PIN even if you enable SSO. |
| PIVDProvider | Integer | 1 = Entrust<br>2 = Intercede<br>3 = Purebred<br>4 = XTec<br>5 = Workspace ONE UEM<br>6 = YubiKey<br>7 = AuthentX ID | 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. |

Table 3-2. Android App Config Key-Value Pair

| Key | Value Type | Description |
|---|---|---|
| EnableKeyChainInstallation | Boolean<br>True = On<br>False = Off | Enables PIV-D Manager to install credentials directly to the Android Keystore through the Android KeyChain interface on unmanaged devices. |

10 Select **Add** to assign the app to the devices in the assignment group and then save and publish Workspace ONE PIV-D Manager as a managed application.

# Use Profiles to Control How Android (Enterprise) Devices Use Derived Credentials Certificates

Deploy a device profile with a credentials payload to Android devices. The profile gets the certificates from the Workspace ONE PIV-D Manager app so the device can use the certificates to access resources.

The current implementation of Workspace ONE PIV-D Manager for Android does not support native email with derived credentials. It does support using Workspace ONE Boxer with derived credentials.

### Prerequisites

Use the Workspace ONE Intelligent Hub for v19.10 or later for Android (Enterprise) support.

### Procedure

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings.
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 as **Derived Credential**, you cannot add credential sources other than derived credentials to the **Credentials** payload.

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. To associate the derived credential, add a Wi-Fi or VPN payload.

   If you are configuring multiple payloads, consider configuring Wi-Fi and VPN separately instead of one profile containing multiple payloads and multiple derived credentials.

7. Select **Save and Publish**.

### Results

The profile displays as pending in the **Profiles List View**.

### What to do next

At this point, end users install and configure Workspace ONE PIV-D Manager on their Android device and the console pushes down and installs the device profile on the managed Android device. For more information, see Chapter 4 Configure Workspace ONE PIV-D Manager on Devices.

## Use Profiles to Control How Android (Legacy) Devices use Derived Credentials Certificates

Deploy a device profile with a credentials payload to Android devices. The profile gets the certificates from Workspace ONE PIV-D Manager app so the device can use the certificates to securely access resources.

### Procedure

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android (Legacy)**.
2. Configure the profile's **General** settings.
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** payload.

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**.

### Results

The profile displays as pending in the **Profiles List View**.

### What to do next

At this point, end users install and configure Workspace ONE PIV-D Manager on their Android device and the console pushes down and installs the device profile on the managed Android device. For more information, see Chapter 4 Configure Workspace ONE PIV-D Manager on Devices.

# PIV-D Manager and YubiKey for Android

VMware Workspace ONE® PIV-D Manager works with YubiKey. The PIV-D Manager mobile app can sign PDF documents on a mobile device with credentials from a YubiKey accessory.

You can register your YubiKey accessory for use with the PIV-D Manager app on your device by following these instructions.

### Prerequisites

Before you begin, you need the following.

- Enrolled device.

  Enrol1 the Workspace ONE Intelligent Hub and PIV-D Manager apps in the usual way, or by following instructions from your enterprise administrator.

- Accessory with installed credentials.

  Your enterprise administrator may issue you with an accessory on which a suitable credential has already been installed, or may provide you with enrollment instructions, for example. Otherwise, you can install an electronic certificate yourself.

  To install a certificate yourself, you will need the following.

- Suitable management software, for example downloaded from the Yubico website.

- Accessory management keys. YubiKey accessories come configured with default keys. Those can be used unless the accessory has been reconfigured.

- Electronic certificate. The certificate must have the key usages: Digital Signature and Non-Repudiation.

The PIV-D Manager app can be used to check that the certificate is suitable for PDF signing. This is covered in the first set of instructions, How to register an accessory.

Procedure

1 Register your YubiKey Accessory

   a Open the PIV-D app. Opening the app might require you to enter a passcode or authenticate in some other way.

   b Open the product selection screen. The first screen shown by PIV-D could be the product selection screen.

   c Choose Product: YubiKey

   d Follow the on-screen instructions for connecting the accessory, either by USB or NFC. PIV-D only accesses the public details of the certificate at this stage and you won't need to enter the accessory PIN.When the accessory has been accessed, the Certificates screen opens in the PIV-D app. The certificate from the accessory should be listed there.

   Be careful not to trigger Yubico OTP (One-Time Passcode) entry. This may cause the browser app to open. If that happens, return to the PIV-D app and try holding the accessory in a different way, to avoid triggering the OTP.

   e Tap the certificate name and check the attributes are as required. The Subject must show the common name (CN) that you want to appear on signed documents. The Key Usage line must show both Digital Signature and Non-Repudiation.

   If any attributes aren't as required, then a different certificate must be loaded on the accessory. Return to your administrator or generate and install an amended certificate of your own.

2 Signing a document with a Yubikey accessory

   a Ensure that your YubiKey device is registered.

   b Share a signable PDF file with PIV-D.

   c Tap the sign button and confirm if prompted.

d Follow the on-screen instructions for connecting the accessory, either by USB or NFC.PIV-D will accesses the private key of the certificate at this stage and you will be prompted to enter the accessory PIN.

Be careful not to trigger Yubico OTP (One-Time Passcode) entry. This may cause the browser app to open. If that happens, return to the PIV-D app and try holding the accessory in a different way, to avoid triggering the OTP.

e Ensure the signature is filled out correctly

# Sign PDFs with Workspace ONE PIV-D Manager for Android

You can sign PDFs with a PIN, facial recognition, or fingerprint using Workspace ONE PIV-D Manager.

You can share documents with the Workspace ONE PIV-D Manager app to render and show the PDF document. If the PDF document contains a signature element, users can add a digital signature with the `SIGNING` derived credential. Users can save or share the signed documents with other PDF supporting apps using Android Sharesheet.

Workspace ONE PIV-D Manager adds a custom document provider to Android's Storage Access Framework (SAF). Users can access signed PDF documents while in other apps like Workspace ONE Boxer and Adobe Acrobat Reader with SAF.

Signing PDFs with Workspace ONE PIV-D Manager has some limitations.

- Workspace ONE PIV-D Manager uses a single signing certificate that can be used for multiple signatures. It does not support the use of multiple signing certificates for PDF signing.
- The system records that PDFs are signed but it does not validate signatures.

**Prerequisites**

- The PDF must have a signature element (allows digital signing).
- Your deployment must use Workspace ONE PIV-D Manager for Android v20.04 or later.
- The corresponding `SIGNING` certificate in Workspace ONE PIV-D Manager for Android must have the `keyUsage` attribute set for digital signing and non-repudiation.
- Device users need a keystore PIN. Users configure their keystore PINs when they activate and import their derived credential certificates. The keystore PIN is different from the Workspace ONE PIV-D Manager passcode.

**Important** Users get six attempts to enter their PINs. On the sixth incorrect PIN entry, the Workspace ONE PIV-D Manager app wipes all data.

- Facial recognition or fingerprint scanning must be configured on the device to utilize biometric signing.
- Biometric Authentication for keystore also requires SSO to be ON.

Procedure

1 Admins configure the Workspace ONE PIV-D Manager app in the Workspace ONE UEM console.

   a Navigate to **Resources > Apps > Native > Public** and edit the Workspace ONE PIV-D Manager app in the view list.

   b Add the key value pair, `EnablePDFSigning` as a Boolean data type with the value of `true`.

   c (optional) Add the key value pair, EnableBiometricAuthentication as a Boolean data type with the value of true to allow for biometric signing. Adding this value pair gives you the option to enable biometric signing within PIV-D Application Settings.

   d Push the Workspace ONE PIV-D Manager to deploy the PDF signing feature.

2 Users share or import the applicable PDF file into the Workspace ONE PIV-D Manager app for signing on their devices.

   a On their devices, users view the applicable PDF file in one of several ways.

      - Share the PDF from the app that usually renders PDFs, either Workspace ONE Boxer, Workspace ONE Content, or Adobe Acrobat Reader.
      - Import the PDF from the Android Storage Access Framework by selecting **Floating Action Button (FAB)** on the **Signed Documents** page.
      - Open an already-signed PDF in the **Signed Documents** page.

      The PDF opens in the Workspace ONE PIV-D Manager app and displays a **SIGN** button if single signature element is present or asks to select the signature elements if mutiple signature fields are present.

   b In the PDF that is opened in Workspace ONE PIV-D Manager, users select **Sign**.

      Workspace ONE PIV-D Manager prompts users for the keystore PIN. Users configured this PIN when they activated and imported their derived credential certificates.

      If users enter an incorrect PIN, Workspace ONE PIV-D Manager does not sign the PDF. Users must enter their PIN again. The max number of attempts is 6.

   c Users have several options to store their signed PDFs with **Save** and **Share**.

      - **Save** - Selecting this button stores the signed PDF in the Workspace ONE PIV-D Manager app. Users can access the saved document from the **Signed Documents** page. This button also makes the document accessible to all apps from the Storage Access Framework.
      - **Share** - Selecting this button shares the signed PDF with other PDF-apps through Android Sharesheet. This shared PDF is not stored in Workspace ONE PIV-D Manager.

# KeyStore PINs for Android Users

To use some features in Workspace ONE PIV-D Manager for Android, like PDF signing, users need an Android KeyStore PIN. The Workspace ONE PIV-D Manager app now supports setting PINS for all derived credential providers.

KeyStore PIN setting is supported in Workspace ONE PIV-D Manager for Android v1.5 and later.

## Entrust KeyStore PIN

Workspace ONE PIV-D Manager takes the PIN setting criteria from the Entrust Smart Credential. Workspace ONE PIV-D Manager prompts for PIN setting when users update the app and when they get the latest version as a fresh installation.

- Updating the app - After validating the previous PIN,Workspace ONE PIV-D Manager prompts users to change their PINs.
- New app installation - After successfully activating credentials, Workspace ONE PIV-D Manager prompts users to set PINs.

## All Other DC Provider KeyStore PINs

Workspace ONE PIV-D Manager takes the PIN setting criteria from the configured KVPs. For a list of available KVPs and how to configure them, access Chapter 3 Send Derived Credentials from the Console to Android Devices. Workspace ONE PIV-D Manager prompts for PIN setting when users update the app and when they get the latest version as a fresh installation.

- Updating the app - After validating credentials, Workspace ONE PIV-D Manager prompts users to create PINs before it displays the credentials landing page.
- New app installation - After successfully activating credentials, Workspace ONE PIV-D Manager prompts users to create PINs.

# PIV-D Certificate Access for Android

VMware Workspace ONE® integrated authentication supports derived personal identity verification credentials. Electronic certificates for end user authentication can be generated by integrating with a derived credential provider. The certificates can be stored securely on end user mobile devices. Stored certificates can be accessed by applications on the mobile device through the Android Keystore system.

Integrated authentication with derived credentials is configured in the Workspace ONE Unified Endpoint Manager (UEM) console. Identity certificate storage on the device is handled by the Workspace ONE PIV-D Manager mobile application for Android.

Derived personal identity verification credentials (PIV-D) certificate access for Android works as follows.

- Integrated authentication by derived credentials is configured in the UEM.

- The Workspace ONE Intelligent Hub application is installed on end user devices, and enrolled with the UEM.
- The Workspace ONE PIV-D Manager application is also installed on end user devices, and enrolled with the UEM via Hub.
- The PIV-D Manager application is enrolled with a derived credential provider.
- PIV-D electronic certificates are generated and stored on the device.
- Other Android applications on the same device request access to stored certificates through the Android Keystore system. Access is only granted if confirmed by the end user.

### Prerequisites

To integrate PIV-D certificate access into your Android application, ensure you have access to the compatible software versions. The following table shows the earliest supported versions of the applicable Workspace ONE components.

| Software | Available |
|---|---|
| Workspace ONE management console | 19.12 |
| Workspace ONE Intelligent Hub for Android | 19.10 |
| Workspace ONE PIV-D Manager for Android | 1.3 |

**Note** Your application doesn't have to integrate the Workspace ONE Software Development Kit for Android.

### Procedure

1 Console Configuration

An integrated authentication configuration that gives accessible PIV-D identity certificates is setup in the Workspace ONE management console. The following instructions are intended for application developers or other users wishing to try out certificate export. Full documentation can be found in the online help.

a Log in to the management console. The dashboard will be displayed.

b Select an organization group.By default, the Global group is selected.

c Navigate to: Devices, Profile & Resources, Profiles.This opens the Profiles list.

d Either add a new profile, or edit an existing profile, as follows. To create a new profile, select Add, Add Profile, then Android. Enter a name for your new profile. To edit an existing profile, click its label in the list. It must be an Android profile.In either case, a profile editing screen will be displayed.

e Select Credentials and then Configure, then make the following selections: Credential Source: Derived Credentials.Key Usage: Authentication.

f Select Save and Publish to commit your changes to the configuration.This completes UEM configuration.See also the Console User Interface Screen Capture in the appendix to this document.

2 Device Configuration

Configure your developer device as follows. Do this after Console Configuration.

a Install the Workspace ONE Intelligent Hub application, for example from the Google Play store.

b Enroll the Hub application with the UEM configured for derived credentials.

c Install the Workspace ONE PIV-D Manager application.The Hub might automatically install PIV-D Manager, depending on UEM configuration.

d Unless your derived credential provider is Workspace ONE, log in to your derived credential provider's website.The website will require login credentials, a smart card, or some other authentication factor.

e Launch PIV-D Manager, choose your credential provider and follow the provided instructions for enrollment.The outcome should be that PIV-D Manager fetches electronic certificates from the provider.

f Hub will present a notification to request permission to install the certificates from PIV-D.Click on the notification and follow the provided instructions to permit certificate installation to the system secure store.

3 Programming Interface

Use the native Android programming interface to access PIV-D certificates. You can try this out in your application after completing Console Configuration and Device Configuration.

The following interfaces are typically used for access to PIV-D certificates. See the Android developer website for reference documentation and programming guides. Links are given here for convenience.

a KeyChain class.The reference includes a typical sequence of calls, at time of writing. See: https://developer.android.com/reference/kotlin/android/security/KeyChain

b KeyChain.choosePrivateKeyAlias static method.Called to prompt the user to select a certificate.

c KeyChainAliasCallback interface.Implemented to receive the user selection. See: https://developer.android.com/reference/kotlin/android/security/KeyChainAliasCallback

d KeyChain.getPrivateKey and KeyChain.getCertificateChain static methods.Called from the KeyChainAliasCallback.alias callback, to access the credentials data.

e Code Snippet

```
class MainActivity : AppCompatActivity(), KeyChainAliasCallback {
override fun onCreate(savedInstanceState: Bundle?) {
super.onCreate(savedInstanceState)
//....
// Following code will prompt the user to choose a certificate when
// the specified TextView control is tapped.
findViewById<TextView>(textViewID).setOnClickListener {
KeyChain.choosePrivateKeyAlias(this, this, null, null, null, -1, null)
}
}
override fun alias(alias: String?) {
// Add a debugger breakpoint on the next line if you want to
// check the alias string value.
alias?.let {
val privateKey: PrivateKey? = KeyChain.getPrivateKey(
this.applicationContext, alias)
val certificateChain: Array<X509Certificate>? = KeyChain.getCertificateChain(
this.applicationContext, alias)
// The certificateChain object can be used to respond to authentication challenges.
}
}
}
```

**Note** Changes can be made by administrators at any time, for example to the UEM configuration, or to the infrastructure. The following possibilities at least should be handled by your application.

- Your KeyChainAliasCallback alias method receives a null parameter.
- Your response to an authentication challenge is rejected.

## Use Android Purebred as Your Derived Credential Provider

You can use Purebred app credentials that are stored in the Android Keystore to authenticate users to other resources managed in the Workspace ONE UEM console.

A Purebred app stores its certificates with the Android Key Store and it shares the alias information of the certificates with the Workspace ONE Intelligent Hub installed on the device. The Workspace ONE Intelligent Hub uses the alias information when it deploys Workspace ONE UEM console profiles on devices.

With the shared alias information, users can authenticate to email and websites, and they can configure WiFi and S/MIME. You configure this feature by adding a custom setting, app config key-value pair to the default SDK profile assigned to the Workspace ONE Intelligent Hub for Android.

### Prerequisites

- Use the Workspace ONE Intelligent Hub for Android, minimum v19.07.
- This feature works for the Android (Legacy) platform.

### Runtime Permissions - DRAFT INFO PLACEHOLDER

To access Purebred certificates, set runtime permissions. If runtime permissions were previously deactivated, then they must be allowed in the app settings to access the certificates. To update runtime permissions, follow these steps:

1 Access the PIV-D app settings.

2 On the App info screen, select **Permissions**.

3 Select **Additional Permissions**.

4 Select **read alias**.

5 On the read alias permission screen, select **Allow**.

### Procedure

1 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

2 Select **Enabled** for **Custom Settings**.

3 Enter `{"PIVDProvider":"3"}` in the **Custom Settings** text box to identify Purebred as the provider.

4 **Save** your settings.

5 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Intelligent Hub Settings**.

6 Set the **SDK Profile** menu item to the default profile by selecting **Android Default Settings @ Global**.

### What to do next

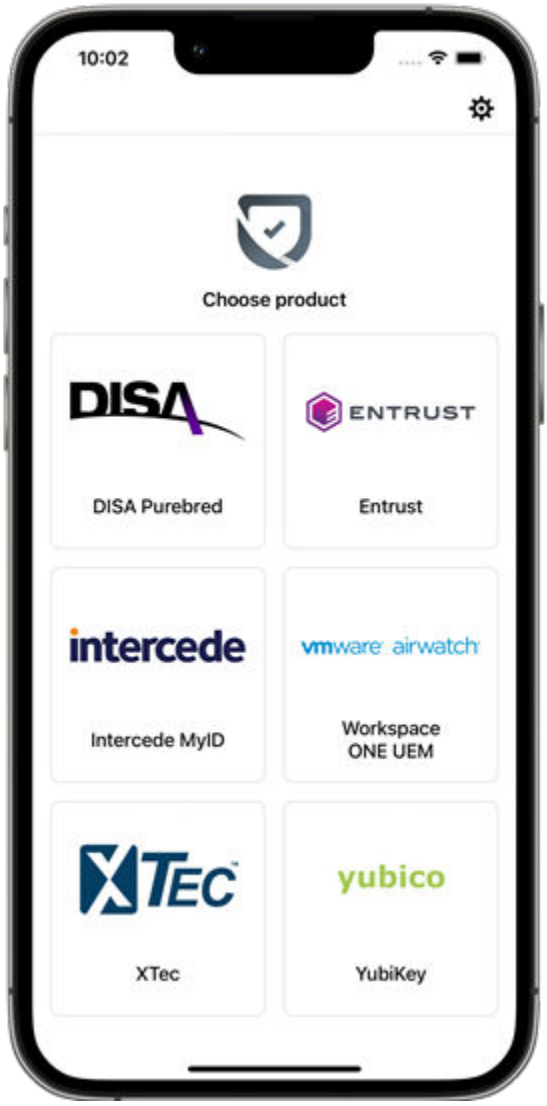
You must deploy a device profile to Android (Legacy) devices with Derived Credentials as the Credentials payload. For information, access Use Profiles to Control How Android (Legacy) Devices use Derived Credentials Certificates .

# Configure Workspace ONE PIV-D Manager on Devices

4

After admins publish the app and deploy the device profile in the Workspace ONE UEM console, users install Workspace ONE PIV-D Manager on their devices.

Users either receive Workspace ONE PIV-D Manager as a managed app or they download it from an app catalog. Administrators can pre-configure the app with app configuration values that show a specific PIV-D provider and optional custom instructions. If no app configuration key value pair (KVP) is set for the `PIVDProvider` parameter, then the app prompts the end user to select a provider when the user launches the app. The available vendors currently supported with the Workspace ONE PIV-D Manager are DISA Purebred, Entrust, Intercede MyID, Workspace ONE UEM, XTec, and YubiKey.




This chapter includes the following topics:

- Install Workspace ONE PIV-D Manager on Devices

# Install Workspace ONE PIV-D Manager on Devices

The process to install Workspace ONE PIV-D Manager on devices is similar on Android and iOS. Following prompts on the device, users configure the app for the derived credential your organization uses for authentication, signing, or encryption.

End users follow these steps on their devices to install Workspace ONE PIV-D Manager.

### Procedure

1 Users enroll the device using the Workspace ONE Intelligent Hub.

2 After the device is enrolled, users tap the prompt to install the Workspace ONE PIV-D Manager. Users can also download the app through the app catalog.

3 Users follow the instructions provided by their admins. Instructions often require users to smart card authenticate to the PIV-D provider self-service portal (SSP).

   If admins did not pre-configure a derived credentials provider with an app config value in the Workspace ONE UEM console, end users must select the provider and follow the configuration steps for the selected provider.

   - DISA Purebred - access How to Configure DISA Purebred.
   - Entrust Identity Enterprise - access How to Configure Entrust Identity Enterprise.
   - Intercede MyID - access How to Configure Intercede MyID.
   - XTec - access How to Configure XTec.
   - Workspace ONE UEM - access How to Configure Workspace ONE UEM CAs.

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

#### Results

After enrollment is complete, the application shows the derived credentials and triggers the installation of any device profiles that use a derived credential.

**Note** Anytime admins update a device profile or create a new one, users must launch the Workspace ONE 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.

## How to Configure DISA Purebred

Set up DISA Purebred derived credentials for your end users' devices managed by Workspace ONE UEM.

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 configuration steps for the selected provider. 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 DoD Cyber Exchange Public.

#### 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 the Signing and Encryption Certificates.

5 Once you import the Authentication Certificate, the Signing Certificate, and the Encryption Certificate, view the certificates from the **Certificate** list view.

## How to Configure Entrust Identity Enterprise

Set up Entrust Identity Enterprise derived credentials for your end users' devices managed by Workspace ONE UEM.

Entrust Identity Enterprise is a commercially off the shelf (COTS) Derived Credentials solution that transforms your mobile device in a virtual smart card for derived credential authentication. You can learn more about it by going to the Entrust website.

### Procedure

1 Start the enrollment process by logging in to the Entrust Identity Enterprise 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 Identity Enterprise 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 Workspace ONE PIV-D Manager app on your iOS device, tap **Scan QR code**, and then enter the one-time password.

### Results

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

## How to Configure Entrust Bluetooth Login

Entrust users can login with Bluetooth to use the Workspace ONE PIV-D Manager app as a virtual smartcard. The app logs in to Windows or Mac desktops and websites that might normally require a physical smartcard for authentication.

### Prerequisites

Users can use the Bluetooth login configuration when they meet following requirements.

- Users have installed the Bluetooth drivers from Entrust on Windows and Mac machines so the devices can pair. Find the drivers at https://trustedcare.entrustdatacard.com.
- The Workspace ONE PIV-D Manager app is enrolled using Entrust as the derived credential provider.

- The admin has set the **EnableEntrustBluetoothLogin** configuration key with a value type of **Boolean** to **true** in the Workspace ONE UEM console when the Workspace ONE PIV-D Manager is assigned.
- If a user is already using PIV-D with Entrust-activated derived credentials, iOS requires the user to reactivate their credentials before they can use Bluetooth login. If the user does not reactivate their credentials, the bluetooth settings do not appear in the app UI.
- Users can reissue a derived credential in Workspace ONE PIV-D Manager 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. Start the Workspace ONE PIV-D Manager app and tap the settings gear icon.
   c. Enable **Bluetooth Login**.
2. Pair Workspace ONE PIV-D Manager with a desktop.
   a. Press the Bluetooth login menu item that displays on the Workspace ONE PIV-D Manager app home page. This action Press begins scanning for nearby devices to pair with or connect to.
   b. Select the desktop to connect to.
   c. If applicable, enter the PIV-D pin and request selection of the certificate to use for authentication.

      This pin is the one created at the time of derived credential enrollment in PIV-D.
3. Log in to a desktop computer or website using Workspace ONE PIV-D Manager.

   Additionally, if the user browses to a website that expects smart card authentication on the desktop, the user can authenticate to the website with the same PIV-D connection.

   If the connection and pin entry are successful, the user is logged in to the desktop.
4. Enable a device to auto-connect by selecting the autoconnect option next to the device name.

   Attempting to auto-connect to another device deactivates the existing auto-connect session.

   After auto-connect is enabled, the Workspace ONE PIV-D Manager app automatically connects to desktops when the device enters Bluetooth range.

## How to Configure Intercede MyID

Set up Intercede MyID derived credentials for your end users' devices managed by Workspace ONE UEM.

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.

## How to Configure XTec

Set up XTec derived credentials for your end users' devices managed by Workspace ONE UEM.

For more information about XTec, access 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 Workspace ONE PIV-D Manager application on your iOS device and tap **Next**.

### Results

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

## Certificates for XTec with Web for iOS Devices

With Workspace ONE PIV-D Manager for iOS with XTec, users can import additional certificates from Workspace ONE Web. This feature allows the use of multiple certificates for different scenarios.

- For details about adding key value pairs (KVPs) to Workspace ONE PIV-D Manager, access Chapter 2 Send Derived Credentials from the Console to iOS Devices.
- For details about adding KVPs to Workspace ONE Web, access Application Configurations for Workspace ONE Web.

### Prerequisites

- Use Workspace ONE PIV-D Manager v1.5.1 or later.
- Use Workspace ONE Web v7.11 or later.

### Procedure

1 Admins add KVPs to the respective apps.

- Add the KVP `EnableManualCertificateImport` to the Workspace ONE PIV-D Manager app as **`true`** in the Workspace ONE UEM console.
- Add the KVP `EnableCertificateShare` to Workspace ONE Web as **`true`** in the Workspace ONE UEM console .

2 On devices, users open Workspace ONE Web, navigate to the applicable certificate, and download it.

3 On devices, users open the certificate in Workspace ONE PIV-D Manager.

4 Users follow the Workspace ONE PIV-D Manager app prompts to import the certificate.

Some certificates have passwords so Workspace ONE PIV-D Manager prompts for this value to decrypt the certificate.

### Results

Workspace ONE PIV-D Manager lists the certificate in the UI and synchronizes the certificate to device profiles configured with derived credentials.

## Import Certificates for XTec on Android

With Workspace ONE PIV-D Manager for Android with XTec, users can manually import additional certificates from any browser. This feature allows the use of multiple certificates for different scenarios.

For details about adding key value pairs (KVPs) to Workspace ONE PIV-D Manager, access Chapter 3 Send Derived Credentials from the Console to Android Devices.

### Prerequisites

Use Workspace ONE PIV-D Manager for Android v1.5 or later.

### Procedure

1 Admins add the KVP `EnableManualCertificateImport` to the Workspace ONE PIV-D Manager app as **`true`** in the Workspace ONE UEM console.

2 On devices, users open a browser, navigate to the applicable certificate, and download it.

3 On devices, users share the certificate with Workspace ONE PIV-D Manager.

4 Users follow the Workspace ONE PIV-D Manager app prompts to import the certificate.

Some certificates have passwords so Workspace ONE PIV-D Manager prompts for this value to decrypt the certificate.

- If Workspace ONE PIV-D Manager does not have an activated credential, then it imports one from XTec. Users set a PIN to use the credential.

- If Workspace ONE PIV-D Manager has an activated credential, then it adds the new credentials to existing credentials. The system maintains the best, supported credential for each type, Authentication, Signing, and Encryption.
- If Workspace ONE PIV-D Manager has an activated credential that is not from XTec, then the certificate import fails.

## How to Configure Workspace ONE UEM CAs

Set up existing certificate authority derived credentials for your end users' devices managed by 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**.

### Results

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